International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Jan-24)

http://dx.doi.org/10.12785/ijcds/150117

Physical Key Generation Using Modified Discrete Wavelet Transforms For The Internet of Things

RakeshSharma [1], Poonam Jindal [2] and Brahmjit Singh [3]

Department of Electronics and Communication, NIT Kurukshetra. Haryana 136119, India

Received 25Feb. 2023, Revised 2Jan. 2024, Accepted 6Jan 2024, Published 15Jan. 2024

Abstract: Security and privacy of data are important factors in the Internet of Things (IoT), which enables safe communication with emerging objects. The non-standardization of security protocols on the internet of things makes them vulnerable to intruders and compromises the process of communication. Conventional cryptography approaches face certain limitations in the generation of keys for authentication and authorization of communication systems. The limitations of the cryptography approach are explored in terms of computational overhead and hardware requirements. Singal processing is an alternative cryptography approach for key generation in physical-layer wireless communication systems. The wireless channel's reciprocity principle is used to generate keys. The important factor in signal-based key generation is the process of quantization. In this manuscript, we propose modified discrete wavelet transform (DWT) methods for key generation in IoT. The modification of discrete wavelet transform methods encapsulates the process of common spatial patterning (CSP). The CSP is another signal processing method for the formation of signal patterns. The proposed method reduces DWT discrepancies and yields a key generation technique that is efficient. Key generation processing used multi-bit quantization to quantify the product of the modified discrete wavelet transform. The proposed algorithm for key generation simulates different numbers of device nodes in indoor and outdoor scenarios. Use MATLAB tools to simulate the process and measure standard parameters such as AKL and KDR. According to the results, the suggested technique outperforms existing key generation algorithms by 3%.

Keywords: IoTs, Physical Layer, Wireless Communication, DWT, CSP, Cryptography

1. Introduction

IoT is a way for communication devices to connect wirelessly and use new technologies. The reachability and acceptability of the internet of things are increasing in every area of development, such as smart health care, smart cities, smart agriculture, and many more. Because of the multiple integrations of emerging devices and communication protocols, new security challenges for secure data transfer arise. Most operational devices use radio frequencies and are compromised by third-party attacks. The vulnerability of radio frequency and communication protocols is a bottleneck problem in the transformation of IoTs. Data security and privacy are significant issues for the IoTs. The majority of the authors focused on network security mechanisms that used traditional cryptography techniques. For the computation of key formation and distribution, cryptography algorithms necessitate a large amount of computational-cost and memory resources.The significant challenges for IoT-enabled communication devices are limited resources such as bandwidth and memory. The limitation of resources hampers the proper functioning and utilization of the classical cryptography approach, the limited functioning of classical cryptography algorithms, and a discrepancy in authentication, authorization, and integrity of communication. The physical layer property-based key generation approach is an alternative approach to IoT security. The physical layer key generation approach is a low-computational processing function that does not require expensive resources. The issue with physical layer key generation-based security approaches is the fading of signals and many other parameters. The physical layer key generation approach has the primary benefit of dynamically building keys between pairs of communication devices by studying channel reciprocity and randomness. Communication systems can use channel reciprocity to determine the statistically connected channel state and retrieve the passcode. Time-varying approaches, on the other hand, consider issues inside the channel state and influence how effectively keys are generated. To quantify the physical layer information of a wireless channel, channel state information (CSI), received signal strength (RSS), or phase can all be employed. Unlike CSI and Sequence, the RSS-based key expansion procedure does not necessitate any hardware modifications in order to be used with widely available wireless devices. As a result, RSS provides the most commonly used statistic in physical layer key generation systems to generate key pairs. Despite numerous investigations on key generation and extraction utilizing RSS, current algorithms have a low frame produc-

E-mail address: rakeshvce2004@gmail.com, poonamjindal81@nitkkr.ac.in, brahmjit@nitkkr.ac.in

tion rate and a large bit dispute rate. In this research, we describe a physical layer key generation mechanism that relies on wireless channel reciprocity. Channel testing, preprocessing, digitization and encoding, data reconciliation, and privacy amplification are the five aspects of the proposed technique. The processing algorithm applies to the collection of channel probing data from transceivers, which separately applies a pattern based on discrete wavelet transform and common spatial patterns (CSP). By adding CSP, the number of bits that don't match when key sequences are made is removed. Our main contributions are summarized as follows: A novel pattern-based key generation approach is proposed to achieve reliable and efficient physical layer key generation. The common spatial pattern reduces bit mismatches after the processing of the modified wavelet transform method. A lightweight key generation algorithm with low communication overhead is proposed. The number of information reconciliation processes has been reduced to 3%. For the proposed key generation method, simulation experiments and performance evaluations are carried out. The state-of-the-art results analysis of the proposed algorithm is compared with the existing DCT and DWT key generation approaches. The rest of the paper is organized as: In Section II, "related work "is specified; "existing methodology " and "proposed methodology "are given in Sections III and IV. In Section V, "experimental analysis" is given; in Section VI, "results and discussion" is mentioned; and finally, "conclusions and future" work is given in Section VII.

2. Related Work

The diversity and simplicity of channel reciprocity measurement-based physical layer-based key generation enhance the reliability and security of internet of things-enabled devices. Most of the authors apply a transform-based approach for the encoding and transformation of bits. Some important recent work is described here. The authors of[1] propose methods for increasing key generation speed while preventing data loss during transmission. Manjit Kaur and colleagues [2] demonstrated that the mutation and dispersion of each row and column are reliant on the original mixed row and column, implying that the suggested approach is sensitive to input data. The encryption process was divided into two stages: row-wise and column-wise. For each phase individually, the permutation and diffusion processes were used. Zhang, Junqing, et al. [3]: This research provides an in-depth examination of wireless key generation-based compact security protocols suited for IoTs. Ning Xie et al.'s[4] provide a comprehensive analysis of the capabilities and methods available for physical layer authentication (PLA). The primary distinction between the two groups is whether Alice actively inserts tags into the raw message. Mike, Yuliana, and others [5] present a synchronized quantization (SQ) strategy that synchronizes data blocks throughout the quantized phase, as well as a signal strength exchange (SSE) method as an efficient information generator in this paper. By performing a mega conversion directly from the measurement channel parameters, the SQ technique removes the signal pre-processing stage. This is proved by a 25.77-fold reduction in computation time. Mike, Yuliana, and others [6] One method for addressing the problems with communication security is physical layer security (PHYSEC). In this study, they investigated PHYSEC, which makes use of channel reciprocity. Consequently, the likelihood of receiving a matching secret key is likewise rising. Additionally, Wie and others [7] suggest that the built-in SKG scheme's stages might be simplified by the combined multilevel quantization (CMQ) approach because it could generate numerous identical results with a focus on inexpensive and hardware-restricted equipment for IoT platforms. This family of approaches offers a revolutionary perspective on interference management for safeguarding wireless communications. In [8], Margelis and others propose the SKY Glow secret key generation system, which is tested on gadgets with IEEE 802.15.4 radios and aimed at resource-constrained IoT platforms. The authors proposed SKY Glow, a resource-constrained IoT device-friendly secret key generation technique that is energy-efficient. Mutaz Elradi, Saeed, and others [9] In order to establish a secure network among WSNs as well as a cloud service in IoT, an authentication key agreement mechanism is put forth in this work. A key pair for WSN identification between a cloud server and a client can be generated using the suggested method. Rushan Lin and colleagues [10] evaluate the received signal strength (RSS) of signals in this study in order to propose an effective physical layer key generation strategy. In order to decrease the high measurement inaccuracy rate and boost key generation rate, they also developed a randomness extractor for a pair of transmitters to improve bit production rate and ensure key randomness. Moving window averaging is used by Ankit Soni and others [11] to pre-process the received signal strength indicator (RSSI) of beacons sent back and forth among Alice and Bob. They describe a method for wireless secret key creation based on moving window averaging (MWA). They were able to assess the success of the proposed approach and conclude that the produced keys were sufficiently random by using the NIST statistical test to check their unpredictability. Guyue Li and colleagues [12] present comprehensive and quantitative research on wireless channel randomization and one-time password (OTP) for message integrity in this paper. The "identical key-based physical layer secure transmission" (IK-PST) and "un-identical key-based physical layer secure transmission" (UK-PST) approaches were presented. While UKPST employs non-identical keys, IK-PST employs the same pair key on both sides. Neal et al. [13]explain interpolating, compensating for signal distortion, and capturing network observations with a multicity adjustable quantized approach that allows for multiple bits per component, described as high-rate uncorrelated bit extraction (HRUBE). The HRUBE technique, which is used to design systems with a defined constraint on the possibility of bit discrepancy, includes an analysis to quantify the probability of bit disagreement. To increase the reciprocity of channel parameters, Dengke Guo [14] presented a simple key generation approach that includes a moving average

