JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

PROFICIENT SECRET KEY GENERATION USING DERIVATES OF THE TRANSFORM FUNCTION FOR THE INTERNET OF THINGS

Reeta Singh[1], Pankaj Kawadkar[2]

[1]Department of Computer Science & Engg., Madhyanchal Professional University, Bhopal, India.

reeta_singh2007@yahoo.com

[2]Department of Computer Science & Engg., Madhyanchal Professional University, Bhopal, India.

kawadkarpankaj@gmail.com

Abstract

Secured data transfer over the internet of things enables communication devices is a very challenging task. Due to the limitation of computational resources, classical cryptography algorithms are vulnerable to cyber threats and loss of integrity and information. Recently, physical layer secret key generation has played a vital role in secured communication on the internet of things. The physical layer key generation approach provides an alternate means of information security using the signal reciprocity of wireless communication. This paper proposed proficient dynamic secret key generation using derivates of transform functions. The derivates of transform functions such as DCT, DWT, DWPT, and many more light transform functions the physical layer key generation employs RSSI channel parameters in conjunction with the discrete wavelet transform to generate low computational secret keys for the authentication of IoT-enabled communication devices. The proposed algorithm is very efficient and reduces the bit disagreement of the key. We use MATLAB software defined radios to conduct the experiment, and we then evaluate the effectiveness of our post-processing techniques. Our approach is helpful for safeguarding future IoT devices since it enhances the ability of targeted nodes to establish matching secret keys while reducing the risk of an eavesdropper. The experimental results of key generation methods suggest that the proposed algorithm is very efficient instead of DCT and DWT.

Keywords: wireless Communication, IoTs, Transform Methods, Cryptography, Physical Layer, RSSI

Introduction

In the current decade, the internet of things has become a core part of our daily activity with many interconnected devices that can be operated by the networks. The integration of different networks and devices results in the emergence of new security threats that provide opportunities for third parties to access and obtain confidential information. The vulnerability of open communication protocols in wireless-based communication systems exposes security goals. The classical cryptography approach applies to the authentication and authorization process for the internet of things. The internet of things devices' limited resource constraints, such as memory, bandwidth, and energy. The classical cryptography algorithm required a high computational process and more memory and bandwidth. Recently, several authors have focused on a lightweight physical key generation approach for the authentication of devices.

Submitted: 24/11/2022 **Accepted**: 09/12/2022

The lightweight key generation protocol uses a hybrid approach of cryptographic algorithms. Using channel observations to create hidden bit sequences on the devices is an intriguing alternative to key distribution. These bit sequences can be used as a seed for a random number generator or directly as an encryption key. The theory of reciprocity for electromagnetic propagation, on which this method is based, contends that the channel between two transceivers is symmetrical during the coherence time. The channel reciprocity concept, which serves as the foundation for key generation, demonstrates the similarity of the channel characteristics created by both users. However, in practise, the majority of wireless devices operate by varying estimations of channel properties. Due to noise from wireless devices and non-simultaneous measurements, this circumstance causes a reduction in the similarity of channel properties. The signal pre-processing step has been included after the measurement procedure in a number of studies in an effort to increase the comparability of the resulting channel characteristics. It has been demonstrated that include this phase can boost the channel characteristics' similarity, as seen by a rise in the correlation coefficient value. The likelihood that two users will obtain the same key increases with the channel characteristics' correlation coefficient value. The research's flaw is that it is still possible for the two users to have different keys, necessitating the error-correcting step in order to get an equal key. Longer computation times are required to make adjustments the more crucial bits that need to be fixed. Due to the exchange of parity bits during this phase, communication between two users takes longer. Channel reciprocity is a different approach to physical layer generation for the internet of things. The RSSI and CRI signals for channel reciprocity are used in key generation methods in IoT enabled devices. The major factor of randomness in channel parameter based key generation is channel parity. The factors of randomness increase the security strength of the key generation approach. The classical approach to key generation methods is replaced by a transform-based key generation approach. The transform-based key generation approach generates secure and reliable keys for authentication using DCT, DWT, WPT, and many derivates of transform methods. The derivates of transform methods explore the hidden features of channel reciprocity. This paper proposed a DWT-based gey generation approach for the internet of things. The proposed algorithm reduces the computational complexity of key generation and provides a better key length for authentication. The proposed algorithm also reduces the bit-mismatch and key disagreement rate. The rest of the article is organised as in Section II: related work, in Section III: proposed methodology and key generation model, in Section IV: description of the experimental analysis, and finally concluded in Section V.

