Defence Science Journal, Vol. 71, No. 4, July 2021, pp. 545-555, DOI : 10.14429/dsj.71.15403

Secret Key Generation Schemes for Physical Layer Security

Megha S. Kumar[#], R. Ramanathan[#,*], M. Jayakumar[#], and Devendra Kumar Yadav[@]

[#]*Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore - 641 112, India*
[@]*DRDO-Scientific Analysis Group, Delhi - 110 054, India*
[*]*E-mail: r_ramanathan@cb.amrita.edu*

ABSTRACT

Physical layer security (PLS) has evolved to be a pivotal technique in ensuring secure wireless communication. This paper presents a comprehensive analysis of the recent developments in physical layer secret key generation (PLSKG). The principle, procedure, techniques and performance metricesare investigated for PLSKG between a pair of users (PSKG) and for a group of users (GSKG). In this paper, a detailed comparison of the various parameters and techniques employed in different stages of key generation such as, channel probing, quantisation, encoding, information reconciliation (IR) and privacy amplification (PA) are provided. Apart from this, a comparison of bit disagreement rate, bit generation rate and approximate entropy is also presented. The work identifies PSKG and GSKG schemes which are practically realizable and also provides a discussion on the test bed employed for realising various PLSKG schemes. Moreover, a discussion on the research challenges in the area of PLSKG is also provided for future research.

Keywords: Wireless networks; Physical layer security; Secret key generation

1. INTRODUCTION

With the progress of wireless networking, huge amount of data exchange takes place over the wireless medium. However, because of the inherent broadcast nature of the wireless medium, the intruder can eavesdrop or jam the legitimate channel with ease, if the intruder is present within the communication range of the legitimate transceivers. This concern for wireless security can be resolved by the algorithms developed for ensuring security of the physical layer. Unlike the traditional cryptographic techniques, which the intruder can easily decrypt with the help of adequate computational power, PLS schemes cannot be exploited with ease even with the backup of enormous computational power, as PLS schemes leverage temporal variation and reciprocity property of the wireless channel to generate shared secret keys. To generate shared secret keys, channel probing, quantisation, encoding, IR and PA stages are carried out separately at both the transmitter and receiver.

The intrinsic broadcast nature of the wireless transmission medium exposes the information to several passive attacks such as traffic analysis, eavesdropping and active attacks such as jamming, man in the middle attack. Conventional cryptographic methods such as Diffiehellman key exchange (DHKE) and discrete logarithm[1] involves complex mathematical computations which the adversary may not be able to perform with ease, as the time involved in cracking the secret code could be much higher than the data validity. However, in future, the security provided by such schemes could be cracked because of the development of quantum computers. Moreover, traditional schemes will not hold long because of the complex key management infrastructure requirement. Yet another innovative idea is quantum cryptography[2] which does not use public key, instead, the technique rely on the laws of quantum theory, such as Heisenberg's uncertainty principle for secret sharing between two end points. However, the technique is very expensive and rare.

The concept of PLS[3-5] has emerged as an alternative to traditional crypto schemes and there is a flurry of research in this area. Key principles involved in PLSKG are, channel reciprocity, temporal variations, and spatial variations. Channel reciprocity indicates that the effect of multipath as well as fading on both ends of the same link are identical. Temporal variations[6] are introduced as a result of the mobility of transmitter, receiver or any object in the surrounding. Spatial correlation means that the channel between two distinct nodes will be unique and an adversary at a third location experiences uncorrelated channel. Therefore, adversary may not be able to obtain the same channel state information (CSI) as legitimate nodes resulting in distinct keys for the legitimate pair and adversary.

The basic system model for PSKG is illustrated in Fig. 1. According to a comparison performed between elliptic curve based DHKE[7] and PLSKG[8-10] in terms of energy consumption and resources, PLSKG proves efficient. Moreover, in the upcoming 5G technologies, the complex key management architecture of traditional cryptographic techniques may not be feasible. In massive, decentralised and low-cost network systems such as IoT, the PLSKG schemes are feasible. PLSKG

Received : 20 January 2020, Revised : 2021
Accepted : 12 February 2021, Online published : 01 July 2021

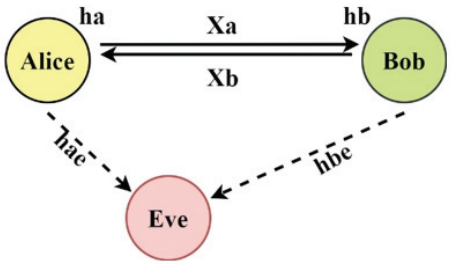

Figure 1. Basic PSKG model. X_a and h_a denotes the probe signal and channel measurements of Alice. X_b and h_b denotes the probe signal and channel measurements of Bob. h_{ae}, h_{be} represents the channel measurements of Eve.

has great practical appeal as it is highly beneficial for resource constrained large scale wireless networks because it simplifies the secret sharing process. Cyber physical systems, vehicular *Ad Hoc* networks, wireless local area networks, wireless sensor networks are some of the areas where PLS techniques can be applied. In this paper, a systematic investigation of the recent PLS schemes for a group of users termed as group secret key generation (GSKG) and between a pair of users termed as pair secret key generation (PSKG) is carried out. Fig. 2 depicts a classification of the various security schemes for wireless networks. The coloured blocks are discussed in detail in this paper.

Major highlights of our work are as follows,

- Provides recent developments in the area of PSKG and GSKG.
- Identifies the widely employed parameters and methods for PLSKG.
- Provides an analysis of various performance benchmarks such as approximate entropy (AE), bit generation rate (BGR) and bit mismatch rate (BMR).
- Identifies the PSKG and GSKG techniques which are practically feasible and describes the testbed employed for realising the techniques.

2. SECRET KEY GENERATION

PLSKG entail five stages at both the transceivers to generate shared secret keys as illustrated in Fig. 3 and they are channel sounding, quantisation, encoding, public discussion/ IR and PA. In Fig. 3, the most commonly employed techniques are provided as an example. However, various other recent PLSKG schemes are discussed in detail in other sections.

(i) Channel sounding: Channel sounding[11] is the technique by which peers involved in wireless transmission and reception assess the channel by means of transmitting symbols referred to as pilot symbols. Received signal strength indicator (RSSI), channel impulse response (CIR), channel frequency response (CFR) are some of the examples.

- *Pre-processing*

The channel measurements are impaired by several discrepancies which are processed by various methods such as PCA, DWT, DCT. The noisy channel measurements on direct quantisation yields distinct keys at the transceivers resulting in failure of the PLSKG system.

(ii) Quantisation and encoding : The randomness at both the transceivers are utilised for quantisation by converting it into bit streams appropriate for key generation. Increasing quantisation[12] bit number increases the BDR, thereby reducing the algorithm performance. To address this concern, every value which are quantised uniformly are encoded with 'nencod' bits. Uniform multilevel quantisation (UMQ) and CDF based quantisation (CDF) are discussed below as an example.