filtering (MAF) pre-processing phase prior to quantization. In this study, Kalyani et al. [15] employ cryptographic-based ways to improve IoT security authentication. We employ extremely dependable Optimal Holomorphic Encryption (OHE) in this study to safeguard sensitive IoT data. Although the OHE with key authentication technique they proposed is effective, dealing with large-scale counts can be time-consuming. In order to ensure security using holomorphic approaches, attempts are being made in future upgrades to expand a multi-cloud design. Miroslav Mitev and colleagues [16] demonstrate that, when compared to the best dynamic programming solution, a heuristic technique with linear complexity incurs relatively minimal loss. Any of the approaches presented here could pave the way for a new generation of proxy security devices. They investigate the usage of SKG in combination with physical unclonable functions (PUF) authentication techniques in this research, demonstrating how this can dramatically speed up key generation and authentication when compared to more traditional techniques. Naseer at el [17] Alice and Bob generate local randomization on their own, which is combined with the distinctiveness of the wireless channel parameters to achieve maximum cryptographic key generation using this technique. Protocols are also evaluated using metrics such as bit generation rate (BGR), bit mismatch rate (BMR), bit error rate (BER), and recently introduced randomness efficiency. In this study, Soumya Banerjee [18] presents a better IoT ecosystem with a compact, anonymous, user-verified session key agreement approach. The proposed scheme's robustness in terms of security was proven by a thorough formal and informal security study. Among others, Junqing Zhang and colleagues [19] argue that any two users can use the wireless channel between them as a cryptographic key because it is a perfect source of randomness. This is applicable to the communications protocol stack's physical layer. In particular, the wireless channel is used to produce cryptographic keys, while the RFF of the transceiver is used to verify the user's identification. Namal and colleagues in [20] present that a Pentium-4 computer was used to design the proposed system. In line with technical advancements, the IoT works with data encryption systems. This embedding technique gives the user the freedom to disguise embedded distortion as noise produced by a specific picture-collecting instrument. Yasmine Harbi and colleagues [21] demonstrate various security issues in this paper, including active attacks, rejection attacks, spoofing, insufficient mutual identification, and a lack of key exchange agreements. They presented the "mutual authentication and session key agreement" (MAKA) approach to encrypt communication in IoT-enabled WSNs. Inka Trisna Dewi [22] proposed a method for automatically creating key bits by utilizing the received signal strength (RSS) between two devices. Baldii and others [23] offer in this paper a brand-new Convolutional Neural Networks (CNN) application based on recurrence plots (RP), in which CNN is used to create images from the original time series produced from digitized RF emissions. The proposed method can be used as a complementary authentication approach rather than a principal approach, but it does require hyperparameter tweaking to reduce the amount of noise. Guyue Li and colleagues [24] found that in their research, cryptographic protocols and techniques are used to establish the security of wireless communications, and one of their basic primitives is secret key distribution. Using examples from IoT network prototypes, massive MIMO and mm-wave communications, and channel reciprocity-based secret key generation, this article examines the technological difficulties and prospects in these areas. Other writers, such as Zijie Ji [25], proposed and investigated wireless communication networks aided by intelligent reflecting surfaces (IRS) for private key generation. To accomplish this, they first specify the bare minimum viable private key capacity for an IRS operating as a passively beaming former in the company of many listeners. For various LoS channel and eavesdropper circumstances, they enhanced their use of their suggested IRS optimization algorithm. In [26], Bacem Mbarek and colleagues developed the IoT to facilitate connectivity and data exchange between systems, objects, and people. One of the IoT infrastructure technologies that has been used to increase propagation and connectivity in IoT networks is radio frequency identification (RFID). In order to offer a safe and effective transaction between the tag and the reader in IoT applications, they have introduced a new RFID authentication protocol called SAM in this work. Long Jiao and colleagues [27] This article outlines the primary 5G wireless network enabling technologies that present an opportunity to address current key generation challenges at the physical layer. Through three case studies, they show how 5G communication technology can help with physical layer key generation, such as thwarting founder eavesdroppers, obtaining a lower bit discrepancy ratio in low SNR conditions, and lowering correlation coefficients under high probing rates. Others include Mohanad Alhasanat [28]: This research presents a ground-breaking key exchange technique for IoT networks. The suggested method distributes encryption keys among network nodes by utilizing channel diversity. This research suggests a new physical-layer key distribution approach for IoT networks. The extraction of uncorrelated keys is ensured by the varied, autonomous, and randomized channel parameters among each node and the main entity. For example, Haji M. Furqan [29] says this paper provides new ways for generating private keys from communication networks in multi-carrier systems in order to ensure the secrecy and authenticity of wireless communication systems. The proposed technique can be explored in several versions, assuming various activation ratios and block sizes. Li Sun, and others[30] IoT functioning requires a high level of communication security. Physical layer security (PLS), one of the methods for communication security, has attracted a lot of interest from both academics and business since it can provide uncrackable, demonstrable, and quantifiable secrecy. This article offers a comprehensive examination of the subsystem security mechanisms employed by IoT. According to Qiao QI and his associates[31], an enormous number of IoT devices must have seamless access to the constrained radio

