**A Novel Privacy Preserving Physical Layer Authentication Scheme for LBS based Wireless Networks**

D.L. Lavanya#, R. Ramaprabha\*, and K. Gunaseelan\*

*#DRDO-Defence Research and Development Laboratory, Hyderbad -500 058, India*

*\*Anna University, College of Engineering Guindy, Chennai – 600 025, India*

*#E-mail: lavanya@drdl.drdo.in*

**Abstract:** With fast development in services related to Location Based Service (LBS) gain more importance amongst all the mobile wireless services. In-order to avail the service in LBS system, information about the location and identity of the user has to be provided to the service provider. Service provider confirms the user’s authentication and location for providing services. In general sharing location information and preserving the user’s privacy is highly challenging task in conventional techniques. To resolve these challenges in authenticating the users, retaining users’ privacy, a new SVD based Privacy Preserved Location Authentication Scheme (SPPLAS) has been proposed. In this proposed method, 128 bits authentication key is generated using physical layer signatures such as CSI(Channel state information),CFO(Carrier frequency offset) and SVD(singular value decomposition) and the MAC is encrypted using authentication key and shared to service provider for the users’ location and identity verifications. Users' privacy is protected as well as users' location information is verified during the handshake phase itself before providing the service. The performance of the proposed scheme is evaluated in terms of BMR (Bits Mismatch Rate), Leakage and BER (Bit Error Rate). The simulation results show that our scheme achieves better robustness and security than the existing location based authentication techniques.

***Keywords: Physical Layer Security, Authentication, Privacy, Location Based Service, Channel State Information, Wi-Fi Networks.***

1. **Introduction**

Wi-Fi hotspots in public places are the most attractive feature of mobile networks which has boomed the development of Location Based Service (LBS). LBS system consists of mobile users (MUs), service providers (SPs) and trusted access points (APs). To avail a specific service, the user has to provide the location information and identification i.e. MAC (Media Access Control) address, to SP through AP. User request service to AP and SP provides requested service by authenticating the user through APs.

Location based services are the most widely used applications which help the MUs with services like maps, nearby places, tracking and so on. But, apart from aiding their comfort, it puts users' privacy at stake. These services are provided to the users after the process of authentication based on their location. As is known, authentication is the process of ensuring the legitimacy of the users before providing service, by correlating the user identity of the incoming request with a set of already available users' credentials. Different systems may use different types of credentials to ascertain a user's identity like device free localization1. Location-based authentication is another procedure to prove an individual's identity by detecting its physical presence at a distinct location. Location-based services use real-time geo-data from a mobile device or smart phone to provide the service. The MUs have to provide their location information to SP for availing the services. Since SP is potentially untrustworthy, an adversary who has compromised the SP can easily obtain user's identity and thereby obtain sensitive information about the user such as home location, health, lifestyle, etc. In some cases, to facilitate SP in the process of localization of users, large numbers of AP are required. Untrusted Wi-Fi access points randomly collect location information. Due to the broadcasting nature of wireless, adversary can easily collect the location data of the target user by eavesdropping through access points. Thus despite various advantages, LBS pose severe privacy threat to the user. Even though the location information can be secured using encryption techniques, these techniques don’t prove to be energy-efficient. Another solution to alleviate this problem is relying on external devices and hardware assisted location authentication, but it leads to complexity and high capitation cost.

To mitigate the privacy threat in availing the location based service, authentication of users' location preserving their privacy is indispensable. Physical layer security, which exploits physical layer properties like CSI and carrier frequency offset (CFO), is a promising paradigm to provide energy-efficient security solutions and enhance the security performance of wireless communication systems2. Utilization of channel based physical layer security converts the open nature of a wireless channel into advantageous feature. Physical layer security holds different types of wireless security techniques, in which location authentication is achieved by physical layer signatures3-4. Authentication based on time varying CFO5 was discussed in a work wherein Kalman filtering is applied on estimated CFO for tracking the current CFO. In another work, a CSI based indoor localisation technique6 was proposed. Bringing out the limitations in RSS estimation for localization, an approach exploring frequency diversity of the subcarriers called FILA was proposed in this work to improve localization accuracy. Further fine grained localization work using array track7 is analysed for a MIMO system. In another work called APPLAUS8, a methodology to verify the location proof of the users maintaining their privacy, was discussed. Non-cryptographic location authentication system9 was proposed which uses small femto cells in addition with access points.