- *UMQ scheme*

The maximum '*max*' and minimum '*min*' value of the input channel measurements are identified.Threshold '*thr*' is computed as given in Eqn (1).

$$thr_i = \min + i\left[\frac{(\max - \min)}{level}\right] \quad (1)$$

where, $1 \le i \le level - 1$

Therefore, the input channel measurements are quantised into the bins given below,

$[min, thr_1]$, $[thr_{i-1}, thr_i]$, $[thr_{level-1}, thr_{max}]$

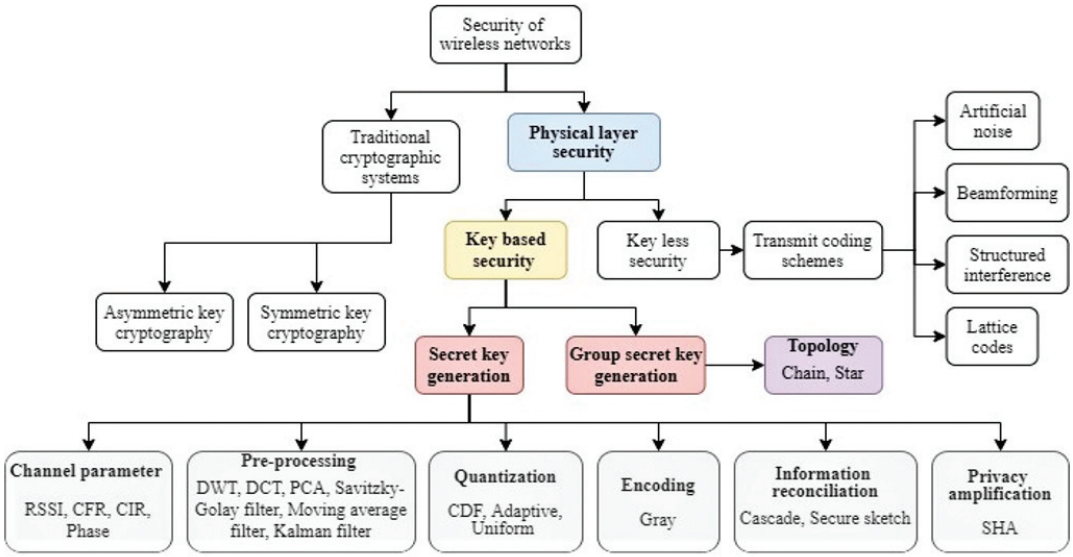

Figure 2. Classification of security schemes for wireless networks.

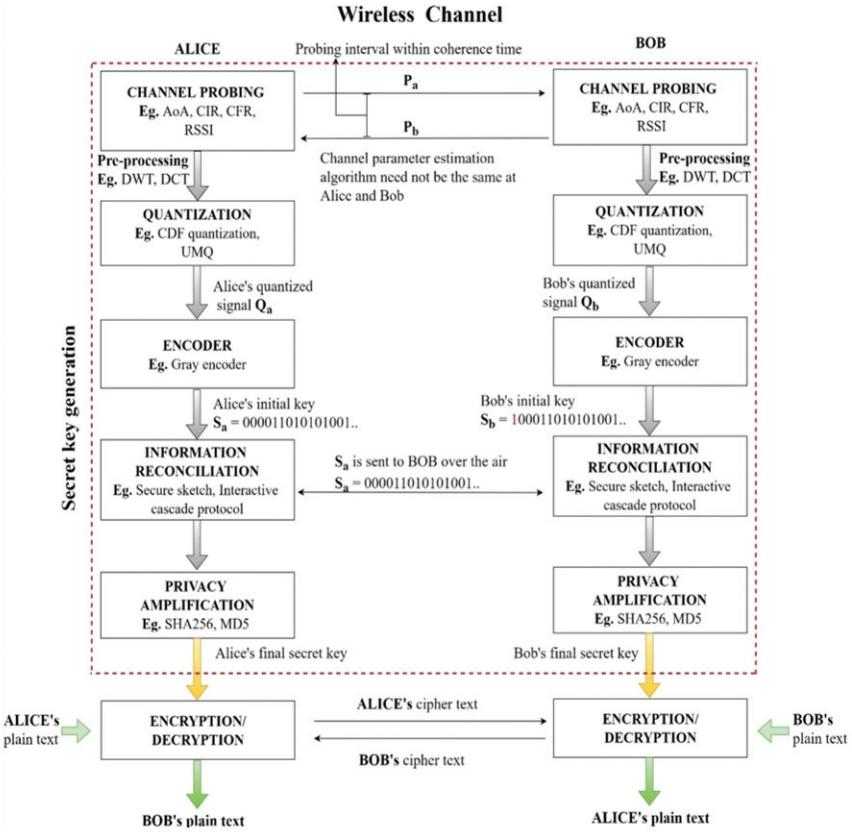

Figure 3. Secret key generation. Here, P_a, $P_b$denotes the probe signals of Alice and Bob. Q_a, Q_b are the quantised signals. S_a, S_b denotes the encoded signals of Alice and Bob.

- *CDF scheme*

Find out the CDF of the pre-processed channel measurements as given in Eqn. (2)

$$thr_i = F^{-1}\left(\frac{i}{level}\right) \tag{2}$$

Where $1 \le i \le level - 1$

Therefore, the input channel measurements are quantised into the bins given below,

$[F^{-1}(0), \quad thr_1], [thr_{i-1}, thr_i], [thr_{level-1}, F^{-1}(1)]$

(iii) Information reconciliation: IR stage is carried out to correct the mismatches existing in the intial key sequence generated after quantisation and encoding stage. Some of the IR[13] algorithms are interactive cascade protocol, secure sketch. For example, in interactive cascade reconciliation, the initial key sequence of Alice and Bob is divided into various blocks. Further, the parity of each block pair is checked to identify the positions where the bits are mismatched and the errors are corrected.

(iv) Privacy amplification: During the IR stage, some amount of information will be leaked to the adversary. The shared bit sequences also consist of high correlation due to pre-processing and encoding. Therefore, it is essential to employ PA[14] to ensure sufficient randomness. Examples are universal hash function, message digest 5 (MD5).

3. COMPARISON OF PSKG AND GSKG SCHEMES

In this section, recent PSKG and GSKG schemes are discussed. The classification is based on topology, attack type, channel parameter, pre-processing, quantisation, IR and PA. In real time scenarios, adversary might not just always rely on passive attacks. With the rapid advancements in technology, it is also possible for the adversary to initiate active attacks. Unlike passive attacks, active attacks modify content of the message being communicated and leads to failure of the PLSKG system. Most of the works rely on RSSI for PLSKG as it is readily available. However, there exist various other channel parameters having the potential to render sufficient randomness for generating shared keys[15]. In highly noisy environments, channel coherence duration will be very small and the channel measurements collected by Alice and Bob will have very low correlation which results in unsuccessful PLSKG. Pre-processing is an additional step employed in PLSKG to enhance correlation among channel measurements by reducing noise thereby increasing the chances of successful key generation. The above mentioned challenges motivated us to investigate more in this area.