spectrum, and this is a requirement for the impending fifth-generation (5G) cellular network. Then, using numerical simulation, they proposed a workable and successful design approach for securing enormous access and demonstrated the performance benefit. In [32], Marko Jacovic and companions present a simple method for creating encryption data at the physical layer to amend IoT security accordingly. They establish an effective technique by combining the pre-existing channel prediction and carrier frequency offset (CFO) components of orthogonal frequency division multiplexing (OFDM) receivers. They talked about traditional OFDM receiver designs and how CFOs and wireless channels might affect them. In [33], Jan and others proposed a simple way for mutual authentication in an encryption system to establish the identity of the participants. This approach employs a basic four-way handshake. According to Yida Wang and colleagues [34], the typical AoI constraint, in particular, compels the transmitters to send message signals with a better chance and puts a definite lower bound on the amount of data transmit power required to achieve nonzero covertness. The transmit probability in concealed communications not only determines the rate at which information signals are generated, but it also shows the prior distribution of the alternate explanation. According to Xudong Jia and colleagues [35], this research provides connectivity and cross-domain cryptographic techniques for IoT. In this approach, the identity-based self-authentication algorithm replaces the traditional private key infrastructure (PKI) authentication mechanism, and the block chain serves as a safeguarding anchor in place of the conventional credential of authority. The authentication technique includes both identity-based cryptography (IBC)-based cross-domain authentication and multifactor authentication. In [36], the authors propose intelligent network resource adjustment that integrates the software-defined network controller with a lightweight machine learning algorithm. According to Farhan Ali and colleagues [37], the key distinctions between 4G and 5G were outlined in the current study. They recommended a considerable amount of spectrum for future generations, tested spectrum ranges, and examined the literature on the 5G and IoT spectrums in this study. It is obvious that 5G requires more bandwidth and more flexible usage. In [38] ,Olivier Bronchain et al., using a newly published, accessible execution of the AES fortified with a number of side-channel attack defenses, discuss the difficulty of fortifying COTS devices and the limitations of locked security assessments. Instead, they make mounting attacks more difficult by requiring additional safeguards. In [39] Yang and others, following the convergence of this process, the created data transmission generator is obtained as the objective channel estimation for a particular application situation. In contrast to standard methodologies, this study presents and assesses a framework for wireless channel modeling based on a generative adversarial network (GAN), combining advanced data processing and complicated theoretical analysis. Ankit Kumar and others [40] seek to increase data protection in this study by increasing the size of the quantum cryptography key that all involved parties share. In order to solve the issue of unsafe storage, quantum cryptography stores the split particles involved, measures them, and then creates what they use. The fundamental elements that determine the security of modern cryptographic methods are improvements in CPU processing speed and mathematical algorithms. Ben Hettwer and others [41] attempt to fill in this gap by employing attribution techniques that seek to understand deep neural network (DNN) selections in order to spot leaky processes in cryptographic implementations. In particular, we have demonstrated a method for leaking operation detection in both protected and unprotected cryptographic systems by computing heat maps of side-channel traces. Physical layer security, for example, can be utilized by Shakiba-Herfeh and others in [42] to ensure the confidentiality of node authentication messages. Unlike equivalent conventional cryptographic techniques, all of which are dependent on computational security, According to Dan Moghimi and others in [43], an attacker can use this data to extract the 256-bit encryption data for the ECDSA and ECS chord identities using lattice methods. In this study, Vesal Hakami and co-authors [44] assume that an energy-harvesting IoT device must employ a time-varying wireless channel to (losslessly) compress and report delay-constrained detecting signals to an IoT network. This is technically equivalent to a multi-agent scenario in which network users interact to work in a multi-state environment. According to Minseok Choi and colleagues in [45], the suggested method keeps track of network and queued state data and changes queue caseloads by properly matching users and allocating power to avoid excessive queuing delays. To overcome transmitter queue backlogs, the suggested system performs user pairing operations for NOMA with optimized power allocations dynamically. This work proposes a delay-constrained and chop-limited mechanism for offloading data in [46]by Huang and others. The vehicle X can commence vehicular communication using the suggested technique. In [47], Hung and others represent delay-constrained buffer-aided networks examined in this research. Reinforcement learning for relay selection is investigated. Both Sarsa and deep Q-learning were investigated. Additionally, we looked into two techniques to study the a priori information from faulty actions. According to Yuvaraja and colleagues [48],the proposed approach makes the best trade-off between increasing network lifetime and decreasing WSN end-to-end delay. This study provides a hybrid particle swarm optimization with the bat algorithm (HPSO-BA) to estimate the endurance of a given network architecture using an efficiency benchmark. Abbas Ali Rezaei [49], for example, provides a novel congestion management technique for traffic with low delay and optimum speed management for healthcare WSNs (HWSNs). The suggested technique incorporates capacity reduction and monitoring phases. The protocol for low-priority (LP) traffic supports two types of traffic: high-priority delicate traffic (HP class) and low-priority quasi-traffic (LP class). Since the delay bound for HP class traffic is constrained, the HP class queue's scheduling weight varies on a periodic basis at the intermediate weighted

fair queuing (WFQ). Scheduler Amina Boudjila and others in [50] examine the delay-constrained least cost (DCLC) problem using several heuristic techniques in this paper. They also provide a one-of-a-kind algorithm with edge between's that is based on the Taboo Search technique (EB). This paper proposes the Taboo Search (TSEB) heuristic for the solitary multicast routing problem (MRP) and conforms it to the multi-objective delay-constrained least-cost (DCLC) issue, which takes into account both expense and postpone constraints. In their article, Miroslav Mitev et al.[51] examine the effects of infusion and responsive jamming attacks on wireless secret key generation (W-SKG). First, it is demonstrated that pilot randomness can reduce replay attacks to spoofing, which are potentially less harmful. Injection man-in-the-middle (MIM) attacks have been demonstrated to be able to transform MIM attacks into less destructive jamming attacks. SVN Santhosh Kumar and colleagues [52]The Fitness Function-based Routing Protocol (FFBRP), which offers the most efficient route to extend network node lifespan, The planned framework is tested with NS2 simulators, and its performance is assessed with metrics like throughput, network throughput, edge delay, and node energy consumption. Soheil Rostami and colleagues [53] investigate and analyze the typical power consumption of a wake-up broadcast device using a semi-Markov process. The proposed solution is an efficient way to reduce device energy consumption while maintaining constant and predictable latency. Ramadevi Chappala et al.[54] provide an adaptive hybrid congestion control protocol (AHCCP) for IoT sensor networks based on route packet leave (RPL). In this protocol, an end device first detects the packets. Depending on traffic, IoT devices are divided into different priority categories. According to the type of traffic, this protocol classifies the packets sensed by the end IoT devices into different categories. Pasumpon Pandian, M.D., and colleagues [55] demonstrated that edge computing, a good substitute for cloud computing, has gained a lot of traction across a wide range of IOT-based activities, particularly in the commercial sector. The proposal is more consistent with the schedule tasks when the delay-constrained jobs are prioritized for edge computing, which is determined by measuring the edge's delay and comparing it to the production time of the tasks. In [56], Xiaoling Wu and colleagues represent the centralized approach, which requires a global understanding of the systems and is problematic in large wireless connections. The decentralized variant of the centralized approach, which requires multicast neighborhood and a swarm scale of 40, is used. In this, they compare the simulation results from hybrid particle swarm optimization (HPSO) and genetic algorithms (GA). According to Javed Iqbal and others in [57], the information might be classified as routine, critical, or delay-sensitive, depending on its reliability. The key QoS requirements for transmitting the collected data are on-time delivery and minimal losses. Even with its many advantages, developing data distribution methods for WBANs is a difficult process due to the constraints of the human body. Deeptha and others in [58] represent that the main idea behind opportunistic routing (OR) is to identify a candidate set of nearby nodes, also known as a candidate set, and employ the benefits of the wireless medium's broadcast capabilities in order to cooperatively send data packets to the destination with the help of the coordinated candidate set. A classification of OR protocols was established by this survey, taking into account the various mechanisms for candidate selection and coordination. Shuyan Hu and colleagues [59] discuss the use, transmission, trade, and management of energy acquired in upcoming wireless networks interacting with microgrids as a short-term appraisal of present accomplishments. The article places a strong emphasis on the transmission of superfluous energy inside wireless networks.

The comprehensive study of the physical layer key generation approach focuses on three segments of key generation stacks, such as channel parameters, quantization, and information reconciliation. The selection of channel parameters depends on several factors, such as the strength of the signal, the rate of attenuation, and many others. Recently, several authors selected RSS channel parameters for key generation approaches. The formation of bits for key generation and quantization is an important phase. The several authors employed different quantization approaches in single-bit and multi-bit quantization. The error rate of quantization increases the bit mismatch ratio and the impact of a mismatch on the security of the key. In our methods, employees use the CSP approach for the formation of bits. The approach of CSP reduces bit mismatches and increases the strength of security. Information reconciliation is a necessary step in key generation. The current approach to information reconciliation is employed in two modes: error control coding (ECC) and cascaded protocol. The multiple operations of XOR increase the computational cost of the key generation approach. Our proposed key generation approach reduces the number of XOR operations in the information reconciliation phase and improves the key agreement rate.

