MACHINE INTELLIGENCE RESEARCH

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

MACHINE LEARNING BASED PHYSICAL LAYER KEY GENERATION APPROACH FOR INTERNET OF THINGS.

Ramesh Shahabade[1], Dr. Mohd Zuber[2]
Department of Computer Science and Engineering
Madhyanchal Professional University, Bhopal, India

Abstract

The communication device on the internet of things has limited resources such as bandwidth and memory. The limitation of resources cannot afford the computational cost of classical cryptography and suffers threats of information. Recently, several authors employed alternate ways of securing the internet of things using channel parameters of wireless communication. This paper proposes a channel parameter-based physical layer key generation approach. The proposed algorithm encapsulates other methods such as discrete wavelet transforms and machine learning algorithms. The employed discrete wavelet transforms methods reduce quantization errors and improve multi-bit formation. The employed clustering algorithm groups the bits in the form of blocks and 128 and 256 bits of keys. The proposed algorithm was simulated using MATLAB tools. For the evaluation of performance, estimate the ADR and length of the generated key. The estimation of ADR is based on the signal-to-noise ratio. The variation in noise changes the behaviours of the generated keys. The proposed algorithm compares with existing algorithms such as DCT, DWT, WPT, and BKQ. The performance of the results suggests that the proposed algorithm is very efficient compared to existing algorithms for physical layer key generation.

Keywords:- IoTs, PLS, Machine Learning, DCT, DWT, Wireless communication

Introduction

The inbred broadcasting characteristics of wireless communication make it vulnerable to security gaps, inviting passive or active attacks from potential eavesdroppers. The characteristics of internet-enabled communication devices are the same as those of wireless communication. Recently, several authors employed different approaches to security applications for internet-of-things-enabled communication devices. The principle of information theory employed a classical cryptography approach for the authentication of nodes. classical cryptography approaches such as RSA, DSA, and many more algorithms for key generation. The employed approach of classical cryptography faces a problem of computational cost and communication overhead. Despite the classical cryptography approach, channel parameters are an alternative way of generating keys. The channel parameter-based key generation underwent physical layer security (PLS). The channel parameters employed in physical layer security include amplitude characteristics and phase characteristics. The amplitude characteristics consist of channel impulse response (CIR), channel frequency response (CFR), and received signal strength (RSS). The conventional methods of physical layer key generation employed both channel characteristics, such as amplitude and phase. The wireless channel can be viewed as a source of entropy in addition to authentication. More specifically, secret key generation (SKG) can be performed using small-scale fading components in channel state information (CSI), for example, as a result of the random movement of entities that cause scattering. A crucial point raised in [12] and [13] regarding the robustness of SKG under unpredictability requirements [28] is the removal of predictable components from the observed CSI as a required pre-processing step prior to performing SKG. In addition, different short Slepian Wolf decoders have been compared in the short block length in [14] with regard to reconciliation. Researchers have created Physical-layer key generation (PKG), a new secure communication method from the physical layer in wire-free communication, to address these issues [4]. This method generates keys without the assistance of a third party by taking advantage of the intrinsic randomness of fading channels between two authorised users, Bob and Alice. Three distinct propagation properties of electromagnetic waves—channel reciprocity, temporal variation, and spatial decorrelation—are necessary for PKG realisation. The foundation for key generation is channel parameters, which, among other things, means that the same channel parameters can be seen at both ends of the same link. In Internet of Things systems, Alice and Bob obtain reciprocal channel responses, with the uplink and downlink occurring in the same carrier frequency band. On the other hand, in frequency division duplexing (FDD) systems, the uplink and downlink suffer different fading and transmit over separate carrier frequencies. The reported survey suggests that machine learning algorithms are employed for the physical layer key generation approach. This paper employed a clustering algorithm for the physical layer key generation process. The proposed algorithm also encapsulated transform-based functions on channel parameters. The rest of the paper explores section II related work, section III proposed methodology, section IV experimental analysis, and finally concludes section V.