3.1 Secret Key Generation between a Pair of Users

Peng[16], *et al.* proposed the loop-back (LB-TDD) scheme consisting of multiple frequency bands for TDD to alleviate the effect of phase offset errors and hardware finger print impairments. Practically, an average KDR of 0.0039 and 0.0079 are obtained in Line of sight (LOS) and Non line of sight (NLOS) scenarios with LB-TDD scheme. In contrast to classical TDD scheme, LB-TDD scheme renders better performance interms of KDR and KGR. However, the KGR performance is less in LOS for both classical TDD and LB-TDD as the effect of multipath is not prominent in LOS scenarios compared to NLOS. When the channel is less random, the adversary might initiate dictionary attack and decode the low entropy secret key. Therefore, in LB-TDD scheme, AE test is analysed before PA and a p value of 0.0832 is obtained for a down sample factor of 16. As the down sample factor increases, less correlated sub carriers are selected, which are useful for randomness but the KGR will be very low. For LB-TDD scheme, a KGR of ~1.6 and slightly greater than 1.6 is obtained for LOS and NLOS scenarios compared to classical TDD. Optimisation of the LB-TDD scheme is therefore essential.

Li[17], *et al.* proposed a pre-processing scheme based on principal component analysis (PCA) in which, certain dominant principal components are selected for reconstructing the signal. PCA scheme outperforms Haar wavelet, discrete cosine transform (DCT) and direct (without pre-processing) schemes with a KER less than 0.001at 4 dB SNR. For the same SNR, KER of DCT scheme is close to PCA with ~ 0.001 but

with a performance loss of 1dB. By ensuring that KER is less than 10^{-3}, KGR for all these schemes are investigated and PCA scheme achieves highest KGR of ~1 with a performance gain of 2dB compared to DCT scheme. AE test is performed before PA stage by averaging the p values of bit sequences. PCA scheme outperforms all other schemes with a p value of 0.5004. Prior works on PSKG techniques, especially for LoRa[18] networks focus only on short range communications. In most of the practical scenarios such as vehicular communications, short range results may not be applicable. Hence, Zhang[19], *et al.* proposed a PSKG scheme for low power WAN's with long range communication ability. Due to large variations in RSSI, differential quantisation is employed. Pearson correlation coefficients (PCC) of 0.9582 and 0.9689 are obtained for outdoor and indoor scenarios respectively. However, the generated keys have very low randomness. For both scenarios, every differential comparison generates a KGR less than or equal to 1 bit per measurement.

Epiphaniou[20], *et al.* proposed a channel gain complement (CGC) scheme for non-reciprocity compensation. There are certain limitations in this work, cascade reconciliation will not work for topologies involving time critical elements and not all IoT devices are equipped with multiple antennas. Hence, practical feasibility is limited. Even though many SKG algorithms are proposed, they lack robustness and the rate of bit mismatch is high. Future work focusses on investigation of turbo error reconciliation especially in the area of Social Internet of Things (SIoT). Proposed scheme outperforms indexing scheme by generating 35 keys per minute for a key length of 128. For AE test, p values in the range of 0.85 to 0.97 bits are achieved per sample. Patwari[21], *et al.* proposed a fractional interpolation scheme in which, no two directional measurements are simultaneously measured, while Karhunen Loeve (KL) decorrelation transformation produces uncorrelated components of the original channel measurements. Moreover, they also provide a theoretical framework for designing systems with low bit disagreement probability and the scheme does not take into account IR and PA. This scheme renders a correlation coefficient of 0.9965 and BDR of 0.022. Improving the distributional assumptions by employing HRUBE to other radio channel measurement modes constitute the future scope.

Key generation in stationary environments is a highly challenging task, mainly due to the lack of randomness in such environments. Therefore, Cheng[22], *et al.* proposed a moving window scheme for tackling this issue. In the proposed scheme, phase of the probe signal is randomised with stochastic coefficients. Further, a moving window is employed which sums the channel estimates in the windows producing completely new observations with remarkable fluctuations. The obtained measurements are quantised using adaptive equal probability quantisation (AEPQ). The proposed scheme outperforms single bit (SBQA) and multiple bit (MBQA) schemes for both indoor and outdoor scenarios with a BMR of 0.0101 and 0.0407 respectively. Aldaghri and Mahdavifar[23], proposed the idea of inducing randomness in channel measurements collected from static or very slow fading channels to ensure fast SKG. As the measurements collected from static channels are highly correlated, low KGR is rendered and therefore, Alice and Bob produce a certain number of random bits which they map to QAM symbols and share via public wireless channel. In low power networks such as IoT, where enabling SKG with low complexity architecture is a challenging task, the method proposed proves helpful. Future work constitutes designing protocols resistant to attacks by eavesdropper even when Eve has partial/full CSI. For static channel, a BMR of 0.11 and for dynamic channel, a BMR of 0.24 is obtained for the Alice-Bob link. AE test rendered a p value of 0.5803 and 0.1772 for static and dynamic channels respectively. The scheme produced a high BGR of 64-96 bits per packet.

Ambekar[24], *et al.* employs a curve fitting based pre-processing (CFKG) scheme to enhance reciprocity of the collected RSSI measurements which is then quantised using adaptive quantisation technique. The proposed scheme can be employed for securing mobile Ad Hoc networks. The CFKG scheme produces a BDR of 0.0302 with an average KGR of 3.39 bits per second. In indoor scenario, a p value of 0.96 is rendered while in outdoor scenario, p value varies depending on the location chosen, with a maximum of 0.82 and minimum of 0.06.Mathur[25], *et al.* translated foregoing information-theoretic ideas into practically feasible protocols and developed a novel secret key extraction algorithm which does not require an authenticated channel. Moreover, a technique to cope with active spoofing attack is developed in which, Eve impersonating as Alice or Bob gets detected, as some of the shared secret bits are used for data-origin authentication. Through the proposed scheme, man in the middle attack can also be combated to an extend.

Two schemes are developed, one is based on RSSI which renders an average secret bit rate of 1.3 bits/second while the second scheme based on CIR renders an average secret bit rate of 1.28b/s in static and 1.17b/s in mobile scenarios respectively. BDR of 0.1198 and BGR of 1.936 bits per second are provided by the scheme. For accurate measurements of the channel, an antenna and a dedicated set of hardware is required which increases the complexity and cost of the system. Therefore, Ambekar[26], *et al.* proposed a scheme called key generation from enhanced channel reciprocity (KGECR), in which the RSSI measurements are pre-processed using $l1$ norm minimisation. KGECR scheme renders an average BDR of 0.045 and constant key generation with a rate of 3.41 bits per second as the quantisation scheme employed is lossless.

The AE test results are same as CFKG scheme with a p value of 0.96 for indoor and a maximum of 0.82 and minimum of 0.06 in outdoor.