3. Existing Methodology

In IoT-based communication systems, the physical layer key generation approach provides full-stack security. It's also an alternative approach to the classical cryptography approach for shared key generation in the authentication process. The main components of physical layer key generation are wireless channel parameters such as RSS, Channel Impulse Response (CIR), and channel state information (CSI). The report survey suggests that RSS channel parameters are a better option for key generation than CIR and CSI. The key generation procedure takes advantage of the inherent unpredictability of different channels to connect shared private keys without the intervention of a third party. Some channel reciprocity variables, such as temporal variation as reflection, distortion, and dispersion of dynamically changing channel routes between communication nodes, have an impact on physical layer key generation. Recently, several authors proposed transform-based methods for key generation approaches using DCT, DWT, and other derivates of the transform function. Lower noise and

content-based key expansion pre-processing are the primary benefits of transformative approaches. The key generation principle is divided into four stages, as shown in Fig. 1. Channel probing, quantization, information reconciliation, and privacy amplification.

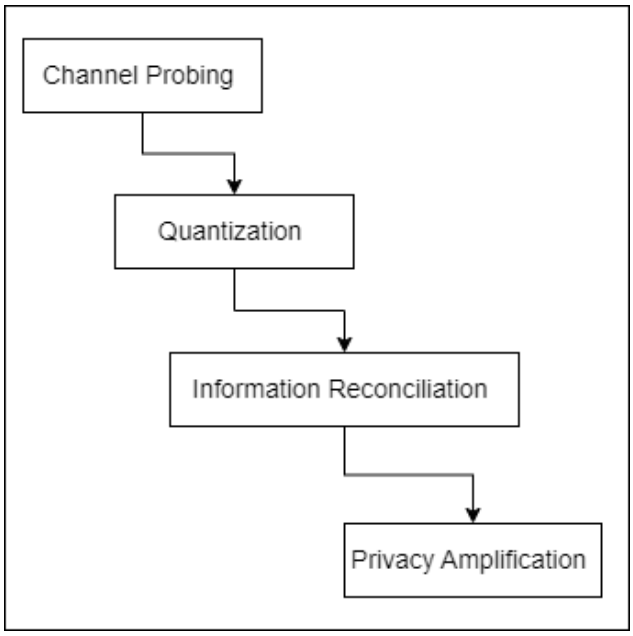

Figure 1. Phase of physical layer key generation approach.

A. Discrete Wavelet Transforms (DWT)

To minimize the discrepancies in channel parameters, we employed DWT methods for the pre-processing of RSS parameters. DWT decomposes the signal into layers of approximate and detailed information. The processing of the DWT method proceeds in a manner of approximation. The approximate parts of the transform methods are estimated as low frequency and high frequency. The processing of functions is described as

The high pass filters H and the low pass filter L process the signal S

$$YLPF[n] = \sum_{k=-\infty}^{\infty} S[k]L[k-n] \tag{1}$$

$$YHPF[n] = \sum_{k=-\infty}^{\infty} S[k]L[k-n] \tag{2}$$

The sampled of approximate and details part as

$$XA = \sum_{k=-\infty}^{\infty} S[k]L[2k-n] \tag{3}$$

$$XD = \sum_{k=-\infty}^{\infty} S[k]L[2k-n] \tag{4}$$

The coefficient XA and XD is part of approximate and details of DWT method and estimate the coefficient value of RSS channel.

B. Common Spatial Pattern (CSP)

In the key generation procedure, the common spatial pattern approach projects the encoder's matrix. The encoding approach reduced errors while increasing the fairness factors of multi-bit operations.

Step-1 normalization of low frequency spatial covariance C of the wavelet segment $D \in R^{M\times L}$

$$C = \frac{DD^T}{trace(Dd^t)} \tag{5}$$

M denotes the number of DWT signals sampled, L the number of samples, and T the transpose operation.

C. Key Generation Model

A three-node eavesdropping model is used. Bob and Alice have been approved as transceivers. Eve plays a hidden assassin who wants to listen in on Alice and Bob's private discussions. This concept is seen in Fig. 2. Furthermore, we suppose that the key generation method is accessible to the general public and that Eve, the eavesdropper, has access to it. To generate keys, the transmitter and receiver must communicate via wireless channels. Eve, the silent opponent, wishes to use the overheard relevant data to extract the opportunities to ensure between legitimate transmitters. The spacing between the silent opponent and the transponder is assumed to be at least 50% of the waveform (i.e., ½). According to [10], when the listener is far apart from the legitimate devices, the broadcast gain between the observer and the legal transponders is self-sufficient. As a result, the eavesdropper is unable to extract any significant channel gain among transceivers using his own channel observations.

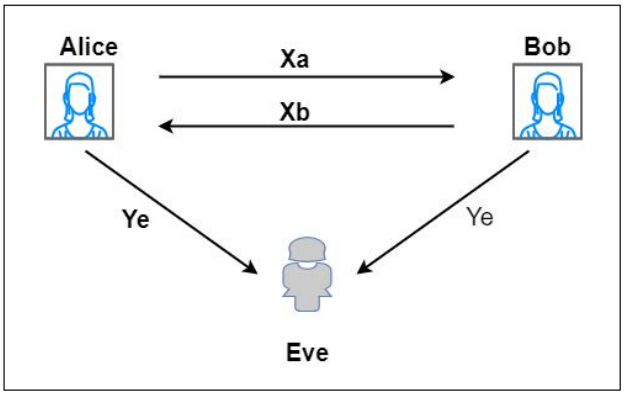

Figure 2. Key generation model based on DWT and CSP.

4. Proposed Methodology

This section describes the proposed algorithm for physical layer key generation based on DWT and CSP transform methods. The proposed technique employs DWT methods

to pre-process the probing signal S (t), the received signal r (t), and z (t) to determine the impact of n (t) on h (t), where T is the coherence time and n (t) is noise at time t. The received signal from Alice and Bob

$$ra(t_1) = s(t_1)h(t_1) + na(t_1) \tag{6}$$

$$rb(t_2) = s(t_2)h(t_2) + nb(t_2) \tag{7}$$

Here $ra(t_1)$ is received signal of Alice on time t_1, and $s(t_1)$ is probing signal and $na(t_1)$, $nb(t_2)$ is noise of Alice and Bob on time t_1, t_2.
Due to impact of noise $h(t)$ cannot directly estimated, now$h(t)$ determines

$$ha(t_1) = h(t_1) + Za(t_1) \tag{8}$$

$$hb(t_2) = h(t_2) + Za(t_2) \tag{9}$$

Here ha and hb is RSS estimated parameter and Za, Zb is impact of noise variation of Alice and Bob. The time $t_1 \neq t_2$ also $h_1 \neq h_2$.

A. Process of Key Generation

1) Probing

The approach of channel probing extracts RSS channel parameters in wireless communication. The distance factors between Alice and Bob's locations determine the strength of RSS signals. The processing of channel signals proceeds as described in equations (8) and (9).

