Defence Science Journal, Vol. 71, No. 2, March 2021, pp. 241-247, DOI : 10.14429/dsj.71.15355

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, Hyderabad - 500 058, India*
[#]*Anna University, College of Engineering Guindy, Chennai - 600 025, India*
[*]*E-mail: lavanya@drdl.drdo.in*

ABSTRACT

With the fast development in services related to localisation, location-based service (LBS) gains more importance amongst all the mobile wireless services. To avail the service in the LBS system, information about the location and identity of the user has to be provided to the service provider. The service provider authenticates the user based on their identity and location before providing services. In general, sharing location information and preserving the user's privacy is a highly challenging task in conventional authentication techniques. To resolve these challenges in authenticating the users, retaining users' privacy, a new SVD (singular value decomposition) based Privacy Preserved Location Authentication Scheme (SPPLAS) has been proposed. In this proposed method, physical layer signatures such as channel state information (CSI) and carrier frequency offset (CFO) are used for generating secret key required for encrypting the user's location and identity information, and thus encrypted user's information is sent to service provider for authentication. Secret key is generated by applying SVD on CSI vector. The proposed scheme aids in authenticating the user through location information while protecting the user's privacy. The performance of the proposed method is evaluated in terms of bit mismatch, leakage and bit error rate performance of receiver and adversary. The simulation results show that the proposed scheme achieves better robustness and security than the existing location-based authentication techniques.

Keywords: Authentication; Channel state information; Location based service; Physical layer security; Privacy; Wi-Fi networks

1. INTRODUCTION

Wi-Fi (wireless fidelity) 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 like MAC (media access control) address, to SP through AP. User request service to SP through AP and SP provides requested service by authenticating the user through APs.

LBS are the most widely used applications that help the MUs with services like maps, nearby places, tracking. 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 user's identity like device-free localisation[1]. Location based authentication is another procedure to prove an individual's identity by detecting its physical presence at a distinct location. LBS 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 the 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 localisation of users, large numbers of AP are required. Untrusted Wi-Fi APs randomly collect location information. Due to the broadcasting nature of wireless, an adversary can easily collect the location data of the target user by eavesdropping through access points. Thus, despite various advantages, LBS pose a 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 by 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 LBS, authentication of users' location preserving their privacy is indispensable. Physical layer security, which exploits physical layer properties like channel state information (CSI) and carrier frequency offset (CFO), is a promising paradigm to provide energy-efficient security solutions and enhance the security performance of wireless communication systems[2].

Received : 07 January 2020, Revised : 09 February 2021
Accepted : 11 February 2021, Online published : 10 March 2021

Utilisation of channel-based physical layer security converts the open nature of a wireless channel into an advantageous feature. Physical layer security holds different types of wireless security techniques, in which confidentiality and location authentication is achieved by physical layer signatures[3-5]. Device authentication by extracting visibility graph features of carrier frequency offset was discussed in a work[6]. In another work, a CSI based indoor localisation technique[7] was proposed. Bringing out the limitations in received signal strength estimation for localisation, an approach exploring frequency diversity of the subcarriers called FILA was proposed in this work to improve localisation accuracy. Further fine-grained localisation work using array track[8] is analysed for a multiple input multiple output (MIMO) system. In another work called APPLAUS[9], a methodology to verify the location proof of the users maintaining their privacy was discussed.

A privacy preserving authentication for vehicular ad hoc network (VANET) is discussed using block chains[10]. Private block chains and public block chains are used in this scheme for authenticating the identity information when a vehicle joins a network for the first time. In another scheme of privacy preserving authentication for sharing security information between vehicles and infrastructure in VANET[11], a road side unit which can verify multiple messages has been proposed. In this scheme mainly it is focused to reduce the authentication time. In another security scheme, a mutual authentication scheme based on mix-content based pseudonym[12] which avoids sneaking of attack vehicles in to a VANET system is discussed. A survey on different privacy preserving authentication schemes has been carried out in detail[13]. The challenges and approaches in privacy preserving authentication for internet of things (IoT) have been discussed[14].

