International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Survey of Key Generation Techniques in Wireless channels for Physical Layer Security

Sujata Kadam[1], Joanne Gomes[2]

Submitted: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

Abstract: Nowadays wireless networks are highly concerned about security. Compared to wireless networks, wired networks are less prone to attacks. The physical layer eavesdropping attack has a significant impact on wireless network security. The use of cryptographic methods at the higher layers of the OSI model is necessary for traditional security in wireless networks. These cryptographic keys can be replaced with key generation at physical layer exploiting the unpredictable channel properties. Current methods for generating wireless keys at the physical layer are examined in this paper. Comprehensive surveys in this regard are conducted of the guiding principles, performance indicators, and key generation process. Techniques for enhancing the effectiveness of key generation are also reviewed. The difficulties of using the strategy in each situation are then discussed, along with key generation applications in diverse situations. The paper ends with several recommendations for future investigations.

Keywords: *Channel probing, Information reconciliation, Key generation, Physical layer security, Wireless network.*

1. Introduction

In wireless networks, security is the quality or state of being secure. It entails fortifying defenses against enemies and those who would harm people either intentionally or accidentally. Wireless communication networks are more susceptible to attacks than wired networks because of it's open nature [1]. Both Passive and active attacks affect wireless networks [2]. An intrusion attempt to overhear data transmission between authorized users is known as a passive attack. Eavesdropping is the most frequent form of passive attack at the physical layer [3]. However, an active attack interferes with authorized users usual interactions, alters the data they transmit to each other, and has a significant negative influence on the system. The most frequent active attack types include information leak, denial of service (DOS), message alteration and fraudulent activity [4]. To protect wireless communication, there has been a lot of study attention. Currently Cryptography is used to allow Secure Communication over an insecure channel. Cryptography is the process of encrypting the messages thereby making it secure from the different attacks. Cryptography can be classified into symmetric key Cryptography and asymmetric key Cryptography. Computational time of cryptographic systems includes encryption/decryption time, key generation time, and key exchange time [5,6]. The size of the key length, which varies for symmetric and asymmetric cryptography, determines how long keys take to generate. Key exchange times vary based on the sender and receiver's communication channels [7,8]. Numerous cryptographic methods have been developed and are used for encryption and decryption [9-10]. As previously mentioned, symmetric and asymmetric algorithms are the two categories under which encryption systems fall. Public key cryptography, also known as asymmetric cryptography, secures communication by using both public and private keys, whereas symmetric

cryptography (also known as Private key cryptography) focuses on ensuring secure communication between sender and receiver by using the same secret key [11-13]. The key is self-certified according to the self-certification mechanism. It is necessary to communicate secretly in order to exchange the key. To define symmetric key cryptography, numerous algorithms have so far been created. These include AES, DES, RC4, and SHA. Unlike public keys, which are known to everyone because of their nature as being public, private keys are held privately in communication. In this strategy, the message is scrambled utilizing the recipient's public key and decoded utilizing the recipient's private key. Digital signatures are utilized to certify the keys here rather than the idea of self-certification. The secrecy is maintained, making this method more convenient and offering superior authentication [14]. This encryption process is implemented using a variety of algorithms. RSA, Diffie-Hellman, ECC, and the digital signature algorithm are among them. Key size is the most crucial factor in symmetric and asymmetric cryptography for communication security. Symmetric cryptography is less secure and its keys are smaller than those used in asymmetric cryptography [15-16]. The issue of complex key management is present in both symmetric and asymmetric encryption techniques. Physical layer security (PLS) is a novel strategy to tackle the issue of cryptographic

[1] *RAIT Institute, Nerul, Navi Mumbai, Maharashtra, India*
ORCID ID: 0000-0003-2075-9818
[2] *SFIT, Borivli, Mumbai, Maharashtra, India*
ORCID ID: 0009-0001-1882-2120
Sujatakadam7890@gmail.com

keys. To get a secure key, PLS utilizes the characteristics of the wireless channel. It is more secure and has advantages over traditional cryptographic approaches used at the upper layers. The development of computing technology has made it possible for hackers to employ trial-and-error approaches to decipher passwords, login credentials, and encryption PLS techniques accomplish information theoretic security using the unpredictable and random properties of wireless networks [17-23]. Higher layers in communication protocols employ conventional encryption methods, while wireless security can also be enhanced at the physical layer. To provide safe communications on the physical layer, PLS makes use of the wireless channel's innate unpredictability [24]. Comparing PLS to other cryptographic algorithms, there are several advantages because it is not dependent on computing complexity. In order to accomplish information theoretic security, PLS techniques make use of the erratic and random features of wireless communications.

In Wyner's wiretap channel model [25], which pioneered keyless security, code design is employed and the channel qualities of authorized users, and eavesdroppers are studied to provide secrecy without the use of keys. Because of the medium's inherent randomness, the eavesdropper's signal-to-noise ratio (SNR) might, in fact, be on pace with or even superior to that of the authorized channel in practice. Thus, in such circumstances, Wyner's views are ineffective. A Gaussian wiretap channel is used in [26]. The generation of keys through wireless channels is one method of establishing the key. On the other hand, efficiently establishing random keys between trustworthy users that cannot be reused is highly difficult. By using key generation instead of public key cryptography, the system's security is increased.

In order to achieve information-theoretic security against being attacked and eavesdropping PLS is becoming more and more popular recently. Information is shared through wireless networks between authorized users, but it is susceptible to different malicious threats on account of broadcast nature of the wireless media [27].

Recent years have seen a great deal of academic interest in physical layer key generation. While theoretical research has demonstrated the capability to produce information-theoretic secure keys, there are still significant obstacles to overcome when putting the theory into practice. It has drawn a lot of interest recently because of its alluring qualities of simplicity and information-theoretic security. Key generation includes various stages such as channel probing, quantization, information reconciliation and privacy amplification. The main difficulties are choosing the compression ratio in the privacy amplification step, dealing with channel measurement correlations, lowering reconciliation overhead, and determining how difficult it is to measure the information that has been leaked to keys, which can be harmful for any cryptosystem. But the PLS ensures that only the intended users will be able to decode sensitive messages by taking advantage of wireless channel features. PLS schemes can be classified as keyless and secret key-based.

eavesdroppers. So current methods for generating wireless keys are examined in this paper. The guiding concepts, performance measures, and key generation process are all thoroughly surveyed. Also reviewed the methods for improving key generation efficiency. The challenges of employing the technique in each circumstance is then examined, along with significant generation applications in various circumstances.

This paper provides detailed analysis of the literature on important key generating system strategies. Additionally, we identify critical key generation research topics that still require clarification and make recommendations for additional studies.

The rest of the paper is organized as follows. Section 2 introduces physical layer Security. Section 3 discusses the key generation procedure. Section 4 explains the performance optimization. In Section 5 a review of different application scenarios is done. Section 6 discusses open research issues and section 7 is the conclusion part.

2. Physical Layer Security

Physical layer threats include eavesdropping and jamming. As demonstrated in Fig 1. eavesdropping is a passive attack. Here the eavesdropper (Eve) seeks to listen the communication taking place between the authorized users (Alice and Bob) [28].

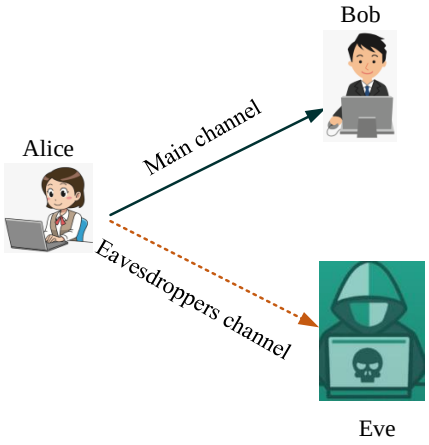

Fig 1. Eavesdropping attack [28]

Performance analysis of PLS with passive eavesdropper have been completed in several papers, including [29–31]. Another possibility is that Eve is actively involved and performs deliberate interference which includes jamming, adulteration, alteration, and denial of service [32]. Analysis of PLS where Alice is an active eavesdropper and is aware

of Eve's channel, may be found in [33]. Since PLS is not dependent on computing complexity, it has a significant advantage over other encryption algorithms. Therefore, even if the eavesdropper has unlimited computing power, the security level attained will not be impacted. PLS is classified in two basic types: Keyless Techniques and Key generation techniques. Both these techniques are as discussed below.

2.1. Keyless Techniques for PLS

For a discrete memory less wiretap channel with a source, destination, and intruder, Wyner researched information theoretic security without requiring secret keys in [25] and looked at its performance constraints. The capacity of the main link from the source node to the destination node must be higher than the capacity of the wiretap link between the source node and the eavesdropper in order to provide completely secure transmission.