2) Pre-processing(DWT)

The pre-processing of the received signal is an important phase of the key generation approach. The approach of pre-processing applied DWT methods. The processing of DWT in the sampling process as

$$coefficentdwt_k(S) = \left(\frac{1}{N} \sum_{S \in N_{(t)}} L_1(h) + L_2(h) \right)^2 \tag{10}$$

Here L_1 and L_2 is coefficient of approximate signals.
The sample of signals orthoprocessing of further signal is

$$Sap(S) = \frac{1}{M} \sum_{S \in N_{(t)}} \frac{dwtk}{h(t)} \tag{11}$$

Here $h(t)$ is the extracted channel and $dwtk$ is the coefficient of transformation. The further processing of the signal in the mode of quantization.

3) Quaternization Phase

The process of converting a sequence of discrete and continuous-valued samples (RSS values) into a discrete quantity of output levels (binary bits) is known as quantization. There are many various quantization systems that have been proposed in the literature and used for key generation; each has pros and cons. To reduce sampling rate and enhance bit discrepancy rate, we adopted a common spatial pattern (CSP) for the best quantization procedure (BDR).The processing of the algorithm is described in figure 3.
The Sap(s) signal is quantized for the binary stream of sampled signal by DWT methods. The stream of bits generated by CSP methods. The CSP methods process the variance matrix of signals in two different $C_1$and C_2, and product is multi-bit stream of keys.

Algorithm 1

1: Input: a Sap(S) time variance t
2: Output:multi bit(1111111100001111) 16 bit
3: Estimate $csp_{(sap,t)}$and $error(Et)$
4: $MB \leftarrow Rk_{(p,k)}$ {the set of reverse$k - N_s$ofS_t}
5: for all $MB \in csp$ and $h \in N_{(s)}$do
6: if $o\ Rk_{(h(t))}$ then
7: $updateMB \leftarrow updateMB \cup \{o\}$
8: end if
9: end for

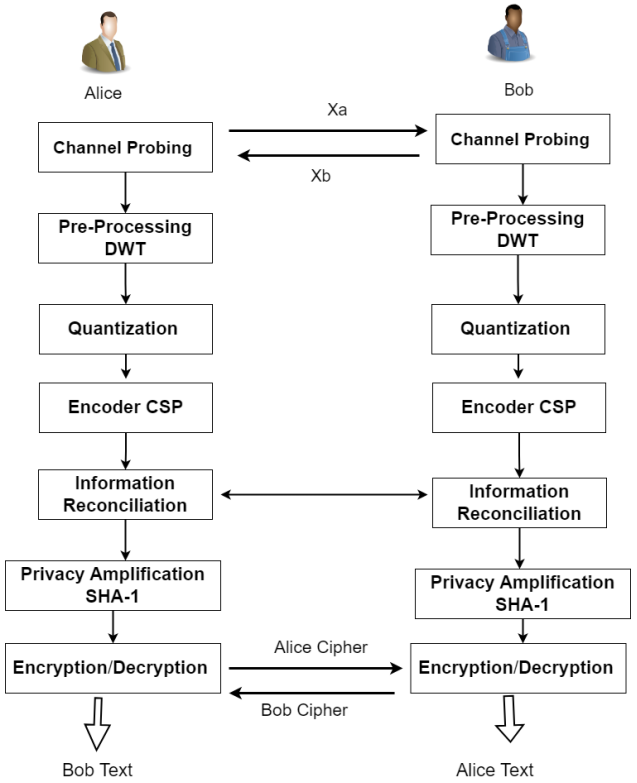

Figure 3. Proposed model of key generation algorithm based on DWT and CSP.

4) Information Reconciliation

Alice and Bob are not able to monitor the channel concurrently because wireless devices use a half-duplex communication protocol. After quantization and encoding, noise sources may cause uneven quantization results. The information reconciliation phase is required to rectify the

misaligned bits between the participants and generate the key pair. The proposed algorithm extends the common spatial pattern algorithm for information reconciliation for the minimization of errors and improves the process of key generation.

Algorithm 2

1: Input: set $MB = \{b_1, ..., b_n\}$
2: Output:set of $MB = \{L(b_1), ..., H(b_n)\}$ values
3: $i \leftarrow 0$
4: for all $MB \in L$ do
5: $Emb(L_b) \leftarrow updatebit$
6: $C^i \leftarrow \{L(b_1)N \in \{1, ..., Q\}\}$
7: end for

5) Privacy Amplification

The participating transceivers apply privacy amplification to the shared key to obliterate the information that was leaked. Two common methods for achieving privacy amplification are the extractor and the 2-universal hash function. The shared key is processed by the associated transceivers individually using the same two universal hash functions in the proposed approach, comparable to the procedure in [40]. The hash functions are chosen at random from the 2-universal hash family, which includes all of the functions h: $h : \{1...M\} \rightarrow \{0, 1\}m$ of the type

$$g(a, b) = (ax + b)modPm \quad (12)$$

$$hab(x) = gab(x)modm \quad (13)$$

For each $a \in \{1.....pM - 1\}$ and $b \in \{0.....pM - 1\}$, pM is a prime number greater than M in this example. Furthermore, the bit sequence is separated into 256-bit blocks, with M equal to 256. The value of m is affected by the randomness of the data bit sequence, the total count of additional bits used during the encryption process, and the information leaked during information reconciliation.

5. Experimental Analysis

The proposed key generation algorithms are simulated in MATLAB software, and the window operating system is version 10. The operating frequency of the communication process is 2.4 GHz. The signal distribution used the digital signal generators of the MATLAB function. The signal strength of RSS is 868 MHz. These parameters measure the performance of modified key generation algorithms [6]. The simulation process is carried out under three scenarios: indoor, outdoor, and hybrid. The proposed key generation algorithm compares with existing transform methods (DWT and DCT). The simulation parameters are mentioned in Table 1.

The outcomes of the key generation strategy employing DCT, DWT, and the proposed method are shown in Figure 4. The key generation approach situation takes place inside, and the separation between Alice and Bob is 2 m. The simulation parameters assessed the performance of average

TABLE I. Simulation parameters

Parameters	Values
System Model	IEEE 802.11
Length of channel	2048
No of communication node	3
Noise model	AWGN
Wavelet	DB2,DB3,DB4
Quantization	CSP(CDF)
Sequence length	1000,2000,3000

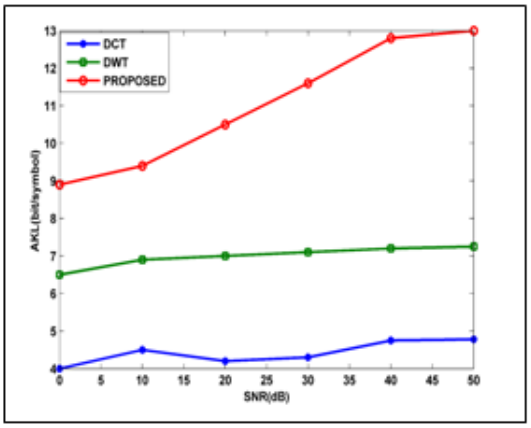

Figure 4. AKL versus SNR under indoor scenario of simulation.

key length (AKL) on various noise ratio segments. The proposed approach improves the average key length value in DCT and DWT compression. The CSP approach improves the proposed algorithm's bit- matching ratio and average key length.

Figure 5 depicts the key generation strategy employing

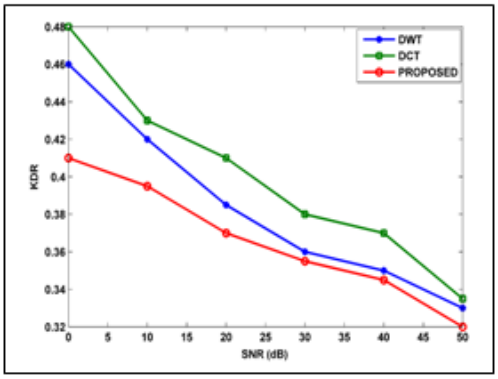

Figure 5. KDR versus SNR under indoor scenario of simulation.