II. Related work

The physical layer security approach to the internet of things has great potential to drop attacks by several eavesdroppers. Recently, several methods have been proposed based on transform methods and machine learning. Machine learning-based key generation algorithms have great potential to prevent the security of node authentication in IoT-enabled secured communication systems. Recently proposed algorithms are described here. In [1], authors propose a method of generating secret keys in PLC networks because of its strong overall performance in terms of KDR, KGR, and security with less complexity in the presence of a single or several non-collusive eavesdroppers. In [2], the authors proposed the RIS-assisted PKG method, which increases the sum secret key rate by more than 2 dB. Furthermore, draw attention to the fact that an attacker can use RISS to launch fresh jamming and leaking attacks and offer corresponding defences. In [3], DTL and meta-learning algorithms can both enhance the performance of generated keys in comparison to techniques without adaptation. Furthermore, the complexity analysis demonstrates that the meta-learning algorithm can outperform the DTL algorithm while requiring less time and CPU and GPU resources. in [4] demonstrate that the key generation rate in a static indoor setting is 15 times higher than it would be without RIS. Then, using a prototype experiment, we produce a RIS flip attack and In order to create more thoroughly secure and intelligent optical networks, they intend to offer more perceptive vision and critical evaluation on the design of new physical layer secret key schemes in optical fibre links. In [7], the subcarrier phase is the initialization of a scrambling code, and scrambling the quantized output is a processing approach that is proposed to lessen the consistency between the secret keys generated by the eavesdropper and the legal communication nodes. In [8], to encrypt data against fibre-tapping, physical layer secret keys take advantage of the random but reciprocal channel properties between valid users. They provide a unique tapping-based eavesdropper strategy that uses the signals of lawful users that have been intercepted to reconstitute their shared characteristics and the secret key. In the [10] study, security parameters have a comparable effect on how multi-path components are resolved, but they have a different effect on the MI. in [11] By utilising the physical layer and introducing security controls across all layers for the first time, physical layer security solutions became competitive contenders for low complexity, low delay, low footprint, adaptive, adaptable, and context-aware security schemes. in [12] From a PLS standpoint, it is important to emphasise the channel control idea and the sensing technologies that make some channel characteristics more accessible. PLS implementation disruptions caused by security attacks that target channel properties rather than communication itself are also covered. In [13], with a focus on IoT networks of restricted devices and wireless sensor networks, the research shows the potential of the proposed protocol as a lightweight, multi-factor substitute for the currently employed computationally costly authentication approaches. In [14], this proposed method yields a performance gain of roughly 5 dB when the BS antenna correlation is 0.3 and the RIS element spacing is half the wavelength. In comparison to the i.i.d. channel model assumption, the proposed beam-forming approach provides a higher PKG. In [17], this research suggests an architecture for C-AmBC networks in the presence of an unauthorised eavesdropper to address this issue. By using analytical derivations to invoke the outage probability (OP) and intercept probability (IP), we specifically look into the dependability and security of the proposed system. In [18], separate the small-scale fading, which should be handled as a source of shared entropy secret key generation (SKG), from the big-scale fading, which may be used as a source of uniqueness, using well-known machine learning (ML) techniques and signal processing-based methodology. In [19], two deep neural networks are used in the learning method to condense the high-dimensional state space and completely utilise the physical authentication experiences. A hierarchical structure is used to shorten exploration time. In [20], to provide a fit-to-all" security solution for IoTs, the proposed model was created in such a way that it may be appropriate for both data-level security and device-level access credential security. in a [21] physical-layer-defined system that makes use of the sensors' signal processing capabilities without the need for any additional hardware, in light of the potential dangers. According to our test using commercial sensors, Sound Fence picks up the majority (more than 95%) of the anomalous sensor readings. In [22], the key generation mechanism is most suited for situations where IoT devices can't rely on ongoing key negotiation with dedicated servers and where devices can't reuse old keys for encryption. In [23], the performance gain of the proposed technique can be 100 times greater than that of the present approaches. The proposed technique can accomplish a secure key distribution with a greater key rate and key entropy compared to the existing schemes, according to experimental data. In [24], this study examines the effectiveness of three PKC protocols, Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Diffie-Hellman (ECDH), which are frequently used for session key establishment and exchange. The author [25] In order to explore the security of the physical layer in the UAV communication system, this article summarises the most recent research findings on safety communication involving UAVs on the physical layer. in [26] proposed an approach to achieve efficiency and robustness. Other advantages of the approach include low computing costs, preservation of the device's privacy, protection from serious security risks, low communication, and minimal storage overhead. In

[27], even in the case of memory leaks, the proposed protocol ensures security and privacy against passive and aggressive attacks. The entities reconstruct a secret polynomial-share using their PUF in order to create temporal secret keys (PTKs) with other entities. In [28], the different potential future implementations of these are also discussed, along with an analysis of all the typical concerns with IoT-assisted wearable sensor systems and the specific problems that must be solved to optimise them for use in healthcare. in [29] the superior randomness, key generation ratio, and key error rate performance of the KGNet-based key generation system. Additionally, the overhead analysis demonstrates that the strategy put forth in this study can be applied to IoT devices with limited resources in FDD systems.

III. Proposed Methodology

This section describes the proposed methodology for the physical layer key generation approach based on channel parameters. The characteristics of channel parameters use amplitude, such as received signal strength (RSS). The modulation and sampling of signals employed discrete wavelet transform (DWT) methods. The DWT (2) methods reduce the quantization error of multi-bit conversion. After the process of sampling, a machine learning algorithm was employed. The employed machine learning algorithms group bits into blocks and form a 128-bit key for physical communication. the processing of the proposed algorithm presented in Figure 2. The first phase of the block diagram estimates the RSS signals. After the estimation of signals, we employed the DWT (2) method for the sampling of signals. After the sampling of signals, we employed clustering algorithms. The clustering algorithms form groups of bits and blocks. The processing of the algorithm is described here.

Sampling

The RSS signals passes through the DWT(2) for sampling of signals process as the maximum frequency of the signal is fs/2. If the signal is decomposed by lower order, the complete frequency signal decomposed into L+1 sub band. The wavelet decomposition layer shown in figure