Contemporary literatures affirm 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. In one such literature, a technique called PRILA2 is used to provide location authentication and privacy preservation by CSI and CFO, obtained via Wi-Fi preambles. Generally, CFO and multipath are considered to be detrimental, while this method leverages them for authentication and privacy-preservation. In this case, physical layer security is established by exploiting hardware impairments. Taking advantage of the channel reciprocity property, this method uses CFO together with CSI to generate CFO patterns that are exclusively known by the transmitter/receiver pair. A secrete key is generated by two layer differential coding (TLDC). To enable authentication without performing localization, this method leverages users’ multipath profiles, which can be extracted from CSI using multiple antennas. The CFO encryption technique proposed in this paper uses channel reciprocity for encryption like that of the several recent efforts10-12.

In order to further improve the performance of this technique in terms of authentication and privacy, in our proposed method called SPPLAS, we have explored the generation of secrete key from singular values obtained by application of SVD on CSI, instead of two layer differential encoding used in PRILA2. The physical signatures of Wi-Fi preambles are used to protect the privacy and location information of the user. This technique allows LBS provider to authenticate and to protect the information even during handshake phase against eavesdropper. The overall performance of our SPPLAS method outperforms the two layer differential encoding method proposed in PRILA2.

The main contribution of this paper is summarized below:

* LBS system with adversaries and the influence of hardware impairments in providing physical layer security are modelled and analysed.
* A new SVD based privacy preserving physical layer authentication scheme for LBS based wireless networks is proposed, implemented and analysed their performances.
* The secret key generation algorithm using SVD and encryption method using CFO ensures location authentication and preserves user’s privacy.
* The proposed method provides significant improvement in terms of BMR, Leakage and BER when compared to the existing method2

1. **System Model**

LBS system model consists of MU, trusted AP, LBS provider and adversaries, as depicted in Fig.1. Service to the user is provided by a LBS provider through trusted AP upon receiving the location information and ID from user. Trusted APs are connected to LBS servers via secured backhaul. User's ID is generally assumed to be user's MAC address or any other ID that can be inferred from MAC address. Service provider checks the truthfulness of the user's reported location and identification. Subsequent to the confirmation of the user's details as authenticated, LBS provider offer services to the user via trusted AP.

Adversaries can be either compromised MUs or external nodes of a Wi-Fi network. Adversaries are assumed to be computationally empowered to eavesdrop and analyse all the frames communicated between user and AP. To increase the complexity of the model, it is assumed that adversaries have multiple antennas and such multiple adversaries are present in the network. Multiple adversaries work together to collect location information using existing localization techniques based on Angel of Arrival13 or other physical layer parameters. Most of the prior physical layer security techniques14-16 are intended to protect only the data frames after the handshake phase and fails to secure the identity (MAC address) of the user. Hence adversaries track the handshake frames and identify the user identity from header and CSI from Wi-Fi preambles.