For safeguarding communication Pradeep and Kanimozhi [34] suggested a hardware effective secure channel coding approach. Compared to traditional cryptosystems, the proposed non-linear system provides increased security. A block diagonal matrix with only a shift register and multiplexer as simple hardware is used. Analysis reveals that the amount of hardware used is less in comparison to the traditional system. The suggested system has very low bit error rate and very high performance ratio.

2.2. Key generation technique for PLS

Key generation technique involves generating a symmetric key between two legitimate users using the properties of wireless channel. Three guiding principles temporal variation, channel reciprocity, and spatial decorrelation are used to generate keys [35]. These principles are as explained below**.**

Temporal Variations: The movement of the source, destination, or any other channel-related item introduces temporal variation. It is possible to generate keys using the randomness produced by such unpredictable movement. In the frequency domain and the spatial domain, there is research being done to take use of unpredictability. Nevertheless, the randomness is comparatively constrained in a stationary channel as these traits are constant. Therefore, temporal variation is still necessary to create a significant amount of randomness [36]. **Channel reciprocity:** It means that multipath fading should be identical at the opposite ends of a link having similar carrier frequency. Measuring signals requires hardware platforms that typically operate in half-duplex mode. On account of the hardware limitations and the noise interference the response received on the uplink and downlink channels are not the same. To increase the channel reciprocity, various methods are employed [37-41].

Spatial variations: The cross-correlation among the authorised users and eavesdroppers channel can also be used to characterise multipath fading, which is experienced by an eavesdropper placed at a distance greater than λ/2 (λ is the wavelength) from the legitimate users [42-46]. The majority of key generation publications have stated that this attribute is crucial for making the key generation system secure. But not all circumstances might be conducive to its satisfaction. Work on spatial variations has been demonstrated in some experiments [47-49]. Since the channel is more correlated in presence of large-scale fading, extra consideration needs to be taken into account [50]. Key generation systems are insecure and need special care to prevent eavesdropping because research suggests that channel observed by eavesdropper are correlated to channel of authorised users if the distance between them is less than half of the wavelength. Spatial decorrelation hasn't generally been researched much, thus additional research is needed.

Fig 2. depicts a key generation paradigm in which Alice and Bob are attempting to create a Physical layer symmetric key. The eavesdropper Eve is listening in from a different location than Alice. A substantial possibility exists that both the users will produce similar key, and the message exchange via open channel keeps Eve in the dark.

This ensures the generated key's security and ensures the

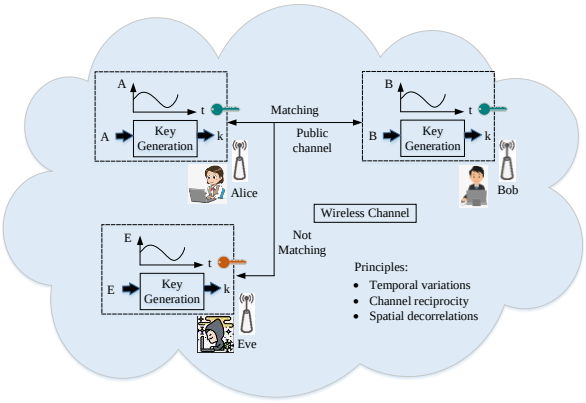

Fig 2. Model for Key generation [51]

key is disseminated equitably, which is important for physical layer key applications. Now further the Key generation technique for PLS is detailed.

Channel probing, quantization, information reconciliation, and privacy amplification are the basic elements of a typical key generation technique at the physical layer which are depicted in Fig 3. below. Each stage is briefly explained further.

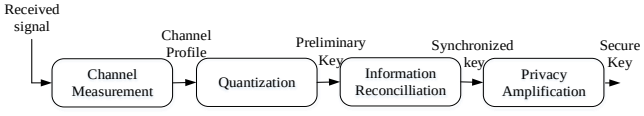

Fig 3. Key generation Technique [35]

Channel Measurements: To build the channel profile, the channel fluctuations are measured using a variety of techniques. Included among these are the received signal strength indicators (RSSI), [48] [52], channel frequency response and deep fades [53].

Quantization: To obtain the preliminary key, the probed samples are quantized into bits. Two level, Adaptive Secret Bit Generation (ASBG), High-Rate Uncorrelated Bit Extraction (HRUBE) [54], and level crossing [55] are some of the quantization techniques.

Information Reconciliation: Errors in the preliminary keys exist as a result of the channel measurement inaccuracies. In order to achieve a synchronised key, the inaccuracies are removed in the information reconciliation (IR) stage using different error-correcting codes.

Privacy Amplification: Amplification of synchronised keys is done in order to decrease the likelihood of key prediction because the eavesdropper can gain the information exchanged during the reconciliation phase. It also makes advantage of fuzzy extractors and secure hashes generation [56].

PLS schemes combine secret key-based secrecy and keyless security. Creating keys from wireless channels is one method of establishing the key. But in reality, it is incredibly difficult, to quickly create random keys between trustworthy users that can't be used again. By using key generation instead of public key cryptography, the system's security is increased. Now next section explains the key generation procedure.

3. Key generation Procedure

As depicted in Fig 4., the key generation process consists of channel probing, quantization, information reconciliation, and privacy amplification [57]. The initiator and responder roles are alternated between the two users. Alice is chosen as the initiator without losing generality.

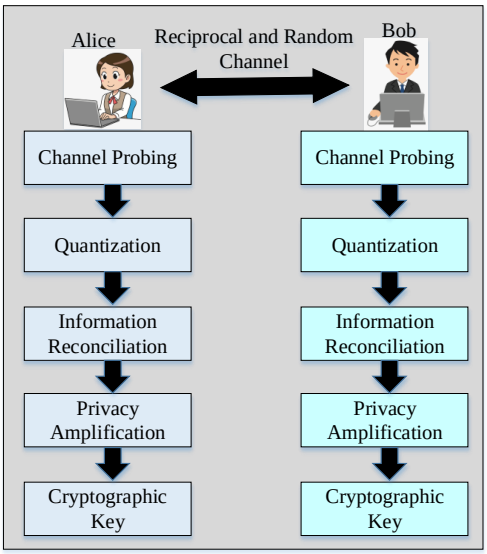

Fig 4. Procedure for key generation [57]

Channel probing is the process of obtaining information from the wireless channel. The different channel parameters such as Channel State Information (CSI), Received Signal Strength (RSS), phase or Angle of arrival (AOA) can be probed. Both Alice and Bob probe the channel. To enhance the channel reciprocity, the channel responses are smoothened before quantizing. This is pre-processing which reduces the probability of disagreement between the channel probes of both the users. The pre-processed channel response is then subjected to quantization to get the initial keys. The initial key between Alice and Bob may differ due to different variations during measurement and noise. The discrepancies in the quantized key must be removed to reduce the mismatch between the initial keys. Information reconciliation is the process of removing these discrepancies. Since the information exchanged during the reconciliation phase is overheard by the eavesdropper, some or all of the key information may be revealed. Therefore, aligned keys are now subjected to privacy amplification to obtain the symmetric secret key. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. Hash functions widely used are Message digest, secure hash functions, whirlpool and so on. At the end of Privacy Amplification stage a symmetric key is generated which is exchanged between Alice and Bob before transfer of the information between them.

3.1 Performance Metrics for Key Generation Techniques

The purpose of key generation is to generate secure symmetric keys. The key generation systems can be evaluated against various performance metrics as discussed below [58].

- **Entropy**

For a random variable x , the definition of its entropy is

$$H(x) = \sum_{i=0}^{n} p(x_i) \log 2 p(x_i) \qquad (1)$$

If x is a collection of n symbols then $p(x_i)$ denotes the probability that each symbol will appear. Entropy of a bit stream is determined using the NIST test suite. A secure key generation system should have high entropy.

- **Bit Mismatch rate (BMR)**

It is the ratio of number of dissimilar bits between Alice and Bob after quantization to the total number of input bits. It is the average bit error rate.

$$BMR = Ne / N \qquad (2)$$

Where Ne is the number of dissimilar bits between Alice and Bob and N is the total number of bits. A good key generation system should have minimum BMR.

- **Key Generation Rate (KGR)**

After accounting for bit losses caused by IR and privacy amplification, KGR is assessed in terms of the final output bits generated. It is the quantity of bits produced each second. The real-time key generation procedure needs a high KGR.

- **Key Disagreement Rate (KDR)**

When Alice and Bob generate keys, KDR is the proportion of distinct bits between those keys, and it is described as,

$$KDR = \frac{\sum_{i=1}^{n} \left| k^a(i) - k^b(i) \right|}{n} \qquad (3)$$

Length of the key is denoted as n. For successful key generation, the KDR must be low [59].

- **Randomness**

The key generation system's most crucial element is randomness. It must meet tight requirements for cryptographic applications. Testing the randomness is frequently done using NIST test suite [60-62]. The quantity of randomness that is available for extraction mostly depends on the environment. High randomness is required to generate secure keys.