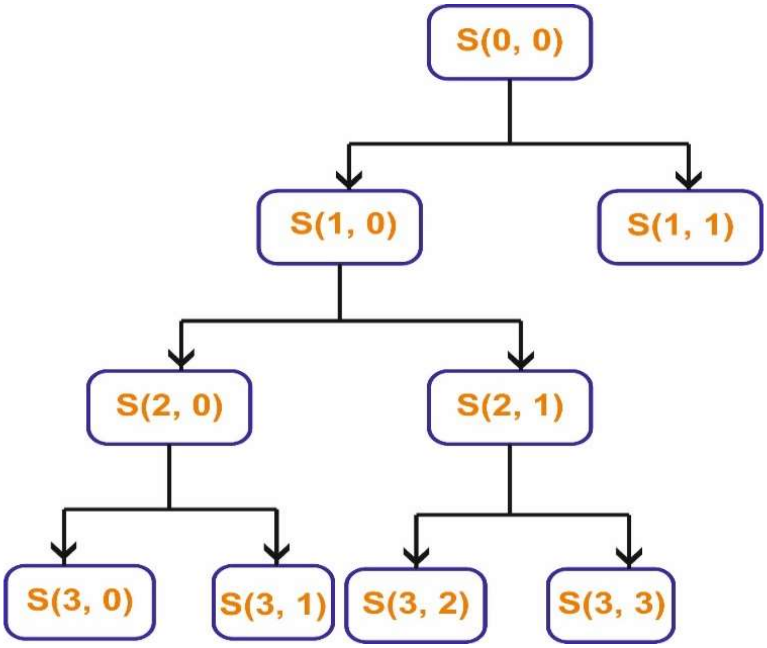

Figure 1: decomposition level of wavelet transform function.

Conder $f(x) \in L^2(R)$ relative to wavelet function $\psi(x) and\ scaling\ function\ \phi(x)$
The DWT defined as

$$W_\phi(j0,k) = \frac{1}{\sqrt{M}} \sum_x f(x)\phi_{j0,k}(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$W_\psi(J,K) = \frac{2}{\sqrt{M}} \sum\nolimits_X f(x)\psi_{j,k}(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Now

$$f(x) = \frac{1}{M}\sum\nolimits_K W_\phi(j0,k)\phi_{j0,k}(x) + \frac{1}{\sqrt{M}}\sum_{J=J0}^{J-1}\sum\nolimits_K W_{\psi(J,K)}\,\psi_{J,K}(X) \ldots\ldots\ldots (3)$$

In the value of M measure, the power of 2. The component of transform estimate M number of coefficients the maximum scale j-1 and minimum coefficient is 0, and detail coefficient define in equation 2.
The proceed signal decompose by dB4 the band of frequency $[f_m/2 \colon f_m]$ of each detail scale of DWT the sampling rate given by $f_m = \frac{f_s}{2l} + 1$ where, fs sampling frequency and l level of decomposition.

Clustering

The process of K-means clustering deals with generation of centre points with merging of intermediate cluster. The maximum iteration of clustering process declines the performance of K-means algorithm [5].

Consider we want to categorise the data into different K groups. The objective of algorithms is minimizing the value of fitness function as squared error describe as

$$Fs = \sum_{j=1}^{k}\sum_{j=1}^{n}\|xi - cj\|^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Here Xi is ith point of data samples Cj is the cluster centres
The process of clustering algorithm follows following steps

1. Define the value of K and represents the data points for the initial groups of centres select randomly.
2. Measure the distance with centre point and assign object in these groups
3. Redefine the centres of intermediate clusters
4. Merger intermediate cluster
5. Repeat step 2 and 3 until meet the condition. And validate the cluster

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: {1 . . . M} → {0, 1} m of the type

$$g(a,b) = (ax+b)mod\ Pm.\ldots\ldots\ldots\ldots\ldots\ldots.(5)$$
$$hab(x) = gab(x)mod\ m.\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

For each a ∈ {1 . . . p M−1} and b ∈ {0 . . . p M−1}, p M 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 encryption process, and the information leaked during information reconciliation.

