ISSN: 2633-4828 Vol. 6 No.1, January, 2024

International Journal of Applied Engineering & Technology

A LIGHTWEIGHT PHYSICAL LAYET KEY GENERATION METHOD USING DISCRETE WAVELET TRANSFORMS FOR THE INTERNET OF THINGS

Ramesh Shahabade[1] and Dr. Mohd Zuber[2]
Department of Computer Science and Engineering, Madhyanchal Professional University, Bhopal, India
rameshshahabade@ternaengg.ac.in and mzmkhanugc@gmail.com

ABSTRACT
This paper proposes a novel method for physical layer key generation using a discrete wavelet transform. The proposed method reduces time complexity and communication overheads and increases the strength of node authentication. The proposed method modified the sampling approach for RSS channel characteristics to minimize the signal deviation. The process of key generation method reduces the number of steps for key generation approach. The process of key generation employed only three phases, such as channel parameters, signal sampling, and privacy amplification. The proposed method was simulated in MATLAB simulation software with 500 nodes in different scenarios, such as outdoor and indoor. The proposed algorithm reduces the key disagreement rate. The performance of the proposed algorithm compares with that of existing algorithms such as DCT, DWT, and WPT. The analysis of the results suggests that the proposed algorithm is better than existing algorithms.

Keywords: oTs, Key Generation, Physical Layer, DCT, DWT, Window Slide

INTRODUCTION
Physical layer security plays a vital role in increasing device-enabled communication, such as the internet of things. The physical layer security approach is an alternative approach to classical cryptography. The classical cryptography approach of key generation for authentication of device communication is very complex in terms of time and cost. Recently, several authors proposed a physical layer key generation approach based on transform-based functions such as discrete wavelet transforms and variants of transform functions. The process of physical layer key generation employed four phases, such as channel probing, quantization, information reconciliation, and privacy amplification. In the channel probing stage, the transceivers send channel-probing frames to each other to obtain channel measurements through the received signals, which carry the random information of the channel. The transceivers turn the channel measurements into consistent binary sequences, or candidate keys, by quantizing and resolving the information. Finally, privacy amplification is implemented to eliminate the information leaked during the above process. Randomness is a key factor in the security of the physical layer key generation approach. The factors of randomness in the discrete wavelet transform approach are higher than in another approach of key generation for the physical layer. The discrete wavelet transform is a modulation approach for RSSI and CSI signals. The modulated signals reduce the errors of quantization in the key generation phase. Despite several approaches to physical layer key generation using channel characteristics and location-specific internet of things secret key generation, Signal-to-noise ratio (SNR) parameters raised several issues in physical layer key generation approaches, such as key disagreement, bit mismatch, and a lower value of randomness. The inability to obtain a consistent shared secret key is intolerable to authentication methods, which utilize the hash functions to generate authentication code. To address the aforementioned problems, this paper proposes modified discrete wavelet transform-based physical layer key generation for authentication for IoT-enabled communication devices. The modified discrete wavelet transforms (MDWT) minimize gap between the security strength of physical layer key generation. The main contribution of this paper is summaries as follows:

1. We proposed novel physical layer key generation based on a modified discrete wavelet transform (MDWT) to reduce key disagreement rates.
2. Due to the high noise of channel parameters, quantization errors are increasing and bit mismatch values are increasing. The proposed method reduces quantization errors and bit mismatches.

3. to test and verify the results of the proposed algorithm and compare them with existing transform-based methods.

The remainder of this paper is organised as follows: Section II presents recent related work in the area of physical layer key generation. Section III presents the proposed methodology for key generation. Section IV presents the experimental analysis of the proposed algorithm. In Section V, conclude papers and set the future direction of physical layer key generation.