Premnath[27], *et al.* proposed an iterative distillation stage between quantisation and IR to pre-process the measurements. In the proposed work, predictable channel attack is investigated using RSSI in which, the adversary initiates planned mobility resulting in desired and easily predictable channel fluctuations between Alice and Bobwhen the environment is static. In multiple bit extraction scheme from a single RSS, the maximum entropy value obtained in stationary environment is 0.56, mobile category is 0.67 and intermediate category is 0.55, secret bit rate for static is 0, mobile is ~0.2 and intermediate is ~0. In secret key extraction using handheld devices for the indoor scenario, a distance of 25 feet is considered between

Alice and Bob and the output BMR is 0.0029 while it is 0.0246 for outdoor. In key extraction for MIMO like sensor networks, the measurements are distilled using iterative distillation and the results are validated for both indoor and outdoor environments. Just 2 iterations of iterative distillation reduced BMR to 0.05. An AE value of ~ 1 is obtained for all N x N configurations in which 'N' is the number of nodes. When N is 5, secret bit rate is ~0.4. The future work constitutes evaluating effect of predictable channel attack using CIR.

The channel measurements collected by the transceivers contain too many discrepancies and the measurements will be highly correlated but not similar. To address this issue, Zhan[28], *et al.* proposed a pre-processing scheme for PSKG using discrete wavelet transform (DWT) based compressor. The compressor is applied to the channel measurements of Alice and Bob using *Sym4* wavelet, before quantising the measurements. The proposed scheme is evaluated in terms of bit mismatch rate, secret bit rate, randomness and complexity. The BMR is less than 0.4 when the quantisation level is 4 and the BMR is less than 0.25 for a quantisation level of 5 when the encoding bits are in the range from 2 to 6. A secret bit rate of 2.5 is obtained when the quantisation level is 16 and encoding bit size is 6. The high pass and low pass filtering operation in DWT takes *O(n)* time resulting in some complexity. Yuliana[29], *et al.* proposeda novel pre-processing approach which combines modified kalman filter (MK) and polynomial regression method to achieve very high correlation between legitimate pairs. The efficient pre-processing scheme eliminates the need for IR and hence, the scheme renders reduced communication and computational cost. The performance of the proposed scheme is evaluated in terms of PCC, BDR, KGR and randomness. MK scheme is applied to RSSI data blocks of length 128. Hence, the correlation increases to 0.819 and 0.766 for LOS and NLOS scenarios respectively after processing the entire RSS datain the aforementioned manner, in contrast to the measured values of 0.757 and 0.698. With this scheme, certain RSSI blocks render very high correlation of 0.99. A KGR of 0.92bps and 0.45bps is achieved for LOS and NLOS scenarios with an average p value of 0.6 and 0.54 respectively. The proposed scheme is able to achieve a BDR of 0 in most of the cases without IR stage. The p values obtained using NIST test suit is > than 0.01 thereby proving that the proposed scheme is a promising solution for PLS.

According to Margelis[30], *et al.* employing DCT[31] improves the performance of PSKG system considerably. Hence, DCT is employed to analyse the power spectrum and high-frequency components are discarded or trimmed. 90% of the power is contained in the low frequency components both in frequency and time scale. By using inverse of DCT, the compressed frequency parameters can be obtained. Zhan[32], *et al.* proposed a novel encoding scheme based on gray code with reusable codebook. The scheme proposed renders enhanced secret bit rate. The encoding scheme is employed with uniform and non uniform quantisation schemes. After quantisation, a distillation stage is performed which eliminates abrupt transitions iteratively. The proposed SKG system is evaluated interms of symbol difference, secret bit rate, BMR and randomness. Here, symbol difference is defined as the absolute difference of symbols which are not matched. With the proposed scheme only small symbol differences are caused by the uniform scheme. As an example, uniform scheme with a quantisation level of 8 and 3 bit encoding renders a BMR greater than 0.3 for 5900 measurements with a packet loss rate of 0.19% . This BMR can be corrected by IR stage after 3 rounds of distillation. For the same scenario, the scheme renders a secret bit rate of 1.6 for a quantisation level of 4 and 3 bit encoding. Moreover, the keys generated using the proposed encoding scheme passes NIST tests proving its suitability for securing wireless applications.

According to Zhang[33], *et al.* exploiting randomness from both time and frequency domains of the channel responses of OFDM subcarriers greatly enhance the chances of successful SKG. To remove the impact of noise in channel measurements, an FIR low pass filter (LPF) is employed. An LPF based pre-pocessing renders good correlation at reduced cost and computational overhead. Further, a single bit CDF based quantisation is employed. The performance is evaluated in terms of randomness, KDR and KGR. For example, a correlation coefficient greater than 0.6 is obtained at a sampling frequency of 200 Hz when LPF is employed, thereof the scheme is feasible for mobile devices as well. The average KDR obtained with the proposed scheme for the same sampling frequency is greater than 0.4 at 0 dB SNR. On evaluating randomness using NIST tests, the p values obtained for all tests except the DFT test is greater than 0.01. Similarly, Lin[34], *et al.* employs adaptive quantisation scheme to achieve reduction in bit disagreements. Moreover, a randomness extractor is also proposed to enhance the performance of the SKG system. For a quantisation level of 3 and 2 bit encoding a BDR of approximately 0.1 is generated. The proposed scheme renders a BGR of 4.3967. Moreover, the key sequences also pass all the NIST tests employed.

Wang[35], *et al.* proposed a novel symmetric key generation system named as MobiKey in which, the phase information collected from commercially available devices are leveraged for generating shared keys. In contrast to amplitude, phase information is rich in randomness and is less susceptible to noise. However, the constraints in antenna sensing area results in issues such as reduced BMR, randomness along with hardware imperfections which makes phase extraction from commercial devices difficult and hence, complicates the SKG process. Therefore, the authors employ corrected phase and adaptive quantisation technique with CDF based coding scheme named as double gray code for generating shared secret keys. The highlight of this scheme is that it is independent of the communication protocol and hence can be employed in various smart home applications such as Zigbee, WiFi and Z Wave. When the channel remains static for a longer period, so as to induce variation, a stepper motor is attached to the antenna. After quantisation, IR stage can be employed using any available schemes such as secure sketch, BCH and followed by a randomisation stage to ensure sufficient randomness in the final key by eliminating selected bits. The proposed scheme is able to generate about 455.68 bits per second. For a sample length of 200, a bit matching greater than 0.96 is obtained. The key sequences pass the NIST tests. Therefore, the proposed scheme is available for generation of shared keys both when the channel is dynamic as well as static.

Table 1 provides the various techniques employed at different stages in the PSKG system. Table 2 provides the performance of the PSKG schemes in terms of disagreement rate, generation rate and approximate entropy.

3.2 Group Secret Key Generation

Most of the works in PLSKG focuses on key generation between a pair of legitimate nodes as GSKG is highly challenging. In GSKG, the channel information utilised for generating secret keys in the physical layer is defined only among two users in terms of randomness and reciprocity. In this section, we elaborate the various schemes employed for GSKG.

