INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 2, PP. 361-369
Manuscript received January 13, 2023; revised April, 2023. DOI: 10.24425/ijet.2023.144372

PCA Based Components Selection Criteria for Computationally Efficient Physical Layer Key Generation (PLKG) System

Tapesh Sarsodia, Uma Rathore Bhatt, Raksha Upadhyay, and Vijay Bhat

***Abstract*—Data security is one of the prime concerns in wireless networks. PLKG has been emerging as an attractive alternative to traditional cryptographic techniques. PLKG is more computationally efficient than cryptography. Moreover, PLKG using Principal component analysis (PCA) as pre-processing may further save computations. This paper proposes three mechanisms to select components of PCA which are based on Information content, Mean and Histfit. Bit Disagreement Rate (BDR) is compared for each mechanism. Histfit based method is found to be best. Since only two components are supposed to be processed for key generation, it is computationally efficient/ power efficient too.**

***Keywords*—wireless networks; received signal strength; Principal component analysis; physical layer key generation; Mean; Histfit**

I. Introduction

MODERN world inching more towards low powered wireless application networks. IoT networks are such long range, low powered wireless networks which are getting more attraction due to recent developments in automation based applications. IoT networks have numerous advantages like smart operation of the devices, easy data collection, good for personal safety and security etc. Due to all these features, IoT networks are able to support various application areas like Alexa models, home automation, smart city monitoring, operating electrical or electronic devices remotely etc.[1-3]. Apart from all these features, IoT networks still facing data security problems over the channel, because of various types of wireless attacks and they are open to intruders/ attackers which can hack data easily[4], predict their locations, or extract confidential information etc. This security problem leads researchers to design IoT networks to be highly reliable and secure. They are trying to design modern IoT networks in such a way that they have proper authentication between users, confidentiality of the data should be maintained, easy and global access controls to the network, more prone to network attacks, software attacks, encryption attacks etc.[5].

Classical cryptography techniques serve the purpose of making IoT networks more secure as far as data security is concern [6]. Typical cryptographic techniques include public key infrastructure, symmetric and asymmetric cryptography etc. These techniques are implemented over upper layers of network architectures and are complex in nature. They require fix and complex key infrastructures for sharing secret keys over the channel, which are not compatible with future generation smart energy aware nodes. So, alternate to these researcher's move towards security at the physical layer and designed PLKG systems for modern IoT-like power-constrained networks. This PLKG technique doesn't share keys over the channel. So, PLKG-based key generation is a reliable solution for future-generation secured networks. Physical layer security techniques utilize channel characteristics to generate keys between legitimate users using RSSI, CSI, Angle of arrival (AoA) etc.[7]. RSSI is the channel parameter which is being shared between two nodes before actual data transmission takes place. By refining the raw RSSI data, network parameters can be improved and it can be achieved by applying various preprocessing technique on raw RSSI. These preprocessing techniques improves system parameters by removing different redundancies from raw data like noise, data dimension etc. Various application areas based on RSSI preprocessing are Human activity recognition (HAR), wireless node identification, channel identification, energy-aware wireless networks, PLKG systems etc. Different techniques available to pre-process RSSI are dimensionality reduction techniques like PCA, Individual component analysis (ICA), decision tree, Linear discriminant analysis (LDA), etc. which help to reduce data dimension which further reduces computational complexities of the network. We can also use filtering techniques like mean filter, gaussian-Kalman filtering, etc. to reduce redundancies in the raw RSSI signal, which results in improved network parameters, transformation techniques like Discrete wavelet transform (DWT), Discrete cosine transform (DCT), etc. also plays crucial role in preprocessing of RSSI, which is reported in various works so far.

So, in a PLKG system RSSI collection and preprocessing of it plays a vital role in designing future generation wireless applications. Now, let us discuss the PLKG system in detail. PLKG system has five main stages[8]: RSS acquisition, preprocessing, quantization and encoding, information reconciliation, and privacy, amplification, as shown in Fig. 1.

T. Sarsodia, U. R. Bhatt, R. Upadhyay are with Institute of Engineering and Technology, Devi Ahilya University, Indore, India (e-mail: tapeshs162@gmail.com, uvrathore@gmail.com, rupadhyay@ietdavv.edu.in).

V. Bhat is with Sage University, Indore, Madhya Pradesh, India (e-mail: bhatvijaybhat@gmail.com).

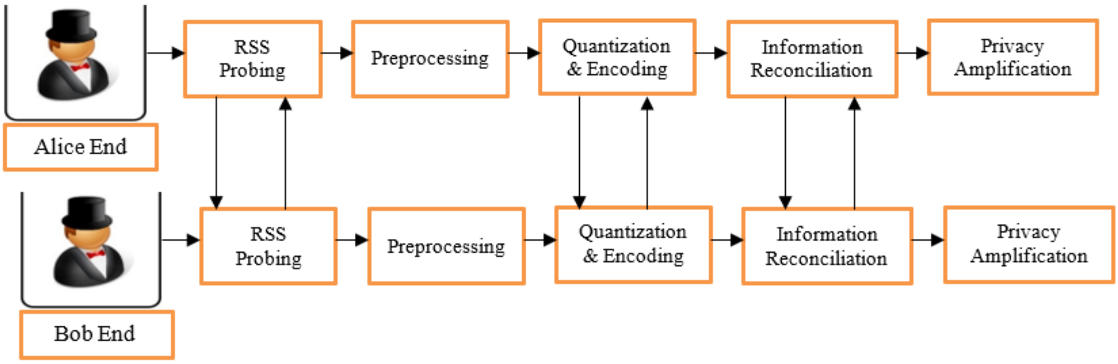

Fig. 1. Steps for PLKG systems

To understand this PLKG system, let us consider a scenario, as shown in Fig. 2, in which two wireless nodes say, Alice and Bob, wants to communicate with each other in presence of an intruder (Eve), who wants to decipher the information exchanged between them. It is considered that Eve is situated at a distance greater than λ/2, where, λ is the communication wavelength between Alice & Eve and Bob & Eve. Eve not able to predict important information shared between Alice and Bob, due to encrypted data. Encryption is done via suitable hash algorithm.

