MACHINE INTELLIGENCE RESEARCH
ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

ENHANCED BIT DISAGREEMENT FOR THE INTERNET OF THINGS USING PHYSICAL LAYER KEY GENERATION BASED ON MODIFIED WINDOWS

Reeta Singh[1], Susheel Kumar Tiwari[2]
[1]Department of Computer Science & Engg., Madhyanchal Professional University, Bhopal, India.
[2]Department of Computer Science & Engg., Madhyanchal Professional University, Bhopal, India.

Abstract
The Internet of Things (IoT) is a paradigm where myriad devices in households, vehicles, and industrial settings interconnect. The proliferation of interconnected devices poses security challenges, making IoT networks susceptible to eavesdropping and replay attacks. To address this issue, a lightweight key generation scheme is proposed in this article, focusing on enhancing quantization and information reconciliation. The proposed approach employs a modified window along with discrete wavelet transform (DWT) for key generation. To validate the effectiveness of the proposed approach, simulations are conducted for varying numbers of device nodes in both indoor and outdoor scenarios. The evaluation of results suggests that the proposed algorithm surpasses existing key generation algorithms in terms of performance and reliability. Furthermore, comparative analyses demonstrate the superior performance of our method compared to other relevant schemes.
Keywords- IoT, PLS, Key Generation, DWT, MW

Introduction

The evolution of network and telecommunications technology has given rise to the Internet of Things (IoT), a paradigm where myriad devices in households, vehicles, and industrial settings interconnect[1,2]. This interconnected web of devices, equipped with diverse sensors and linked through various networks, enables autonomous data exchange, minimizing the need for human intervention. The IoT infrastructure relies on a communication network facilitating seamless information collection and exchange among devices[3,4,5]. However, the wireless nature of data aggregation poses security challenges, making IoT networks susceptible to eavesdropping. In addressing IoT security, traditional methods often implement cryptography at higher layers, yet maintaining a balance between high security and low computational costs remains challenging. Physical-layer security (PLS) emerges as a promising solution, overcoming limitations of conventional security policies. Despite its potential, practical application hurdles persist, such as insufficient key generation rates, especially in cases like physical layer key extraction[6,7,8]. The Open Communication Model in IoT promotes interoperability, standardization, and openness in communication protocols, fostering a common foundation for diverse devices and systems. Meanwhile, the physical layer key generation approach offers an alternative solution rooted in information theory security, providing supplementary security to the wireless mechanisms at the physical layer. Physical layer key generation leverages principles like channel reciprocity, temporal variation, and spatial decorrelation. Channel reciprocity ensures identical channel

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

measurements between uplink and downlink signals, while temporal variation results from changes in channel paths over time due to relative movement. Spatial decorrelation guarantees that the observation of a legitimate channel is challenging for an eavesdropper located far from the legitimate nodes[9,10,11]. Despite the promise of physical layer key generation, challenges persist, including the need for further research to enhance IoT security. Issues such as the generation rate of extracted keys and the impact of artificial noise on communication resources necessitate ongoing exploration to refine and optimize this approach for practical IoT applications. Despite the high correlation in channel measurements between two legitimate nodes, variations still exist due to asymmetric factors like environmental noise, hardware characteristics, and non-simultaneous measurements. These discrepancies pose a challenge in generating shared keys. To address this issue, a lightweight key generation scheme tailored for IoT is proposed in this article, focusing on enhancing quantization and information reconciliation. In the proposed scheme, secret keys are extracted from amplitude information obtained from channel estimates by the legitimate nodes [12]. A novel quantization scheme, coupled with preprocessing techniques, significantly improves key agreement between the nodes. This enhancement allows for proper relaxation of the error correction capacity within the information reconciliation protocol [13]. Furthermore, modifications are made to the Cascade protocol to strike a balance between error correction capacity and implementation complexity. By optimizing this trade-off, the protocol becomes more efficient in reconciling information discrepancies between the legitimate nodes, thereby improving the overall robustness and reliability of the key generation process for IoT devices. This paper proposes a modified window selection approach using the transform function. The modified Windows process improves the agreement of keys for authentication of nodes [14]. The employed transform methods sampled the channel property and reduced the process of quantization. The rest of the paper is organised as follows: in Section II, related work on key generation in the internet of things; in Section III, methodology of key generation; in Section IV, experimental results of the proposed algorithm; and in Section V, conclusion and future scope.