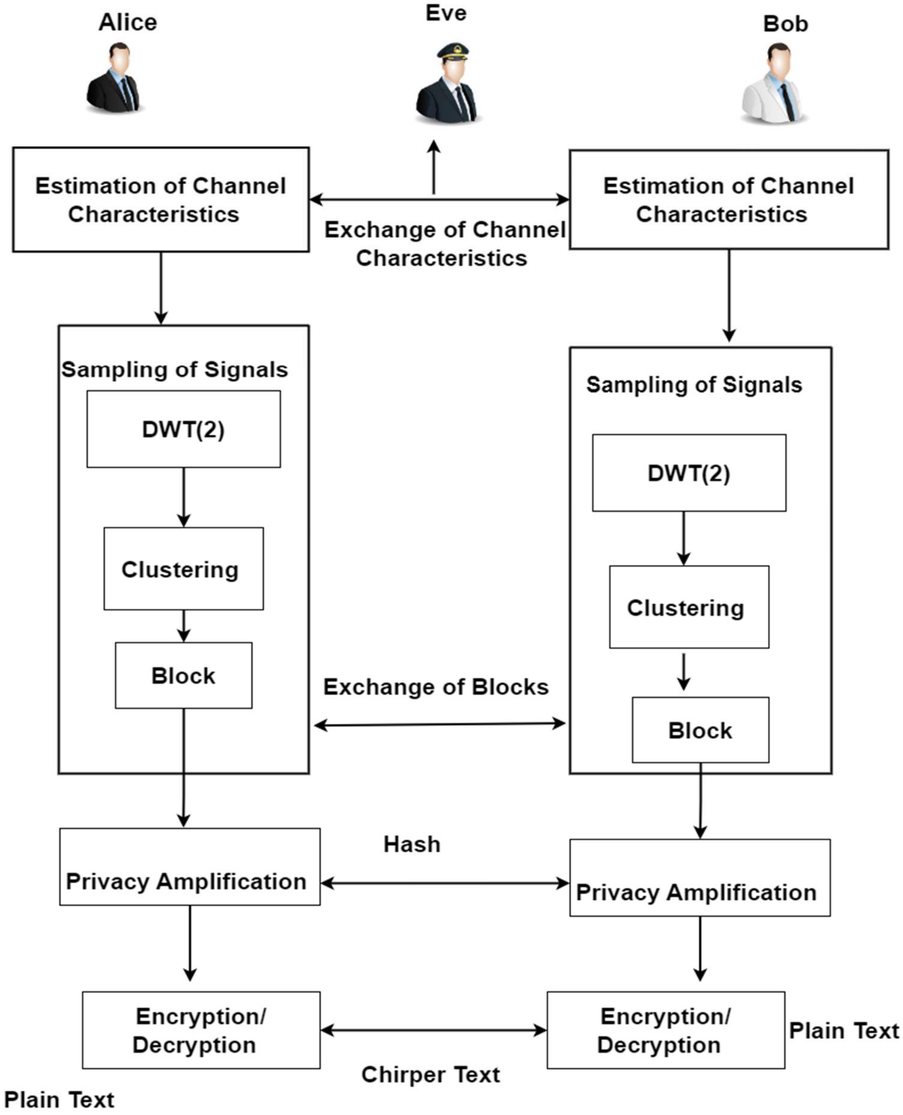

Figure 2 Proposed Model of Physical Layer Key Generation Using Machine Learning

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 17 No. 02 (2023)

IV. Simulation & Results 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 868MHz. These parameters measure the performance of modified key generation algorithms [6]. The simulation process is carried out under three scenarios: indoor and outdoor. The proposed key generation algorithm compares with existing transform methods DWT, WPT, BKQ and DCT. The simulation parameters mention on table-1.

Table1: 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
Clustering	K-means
Sequence length	1000,2000,3000

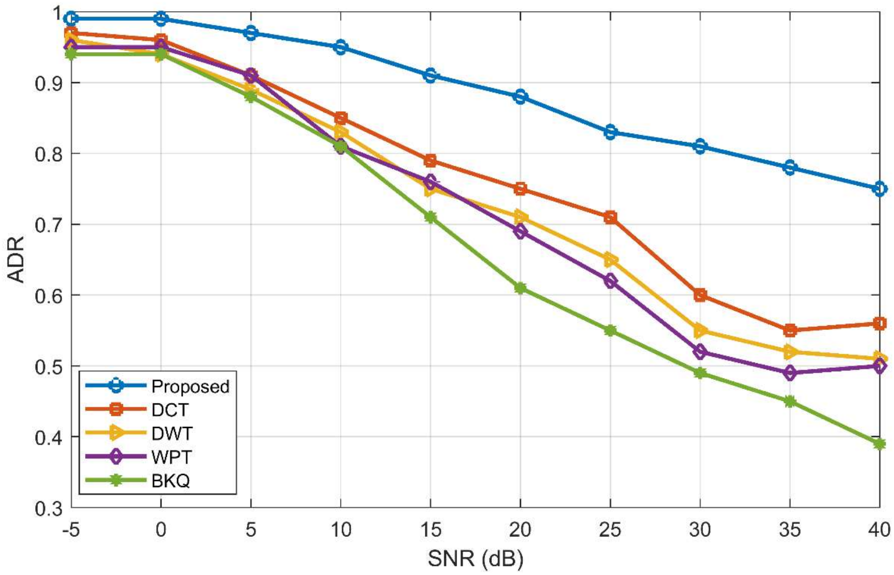

Figure 3 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, BKQ, and WPT.

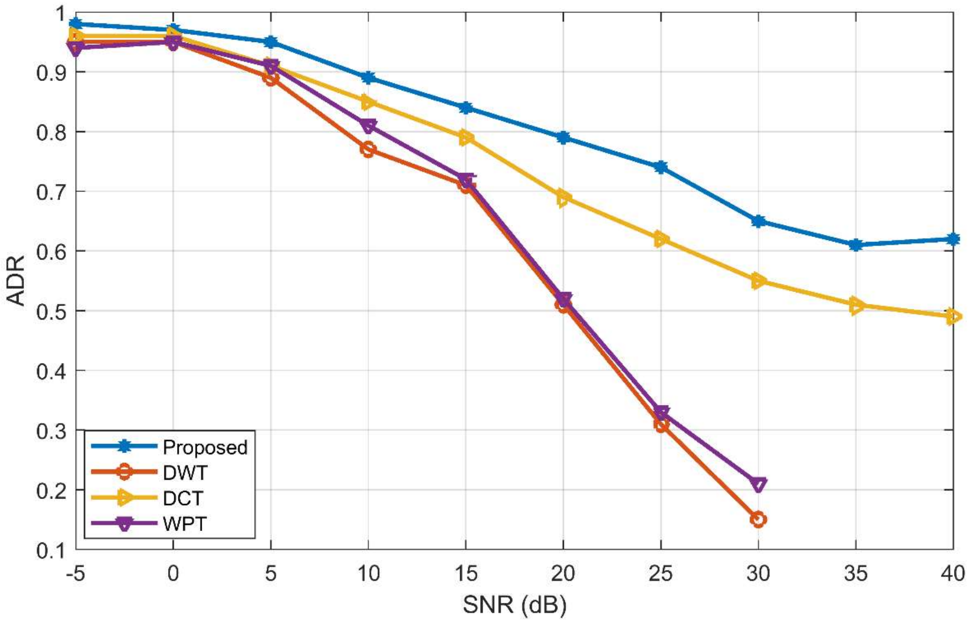

Figure 4 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, and WPT.