II. RELATED WORK

The security challenges of wireless communication bring opportunities for security authentication using channel parameters for physical layer key generation. Recently, several authors proposed methods based on classical cryptography and transform-based functions. In [1], the authors proposed model is to utilise the inherent co-channel interferences in cellular IoT networks to provide a secure massive access architecture. This study examines important generation issues for an Internet of Things multi-relay wireless network, taking into account the relationship between eavesdropping and authorised channels. In [3], utilising both physical layer authentication and cryptography-based authentication, they show that the proposed methodology considerably decreases the signalling overhead while retaining competitive authentication performance. In [4], the outcomes demonstrate that the proposed scheme produced a bit error rate that was nearly identical to the MDFH. In [5], the time-frequency filter bank is a revolutionary key-generation mechanism implemented by the PLS-Box. By using filter-bank processing, the entropy of the radio channel is both collected and converted into a reciprocal security key. In [6], high-rate secret key creation is made possible by Alice and Bob separately producing local randomness, which is combined with the wireless channel coefficients' uniqueness. [7] Secrecy outage probability (SOP) and average secrecy capacity (ASC) are used to assess the performance. to assist analysis in terms of the respective moment-generating function (MGF) and characteristic function of the joint fading and interferer statistics. In [8], the proposed technique divides up the encryption keys among network nodes by making use of channel diversity. The proposed mechanism's assurance of simultaneously distributing various keys of varying lengths to all nodes is one of its main unique features. in [9] proposed a physical layer security plan for OFDM-based Internet of Things systems. By using channel measurement rather than pre-extracted data, it can alleviate the drawback of key extraction. In [11], we propose the balance mechanism (BM) and apply it to three K-means quantization algorithms in order to address the issue of weak uniformity generated by K-means. In [13] message-based tag embedding", this technique achieves PLA by integrating an authentication signal (tag) in a message transmission. It differs from conventional PLA techniques that make use of consistent power tags. in [14] To improve the unpredictability of quantization, we suggest using D-Gray coding. Due to its implementation on a number of commercial devices, MobiKey offers comparative advantages in key-generation consistency, unpredictability, and security. In [15], a secret key is designed for use in multi-hop wiretap-ad hoc networks, where it is possible for eavesdroppers to keep an eye on every transmitting node on a valid link. We provide a thorough characterization of the multi-hop wiretap model that eavesdroppers use using receiver-diversity approaches. In [16], physical-layer security has been identified as a possible means of protecting the privacy and confidentiality of communications in such strict circumstances. in [17] Numerical studies demonstrate the tightness of the proposed approximations. Both theoretical and numerical findings show that the physical layer key generation process is appropriate and useful when taking into account the security of spacecraft communication lines. In [18], expand the pairwise schemes to include a group of users in both chain and star topologies of networks. In [19] mobile WSN to be utilised in SCPM, a very reliable and effective QoS-centric reinforcement-learning-based DPM model has been constructed in this work. in [20] We discovered that this approach is vulnerable to desynchronization assaults, user cooperation, and a lack of sensor-node anonymity.

III. PROPOSED METHODOLOGY

We proposed physical layer key generation approach based on modified discrete wavelet transform functions. The proposed algorithm consists of three phases, such as estimation of channel characteristics, quantization, and privacy amplification as shown in figure1.