DCT, DWT, and the proposed algorithm. The key generation algorithm's simulation mode is indoor environments, and the separation between Alice and Bob is 2 m. The key disagreement rate (KDR) is used to estimate the performance of the outcomes. The key disagreement rate was determined by generated key's bit mismatch. The lower the value of KDR, the better this approach outperforms DCT and DWT.

The performance of key generation techniques employing

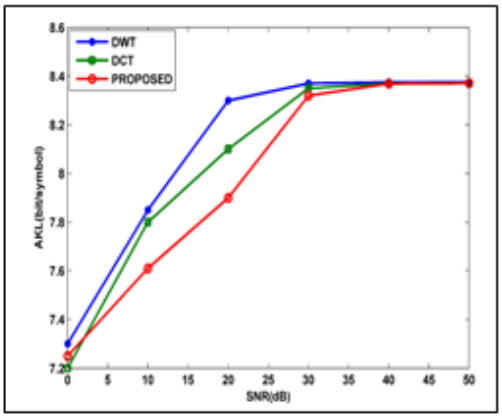

Figure 6. AKL versus SNR under outdoor scenario of simulation

DCT, DWT, and the suggested approach is shown in Figure 6. The simulation scenario is outdoor , with numerous obstacles, and the signal attenuation rate is high. The rate of attenuation decreases the signal's strength and increases the rate of bit mismatch. In the case of an outdoor scenario, the proposed algorithm of average key length produces lower results than DCT and DWT. The CSP function cannot control the impact of too much noise.

Figure 7 shows the results of key generation methods based

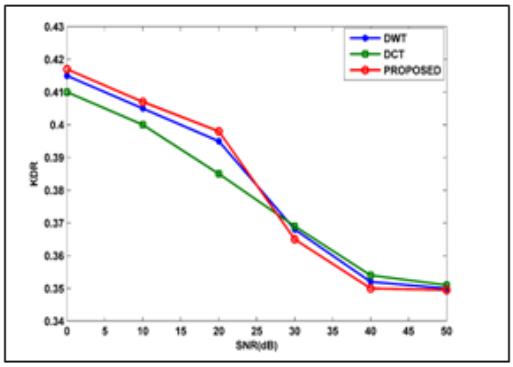

Figure 7. KDR versus SNR under outdoor scenario of simulation.

on DCT, DWT, and the proposed algorithm. Alice and Bob's simulation environments are both outside, and the length separating them is 10 meters. The noise value increases in an outside environment, affecting the key generation method. The estimate of peripheral functions is the proposed algorithm's key disagreement rate, which fluctuates with noise intensity (low and high). In this scenario, the proposed algorithm performs inferiorly to the DCT and DWT algorithms.

Figure 8 depicts the results of a hybrid simulation scenario

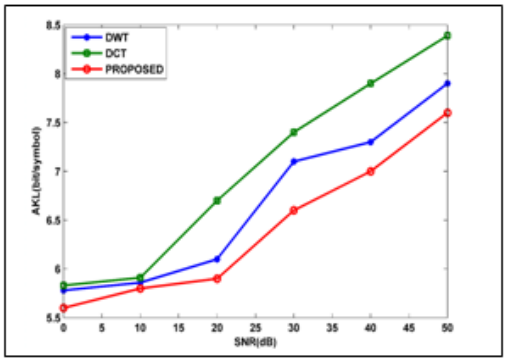

Figure 8. AKL versus SNR under hybrid scenario of simulation.

that measures the average key length on various noise segments. Alice and Bob's distance varies between 2 and 10 meters. The separation between Alice and Bob influences the fluctuation of the noise impact. In the hybrid mode of simulation, the performance of the average key length value is decreased instead of DCT and DWT.

The outcomes of the key disagreements in the hybrid

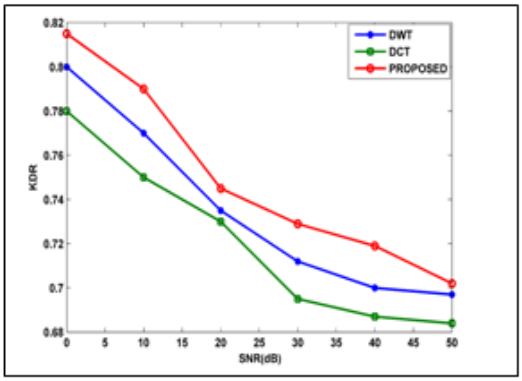

Figure 9. KDR versus SNR under hybrid scenario of simulation.

simulation scenario are shown in Figure 9. In a hybrid simulation environment, the separation among Alice and Bob can range from 2 to 10 meters. In the suggested approach, the modification of distance and the influence of

noise components increase the value of the bit-mismatch. The increase in KDR implies that the suggested method performs lower than DCT and DWT.

The results of bit-operation on the key generation algorithm

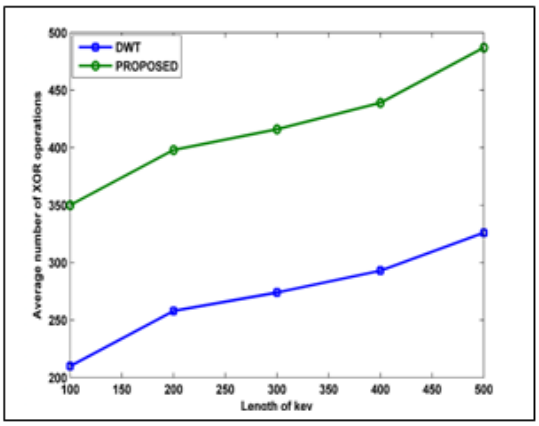

Figure 10. Average number of XOR operations versus length of key in information reconciliation.

utilizing DWT and the proposed approach are shown in Figure 10. The suggested approach increases both the number of XOR operations and the matching ratio for multi-bit operations. The operation of a bit is determined by the length of the key.

The results of the key disagreement rate on the number of

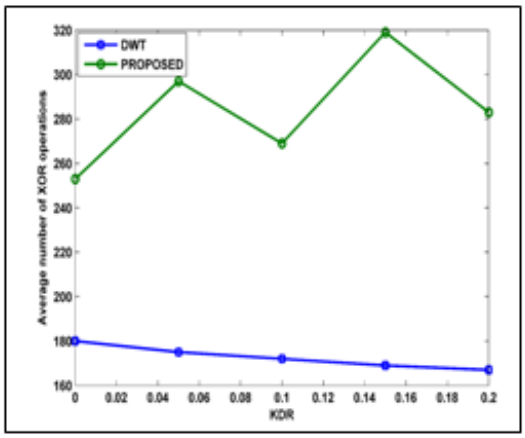

Figure 11. Average number of XOR operations versus KDR in information reconciliation.

XOR operations on a multi-bit are shown in Figure 11. The value of KDR increases as the operation of XOR increases. The additional XOR operations enhance the complexity of

TABLE II. Variation of average key length (AKL) using different noise segment in simulation indoor scenario.

SRN(dB)	DCT[10]	DWT[11]	Proposed
10	4.3	6.5	9
20	4.1	6.7	9.3
30	4.4	6.7	10.3
40	4.6	6.8	11.5
50	4.8	7.1	12

TABLE III. Variation of key disagreement rate(KDR) using different noise segment in simulation indoor scenario

SRN(dB)	DWT[11]	DCT[10]	Proposed
10	0.46	0.48	0.41
20	0.39	0.41	0.37
30	0.36	0.39	0.36
40	0.35	0.38	0.35
50	0.33	0.34	0.32

the proposed technique above DWT.