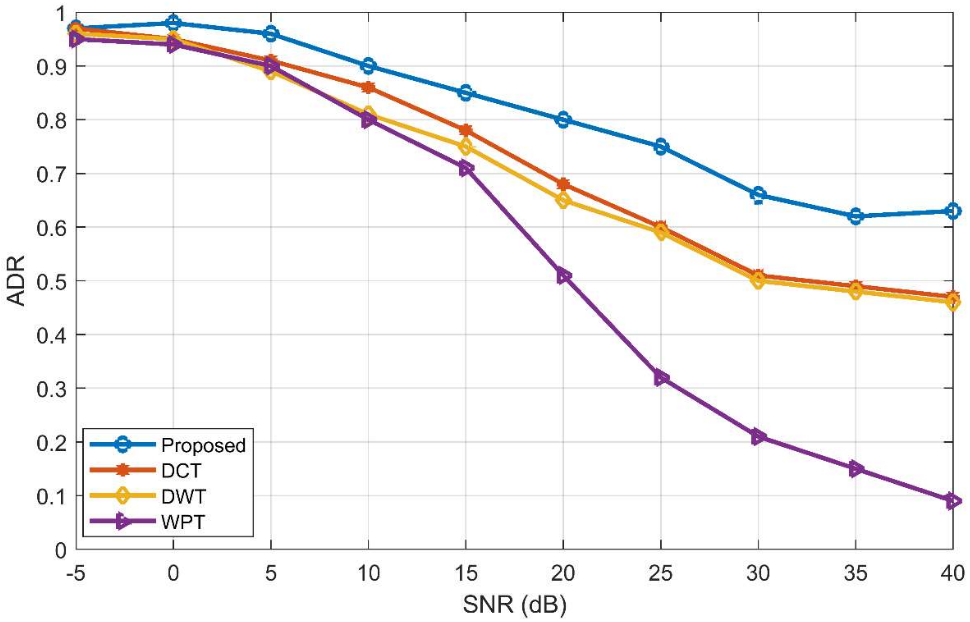

Figure 5 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, and WPT.

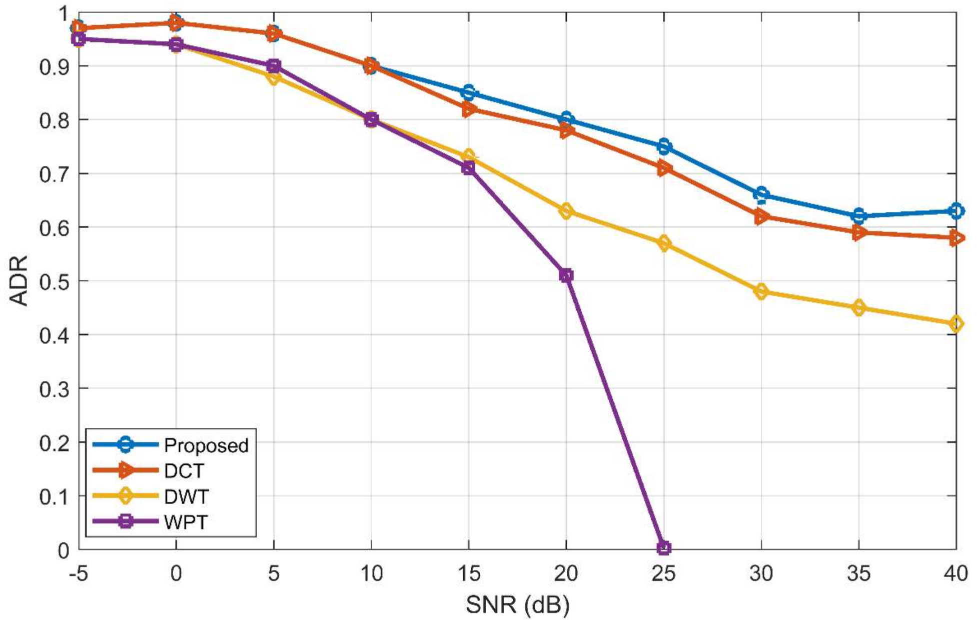

Figure 6 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, and WPT.