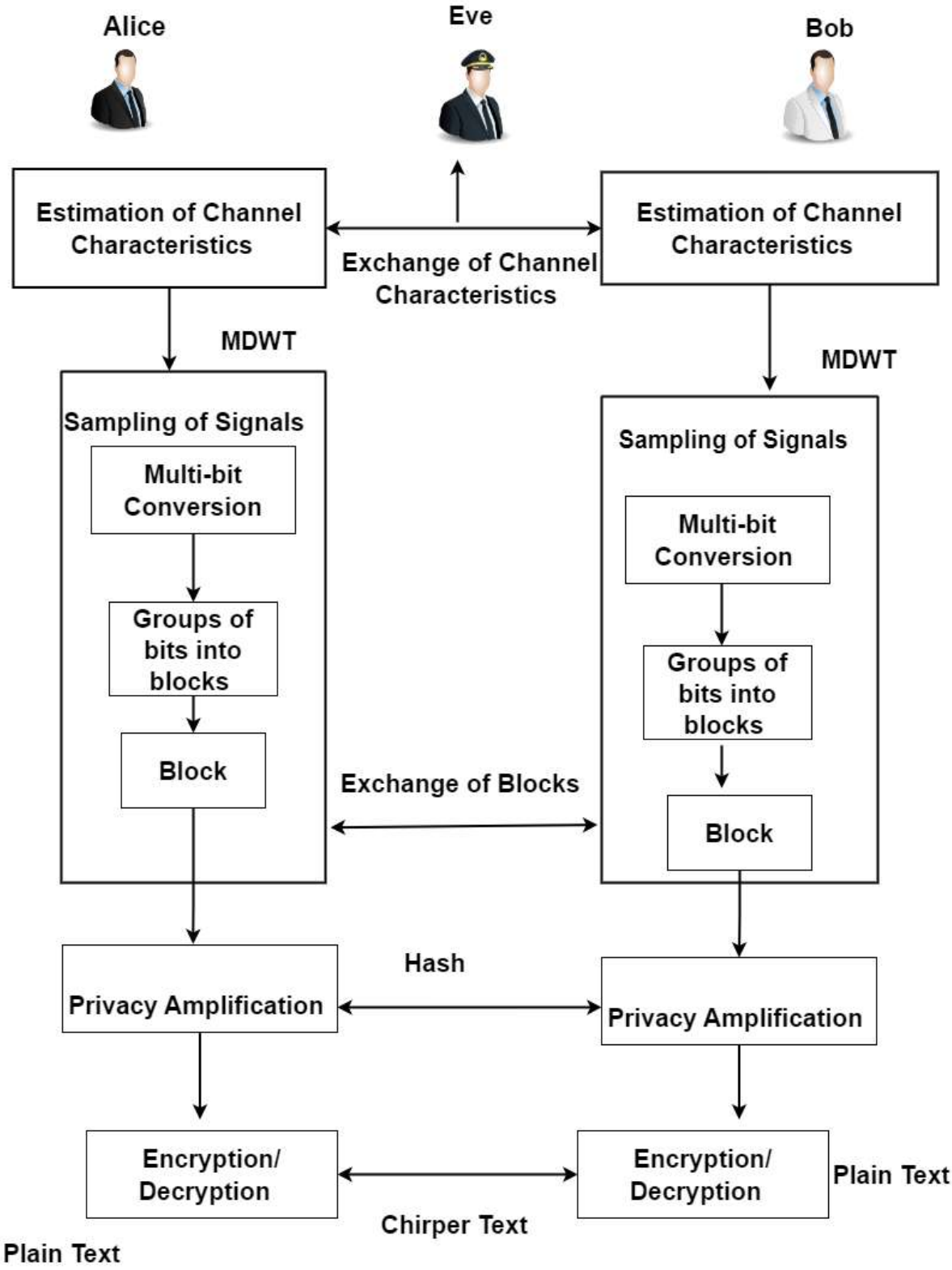

Figure 1: proposed model of physical layer key generation using MDWT

The proposed algorithm is very simple and secured instead of existing model of key generation [12,13,14,15]. The proposed model able to reduces computational cost and communication overhead for the process of communication.

The first phase of proposed model work as for measuring RSS channel parameters Yz. Between two different nodes. The subscript z replaces with Alice and Bob. And other third-party channel estimation measure as Eve.

The processing of RSS channel parameters as

$$K_A = [KA(1), KA(2), \dots\dots\dots, KA(n)]^T \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

$$K_B = [KB(1), KB(2), \dots\dots\dots, KB(n)]^T \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

$$K_E = [KE(1), KE(2), \dots\dots\dots, KE(n)]^T \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3)$$

The second phase of proposed model sampling of collected signals of RSS and formation of multi-bit the process of bit conversion expressed in equation as

$$MD=\begin{cases} Ku \le Mu - \left(\frac{\sigma u}{a}\right), 00 \\ Mu - \left(\frac{\sigma u}{a}\right) < Ku < Mu, 01 \\ Mu \le Ku < Mu + \left(\frac{\sigma u}{a}\right), 11 \\ Ku \ge Mu + \left(\frac{\sigma u}{a}\right), 10 \end{cases} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (4)$$

$$MB = MD(1), MD(2), \dots\dots\dots MD(n)T \dots\dots\dots\dots\dots\dots\dots (5)$$

Here (σ) is sampling deviation and Mu is rate of sampling of RSS signals. The multi-bit conversion process carried out in two bits and three bits such as 00 or 000.