In literature mainly, GSKG schemes for star topology utilising RSS is explored, which is then extended for independent as well as overlapped multi-cluster topology in which every cluster is a single star topology[36] or chain topology[37] and mesh topology is less explored. Wei[36], *et al.* proposed a scheme which utilises RSS for generating secret keys for single, independent and multi-cluster topologies. However, while generating secret keys, there can be potential channel conflicts and a decreased probing efficiency. To combat this issue, the network is split into star topology. In this scheme an independent key is shared between member nodes by the root node. Root node facilitates generation of group secret key and manages to share it safely among its members using XOR process between group key

Table 1. PSKG schemes for wireless networks

Ref.	System	Attack type	Ch. parm.	Pre-processing	Quantisation	IR	PA
Peng[16], *et al.*	TDD / OFDM	Passive, Active	CFR	LB-TDD	Threshold	Mapping table	Hash
Li[17], *et al.*	MIMO/ OFDM	Passive	CFR, CIR	PCA	CDF	LDPC bit flipping	MD5
Zhang[19], *et al.*	LP-WAN	Passive	RSSI	CGC	Differential	Secure sketch	Hash
Epiphaniou[20], *et al.*	VANET	-	Synthetic data	CGC	Single threshold	Turbo codes	-
Patwari[21], *et al.*	SISO	Passive	RSSI	FI, KL Transform	Multi bit adaptive	-	-
Cheng[22], *et al.*	SISO, MIMO	Passive, Predictable attack	Amplitude	Moving window, Artificial noise	Adaptive equal probability	BCH codes	Secure Hash
Aldaghri, Mahdavifar[23]	IoT	Passive	CIR	Induced randomness	Adaptive lossy	Secure sketch, Convolutional codes	Hash
Ambekar[24], *et al.*	SISO	Passive	RSSI	Curve fitting	Adaptive	Turbo codes	SHA1
Mathur[25], *et al.*	MIMO/ OFDM	Passive, Active	CIR, RSSI	-	Level crossing algorithm	-	-
Ambekar[26], *et al.*	Mobile Ad Hoc SISO	Passive	RSSI	*l1* norm minimisation	Lossless binary	Localised IR	SHA-1
Premnath[27], *et al.*	MIMO	Passive, Predictable channel attack	RSSI	Iterative distillation	Adaptive lossy	Interactive cascade	Hash
Zhan[28] , *et al.*	SISO	Passive	RSSI	DWT	Uniform	Interactive cascade	Hash
Yuliana[29], *et al.*	SISO	passive	RSSI	Modified kalman filter, polynomial regression	Uniform	Gray	-
Zhan[32], *et al.*	SISO	passive	RSSI	-	Uniform, CDF	balanced gray code	Cascade protocol
Lin[34] , *et al.*	SISO	Passive	RSSI	Wavelet shrinkage using rigrsure	Adaptive	Gray	Cascade
Wang[35], *et al.*	SISO	Active, passive	Phase	Linear transformation, savitzkygolay filtering	Adaptive	Double gray code	Cascade, Secure sketch, BCH

Table 2. Performance comparison of PSKG schemes

Ref.	Disagreement rate	Generation rate	AE
Peng[16], *et al.*	**LOS** 0.0039 **NLOS** 0.0079	**LOS** ~1.6 **NLOS**>1.6	0.0832
Li[17], *et al.*	<0.001	~1	0.5004
Zhang[19], *et al.*	**O** 0.0529, **I** 0.0039,	≤1	**O** 0.065, **I** 0.1
Epiphaniou[20], *et al.*	0.02	35	~ 0.97
Patwari[21], *et al.*	0.022	22	-
Cheng[22], *et al.*	**O** 0.0407, **I** 0.0101	**O** 0.89, **I** 1.02	-
Aldaghri, Mahdavifar[23]	**S** 0.11, **M** 0.24	64-96	-
Ambekar[24], *et al.*	0.0302	3.39	**O** 0.82 max., 0.06 min., **I** 0.96
Mathur[25], *et al.*.	0.1198	1.936	-
Ambekar[26], *et al.*	0.045	3.41	**O** 0.82 max. 0.06 min., **I** 0.96
Premnath[27], *et al.*	0.05	~0.4	~1
Zhan[28] , *et al.*	<0.15	>2	0.88
Yuliana[29], *et al.*.	**LOS**<0.55, **NLOS**<0.75	**LOS** 0.92, **NLOS** 0.45	**LOS** 0.59 – 0.98, **NLOS** 0.18-0.91
Zhan[32], *et al.*	<0.45	<3.2	0.21 – 0.96
Lin[34] , *et al.*	<0.225	<5	0.358-0.716
Wang[35], *et al.*	-	<1, 455.8 bps	-

* LOS: Line of sight, NLOS: Non line of sight ,O: Outdoor, I: Indoor, S: Static

and respective shared keys. The proposed scheme is robust against dynamics in the network. Results are analysed for a five node network by analysing the trend of group KGR (GKGR) against probing rate. GKGR is evaluated for both static and mobile scenarios. The average deviation in GKGR between static and mobile scenarios is 12 bits/s. In static scenario, for a probing rate of 75 Hz, the GKGR is ~10bps while in mobile scenario, for the same probing rate, GKGR is ~30bps. For a probing rate of 100Hz, for static scenario outdoor, KDR is 0.17 and static indoor is 0.15. Similarly, for outdoor scenario with mobility, KDR is 0.12 and indoor scenario with mobility, KDR is 0.08. For a network size of 10, for static scenario a PCC of ~0.85 is obtained and for mobile, ~0.95 is obtained. Tunaru[38], *et al.* proposed a GSKG scheme using IR-UWB signals rich in randomness due to its high multipath resolution abilities. Hence, such a scheme can provide high secrecy. Moreover, existing works on cooperative GSKG involves generation of initial pair wise secret key and further forming group keys which introduces latency and traffic.

Therefore, a three node mesh topology employing public common channel for generating the group key is investigated. Nonetheless, no eavesdropping attack is incorporated and analysis of leaked information is also not considered. An average BMR of ~0.01and an average bit match of ~0.9 is obtained for an SNR of 15dB and a quantisation guard band of 0.02 is considered. Xu[39], *et al.* proposed a GSKG scheme for single antenna nodes. Proper choice of quantisation mechanism can give good secret key rate. Although various quantisation schemes are investigated in literature, the works do not explore key generation between various users and hence, cannot be considered for applications that require a group key. Therefore, Thai[40], *et al.* proposed a novel SKG technique for mesh topology in which each of the nodes are set up with numerous antennas and are linked to each of the other nodes through direct channels. As long as all other nodes can listen to pilot data from other nodes in mesh topology, authors utilise the information of multiple channels to increase key rate. BMR values for different time slots are evaluated and for a time slot of 0.1, a BMR of ~0.65 is obtained and BMR reduces to almost 0 in slot 1.