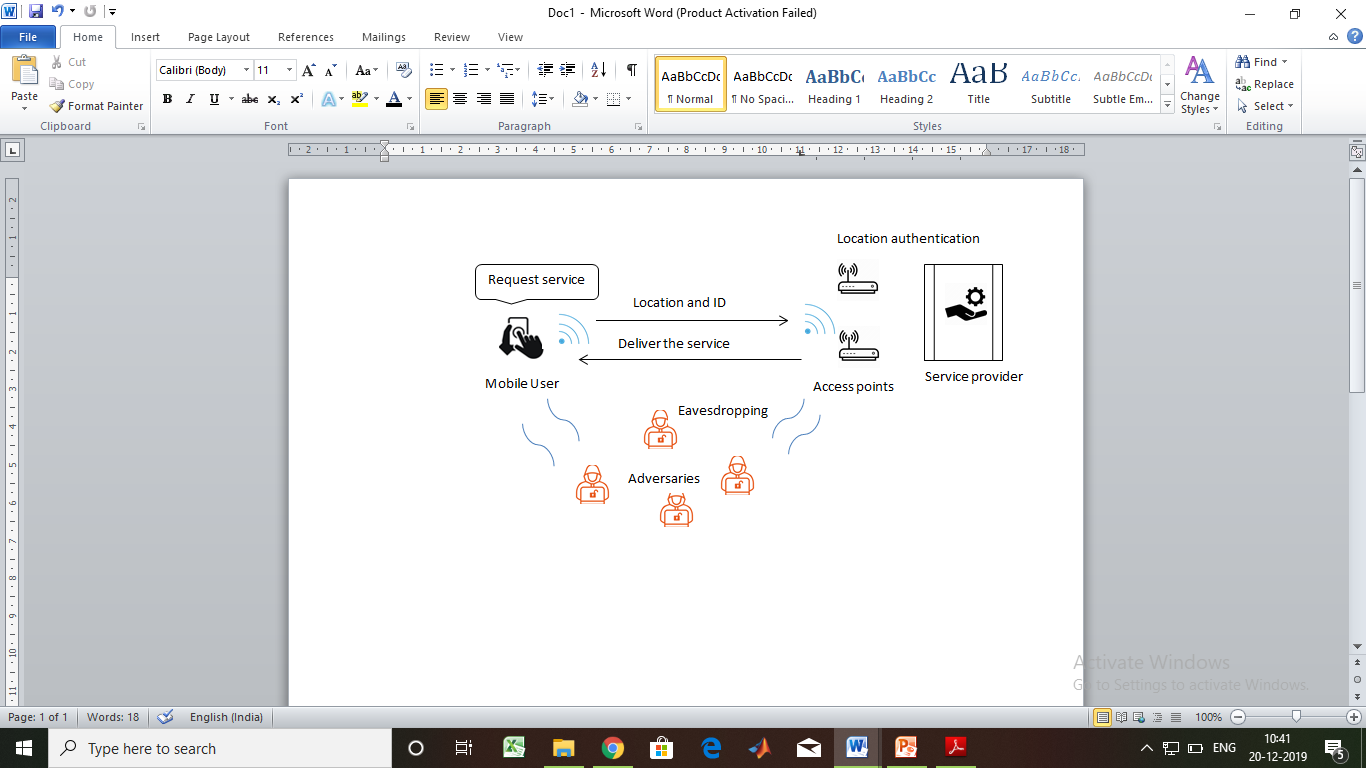


Figure1**.** LBS system architecture

* 1. **Hardware impairments**

Apart from the non-ideal channel and noise, hardware parts of the receiver also degrade the baseband receiver performance. Such hardware non-idealities which influence the baseband receiver are CFO, sampling clock offset, power amplifier phase noise, to name a few. In this paper, CFO is used as a physical layer parameter for incorporating security.

In a typical wireless communication, the signal to be transmitted is up-converted to a high frequency carrier before transmission. CFO occurs when the carrier signal contained in received signal is not synchronized with local oscillator signal used for down conversion at the receiver. This may be due to mismatch in transmitter carrier frequency and receiver carrier frequency or due to Doppler Effect when the transmitter or receiver is moving. Due to this, the received baseband signal is centred at, instead of DC (0 Hz), where (1)

The received baseband signal r(t) is represented as

(2)

Where x(t) is transmitted signal and Fs is sampling frequency.

In case of single carrier,

(3)

(4)

Where A(t) and θ(t) are magnitude and phase of the received signal.

**3. Proposed SPPLAS**

The aim of the proposed method is to facilitate the LBS provider to authenticate user’s location with maintaining user's location privacy, using physical layer signatures. This can be achieved by encrypting all the data transmission frames right from handshake frames. The novelty of the proposed method lies in the generation of the secret key used for encryption. The secret key is generated by SVD of the CSI obtained from the handshake Wi-Fi preambles.

The flowchart of the communication protocol between MU and LBS provider as per the proposed method is shown in Fig. 2. Firstly, the MU requests service from LBS provider by establishing a handshake. During this ‘session initialisation’ process, handshake frames are exchanged between the LBS provider and MU. From these frames, they both extract CSI information and CFO from their respective handshake frames. SVD of CSI is done to generate a secret key for encryption process using CFO injection.