The processing of algorithm describes here

Begin

Input:

RSS channel parameters Ku

Define sampling rate and deviation of RSS signals as (σ) and maximum channel characteristics is Mu

The number of bit conversion of each sample of RSS parameters

Bit conversion length N

Block of Bits conversion BN

Output:

The multi-bit sequence KeyU

1. Estimate the number of areas 2^U.
2. Estimate K bit in each area with code[C1, C2,……,Cn]
3. For i ← 1 to n do
4. $MB = MD(1), MD(2), \dots\dots\dots MD(n)T$
5. End for
6. For i← 1 to BN

7. KBi=o
8. For j← 1 to 3
9. KBi=Kbi_Kuji
10. End for
11. If KBi==3
12. Keyui=1
13. Elseif KBi==0
14. Keyui=0
15. Else
16. Key ui cancel
17. End if
18. End for

IV. EXPERIMENTAL ANALYSIS

To validate proposed key generation algorithm simulations in MATLAB tools. MATLAB tools provide various communication and modulation functions for the simulation of transform methods. The proposed algorithm simulates with system configuration Windows 11, RAM 8GB and HDD 1TB. For the simulation employed IEEE802.!! Models. The total number of IOTs devices is 500. The performance of the algorithm estimates as false positive detection, false negative detection, detection rate and packet delivery ratio [19,20]. The simulation parameters mentioned in table 1.

Table 1: simulation parameters of key generation algorithms

Parameters	Value
Coverage area (m x m)	2000 x 2000
MAC	IEEE 802.11
Transport	UDP
Range of communication	300 m
Bandwidth	3 Mbps
Traffic type, rate	CBR, 10 packets/sec
Model of mobility	Random way point
RX and TX ratio	90%
Number of nodes, and Packet size	500, 256 Kbps
Number of connections, and Pause time	50, 100 sec
Maximum mobility (varying)	5 m/sec - 25 m/sec
Simulation time (varying)	500-2000

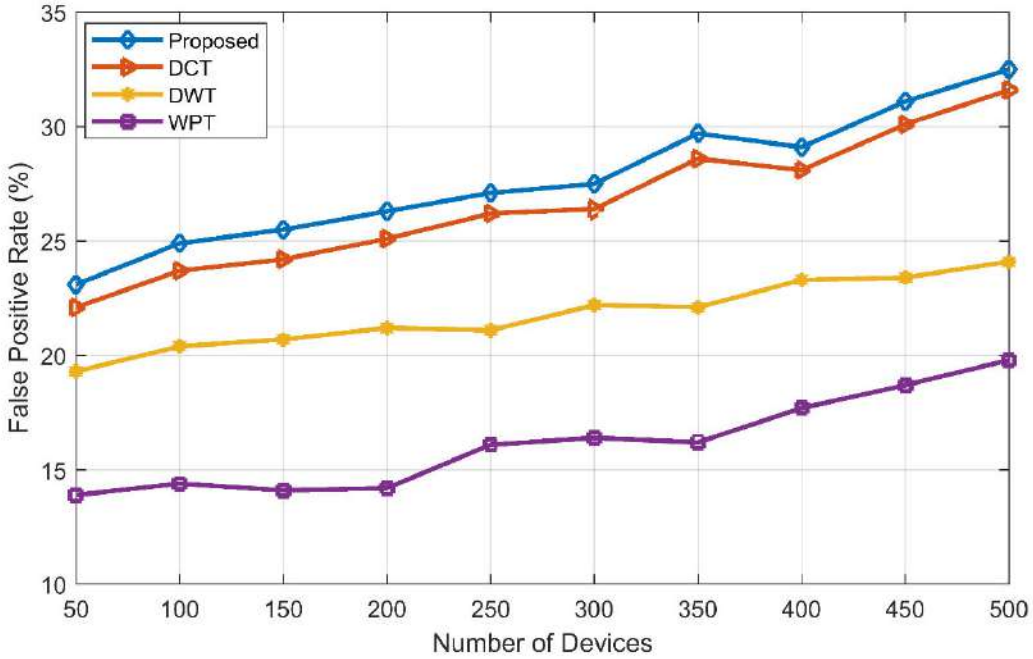

Figure 2 Performance analysis of false positive rate and number of device of key using Proposed, DCT, DWT and WPT