Most of the GSKG schemes do not tackle the issue of information leakage, low key agreement, and cost. Therefore, Li[41], *et al.* proposed a lightweight GSKG scheme which exploit non reconciled received signal strength (GNSS) for wireless networks which are mobile. Here, the authors study star and chain topologies. The proposed technique involves two steps, first is PSE, in which pair wise bit sequences having high correlation are extracted between wireless channels among every pair of legitimate users while second is, GKS, in which a group secret key is shared by securing with the pair wise bit sequences. Highly agreeing keys and less information leakage are the main highlights of the proposed scheme. The BER obtained is between 0.05 and 0.1 for 3 users in star topology and slightly above 0.05 for 3 users in chain topology. Zhang[42], *et al.* proposed a GSKG technique for multi-user OFDMA networks configured as star topology. Even though substantial efforts are applied to wards generation of group secret keys, channel sounding still needs to be done in pairs which increases the computational overhead thereby increasing the number of transmissions and channel occupations. One of the highlights of this work is that, there is no need for a dedicated communication link for channel probing as the key generation happens along with normal data transmission. The technique offers low complexity with no additional consumption of energy for channel probing and hence useful for IoT devices. Reduced interference amidst all users, increased reciprocity of channel, great key uniqueness, randomness and reduced key generation overhead are the highlights of the scheme. In this technique, a PCC of ~ 0.4 is obtained at 0 dB SNR and for an SNR of 5dB, a maximump value of 0.403, correlation in the range ~0.65 to 0.78 and KDR of ~0.2 – 0.25 is obtained for multiple users. Tables 3 and 4 summarises the GSKG techniques and its performance. Table 5 provide the testbeds used for practically feasible schemes.

Table 3. GSKG schemes for wireless networks

Ref.	Topology	Attack type	Ch. parm.	Pre-processing	Quantisation	IR	PA
Wei[36], *et al.*	Single, multi -cluster	Passive	RSSI	-	-	Cascade	Merkle Damgard Hash function
Tunaru[38], *et al.*	Mesh	Passive	CIR	-	Adaptive	Secure sketch,	Universal Hash
Thai[40], *et al.*	Mesh	Passive	RSSI	-	Scalar, Vector	Cascade	Hash Lemma
Li[41], *et al.*	Star, chain	Passive	RSSI	-		-	Hash
Zhang[42], *et al.*	Star	-	CFR	-	Mean value	Reed Solomon code	-

Table 4. Performance comparison of GSKG schemes

Ref	Mismatch rate	Generation rate	AE
Wei[36], *et al.*	**OS** 0.17,**OM** 0.12 **IS**0.15,**IM**0.08	**S**~10 **M**~30	-
Tunaru[38], *et al*	~0.01	-	-
Thai[40], *et al.*	~0.65	-	-
Li[41], *et al.*	~0.05	-	-
Zhang[42], *et al.*	~0.2	-	$\leq$0.403

* S denotes static, M denotes mobile, IS denotes indoor static, OS denotes outdoor static, OM denotes outdoor mobile, IM denotes indoor mobile

4. RESEARCH CHALLENGES

PLSKG schemes have a lot of advantages. It addresses the issue of key distribution, ensures authentication and even renders good secrecy even if the channel conditions of adversary is better than the legitimate channel. However, there are certain challenges which are yet to be addressed. Even though good secrecy can be achieved with SKG schemes, achieving perfect secrecy is not easy as the length of the secret keys generated is limited by the channel variations. In literature, most of the SKG schemes are developed with the assumption that Eve has less computational power and resources than the legitimate pair which is not always true. Moreover, the fact that Eve has knowledge of Bob's channel cannot be overlooked and hence, it is also possible for Eve to break the secrecy. The need for processing at both transceivers induce delay, overhead and power constraints. Apart from this, as SKG schemes are restricted to TDD systems, the system is also vulnerable to reciprocity and channel estimation errors which results in high mismatch in the shared keys generated. Direct quantisation of noisy measurements result in failure of the SKG system and hence, pre-processing[43] the collected measurements prior to quantisation is essential. Severity of the aforementioned issues increase in the case of GSKG as more wireless nodes are involved in the generation of shared keys in contrast to generation of shared keys for a pair of nodes. In GSKG systems, as the number of users increase, more channels are available among them which can be used to generate a portion

Table 5. Practically feasible PSKG and GSKG schemes

Ref.	Scheme	Testbed	Practical feasibility
Peng[16], *et al.*	PSKG	USRP N210	Yes
Zhang[19], *et al.*	PSKG	Arduino Uno	Yes
Patwari[21], *et al.*	PSKG	Crossbow Telos B Wireless Sensors	Yes
Cheng[22], *et al.*	PSKG	Transceiver (300MHz band) with Omnidirectional antenna	Yes
Ambekar[24], *et al.*	PSKG	Four laptops with different wireless cards	Yes
Mathur[25], *et al.*	PSKG	802.11 board with commercial 802.11 development platform with FPGA-based customised logic, CIR 802.11a/b/g modem IP, 3 off-the shelf 802.11 radios.	Yes
Ambekar[26], *et al.*	PSKG	Dell laptops (Alice-Atheros wireless card, Bob-Intel Pro wireless card)	Yes
Premnath[27], *et al.*	PSKG	Crossbow TelosB Wireless Sensors, Google Nexus One Smartphones equipped with Broadcom BCM 4329 chipset-based 802.11 wireless network cards	Yes
Yuliana[29], *et al.*	PSKG	Raspberry Pi, TL-WN722N 802.11 b/g/n wireless card.	Yes
Zhan[32] , *et al.*	PSKG	Intel wireless cards Atheros ar9285	Yes
Wang[35], *et al.*	PSKG	Intel WiFi Link 5300 or Atheros AR9590 NIC	Yes
Lin[34] , *et al.*	PSKG	rt2870 chip	Yes
Wei[36], *et al.*	GSKG	LT25 laptops with Atheros AR 5B95 802.11a/g/n wireless card. OS Fedora Linux with kernel version 2.6.34.8-68.fc13.i686.	Yes
Zhang[42], *et al.*	GSKG	Wireless motes with STM8L101 Microcontroller, Built-in antenna, CC1101 radio chip, Operating Freq. 430 MHz	Yes, IoT networks
Thai[40], *et al.*	GSKG	USRP-RIO 2952 (2.484 GHz)	Only for multi antenna devices

of the key. However, such schemes require a lengthy channel coherence time because of the need to sense the entire channel information while the channels remain the same. Low key rate, optimal power allocation, increased information leakage and need for longer coherence time are some of the challenges in GSKG compared to PSKG. SKG between a pair of legitimate users is vividly researched while GSKG[45] techniques are very few. Key generation in static channel[44] is another big challenge and the literature lacks sufficient practically feasible schemes in this area. Similarly, in FDD systems, due to the distinct uplink and downlink frequencies, successful key generation is very difficult. Moreover, SKG and GSKG schemes robust against active attacks are only very few. The high computational power requirement of PLSKG schemes is a challenge for low power IoT devices. Hence, developing PLSKG schemes with optimum power usage is also an unresolved issue.

5. CONCLUSION

The need to secure wireless communication has become crucial as the intrinsic broadcast nature of the wireless transmission medium exposes the information to several passive and active attacks. PLS is a promising technique in this regard as it does not require costly and complex infrastructure for key management in contrast to its companion technique, traditional cryptography. This paper provides a comprehensive analysis of the various techniques employed at various stages of both PSKG and GSKG, such as channel probing, pre-processing, quantisation, encoding, IR and PA. A detailed analysis of PSKG and GSKG schemes so as to identify practically feasible techniques are also carried out. A performance comparison of the various techniques employed in the generation of secret keys by using bit disagreement rate, approximate entropy and bit generation rate is also presented. Even though, various efficient PLSKG schemes are available in literature, there exist a lot of issues which limit the performance of PLSKG. Therefore, a discussion on the existing challenges are also provided to aid the readers for research in PLSKG.