Contemporary literatures affirm that privacy-preserving location authentication can be established in a Wi-Fi-based LBS system by exploiting the physical layer signatures obtained from Wi-Fi preambles. In one such literature, a technique called privacy preserving location authentication (PriLA^2) is used to provide location authentication and privacy preservation by CSI and CFO, obtained through Wi-Fi preambles. In general, multipath and CFO are considered to be disadvantageous, but in this method, these are leveraged for achieving authentication and privacy. In this case, physical layer security is established by exploiting hardware impairments. Taking advantage of the channel reciprocity property, this method uses CFO along with CSI to extract CFO patterns that are known only to the transmitter/receiver pair. Two-layer differential coding (TLDC) technique is used to generate secret key. This method leverages users' multipath profiles obtained for CSIs of multiple antennas to provide authentication instead of localisation process.

To further improve the performance of this existing technique in terms of authentication, complexity and privacy, a security scheme named as SPPLAS (SVD (Singular Value Decomposition) based Privacy Preserved Location Authentication Scheme) has been proposed where a secret key is generated from singular values obtained by application of SVD on CSI, instead of TLDC used in PriLA^2. This technique allows LBS providers to authenticate and to protect the information even during the handshake phase against eavesdropper. The overall performance of SPPLAS method outperforms the existing PriLA^2 method.

The main contribution is summarised below:

- LBS system with adversaries and the influence of hardware impairments in providing physical layer security are modelled and analysed.
- A novel method called SPPLAS, an SVD based privacy preserving physical layer authentication scheme for Wi-Fi based LBS networks is proposed and its performance is analysed.
- In this method, the secret key generation algorithm using SVD and encryption method using CFO ensures location authentication and preserves user's privacy.
- The proposed method provides a significant improvement in terms of leakage, bit mismatch rate and bit error rate as compared to the existing method.

2. SYSTEM MODEL

LBS system model consists of MU, trusted AP, LBS provider or service provider and adversaries, as depicted in Fig. 1. Service to the user is provided by an LBS provider through trusted AP upon receiving the location information and identity (ID) from the user. Trusted APs are connected to LBS servers through a secured backhaul. The user's ID is generally assumed to be the user's MAC address or any other ID that can be inferred from the MAC address. The service provider checks the truthfulness of the user's reported location and identification. After the confirmation of the user's details as authenticated, the LBS provider offers services to the user through 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. Also, it is assumed that the procedure for key generation and encryption is open to adversaries. Multiple adversaries can work together to collect location information using existing localisation techniques based on the angle of arrival[15] or other physical layer parameters. Most of the prior physical layer security techniques[16-19] are intended to protect only the data frames after the handshake phase and fail 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.

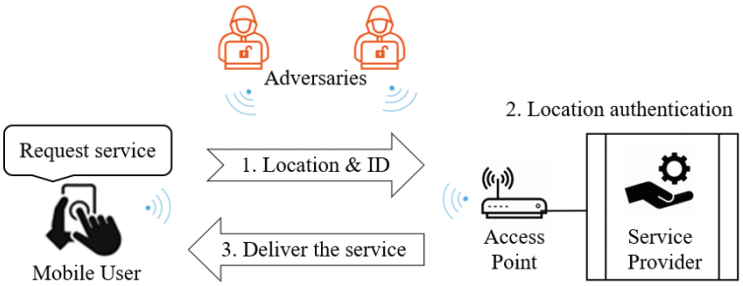

Figure 1. LBS system architecture.

2.1 Hardware Impairments

Apart from the non-ideal channel and noise, hardware parts of the receiver also degrade the baseband receiver performance. Such hardware impairments which influence the baseband receiver are CFO, sampling clock offset, power amplifier phase noise and so on. In this research work, CFO is used as a physical layer signature for incorporating security.

In a wireless communication system, the signal is up-converted to a high frequency carrier signal before transmission. CFO occurs when the carrier signal contained in the received signal is not synchronised with the local oscillator signal used for down conversion at the receiver. This may be due to mismatch in transmitter carrier frequency f_{ctx} and receiver carrier frequency f_{crx} or due to Doppler Effect when the transmitter or receiver is moving. Due to this, the received baseband signal is centred at Δf, where

$$\Delta f = f_{ctx} - f_{crx} \tag{1}$$

The received baseband signal $r(t)$ is represented as

$$r(t) = x(t).e^{j(2\pi\Delta ft/F_s)} \tag{2}$$

where $x(t)$ is transmitted signal and F_s is the sampling frequency. In the case of a single carrier, the received signal with magnitude $A(t)$ and phase $\theta(t)$ is represented as,

$$r(t) = A(t).e^{j\theta(t)}.e^{j(2\pi\Delta ft/F_s)} \tag{3}$$

$$r(t) = A(t).e^{j\left[\theta(t)+\left(\frac{2\pi\Delta ft}{F_s}\right)\right]} \tag{4}$$

