International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys.13, No.1 (Apr-23)

http://dx.doi.org/10.12785/ijcds/130183

Efficient Secret Key Generation Using Langrage's Interpolation and Discrete Wavelet Transform Function for Internet of Things

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

[1]*Department of Electronics and Communication, NIT Kurukshetra. Haryana 136119, India*
[2]*Department of Electronics and Communication, NIT Kurukshetra. Haryana 136119, India*
[3]*Department of Electronics and Communication, NIT Kurukshetra. Haryana 136119, India*

Received 15 Aug. 2022, Revised 23 Dec. 2022, Accepted 6 Feb. 2023, Published 16 Apr. 2023

Abstract: Data security during information flow has been a difficult challenge in Internet of Things (IoT). To improve security status various conventional cryptographic methods such as public, private, and hybrid key generation had been utilized by various researchers. But these methods are associated with a lack of secure communication between two or more devices. In view of this, a lot of effort is being put into the physical layer of security. In this concept signal-based encryption and key generation are used as the major components in the security of data. In this research, we present a physical layer security technique based on wavelet transforms and Langrage's interpolation. The wavelet based function precedes the sampling of Received Signal Strength (RSS) and convolution of the Langrage's interpolation and generates a session shared key for communication. The size of the generated key is 128 bits and 1024 bits during the authentication process of sharing information. The proposed algorithm's performance is evaluated through a simulation modeling environment. Different standard data bench for performance analysis is also used. The proposed technique is evaluated in two scenarios; Line of Sight (LoS) and Non-Line of Sight (NLoS). The proposed algorithm is contrasted with key generation techniques based on Lagrange and Skyglow (SKG).As compare to Skyglow and Lagrange's algorithms, the proposed algorithm achieves a 3-5% improvement in overall efficiency for key generation validation.

Keywords: IoT, Key Generation, WSN, Security, LI, DWT, RSA, DCT

1. INTRODUCTION

The generation of communication changes the role and responsibility of resources for the betterment of future technology. IoT is an innovative communication platform for all types of interdisciplinary domains such as medical, agriculture and transportation, etc [1]. With IoT, a massive amount of data is now being exchanged between different devices. Security of information is a significant concern these days. A number of active and passive attacks are possible . To prevent these attacks a number of physical layer security and cryptographic primitives are developed by various researchers. Different cooperative jamming, amplify and forward (AF), decode and forward (DF), and physical layer security (PLS) techniques are available in the literature. These techniques are analyzed regarding secrecy capacity, secrecy rate, and outage probability.Wireless physical layer security (WPLS) is an effective technology for both existing and new wireless services. The main components that add diversity and toughness to the WPLS concept are physical layer authentication (PLA), antenna selection (AS), and relay node selection. Machine learning has lately become a promising method for reducing the scale and complexity of wireless devices. IoT devices are resource constrained, thus the existing cryptographic or PLS mechanisms are complex in nature. They cannot be implemented in IoT devices[2] [3]. The main problem with IoT devices is that they have limited resources such as memory and computing capability [4]. The limited resource capacity of the device increases the vulnerability of the security of communication data. Security concern adopts conventional cryptography methods such as public, private, and hybrid. These cryptography methods failed to ensure secure communication between two or more devices [5][6][7]. The diversity and applicability of IoT-based communication increase the potential vulnerability to security and authentication [8][9]. The secured communication protocol creates a new milestone in device-based communication. Conventional security protocols and cryptography algorithms cannot provide the full mode of security and authentication in wireless communication. The limitations of wireless embedded devices include memory, processing unit, energy, and computational capability of devices.To ensure the

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

safety of the information being transferred, the standard symmetrical cryptosystem protocol entails the sharing of secret keys or credential management [10][11][12], where the computational capabilities of the device influences the security of this protocol. The technique will be readily attempted in the future when computational capabilities of eavesdropping devices improve, for example, through the use of quantum computing technologies [13][14].Spreading a secret key across a huge network, on the other hand, is difficult because it requires significant private key transfer to facilitate the formation of private keys among gadgets. A few researchers have concentrated on symmetric cryptography attempts to create low-cost and practical remedies that may be deployed as portable cryptographic solutions for IoT devices [15][16].The Skyglow (SKG) scheme is a nice option for a number of reasons, including the use of unpredictability from wireless channels, which ensures its security in theoretically, the fact that it can be carried out between two persons without the requirement for third-party support, as well as the fact it being inexpensive, making it appropriate for IoT [17].To improve security, various authors have proposed key generation methods in IoT-based communication devices [18]. The future of key generation methods is determined by key length and computational complexity[6][7] . A novel key generation algorithm is proposed in this paper, with a combination of Langrage's interpolation and discrete wavelet transform function. Langrage's interpolation function was previously used for sharing information and encoding data in 1980. These mathematical functions provide the point of intersection for the hiding of data during the process of transmission process [19]. The sharing and hiding of information is used for the process of key interval generation. In discrete wavelet transforms, sample signals are formed and creates a series of waves in the frequency-time representation of signals. The representation of signals used the sampling of the key for the process of generation. The wavelet's low-frequency value is utilized to generate a secret key[20][21].