6. Result And Discussion

The performance of key generation algorithms based on DCT, DWT, and the proposed algorithm is presented in this section. The variation in results is dependent on the variation in the signal-to-noise ratio. In both indoor and outdoor scenarios, the signal-to-noise ratio is considered the same. The key generation algorithm's influence parameters are average key length and key disagreement rate. Tables 2, 3, 4, and 5 describe the KDR and AKL results. These tables consist of SNR values and measure the different results of algorithm performance in compression of existing algorithms for key generation based on transform methods.

There are two performance parameters, such as key disagreement rate and average key length, that are used to compare existing key generation DCT and DWT algorithms. The proposed algorithm employed a common spatial pattern (CSP). The CSP approach improves the length of the key size, enhances the bit pattern, and reduces the bit mismatch rate value of the generation approach. The different intervals of signal-to-noise ratio vary the performance of the key

TABLE IV. Variation of average key length (AKL) using different noise segment in simulation outdoor scenario.

SRN(dB)	DWT[11]	DCT[10]	Proposed
10	7.3	7.2	7.2
20	7.9	7.8	7.6
30	8.4	81	7.9
40	8.5	8.4	8.3
50	8.4	8.4	8.4

TABLE V. Variation of key disagreement rate(KDR) using different noise segment in simulation outdoor scenario.

SRN(dB)	DWT[11]	DCT[10]	Proposed
10	0.42	0.41	0.42
20	0.4	0.4	0.41
30	0.37	0.37	0.36
40	0.35	0.36	0.35
50	0.35	0.35	0.35

generation algorithm. In an indoor scenario, the minimum value of SNR is 10 and the maximum noise value is 50. The average key length increases by 5% from the DCT algorithm of the key generation approach and by 3% from the DWT transform method during the initial stage of key generation. The overall impact of average key length over an indoor scenario is a 4% increase when compared to the DCT algorithm and a 2.5% increase when compared to the DWT algorithm. The key disagreement rate is another parameter of the key generation algorithm that was measured in an indoor scenario with the same signal-to-noise ratio and estimated results. The results of KDR vary randomly in the cases of DCT and DWT. However, in the case of the proposed algorithm, the variation of KDR values is decreasing and the proposed algorithm's efficiency is improving. Instead of DCT, the value of KDR is reduced by about 3%, and the value of DWT is reduced by about 1.5%. The continuously decreasing value of KDR validates the key generation algorithm's efficiency. The outdoor scenario of results with the same SNR values alters the behaviour of the key generation algorithm and demonstrates that it is 3% better than the existing key generation algorithm.

7. Conclusion And Future Work

paper's goal is to offer an efficient physical layer key generation method based on the discrete wavelet transforms and the CSP approach. In terms of error minimization and multi-bit quantization, the suggested method is extremely efficient. The covariance matrix of CSP reduces the sample mismatch value and produces 16 bits. To boost the bit production rate even more and ensure the key's randomness, we also suggested a randomness extractor. To validate the proposed approach, we used wireless network card gadgets as the receivers and transmitters in experiments. The outcomes of the studies demonstrated that the devices could create keys using our proposed technique. Additionally, the comparisons showed that our method performed better 3% than those of other relevant schemes. The proposed algorithm defends against active attacks by Eve. Eavesdropping, on the other hand, is a simple and indirect attack strategy. Upcoming IoT devices will be subjected to a wide range of active malicious attacks, including message manipulation, data leakage, pilot spoofing, jamming, impersonating, and so on. The feasible secrecy rate and the chance of a secrecy outage are two performance indicators that are frequently used in DWT. From the perspective of information theory, some measures are suggested. Future IoT user expectations will be diverse due to the variety of devices and services. As a result, new measures for judging the effectiveness of PLS systems must be proposed. The new metric should provide a comprehensive evaluation of the developed approaches while taking into account multidimensional user requirements such as secrecy, latency, capacity, packet delay, and so on.

References

[1] B. Han, S. Peng, C. Wu, X. Wang, and B. Wang, "Lora-based physical layer key generation for secure v2v/v2i communications," *Sensors*, vol. 20, no. 3, p. 682, 2020.

[2] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based e-health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, 2021.

[3] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for iot security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[4] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2020.

[5] M. Yuliana, Wirawan, and Suwadi, "An efficient key generation for the internet of things based synchronized quantization," *Sensors*, vol. 19, no. 12, p. 2674, 2019.

[6] Yuliana, Mike, Wirawan, and Suwadi, "A simple secret key generation by using a combination of pre-processing method with a multilevel quantization," *Entropy*, vol. 21, no. 2, p. 192, 2019.

[7] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, and B. Ottersten, "Energy-and cost-efficient physical layer security in the era of iot: The role of interference," *IEEE Communications Magazine*, vol. 58, no. 4, pp. 81–87, 2020.

[8] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, "Efficient dct-based secret key generation for the internet of things," *Ad Hoc Networks*, vol. 92, p. 101744, 2019.

[9] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "Akaiots: authenticated key agreement for internet of things," *Wireless Networks*, vol. 25, pp. 3081–3101, 2019.

[10] R. Lin, L. Xu, H. Fang, and C. Huang, "Efficient physical layer key generation technique in wireless communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–15, 2020.

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

[12] G. Li, Z. Zhang, J. Zhang, and A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 357–369, 2020.

[13] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2009.

[14] D. Guo, K. Cao, J. Xiong, D. Ma, and H. Zhao, "A lightweight key generation scheme for the internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12 137–12 149, 2021.

[15] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in internet of things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[16] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, pp. 1–29, 2020.

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

[18] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K.-K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8739–8752, 2019.

[19] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the internet of things: Authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[20] H. Naman, N. Hussien, M. Al-dabag, and H. Alrikabi, "Encryption system for hiding information based on internet of things," 2021.

[21] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the internet of things," *Ad Hoc Networks*, vol. 94, p. 101948, 2019.

[22] I. T. Dewi, A. Sudarsono, P. Kristalina, and M. Yuliana, "Reciprocity enhancement in v2v key generation system by using hpk method," in *2019 International Electronics Symposium (IES)*. IEEE, 2019, pp. 6–13.

[23] G. Baldini, R. Giuliani, G. Steri, and R. Neisse, "Physical layer authentication of internet of things wireless devices through permutation and dispersion entropy," in *2017 global internet of things summit (GIoTS)*. IEEE, 2017, pp. 1–6.

[24] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5g and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, p. 497, 2019.

[25] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin *et al.*, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2020.

[26] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for internet of things," *Internet of things*, vol. 9, p. 100160, 2020.

[27] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5g wireless networks," *IEEE wireless communications*, vol. 26, no. 5, pp. 48–54, 2019.

[28] M. Alhasanat, S. Althunibat, K. A. Darabkh, A. Alhasanat, and M. Alsafasfeh, "A physical-layer key distribution mechanism for iot networks," *Mobile Networks and Applications*, vol. 25, pp. 173–178, 2020.

[29] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Communications Letters*, vol. 25, no. 1, pp. 59–63, 2020.

[30] L. Sun and Q. Du, "A review of physical layer security techniques for internet of things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[31] Q. Qi, X. Chen, C. Zhong, and Z. Zhang, "Physical layer security for massive access in cellular internet of things," *Science China Information Sciences*, vol. 63, pp. 1–12, 2020.

[32] M. Jacovic, M. Kraus, G. Mainland, and K. R. Dandekar, "Evaluation of physical layer secret key generation for iot devices," in *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*. IEEE, 2019, pp. 1–6.

[33] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for internet of things," *Future Generation Computer Systems*, vol. 92, pp. 1028–1039, 2019.