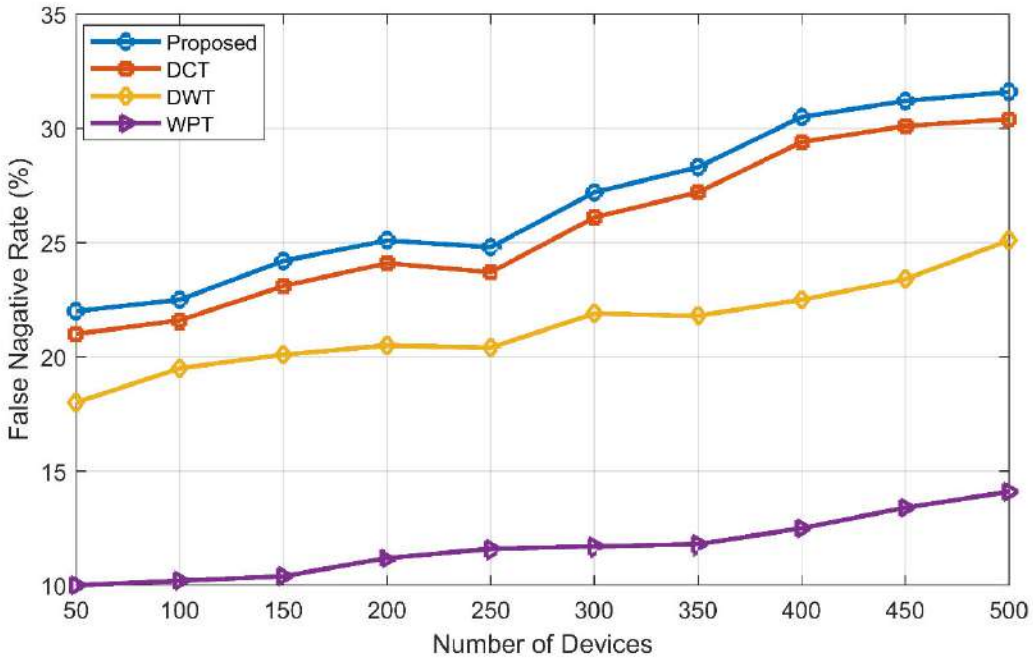

Figure 3 Performance analysis of false negative rate and number of devices of key using Proposed, DCT, DWT and WPT