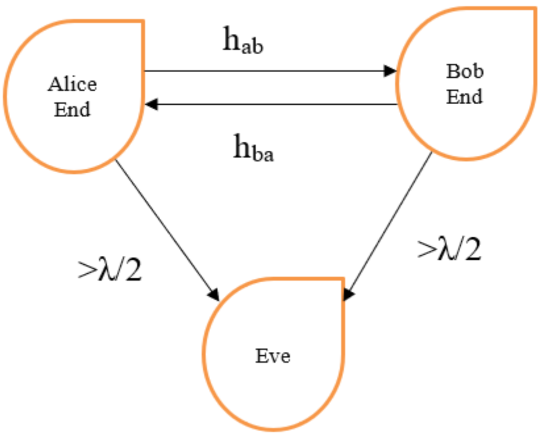

Fig. 2. Channel modelling with passive Eve [9]

It is clear from the figure 1 that, initially, RSS data was exchanged between Alice and Bob in probing period via beacons exchanged between them. This RSS data contains channel response between them [9]. The channel is probed for sufficient time intervals so that a sufficient number of samples can be acquired. In stage 2 preprocessing of raw RSSI is done which is used to improve performance parameters of PLKG system. Preprocessing can be done by any one of the methods discussed ahead like PCA, Individual Component Analysis (ICA), Kalman filtering, median filtering, etc.[10-15]. Preprocessed data is then forwarded to the next stage. Before forwarding it to quantization stage, in dimensionality reduction technique required number of components are selected which helps to reduce data dimensions and also computational delays in the subsequent blocks for the PLKG system. In stage 3, this preprocessed data is quantized using different available quantizers. In this stage, the RSSI data is converted into a bit stream, which is further processed to generate keys. Quantization helps in further improvement in PLKG system parameters like BDR and Entropy. Different types of quantizers are available such as, lossy and lossless quantizers: lossy quantizers help to generate less no of bits per sample with high entropy in the quantized bits whereas lossless quantizers have extra setup to improve randomness and generated one or more no of bits per sample. Then quantization can also be done using uniform and non-uniform quantizer or adaptive quantizer. In uniform quantizer, quantization levels were uniformly distributed whereas, in adaptive quantizer additional criteria required to set quantization levels. Furthermore, quantizers used by researchers are linear quantizer, double threshold quantization method, Llyod max quantizer etc. [16-22]. Next, in stage four, information reconciliation takes place, which allows partial information sharing between Alice and Bob. This process ensures exact same keys at both ends. Various error-control coding techniques such as low-density parity check (LDPC) code, Bose-Chaudhuri-Hocquenghem (BCH) code, Turbo code, hamming code, etc.[23-26], helps to generate same keys at both ends. As partial information is exchanged over channel, so they are now open to intruders/attackers and can be deciphered easily. So, to avoid such problem, the last stage of the PLKG system is used as privacy amplification. This stage helps to generate more randomized and encrypted keys using different secure hash algorithms. Various secure hash algorithms available are: SHA 1, SHA 2, SHA 160, SHA 256, etc. [27–29].

PLKG system is a promising solution for secure future generation wireless networks, because it overcomes the problems related to traditional cryptographic techniques. It is evident from the discussion made ahead that preprocessing of raw RSSI using dimensionality reduction preprocessing such as PCA plays an important role in designing an improved PLKG for low power wireless network. PCA has capability to reduce data dimensions effectively, because it provides multiple components, out of which few can be selected on some predefined basis. PCA gains its importance because of various advantages like: it is computationally efficient because it uses linear algebra to solve problems. Furthermore, it helps machines to converge faster. It also helps to reduce the overfitting of the prediction algorithms. So, due to all these advantages, various authors use PCA as preprocessing / dimensionality reduction technique and generate better results for their proposed PLKG networks. Some of the contributions using PCA is discussed ahead. Ankit Soni et.al. [30] propose a novel method to generate secure keys between Alice and Bob with improved BDR, randomness, and computational complexity. They propose to use PCA as preprocessing technique, which reduces data dimensions. This dimension reduction helps to improve system performance in terms of reduced computational complexities of subsequent blocks of the PLKG system. Their results show that BDR improves significantly for low-powered IoT-like systems. In [31] author proposes the PCA method to reduce the dimensions of the input data vector and use only principal dominant components to generate their security keys. The author also verified their proposed work using the practical experimental setup with node MCU ESP8266 and also check the randomness of generated keys using the NIST test. The author in [32] proposes a novel hybrid AvDR algorithm, in which they use a moving averaging-based filtering technique for reducing white, coloured noise effects in RSSI data. The author first removed unwanted severances from the data set using a filtering technique then uses PCA as a dimensionality reduction technique to reduce data dimensions. From the reduced data set, dominant principal components based on information content and cross-correlation were selected, which helps to reduce computational delays furthermore. They compare their results based on BDR, randomness among keys, for different scenarios like data containing: White noise only, White and Colored Noise, White & Colored with MWA and White & Colored with AvDR and found their proposed algorithm outperforms all four methods. Raksha Upadhyay et. al. [33] show a comprehensive study on how PCA works for a PLKG system with AWGN noise and Racian Channel modelling. For the implementation of the proposed work, the author used an experimental set-up using Node MCU ESP8266 (at the frequency of 2.4 GHz).In this work, different groups of data sets with varying dimensions were made and it has been shown that the data set with dimension 15*10 outperform, out of 15 principal components, 5 components are selected based on maximum information content. It has been shown in the paper that PCA with high SNR gives the best result in terms of dimensionality reduction. So, it is concluded that component selection based on information content helps to improve PCA performance in a better way. In [34] author presented a comprehensive study on how Discrete Wavelet Transform (DWT) and PCA behave for LoRaWAN-type networks. The author uses DWT and PCA as preprocessing techniques to remove those components which create redundancies in the collected data set. The proposed work compares the performance of both preprocessing techniques with a different number of components used and block size, based on the Key disagreement rate (KDR) and correlation between them. Their results show that PCA outperforms DWT in terms of reduced KDR and higher correlation among selected components.