ACKNOWLEDGEMENT

The authors would like to acknowledge the project support by EMR grant (ERIP/ER/201801009/M/01/1742) by ERIPR DRDO, New Delhi.

REFERENCES

1. Mccurley, K. S. The discrete logarithm problem. *In* Proceedings of Symposia in Applied Mathematics Cryptology and Computational Number Theory, pp. 49–74.
   doi: 10.1090/psapm/042/1095551
2. Bennett, C. H. & Brassard, G. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM SIGACT News*, 1989, **20**(4), 78–80.
   doi: 10.1145/74074.74087
3. Mukherjee, A.; Fakoorian, S. A. A.; Huang, J. & Swindlehurst, A. L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 2014, **16**(3), 1550–1573.
   doi: 10.1109/surv.2014.012314.00178
4. Zhang, J.; Woods, R.; Duong, T. Q.; Marshall, A.; Ding, Y.; Huang, Y.& Xu, Q. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access*, 2016, 4, 4464-4477.
   doi: 10.1109/ACCESS.2016.2604618
5. Zhang, J.; Woods, R.; Duong, T. Q.; Marshall, A. & Ding, Y. Experimental study on channel reciprocity in wireless key generation. *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2016.
   doi:10.1109/spawc.2016.7536825
6. Zou, Y.; Zhu, J.; Wang, X. & Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE,* 2016, **104**(9), 1727-1765.
   doi:10.1109/jproc.2016.255852
7. Zhang, J.; Duong, T. Q.; Marshall, A. & Woods, R. Key Generation From Wireless Channels: A Review. *In* IEEE Access, **4**, 2016, pp.614–626.
   doi:10.1109/access.2016.2521718
8. Yadav, P. & Ramanathan, R. Dynamic key generation using single threshold multiple level quantisation scheme for secure wireless communication. *In* 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2017, pp. 34-38.
   doi: 10.1109/wispnet.2017.8299714.
9. Ramesh, M. V. Design, development, and deployment of a wireless sensor network for detection of landslides. *Ad Hoc Networks*, 2014,**13**, 2–18.
   doi: 10.1016/j.adhoc.2012.09.002
10. Zenger, C. T.; Pietersz, M.; Zimmer, J.; Posielek, J.-F.; Lenze, T. & Paar, C. Authenticated key establishment for low-resource devices exploiting correlated random channels. *Computer Networks*, 2016, **109**, 105–123.
    doi: 10.1016/j.comnet.2016.06.013
11. Wang, Q.; Wei, M. & Zhu, Y. Channel Estimation for Frequency Division Duplexing Multi-user Massive MIMO Systems via Tensor Compressive Sensing. *Def. Sci. J.,* 2017, **67**(6), 668.
    doi:10.14429/dsj.67.10984
12. Han, Q.; Liu, J.; Shen, Z.; Liu, J.& Gong, F. Vector partitioning quantization utilizing K-means clustering for physical layer secret key generation. *Information Sciences,*2020,**512**, 137-160.
    doi:10.1016/j.ins.2019.09.076
13. Li, G.; Zhang, Z.; Yu, Y.& Hu, A. A Hybrid Information Reconciliation Method for Physical Layer Key Generation. *Entropy,*2019, **21**(7), 688.
    doi:10.3390/e21070688
14. Y. Wei; K. Zeng & P. Mohapatra. Adaptive wireless channel probing for shared key generation based on PID controller. *IEEE Trans. Mobile Comput.,* 2013*,* **12**(9), 1842–1852.
15. Kambala, S.; Vaidyanathaswami, R. & Thangaraj, A. Implementation of Physical Layer Key Distribution using

Software Defined Radios. *Def. Sci. J.,* 2013,**63**(1), 6-14. doi:10.14429/dsj2013.6592

16. Peng, L.; Li, G.; Zhang, J.; Woods, R.; Liu, M. & Hu, A. An Investigation of Using Loop-Back Mechanism for Channel Reciprocity Enhancement in Secret Key Generation. *IEEE Transactions on Mobile Computing*, 2019, **18**(3), 507–519. doi: 10.1109/tmc.2018.2842215
17. Li, G.; Hu, A.; Zhang, J.; Peng, L.; Sun, C. & Cao, D. High-Agreement Uncorrelated Secret Key Generation Based on Principal Component Analysis Preprocessing. *IEEE Transactions on Communications*, 2018, **66**(7), 3022–3034. doi: 10.1109/tcomm.2018.2814607
18. Ruotsalainen, H. & Grebeniuk, S. Towards Wireless Secret key Agreement with LoRa Physical Layer. *In* Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018, 2018.
19. Zhang, J.; Marshall, A. &Hanzo, L. Channel-Envelope Differencing Eliminates Secret Key Correlation: LoRa-Based Key Generation in Low Power Wide Area Networks. *IEEE Transactions on Vehicular Technology*, 2018, **67**(12), 12462–12466. doi: 10.1109/tvt.2018.2877201
20. Epiphaniou, G.; Karadimas, P.; Ismail, D. K. B.; Al-Khateeb, H.; Dehghantanha, A. & Choo, K.-K. R. Nonreciprocity Compensation Combined With Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks. *IEEE Internet of Things Journal*, 2018, **5**(4), 2496–2505. doi: 10.1109/jiot.2017.2764384
21. Patwari, N.; Croft, J.; Jana, S. & Kasera, S. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements. *IEEE Transactions on Mobile Computing*, 2010, **9**(1), 17–30. doi: 10.1109/tmc.2009.88
22. Cheng, L.; Li, W.; Ma, D.; Wei, J. & Liu, X. Moving window scheme for extracting secret keys in stationary environments. *IET Communications*, 2016, **10**(16), 2206–2214. doi: 10.1049/iet-com.2015.1219
23. Aldaghri, N. & Mahdavifar, H. Fast Secret Key Generation in Static Environments Using Induced Randomness. *In*2018 IEEE Global Communications Conference (GLOBECOM), 2018. doi: 10.1109/glocom.2018.8647945
24. Ambekar, A.; Hassan, M. & Schotten, H. D. Improving channel reciprocity for effective key management systems. *In*2012 International Symposium on Signals, Systems, and Electronics (ISSSE), 2012. doi: 10.1109/issse.2012.6374318
25. Mathur, S.; Trappe, W.; Mandayam, N.; Ye, C. & Reznik, A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. *In* Proceedings of the 14th ACM International Conference on Mobile Computing and Networking - MobiCom 08, 2008. doi: 10.1145/1409944.1409960
26. Ambekar, A.; Kuruvatti, N. & Schotten, H. Improved method of secret key generation based on variations in wireless channel. *In* Proc. of IWSSIP Conference, Vienna, 2012, pp. 60-63.
27. Premnath, S. N.; Jana, S.; Croft, J.; Gowda, P. L.; Clark, M.; Kasera, S. K. & Krishnamurthy, S. V. Secret Key Extraction from Wireless Signal Strength in Real Environments. *IEEE Transactions on Mobile Computing*, 2013, **12**(5), 917–930. doi: 10.1109/tmc.2012.63
28. Zhan, F.;& Yao, N. On the using of discrete wavelet transform for physical layer key generation. *Ad Hoc Networks,*2017, **64**, 22-31. doi:10.1016/j.adhoc.2017.06.00
29. Yuliana, M.; Wirawan&Suwadi. A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization. *Entropy,*2019, **21**(2), 192. doi:10.3390/e21020192
30. Margelis, G.; Fafoutis, X.; Oikonomou, G.; Piechocki, R.;Tryfonas, T. & Thomas, P. Efficient dct-based secret key generation for the internet of things.*Ad Hoc Networks*, 2019,**92**, 101744. doi:10.1016/j.adhoc.2018.08.014
31. A. Aliabadian; M. R. Zahabi& M. Mobini. Optimal Singular Value Decomposition Based Pre-coding for Secret Key Extraction from Correlated Orthogonal Frequency Division Multiplexing Sub-channels. *International Journal of Engineering*, 2020, **33**(7). doi:10.5829/ije.2020.33.07a.07
32. Zhan, F.; Yao, N.; Gao, Z.; Lu, Z. & Chen, B. Efficient key generation leveraging channel reciprocity and balanced gray code. *Wireless Networks*, 2017. doi:10.1007/s11276-017-1579-x
33. Zhang, J.; Marshall, A.; Woods, R. & Duong, T. Q. Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers. *IEEE Transactions on Communications,* 2016*,* **64**(6), 2578-2588. doi:10.1109/tcomm.2016.2552165
34. Lin, R.; Xu, L.; Fang, H. & Huang, C. Efficient physical layer key generation technique in wireless communications. *EURASIP Journal on Wireless Communications and Networking,*2020, **1**. doi:10.1186/s13638-019-1634-7
35. Wang, L.;An, H.; Zhu, H. & Liu, W. MobiKey: Mobility-Based Secret Key Generation in Smart Home. *IEEE Internet of Things Journal,* 2020, **7**(8), 7590-7600. doi:10.1109/jiot.2020.2986399
36. Wei, Y.; Zhu, C. & Ni, J. Group Secret Key Generation Algorithm from Wireless Signal Strength. *In* 2012 Sixth International Conference on Internet Computing for Science and Engineering, 2012, pp. 239-245. doi: 10.1109/icicse.2012.64
37. 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 Transactions on Mobile Computing*, 2014, **13**(12), 2820–2835.