II. Related Work

The approach of physical layer-based key-generation was first produced in the mid-1990s and theoretically analysed in 1993. The efficiency and utility of physical layer key-generation provides an efficient and secure communication process. Several studies give the direction of improvements in the key generation approach. Some recently evolved algorithms of key generation are described here. In order to create a comprehensive IoT security architecture, this article covers these protocols and demonstrates how they might be combined. 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. Additionally, their applications and protocols have been examined. Both ways work because they are based on the physical layer of the communication protocol stack. This means that they can be used alone as a security architecture. In response to Mike, Yuliana, and others [2] in this research, we present a synchronised quantization (SQ) approach as a component of the SSE system that synchronises data blocks in the quantization phase, as well as a signal strength exchange (SSE) system as an effective key generation system. This is shown by a reduction in part A's computing time of up to 25.77 times and 26.08 times, as well as a reduction in part A's communication/synchronization time of up to 1.55 times and 1.52 times. Additionally, Part B demonstrates how SSE systems can cut down computing time to 2.60 times and 2.47 times. The security requirements were also met by the built-in SSE system, because an unauthorised node couldn't make an equal key. Ankit Soni and colleagues ([3]) By employing moving window averaging to pre-process the received signal strength indicator (RSSI) of beacons sent back and forth between Alice and Bob, we present a wireless secret key generation approach in this study (MWA). At lower SNR ranges, our suggested technique significantly improves performance. The effectiveness of the suggested approach is additionally assessed by validating the generated keys' unpredictability using a test set from the National Institute of Standards and Technology (NIST). We tested how well the suggested method worked by using the NIST statistical test suite to check how random the generated keys were. We found that they were sufficiently random. This study by G. Kalyani et al. [4] focuses on the IEEE 802.15.4 MAC standards, in which the security field is part of the MAC header. The ElGamal public key cryptosystem was used to introduce the best authentication key and implement partially holomorphic encryption for the sensitive data security authentication on this MAC header. In this work, it was suggested that the CMLA algorithm be used with an optimal key generation method. [5] George Margelis and others The SKYG low-secret key generation system, which is presented in this paper and tested on gadgets with IEEE 802.15.4 radios, is aimed at resource-constrained IoT platforms. The maximum realistic number of secret bits that can be recovered from a message exchange is what we first look at. We elaborate on the operation of the suggested approach and compare these upper bounds to the current state-of-the-art. The proposed technique adds a DCT stage between the sampling and quantization stages, producing high-entropy bit sequences and eliminating the need for the privacy amplification stage. The method is also good because it works in the frequency domain, which lets the protocol get rid of high-frequency parts that don't have anything to do with each other. In line with Ning Zhang and others [6], we suggest a relay-aided vectored (RAV) secure transmission system in this paper to protect IoT networks' downlink communication from potential pilot contamination attacks. The suggested technique uses what is received to estimate the CSI for beam forming and predesign and does not distinguish between pilot sequences delivered by an adversary and the receiver. This work proposes a frequency-selective approach to authenticated secret key extraction for multipath fading channels. We take advantage of the received signal strength of many frequencies to carry out location-based device authentication and quick secret key extraction. This method shows how real-world applications could use the characteristics of the wireless channel to build an IoT security strategy that is based on a light physical layer. Bin Dai and others [8] This article establishes a generic paradigm for improving channel feedback to improve physical layer security (PLS) in Internet of Things (IoT) devices. To be more precise, we first investigate the compound wiretap channel (WTC) with feedback, which is a perfect example of how feedback may be used to improve the PLS in the downlink transmission of IoT systems. For this perfect model, a new feedback method is suggested, and a lower limit on the secrecy capacity is made to go with it. Long Jiao and colleagues [9] the key-enabler techniques in 5G wireless networks are listed in this study since they present an opportunity to address current problems with physical layer key generation. We look at the primary generation methods that are currently in use and talk about ways to fix the problems we have now. Baowei Wang and colleagues [10] ensure data privacy and access control. Each subspace's data is encrypted with the associated sub-key before being transmitted to the base station. Obtaining the correct sub key from the data is required by anyone who wishes to read or utilise data with a specific attribute at a specific time. owner or the source node. This study examined the access control issue for multi-attribute data in a two-dimensional plane in a people-centric Internet of Things. Numerous subspaces relating to the data's attributes and creation time have been created. A unique method for authenticating Internet of Things (IoT) wireless devices utilising their radio frequency (RF) emissions is presented. This method makes use of Convolutional Neural Networks (CNN) in conjunction with Recurrence Plots (RP). In recent years, a lot of research has shown that wireless devices can be verified by their RF emissions. This is because physical changes during communication cause the RF signal to change in different ways. Existing prototypes using various IoT protocols are evaluated in actual contexts to further show the viability of CRKG in real-world communication systems. These are prospective technologies for wireless networks supporting extremely high data rates and a large number of devices in 5G and beyond. We also talk about various strategies to address these problems. The ability of future wireless networks to generate physical layer secret keys in more places will help to spread physical layer-based security methods and schemes. Marko Jacovic and his associates [13] In order to enable improved IoT security, we present a low-complexity method for creating secret keys at the physical layer in this study. For an effective method, we make use of the pre-existing channel estimation and carrier frequency offset (CFO) components of Orthogonal Frequency Division Multiplexing (OFDM) receivers. We showed our key generation algorithm, which is based on how the CFO and channel of a pair of nodes are different. In this study, Gaopeng Yan et al. [14] offer a unique approach to improving the security of IOTCPS. A digital front end is introduced to hide the transmitted message's centre frequency and bandwidth. We contrast the bit-error-rate (BER) capabilities of an authorised receiver and an eavesdropper in order to gain access to system security. Results indicate that this strategy considerably improves security. In this work, we examine the total efficiency performance of the BBBSS protocol from EDPA and the BCH code from ECCA against pass number and bit disagreement ratio (BDR), respectively. Then, we combine their advantages to create a novel hybrid information reconciliation protocol (HIRP). It gets a median value for information leakage, interaction latency, and computing time by making trade-offs between the different performance measures. According to Yu Jiang and others [16], the security approach for conversation key generation and authentication between IoT devices at the physical layer is proposed in this study. The physical layer parameters are built based on the strength of the received signals at various frequencies. The double threshold quantized data is utilised for key agreement and location-based authentication with the aid of packet interleaving, smoothing, and normalisation. The