2. RELATED WORK ON KEY GENERATION

The key length and computational time of key generation process decide how long it takes to generate the key. Various researchers have made ongoing efforts in the domain of key generation techniques for the security of IoT devices. Key size, flexibility, the design of the algorithm, the process of a substation, and other features and factors all have an influence on the key generation process.Table 1 provides a complete description of the algorithms and the various factors that impact the key generation process [22][23][24] [25]. In this table, different existing algorithms are mentioned along with their key length, input text length, etc. Advanced cryptographic algorithms have high computing, storage, and processing requirements that IoT devices cannot meet due to resource constraints. As a result, finding a way to implement required security mechanisms at a low cost and with minimal overhead is essential for the IoT . Table 2 provides the reported study of attacks in all security stacks in IoT. IoT- based communication devices are compromised with various security threats in different layers such as physical, network, and application layers for the integrity and security of data. In physical, network, transport, and application layers there are man in the middle, deprivation of delivery, breach of confidentiality, spoofing an IP address and network outage assaults are present. There are some manmade assaults like fake nodes; malicious data, tampering and node capture are the most common attacks in the physical layer. These assaults are required to be more addressed by various researchers. These layers are responsible for end-to-end communication in IoT enable communication systems. IoT also has some significant challenges that make users wary to adopt this technology. Some of the IoT issues listed like power consumption and bandwidth, sensing, lightweight computing, and complexity needs to be addressed by researchers [26][27][28][29][30] [31].

3. LANGRAGE'S AND WAVELET TRANSFORM

In terms of data security, Langrage's Interpolation (LI) is essential. In IoT devices, the formation of polynomial and coordinate points intercept signals and interpolates in terms of wavelet for the transformation process. Furthermore, intercept processing estimates the unique points and provides strength during the session key generation. Here we describe the mathematical functions of langrage's interpolation. The langrage's interpolation method used for the distribution of key and for the process of creation of key[8] [25].

1) A collection of data points (x_i, y_i), i = 0,1....n is derived by a function $f(x)$ such that $y_i = f(x)$, i = 0,1....n. A reasonable interpolation function, $I(x)$ is expressible as

$$I(x) = \sum_{i=0}^{n} L_i(x) \cdot f(x_i)\, L_0(x) \cdot f(x_0) + L_1(x) \cdot f(x_1) + \cdots + L_n(x) \cdot f(x_n) \tag{1}$$

2) The functions $L_i(x), i = 0, 1, ..., n$ are selected to fulfill

$$L_i(x) = \{^{0: x=x_0, x_1, ..., x_i-1, x_i+1, ..., x_n}_{1: x=x_i} \tag{2}$$

Equation (1) represents function I(x) is sum of interpolation of signals and represents signal dot product. The equation (2) set the range of intercept point of coordinates.

The wavelet transform is essential for signal data sampling and image processing. The layer-wise decomposition of transform lifts the process of quantization in terms of absolute value estimation.

In Discrete Wavelet Transform (DWT), a signal is assessed on a small number of scales with varying quantities of translations at each scale. A critical sample of the CWT W(a,b) is obtained by putting $a = 2^{-j}$and $b = k \cdot 2^{-j}$ where

TABLE I. Review of Existing Key Generation Algorithms used in Various Block Ciphers