3. PROPOSED SPPLAS

The proposed method aims to facilitate the LBS provider to authenticate the user's location while maintaining the 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 and CFO information from their respective handshake frames. SVD of CSI is performed to generate a secret key for encryption process using CFO injection. The subsequent frame of the user, containing the details of MAC address and location information, is encrypted using the generated secret key and CFO injection before transmission. After receiving the encrypted frame, the LBS provider decrypts the frame by performing the reverse operation using the secret key and CFO. The LBS provider thus extracts the user's identification and location information from received encrypted frames. This information of the user is compared with the existing credentials at SP and verified. Subsequent to successful authentication, service is provided to the user.

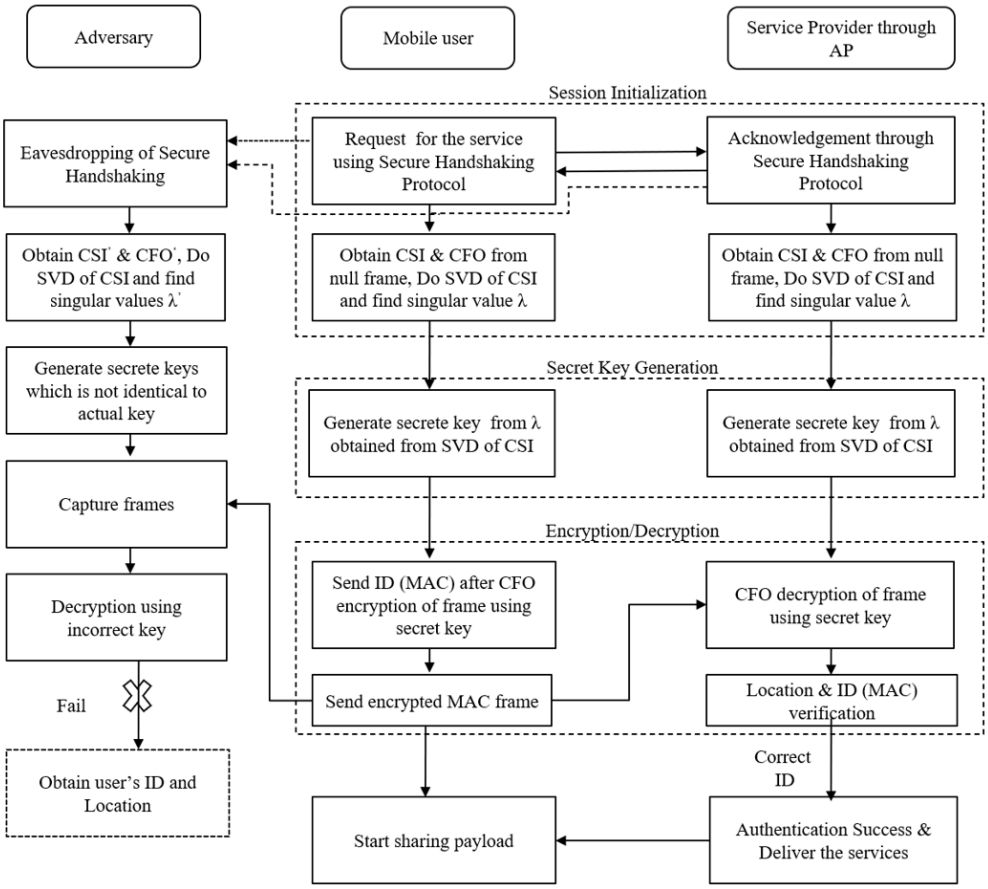

Figure 2. Flowchart of the SPPLAS.