II. Related Work

Certainly! Security in IoT-enabled communication systems is indeed a significant concern, given the proliferation of interconnected devices and the potential vulnerabilities they may introduce. To address this concern, several authors have proposed physical layer key generation approaches, leveraging the inherent properties of communication channels to enhance security. Physical layer security offers a robust means of securing information in communication systems by exploiting the characteristics of the physical transmission medium. explore some of the recently developed algorithms for key generation in IoT: A filter bank-based technique is used in [1] by the author of this paper to enable the production of secret security keys from a wideband radio channel, independent of the baseband modem implementation. The use of SKG techniques helps understand their hidden bit rate in various channel circumstances. In [2], even without knowing the channel state of an eavesdropper, the author's suggested secure beam forming and artificial noise (AN) techniques can increase the erotic secrecy rates of uplink and downlink channels (CSI). In order to reduce computation, we introduced SCOS, in which an ICV might flood some

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

calculation duties to a MEC server. The author [3] On a CAN bus prototype and an actual car, the proposed technique has an accuracy rate of 99.67% and 97.04%, respectively. Additionally, the proposed approach may attain a mean accuracy of above 99% in a temperature-drifting environment. To successfully get beyond the aforementioned shortcomings of the earlier systems [4], the author and I offer two multiple-channel impulse response (CIR)-based PLA schemes. To successfully solve the aforementioned shortcomings of the earlier methods, we provide two multiple-channel impulse response (CIR)-based PLA techniques. The goal of [5] is to present a thorough roadmap on significant concerns that have been raised by the authors and other contributors and to debate unresolved questions regarding the application of PLS in sixth-generation systems. To improve the accuracy of PHY-layer authentication, the author of [6] proposes a non-parametric clustering technique based on unsupervised machine learning (ML). The suggested authentication method may deliver solid performance with little complexity. The simulation findings show that the F1 measure can achieve more than 99% without the attackers' previous knowledge. We ran two sets of experiments, one using computer-simulated channel data and the other using real experiment data produced by our wireless test, in order to evaluate the performance of the suggested strategy [7].. In addition to TP-Net, we also look at GC-Net and VGG, two traditional CNN architectures. Additionally, the threshold-based approach is used as well. The JRP technique was suggested in [8] over the pertinent benchmarks located in the literature. Intriguingly, for both the NCE and CE scenarios, the ESR rises with the density of untrusted relays, which is a benefit of the increased likelihood of choosing a relay with a stronger second-hop channel. We suggest Sound Fence, a physical-layer defined system [9], in the author, which makes use of the sensors' signal processing capabilities without the need for any additional hardware. In addition, we put up the idea of Sound Fence, a physical-layer-defined system that operates on widely available ultrasonic sensors and blocks erroneous signals or sensor readings. A variety of key generation techniques and systems have been developed in recent years, according to the authors [10]. In this study, we examine and classify current key generation systems using a brand-new taxonomy. Key generation systems have been proposed and developed in a sizable number. We have studied, analysed, and contrasted recent solutions in this study. The author [11] We also discuss the benefits and drawbacks of various protocol standards for a range of IoT application scenarios, such as linked cars, smart homes, health, and consumer electronics. The author [12] then, in order to obtain a lightweight and effective information reconciliation, provides an updated Cascade methodology. The suggested scheme's keys also pass the NIST randomness tests with flying colours. The author [13] recommends using this simplified post-quantum technique to improve the security of IoT devices. This survey's primary goals were to give the scientific community in-depth knowledge on fundamental mathematical concepts, as well as to address real-time implementation, hardware architecture, unsolved issues, attack vectors, and the importance of Internet of Things (IoT) networks. The author [14] With a reduction in the search space of 87.2% and an accuracy of 97.4%, the ML methodology enables us to predict these attacks well. We use the hacking of a connected car's in-vehicle network to show how our method can be used. The author [15] states that following that, data fusion is performed in accordance with the Minimal Mean Square Error (MMSE) criterion. The simulation results show that the suggested approach for resolving contradictory IoT data is remarkably effective and efficient. The author's [16] paper seeks to provide an overview of the Internet of