3.2 Channel parameters for Key Generation

The channel parameters are the most crucial component of the key generation system [63-65].

Received Signal Strength (RSS)

In key generation, RSS is currently the major widely utilized parameter, especially for practical implementations because of its accessibility. Only one RSS value may be extracted from each packet since RSS is a coarse-grained channel information measure, which restricts the KGR. Additionally, RSS is susceptible to known channel attacks. Additionally, different manufacturers' gadgets may interpret RSS in different ways, necessitating extra caution.

Channel State Information (CSI)

A fine-grained channel parameter called CSI offers specific channel details. The channel properties of a communication link are referred to as channel state information. By combining the effects of, for instance, scattering, fading, and power decay with distance, this information illustrates how a signal travels from the transmitter to the receiver. Experimental evidence has demonstrated that CSI-based systems are resistant to predicted channel attacks and they give a high KGR.

Channel Impulse Response(CIR)

Both amplitude and phase information are present in the channel impulse response. In an interior context, the power of CIR follows an exponential distribution as it degrades over time.

Channel Frequency Response (CFR)

Channel effect in frequency domain is provided by CFR, which deals with the frequency domain.

Angle of Arrival (AoA)

Techniques for AoA estimation use antenna array systems. By analyzing how a signal interacts with an antenna array, the AOA estimation method predicts the direction of arrival of a received signal. In many military and civilian applications, particularly those involving security, estimating the AoA is an essential step.

Channel probing which is the first block of the key generation procedure is discussed in the next section.

3.3 Channel Probing

The most important stage in extracting the randomness from a channel is channel probing, which calls for two users (Alice and Bob) to alternately measure the shared channel. Bob and Alice both probe the channel alternately. It is possible to measure the different channel parameters such as RSS, AOA, and CIR.

With an electronically steered parasitic array radiator (ESPAR) smart antenna, Tomoyunki Aono et al. [66] have leveraged the fluctuation of channel properties. By manipulating the ESPAR antenna's reactance settings, it was possible to intentionally increase the channel characteristics fluctuation while using its beam-forming approach. From 384 measured RSSI values, a 128-bit secret key was produced.

When creating shared secret keys with the Multiple Antenna Key Generator (MAKE) with multi-level quantization, Kai Zeng et al. [67] evaluated the advantage of multiple antenna systems over single antenna systems. By utilizing readily available 802.11n multiple antenna devices, the authors have suggested MAKE in a real wireless system. In comparison to single antenna systems, the bit production rate is increased experimentally by using laptops with three antennae (MAKE).

For obtaining the required KGR and improving the probing performance Yunchuan wei et al. [68] focused on the adaptive channel probing. In a more static channel, one should probe more quickly, whereas in a more variable channel, one can probe more slowly to attain the same KGR. As a result, the authors have developed an adaptive channel probing technique that, without knowing the precise mapping between the probing rate and KGR, adaptively adjusts the probing rate to reach a desired KGR. According to the results of the research, the entropy rate for a static scenario can only increase to 0.27 whereas it increases to 0.71 for a mobility scenario at a probing rate of 5 Hz.

Adaptive Channel Probing using a PID Controller is shown in Fig 5.

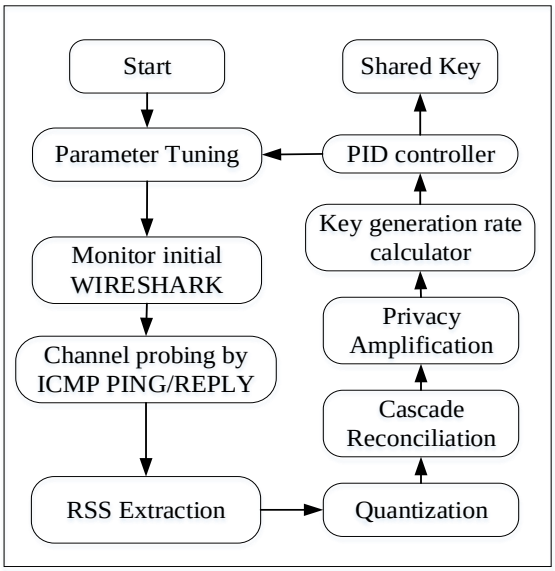

Fig 5. System for Adaptive Channel Probing [68]

It is possible to investigate many wireless channel types, including the Rayleigh, Rician, and Nakagami channels [69] [70].

Fading in wireless communication is the fluctuation of a signal's attenuation due to numerous factors. Time, geography, and radio frequency are some of these factors. A random process is frequently used to model fading. A communication channel that deteriorates with time is called a fading channel. Signals that arrive at a receiver through multiple pathways and experience multipath fading, shift in relative strength and phase. The amplitudes, phases, and directions of arrival of multipath signals are spread at random. The reception antenna is the location where signals mix vectorially and get distorted or fading. The coherence bandwidth can be used to measure the multipath channel's bandwidth.

The largest frequency difference for which signals still exhibit substantial amplitude correlation is defined as the coherence bandwidth. Multipath fading can be implemented using a variety of models or distributions, including Rayleigh, Rician, Nakagammi, Weibull, and others. According to the demands of the fading profile, these channel distributions or models are created to include fading in the baseband data stream.

When measurements are made during the channel's coherence time, the radio channel between Alice and Bob is the reciprocal of the radio channel between Bob and Alice. Because the multipath characteristics of the radio channel are the same in both directions of a link, reciprocity is possible. The sources of non-reciprocities must be considered for successful key creation. The result of these non-reciprocities is the bit disagreement in the key. Hence the channel responses are smoothed before quantization to increase the channel reciprocity and boost the efficiency of the key generation process. The probability of a discrepancy between Alice and Bob's channel probes is decreased by this pre-processing. The authors of [71] improved the channel reciprocity using three different techniques.

- L1 norm minimisation
- Polynomial Regression
- Kalman Filtering

Table 1 shows BMR and KGR for the three algorithms.

Table 1. BDR and KGR for RSSI profiles

Algorithm type	BMR (%)	KGR (bps)
L1-norm	4.5	3.41
Polynomial Regression	3.02	3.39
Kalman Filtering	6.21	3.2

A DCT-based pre-processing technique was proposed by S. Yasukawa et al. in [72] to remove redundancy from recorded amplitude characteristics. The authors of [73] have employed techniques to convert correlated, real-valued radio channel signal measurements at two nodes into uncorrelated binary data that has a high chance of bit agreement. To address the difficulties of non-reciprocities, the authors of [74] have presented an adaptive ranking based uncorrelated bit extraction (ARUBE) approach. The authors of [75] have thought about how filtering could lessen disagreement. To match the logarithmic nature of signal strength measurements provided by the receiver RSSI output data, a Savitzky Golay filter is applied. The preprocessed samples are given to a Quantizer. The different Quantization methods are discussed in the next section.

3.4 Quantization

Quantization is the process of converting analogue samples into bits. much as an analog-to-digital converter. The quantization level QL in key generation refers to the number of key bits quantized from each measurement. The signal-to-noise ratio (SNR) of the channel is used to change the quantization level due to the difference in received signals from any two users. To lessen the key disagreement gray codes are utilized in multi-bit quantization. The thresholds serve as the benchmarks by which the measurements are divided into several categories. The thresholds are often determined using the mean value μ or along with standard deviation σ [55], [76], and cumulative distribution function CDF . In [76] two thresholds are used such that

$$\eta+ = \mu + \alpha \times \sigma; \qquad (4)$$

$$\eta- = \mu - \alpha \times \sigma \quad (5)$$

Where 0 < α <1

The measurements between $\eta+$ and $\eta-$ are dropped. If the probed sample value is above $\eta+$ the quantizer output is 1 and if it is below $\eta-$ the quantizer output is 0. Using this quantization, the bit disagreement gets reduced but then too the eavesdropper can obtain the secret key. In [77] and [78] performance evaluation and quantization scheme comparison is done.

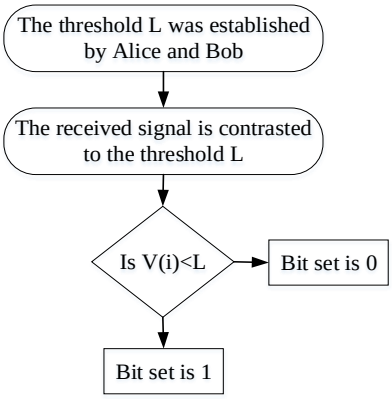

Fig 6. Binary quantization [66]

Binary Quantization with a single threshold (median value) has been proposed by Aono et al [66]. The quantizer output is either 1 or 0 depending on whether the sample value is above or below the threshold. The Binary Quantization is shown in Fig 6.The positions of deep fades in the RSS readings are found in [53] by Azimi Sadjadi et al. When the measurements are less than the deep fade threshold, a 0 is placed, and a 1 is placed otherwise. Low-entropy bit streams are generated rapidly. The binary-generated sequence isn't always truly random. Bursts of "1111...1" or "000...0" are frequently used in its construction. This occurs when the channel has insufficient variability. The attacker may quickly crack the key. Low entropy and large bit mismatch rates are present in generated key bits.