Alhorithm	Authors	Input Text	Flexi-bility	Modification	Remarks	Algotitm Structure	Key size (Max/ Min)	Substitution s-box	Number of iteration rounds	Cipher Type
DES	Bahnasawi et.al[24]	64 bits	No	-	DES doesn't support any changes	Feistel cipher network	56	8	16	Block cipher
TDES	Revadigar et.al[22]	64 bits	Yes	168	TDES has been extended to 168 bits with different key sizes	Feistel cipher network	168	8	48	Block cipher
Blowfish	Xu Weitao et.al[23]	64 bits	Yes	64-448	The size of the key must be divisible through 32bits.	Feistel cipher network	128-448	4	16	Block cipher
IDEA	Wan jiang et.al[25]	64 bits	No	-	The certain modifications are not supported by IDEA.	S-permutation network	128	N/A	8	Block cipher
TEA	Wan jiang et.al[25]	64 bits	No	-	Changes to the Feistel Structure (TEA) are not supported	Feistel cipher network	128	N/A	64	Block cipher
CAST	Wan jiang et.al[25]	64 bits	Yes	64, 128, 256	The 64-bit CAST network is a versatile network that has been enhanced with protection and confidence to 128-256 bits.	Feistel cipher network	40-128	4	12-16	Block cipher
AES	Bahnasawi et.al[24]	128 bits	Yes	128, 192, 256	Rijndael algorithm can be extended to a key size of 64 bits.	Feistel cipher network	128, 192, 256	1	10, 12, 14	Block cipher
RC6	Jindal et.al[5]	128 bits	Yes	128-2048	It includes VKL capable of being enhanced to 2048 bits, but it needs to be a massive number of 32 bits.	Feistel cipher network	128, 192, 256	N/A	20	Block cipher
Serpent	Xu Weitao et.al[23]	128 bits	Yes	256	The keys have always been equipped up to 256 bits. A "1" bit is followed by "0" bit in the padding.	Feistel cipher network	128, 192, 256	8	32	Block cipher
Twofish	Panchal et.al[21]	128 bits	Yes	256	Except for the default sizes, its keys are often equipped with "0" bits up to the subsequent default size.	Feistel network	128, 192, 256	4	16	Block cipher
MARS	Panchal et.al[21]	128 bits	Yes	128-448	It supports VKL, but key size has to be exact copies of 32 bits in order to function.	Feistel cipher network	128-448	1	32	Block cipher
Genetic Algo	Kannouf et.al[18]	128 bits	-	256	-	Feistel cipher network	-	1	16	Block cipher

j and k are integers representing scale and translation, respectively. Following this modification,

$$\Psi_j, k(t) = 2^{j/2} \cdot (2^j \cdot t - k) \quad (3)$$

The equation (3) is mother wavelet transform form in terms of scaling and translation.

For any integers jandk, these wavelets form an orthonormal basis$\Psi_0, 0(t) = \Psi(t)$, the mother wavelet. The mother wavelets are translated and dilate to make further wavelets. Discrete wavelet transformations are thus denoted by $W(j,k)$

$$W(j,k) = \int_t^{\cdot} f(t) \cdot 2^{j/2} \cdot \Psi(2^j - k) \cdot d \quad (4)$$

The equation (4) represents the Discrete Wavelet transform for the sampling of RSS. The technique of keeping a minimum number of wavelet coefficients to reflect all the data