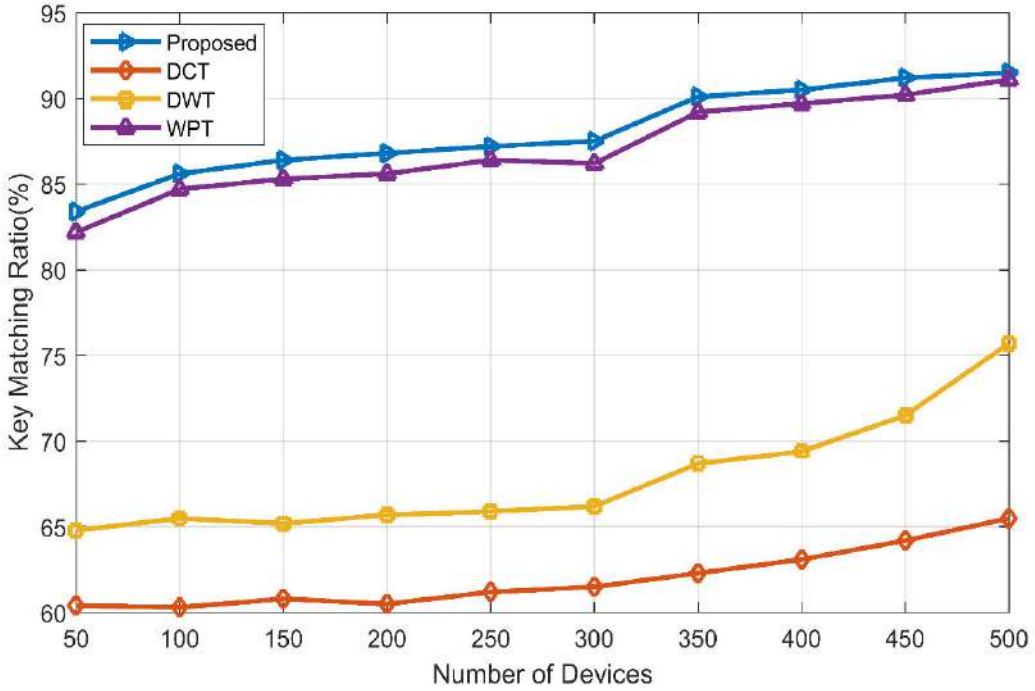

Figure 5 Performance analysis of key matching ratio and number of devices using Proposed, DCT, DWT and WPT

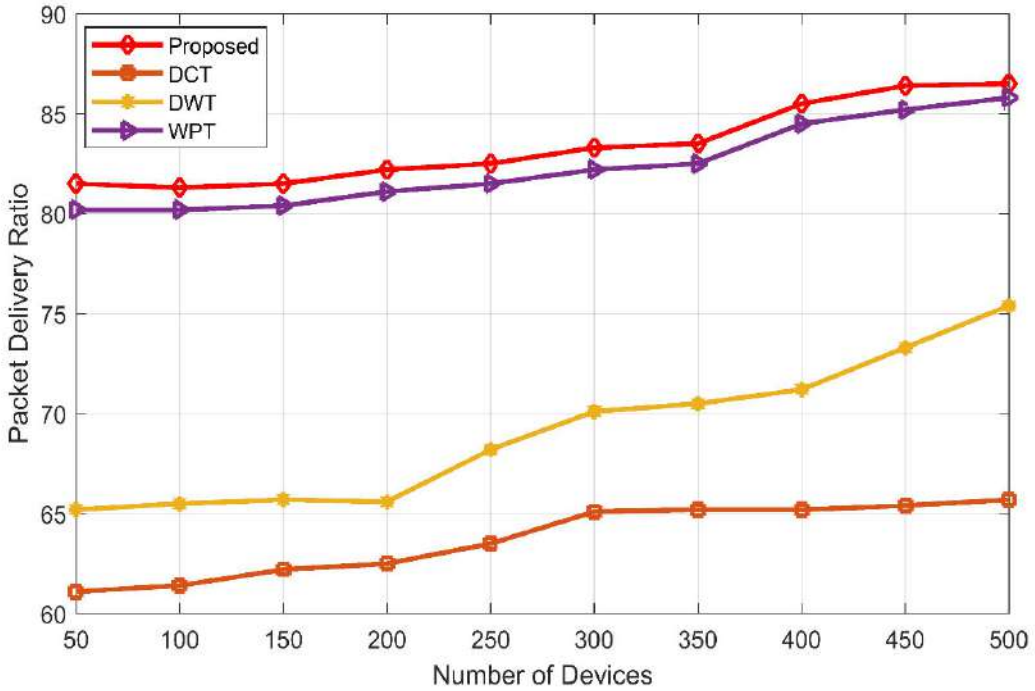

Figure 6 Performance analysis of packet delivery ratio and number of devices using Proposed, DCT, DWT and WPT