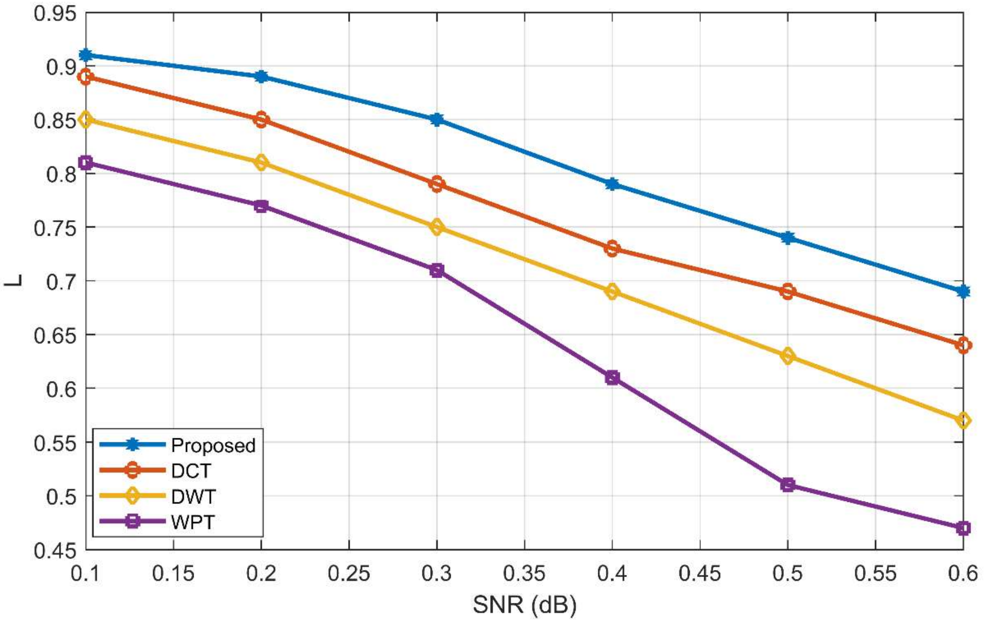

Figure 7 performance analysis of L and SNR (dB) using Proposed, DCT, DWT, and WPT.

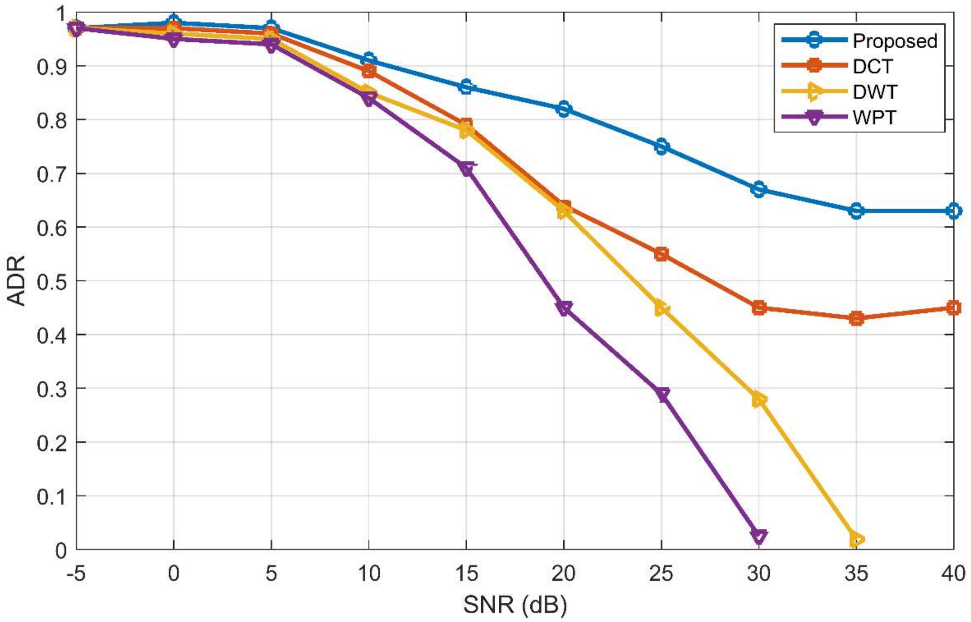

Figure 8 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, and WPT.

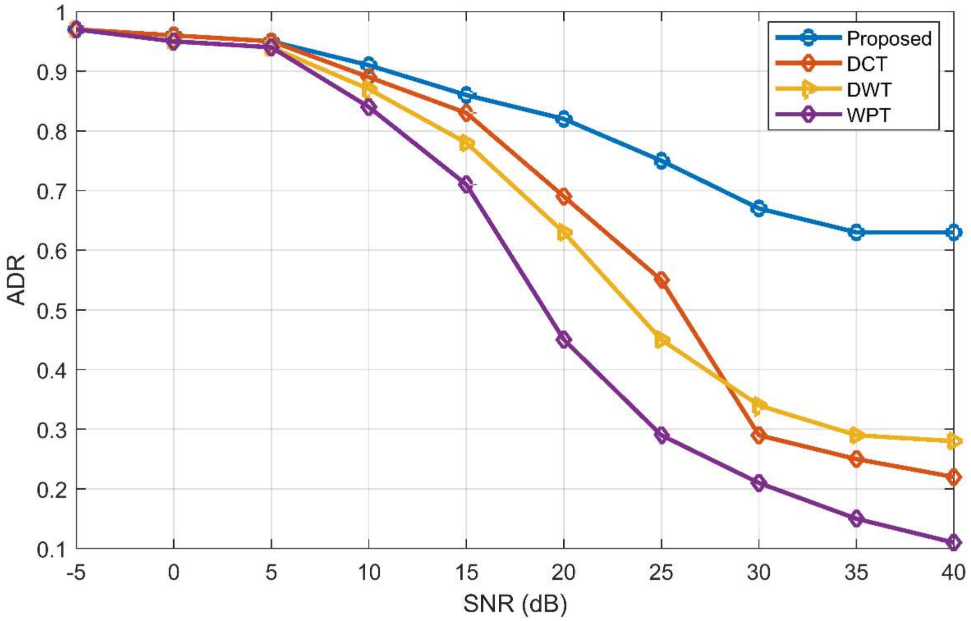

Figure 9 performance analysis of ADR and SNR (dB) using Proposed, DCT, DWT, and WPT.