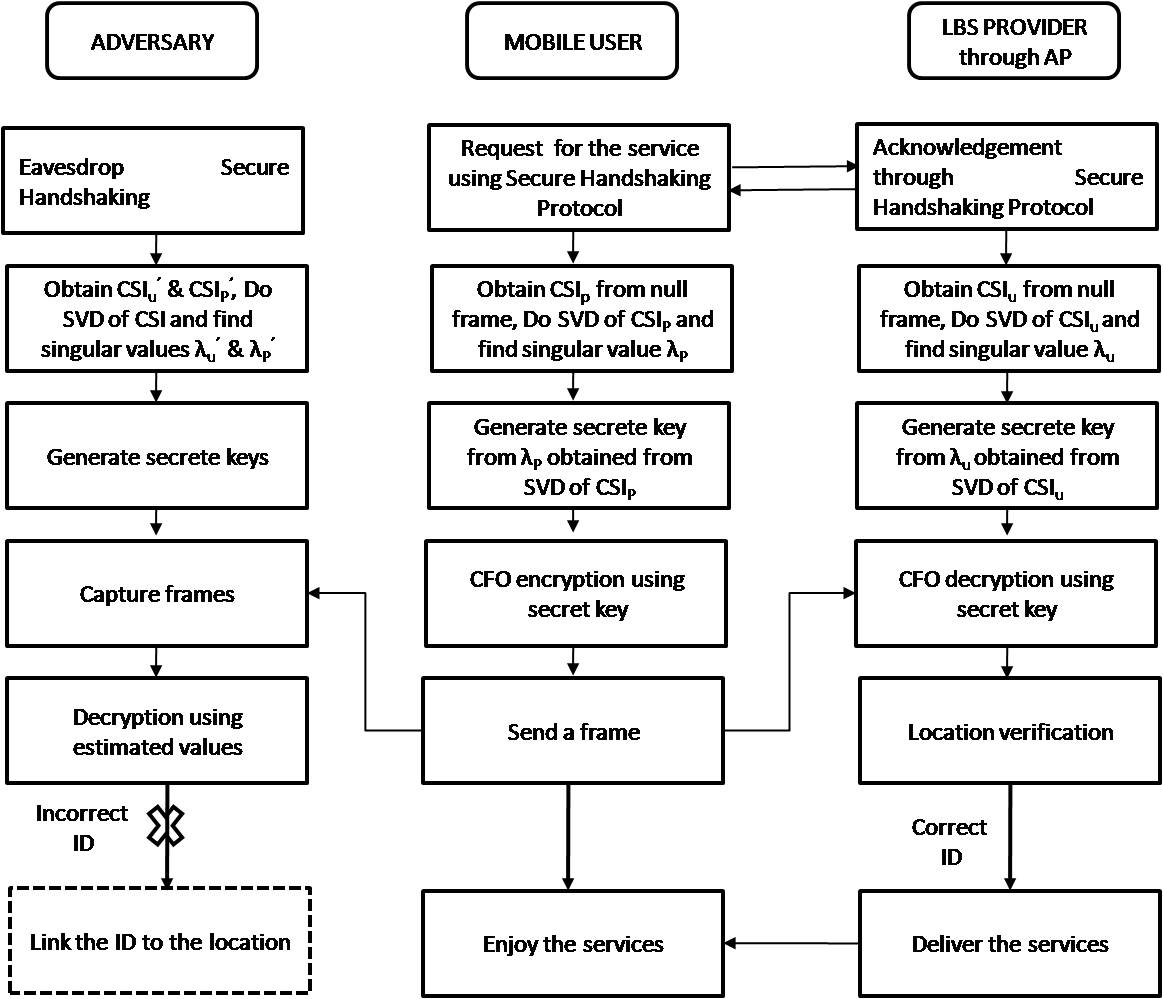


Figure2. Flowchart of the SPPLAS

Subsequent frame of the user, containing the details of MAC address and location information, are encrypted using the generated secret key and CFO injection before transmission. After receiving the encrypted frame, the LBS provider decrypts the frame by secret key & CFO injection, obtained using CSI and CFO extracted during handshake phase. The LBS provider thus extracts the user’s identification and location information from received encrypted frames