Therefore, it is clear from the above literature that RSSI pre-processing and use of effective component selection technique results in improved system performance. Hence, the motivation behind the paper is to reveal different ways of selecting components which helps to improve network performance in terms of BDR in a better way. In this paper, we present different criteria for selecting number of components, which helps to generate more randomized key sequences along with PCA as a preprocessing method. We compare our work with existing algorithm that uses PCA as preprocessing technique and perform component selection using information contained in preprocessed components. Performance of different component selection methods was compared in terms of BDR and found that component selection based on Histfit outperforms. The rest of the paper is organized as: section 2 contains the proposed work and methodology. Section 3 explains the simulation and results and section 4 concludes the paper, followed by references.

II. METHODS

For the considered PLKG system, out of five main stages preprocessing of raw RSSI and component selection are very crucial aspects for improving system performance. For preprocessing of raw RSSI, we use PCA and for effective component selection we use any of the three criteria discussed below:

A. Component Selection Methods

Selection of required and relevant components is a crucial aspect because it reduces computational complexities, which in turn reduces power requirement of the system. This feature helps to design more effective future generation smart energy aware networks. For an efficient component selection, we suggest three criteria (1) Information content based (2) Mean based (3) Histfit and Standard deviation based. Let us discuss these criteria one by one.

1) Information Content based

In this method of component selection, we select components as per information content by them, which are termed as principal components. In this criterion we select only those components which contains minimum 70-90% information in them [30]. The information content was calculated as per equation 1 [30] below, where s is the number of principal components selected out of k components generated after PCA preprocessing.

$$\boldsymbol{I_c = 100 \sum_{p=1}^{s} I_p \,/ \sum_{j=1}^{k} hjj} \dots\dots\dots\dots\dots\dots\dots.(\mathbf{1})$$

we can select ‘n’ number of principal components out of available ‘k’ preprocessed components. By doing so, we are actually reducing number of samples to be processed for key generation and hence, power consumption of the network is reduced.

2) Mean Based

In this method initially, we calculate the mean of actual RSSI signals for both Alice and Bob's end. After this, we calculate the mean of ‘k’ number of preprocessed components individually. Then, out of ‘k’ number of components we select only those ‘n’ components which have a mean much closer to the mean of Alice and Bob end. The formula used for the mean is shown in equation 2 below, where n is the number of components and x is the component signal vector.

$$\mu = \frac{1}{n}\sum_{j=1}^{n-1} x_j \dots\dots\dots\dots\dots\dots\dots\dots\dots..\dots..(2)$$

3) Histfit and standard deviation Based

In this method of component selection, we will plot Histfit graphs for all ‘k’ number of preprocessed components and by calculating their standard deviation, we will categorise these components as more information signal or as a noisier signal. We select least deviated components as more information signal. Whereas components having high standard deviation are considered as noise or low information signals. After selecting ‘n’ number of more information components from this set of components, we forwded them to generate keys and lastly BDR is calculated.

B. *Proposed PLKG system*

In proposed PLKG system, we try to give more emphasis on preprocessing stage and component selection method, because it affects network performance greatly. Fig.3 shows the proposed PLKG system considering component selection method as an important aspect. In stage 1of proposed PLKG system, channel sensing was done in which both Alice and Bob exchanged RSSI (beacons) between them to sense channel performance. Here we use Racian channel model with AWGN noise for channel simulation. In stage 2 of preprocessing, we apply PCA as a preprocessing/dimensionality reduction technique to reduce the raw RSSI data set to a new data set with reduced dimensions.

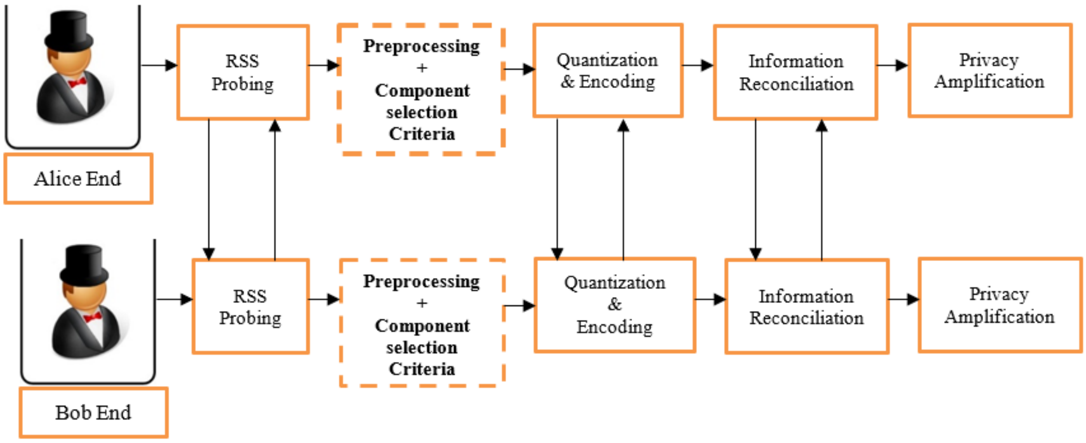

Fig. 3. Proposed PCA preprocessing based PLKG system

The steps involved in implementing PCA block is shown in Algorithm 1. Initially, PCA takes probed RSSI input data matrix of dimension m*k which is to be processed. Then mean of the input matrix is calculated. Now, with the help of input matrix and its mean, PCA generates a covariance matrix for the data set. Now, from this covariance matrix, PCA suggest to choose number of components as per our requirement. This helps to reduce the dimension of input data matrix from m*k to m*n. This final m*n data matrix gives us a set of principal components and further it is utilized for selection of ‘n’ number of components as per our requirement.