TABLE II. Review of IOT Levels and Related Security Issues

IoT levels	Issues of security	Implications	Layers affected	Solutions
Low-level	Obstacles jamming	Denial-of service attacks and disruption	Physical layer	Monitoring link quality, calculating packet transmission ratios, encrypting error-correcting code packet data, and varying frequency and location are all required.
Low-level	Sybil and spoofing attacks at a low level	Denial-of service attacks and network disruption	Physical layer	Measurements of signal strength and channel estimation.
Low-level	Initialization and configuration of the system are insecure	Breach of privacy and deprivation of delivery	Physical layer	Making artificial noise and modulating data transmission rates between nodes.
Low-level	Physical interface that is insecure	A data breach and a rejection attack	Hardware	Using software/firmware, TPM modules based on hardware, and experimenting and debugging tools to avoid USB access.
Low-level	An incident of sleep deprivation	Energy usage	Link layer	A multi-layer system for detecting intrusions is used.
Intermediate level	Fragmentation causes replay or duplication attacks	Invasion of privacy and deprivation of provider	6LoWPAN network layer	For protection against replay attacks, timestamp and nonce options were added, as well as fragment verification using hash chains.
Intermediate level	Finding a risky neighbour	IP Address Forgery	Network layer	Signatures based on elliptic curve cryptography (ECC) for authentication.
Intermediate level	Attack with a reservation buffer	A assembly buffer is unavailable	6LoWPAN network layer and adaptation layer	Using a split buffer technique requires the transmission of all fragments.
Intermediate level	Routing attack with RPL	Eavesdropping and man-in-the-middle threats	Network layer IPv6	Authentication via encryption and signatures, as well as node behavior tracking.
Intermediate level	Sinkhole and wormhole attacks	Deprivation of delivery assault	Network layer	The features include rank certification via a cryptographic chain function, integrity management level, node/communication activity analysis, and object tracking via an intrusion detection system (IDS), encrypted communication key distribution management, structure traversals, and transmit power assessment.
Intermediate level	Sybil attacks	Breach of privacy, spamming, Byzantine issues, and inconsistent broadcast	Network layer	Random social network travels, user activity evaluation, and management of profiles of trustworthy and untrustworthy customers.
Intermediate level	Secure transmission and authentication	Breach of privacy	6LoWPAN Adaptation, Transit, and Network Layers	Compressed AH and ESP are examples of TPM using RSA, SHA1/AES, composite verification, validation with fuzzy extruder, compressed AH, IACAC using Elliptic Curve Cryptography, transmitted logs, and synchronous homomorphism modeling.
Intermediate level	Transport-level edge security	Breach of privacy	Transport layer, and network layer	IKEv2 employs compressed UDP, a Link layer with the nonce, a 6LoWPAN Boundary Network with ECC, an AES/SHA-based DTLS cypher, reduced IPSEC, DTLS preamble reduction, and Advanced encryption protection with authentication and access.
Intermediate level	Session establishment and resumption	Denial-of-carrier assaults	Transport layer	Using symmetric keys and a long-lived secret key, authorization and encryption are performed.
High-level and intermediate-level	Internet security with CoAP	Denial-of-carrier assaults on a network	Application layer, and network layer	Communication screening for TLS/DTLS and HTTP/CoAP, Reflection Gateway and Resource Directory, TLS-DTLS tunnel, and 6LBR-based data filtration are all supported.
High-level and intermediate-level	Insecure software/firm ware	A privacy violation, a rejection intrusion, and a network power failure	Application layer, transport layer, and network layer	Periodic application upgrades, the use of document identities, and security with confirmation are all highly urged.
High-level and intermediate-level	Protection of middle ware	A privacy violation, a rejection intrusion, and a network power failure	Application layer, transport layer, and network layer	To provide encrypted connection, identification, security rules, access control across devices, access points, and M2M modules, middleware M2M security, and accessible interface with encrypted and authentication approaches are all used.
High-level	Interfaces that are insecure	A privacy violation, a rejection intrusion, and a network power failure	Application layer	Weak passwords are not allowed, and the interface is tested against software tool vulnerabilities (SQLi and XSS), as well as utilizing https and firewalls.

in the original function is referred to as critical sampling. In CWT, transform coefficients are obtained for every (a,b) combination, whereas transform coefficients are found at a few places in DWT.

4. KEY GENERATION ALGORITHM

Various key generation algorithms used transform function and signal quantization methods in wireless communication. Channel parameters such as RSS are employed in key generation and key extraction for IoT devices. The SKG algorithms used the Discrete Cosine Transform (DCT) function for the quantization process that improved bit reliability and reduced Bit Error Rate (BER). The Skyglow algorithm reduces the utilization of radio frequency in case of receptions and transmissions. These algorithms have not used the process of privacy amplification for the generation of keys[23] [25] [32].The generated key length of Skyglow is 128bits. The Key entropy of Skyglow is very high and enhances the reliability of IoT- based communication systems. Some authors used a key generation system of five stages and some used four steps. Figure 1 depicts the key generation phases. The first phase in the procedure is determining the channel properties between two authorized parties. The measured difference value is higher than used for the process of preprocessing. The next step is the quantization of signals into single bit value and multi-bit value. After the process of quantization, the measured bit value difference is called the error-correcting phase and then finally proceed for the privacy amplification. In privacy amplification hash code algorithm is used for the creation of a message digest.