**3.1 Secure Handshake Phase**

Adversaries collect the location information of user from the frame sent by user during handshake phase. In order to protect the MAC address of the user from adversaries during handshake phase, a secured handshake phase protocol is being followed, as shown in Fig.3. First, MU sends a NULL request frame to LBS provider. In this request frame, the source address is set as ‘NULL’. From this frame, LBS provider extracts the CSIu and CFO information of user from preamble, applies SVD on CSIu and calculates eigen value λu from matrix CSIu. At LBS server, for every user *u*, a mapping of *λu  CSIu*, CFO is maintained. Subsequently LBS provider sends an acknowledgement (ACK) frame to MU, where user gets MAC address, CSI information of LBS provider CSIp and applies SVD on CSIp and calculates λp. Secret key is generated from λp obtained by applying using SVD on CSIp. Later, user encrypts and transmits all the frames including header and payload with generated secret key and CFO. Due to reciprocal property of wireless channel, channel information of both user and LBS provider will be identical. Though adversaries eavesdrop all the frames between user and LBS provider link, they cannot decrypt the frame correctly because the estimated λp', λu', CSIu' and CSIp' are not identical with their real counterparts. Consequently, the user’s privacy is protected and localization by adversaries is prevented.

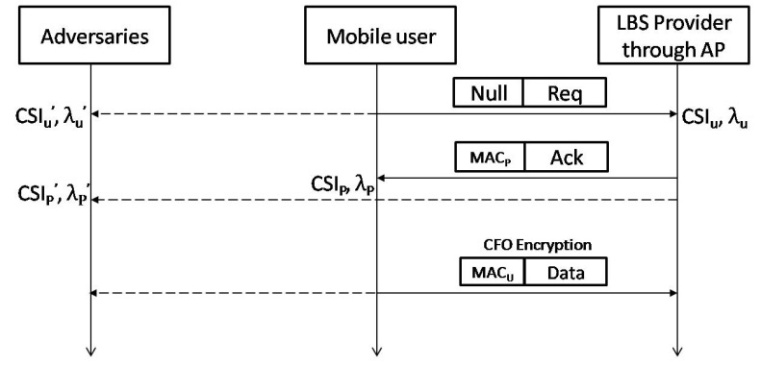


Figure3. Secure handshake protocol

**3.2 Secret Key Generation and CFO encryption**

The crux of the secret key generation lies in exploiting the reciprocity nature of the wireless channel. Ideally, the estimated CSIs at transmitter and receiver should be identical but it is not so due to various reasons. Practically it would be the distorted version of the one estimated by other side. To protect the maximum information available in CSI curve, SVD encoding scheme is deployed.

The proposed coding scheme extracts singular values of CSI matrix using SVD and maps it to a predefined pattern to generate the 128 bits secrete key for authentication. After the handshake phase, MU and SP independently performs Algorithm to generate secret key. Formally, singular value decomposition of H matrix is the factorization of the form where U and is unitary matrix, is diagonal matrix with non-negative real numbers on the diagonal. The diagonal values of λi (where i= {0…. p}) are the singular values of matrix H. Each singular value of matrix is converted to binary and concatenated to generate secret key of size 128. If converted bits are less than the required bit size then same singular values are repeated to get required size. If converted bits exceed the required key size, then only dominant singular values are considered to generate secret key *K*. After generating secret key *K*, we leverage *K* to form vector pattern of length L and convert each vector pattern to decimal value. The CFO vector is determined by multiplying CFO with decimal values. For each symbol in frame, we inject jth CFO vector to ith symbol, where. Since *K* is the secret key available only with user and provider, the adversaries obtain no knowledge about the generated CFO vector.