V. CONCLUSION & FUTURE WORK

This paper proposes the MDWT model for an efficient key generation approach for the internet of things. The proposed model of key generation is very efficient in terms of computational cost and communication overhead. The proposed algorithm changes the quantization process and bit conversion approach, reduces the bit mismatch rate, and improves the generation of keys. The proposed algorithm is simulated in MATLAB environments with dedicated parameters. The simulation parameters mention a dedicated area and are employed on IEEE 802.11 protocol stacks. The performance of the proposed algorithm compares with existing algorithms for key generation such as DCT, DWT, and WPT. The analysis of the results shows that the proposed algorithm reduces the bit-mismatch ratio and improves the rate of key generation. The randomness of key factors increases the security strength of keys and improves the physical layer security of IoTs. The test results demonstrated that, under both unobstructed and obstructed conditions, the sampling method could generate equal 128-bit keys without requiring the signal pre-processing and error-correcting phases. KSR values were found to reach 1.05 bps. The efficiency of the proposed model in comparison to the current system is also demonstrated by testing computing time and communication overhead in two scenarios. The results show that part A's computing time was reduced by up to 25.77 times for unobstructed scenarios and 26.08 times for obstacles, while communication and synchronization times were reduced by up to 1.55 times for unobstructed scenarios and 1.52 times for obstacles

REFERENCES

[1]. Qi, Qiao, Xiaoming Chen, Caijun Zhong, and Zhaoyang Zhang. "Physical layer security for massive access in cellular Internet of Things." Science China Information Sciences 63 (2020): 1-12.

[2]. 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.

[3]. Lee, Yonggu, Euiseok Hwang, and Jinho Choi. "Physical layer aided authentication and key agreement for the Internet of Things." In 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1-7. IEEE, 2020.

[4]. Alsadi, Ali, and Seshadri Mohan. "A new frequency hopping scheme to secure the physical layer in the Internet of things (IoT)." In 2020 Wireless Telecommunications Symposium (WTS), pp. 1-8. IEEE, 2020.

[5]. 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.

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

[7]. Makarfi, Abubakar U., Khaled M. Rabie, Omprakash Kaiwartya, Kabita Adhikari, Galymzhan Nauryzbayev, Xingwang Li, and Rupak Kharel. "Toward physical-layer security for internet of vehicles: Interference-aware modeling." IEEE Internet of Things Journal 8, no. 1 (2020): 443-457.

[8]. Alhasanat, Mohanad, Saud Althunibat, Khalid A. Darabkh, Abdullah Alhasanat, and Moath Alsafasfeh. "A physical-layer key distribution mechanism for IoT networks." Mobile Networks and Applications 25 (2020): 173-178.

[9]. Liu, Jingwei, Qin Hu, Rong Suny, Xiaojiang Du, and Mohsen Guizani. "A physical layer security scheme with compressed sensing in OFDM-based IoT systems." In ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2020.

[10]. Zarei, Meysam. "Securing Internet of Things against Physical Layer Attacks Using Hybrid Security Algorithm (HSA)." (2020).

[11]. 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.

[12]. Wei, Zhongxiang, Christos Masouros, Fan Liu, Symeon Chatzinotas, and Bjorn Ottersten. "Energy-and cost-efficient physical layer security in the era of IoT: The role of interference." IEEE Communications Magazine 58, no. 4 (2020): 81-87.

[13]. Gu, Zhifang, He Chen, Pingping Xu, Yonghui Li, and Branka Vucetic. "Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications." IEEE Transactions on Information Forensics and Security 15 (2020): 3722-3733.

[14]. Wang, Lin, Haonan An, Haojin Zhu, and Wenyuan Liu. "MobiKey: Mobility-based secret key generation in smart home." IEEE Internet of Things Journal 7, no. 8 (2020): 7590-7600.

[15]. 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.

[16]. Osorio, Diana Pamela Moya, Edgar Eduardo Benitez Olivo, Hirley Alves, and Matti Latva-Aho. "Safeguarding MTC at the physical layer: Potentials and challenges." IEEE Access 8 (2020): 101437-101447.

[17]. 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.

[18]. Li, Guyue, Zheying Zhang, Junqing Zhang, and Aiqun Hu. "Encrypting wireless communications on the fly using one-time pad and key generation." IEEE Internet of Things Journal 8, no. 1 (2020): 357-369.

[19]. Hosahalli, Doreswamy, and Kunal G. Srinivas. "Enhanced reinforcement learning assisted dynamic power management model for internet-of-things centric wireless sensor network." IET Communications 14, no. 21 (2020): 3748-3760.

[20]. Shin, Sooyeon, and Taekyoung Kwon. "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things." IEEE access 8 (2020): 67555-67571.