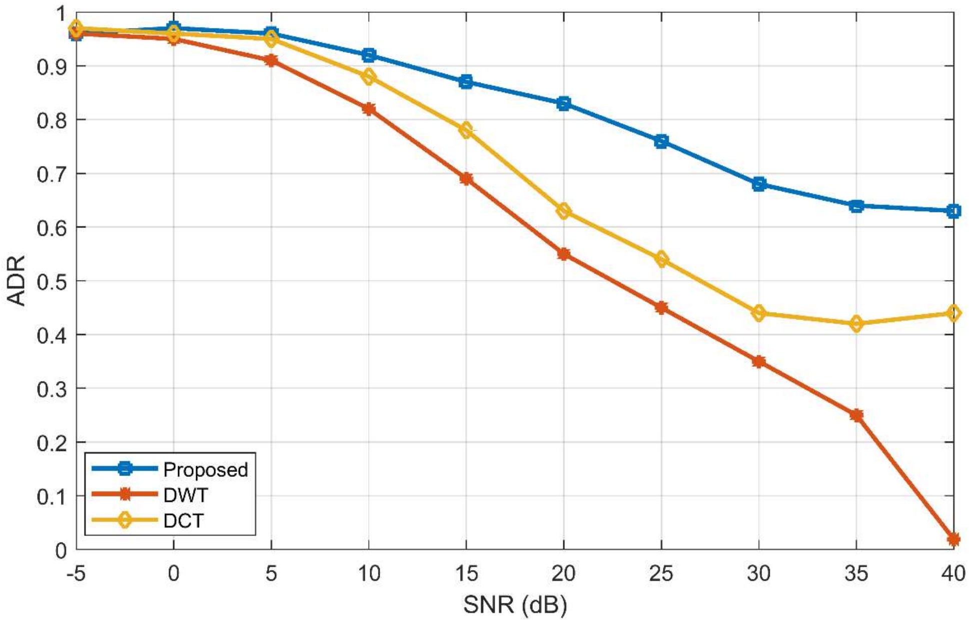

Figure 10 performance analysis of ADR and SNR (dB) using Proposed, DCT, and DWT.

V. Conclusion & Future Work

This paper proposes machine learning-based physical layer key generation for authentication in IoT-enabled communication systems. The proposed algorithm is very simple and efficient in terms of computational cost and communication overhead. The processing of the proposed algorithm encapsulates discrete wavelet transform (DWT) for sampling and quantization processes. The employed DWT methods reduce the rate of quantization and improve the blocking of bits. The process of block generation employed a clustering algorithm. The employed clustering algorithm improves the grouping of bits in the form of 128 bits and 256 bits. We enhanced the original protocol by sacrificing some needless error correction capabilities in exchange for reduced implementation complexity and increased efficiency because of the suggested quantization scheme's high level of reliability. The outcomes demonstrate that our strategy can produce keys that are both dependable and efficient while requiring less work to implement. There have also been suggestions made regarding the remaining difficulties in making these schemes more widespread and resilient. In contrast to earlier research, this paper has concentrated on real-world prototypes and implementations, providing insights for their potential applications in the Internet of Things to improve wireless security.

References

[1]. Zhang, Jiarui, Xiaosheng Liu, Ying Cui, and Dianguo Xu. "Physical-Layer Secret Key Generation in Power Line Communication Networks." *IEEE Access* 10 (2022): 48539-48550.

[2]. Li, Guyue, Lei Hu, Paul Staat, Harald Elders-Boll, Christian Zenger, Christof Paar, and Aiqun Hu. "Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive?." *IEEE Wireless Communications* 29, no. 4 (2022): 146-153.

[3]. Zhang, Xinwei, Guyue Li, Junqing Zhang, Aiqun Hu, and Xianbin Wang. "Enabling Deep Learning-based Physical-layer Secret Key Generation for FDD-OFDM Systems in Multi-Environments." *arXiv preprint arXiv:2211.03065* (2022).

[4]. Gao, Ning, Yu Han, Nannan Li, Shi Jin, and Michail Matthaiou. "When Physical Layer Key Generation Meets RIS: Opportunities, Challenges, and Road Ahead." *arXiv preprint arXiv:2210.02337* (2022).

[5]. Mitev, Miroslav, Thuy M. Pham, Arsenia Chorti, André Noll Barreto, and Gerhard Fettweis. "Physical Layer Security--from Theory to Practice." *arXiv preprint arXiv:2210.13261* (2022).

[6]. Hu, Wenxiu, Zhuangkun Wei, Sergei Popov, Mark Leeson, and Tianhua Xu. "Tapping Eavesdropper Designs against Physical Layer Secret Key in Point-to-Point Fiber Communications." *Journal of Lightwave Technology* (2022).

[7]. Wang, Dan, Feng Chen, Yongtai Chen, Mingjie Zheng, and Jingui Zheng. "Scramble-Based Secret Key Generation Algorithm in Physical Layer Security." *Mobile Information Systems* 2022 (2022).

[8]. Hu, Wenxiu, Zhuangkun Wei, Mark Leeson, and Tianhua Xu. "Eavesdropping Against Bidirectional Physical Layer Secret Key Generation in Fiber Communications." In *2022 IEEE Photonics Conference (IPC)*, pp. 1-2. IEEE, 2022.

[9]. Li, Guyue, Haiyu Yang, Junqing Zhang, Hongbo Liu, and Aiqun Hu. "Fast and secure key generation with channel obfuscation in slowly varying environments." In *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*, pp. 1-10. IEEE, 2022.

[10]. Mitev, Miroslav, André Noll Barreto, Thuy M. Pham, and Gerhard Fettweis. "Secret key generation rates over frequency selective channels." In *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*, pp. 1-5. IEEE, 2022.