***ALGORITHM: Secrete Key generation and encryption using SVD & CFO***

**Secrete Key generation**

Initialize secret Key *K*= [ ];

Input: CSI vector length N, Size of H Matrix

Step1: Obtain the CSI vector [];

Step2: Reshape CSI vector of length p into Matrix H of dimension m x n; []

Step3: Compute SVD for channel matrix by decomposing H into U VH

Where p=min {m, n}

Step 4: Arrange non-negative real numbers of diagonal matrix into singular value vector

Step 5: Convert each singular value into binary bits and append corresponding bits to Key *K;*

Output: Secret key *K*

***Encryption***

Input: Secret key *K*; estimated CFO; number of symbols in the frame S, length L;

Step4: Reshape secret key *K* into vector of length L;

Step5: Convert binary bits of each generated vector into decimal value;

Step6: Generate CFO vectors by multiplying decimal values with;

Step6: For each S, Compute the index j of CFO used for encryption using;

Step7: Inject the jth CFO value to the ith symbol;

Output: Encrypted frame

**4. Simulation results**

The performance evaluation of the proposed method is carried out through Matlab simulations. Three nodes were considered for the simulation process – MU, SP and adversary. Adversary acts as a passive eavesdropper who tries to decode the user’s frame for localization purpose. The performance of the proposed method was evaluated using three performance metrics namely, leakage, BMR and BER. Leakage is the ratio of matched bits between the sender, either MU or SP, and the adversary. It measures the amount of information learned by adversary. An encryption scheme with low leakage is more secured.

To validate the security level provided by our method, simulations were carried out assuming a fixed distance of 5 m between MU and SP while the adversary is placed at various distances apart from the sender. Information leakage to the adverasy in both the methods, during communication between user and provider, at various distances as a function of SNR is shown in Fig.4. It can be observed that in both the methods, more information is leaked to the adversary who is at shorter distance for obvious reasons; nearer adversary shares more similar multipath profiles and channel responses with user and provider. As the distance increases the leakage decreases. Comparing both the results, it can be vivivdly seen that our proposed methtod of encryption with SVD outperforms TLDC method proposed in PRILA2, for shorter as well as longer distances.



Figure4. Information leakage to the adversary at various distances.

Second performance metrics is the BMR, which is the ratio of number of mismatching bits between the secrete keys generated independently at user and provider to the total number of bits in secrete key. This measures the robustness of encryption scheme and a low BMR is always preferred.





Figure5(a). BMR of existing method for different bucket size

Figure5(b). BMR of proposed method for different SVD matrix size

Figure5. Bits Mismatch rate of existing and SPPLAS method

Fig. 5(a) shows the BMR, for different bucket size, for the TLDC method proposed in PRILA2.This method achieves low BMR when the number of buckets is not more than 5. The reason is that when the number of buckets is large, the entropy of bucket is quite small, implying low uncertainty in the bits generated by buckets. Hence, for large number of bucket size, the mismatch rate is high leading to low security level. Towards verfying the robustness of our proposed method, its mismach rate is ploted against different SVD matrix size as shown in Fig. 5(b). Matrix size of our methtod is the counter part to bucket size of method proposed in PRILA2.



Figure6. BER performance of the system for 4 QAM

It can be seen that the variation in BMR with respect to matrix size is not significant in our proposed method. But the mismatch rate of PRILA2 is growing higher when bucket size is increasing whereas mismatch rate in our method is persistently low which is preferred.Further the BER performance of both the methods are compared. In this performance analysis, the effect on decoding performance, with and without of CFO encryption, is ascertained. Quardrature amplitude modulatiton (QAM) of different levels were considererd for this analysis. Fig. 6 shows the BER performance of the system without any encryption and with two methods of encrption for 4 QAM. It can be seen that CFO encryption based on PRILA2 and our method has little impact on decoding performance.This slight difference in decoding performance is caused by CFO mismatch measured by the user and provider. Hence, for lower order QAMs, the BER performance with CFO encrption based on PRILA2 and our method are similar and shows comparable BER.



Figure7. BER performance of the system for 64 QAM

Fig. 7 shows the BER performance of the system without encryption and with two methods of encryption for 64 QAM. As the order of QAM increases, CFO encryption based on our method performs better than PRILA2 by achieving better BER performance.