Sana Tmar-Ben Hamida et al. in [79] offers a new adaptive Quantization technique based on Noise variance. In the environment, the user M calculates the noise variance N . M quantifies the channel estimation $\hat{h}m(t)$ over a period of time. There are two thresholds established.

$$L^{+} = Max(\hat{h}m(t)) \quad (6)$$

$$L^{-} = Min(h\hat{}m(t)) \quad (7)$$

If h^m(t) > L^+ , $BV_m(i)$ =1
else

if h^m(t) < L^-, $BV_m(i)$ =0 (8)

Here, $BV_m(i)$ is the binary vector. M adjusts the threshold values

$$L^{+} = L^{+} + \max (h\hat{}m(t)/ \delta)$$
$$\&$$
$$L^{-} = L^{-} - \min (h\hat{}m(t)/ \delta) \quad (9)$$

Here, δ is a protocol parameter.
Repeat the aforementioned procedures until the desired level of noise is attained. The length of the secret key increases when the parameter δ is increased.

Kai Zeng et al. in [67] proposed multilevel quantization. It is done to quantify the small-scale measurements. Depending on the shared randomness between Alice and Bob, there are a finite number of levels among whom the measurements are divided. Binary is replaced with multi-level quantization if the channel provides sufficient mutual information.
To produce high entropy bits, Sriram Nandha et al. suggested an Adaptive Secret bit generation (ASBG) quantization in [76]. The thresholds are determined separately for each block once the RSS readings are partitioned into smaller blocks of block size. The quantizer can adjust to slow changes in RSS owing to the adaptive threshold. The average number of secret bits retrieved each measurement is known as the secret bit rate. Two major problems exist with single bit extraction. The samples are dropped using these techniques when they are near thresholds. Additionally, as many probes are needed it results in inefficient use of the wireless medium. The authors suggested an adaptive approach for multiple bits retrieving from a single RSS data to improve the hidden bit rate. The results of the experiments lead the authors to the conclusion that a larger block size reduces the bit mismatch rate. ASBG gives bit streams with highest entropy. Additionally, grey code minimises BMR for multiple bit extraction when compared to a standard binary sequence.

Guillaume, R. et al. conducted a fair evaluation of several quantization techniques in [78]. The quantization methods for the Internet of Things are explored by U.R. Bhatt et al. in [80]. The quantizer in [81] is based on the Lloyd-max-based quantizer, which minimizes the error in the quantization. In [82], Modified Kalman (MK) pre-processing is applied, which gives key with less randomness. For obtaining secure keys randomness must be maximum.

A vector Partitioning algorithm was proposed by Qingqing Han et al. in [83]. Vector partitioning is the process of dividing a vector space into numerous non-overlapping parts; in this case, the algorithm used to map the regions into

corresponding bits was based on the requirements. Then the k-means clustering method was added to that algorithm, along with two more k-means algorithms, lossy and compensating k-means.

High KGR and low bit mismatch rate criteria for secret key generation are proposed here using an improved Channel quantization alternating (ICQA) algorithm [84]. Using test results for CFR amplitude values, the proposed algorithm filters the phase values of the CFR, and the Channel quantization algoritm (CQA) subsequently quantizes the reserved phase values. The suggested algorithm ensures a low BMR while enhancing KGR.The secret key generation from the channel samples was done by Adil et al. [85] using the non-uniform quantization method. The next section discusses the information reconciliation techniques.

3.5 Information Reconciliation

After quantization, there might still be significant discrepancies among the preliminary keys. IR removes these discrepancies and makes both the keys same.

As shown in the Fig 7., there are two different types of Information reconciliation schemes.

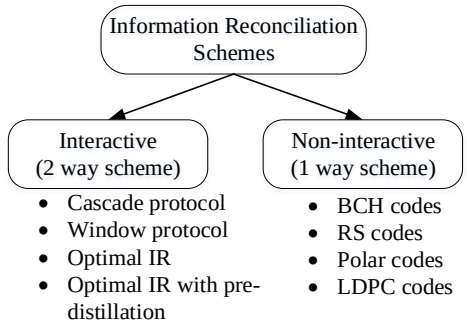

Fig 7. Information reconciliation schemes

The BBBSS protocol, which functions as a quantum transmission protocol, is proposed by Bennett, C.H., and Brassard, G. in [86]. Here parity bits are exchanged. The simple and easy binary search method is used to locate and rectify the incorrect bits, but it necessitates frequent direct communication.

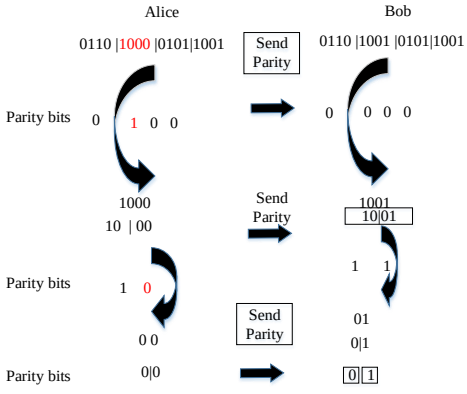

Fig 8. Cascade Protocol Illustration

A CASCADE protocol for interactive reconciliation was proposed by Gilles Brassard et al in [87]. The simplicity of the Cascade protocol makes it popular. By computing parity checks of the relevant blocks, it fixes errors. Based on the BMR estimated before execution, cascade is executed in a fixed of passes. Both Alice and Bob agree to a random exchange by negotiating a public channel as the first step in the protocol. It needs $1+\log_2 N$ communications for one iteration. Fig 8. illustrates the working of cascade protocol. For each block, parity bits are determined. Alice's parity bits are compared to Bob's parity bits. Blocks are broken into smaller blocks if the parity bits are different for each block. The parity bits for the sub block are calculated and compared similarly. Winnow protocol was suggested by W.T. Buttler et al. [88]. By using hamming codes for error correction, the Winnow protocol seeks to minimize interaction between parties that are communicating. Better throughput and less interaction are offered, although efficiency is same as that of cascade. Winnow protocol results in adding more errors to a block that already contains one or more errors, increasing the probability that bits would mismatch. Wang, Q. et al. in [89] suggest a new IR protocol to boost the effectiveness of the Winnow protocol. The suggested technique improves both the information rate and Bob's BMR, which enables the subsequent privacy amplification to be carried out at ease. As a result, the rate of secret key agreement's entire information is increased. The optimal IR protocol and pre-distillation procedure were proposed in [90, 91] by Wang, Q et al. Optimal IR causes BMR to rapidly decline. Since only two bits are sent and removed, the Data Remaining Rate (DRR) is increased. For initial BMR above 0.15, this protocol is most effective, and for initial BMR equal to 0.3, the DRR increases 49 times. BCH Based Slepian Wolf Coding has been proposed by Treeviriyanupab, P et al. in [92]. The effectiveness of polar codes has been discussed in [93] by S. Peng et al. Polar codes have the ability to achieve a property owing to a special building technique called channel polarization. The bit-channels will be split into noiseless bit-channels and pure-noise bit-channels via channel polarization. As the most important part of vehicle-vehicle communication, Turbo codes were successfully integrated with non-reciprocal compensation in [94]. Due to the low density of their parity check matrices, LDPC codes are so named. Using rate-adaptive LDPC codes, J. Martinez-Mateo and colleagues suggested a new methodology for error correction in [95]. Iteratively transmitting more symbols reduces the amount of information sent for correction while still allowing the protocol to fix errors that fall within a known error rate range. N.Bonello et al. discuss the LDPC codes in [96]. Tanner graph is frequently used to graphically describe LDPC codes. It facilitates in the description of the decoding method and offers a comprehensive representation of the code. With these codes, source coding with side information can be encoded almost to the theoretical limit.

Rateless coding for LDPC codes has been proposed by D. Elkouss et al. in [97]. Two effective methods for adjusting a channel code's rate are shortening and puncturing. For a Quantum Key distribution system error correction is discussed in [98]. It uses a winnow technique based on an FPGA with hamming error correction and high speed parity. A protocol for adaptive IR has been proposed by Zheying Zhang et al. in [99]. Information leakage rate and Reconciliation success rate are both considered in the evaluation metric known as reconciliation efficiency. Nevertheless, in some circumstances, performance of reconciliation may be impacted by time delay brought on by information interaction and calculation overhead. To compare existing methods, a thorough evaluation metric is therefore necessary. In addition, the channel characteristics in actual mobile communication systems are constantly changing, and the majority of the available reconciliation algorithms are only effective under specific channel state information. A reconciliation mechanism that can adjust to time-varying channel conditions is therefore necessary.