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

Things and its applications. The most recent trends, state of affairs, new discoveries, security, privacy, IoT applications, and future research areas are all presented. The author [17] Compared to the two ACO approaches and the GA and CAT optimisation algorithm combo, this strategy increased fitness between various scenarios. Further research could be used to improve the proposed strategy in a number of ways. According to the author [18], this marks the first instance of deep learning being used for PKG in FDD systems. It is confirmed that the suggested KGNet-based FDD system key generation strategy may be used for key generation for FDD systems by evaluating it using the KER, KGR, and randomness. The author [19] According to the suggested architecture, an IoT node creates a phase-modulated random key or data and sends it to a master node while being watched by an observer known as Eve. The author [20] For the proposed NOMA-based MIMO with PNC, taking into consideration huge IoT scenarios, performance assessments based on both sum data rate and bit error rate are provided. Based on the BER performances of IoT devices, a scheme for the proposed user-set selection was put on display. According to the author [21], at the beginning, MATLAB was used to research and simulate both systems. It was also investigated how many encryption keys would actually be needed with such hyper-chaotic maps. The author [22] examined the effects of a malicious third device's proximity attack and discovered that it is capable of listening in on significant portions of the generated key, jeopardising overall security. According to the author [23], with a short-term session key generation procedure, the suggested approach also tackles the issue of access control for new IoT devices. The effectiveness of the suggested approach against eavesdropping and replay attacks is demonstrated through security analysis. The author [24] To overcome the drawbacks of current PLS methods, this study suggests LoRA-LiSK, a practical and effective shared secret key generation scheme for LoRa networks. Moreover, it has a lower communication overhead than the existing work. The author [25] Therefore, we consider the random matrix theory for PL-SKG that we've developed to be a viable approach that demonstrates a cutting-edge signal processing paradigm to secure wireless communication channels. The author [26] A satellite-air-ground MCN that is environment-aware, service-driven, and integrated is what we foresee using external auxiliary information, such as the sea state and atmospheric conditions, based on this debate. The author [27] In terms of encryption and decryption, the proposed model was roughly 50.04% and 55.29% higher and 51.36% and 58.41% higher, respectively. The examination shows that the throughput rate has significantly increased (by more than 50%). The performance results obtained show that the proposed method is efficient and effective in terms of performance and security. The author [28] said this study sought to offer a comprehensive understanding of recent advancements in smart energy systems made possible by IoT devices, supported by excellent published literature. The IoT global energy market topped USD 6.8 billion in 2015, and it is anticipated to reach USD 26.5 billion by 2023, with a compound annual growth rate of 15.5% in 2016–23. The author [29] Yet, in recent times, the Internet of Things has been a target for attacks, which are made worse by the increased connection. In this section, we'll talk about common Internet of Things security concerns and attacks, as well as strategies for preventing them. The author [30] As a result, we propose a better plan to fix the security gaps found. Our method is demonstrably secure, and performance research demonstrates that it saves money when compared to other methods by cutting computing costs by 15.34% and communication costs by 40.68%. The author [31] The complexity of encoding is increased by these methods. FELICS and Matlab

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

tools simulate the proposed technique. The implementation of this algorithm makes use of several data types, including text and graphics.

III. Proposed methodology

This section describes the proposed method for generating physical layer key generation for node authentication in primary communication. The proposed algorithm employs discrete wavelet transforms and modified window sequences of bits for the conversion of bits. The first section of the algorithm describes the principle of the key generation approach, and the second section describes the methodology.

Principle of Key Generation

The wireless channel serves as the backbone for communication among IoT devices, offering symmetrical characteristics and high predictability. However, this predictability also renders the wireless channel vulnerable to various security threats, including man-in-the-middle attacks, noise attacks, jamming attacks, and scanning and signalling attacks. Conventional cryptography approaches for key generation may be impractical due to the resource limitations of IoT devices, despite attempts to leverage properties of the wireless channel such as Received Signal Strength (RSS). Several reasons justify the utilization of wireless channel properties in communication, including its symmetrical nature, signal attenuation with distance, and susceptibility to interception. To address the challenges posed by the wireless channel's predictability, authors often employ frequency-based transform functions for key generation and extraction. These transform functions, serving as quantization mechanisms, enhance signal reliability. This paper employs discrete wavelet transform and discrete cosine transform for quantization and key generation to facilitate secure communication between two IoT devices. The key generation system model, illustrated in Figure 1, involves three parties: Alice, Bob, and Eve. Alice and Bob are authorized parties engaged in communication, while Eve acts as a potential communication interloper or passive attacker. Both Alice and Bob utilize RSS channel parameters for information sharing, employing the concept of channel probing. Signals Xa and Xb are transmitted by Alice and Bob, respectively, with their signal strengths symmetrically matched (Xa = Xb). Two scenarios involving Eve are considered: one where Eve possesses knowledge of the message key and decodes information from Alice and Bob, and another where Eve is unaware of the key and tampers with RSS information to extract key values for decoding information. information for the extraction of key value for decode information [16, 24, 25].