physical layer parameters are built based on the strength of the received signals at various frequencies. The double threshold quantized data is used for key generation and identification through data pre-processing techniques such as packet interleaving, smoothing, and normalising. In this study by Anik Soni and colleagues [17], we suggest using principal component analysis to reduce the dimensionality of the input vector of received signal strength for key generation. For secure key generation, we only take into account the column vectors corresponding to a small number of dominant principal components rather than all the columns of the input vector, and we choose the principal components extracted from the input vector based on information content and cross correlation. By eliminating redundant samples from the data space, we minimise the numerical complexity of the key generation system and enhance BDR performance while also significantly reducing power consumption. Others include Michael Baldi. [18] This research proposes a novel method for safely creating and exchanging secret keys in passive optical networks. It makes use of key distillation based on coding techniques and physical layer randomness. The primary attack methods are taken into account, and the design criteria for the suggested procedure are presented using both analytical and numerical examples. Using conventional techniques based on ECCs, protected key creation and sharing is made possible by the dispersion of errors caused by very low power levels. This approach seems intriguing in light of potential upcoming updates to pertinent standards. By analysing the intricate features and data patterns, Ali Hassan Sodhro et al. [19] present a unique cross-layer based energy optimization algorithm (CEOA) in mIoT systems. According to experimental investigation, the suggested CEOA outperforms Baseline, its rival, in terms of effective power management and monitoring. The cutting-edge tendencies between AI and MIoT are presented in this study. Muthukumar N. [20] provides an Industrial Internet of Things (IIoT) architecture and a Model-Based Engineering (MBE) approach for the design, verification, and automatic code generation of control applications in process industries. This meta-model served as the foundation for model-based engineering. Additionally, it produced the specifications for the design and verification. Using the Model-Based Design (MBD) method, MPC, a smart controller that keeps solving an optimization routine, was made for the target platform. Zahra Ghanbari and her co-workers [21] This work reviews the resource distribution in the IoT methodically and analytically. The web databases were searched, and 143 articles were discovered. Finally, 39 articles were chosen using various filters whose approaches are closely relevant to resource allocation in the IoT. IEEE is mentioned in the majority of the articles (51.2%), and 20 of those articles are chosen. In their study of critical generating issues for an IoT multi-relay wireless network, Peng Xu et al. [22] took into account the relationship between authorised channels and eavesdropping. Both non-colluding and partially colluding eavesdropper scenarios are addressed by key generation systems. The three phases of the key agreement procedure were divided into two in the suggested key generation schemes. In order to create a secret key in step 1, we first made use of the distinction between the eavesdropping channels and the random channels connected to the relay nodes. In the second phase, the shared residual randomness between each relay pair was used to make a second secret key. Michael Zoli and other [23] authors bring attention to a number of PLS open problems, such as radio-frequency flaws and baseband communication modem accessibility. The objective is to demonstrate the broad application of our current wireless systems, opening the door for the advancement of current concepts. This novel method seeks to improve key generation performance by utilising dynamic time-frequency wideband signal processing. By using a straightforward simulation in both a typical 3GPP and a non-typical 3GPP scenario, we were able to demonstrate the overall model of the filer-bank and its advantages. Two PLS-Box filter-bank examples have also been given to show that our methods can be used with OFDM and UWB systems as they are now. To enable high-rate secret key generation using this technique, Alice and Bob independently produce local randomness to be combined with the distinctiveness of the wireless channel coefficients. In this work, two scenarios are taken into account: the first is when Alice and Bob have a direct link and communicate directly; the second is when they do not and instead communicate through an unreliable relay. After sharing the induced randomness, Alice and Bob process the data to make samples that are highly related to each other. These samples are then used to make the key. Han, Qingqing, and others [25] This study introduces the idea of vector partitioning quantization (VPQ) and further develops many new quantization techniques that can simultaneously use amplitude and phase. First, a thorough discussion of conventional amplitude quantization (TAQ) and conventional phase quantization (TPQ) is provided. Later, the idea of the ideal RVPQ is put forth, and we use theoretical error probability to compare it to the established approaches. Additionally, the BKQ algorithm and two enhanced algorithms—LKQ and CKQ—are proposed, and we elaborate on each of them. The BM algorithm is proposed to make up for K-mean’s lack of uniformity, and we use BM to three K-means quantization to make the keys that are made even more random. In Biao Han and others [26], the physical layer key generation is applied to the V2I and V2V situations in this article. A physical key generation technique based on LoRa was created to secure V2V and V2I communications. The communication is based on the Long Range (LoRa) protocol, which may create safe keys by using consensus information from long-distance measurements of the Received Signal Strength Indicator (RSSI). This will be the subject of our upcoming study. Additionally, we'll keep looking for improved quantization techniques to boost our key's unpredictable and key creation pace. Since current off-the-shelf LoRa nodes can only give RSSI information, it would be interesting to look into other channel properties like Channel Impulse Response (CIR) to speed up signal gathering. This secret key was produced in multi-hop wiretap ad-hoc networks, where all the transmitting nodes of a reliable link may be monitored. We significantly characterise the multichip wiretap model using the eavesdroppers' receiver diversity strategies. When snoops try to find their received signals by using maximal-ratio combining or maximal-gain selection, the security performance of the method is evaluated. [28] A novel physical layer secret key generation method for inter-spacecraft communication links In order to extract identical secret keys from separate observations, spacecraft use the Doppler frequency shifts of their reciprocal spaceship links as a special source of secrecy. The important disagreement rate is expressed theoretically by our work (KDR). For the first time in the literature, we have presented a security method for inter-spacecraft linkages (ISLs) in this paper. The suggested technique guarantees ongoing secrecy between two remote nodes. The proposed method's secrecy is based on the spacecraft's symmetric Doppler frequency data. The key disagreement rate (KDR) is calculated by taking into account the mistakes that spacecraft make when they try to estimate. Rakesh Bandarupalli and others [30]: in this work, the lightweight, secure Group Communication (GC) is designed using the Advanced Encryption Standard (AES), and the data integrity is then maintained using Public Key Infrastructure (PKI). The method produced safe GCs in the network against assaults, lower bandwidth use, and network overhead in key re-distribution and management operations by employing the AES-PKI algorithm. In the IoT concept, detecting inaccurate sensor readings is a key concern for secure communication and power consumption, where data integrity and energy efficiency are requirements. As a result, cryptography, an efficient technology, ensures the integrity of sensed data. LLNs have a dynamic topology and limited resources, which makes it hard to manage keys in these networks.