3.1 Secure Handshake Phase

Generally, adversaries collect the location information of the user from the frame sent by user during handshake phase. To protect the MAC address of the user from adversaries during the 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 CSI_u and CFO_u information of the user from the preamble, applies SVD on CSI_u and calculates eigen value λ_u from matrix CSI_u. At LBS server, for every user *u*, a mapping of $\lambda_u \rightarrow CSI_u$, CFO_u is maintained. Subsequently, LBS provider sends an acknowledgment (ACK) frame to MU, where user gets MAC address, CSI information of LBS provider CSI_p and applies SVD on CSI_p and calculates λ_p. The secret key is generated from λ_p obtained by applying using SVD on CSI_p. Later, the user encrypts and transmits all the frames including header and payload with generated secret key and CFO. Due to the reciprocal property of the wireless channel, channel information of both user and LBS provider will be identical. Though adversaries eavesdrop all the frames in legitimate link, they cannot decrypt the frame correctly because the estimated CSI_u', CSI_p', CFO_u' and CFO_p' are not identical with their real counterparts. Consequently, the user's privacy is protected and localisation by adversaries is prevented.

3.2 Secret Key Generation and CFO Encryption

The core 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 another side. To protect the maximum information available in CSI curve, SVD encoding scheme is deployed. The CSI vector is generated by CSI estimation of legitimate channel at transmitter and receiver by sampling the channel in its coherence time. CSI vector length is fixed based on the number of samples taken during coherence time.

The proposed coding scheme extracts singular values of CSI matrix using SVD and maps it in a defined pattern as per the Algorithm 1, to generate the 128 bits secret key for authentication. After the handshake phase, MU and SP independently perform the algorithm to generate secret key. Formally, singular value decomposition of H matrix is the factorisation of the form $U\Lambda V^H$ where U and V^H are unitary matrices and Λ is a non-negative real number diagonal matrix. The diagonal values of λ_i, where i = {0…. (p-1)} are the singular values of matrix H. Each singular value of matrix Λ is converted to binary and concatenated to generate secret key of size 128. If converted bits are less than the required bit size then the same singular values are repeated to get the required size. If converted bits exceed the required key size, only dominant singular values are considered to generate secret key *K*. After generating *K*, it is leveraged to form CFO vectors $[c_0, c_1, \ldots, c_M]$ where $M = \left(k/L\right) - 1$, *k* is key length and *L* is CFO vector length. Subsequently, CFO vectors in binary are converted to decimal. Then, CFO vectors

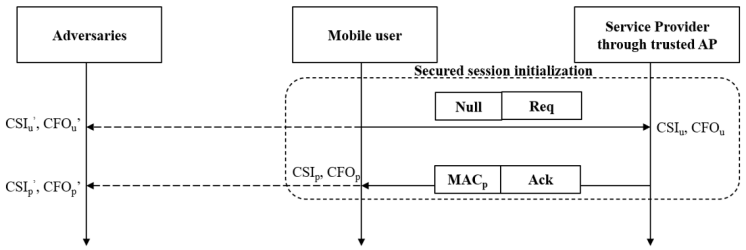

Figure 3. Secure handshake protocol.

are multiplied with Δf to form Hash vectors. For each frame, j[th] index of Hash vector is computed for concatenation using j=i mod L and subsequently j[th] Hash vector is concatenated to i[th] symbol. Finally, the concatenated frame is encrypted with secret key *K*. Since *K* is available only with user and provider, the adversaries obtain no knowledge about the encrypted frame.

Algorithm 1: Secrete Key generation and encryption using SVD & CFO

Secrete Key generation

Initialise Secret Key *K*= [ ];

Input: CSI vector of length N, Size (mxn) of H Matrix

Step1: Obtain the CSI vector $[h_1, h_2, h_3, .., h_N]$;

Step2: Reshape CSI vector of length p into Matrix H of dimension *m x n*; $[h_1, h_2, h_3, .., h_N] \rightarrow H_{mxn}$

Step3: Compute SVD for channel matrix by decomposing H into $U\Lambda V^H$;

$$\Lambda = \begin{bmatrix} \lambda_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_{p-1} \end{bmatrix}$$ where *p*=min {*m, n*};

Step 4: Arrange non-negative real numbers of diagonal matrix Λ into singular value vector; $\lambda = \{\lambda_0 \lambda_1 \ldots . \lambda_{p-1}\}$;

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 Δf ; Number of symbols in the frame S, CFO vector length L, Key length *k*;

Step6: Compute CFO vector using $c_i = k\left(L * i\right)$ to, $k\left(L*\left(i+1\right)-1\right)$ where $i = \{0\ to\left(\frac{k}{L}\right)-1\}$ and convert to decimal values using $d_i = bin2dec\left(c_i\right)$;

Step7: Generate Hash vectors by multiplying CFO vectors with Δf using $V_i = d_i \Delta f$;

Step8: for each frame S_i do

Compute the index j of Hash vector for concatenation using j = i Mod L;

Concatenate the j[th] Hash vector to the i[th] symbol using $S_i = S_i \| V_j$;

end for

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 localisation purposes. It is assumed that all the sequence of operations in key generation and encryption is open to eavesdropper. The simulation parameters used are key length - 128-bit, CSI matrix size-16, Rayleigh channel, CFO vector length-16, information data size-10^4. The performance of the proposed method was evaluated using three performance metrics namely, leakage, bit mismatch rate (BMR) and bit error rate (BER). Existing method denotes PriLA[2] and proposed method denotes SPPLAS method.