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

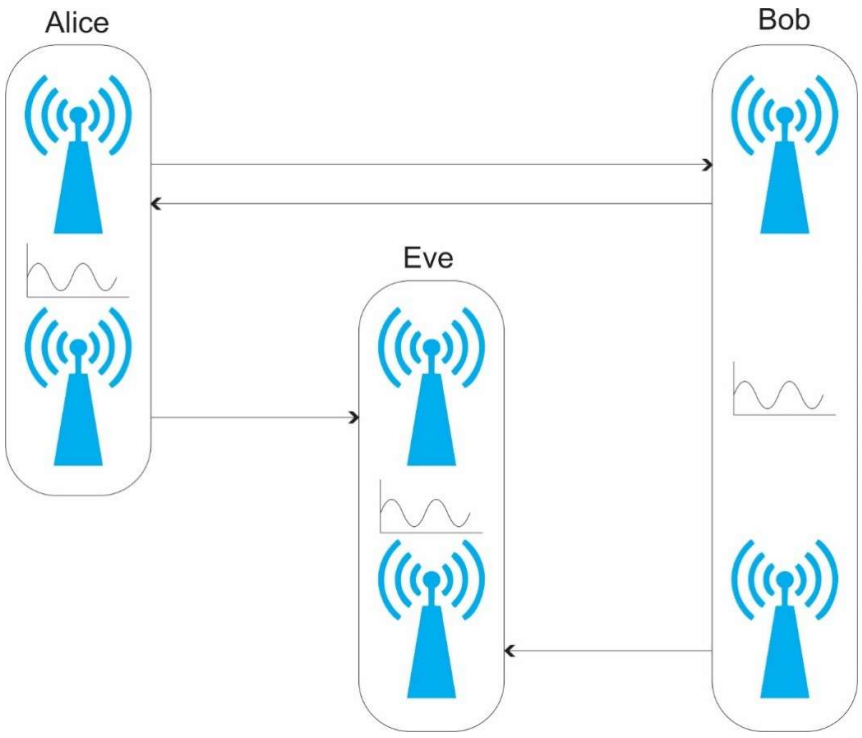

Figure 1 the process block diagram of RSS based communications in two authorized parties Alice and Bob. The third-party Eve as message and key intercept.

The key generation methods proposed in this study leverage two transformations and exploit the property of channel reciprocity. The process involves the utilization of Modified Window Sequence Selection (MWS) and Discrete Wavelet Transform (DWT) for sampling and encoding signals to form bits. Additionally, the application of discrete wavelet transforms enhances the randomness of the generated key, thereby reducing the security risks associated with information sharing. The key generation process can be described as follows:

1. We apply DCT transform on the receive RSS signals value. The DCT transform sampled in finite time series of sample into sum of different frequency. For the selection of modified window selection

$$X_k = \sum_{n=0}^{N-1} x_n cos\left[\frac{\Pi}{N}(n+\frac{1}{2})k\right] \quad k = 0, \dots\dots\dots..N \dots\dots\dots..(1)$$

2. The sample of DCT signal input of wavelet transform as

Wavelet transform applied long time windows, in order to get high frequency data. the processing of wavelet transforms of DCT sample frequency mapped as relative frequency process

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

The DWT defined as

$$W_\phi(j0,k) = \frac{1}{\sqrt{M}}\sum_x f(x)\phi_{j0,k}(x) \dots\dots\dots\dots\dots\dots\dots\dots\dots.(2)$$

$$W_\psi(J,K) = \frac{2}{\sqrt{M}}\sum_X f(x)\psi_{j,k}(x) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(3)$$

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

Now

$$f(x) = \frac{1}{M}\sum_{K} W_{\phi}(j0,k)\phi_{j0,k}(x) + \frac{1}{\sqrt{M}}\sum_{J=J0}^{J-1}\sum_{K} W_{\psi(J,K)}\psi_{J,K}(X) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (4)$$

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 3.

3. Select the decomposed higher frequency and estimate the mean of sample as threshold selection of frequency section

4. estimate the real value of transform of sample signal x(t). arrange these signals as ascending order. Now new sequence of signal as

$$X(k) = (arrange|s|2), (k = 0,1, \dots\dots\dots\dots\dots\dots Nr-1) \dots\dots\dots\dots\dots\dots\dots\dots\dots (5)$$

Here Nr is length of signal

5. Measure the value of threshold for the selection of frequency

$$th_{k=}\sqrt{f(k),\ (k = 0,1, \dots\dots\dots\dots., Nr-1)} \dots\dots\dots\dots\dots\dots (6)$$

6. Process of binary function is call for bit representation

7. Framed the bit value of 4-octact vector

8. Change the ordered and sequency of bit with rand () function

9. Finally, key is generated

10. Exit

The processing of key generation algorithm present in figure (2). Figure (2) explore step by step process of algorithm development.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