Algorithm 1. Steps for PCA algorithm as preprocessing technique

PCA Algorithm Steps
Input data $[Ru]_{m*k} \leftarrow$ [RSSI raw data with N number of samples]
Calculation of mean of input data $[R\mu]_{m*1} \leftarrow [\frac{1}{N}\sum_{u=1}^{N} R_u]$
Subtraction of mean from input data $[Ra]_{m*k} \leftarrow [\sum_{u=1}^{N} Ru - R\mu]$
Creation of Covariance matrix $[Cm]_{m*m} \leftarrow [\frac{1}{N-1}(Ra * Ra^T)]$
Sorting Eigen values and eigen vectors from covariance matrix $[V, \lambda] \leftarrow [Cm]$
Selection of eigen vectors having largest eigen values $[D] \leftarrow$ [max Ev]
Dimension reduction $[K]_{m*n} \leftarrow [D^T*Ra]$

So, from algorithm 1 we are able to reduce raw RSSI data dimensions from [Ru]m*k to [K]m*n. This helps to reduce power requirement and computational complexity of further stages for the proposed PLKG system.

After receiving processed components, we apply proposed component selection criterions on them. After selecting relevant number of components using proposed criteria’s, we move further to stage 3, as shown in Algorithm 2. In stage 3 we apply linear quantization to convert the data vector into bits form for further processes. These quantized bits are then applied to linear block coding algorithms in stage 4 to encrypt the data for further security. In this stage, primary keys were shared between Alice and Bob to check errors in their corresponding bit sequences at Alice and Bob end. These errors can be corrected using error-correcting codes in such a way that final keys should have low disagreement between them. At last, to remove the effects of sharing primary keys over the channel and encryption of final keys, we apply SHA160 code to encode our key sequence. This encoding performs the function of not only encrypting the keys but also

improves the randomness in the final generated keys at both Alice and Bob's end.

Algorithm 2. Steps for Proposed PLKG system

Proposed PLKG System
//Raw RSSI **Input data :** {RSSI}
Step 1: Channel Prediction $\hat{r}_u \leftarrow$ $RSSI_u$
Step 2: Preprocessing Stage **2(a): Formation of Input Block matrix** $[\hat{R}_u]_{m*n} \leftarrow [\hat{r}_u]$
2(b): Reducing dimension using PCA algorithm $[\hat{R}_u]_{m*k} \leftarrow [\hat{R}_u]_{m*n}$
Step 3: Component Selection based on either of 3 methods below 1. Component selection using information content based criteria. 2. Component selection using mean based criteria. 3.Component selection using Histfit criteria.
Step 4 :Linear Quantization $[\hat{R}_u]_{m*k} :\{0,1\} \leftarrow \mathcal{LQ}([\hat{R}_u]_{m*k})$
Step 5: Information Reconciliation $SK_u:\{0,1\} \leftarrow \iota\mathbb{R}([\hat{R}_u]_{m*k} :\{0,1\})$
Step 6: Privacy Amplification (Hash coding) $SK_u^{160}:\{0,1\}^{L=160} \leftarrow \mathcal{H}(SK_u:\{0,1\})$
Final Output : SK_u^{160} //160 Bit Secured Key

Finally, we compute BDR for key sequences generated at both Alice and Bob end using equation 3. Where $A_k(i)$ *and* $B_k(i)$ are bit sequences generated at Alice and Bob end respectively and l_k is the length of key.

$$BDR = \frac{\sum_{i=1}^{l_k} |A_k(i) - B_k(i)|}{l_k} \dots\dots\dots\dots\dots\dots\dots\dots (3)$$

III. RESULTS AND DISCUSSIONS

To carry out simulation of proposed system along with the preprocessing technique, we use MATLAB platform. The total sample size is considered 1 X 2000 at both Alice and Bob end as shown in Fig. 4. Furthermore, to make the system a real practical scenario we add Additive white gaussian noise (AWGN) to samples at Alice and Bob's end.

Figure 5 shows 20 components generated after preprocessing using PCA at Alice and Bob. It is clear from the figure the first few components contain maximum information as depicted by maximum variation in the signal and decreases till last component with least variation.