4.1 Leakage Rate

Leakage is the ratio of matched bits between the legitimate user, either MU or SP and the adversary. It measures the amount of information leaked to the adversary. An encryption scheme with low leakage is more secured. To validate the security level provided by the proposed method, simulations were carried out assuming a fixed distance of 5 m between MU and SP while the adversary is assumed to be at various distances away from the sender. Information leakage to the adversary 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 a shorter distance for obvious reasons like the channel responses and multipath profiles being more similar for a nearer adversary. However the secret key and CFO manipulated by eavesdropper is not identical to the actual credentials of legitimate users. Hence adversary cannot infer any usefull information. The worstcase leakage is only 10%. As the distance increases the leakage decreases. Comparing both the results, it can be vividly seen that the proposed method of encryption with SVD outperforms the TLDC method proposed in existing method, for shorter distances as well as longer distances.

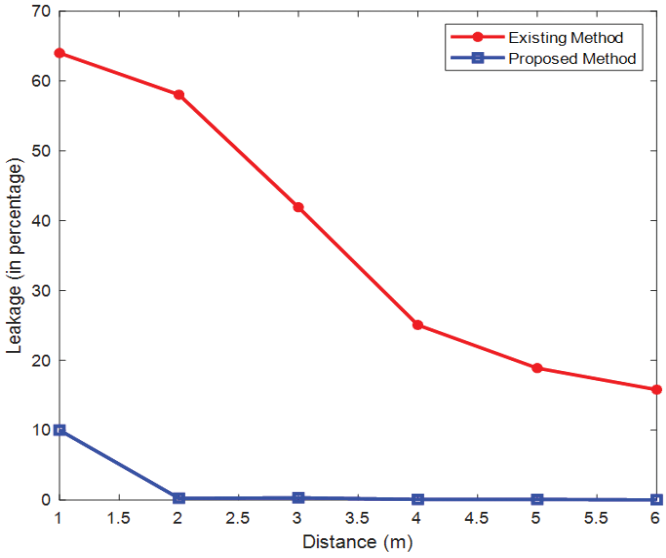

Figure 4. Information leakage to the adversary at various distances.

4.2 Bit Mismatch Rate

The second performance metric is the BMR, which is the ratio of the number of mismatching bits between the secret keys generated independently at user and service provider to the total number of bits in secret key. This measures the robustness of the key generation process and a low BMR is always preferred. Fig. 5(a) shows the BMR, for different bucket sizes which are used in the TLDC method proposed in existing method. This method achieves low BMR when the number of buckets is not more than 5. The reason being the small size of entropy for large number of buckets, resulting in low uncertainty in the generated bits. Hence, for a large number of bucket sizes, the mismatch rate is high leading to a low security level.

Towards verifying the robustness of the proposed method, the mismatch rate for the SPPLAS method is plotted against different SVD matrix size as shown in Fig. 5(b). The matrix size of the proposed method is the counterpart to the bucket size of the existing method. It can be seen that the variation in BMR with respect to matrix size is not significant in proposed method. But the mismatch rate of existing method