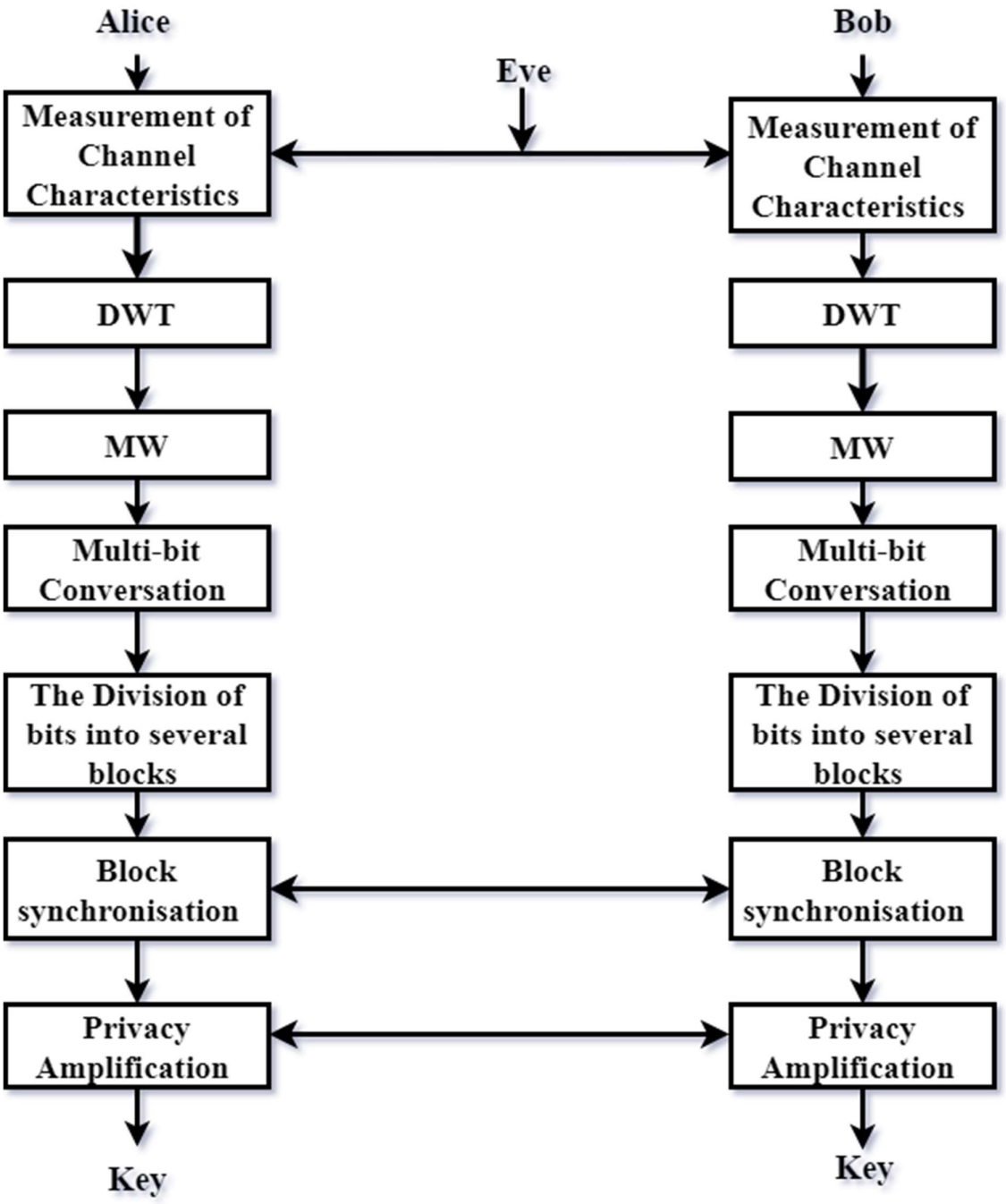

Figure 2 proposed model of physical layer key generation for IoT.

IV. 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 868MHz. These parameters measure the performance of modified key generation algorithms [16]. The simulation process is carried out under three scenarios: indoor, outdoor and hybrid. The proposed key generation algorithm compares with existing transform

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

methods DWT and DCT. The simulation parameters mention on table-.1.

Table-1 Simulation 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
Quantization	CDF
Sequence length	1000,2000,3000