In [99], a comprehensive reconciliation efficiency index (CREI) is proposed along with an adaptive information reconciliation scheme selection (AIRSS) procedure in order to optimize CREI. This index is used to assess the effectiveness of current reconciliation schemes. The simulation results demonstrate the advantages of AIRSS and offer suggestions for choosing a reconciliation scheme in certain contexts. Li et al. [100] used a hybrid strategy for information reconciliation. The technique combines interactive and non-interactive methods of error correction. To minimize information leakage, time delays, and calculation time, the developed model contains three phases: training, table lookup, and testing. In order to validate the concept, it was tested using single input, single output, and single eavesdropper based system designs. In [101] Polar codes are discussed. Here Shannon limit approach (SLA) is utilized which gives efficiency of 1.055. Next section gives the Privacy Amplification technique which is needed to eliminate the information disclosed during error correction process from the generated key.

3.6 Privacy Amplification

During the IR step, certain information is broadcast publicly, where the eavesdropper can also hear it. The security of the key sequence may be compromised as a result. The exposed information is then removed using privacy amplification. This can be accomplished using the extractor or universal hashing algorithms like the MD5 hash function, leftover hash lemma, or secure hash algorithm. The final key is derived using a hash function. Any function that converts data of any size to data of a specific size is referred to as a hash function. Input for digital signatures was at first suggested to be generated.

A cross-design between these two stages is necessary since privacy amplification and IR always occur concurrently. In actuality, it might be challenging to pinpoint the exact location in the data where the leakage occurs or to estimate how much information has been disclosed.

The channel probing stage's sampling and data storage are the only non-complex processes necessary for the key generation implementation, which is typically low cost. With the exception of modifying the drivers, all of these processes can be carried out using commercially available hardware. Depending on how the system is implemented, different key generation processes are used. In order for the systems to reach perfect agreement after quantization, all key generation systems require channel sampling and quantization but may not use IR and privacy amplification. The various hashing algorithms and the Key length are listed in Table 2.

Table 2. Message Digest and Hash functions

Message Digest and Hash Functions	**Length of Key generated (bits)**
MD2,MD4,MD5	128
MD6	Variable upto 512
SHA-0	160
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512

The exponential bound and the min-entropy bound have been

compared by S. Watanabe et al. in [102]. They presented a new bound that employs a hybrid of the inf-spectral and Renyi entropies to interpolate the min entropy constraint and exponential bound. Hayashi et al. created a random hash function in [103] with nlogn-level computational complexity and shorter random seed lengths. It is possible to create new extractors by concatenating traditional extractors with virtually dual universal 2 hash algorithms. Modified Toeplitz matrix is used as the extractor as its complexity is n log n for input length n. Message digest, whirlpool, and other hashing algorithms are frequently employed.

Table 3 gives the research problems at each block of the key generation procedure.

Table 3. Research Problems at different blocks of Key Generation

Sr. No	Processing steps	Objective	Research problems
1	Channel probing	Measurements of the channels through the signals that have been received	✓ Pre-processing: Interpolation and/or filtering to improve signal cross-correlation. ✓ Channel parameters: The sampling effectiveness is determined by the granularity of the selected parameter. ✓ Channel probing rate: The elimination of redundancy in the measurements
2	Quantization	Binary value conversion for channel measurements	✓ Quantization level are chosen. ✓ Performance optimization
3	Information reconciliation	Using protocols or error correction codes, correcting the mismatched bits between Alice and Bob	✓ Optimising the relationship between information leakage and corrective capacity
4	Privacy amplification	To remove the information disclosed during information reconciliation stage	✓ Information reconciliation cross design ✓ Amount of information that has been leaked is determined

4. Performance Optimization

This section explains how to choose the different parameters for efficient key generation. Designing key generation systems with the goal of achieving optimal performance is possible by carefully considering each stage of key generation. By carefully choosing the channel parameter and probing rate, among other factors, KGR can be enhanced. These factors are enumerated as follows:

- From the fine-grained CSI, randomness extraction
- Extraction of more channel information through multiple antenna diversity.
- Adaptive channel probing
- Relay nodes are introduced, and this allows for the utilization of channel information between users and relay nodes.
- Multi-bit quantization.
- To get many probes in a single coherence time, use a random beginning phase.

If the system allows, it's also possible to combine the aforementioned techniques to further enhance the KGR. Particularly in low SNR settings, the BMR will typically be significant if the sampled channel characteristics are explicitly quantized. Greater KGRs can also be achieved using higher quantization levels, although in low SNR conditions, this may also result in higher BMRs. By varying and randomizing the channel, the entropy of the key can be increased. Usually, randomness cannot be compromised. In order to construct a key generation system that meets the needs of the system and the environment, a reasonably optimal tradeoff between KGR and BMR should be made. Table 4 compares a few significant generation systems in terms of performance and technical specifications.

Table 4. Comparison of Key generation systems

Representative Work	Test bed	Parameter	Channel Probing	Quantization	KGR	BMR
Mathur et al.[55]	Commercial 802.11a/b/g modem IP	RSS,CIR	Using 802.11 packets	Level Crossing algorithm	1.3 bits/s	15.85%
Jana et al.[76]	Laptops with Intel PRO/wireless 3945 ABG wireless network cards operating in	RSS	Using 802.11 transceivers in half duplex mode	Adaptive Secret bit generation (ASBG)	16bits/s	11%

	the 802.11g mode.					
Zeng et al.[67]	Laptops with intel wifi link 5300 NIC	RSS	Multiple antenna key generator (MAKE) using 802.11 n multiple antenna devices	Multilevel	10 bits/s	10%
Patwari et al.[54]	Crossbow TelosB wireless sensors	RSS	Using the Telos B 802.15.14 radios	Multibit adaptive	10-22 bits/s	0.54%-2.2%
Liu et al.[40]	Laptops with intel wifi link 5300 NIC	CSI	Using Laptops equipped with Intel 5300	Multibit	60-90 bits/Packet	8%
Wei et al.[68]	Laptops with Atheros NIC	RSS	Adaptive channel probing scheme based on Lempel Ziv complexity (LZ76) and Proportional-integral-derivative (PID) controller	Level Crossing algorithm	100 bits/s	NA
Ali et al.[75]	Experiment conducted in indoor office environment and RF anechoic chamber	RSS	Using MICAz Sensor motes	Level Crossing algorithm	0.037-0.295 bits/s	0-1.6%
Aono et al.[66]	ZigBee chips chipcom-CC2420	RSSI	Using Electronically Steerable Parasitic array radiator[ESPAR]	Binary	200 bits/s	0.33%
Aldaghri et al.[69]	NYUSIM channel Simulator	CSI,RSS	Using OFDM Subcarriers	Adaptive Secret bit generation (ASBG)	64 bits/Packet	1%-13 %
Yuliana Mike et al.[82]	3 Raspberry pi 3 Type B devices with TL-WN 7222N 802.11 b/g/n wireless card	RSS	Using Raspberry pi3 devices	Combined Multilevel Quantization (CMQ)	0.92-0.45 bits/s	0.5%-0.7%
Ankit Soni et al.[81]	IOT subsystem with three controllers	RSS	Using Controller and Sensor motes	Lylod –Max based quantizer	NA	0.45%-0.1%

5. Application Scenario

Key generation has previously had various different regions of prototype. This section reviews applications in various environments and discusses the difficulties in each area.

Internet of Things (IOT)

Numerous incidents demonstrate the IoT devices vulnerability, which in some demographic groups could result in severe losses both financially and personally. PLS is utilized in [104] to increase the security of IOT systems. A simple authenticated secret key extraction is suggested in [105]. In [81] moving window averaging method is used for IOT.

Orthogonal Frequency Division multiplexing (OFDM)

In order to satisfy the demands of next-generation networks and the users' ever-increasing demand, OFDM has emerged as a possible alternative. Due to the broadcast nature of wireless transmission, this technology is susceptible to both passive and active attackers, namely eavesdroppers with the power to collect, decrypt, and retrieve the transmitted signals. In [106], PLS in an OFDM channel is proposed. It is demonstrated in [107] that a high KGR can be obtained by utilizing the channel response from multiple OFDM subcarriers.

Long Range Radio Wide Area Network (LORAWAN)

A security strategy for communications between end devices and network/application servers is clearly defined in the LoRaWAN specification. Due to its low power and long range communication, LoRaWAN, an unlicensed band based long range wide area network specification, is extremely suitable for the activities or operations in an IoT context. In [108] wireless key generation for LoRaWAN is explored. For the LoRaWAN to utilize less power, three different communication modes, asynchronous communication, and star-of-stars topology are used. The LoRaWAN uses PLS to improve the security of network communication [109].