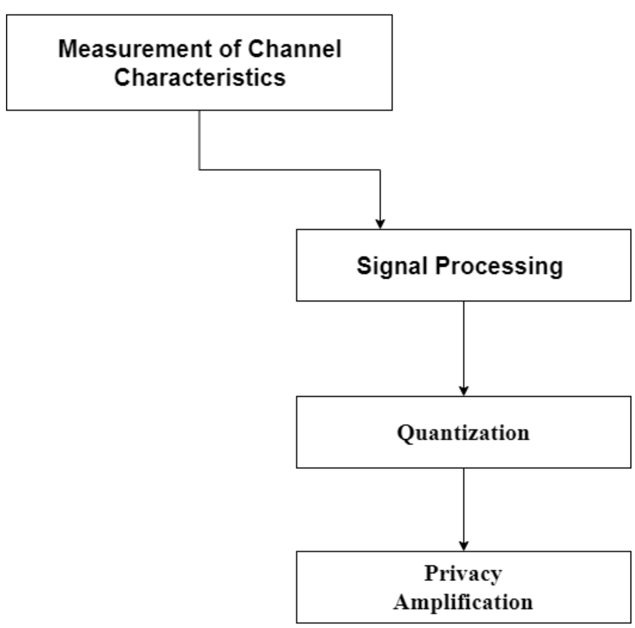

Figure 1. Key Generation Algorithms using four phase

5. PRINCIPLE OF KEY GENERATION

The communication capability of IoT devices is significantly impacted by prevailing wireless channel. The wireless channel is highly unpredictable. Moreover, these channels are broadcast in nature. IoT implementations are therefore vulnerable to security threats. For the authentication of data, various key generation techniques are used. These includes cryptography algorithm such as RSA, AES, ECC, and many more cryptography algorithms[28][29].Now, the properties of wireless channel such as RSS are also explored . As known, IoT devices have memory and energy limitations. The RSS parameters minimize the computational cost of the key generation and enhance the efficiency of IoT communication models. There are the various reasons to use channels property of wireless communication as mentioned below [33].

1) The nature of the wireless channel is symmetrical, so participants in the communication process received identical signals.
2) Variation of RF signals according to their motion of devices.
3) The location variation of participants decreases the strength of the signal and third-party interception of communication.

6. SYSTEM MODEL OF KEY GENERATION

Figure 2 shows the key generation system model. Alice, Bob, and Eve were the three parties involved in the key generation model. Alice, Bob, and Eve are the three parties involved in key generation model. Eve is a key communication modulator or passive attacker. The RSS Channel parameters were used by both Alice and Bob for information sharing based on the concept of channel probing. The Ya signal is transmitted by Alice and Yb signal is Transmitted by Bob. The symmetric signal strength is equal in both cases (Ya=Yb). Here two cases consider in the case of Eve. Eve knows about the key of the message and decodes the information of both parties Alice and Bob. Another condition is Eve cannot aware of keys and tamper the RSS information for the extraction of key- value for decode information [8][32][34].

7. THE PROPOSED ALGORITHM

There are three phases to modifying key generation algorithms. The RSS channel parameter is collected in the initial phase, and the collected signal is transformed into discrete wavelet transforms in the second phase, and finally, the transformed signal is mapped into langrage's interpolation for the generation of bit value. The elimination of preprocessing phase and privacy amplification improves the computational cost of the key generation algorithm. The collection of RSS signals is dependent on the device type, such as how communication proceeds in line of sight, no line of sight, and device mobility. The intensity of the signal is determined by the measurement process. The process of signal deviation (NLoS) measures the phase difference of noise. The process of algorithms is shown in Figure 3.

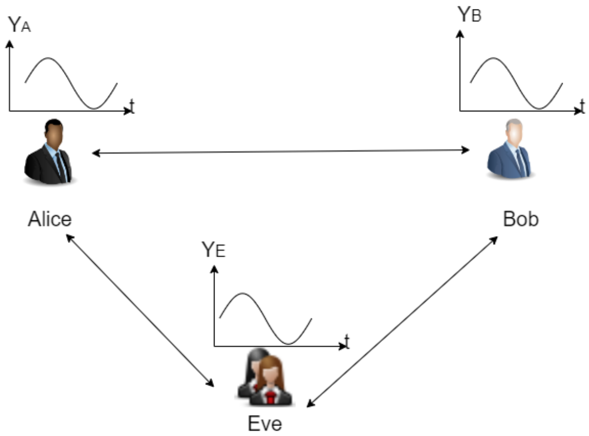

Figure 2. Two authorized parties, Alice and Bob, communicate via RSS. Eve, a third party attacker

The first phase of key generation algorithms collects the RSS signal as Y_u.The Value of Y_u signal changes with Y_a, Y_b, and Y_e. The signal of Y_a, Y_b , and Y_e denotes the value of Alice, Bob , and Eve. The measured character of signal interpolates in langrage's a

1. A set of signals $f(x) = (Y_a, Y_b, Y_e)$ is function of $f(x)$ so that $Y = f(x)$.
2.$I(x) = \sum_{i=a}^{b} L_i(x).f(x_i)$ the function of interpolation ties to meet the condition of Y_u.
3.$Y_u = Y_a{\cdot}Y_b$ and $y = f(x)$.