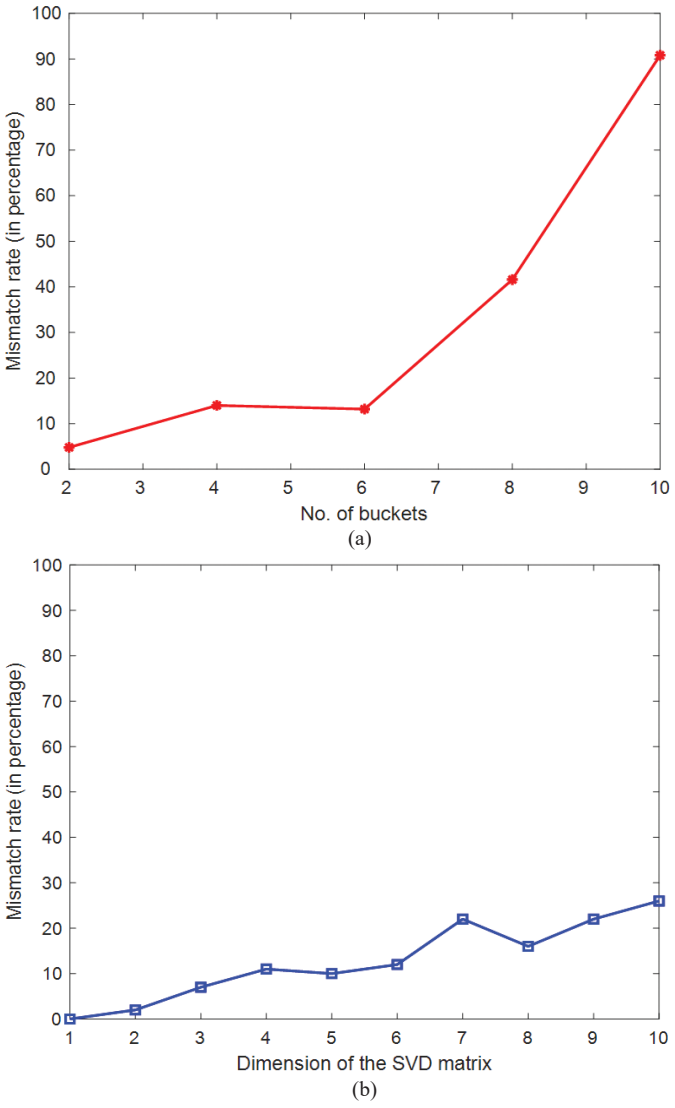

Figure 5. (a) BMR of existing method for different bucket size and (b) BMR of the proposed method for different SVD matrix size.

is growing higher when bucket size is increasing whereas the mismatch rate in proposed method is persistently low which is preferred.

4.3 BER Performance

The BER performance of the intended receiver for both the methods in the presence of adversary is compared. In this performance analysis, the effect on decoding performance, with and without CFO encryption, is also ascertained. Quadrature amplitude modulation (QAM) of different levels was considered for this analysis. Adversary model assumed for this analysis is that the key generation procedure and encryption is open to adversary. Since adversary cannot be in same location as that of user, the channel characteristics of adversary are different. For simulation purpose, adversary is modelled to have random CSI and CFO for key generation and encryption.

Figure 6 shows the BER performance of a 4 QAM system of the legitimate receiver using proposed method and existing method in the presence of adversary. The BER of the receiver using the proposed SPPLAS method is less than that of the existing method. Thus proposed method show better error rate performance than existing method. The adversary is modelled to eavesdrop and decrypt the SPPLAS frames between the legitimate users. The BER of the adversary is consistently high for all values of SNR. Though the adversary can be closer to user (high SNR values), the location is not identical to that of legitimate receiver and hence adversary cannot generate the secret key and CFO identical to that of legitimate users. Apparently the decryption by adversary cannot be done correctly to decode the information of the legitimate users.

Figure 7 shows the BER performance of the receiver in the presence of adversary for both the methods of encryption for 64 QAM system. The performance is similar to that of 4 QAM except for the need of high SNR to achieve low BER for the intended receiver, for obvious reasons of higher order modulation. But adversary's BER performance is poor irrespective of high SNR because the generated secret key and encrpytion by adversary using random CSI and CFO is not identical to that of user. Thus adversary cannot decode any useful information from the eavesdropped frames. Consequently, even for higher order QAM, proposed method performs better than existing method by achieving better BER performance.

5. CONCLUSIONS

A new physical layer privacy protection location authentication scheme in LBS based wireless networks have been proposed and analysed. In this proposed method, inherent CFO and CSI are extracted from Wi-Fi preambles and signature is generated using the secret key for location authentication. Then the frames are encrypted using the secret key to preserve the users' privacy. The performance of the proposed method is analysed and compared with an existing method. The simulation results show significant improvements in BMR, leakage, and BER than the existing physical layer security schemes. The proposed scheme can be implemented for existing LBS systems for better secrecy and robustness.