[34] Y. Wang, S. Yan, W. Yang, and Y. Cai, "Covert communications with constrained age of information," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 368–372, 2020.

[35] X. Jia, N. Hu, S. Su, S. Yin, Y. Zhao, X. Cheng, and C. Zhang, "Irba: An identity-based cross-domain authentication scheme for the internet of things," *Electronics*, vol. 9, no. 4, p. 634, 2020.

[36] S. Math, P. Tam, and S. Kim, "Reliable federated learning systems based on intelligent resource sharing scheme for big data internet of things," *IEEE Access*, vol. 9, pp. 108 091–108 100, 2021.

[37] F. Ali, Y. He, G. Shi, Y. Sui, and H. Yuang, "Future generation spectrum standardization for 5g and internet of things." *J. Commun.*, vol. 15, no. 3, pp. 276–282, 2020.

[38] O. Bronchain and F.-X. Standaert, "Side-channel countermeasures' dissection and the limits of closed source security evaluations," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 1–25, 2020.

[39] Y. Yang, Y. Li, W. Zhang, F. Qin, P. Zhu, and C.-X. Wang, "Generative-adversarial-network-based wireless channel modeling: Challenges and opportunities," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 22–27, 2019.

[40] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491–498, 2019.

[41] B. Hettwer, S. Gehrer, and T. Güneysu, "Deep neural network attribution methods for leakage analysis and symmetric key recovery," in *Selected Areas in Cryptography–SAC 2019: 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers 26*. Springer, 2020, pp. 645–666.

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

[43] D. Moghimi, B. Sunar, T. Eisenbarth, and N. Heninger, "{TPM-

FAIL}:{TPM} meets timing and lattice attacks," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2057–2073.

[44] V. Hakami, S. Mostafavi, N. T. Javan, and Z. Rashidi, "An optimal policy for joint compression and transmission control in delay-constrained energy harvesting iot devices," *Computer Communications*, vol. 160, pp. 554–566, 2020.

[45] M. Choi, J. Kim, and J. Moon, "Dynamic power allocation and user scheduling for power-efficient and delay-constrained multiple access networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 10, pp. 4846–4858, 2019.

[46] C.-M. Huang and C.-F. Lai, "The delay-constrained and network-situation-aware v2v2i vanet data offloading based on the multi-access edge computing (mec) architecture," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 331–347, 2020.

[47] C. Huang, G. Chen, and Y. Gong, "Delay-constrained buffer-aided relay selection in the internet of things with decision-assisted reinforcement learning," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10 198–10 208, 2021.

[48] M. Yuvaraja, R. Sabitha, and S. Karthik, "Hybrid pso-bat algorithm with fuzzy logic based routing technique for delay constrained lifetime enhancement in wireless sensor networks," *Journal of Internet Technology*, vol. 21, no. 2, pp. 479–487, 2020.

[49] F. Pasandideh and A. A. Rezaee, "An optimized service differentiated congestion management protocol for delay constrained traffic in healthcare wsn's," *Journal of Communication Engineering*, vol. 9, no. 1, pp. 126–153, 2020.

[50] A. Boudjelida and A. Lemouari, "Solving the delay-constrained least-cost routing problem using tabu search with edge betweenness," in *E3S Web of Conferences*, vol. 229. EDP Sciences, 2021, p. 01009.

[51] M. Mitev, A. Chorti, E. V. Belmega, and M. Reed, "Man-in-the-middle and denial of service attacks in wireless secret key generation," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[52] S. Santhosh Kumar, M. Selvi, A. Gayathri, D. Ruby, and A. Kannan, "Energy efficient rule based intelligent routing using fitness functions in wireless sensor networks," *Int J Innov Technol Explor Eng*, vol. 8, no. 12, pp. 5414–5420, 2019.

[53] S. Rostami, S. Lagen, M. Costa, M. Valkama, and P. Dini, "Wake-up radio based access in 5g under delay constraints: Modeling and optimization," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 1044–1057, 2019.

[54] R. Chappala, C. Anuradha, and P. Murthy, "Adaptive alternative path and rate based congestion control for 6lowpan, wsn towards internet of things," *Indian Journal of Computer Science and Engineering*, vol. 11, no. 5, pp. 446–453, 2020.

[55] D. A. P. Pandian, "Enhanced edge model for big data in the internet of things based applications," *Journal of trends in Computer Science and Smart technology*, vol. 1, no. 1, pp. 56–67, 2019.

[56] X.-l. WU, "Multicast power minimization algorithm based on pso for multicast algorithm."

[57] J. I. Bangash, A. W. Khan, A. Sheraz, A. Khan, and S. Umair, "Qos-aware data dissemination mechanisms for wireless body area networks," in *Mobile Devices and Smart Gadgets in Medical Sciences*. IGI Global, 2020, pp. 74–96.

[58] R. Deeptha, "Survey on opportunistic routing protocols in multihop wireless networks," *Management*, 2021.

[59] S. Hu, X. Chen, W. Ni, X. Wang, and E. Hossain, "Modeling and analysis of energy harvesting and smart grid-powered wireless communication networks: A contemporary survey," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 461–496, 2020.

Rakesh Sharma Rakesh Sharma received B.E degree in Electronics and Communication Engineering from Maharishi Dayanand University, Haryana in 2005, M.E degree in Electronics and Communication Engineeringfrom Maharishi Dayanand University, Haryana in 2009 (India). He is working as Assistant Professor with Electronics and Communication Engineering Department, DAV College of Engg. And Technology, Mohindergarh,Haryana, India and he is Ph.D Scholar at National Institute of Technology, Kurukshetra, India.His research interests include security algorithms for wireless networks and mobile communication.

Poonam Jindal Poonam Jindal received B.E degree in Electronics and Communication Engineering from Punjab Technical University, Punjab in 2003, M.E degree in Electronics and Communication Engineering from Thapar University, Patiala in 2005 (India). She is working as Assistant Professor with Electronics and Communication Engineering Department, National Institute of Technology, Kurukshetra, India and completed her Doctoral Degree at National Institute of Technology, Kurukshetra, India. She has published 65 research papers in International/National journals and conferences. Her research interests include security algorithms for wireless networks and mobile communication. She is a member of IEEE

Brahmjit Sigh Brahmjit Singh (Fellow of IETE and Senior Member IEEE) obtained his Bachelor of Engineering Degree from MNIT Jaipur, Master of Engineering from IIT Roorkee, and Ph.D. from GGSIP University Delhi. He is serving as Professor with ECE Department NIT Kurukshetra. Presently he is the Regional Coordinator, Regional Academic Centre for Space (RAC-S) - a joint initiative of ISRO and NIT Kurukshetra. He has been the Dean Planning and Development, Dean Research and Consultancy, and Chairman Department of ECE and Computer Engineering at NIT Kurukshetra. He developed a high-end computing faculty and established an industry supported Center of Excellence in Smart Manufacturing at NIT Kurukshetra. He has published 190 research papers in international/national journals/conferences, one edited volume of a book, seven book chapters and two sponsored research projects to his credit. Thirteen students have successfully completed their Ph.D. degree and three under progress. His research interest includes Machine Learning in Wireless Communication, and 6G Technologies. He is the recipient of the Best Faculty Award (Administration)-2019 conferred by NIT Kurukshetra and the best research paper award from the IE (India). He is associated with NBA and NAAC as program evaluator and assessor respectively and member of BoG/Academic Council of various institutes/universities. He is currently serving as the Vice Chair IEEE ComSoc Delhi Chapter and Executive Member of IETE Chandigarh Centre.