III. Proposed methodology

This section describes the proposed methodology of physical layer key-generation for the internet of things. The proposed algorithms encapsulate the derivates of transform methods. The derivates of transform methods scale the processing of quantization and reduce the error of bit sequence formation. The first segment of the key generation approach describes the principle of key generation, the model of key generation, and finally the algorithm of key generation.

System model of Key Generation

The system model of key generation is described in figure 1. The model of key generation used three parties is called Alice, Bob and Eve. The Alice and Bob is two authorized party for the process of communication. The Eve plays an important role of communication intervention or passive attacker. The Alice and Bob both used the RSS channel parameters for the sharing of information based on the concept of channel probing. The Ya signal transmit by Alice and Yb signal Transmit by the Bob. The symmetric of signal strength is equal in both case (Ya=Yb). Here two cases consider in case of Eve. Eve knows about the key of message and decode the information of two parties Alice and Bob. Another condition is Eve cannot aware of key and tamper the RSS information for the extraction of key value for decode information.

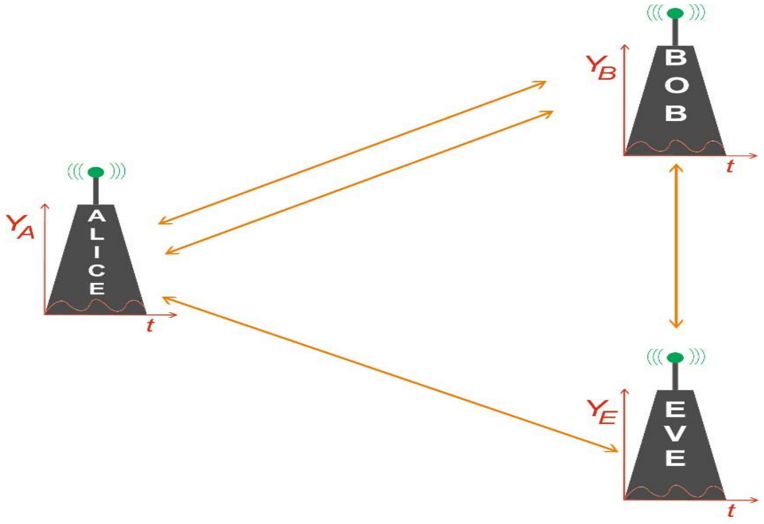

Figure 1: the process block diagram of RSS based communications in two authorized parties Alice and Bob. The third-party Eve as message and key intercept.

Proposed Algorithm

The proposed key generation algorithm collects the RSSI signals of IoT devices. The collected signals sampled with DWT methods. the derivates of transform methods scale the function of encoding and generates multi-bit sequence. The generated bit of secrete key encrypted the information and decrypted message. The randomness of key factors increases security of generated key the processing of key generation describes

WT: wavelet transform
VC: signal collector
Ni {sample rate}
Fa final received
Fi initiation of signal
$\gamma_{.}$:: selection of threshold for signal
G signal group
Wi balance factor
Do sampling of signal

Step 1. Sampling. The process of WT used VC as part of sampling process of collected signal

$$ni \in vf(vf)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} \qquad (1)$$

For Ni, the set of sample signals

$$Ni = P(ni)\alpha \ldots\ldots\ldots\ldots\ldots..(2)$$

With Fi the process of relation with derivation

$$di = \gamma_j \;\; j \frac{Xi}{G_{j,z}} \ldots\ldots\ldots\ldots\ldots\ldots.(3)$$

Derivates of TF-1 of noise process with selection factor

$$g_{j,z}\, di \times Wi \ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Check value of noise during process of collection

$$Do\ =\ \sum_{j=1}^{N}\left\lfloor\frac{Gi}{Xi}\right\rfloor=\sum_{j=1}^{N}\lfloor wi\rfloor\ \ldots\ldots\ldots\ldots\ldots..(5)$$