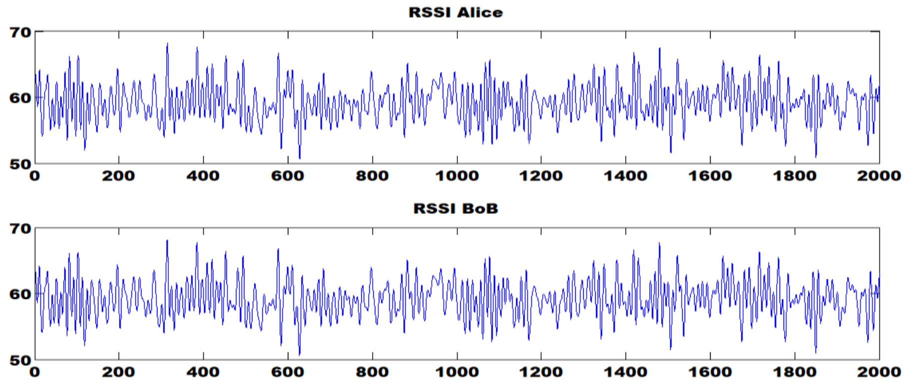

Fig. 4. RSSI for Alice and Bob End

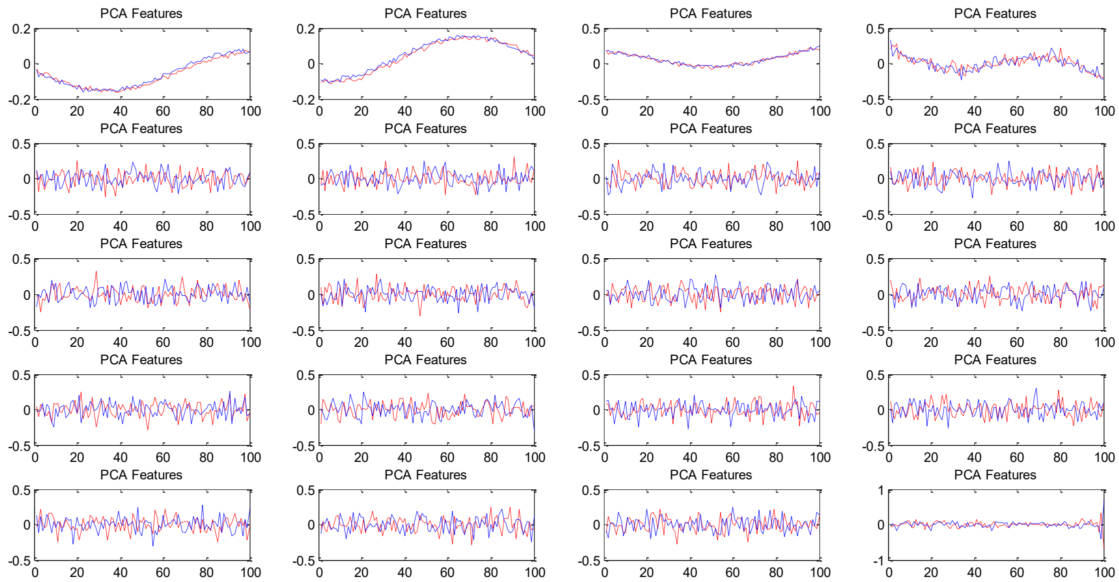

Fig. 5. Principal components extracted after preprocessing

Now, we need to select 'n' number of components out of these 20 preprocessed components using any of the proposed criterions i.e. (a) Information content based (b) Mean based (c) Histfit and standard deviation based.

A. Component selection using information content by individual components

In this method, we calculate the cumulative energy content and relative energy content, as shown in fig. 6, for each 20 components generated after preprocessing stage. In this method, we select only those components which passes threshold criteria of having 70% to 90% information in them. From Fig. 6 it is clear that as per threshold criteria, we can choose first two components and can reject rest of the low information content components. After selection of this two components out of 20 generated components, we calculate BDR for the generated keys using those two components.

Above selection criteria can also be justified by calculating correlation between 20 processed components. We calculate correlation of S_{th} component at Alice end with S_{th} component at Bob end. The correlation for these 20 components is shown in Table I. From the table, it is concluded that the initial two components selected by our criteria have a maximum correlation with each other, which shows that they will have maximum matching keys at both end, resulting in minimum BDR.

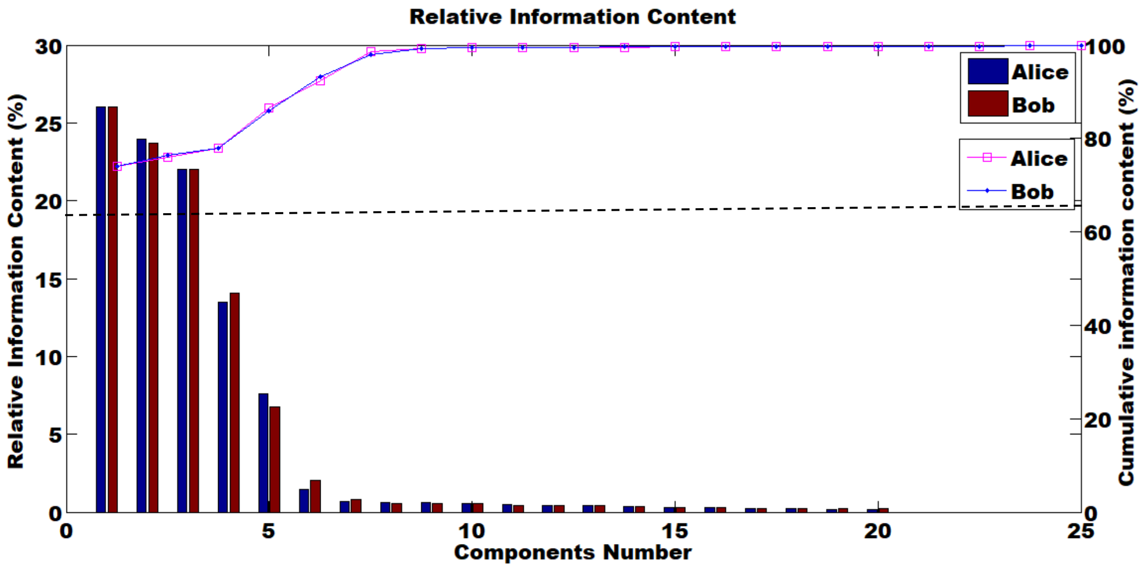

Fig. 6. Information extracted from Principal components

TABLE I
CORRELATION COEFFICIENT OF DIFFERENT PRINCIPAL COMPONENTS AT BOTH ALICE AND BOB END CORRESPONDINGLY

Correlation coefficient of different principal components										
ρ_{AB}	***0.9683***	***0.9484***	0.9700	0.9651	0.9263	0.6595	0.06967	0.1258	0.0255	0.0883
I_{th} PC	1	2	3	4	5	6	7	8	9	10
ρ_{AB}	0.1724	0.0746	0.1358	0.0035	0.0166	0.0423	0.0469	0.1014	0.0123	0.1314
I_{th} PC	11	12	13	14	15	16	17	18	19	20