**5. Conclusion**

A new location authentication method preserving user's privacy in LBS based wireless networks, using physical layer signatures has been proposed and analysed in this paper. In this method, inherent CFO and CSI (SVD) are extracted from Wi-Fi preambles to preserve users' location information. Our proposed scheme, CFO encryption using SVD is compared with its counterpart, CFO encryption using TLDC. The performance of the proposed scheme is analysed through suitable evaluation metrics. These performance evaluations suggests that our scheme preserves location privacy and can be implemented to existing LBS systems with slight upgradation. Our proposed scheme which exploits SVD on CSI to generate key, achieves better security and robustness than the prior techniques.

***References***

1. Nasrullah Pirzada, Yunus Nayan, Fazli Subhan & Mohd Fadzil Hassan, Design of an indoor localization system using device-free localization technique. *IEEE International Conference on Control System, Computing an Engineering (ICCSCE*), 2012, 23-25.
2. Wei Wang, Yingjie Chen, & Qian Zhang, Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures. *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, 2016, **15**(2), 1218-25
3. Yi.-Sheng Shiu, Shih Yu Chang, Hsiao Chun Wu, Scott C.-H. Huang & Hsiao-Hwa Chen, Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communication,* 2011, **18**(2), 66-74.
4. Dan Shan, Kai Zeng, Weidong Xiang, Paul Richardson & Yan Dong, PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks. *IEEE Journal on Seected Areas in Commun*ication, 2013, **31**(9), 1817-27.
5. Weikun Hou, Xianbin Wang, Jean-Yves Chouinard & Ahmed Refaey, Physical layer authentication for mobile systems with time-varying carrier frequency offsets. *IEEE Transaction on Communications*, 2014, **62**(5), 1658-67.
6. Kaishun Wu, Jiang Xiao, Youwen Yi, Dihu Chen, Xiaonan Luo, & Lionel M. Ni, CSI-based indoor localization. *IEEE Transactions on Parallel and Distribution Systems*, 2013, **24**(7), 1300-09
7. Jie Xiong & Kyle Jamieson, Array track: A fine-grained indoor location system. Proc. USENIX Symposium on Networked Systems Design and Implementation, 2013, 71-84.
8. Zhichao Zhu & Guohong Cao, Toward privacy preserving and collusion resistance in a location proof updating system, *IEEE Transactions on Mobile Computing,* 2013, **12**(1), 51–64.
9. Jack Brassil, Pratyusa K. Manadhata, & Ravi Netravali, Traffic signature-based mobile device location authentication, *IEEE Transactions on Mobile Comput*ing 2014, **13(**9) 2156–69.
10. Christina Popper, Nils Ole Tippenhauer, Boris Danev & Srdjan Capkun, Investigation of signal and message manipulations on the wireless channel,*Proceedings of European Symposium on Research in Computer Security*, 2011, 40–59.
11. Yue Qiao, Kannan Srinivasan, & Anish Arora, Puzzle: A shape-based secret sharing approach by exploiting channel reciprocity in frequency domain, *USENIX Symposium on Network System Design and Implementation (NSDI),* 2014, 1–14.
12. Sriram Nandha Premnath, Suman Jana, Prarthana Lakshmane Gowda, Mike Clark, Sneha Kumar Kasera, Neal Patwari & Srikanth V. Krishnamurthy. Secret key extraction from wireless signal strength in real environments, *IEEE Transactions on Mobile Computing* 2013, **12**(5), 917–30.
13. Hongbo Liu, Jie Yang, Yan Wang, Yingying Chen, & Can Emre Koksal, Group secret key generation via received signal strength: Protocols, achievable rates, and implementation, *IEEE Transactions on Mobile Computing,* 2014, **13(**12), 2820– 35.
14. Kang G. Shin, Xiaoen Ju, Zhigang Chen & Xin Hu, Privacy protection for users of location-based services, IEEE Wireless Communications, 2012, **19**(1), 30–39.
15. Chi-Yin Chow, Mohamed F. Mokbel, & Tian He, A privacy-preserving location monitoring system for wireless sensor networks. *IEEE Transactions on Mobile Computing*, 2011, **10**(1), 94–107.
16. Xiang-Yang Li & Taeho Jung, Search me if you can: Privacy-preserving location query service, *IEEE INFOCOM,* 2013, 2760–68.