Selection of threshold limit for attacks level

$$IE=min\sum_{z=1}^{Z^{0}}\sum_{j=1}^{N+1}Pf\ \ldots\ldots\ldots\ldots.(6)$$

$$s.t.\sum_{n=1}^{w}IE=Ni,\qquad\forall j\qquad\qquad(7)$$

Step 2. Mapping of signal to TF-1according to value of details

N$(ni)\ (i\ =\ 1,\ldots,N\ +\ 1;\ z\ =\ 1,\ldots,Z^{0})$

$$G=\begin{cases} & \sum_{k=1}^{k}{}^{0}Do \qquad i \\ +1 & \qquad\qquad\qquad otherwise\end{cases}\ \ldots.(8)$$

$$Ad=\begin{cases}R & if\ \sum_{j=1}^{N+1}\leq iteration\\ O & \qquad otherwise\end{cases}\ \ldots\ldots\ldots\ldots\ldots\ldots.(9)$$

$$\text{Rr}\left\{\sum_{k=1}^{n}Fc+Cm+X(xi)\right\}\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.(10)$$

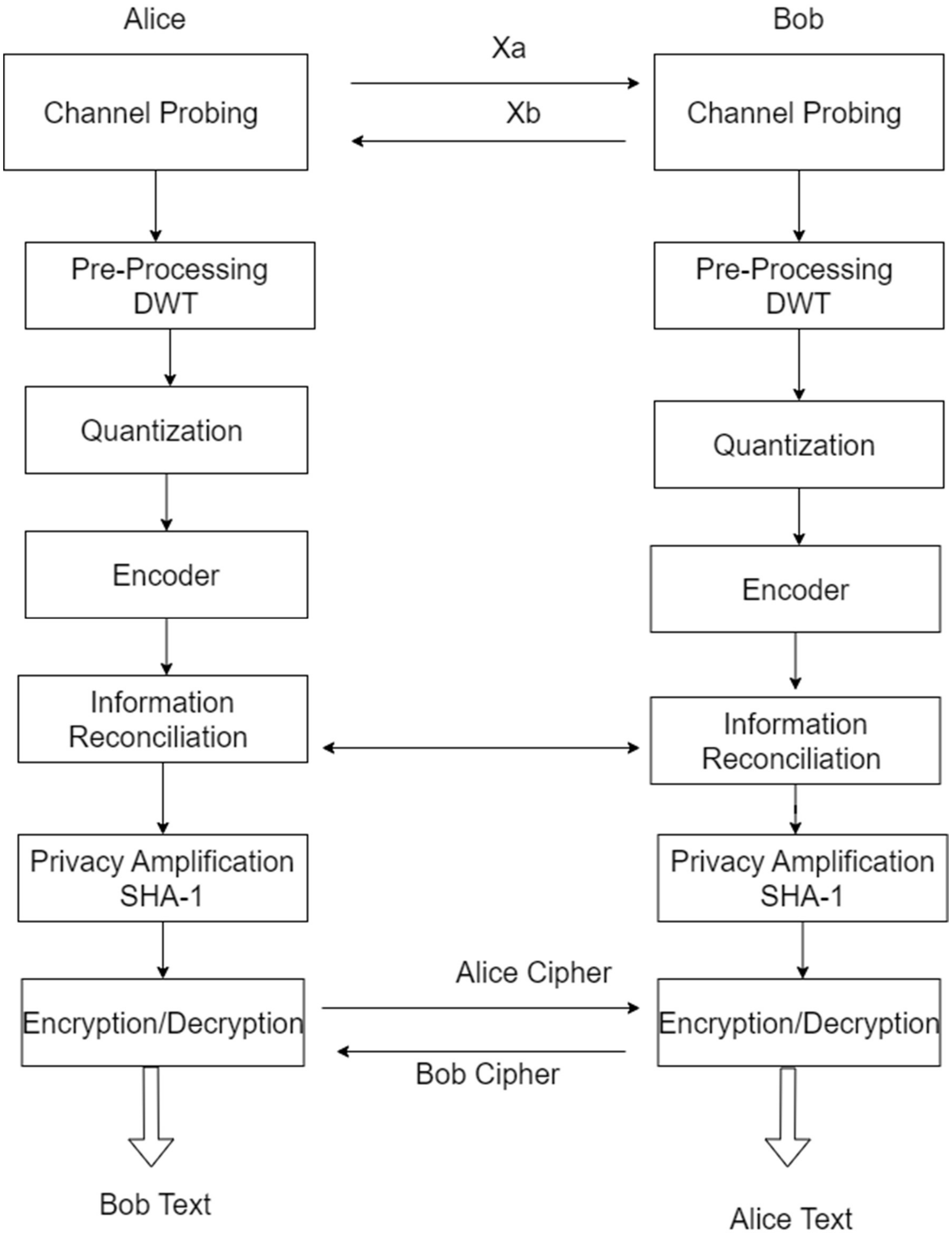

Figure 2 process block diagram of proposed model of key generation

IV. Experimental Analysis

The proposed key generation algorithm is simulated in MATLAB tools. MATLAB tools provide various function for the implementation of RSSI and transform based function such as DCT and DWT. 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 868MHz. These parameters measure the performance of modified key generation algorithms [6]. The simulation process is carried out under two scenarios: indoor and outdoor. The proposed key generation algorithm compares with existing transform methods DWT and DCT. The simulation parameters mention on table-1

Table-1Simulation parameters

Parameters	Value
System Model	IEEE 802.11
Length of channel L	2048
No of communication node	3
Noise model	AWGN
Wavelet	DB2, DB3, DB4, DB5
Quantization	CDF
Sequence length	1000,2000,3000