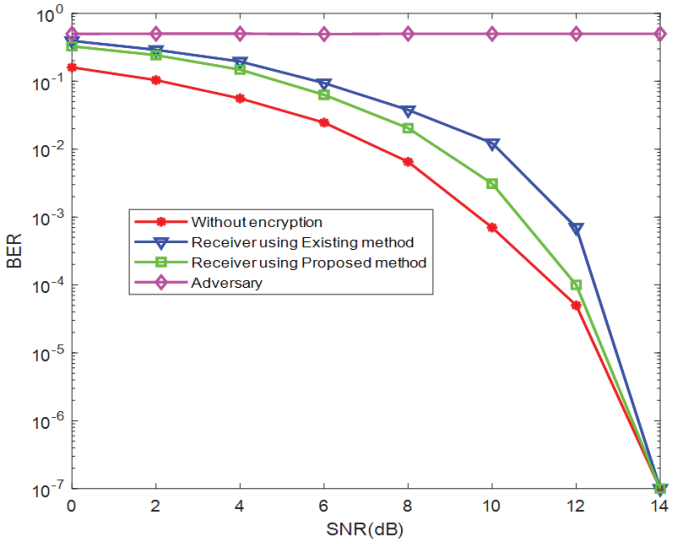

Figure 6. BER performance in the presence of adversary for 4 QAM.

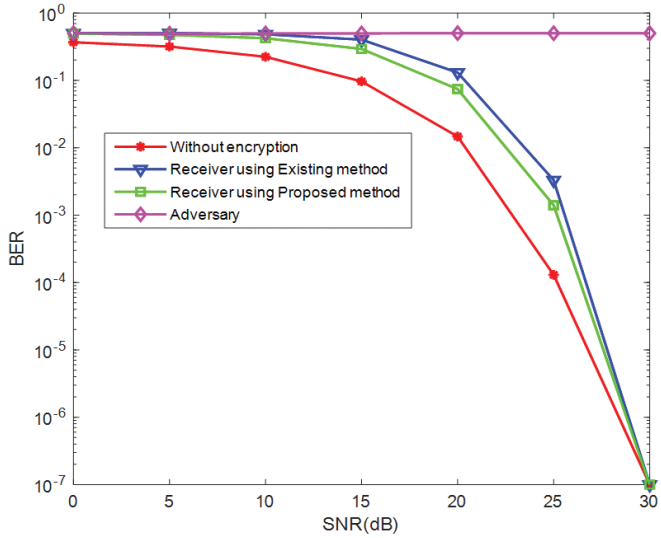

Figure 7. BER performance in the presence of adversary for 64 QAM.

REFERENCES

1. Shi, S.; Sigg, S.; Chen, L. & Ji, Y. Accurate location tracking from CSI-based passive device-free probabilistic fingerprinting. *IEEE Trans. Vehicular Technol.,* 2018, **67**(6), 5217-30. doi: 10.1109/TVT.2018.2810307
2. Wang, W.; Chen, Y. & Zhang, Q. Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures. *IEEE Trans. Wireless Commun.*, 2016, **15**(2), 1218-25. doi: 10.1109/TWC.2015.2487453
3. Xiang-ning, M.; Kai-jia, L.; & Hao, L. A physical layer security algorithm based on constellation. *In* Proceedings of the IEEE International Conference on Communication Technology (ICCT), Chengdu, China, 2017, pp. 50-53. doi: 10.1109/ICCT.2017.8359482
4. Zhang, Z.; Guo, D.; Zhang, B. & Yuan, J. Research on

physical layer security technology of multi-antenna system, *In* Proceedings of the International Conference on Electronics Instrumentation & Information Systems (EIIS)*,* Harbin, China, 2017, pp. 1-4.
doi: 10.1109/EIIS.2017.8298625