Wi-Fi and LTE

The need to increase the security of data sent over the air interface is widely required in public wireless communication systems similar to Wi-Fi and LTE. By utilizing the inherent randomness of wireless channels, PLS has emerged as an alternate method for creating strong secret keys. PLS performance is examined in [110] utilizing LTE and Wi-Fi signals.

Wireless Sensor Networks (WSN)

WSNs are frequently employed in fields including environmental monitoring, healthcare, and the military [111], where it is obvious that the transferred data must be protected. To defend against attacks and improper behavior, the information and resources are protected by security services in the WSN. The authors in [112] suggest using the SKG protocol to lengthen network lifetime while preserving WSN security.

Vehicular Communication

In order to enable autonomous driving, vehicle-to-vehicle (V2V) communications are of utmost importance in intelligent transportation systems (ITS). Due to the wireless medium's potential for unauthorized users to passively eavesdrop or modify communications, security is of utmost importance. [113] & [114] presented a key-generation technique for PLS in V2V communications.

Field programmable gate array (FPGA)

PLS is used in [115] to simulate the two communication nodes and the eavesdropper using three FPGA-based WARP kits. The secret key's BMR and entropy are evaluated and compared to classical algorithms.

6. Open Research Issues

Still researchers have many issues, which need to be tackled thereby increasing the robustness of the key generation system. A few research scopes are summarized below:

- The spatial decorrelation property does not hold well in some channel conditions. Hence, key generation systems need to be analyzed for such conditions.
- Researchers have tried to introduce randomness into Static channels by using different beam forming and jamming methods. These methods require multiple antennas. Therefore, the ability to work in a stationary environment is an important requirement when implementing key generation systems.
- Ideally, the BMR should be zero. However, due to different factors such as noise, half-duplex probing the error arises. Researchers have used different interactive and non-interactive reconciliation schemes to reduce the BMR. Still work need to be done to reduce it further.
- Non-reciprocity in measuring the signals at the side of Alice and Bob further leads to increase in BMR. Ongoing research effort is going on to adopt full duplex hardware. But most of the commercial wireless devices work in half duplex mode. Researchers have used interpolation to compensate non-simultaneous measurements and low pass filtering to suppress the noise. Still work need to be done on improving the channel reciprocity by using signal-processing techniques to ensure perfect reciprocity.
- An efficient key generation system has high entropy to generate secret keys. Different quantization techniques have been used to generate secret keys with different entropies. Work needs to be done to improve the entropy further by using innovative quantization methods.
- Key generation is vulnerable to both passive eavesdropping and active attacks. Hence, research into how we can defend against such attacks is essential.
- Upper layer security protocols like WEP (Wired equivalent privacy) and WPA (Wifi protected access)

are widely deployed and the implementation of PLS is considered to be a part of a layered approach.

- With half-duplex network, key-based security cannot have ideally symmetrical channel estimations. Also with full duplex, the efficiency of key agreement will be greatly improved.

7. Conclusion

A possible method for securely distributing secret keys among authorized users is generating keys using randomness of wireless communication. The challenges with wireless network security were discussed in this paper. Particularly, we examined the technique, measurements, and essential generation principles. Optimizing the key generation performance was another topic we discussed. To further understand the characteristics and difficulties of each setting, various application scenarios were studied. To make key generation more reliable, there are still unsolved issues. Group key generation, attacks on key generation systems, and key generation in static contexts are some future study areas that will be taken into consideration.

References

[1] Huanan, Z., Suping, X. and Jiannan, W., 2021. Security and application of wireless sensor network. *Procedia Computer Science*, *183*, pp.486-492.

[2] Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L. and Zeng, K., 2019. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE internet of things journal*, *6*(5), pp.8169-8181.

[3] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.K. and Gao, X., 2018. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, *36*(4), pp.679-695.

[4] Tang, J., Wen, H., Zeng, K., Liao, R.F., Pan, F. and Hu, L., 2019. Light-weight physical layer enhanced security schemes for 5G wireless networks. *IEEE Network*, *33*(5), pp.126-133.

[5] Elminaam, D.S.A., Kader, H.M.A. and Hadhoud, M.M., 2008. Performance evaluation of symmetric encryption algorithms. *IJCSNS International Journal of Computer Science and Network Security*, *8*(12), pp.280-286.

[6] Wander, A.S., Gura, N., Eberle, H., Gupta, V. and Shantz, S.C., 2005, March. Energy analysis of public-key cryptography for wireless sensor networks. In *Third IEEE international conference on pervasive computing and communications* (pp. 324-328). IEEE.

[7] Singh, S.P. and Maini, R., 2011. Comparison of data encryption algorithms. *International journal of computer science and communication*, *2*(1), pp.125-127.

[8] Dongjiang, L., Yandan, W. and Hong, C., 2012, August. The research on key generation in RSA public-key cryptosystem. In *2012 Fourth international conference on computational and information sciences* (pp. 578-580). IEEE.

[9] Mikhail, M., Abouelseoud, Y. and Elkobrosy, G., 2014, January. Extension and application of El-Gamal encryption scheme. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-6). IEEE.

[10] Naureen, A., Akram, A., Maqsood, T., Riaz, R., Kim, K.H. and Ahmed, H.F., 2008, May. Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks. In *VTC Spring 2008-IEEE Vehicular Technology Conference* (pp. 163-167). IEEE.

[11] Farah, S., Javed, Y., Shamim, A. and Nawaz, T., 2012, December. An experimental study on performance evaluation of asymmetric encryption algorithms. In *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science, (EECS-12)* (pp. 121-124).

[12] Tripathi, R. and Agrawal, S., 2014. Comparative study of symmetric and asymmetric cryptography techniques. *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, *1*(6), pp.68-76.

[13] Padmavathi, B. and Kumari, S.R., 2013. A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution. *IJSR, India*, *2*(4), pp.170-174.

[14] Chandra, S., Paira, S., Alam, S.S. and Sanyal, G., 2014, November. A comparative survey of symmetric and asymmetric key cryptography. In *2014 international conference on electronics, communication and computational engineering (ICECCE)* (pp. 83-93). IEEE.

[15] Singh, G., 2013. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19).

[16] Patil, A. and Goudar, R., 2013. A comparative survey of symmetric encryption techniques for wireless devices. *International journal of scientific & technology research*, *2*(8).

[17] Sun, L. and Du, Q., 2018. A review of physical layer security techniques for Internet of Things: Challenges and solutions. *Entropy*, *20*(10), p.730.

[18] Melki, R., Noura, H.N. and Chehab, A., 2021. Physical layer security for NOMA: Limitations, issues, and recommendations. *Annals of Telecommunications*, *76*(5), pp.375-397.

[19] Rodriguez, L.J., Tran, N.H., Duong, T.Q., Le-Ngoc, T., Elkashlan, M. and Shetty, S., 2015. Physical layer security in wireless cooperative relay networks: State of the art and beyond. *IEEE Communications Magazine*, *53*(12), pp.32-39.

[20] Shakiba-Herfeh, M., Chorti, A. and Vincent Poor, H., 2021. Physical layer security: Authentication, integrity, and confidentiality. *Physical Layer Security*, pp.129-150.

[21] Zou, Y., Zhu, J., Wang, X. and Hanzo, L., 2016. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), pp.1727-1765.

[22] Zhang, J., Duong, T.Q., Woods, R. and Marshall, A., 2017. Securing wireless communications of the internet of things from the physical layer, an overview. *Entropy*, *19*(8), p.420.

[23] Gao, Y., Hu, S., Tang, W., Li, Y., Sun, Y., Huang, D., Cheng, S. and Li, X., 2018. Physical layer security in 5G based large scale social networks: Opportunities and challenges. *IEEE Access*, *6*, pp.26350-26357.

[24] Bai, L., Zhu, L., Liu, J., Choi, J. and Zhang, W., 2020. Physical layer authentication in wireless communication networks: A survey. *Journal of Communications and Information Networks*, *5*(3), pp.237-264.

[25] Wyner, A.D., 1975. The wire-tap channel. *Bell system technical journal*, *54*(8), pp.1355-1387.

[26] Leung-Yan-Cheong, S. and Hellman, M., 1978. The Gaussian wire-tap channel. *IEEE transactions on information theory*, *24*(4), pp.451-456.

[27] Din, F.U. and Labeau, F., 2018, May. Multiple antenna physical layer security against passive eavesdroppers: A tutorial. In *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)* (pp. 1-6). IEEE.

[28] Delaveau, F., Mueller, A., Ngassa, C.K., Guillaume, R., Molière, R. and Wunder, G., 2016. Perspectives of physical layer security (physec) for the improvement of the subscriber privacy and communication confidentiality at the air interface. *Perspectives*, *27*, p.28.