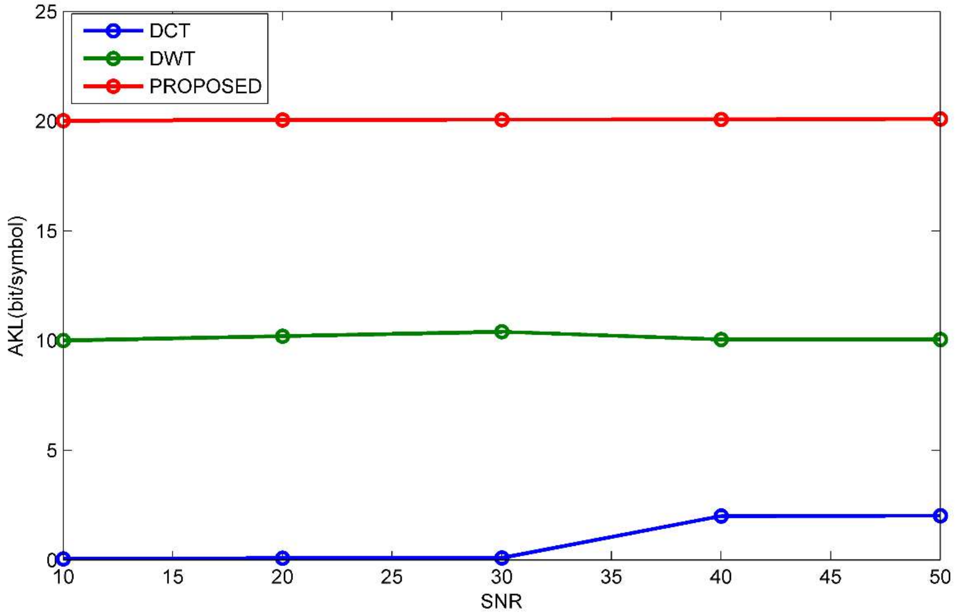

Figure 3 performance of proposed algorithm for key generation to estimate AKL against SNR in indoor scenario.

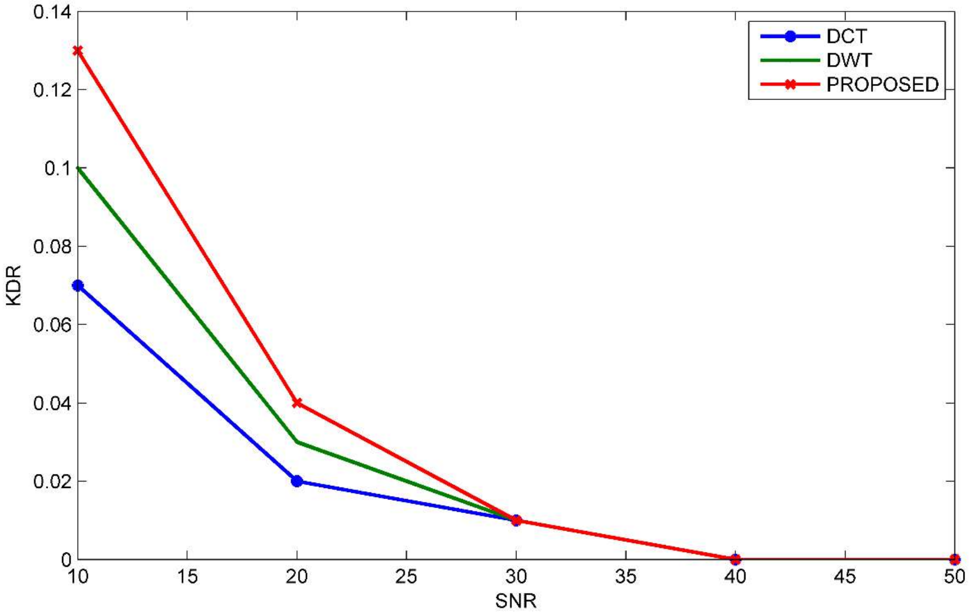

Figure 4 performance of proposed algorithm for key generation to estimate KDR against SNR in indoor scenario.

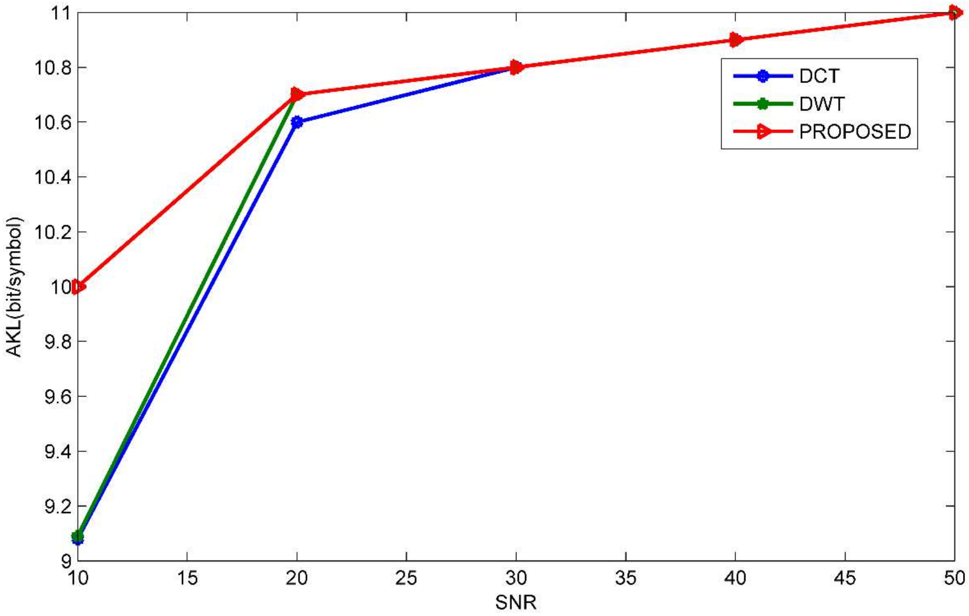

Figure 5 performance of proposed algorithm for key generation to estimate AKL against SNR in outdoor scenario.