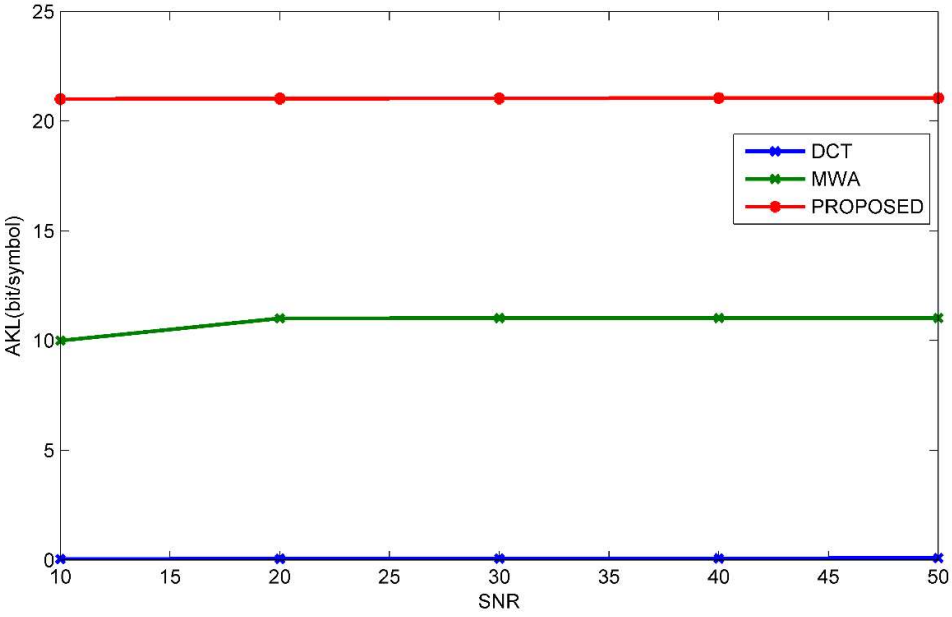

Figure 3 Performance analysis of average key length against SNR

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

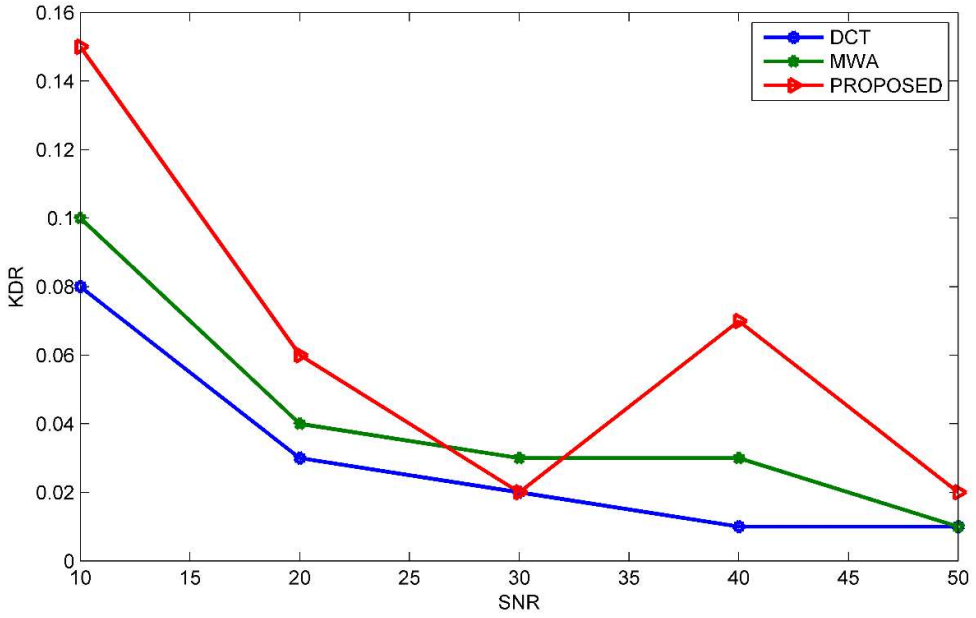

Figure 4 Performance analysis of key disagreement against SNR

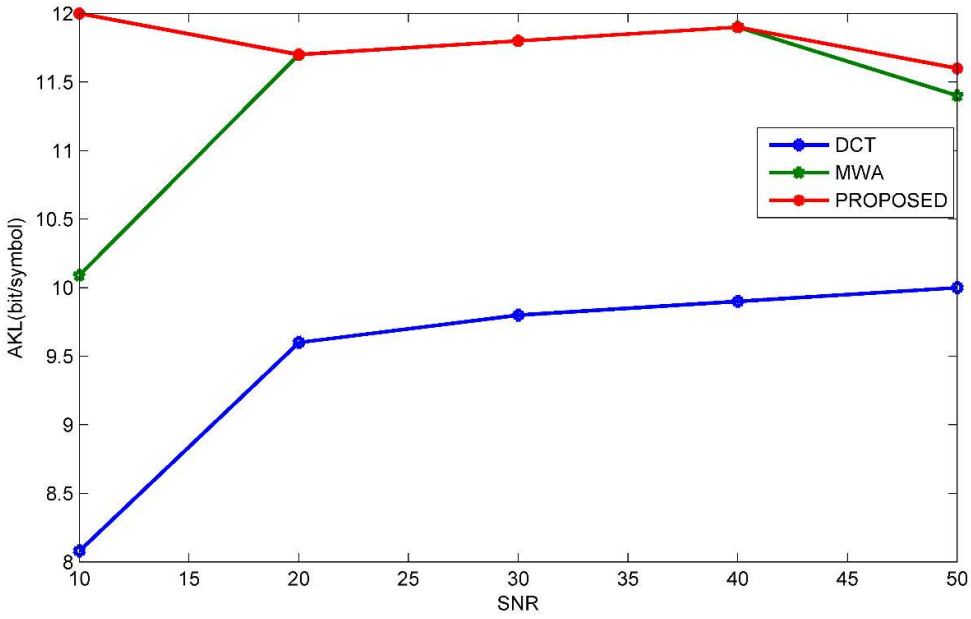

Figure 5 Performance analysis of average key length against SNR

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

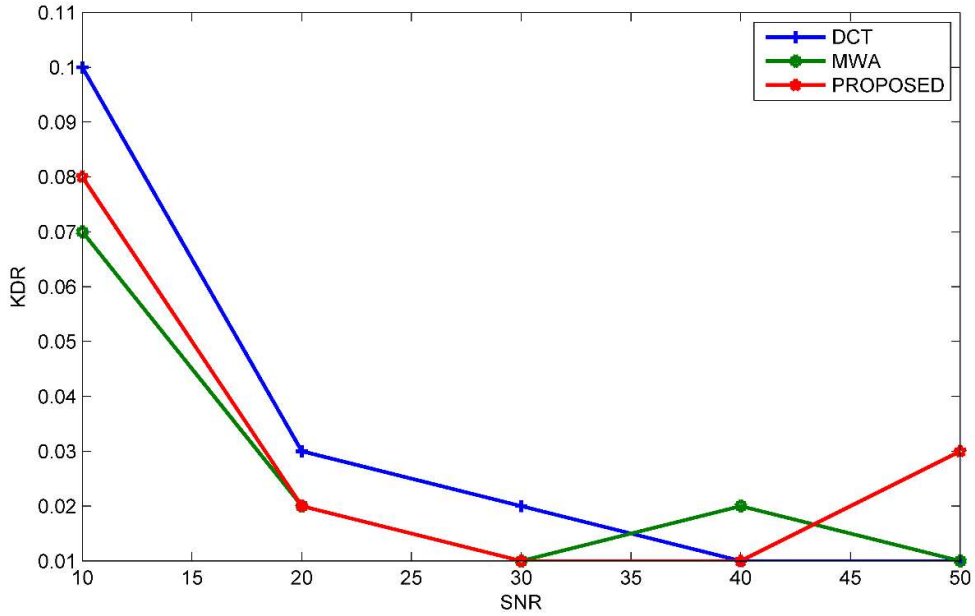

Figure 6 Performance analysis of key disagreement against SNR

V. Conclusion & Future Work

. We proposed a refined approach to key generation in the Internet of Things (IoT) by proposing modified window along with discrete wavelet transform (DWT). The modification involves incorporating the process of bit sequence an additional signal processing method known for shaping signal patterns. This proposed method aims to mitigate DWT discrepancies, resulting in a more efficient key generation process. The key generation process employs multi-bit quantization to assess the product of the modified discrete wavelet transform. To validate the effectiveness of the proposed algorithm, simulations are conducted for varying numbers of device nodes in both indoor and outdoor scenarios. MATLAB tools are utilized for the simulation, and standard parameters such as AKL (Average Key Length) and KDR (Key Disagreement Rate) are measured. The evaluation of results suggests that the proposed algorithm surpasses existing key generation algorithms in terms of performance and reliability. The study results indicate the successful creation of keys by devices through our proposed technique. Furthermore, comparative analyses demonstrated the superior performance of our method compared to other relevant schemes. Notably, the algorithm we propose is adept at defending against active attacks by entities like Eve, surpassing the limitations of passive eavesdropping. While eavesdropping remains a straightforward and passive attack method, the evolving landscape of IoT introduces potential threats such as message tampering, data disclosure, pilot spoofing, jamming, and masquerading. In the context of discrete wavelet