5. Lavanya, D.L.; Ramaprabha, R.; Gunaseelan, K. & Vaishnavi, V. Physical layer security using an adaptive modulation scheme for improved confidentiality. *IET Communications*, 2019, **13**(20), 3383-90.
doi: 10.1049/iet-com.2019.0031
6. Zeng, S.; Li, X.; Salem, A. & Zhao, D. Physical Layer Authentication Based on CFO and Visibility Graph, *In* Proceedings of the International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 147-152.
doi: 10.1109/NANA.2018.8648709
7. Wu, K.; Xiao, J.; Yi, Y.; Chen, D.; Luo, X. & Ni, L.M. CSI-based indoor localization. *IEEE Trans. Parallel Distributed Syst.*, 2013, **24(**7), 1300-09.
doi: 10.1109/TPDS.2012.214
8. Xiong, J. & Jamieson, K. Array track: A fine-grained indoor location system. *In* Proceedings of the USENIX Symposium on Networked Systems Design and Implementation, 2013, pp. 72-84.
doi: 10.5555/2482626.2482635
9. Zhichao, Z. & Guohong, C. Toward privacy preserving and collusion resistance in a location proof updating system. *IEEE Trans. Mobile Comput.,* 2013, **12**(1), 51-64.
doi: 10.1109/TMC.2011.237
10. Bachira, G. & Hongwei, L. Blockchain-Based Privacy-Preserving Authentication and Message Dissemination Scheme for VANET. *In* Proceedings of the International Conference on Systems, Control and Communications, 2019, pp. 16–21.
doi: 10.1145/3377458.3377466.
11. Yang, M & Hongliang, C, Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs. *Hindawi Mobile Information Systems*, 2019, Article ID 7593138, 19 pages.
doi: 10.1155/2019/7593138
12. Mengjia, Z. & Huibin, X. Mix-Context-Based Pseudonym Changing Privacy Preserving Authentication in VANETs. *Hindawi Mobile Information Systems*, 2019, Article ID 3109238, 9 pages.
doi: 10.1155/2019/3109238
13. Deepu, M. & Hima, A.R. A survey on different privacy-preserving authentication schemes in VANET. *In* Proceedings of the IOP Conference Series: Materials Science and Engineering, 2018, **396**(1), 012033.
doi:10.1088/1757-899X/396/1/012033
14. Wang, S.; Wang, J.; & Zhengtao, Y. Privacy-preserving authentication in wireless IoT: Applications, approaches, and challenges. *Wireless Communications*, 2018, **25**(6), 60-67.
doi: 10.1109/MWC.2017.1800109
15. Sriram, N. P.; Suman, J.; Prarthana, L. G.; Mike, C.; Sneha, K. K.; Neal, P. & Srikanth V.K. Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mobile Comput.,* 2013, **12**(5), 917–30.
doi: 10.1145/1614320.1614356
16. Liu, H.; Yang, J.; Wang, Y.; Chen, Y.; & Koksal, C.E. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. *IEEE Trans. Mobile Comput.,* 2014, **13(**12), 2820-35.
doi: 10.1109/TMC.2014.2310747
17. Shin, K.G.; Ju, X, Chen.; & Hu, X. Privacy protection for users of location-based services. *IEEE Wireless Commun.*, 2012, **19**(1), 30–39.
doi: 10.1109/MWC.2012.6155874
18. Chow, C.; Mokbel, M.F. & He, T. A privacy-preserving location monitoring system for wireless sensor networks. *IEEE Trans. Mobile Comput.*, 2011, **10**(1), 94–107.
doi: 10.1109/TMC.2010.145
19. Li, X. & Jung, T. Search me if you can: Privacy-preserving location query service. *In* Proceedings of the IEEE INFOCOM, Turin, Italy, 2013, pp. 2760–68.
doi: 10.1109/INFCOM.2013.6567085

CONTRIBUTORS

Ms D.L. Lavanya received ME in Communication Systems from the PSG College of Technology, Coimbatore, India. She has been working as a Scientist in DRDL, Hyderabad since 2000. Her research interests include instrumentation for static testing of rocket motors, underwater instrumentation and wireless communication systems. She is pursuing part time PhD from Anna University, Chennai, India, since 2015.
Her contribution in this paper includes conceptualisation of the problem, mathematical formulation, matlab simulation, analysis of results, preparation and organisation of the manuscript.

Ms R. Ramaprabha is doing Research in Department of ECE, Anna University, Chennai. Her area of interests includes: Wireless Communication, Cognitive radio networks, Physical layer security.
Her contribution in this paper includes mathematical formulation, matlab simulation and organisation of the paper.

Dr K. Gunaseelan received PhD from Anna University, Chennai, India, in 2009. He has been working as a Senior Assistant Professor in College of Engineering, Guindy, since 2010. His research interests include digital signal processing and wireless communication systems. He has published more than 20 papers in national and international journals.
His contributions in this paper include the overall architecture, guidance in the preparation of manuscript and in revision of the paper.