Now the measure the temporal variation of signal strength as

$$T_{Y_a \cdot Y_b} = \frac{\sum_{i=1}^{n}(Y_{a_i} - \phi_a)(Y_{b_i} - \phi_b)}{\sqrt{\sum_{i=1}^{n}(Y_{a_i} - \phi_a)^2}\sqrt{\sum_{i=1}^{n}(Y_{b_i} - \phi_b)^2}} \quad (5)$$

the ϕ the variation of signals and represents signal as shown below,

$$y_a = [y_a(1), y_a(2).........y_a(n)]^T$$
$$y_b = [y_b(1), y_b(2).........y_b(n)]^T$$
$$y_e = [y_e(1), y_e(2).........y_e(n)]^T$$
$$y_{e'} = [y_{e'}(1), y_{e'}(2).........y_{e'}(n)]^T$$

The interpolation of Alice, Bob and Eve is quantized and transformed by the wavelet transform function in terms of bit formation of RSS signal as given in equation (6)

$$WT(bits) = \left\{ \begin{array}{ll} WT \leq y_a, & 00 \\ WT \geq y_a, & 01 \\ WT \leq y_b, & 10 \\ WT \geq y_b, & 11 \end{array} \right\} \quad (6)$$

8. RESULTS AND ANALYSIS

The modified 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

Algorithm 1

Require:
RSS channel characteristic Y_u
The formation variation of RSS signal T
The bit formation of RSS M
The length of bit N
Ensure:
The sequence of keys: [0101010Ç ª]
Assign the number of nodes 2^k.
Estimation of M bit in each node with W_T [P_1, P_2^K].
for
  $i \leftarrow 1$ to n **do**
  if $Y_{ui} \leq T - T/n$ **then**
    Node 1
    $N_{ui} = P_1$
  end if
  if $T - T/n < Y_{ui} < T$ **then**
    Node 2
    $N_{ui} = P_2$
  end if
  $T < Y_{ui} + T/n$
  Node 3
  $Y_{ui} >= T + T/n$
  Node 4
  M = [P1, P2, P3, P4...........]
end for

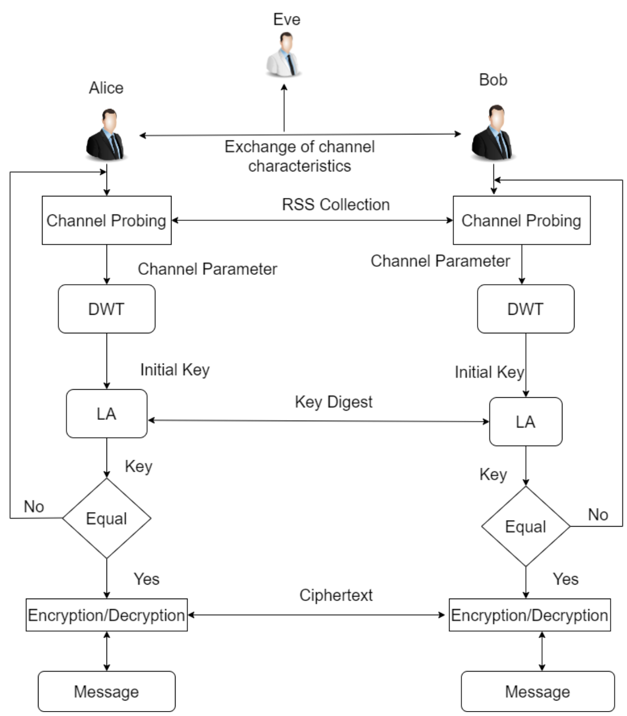

Figure 3. Proposed key generation algorithm based on wavelet transform and langrage's interpolation.

digital signal generators of MATLAB function. The signal strength of RSS is 868MHz. These parameters measure the performance of modified key generation algorithms [8]. The simulation parameters mention on table-3 [24][34].

1) BER(Bit Error Rate): The bit incompatibility likelihood among two generated keys is assigned by BER.
2) KAR (Key Agreement Rate): KAR calculates the likelihood of producing similar keys with no interferences.
3) KLR (Key Leakage Rate): KLR assigns a possibility to Eve recreating the key while using the non - encrypted disorder..
4) Key Entropy: The generated key ought to be arbitrary, preferably through one entropy.
5) SBP (Secret Bits per Packet): SBP assigns the number of produced bits per text replace to communication parties. SBP is an indicator of energy performance.