B. Component selection using mean based method

In this method, we select components based on the mean as the statistical parameter. Initially, we calculate the mean of the actual RSSI signal at Alice and Bob's end individually. Then, we calculate the mean of all 20 components generated after preprocessing. Now we select only two components (as we select 2 components in the above criteria, so for sake of comparison we select 2 components as well in the rest of the criteria) which are closer to the actual mean of Alice and Bob RSSI signals. Then BDR is calculated using those two components for the generated keys. Table II shows the actual mean values of Alice and Bob's RSSI data and the mean of 20 components in a sorted form. In this manner we are able to select only those components which have closeness to actual RSSI signal and it resembles that, component which is selected is actual information signal.

TABLE II
VALUES OF MEAN FOR ALL 20 COMPONENTS AFTER PREPROCESSING USING PCA ALGORITHM

At Alice End Actual mean - 49.5470		**At Bob end Actual mean - 49.5265**		**At Alice End Actual mean - 49.5470**		**At Bob end Actual mean - 49.5265**	
Component Number	Mean value	Component Number	Mean value	Component Number	Mean value	Component Number	Mean value
C13	12.59	C13	12.37	C10	11.12	C18	11.24
C9	11.93	C3	11.96	C8	11.10	C10	11.06
C20	11.89	C15	11.91	C1	11.08	C14	10.96
C6	11.84	C9	11.87	C19	10.80	C16	10.95
C3	11.84	C20	11.83	C12	10.80	C7	10.87
C15	11.78	C6	11.76	C7	10.77	C1	10.80
C4	11.75	C2	11.61	C5	10.76	C12	10.66
C2	11.55	C4	11.58	C14	10.69	C19	10.61
C17	11.19	C17	11.49	C16	10.34	C11	10.58
C18	11.16	C8	11.29	C11	10.32	C5	10.35

C. *Component selection using Histfit and standard deviation criteria*

In this method of component selection, we use Histfit patterns of 20 components generated after preprocessing, as shown in Fig.7. Histfit graphs helps to analyse the data set using histograms and corresponding gaussian curve fittings.

Now, we calculate standard deviation of each Histfit graph, which is shown in Table III. After calculating the standard deviation of each 20 component, we categorize them as more information component and noisy component based on standard deviation value. From these two categories we select two components as more information content component and two components as noisy component on the basis of Histfit and std deviation among 20 preprocessed components. These two components at both ends, from each category will be selected for further key generation and BDR calculation.

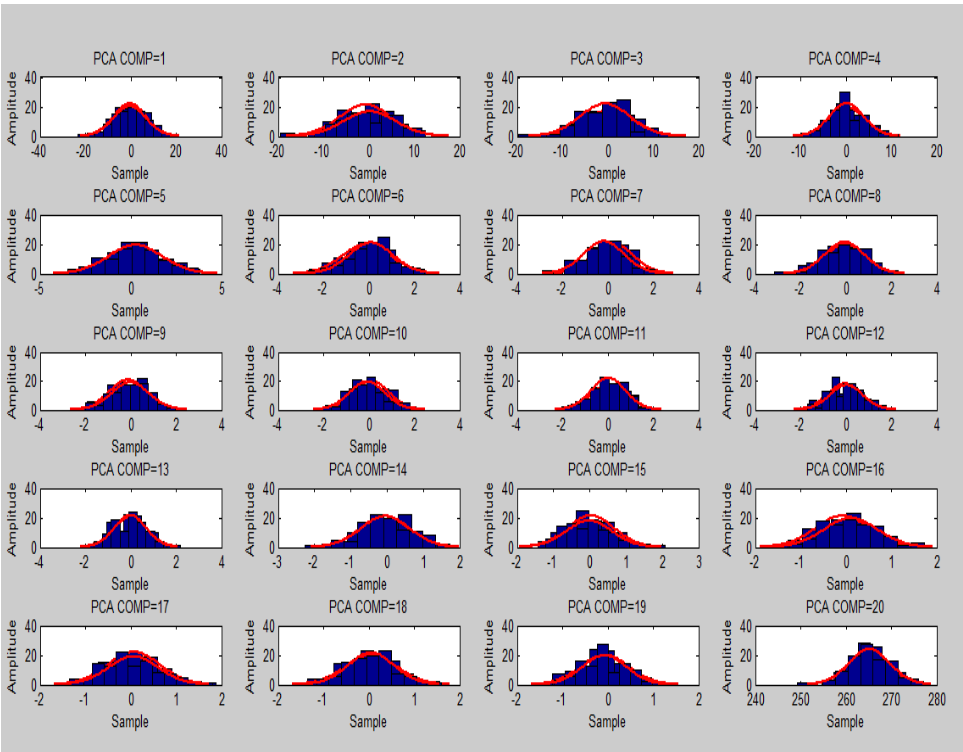

Fig. 7. Histfit of extracted Principal components

Table III
Values of standard deviation of Histfit for all 20 components

At Alice End		At Bob end	
Component Number	**Std. Dev.**	**Component Number**	**Std. Dev.**
19	5.325	3	6.004
9	6.046	4	6.169
4	6.162	20	6.577
3	6.306	1	6.598
15	6.325	8	6.678
1	6.364	9	6.76
18	6.366	16	6.966
20	6.491	11	7.127
13	6.691	14	7.16
14	6.708	5	7.175
2	6.872	6	7.182
7	6.881	12	7.343
10	6.922	2	7.455
5	7.001	19	7.49
12	7.1	10	7.711
11	7.119	17	7.822
16	7.19	7	7.844
8	7.293	18	8.006
17	7.368	13	8.166
6	7.812	15	8.187

Now, after understanding the three component selection criteria, we select best two components from each criterion to generate final secure keys. Finally, after generating keys for each proposed criteria, we calculate BDR at different SNR values and figure 8 shows the relationship between them. From figure 8, it is concluded that component selection using criteria - PCA with Histfit outperforms. First two selection criteria underperform because channel offers racian distribution along with AWGN noise, which reduces the evenness of gaussian curve and may shift the mean value of overall signal and multiple PCA components.