[29] Boche, H. and Deppe, C., 2018. Secure identification under passive eavesdroppers and active jamming attacks. *IEEE Transactions on Information Forensics and Security*, *14*(2), pp.472-485.

[30] Bhushan, B. and Sahoo, G., 2018. Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications*, *98*, pp.2037-2077.

[31] Liu, Z., Li, N., Tao, X., Li, S., Xu, J. and Zhang, B., 2017, October. Artificial-noise-aided secure communication with full-duplex active eavesdropper. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-7). IEEE

[32] Timilsina, S., Baduge, G.A.A. and Schaefer, R.F., 2018. Secure communication in spectrum-sharing massive MIMO systems with active eavesdropping. *IEEE Transactions on Cognitive Communications and Networking*, *4*(2), pp.390-405.

[33] Li, L., Petropulu, A.P. and Chen, Z., 2017. MIMO secret communications against an active eavesdropper. *IEEE Transactions on Information Forensics and Security*, *12*(10), pp.2387-2401.

[34] Pradeep, R. and Kanimozhi, R., 2021. Hardware Efficient Architectural Design for Physical Layer Security in Wireless Communication. *Wireless Personal Communications*, *120*(2), pp.1821-1836.

[35] Ambekar, A., Hassan, M. and Schotten, H.D., 2012, October. Improving channel reciprocity for effective key management systems. In *2012 International Symposium on Signals, Systems, and Electronics (ISSSE)* (pp. 1-4). IEEE.

[36] Zhang, L., Wang, P., Zhang, Y., Chi, Z., Tong, N., Wang, L. and Li, F., 2023. An adaptive and robust secret key extraction scheme from high noise wireless channel in IIoT. *Digital Communications and Networks*, *9*(4), pp.809-816.

[37] Wilhelm, M., Martinovic, I. and Schmitt, J.B., 2013. Secure key generation in sensor networks based on frequency-selective channels. *IEEE Journal on Selected Areas in Communications*, *31*(9), pp.1779-1790.

[38] Yao, L., Ali, S.T., Sivaraman, V. and Ostry, D., 2012, September. Decorrelating secret bit extraction via channel hopping in body area networks. In *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC)* (pp. 1454-1459). IEEE.

[39] Mathur, S., Miller, R., Varshavsky, A., Trappe, W. and Mandayam, N., 2011, June. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th international conference on Mobile systems, applications, and services* (pp. 211-224).

[40] Liu, H., Wang, Y., Yang, J. and Chen, Y., 2013, April. Fast and practical secret key extraction by exploiting channel response. In *2013 Proceedings IEEE INFOCOM* (pp. 3048-3056). IEEE.

[41] Xi, W., Li, X.Y., Qian, C., Han, J., Tang, S., Zhao, J. and Zhao, K., 2014, May. KEEP: Fast secret key extraction protocol for D2D communication. In *2014 IEEE 22nd International Symposium of Quality of Service (IWQoS)* (pp. 350-359). IEEE.

[42] Wallace, J.W. and Sharma, R.K., 2010. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis. *IEEE Transactions on Information Forensics and Security*, *5*(3), pp.381-392.

[43] Chen, C. and Jensen, M.A., 2010. Secret key establishment using temporally and spatially correlated wireless channel coefficients. *IEEE Transactions on Mobile Computing*, *10*(2), pp.205-215.

[44] Quist, B.T. and Jensen, M.A., 2013. Maximizing the secret key rate for informed radios under different channel conditions. *IEEE transactions on wireless communications*, *12*(10), pp.5146-5153.

[45] Jorswieck, E.A., Wolf, A. and Engelmann, S., 2013, December. Secret key generation from reciprocal spatially correlated MIMO channels. In *2013 IEEE Globecom Workshops (GC Wkshps)* (pp. 1245-1250). IEEE.

[46] Quist, B.T. and Jensen, M.A., 2015. Maximization of the channel-based key establishment rate in MIMO systems. *IEEE Transactions on Wireless Communications*, *14*(10), pp.5565-5573.

[47] Hamida, S.T.B., Pierrot, J.B. and Castelluccia, C., 2010, September. Empirical analysis of UWB channel characteristics for secret key generation in indoor environments. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (pp. 1984-1989). IEEE.

[48] Marino, F., Paolini, E. and Chiani, M., 2014, September. Secret key extraction from a UWB channel: Analysis in a real environment. In *2014 IEEE International Conference on Ultra-WideBand (ICUWB)* (pp. 80-85). IEEE.

[49] Madiseh, M.G., He, S., McGuire, M.L., Neville, S.W. and Dong, X., 2009, June. Verification of secret key generation from UWB channel observations. In *2009 IEEE International Conference on Communications* (pp. 1-5). IEEE.

[50] Trappe, W., 2015. The challenges facing physical layer security. *IEEE communications magazine*, *53*(6), pp.16-20.

[51] Zhang, J., Duong, T.Q., Marshall, A. and Woods, R., 2016. Key generation from wireless channels: A review. *Ieee access*, *4*, pp.614-626.

[52] Badawy, A., Elfouly, T., Khattab, T., Mohamed, A. and Guizani, M., 2016. Unleashing the secure potential of the wireless physical layer: Secret key generation methods. *Physical Communication*, *19*, pp.1-10

[53] Azimi-Sadjadi, B., Kiayias, A., Mercado, A. and Yener, B., 2007, October. Robust key generation from signal envelopes in wireless networks. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 401-410).

[54] Patwari, N., Croft, J., Jana, S. and Kasera, S.K., 2009. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, *9*(1), pp.17-30.

[55] Mathur, S., Trappe, W., Mandayam, N., Ye, C. and Reznik, A., 2008, September. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking* (pp. 128-139).

[56] Quynh, H., 2015. *Dang: Secure hash standard-federal information processing standard publication 180-4*. Tech. rep., Gaithersburg, MD USA.

[57] Kadam, S. and Gomes, J., 2022, December. Comparative Analysis of Quantization Schemes for Physical Layer Key generation. In *2022 5th International Conference on Advances in Science and Technology (ICAST)* (pp. 548-553). IEEE.

[58] Yuliana, M., 2017, May. Performance evaluation of the key extraction schemes in wireless indoor environment. In *2017 International Conference on Signals and Systems (ICSigSys)* (pp. 138-144). IEEE.

[59] Juby Susan, Mathew Hari. S, Techniques in Key Generation, IJIRST –International Journal for Innovative Research in Science & Technology|, Volume 3, Issue 08 | January 2017 ISSN (online): 2349-6010.

[60] Premnath, S.N., Jana, S., Croft, J., Gowda, P.L., Clark, M., Kasera, S.K., Patwari, N. and Krishnamurthy, S.V., 2012. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on mobile Computing*, *12*(5), pp.917-930.

[61] Guillaume, R., Winzer, F., Czylwik, A., Zenger, C.T. and Paar, C., 2015, September. Bringing PHY-based key generation into the field: An evaluation for practical scenarios. In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)* (pp. 1-5). IEEE.

[62] Ohira, T., 2005, October. Secret key generation exploiting antenna beam steering and wave propagation reciprocity. In *2005 European Microwave Conference* (Vol. 1, pp. 4-pp). IEEE.

[63] Liu, Y., Draper, S.C. and Sayeed, A.M., 2012. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transactions on information forensics and security*, *7*(5), pp.1484-1497.

[64] Shehadeh, Y.E.H. and Hogrefe, D., 2011, February. An optimal guard-intervals based mechanism for key generation from multipath wireless channels. In *2011 4th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1-5). IEEE.

[65] Shehadeh, Y.E.H., Alfandi, O., Tout, K. and Hogrefe, D., 2011, April. Intelligent mechanisms for key generation from multipath wireless channels. In *2011 Wireless Telecommunications Symposium (WTS)* (pp. 1-6). IEEE.

[66] Aono, T., Higuchi, K., Ohira, T., Komiyama, B. and Sasaoka, H., 2005. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *IEEE Transactions on Antennas and Propagation*, *53*(11), pp.3776-3784.

[67] Zeng, K., Wu, D., Chan, A. and Mohapatra, P., 2010, March. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9). IEEE.

[68] Wei, Y., Zeng, K. and Mohapatra, P., 2012. Adaptive wireless channel probing for shared key generation based on PID controller. *IEEE Transactions on Mobile Computing*, *12*(9), pp.1842-1852.

[69] Aldaghri, N. and Mahdavifar, H., 2020. Physical layer secret key generation in static environments. *IEEE Transactions on Information Forensics and Security*, *15*, pp.2692-2705.

[70] Liu, Y., Chen, H.H. and Wang, L., 2016. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials*, *19*(1), pp.347-376.

[71] Ambekar, A. and Schotten, H.D., 2014, May. Enhancing channel reciprocity for effective key management in wireless ad-hoc networks. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)* (pp. 1-5). IEEE.