transform (DWT), two vital performance indicators—feasible secrecy rate and the likelihood of secrecy outage—are frequently employed. In light of information theory perspectives, additional measures are suggested to comprehensively evaluate the efficacy of Physical Layer Security (PLS) systems. As future IoT landscapes are characterized by diverse user expectations arising from a myriad of devices and services, there is a pressing need to propose new metrics for assessing the effectiveness of PLS systems. This adaptation becomes crucial for addressing the evolving challenges posed by various active

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

malicious attacks in the IoT ecosystem.

References

[1]. Zoli, Marco, Miroslav Mitev, André N. Barreto, and Gerhard Fettweis. "Estimation of the Secret Key Rate in Wideband Wireless Physical-Layer-Security." In 2021 17th International Symposium on Wireless Communication Systems (ISWCS), pp. 1-6. IEEE, 2021.

[2]. Liu, Yiliang, Wei Wang, Hsiao-Hwa Chen, Feng Lyu, Liangmin Wang, Weixiao Meng, and Xuemin Shen. "Physical layer security assisted computation offloading in intelligently connected vehicle networks." IEEE Transactions on Wireless Communications 20, no. 6 (2021): 3555-3570.

[3]. Ohira, Shuji, Araya Kibrom Desta, Ismail Arai, and Kazutoshi Fujikawa. "PLI-TDC: Super fine delay-time based physical-layer identification with time-to-digital converter for in-vehicle networks." In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, pp. 176-186. 2021.

[4]. Xie, Ning, Junjie Chen, and Lei Huang. "Physical-layer authentication using multiple channel-based features." IEEE Transactions on Information Forensics and Security 16 (2021): 2356-2366.

[5]. Shakiba-Herfeh, Mahdi, Arsenia Chorti, and H. Vincent Poor. "Physical layer security: Authentication, integrity, and confidentiality." In Physical Layer Security, pp. 129-150. Springer, Cham, 2021.

[6]. Xia, Shida, Xiaofeng Tao, Na Li, Shiji Wang, Tengfei Sui, Huici Wu, Jin Xu, and Zhu Han. "Multiple correlated attributes based physical layer authentication in wireless networks." IEEE Transactions on Vehicular Technology 70, no. 2 (2021): 1673-1687.