So, the proposed work gives a new dimension to the PLKG system as far as the component selection was concern. Result shows that component selection affects the system parametrs and will be improved by using proper component selection method.

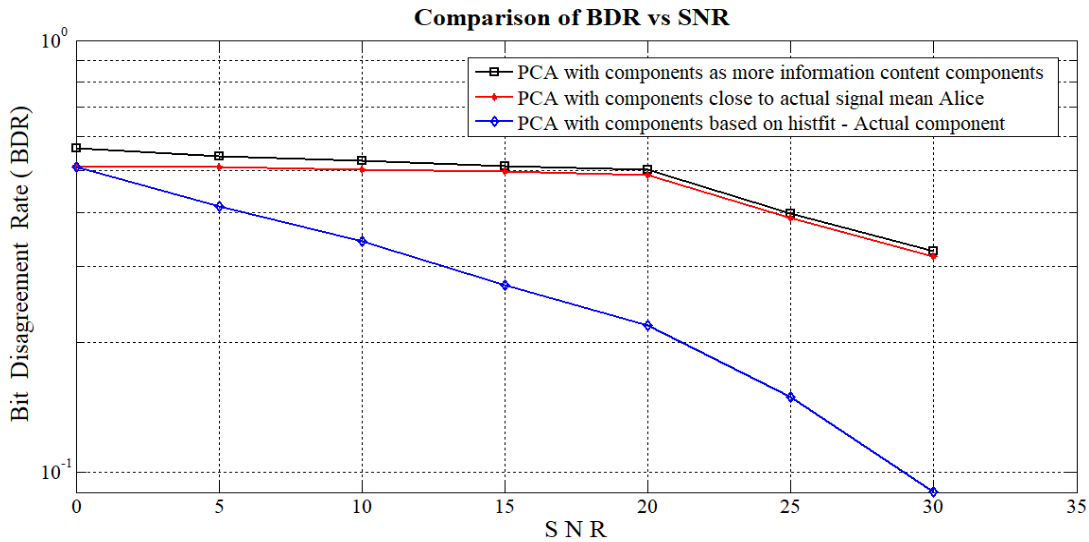

Fig. 8. BDR Vs SNR graph for PCA algorithm using different component selection approach

IV. CONCLUSION

Recent advancements in future-generation wireless applications lead to advancement in highly secured and easily accessible wireless networks like IoT. This type of network utilizes the merits of wireless networks to provide such solutions, but simultaneously they are moving towards easy access to intruders over a wireless channel. To make them more secure and reliable, various research carried out in the past few decades summarizes that physical layer securities are more promising solutions instead of traditional cryptographic techniques. In this paper, we present a comprehensive study of the component selection technique of a PCA based PLKG system for probed signals exchanged between Alice and Bob. We evaluate the performance of component selection using: information or energy content of the signal, mean method, Histfit and standard deviation method. The study compares the performance of different methods based on BDR over different SNR values. Results shows that preprocessing of RSSI and proper component selection method helps to improve network parameters more effectively. Histfit and standard deviation based component selection criteria outperforms. In future, we can analyze such work with different dimensionality reduction techniques like individual component analysis (ICA) as preprocessing techniques along with other statistical parameters like kurtosis as component selection criteria.

ACKNOWLEDGEMENTS

We would like to acknowledge IET, DAVV, Research Centre, Indore, India. This paper can be used as part of a Ph.D. thesis in the future for the first author.

FUNDING STATEMENT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] S. Das, S. Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure," Computers and Electrical Engineering, 101, 107991. 2022.

[2] N. S. Patankar, P. Kumar, R. Karan and A. Dubey, "Efficient Secrete Key Generation for Internet of Things Communication Device Using Discreet Wavelet Packet Transform," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 459-464, 2021. https://doi.org/10.1109/CSNT51715.2021.9509689

[3] V. Kumar et. al., "Seamless Wireless Communication Platform for Internet of Things Applications," In IEEE Wireless Communications, 2022. https://doi.org/10.1109/Mwc.006.220009

[4] M. Mitev, A. Chorti, E. V. Belmega, and H. V. Poor, "Protecting Physical Layer Secret Key Generation from Active Attacks," Entropy, vol. 23, no. 8, p. 960, Jul. 2021, https://doi.org/10.3390/e23080960

[5] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), pp. 1-5, 2019. https://doi.org/10.1109/3ICT.2019.8910320

[6] G. Mustafa, R. Ashraf, M. A. Mirza, A. Jamil, and Muhammad, "A review of data security and cryptographic techniques in IoT based devices," In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18). Association for Computing Machinery, New York, NY, USA, Article 47, 1–9, 2018. https://doi.org/10.1145/3231053.3231100

[7] Y. Liu, H. Chen and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347-376, First quarter 2017. https://doi.org/10.1109/COMST.2016.2598968

[8] T.Sarsodia, U. R. Bhatt, and R. Upadhyay, "Applications of RSSI Preprocessing in Multi-Domain Wireless Networks: A Survey," Advances in Computing and Network Communications. Springer, Singapore, 389-403, 2021.

[9] A. Soni, R. Upadhyay, & A. Kumar, "Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging," Physical Communication, 33, 249-258, 2019.

[10] J. Zhou, & X. Zeng. "Physical-layer secret key generation based on domain-adversarial training of autoencoder for spatial correlated channels," Applied Intelligence, 1-16, 2022.