[72] Yasukawa, S., Iwai, H. and Sasaoka, H., 2008, December. Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM. In *2008 International Symposium on Information Theory and Its Applications* (pp. 1-6). IEEE.

[73] Liu, H., Yang, J., Wang, Y. and Chen, Y., 2012, March. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In *2012 Proceedings IEEE Infocom* (pp. 927-935). IEEE.

[74] Croft, J., Patwari, N. and Kasera, S.K., 2010, April. Robust uncorrelated bit extraction methodologies for wireless sensors. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks* (pp. 70-81).

[75] Ali, S.T., Sivaraman, V. and Ostry, D., 2012, April. Zero reconciliation secret key generation for body-worn health monitoring devices. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks* (pp. 39-50).

[76] Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N. and Krishnamurthy, S.V., 2009, September. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on Mobile computing and networking* (pp. 321-332).

[77] Zenger, C., Zimmer, J. and Paar, C., 2015. Security analysis of quantization schemes for channel-based key extraction. *EAI Endorsed Transactions on Security and Safety*, *2*(6), pp.267-272.

[78] Guillaume, R., Mueller, A., Zenger, C.T., Paar, C. and Czylwik, A., 2014, August. Fair comparison and evaluation of quantization schemes for phy-based key generation. In *OFDM 2014; 18th International OFDM Workshop 2014 (InOWo'14)* (pp. 1-5). VDE.

[79] Hamida, S.T.B., Pierrot, J.B. and Castelluccia, C., 2009, December. An adaptive quantization algorithm for secret key generation using radio channel measurements. In *2009 3rd International Conference on New Technologies, Mobility and Security* (pp. 1-5). IEEE.

[80] Bhatt, U.R., Sharma, R., Soni, A. and Upadhyay, R., 2018. Analysis of quantization schemes in secure key generation for internet of things. *Int J Electr Eng*, *10*(2), pp.665-672.

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

[82] Yuliana, M., Wirawan and Suwadi, 2019. A simple

secret key generation by using a combination of pre-processing method with a multilevel quantization. *Entropy*, *21*(2), p.192.

[83] Han, Q., Liu, J., Shen, Z., Liu, J. and Gong, F., 2020. Vector partitioning quantization utilizing K-means clustering for physical layer secret key generation. *Information sciences*, *512*, pp.137-160.

[84] Huang, L., Guo, D., Xiong, J. and Ma, D., 2020, October. An improved CQA quantization algorithm for physical layer secret key extraction. In *2020 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 829-834). IEEE.

[85] Adil, M., Wyne, S. and Nawaz, S.J., 2021. On quantization for secret key generation from wireless channel samples. *IEEE Access*, *9*, pp.21653-21668.

[86] Bennett, C.H. and Brassard, G., 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, pp.7-11.

[87] Brassard, G. and Salvail, L., 1993, May. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 410-423). Berlin, Heidelberg: Springer Berlin Heidelberg.

[88] Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Donahue, C.H. and Peterson, C.G., 2003. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, *67*(5), p.052303.

[89] Q. Wang, X. Wang, Q. Lv, X. Ye, L. You and R. Zeng, "A New Information Reconciliation Protocol in Information Theoretically Secret Key Agreement", Journal of Computational Information Systems, vol.10, no. 21, pp. 9413–9420, (2014).

[90] Wang, Q., Wang, X., Lv, Q., You, L. and Yu, W., 2015, October. Pre-process method for reducing initial bit mismatch rate in secret key generation based on wireless channel characteristics. In *2015 IEEE 16th International Conference on Communication Technology (ICCT)* (pp. 888-891). IEEE.

[91] Wang, Q., Wang, X., Lv, Q. and Bao, J., 2016. Methods for improving the rate of secret key generation based on wireless channel characteristics. *Journal of Networks*, *11*(2), p.46.

[92] Treeviriyanupab, P., Sangwongngam, P., Sripimanwat, K. and Sangaroon, O., 2012, May. BCH-based Slepian-Wolf coding with feedback syndrome decoding for quantum key reconciliation. In *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology* (pp. 1-4). IEEE.

[93] Shi, P., Tang, W., Zhao, S. and Wang, B., 2012, November. Performance of polar codes on wireless communication channels. In *2012 IEEE 14th International Conference on Communication Technology* (pp. 1134-1138). IEEE.

[94] Epiphaniou, G., Karadimas, P., Ismail, D.K.B., Al-Khateeb, H., Dehghantanha, A. and Choo, K.K.R., 2017. Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks. *IEEE Internet of Things Journal*, *5*(4), pp.2496-2505.

[95] Martinez-Mateo, J., Elkouss, D. and Martin, V., 2010, September. Interactive reconciliation with low-density parity-check codes. In *2010 6th International Symposium on Turbo Codes & Iterative Information Processing* (pp. 270-274). IEEE.

[96] Bonello, N., Chen, S. and Hanzo, L., 2010. Low-density parity-check codes and their rateless relatives. *IEEE Communications Surveys & Tutorials*, *13*(1), pp.3-26.

[97] Elkouss, D., Martinez-Mateo, J. and Martin, V., 2012. Untainted puncturing for irregular low-density parity-check codes. *IEEE Wireless Communications Letters*, *1*(6), pp.585-588.

[98] Tang, S.B. and Cheng, J., 2019. Research on error-correction algorithm of high-speed QKD system based on FPGA. *International Journal of Quantum Information*, *17*(02), p.1950013.

[99] Zhang, Z., Li, G. and Hu, A., 2019, April. An adaptive information reconciliation protocol for physical-layer based secret key generation. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)* (pp. 1-5). IEEE.

[100] Li, G., Zhang, Z., Yu, Y. and Hu, A., 2019. A hybrid information reconciliation method for physical layer key generation. *Entropy*, *21*(7), p.688.

[101] Tang, B.Y., Liu, B., Yu, W.R. and Wu, C.Q., 2021. Shannon-limit approached information reconciliation for quantum key distribution. *Quantum Information Processing*, *20*, pp.1-16.

[102] Watanabe, S. and Hayashi, M., 2013, July. Non-asymptotic analysis of privacy amplification via Rényi entropy and inf-spectral entropy. In *2013 IEEE International Symposium on Information Theory* (pp. 2715-2719). IEEE.

[103] Hayashi, M. and Tsurumaru, T., 2016. More efficient privacy amplification with less random seeds via dual universal hash function. *IEEE Transactions on Information Theory*, *62*(4), pp.2213-2232.

[104] Pecorella, T., Brilli, L. and Mucchi, L., 2016. The role of physical layer security in IoT: A novel perspective. *Information*, *7*(3), p.49.

[105] Jiang, Y., Hu, A. and Huang, J., 2019. A lightweight physical-layer based security strategy for Internet of things. *Cluster Computing*, *22*(Suppl 5), pp.12971-12983.

[106] Chou, T.H., Draper, S.C. and Sayeed, A.M., 2010, June. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In *2010 IEEE International Symposium on Information Theory* (pp. 2518-2522). IEEE.

[107] Sayeed, A. and Perrig, A., 2008, March. Secure wireless communications: Secret keys through multipath. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 3013-3016). IEEE.

[108] Xu, W., Jha, S. and Hu, W., 2018, August. Exploring the feasibility of physical layer key generation for LoRaWAN. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 231-236). IEEE.

[109] Tsai, K.L., Leu, F.Y., Hung, L.L. and Ko, C.Y., 2020. Secure session key generation method for LoRaWAN servers. *IEEE Access*, *8*, pp.54631-54640.

[110] Kameni Ngassa, C.L., Molière, R., Delaveau, F., Sibille, A. and Shapira, N., 2017. Secret key generation scheme from WiFi and LTE reference signals. *Analog Integrated Circuits and Signal Processing*, *91*, pp.277-292.

[111] Moara-Nkwe, K., Shi, Q., Lee, G.M. and Eiza, M.H., 2018. A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. *IEEE Access*, *6*, pp.11374-11387.

[112] Bashaa, M.H., Al-Alak, S.M. and Idrees, A.K., 2019, April. Secret key generation in wireless sensor network using public key encryption. In *Proceedings of the international conference on information and communication technology* (pp. 106-112).

[113] Bottarelli, M., Karadimas, P., Epiphaniou, G., Ismail, D.K.B. and Maple, C., 2021. Adaptive and optimum secret key establishment for secure vehicular communications. *IEEE Transactions on Vehicular Technology*, *70*(3), pp.2310-2321.

[114] Wan, J., Lopez, A.B. and Al Faruque, M.A., 2016, April. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. In 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS) (pp. 1-10). IEEE

[115] Badawy, A., Khattab, T., ElFouly, T., Mohamed, A. and Trinchero, D., 2014, October. Secret key generation based on channel and distance measurements. In *2014 6th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT)* (pp. 136-142). IEEE.