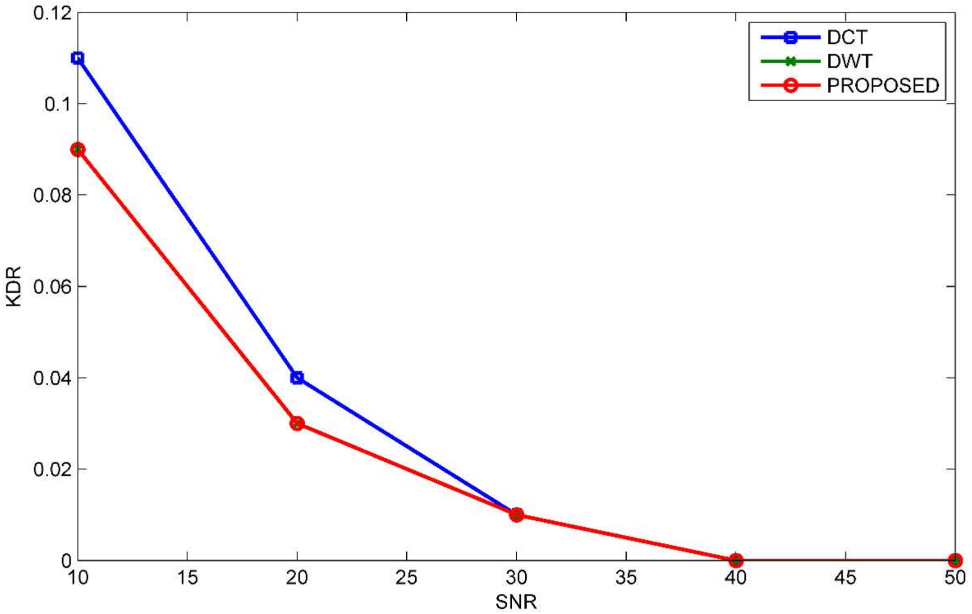

Figure 6 performance of proposed algorithm for key generation to estimate KDR against SNR in outdoor scenario.

V. Conclusion & Future Work

In this paper, we propose an efficient key generation method for improving the security of secure communication in internet of things-enabled devices. The proposed algorithm simulates two scenarios: indoor and outdoor scenarios, with dedicated parameters. results in the validation of results in terms of KDR and AKL. The reduced value of the key disagreement rate of the proposed algorithm indicates the strength of security. The proposed algorithm results are compared with the existing two algorithms, DCT and DWT. The performance of the proposed algorithm overcomes the limitations of DCT and DWT. The Coif 4, Sym 4, and Db4 wavelets are used for the analysis. Despite the tiny difference, Sym4 and Db4 wavelets often produce better results than Coif 4. The NIST randomness tests were assessed to determine the viability of using DWPT for PLS, and all sequences passed the tests, demonstrating sufficient unpredictability. In this study, the processes of information reconciliation and privacy amplification are not used. DWT pre-processing has the ability to produce outcomes that are much improved than we anticipate by properly choosing the wavelet packet decomposition level, wavelet packet atoms, and thresholds. Given that CDF quantization is used, the suggested approach has a low level of complexity. Due to DWT's binary operation, pre-processing complexity is a little bit greater than with DWT. Future scope includes extending the proposed algorithms to real-time scenarios.

References

[1]. Zhang, Junqing, Sekhar Rajendran, Zhi Sun, Roger Woods, and Lajos Hanzo. "Physical layer security for the Internet of Things: Authentication and key generation." *IEEE Wireless Communications* 26, no. 5 (2019): 92-98.

[2]. Yuliana, Mike. "An efficient key generation for the Internet of Things based synchronized quantization." *Sensors* 19, no. 12 (2019): 2674.

[3]. Soni, Ankit, Raksha Upadhyay, and Abhay Kumar. "Wireless physical layer key generation with improved bit disagreement for the internet of things using moving window averaging." *Physical Communication* 33 (2019): 249-258.

[4]. Kalyani, G., and Shilpa Chaudhari. "Data privacy preservation in MAC aware Internet of things with optimized key generation." *Journal of King Saud University-Computer and Information Sciences* (2019).

[5]. Margelis, George, Xenofon Fafoutis, George Oikonomou, Robert Piechocki, Theo Tryfonas, and Paul Thomas. "Efficient DCT-based secret key generation for the Internet of Things." *Ad Hoc Networks* 92 (2019): 101744.

[6]. Zhang, Ning, Renyong Wu, Shenglan Yuan, Chao Yuan, and Dajiang Chen. "RAV: Relay aided vectorized secure transmission in physical layer security for Internet of Things under active attacks." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8496-8506.

[7]. Jiang, Yu, Aiqun Hu, and Jie Huang. "A lightweight physical-layer based security strategy for Internet of things." *Cluster Computing* 22, no. 5 (2019): 12971-12983.

[8]. Dai, Bin, Zheng Ma, Yuan Luo, Xuxun Liu, Zhuojun Zhuang, and Ming Xiao. "Enhancing physical layer security in internet of things via feedback: a general framework." *IEEE Internet of Things Journal* 7, no. 1 (2019): 99-115.