[11] L. Alsmadi, X. Kong, K. Sandrasegaran and G. Fang, "An Improved Indoor Positioning Accuracy Using Filtered RSSI and Beacon Weight," in IEEE Sensors Journal, vol. 21, no. 16, pp. 18205-18213, 15 Aug.15, 2021, https://doi.org/10.1109/JSEN.2021.3085323

[12] R. Venkatesh, Vikas Mittal, and Hrudaya Tammana, "Indoor Localization in BLE using Mean and Median Filtered RSSI Values," 5th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 227-234. IEEE, 2021.

[13] R. Upadhyay, P. Panse, A. Soni and U. R. Bhatt, "Principal Component Analysis as a Dimensionality Reduction and Data Preprocessing Technique," Proceedings of Recent Advances in Interdisciplinary Trends in Engineering & Applications (RAITEA) 2019, http://dx.doi.org/10.2139/ssrn.3364221

[14] Y. Shen, B. Hwang and J. P. Jeong, "Particle Filtering-Based Indoor Positioning System for Beacon Tag Tracking," in IEEE Access, vol. 8, pp. 226445-226460, 2020, https://doi.org/10.1109/ACCESS.2020.3045610

[15] G. Qi, Y. Jin and J. Yan, "RSSI-based Floor Localization Using Principal Component Analysis and Ensemble Extreme Learning Machine Technique," 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP), pp. 1-5, 2018. https://doi.org/10.1109/ICDSP.2018.8631549

[16] S. Lv, H. Hong, L. Yang, J. Ding and R. Song, "Solving In-door Human Activity Recognition via RFID based on Unsupervised Domain Adaptation," 2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS), pp. 388-392, 2022. https://doi.org/10.1109/ICPICS55264.2022.9873745

[17] G. Li, H. Yang, J. Zhang, H. Liu and A. Hu, "Fast and Secure Key Generation with Channel Obfuscation in Slowly Varying Environments," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, pp. 1-10, 2022. https://doi.org/10.1109/INFOCOM48880.2022.9796694

[18] A. D. Wyne, "The wire-tap channel," Bell system technical journal, 54(8), 1355-1387, 1975.

[19] T. Jolliffe, "Principal component analysis," 2002. Available: http://link.springer.com/book/10.1007%2Fb98835.

[20] J. L. Padilla, P. Padilla, J. F. Valenzuela-Valdés, J. Ramírez, & J. M. Górriz, "RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation," Measurement, 58, 468–475, 2014.

[21] O. Graur, N. Islam, & W. Henkel, "IEEE Globecom Workshops (GC Wkshps)" Washington, DC, 1-7, 2016.

[22] M. Adil, S. Wyne, & S. J. Nawaz, "On quantization for secret key generation from wireless channel samples.," IEEE Access, 9, 21653-21668, 2021.

[23] K. Moara-Nkwe, Q. Shi, G. M. Lee and M. H. Eiza, "A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 11374-11387, 2018. https://doi.org/10.1109/ACCESS.2018.2806423

[24] O. Graur, "Quantization and LDPC-based Key Reconciliation for Physical Layer Security (Doctoral dissertation, Jacobs University Bremen)," 2022.

[25] V. Kalokidou, M. Nair, & M. A. Beach, "LoRaWAN Performance Evaluation and Resilience under Jamming Attacks," In 2022 Sensor Signal Processing for Defence Conference (SSPD), pp. 1-5, IEEE, 2022.

[26] B. Y. Tang, C. Q. Wu, W., Peng, B. Liu, & W. R. Yu, "Polar Codes-based Information Reconciliation Scheme with Frozen Bits Erasure Strategy for Quantum Key Distribution," arXiv, 2022. preprint arXiv:2203.02074.

[27] L. Zhang, X. Huang, Z. Chai, Z. Shen, W. Hu, & X. Yang, "Unidirectional physical layer secure key distribution in a fiber channel assisted by neural networks," Optics Letters, 47(16), 4263-4266, 2022.

[28] J. Li, "Comparative Analysis of Some Typical Encryption Algorithms and Hash Algorithms," In 2022 International Conference on Big Data, Information and Computer Network (BDICN), pp. 27-30, IEEE, 2022.

[29] J. G. Sekar, C. Arun, S. Rushitha, B. Bhuvaneswari, S.C. Sowmya, & N. S. Prasuna, "An improved two-dimensional image encryption algorithm using Huffman coding and hash function along with chaotic key generation," In AIP Conference Proceedings Vol. 2519, (1), p. 030105, AIP Publishing LLC, 2022.

[30] A. Soni, R Upadhyay, & A. Kumar, "Low Complexity Preprocessing Approach for Wireless Physical Layer Secret Key Extraction Based on PCA" Wireless Pers Commun 125, 2865–2888, 2022. https://doi.org/10.1007/s11277-022-09689-9.

[31] A. Soni, R.Upadhyay and A. Kumar, "Dimensionality Reduction in Wireless Physical Layer Key Generation," 2019 IEEE 16th India Council International Conference (INDICON), pp. 1-4, 2019. https://doi.org/10.1109/INDICON47234.2019.9029059

[32] A. Soni, R. Upadhyay, and A. Kumar, "AvDR-Based Wireless Secure Key Generation with Colored Noise for IoT," Fluctuation and Noise Letters 19(01), 2050013, 2020.

[33] R. Upadhyay et al, "A study on principal component analysis over wireless channel," J. Telecommun. Electron. Comput. Eng., 11(4), 5-9,2019.

[34] P. I. Da Cruz, , R. Suyama, and M. Bellezoni Loiola. "Increasing key randomness in physical layer key generation based on RSSI in LoRaWAN devices," Physical Communication 4, 101480, 2021.