[7]. Chen, Yi, Pin-Han Ho, Hong Wen, Shih Yu Chang, and Shahriar Real. "On Physical-Layer Authentication via Online Transfer Learning." IEEE Internet of Things Journal 9, no. 2 (2021): 1374-1385.

[8]. Ragheb, Mohammad, S. Mostafa Safavi Hemami, Ali Kuhestani, Derrick Wing Kwan Ng, and Lajos Hanzo. "On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry approach." IEEE Transactions on Information Forensics and Security 17 (2021): 53-68.

[9]. 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.

[10]. Xu, Weitao, Junqing Zhang, Shunqi Huang, Chengwen Luo, and Wei Li. "Key generation for Internet of Things: a contemporary survey." ACM Computing Surveys (CSUR) 54, no. 1 (2021): 1-37.

[11]. Zeadally, Sherali, Ashok Kumar Das, and Nicolas Sklavos. "Cryptographic technologies and protocol standards for Internet of Things." Internet of Things 14 (2021): 100075.

[12]. Guo, Dengke, Kuo Cao, Jun Xiong, Dongtang Ma, and Haitao Zhao. "A Lightweight Key Generation Scheme for the Internet of Things." IEEE Internet of Things Journal 8, no. 15 (2021): 12137-12149.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

[13]. Asif, Rameez. "Post-quantum cryptosystems for Internet-of-Things: a survey on lattice-based algorithms." IoT 2, no. 1 (2021): 71-91.

[14]. Saha, Tanujay, Najwa Aaraj, Neel Ajjarapu, and Niraj K. Jha. "SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and cyber-physical systems based on machine learning." IEEE Transactions on Emerging Topics in Computing (2021).

[15]. Ismael, Waleed M., Mingsheng Gao, Zhengming Chen, Zaid Yemeni, Ammar Hawbani, and Xuewu Zhang. "Edcra-iot: Edge-based data conflict resolution approach for internet of things." Pervasive and Mobile Computing 72 (2021): 101318.

[16]. Goyal, Parul, Ashok Kumar Sahoo, Tarun Kumar Sharma, and Pramod K. Singh. "Internet of Things: Applications, security and privacy: A survey." Materials Today: Proceedings 34 (2021): 752-759.

[17]. Ren, Xiaojun, Zhijun Zhang, and Seyedeh Maryam Arefzadeh. "An energy-aware approach for resource managing in the fog-based Internet of Things using a hybrid algorithm." International Journal of Communication Systems 34, no. 1 (2021): e4652.

[18]. 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.

[19]. 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.

[20]. Yılmaz, Saadet Simay, Berna Özbek, Mert İlgüy, Bismark Okyere, Leila Musavian, and Jonathan Gonzalez. "User Selection for NOMA-Based MIMO With Physical-Layer Network Coding in Internet of Things Applications." IEEE Internet of Things Journal 9, no. 16 (2021): 14998-15006.

[21]. Tang, Xinyao, and Soumyajit Mandal. "Encrypted physical layer communications using synchronized hyperchaotic maps." IEEE Access 9 (2021): 13286-13303.

[22]. Zoli, Marco, Andre N. Barreto, and Gerhard Fettweis. "Investigating the eavesdropper attack in physical layer security wireless key generation: a simulation case study." In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), pp. 1-5. IEEE, 2021.

[23]. Sumathi, V., G. Nageswara Rao, M. Parimala Devi, and Ravisankar Malladi. "A novel RSS based light weight digital certificate and key generation scheme for coherent communication of IoT devices." Materials Today: Proceedings (2021).

[24]. Junejo, Aisha Kanwal, Fatma Benkhelifa, Boon Wong, and Julie A. Mccann. "LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks." IEEE Internet of Things Journal 9, no. 6 (2021): 4110-4124.

[25]. Wei, Zhuangkun, and Weisi Guo. "Random matrix based physical layer secret key generation in static channels." arXiv preprint arXiv:2110.12785 (2021).

[26]. Wei, Te, Wei Feng, Yunfei Chen, Cheng-Xiang Wang, Ning Ge, and Jianhua Lu. "Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges." IEEE Internet of things journal 8, no. 11 (2021): 8910-8934.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 18 No. 01 (2024)

[27]. Mousavi, Seyyed Keyvan, and Ali Ghaffari. "Data cryptography in the internet of things using the artificial bee colony algorithm in a smart irrigation system." Journal of Information Security and Applications 61 (2021): 102945.

[28]. Ahmad, Tanveer, and Dongdong Zhang. "Using the internet of things in smart energy systems and networks." Sustainable Cities and Society 68 (2021): 102783.

[29]. Ahmed, Majd S. "Designing of internet of things for real time system." Materials Today: Proceedings (2021).

[30]. Fan, Qing, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo. "A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain." Journal of Systems Architecture 117 (2021): 102112.

[31]. Al-Ahdal, Abdulrazzaq HA. "Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 12 (2021): 133-143.