Table 4: Under this context, the simulation results of both line of sight and non-line of sight indoor scenarios, there are no obstacles in IoT devices. The proposed algorithm is very effective in this case and obtained minimum data loss, and reduces the error of message in terms of BER. The algorithm also focuses on the computational process of KAR and reduces the KLR. The parameter value of KLR reduces and proves the utility of the transform function in the key generation process. The existing algorithm also obtained good results in indoor scenarios, but proposed techniques improve the overall performance of the simulation.

Table 5: In this case, the simulation results of outdoor scenarios, Lines ofsight and non-line ofsight both apply to multiple obstacle points. The results are analyzed using two parameters: bit error rate (BER) and key agreement rate (KAR). The modified algorithm incorporates with transform function and langrage's interpolation. The langrage's interpolation intercepts the point of the RSS signal. It reduces interference and noise. Due to the intercept point of RSS signals, noise eliminates, and loss of data is minimized; hence, the value of BER is decreased instead of existing methods. Also, the results of KAR improve in outdoor scenarios. The reduced number of steps increases the possibility of a key agreement rate.
Figure 4. Represents the all-simulation results in all three-condition scenarios, LoS, nLoS, and IoT devices' mobility. The proposed method applied in all these cases reduces BER due to proper sampling of intercept points of RSS signals with Langrage's interpolation. The interpolation point reduces the bit mismatch and authenticates nodes with the provided key. The existing algorithm use quantization for the formation of bits. The methods of quantization not converted all signals into bits, and the range of error increases the BER. The proposed algorithm reduces 3% of BER values instead of existing methods.

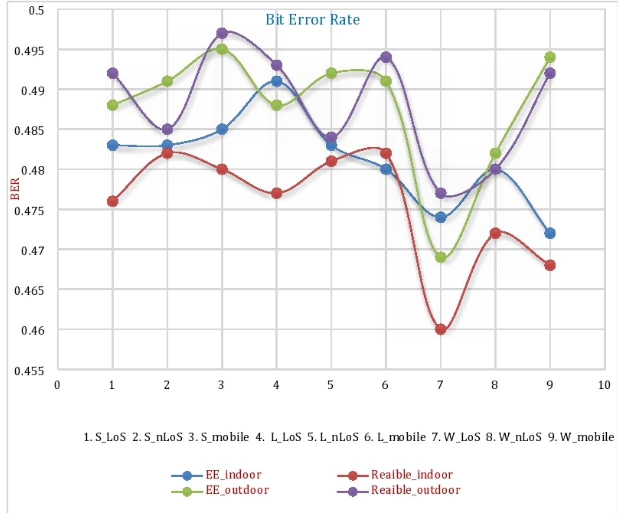

Figure 4. Performance evaluation of BER in Skyglow, Lagrange and Wavelet-Lagrange in the both scenarios indoor and outdoor.

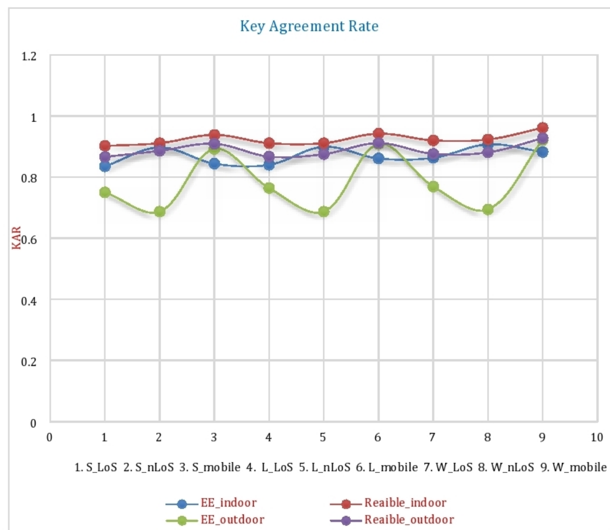

Figure 5. Performance evolution of KAR in Skyglow, Lagrange and Wavelet-Lagrange in both scenarios indoor and outdoor..

Figure 5 Describes the Key Agreement Rate (KAR) results in all three conditions of simulation such as LoS, NLoS, and mobility. The value of KAR increases in the proposed algorithm's case and authentication of IoT devices increases. Due to layer sampling, the transform function of RSS signals mapped with the key formation and maximized the randomness factor instead of the existing key generation algorithm. The proposed method also decreases the bit discrimination of different devices of IoT. Now the value of KAR increases 5% in compression of existing algorithms.