[9]. Jiao, Long, Ning Wang, Pu Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng. "Physical layer key generation in 5G wireless networks." *IEEE Wireless Communications* 26, no. 5 (2019): 48-54.

[10]. Wang, Baowei, Wei Li, and Neal N. Xiong. "Time-based access control for multi-attribute data in internet of things." *Mobile Networks and Applications* 26, no. 2 (2021): 797-807.

[11]. Baldini, Gianmarco, Raimondo Giuliani, and Franc Dimc. "Physical layer authentication of Internet of Things wireless devices using convolutional neural networks and recurrence plots." *Internet Technology Letters* 2, no. 2 (2019): e81.

[12]. Li, Guyue, Chen Sun, Junqing Zhang, Eduard Jorswieck, Bin Xiao, and Aiqun Hu. "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities." *Entropy* 21, no. 5 (2019): 497.

[13]. Jacovic, Marko, Martin Kraus, Geoffrey Mainland, and Kapil R. Dandekar. "Evaluation of physical layer secret key generation for IoT devices." In *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*, pp. 1-6. IEEE, 2019.

[14]. Yan, Gaopeng, Zian Wang, Yongan Qian, and Yongpeng Wu. "Physical layer security of digital front end based Internet of Things communication in power systems." In *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pp. 236-241. IEEE, 2019.

[15]. Li, Guyue, Zheying Zhang, Yi Yu, and Aiqun Hu. "A hybrid information reconciliation method for physical layer key generation." *Entropy* 21, no. 7 (2019): 688.

[16]. Jiang, Yu, and Siqing Chen. "A Novel Physical-layer Security Scheme for Internet of Things." In *Journal of Physics: Conference Series*, vol. 1176, no. 4, p. 042090. IOP Publishing, 2019.

[17]. Soni, Ankit, Raksha Upadhyay, and Abhay Kumar. "Dimensionality reduction in wireless physical layer key generation." In *2019 IEEE 16th India Council International Conference (INDICON)*, pp. 1-4. IEEE, 2019.

[18]. Baldi, Marco, Franco Chiaraluce, Lorenzo Incipini, and Marco Ruffini. "Code-based physical layer secret key generation in passive optical networks." *Ad Hoc Networks* 89 (2019): 1-8.

[19]. Sodhro, Ali Hassan, Mohammad S. Obaidat, Sandeep Pirbhulal, Gul Hassan Sodhro, Noman Zahid, and Abhimanyu Rawat. "A novel energy optimization approach for artificial intelligence-enabled massive internet of things." In *2019 International symposium on performance evaluation of computer and telecommunication systems (SPECTS)*, pp. 1-6. IEEE, 2019.

[20]. Muthukumar, N., Seshadhri Srinivasan, Kannan Ramkumar, Deepak Pal, Juri Vain, and Srini Ramaswamy. "A model-based approach for design and verification of Industrial Internet of Things." *Future generation computer systems* 95 (2019): 354-363.

[21]. Ghanbari, Zahra, Nima Jafari Navimipour, Mehdi Hosseinzadeh, and Aso Darwesh. "Resource allocation mechanisms and approaches on the Internet of Things." *Cluster Computing* 22, no. 4 (2019): 1253-1282.

[22]. Xu, Peng, Dongyang Hu, and Gaojie Chen. "Physical-layer cooperative key generation with correlated eavesdropping channels in IoT." In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pp. 29-36. IEEE, 2020.

[23]. Zoli, Marco, André Noll Barreto, Stefan Köpsell, Padmanava Sen, and Gerhard Fettweis. "Physical-Layer-Security Box: a concept for time-frequency channel-reciprocity key generation." *EURASIP Journal on Wireless Communications and Networking* 2020, no. 1 (2020): 1-24.

[24]. Aldaghri, Nasser, and Hessam Mahdavifar. "Physical layer secret key generation in static environments." *IEEE Transactions on Information Forensics and Security* 15 (2020): 2692-2705.

[25]. Han, Qingqing, Jingmei Liu, Zhiwei Shen, Jingwei Liu, and Fengkui Gong. "Vector partitioning quantization utilizing K-means clustering for physical layer secret key generation." *Information sciences* 512 (2020): 137-160.

[26]. Han, Biao, Sirui Peng, Celimuge Wu, Xiaoyan Wang, and Baosheng Wang. "LoRa-based physical layer key generation for secure V2V/V2I communications." *Sensors* 20, no. 3 (2020): 682.

[27]. Yang, Yuli, Meng Ma, Sonia Aïssa, and Lajos Hanzo. "Physical-layer secret key generation via CQI-mapped spatial modulation in multi-hop wiretap ad-hoc networks." *IEEE Transactions on Information Forensics and Security* 16 (2020): 1322-1334.

[28]. Topal, Ozan Alp, Gunes Karabulut Kurt, and Halim Yanikomeroglu. "Securing the inter-spacecraft links: Doppler frequency shift based physical layer key generation." In *2020 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, pp. 112-117. IEEE, 2020.

[29]. Moara-Nkwe, Kemedi. "Physical Layer Key Generation in Resource Constrained Wireless Communication Networks." PhD diss., Liverpool John Moores University, 2020.

[30]. Rakesh, Bandarupalli, and H. Parveen Sultana. "A novel methodology for secure group communication in Internet of Things." *Materials Today: Proceedings* (2021).