doi: 10.1109/tmc.2014.2310747
38. Tunaru, I.; Denis, B.; Perrier, R. &Uguen, B. Cooperative Group Key Generation Using IR-UWB Multipath Channels. *In*2015IEEEInternational Conference on Ubiquitous Wireless Broadband (ICUWB), 2015, pp. 1-5.
doi:10.1109/icuwb.2015.7324430
39. Xu, P.; Cumanan, K.; Ding, Z.; Dai, X. & Leung, K. K. Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization. *IEEE Transactions on Information Forensics and Security*, 2016, *11*(8), 1831–1846.
doi: 10.1109/tifs.2016.2553643
40. Thai, C. D. T.; Lee, J.; Prakash, J. & Quek, T. Q. S. Secret Group-Key Generation at Physical Layer for Multi-Antenna Mesh Topology. *IEEE Transactions on Information Forensics and Security,* 2019, **14**(1), 18–33.
doi: 10.1109/tifs.2018.2837661
41. Li, G.; Hu, L. & Hu, A. Lightweight Group Secret Key Generation Leveraging Non-Reconciled Received Signal Strength in Mobile Wireless Networks. *In*2019 IEEE International Conference on Communications Workshops (ICC Workshops), 2019.
doi: 10.1109/iccw.2019.8757181
42. Zhang, J.; Ding, M.; Lopez-Perez; D., Marshall, A. &Hanzo, L. Design of an Efficient OFDMA-Based Multi-User Key Generation Protocol. *IEEE Transactions on Vehicular Technology*, 2019, **68**(9), 8842–8852.
doi: 10.1109/tvt.2019.2929362
43. Gopinath, S.; Guillaume, R.; Duplys, P. & Czylwik, A. Reciprocity enhancement and decorrelation schemes for PHY-based key generation. *In* 2014 IEEE Globecom Workshops (GC Wkshps), 2014, pp. 1368–1372.
doi: 10.1109/glocomw.2014.7063624
44. Huang, P. & Wang, X. Fast secret key generation in static wireless networks: A virtual channel approach. *In* 2013 Proceedings IEEE INFOCOM, 2013, pp. 2292–2300.
doi: 10.1109/infcom.2013.6567033
45. Jiao, L.; Wang, P.; Wang, N.; Chen, S.; Alipour-Fanid, A.; Le, J. & Zeng, K. Efficient Physical Layer Group Key Generation in 5G Wireless Networks. *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020.
doi: 10.1109/cns48642.2020.9162261

CONTRIBUTORS

Ms Megha S. Kumar received her MTech in Communication and Signal Processing from Amrita Vishwa Vidyapeetham, Coimbatore, India in 2017 and currently she is working towards her PhD in the area of Wireless Network Security. Her area of interest lies in Wireless Communication and Applications.
In the current work, she conducted the study, and prepared manuscript after analysing a comprehensive literature survey.

Dr R. Ramanathan received his MTech in Computational Engineering and Networking and PhD in Electronics and Communication from Amrita Vishwa Vidyapeetham, Coimbatore, India in 2011 and 2015 respectively. Since July 2006, he has been with the Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, where he is currently an Assistant Professor. His areas of research include optimisation and signal processing for wireless communication and networks, MIMO and OFDM communications, Bio-inspired Computing, Wireless Sensor Networks, Physical layer signal design and security and Convex Optimisation.
In the current work, he planned and led the study, and carried out revisions in the manuscript.

Dr M. Jayakumar received his PhD in Microwave Electronics from the University of Delhi and MTech in Electronics from the Cochin University of Science and Technology in 1996 and 1989 respectively. He has more than 70 research publications in international journals and conferences and several textbook articles. His area of research includes, radio frequency electronics, planar antennas, microwave integrated circuits and devices and wireless communication systems for airborne vehicle applications. He is Professor and Chairperson in the Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Coimbatore.
In the current work, he guided the team, participated in discussions on concluding inferences and reviewed the manuscript.

Dr Devendra Kumar Yadav obtained MTech in Digital Electronics & Advanced Communication from Karnataka Regional Engineering College, Surathkal in the year 2002. He completed PhD in signal processing from Department of Electrical Engineering, Indian Institute of Technology Delhi, India, in 2019. Since 2002, he is working for Defense Research & Development Organisation. His research interest includes Signal processing, wavelets and filter banks, and secure key generation.
In the current work, he participated in discussions on literature and reviewed the manuscript.