[11]. Chorti, Arsenia, André Noll Barreto, Stefan Köpsell, Marco Zoli, Marwa Chafii, Philippe Sehier, Gerhard Fettweis, and H. Vincent Poor. "Context-aware security for 6G wireless: The role of physical layer security." *IEEE Communications Standards Magazine* 6, no. 1 (2022): 102-108.

[12]. Kihero, Abuu, Haji Furqan, M. M. Sahin, and Huseyin Arslan. "Revisiting the Wireless Channel from Physical Layer Security Perspective." *arXiv preprint arXiv:2206.00936* (2022).

[13]. Mitev, Miroslav, Mahdi Shakiba-Herfeh, Arsenia Chorti, Martin Reed, and Sajjad Baghaee. "A physical layer, zero-round-trip-time, multifactor authentication protocol." *IEEE Access* 10 (2022): 74555-74571.

[14]. Hu, Lei, Guyue Li, Xuewen Qian, Derrick Wing Kwan Ng, and Aiqun Hu. "Joint Transmit and Reflective Beamforming for RIS-assisted Secret Key Generation." In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 2352-2357. IEEE, 2022.

[15]. Ruotsalainen, Henri, Guanxiong Shen, Junqing Zhang, and Radek Fujdiak. "LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review." *Sensors* 22, no. 9 (2022): 3127.

[16]. Lavanya, D. L., R. Ramaprabha, B. Thangapandian, and K. Gunaseelan. "Novel privacy preserving authentication scheme based on physical layer signatures for mobile payments." *SN Computer Science* 2 (2021): 1-11.

[17]. Li, Xingwang, Yike Zheng, Wali Ullah Khan, Ming Zeng, Dong Li, G. K. Ragesh, and Lihua Li. "Physical layer security of cognitive ambient backscatter communications

for green Internet-of-Things." *IEEE Transactions on Green Communications and Networking* 5, no. 3 (2021): 1066-1076.

[18]. Srinivasan, Muralikrishnan, Sotiris Skaperas, and Arsenia Chorti. "On the Use of CSI for the Generation of RF Fingerprints and Secret Keys." In *WSA 2021; 25th International ITG Workshop on Smart Antennas*, pp. 1-5. VDE, 2021.

[19]. Xiao, Liang, Xiaozhen Lu, Tangwei Xu, Weihua Zhuang, and Huaiyu Dai. "Reinforcement learning-based physical-layer authentication for controller area networks." *IEEE Transactions on Information Forensics and Security* 16 (2021): 2535-2547.

[20]. Krishna, Priya Gurumanapalli, and Nagendra Muthuluru. "Feistel Network Assisted Dynamic Keying based SPN Lightweight Encryption for IoT Security." *International Journal of Advanced Computer Science and Applications* 12, no. 6 (2021).

[21]. Lou, Jianzhi, Qiben Yan, Qing Hui, and Huacheng Zeng. "SoundFence: Securing ultrasonic sensors in vehicles using physical-layer defense." In *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1-9. IEEE, 2021.

[22]. Pothumarti, Raghu, Kurunandan Jain, and Prabhakar Krishnan. "A lightweight authentication scheme for 5G mobile communications: a dynamic key approach." *Journal of Ambient Intelligence and Humanized Computing* (2021): 1-19.

[23]. Lou, Chunwei, Mingsheng Cao, Rongchun Wu, Dajiang Chen, and Hua Xu. "A lightweight key generation scheme for secure device-to-device (D2D) communication." *Wireless Communications and Mobile Computing* 2021 (2021): 1-17.

[24]. Butt, Amir Aziz, Gohar Rehman Chughta, Asif Kabir, Zahid Mahood, and Judit Oláh. "Analysis of Key Establishment Techniques for Secure D2D Communication in Emerging 5G Cellular Networks." (2021).

[25]. Li, Jiawei, Ruixia Cheng, Junwen Zhu, Yu Tian, and Yiwen Zhang. "Wireless secure communication involving UAV: an overview of physical layer security." In *MATEC Web of Conferences*, vol. 336, p. 04005. EDP Sciences, 2021.

[26]. Masud, Mehedi, Mamoun Alazab, Karanjeet Choudhary, and Gurjot Singh Gaba. "3P-SAKE: privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks." *Computer Communications* 175 (2021): 82-90.

[27]. Othman, Wajdy, Miao Fuyou, Kaiping Xue, and Ammar Hawbani. "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city." *IEEE Transactions on Vehicular Technology* 70, no. 12 (2021): 12902-12917.

[28]. Mamdiwar, Shwetank Dattatraya, Zainab Shakruwala, Utkarsh Chadha, Kathiravan Srinivasan, and Chuan-Yu Chang. "Recent advances on IoT-assisted wearable sensor systems for healthcare monitoring." *Biosensors* 11, no. 10 (2021): 372.

[29]. Zhang, Xinwei, Guyue Li, Junqing Zhang, Aiqun Hu, Zongyue Hou, and Bin Xiao. "Deep-learning-based physical-layer secret key generation for FDD systems." *IEEE Internet of Things Journal* 9, no. 8 (2021): 6081-6094.

[30]. Ebrahimi, Najme, Hun-Seok Kim, and David Blaauw. "Physical layer secret key generation using joint interference and phase shift keying modulation." *IEEE Transactions on Microwave Theory and Techniques* 69, no. 5 (2021): 2673-2685.