Figure 6. Describe the possibility of key vulnerability during the process of devices authentication in an IoT

TABLE III. Simulation parameters

Parameters	Values
System Model	IEEE 802.11
Key Size	128
No of communication node	3
Noise model	AWGN
Wavelet	DB2,DB3,DB4
Quantization	LI
Sequence length	1000,2000,3000

TABLE IV. Analysis of skyglow, Lagrange and Wavelet- Lagrange

Indoor Scenarios	SKG			LKG			WL		
Parameters	LoS	nLoS	Mobile	LoS	nLoS	Mobile	LoS	nLoS	Mobile
BER	0.483	0.483	0.485	0.491	0.483	**0.480**	0.474	0.480	0.472
KAR	0.835	0.897	0.844	**0.840**	0.899	0.861	0.863	0.907	0.882
KLR	0.007	0.010	0.004	0.007	0.09	**0.005**	0.008	0.09	0.005
Entropy	0.997	0.998	0.997	0.982	0.996	**0.997**	0.988	0.998	0.998

TABLE V. Analysis of skyglow, Lagrange and Wavelet- Lagrange

Outdoor Scenarios	SKG			LKG			WL		
Parameters	LoS	nLoS	Mobile	LoS	nLoS	Mobile	LoS	nLoS	Mobile
BER	0.488	0.491	0.495	**0.488**	0.492	0.491	0.469	0.482	0.494
KAR	0.750	0.687	0.892	0.764	**0.687**	0.908	0.769	0.694	0.921
KLR	0.002	0.003	0.001	0.003	0.002	**0.002**	0.003	0.003	0.002
Entropy	0.997	0.997	0.997	**0.998**	0.997	0.996	0.998	0.998	0.997

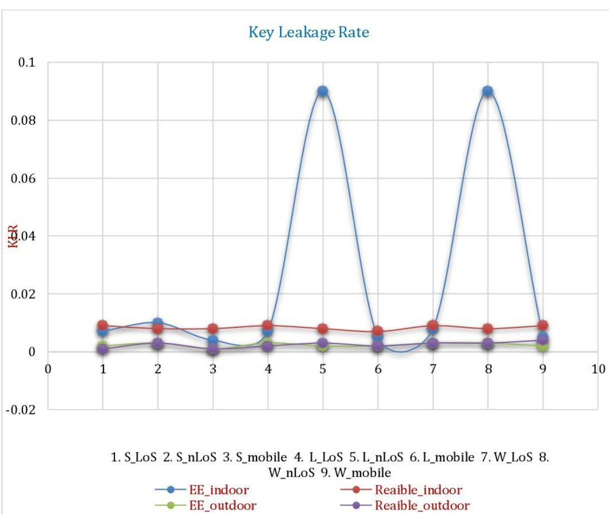

Figure 6. Performance evolution of KLR in Skyglow, Lagrange and Wavelet-Lagrange in both scenarios indoor and outdoor.

communication system. The Reduced value of KLR indicates that the proposed algorithm provides a secured communication key in all simulation conditions. The key formation through a sampling of wavelet transform increases the standard key formation such as 128 bits. The existing algorithms generate a key size of about 128 bits. Because of the unavailability of a standard key size, it was tempered by third party Eve. The overall strength of the key is increased up to 5% instead of existing algorithms.

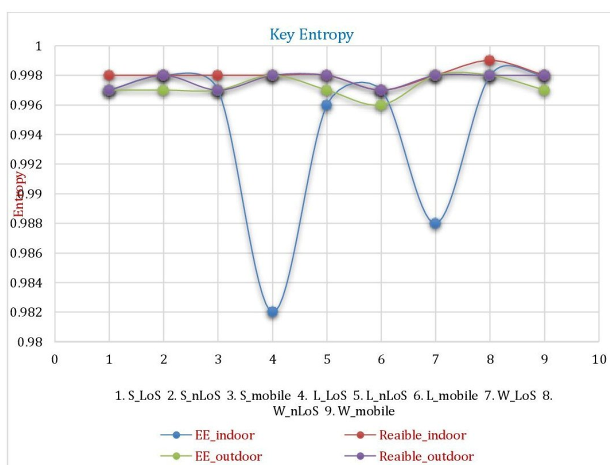

Figure 7. Performance evolution of KAR in Skyglow, Lagrange and Wavelet-Lagrange in both scenarios indoor and outdoor..

Figure7. Describes the randomness factor of the

generated key in all three conditions such as LoS, nLos , and mobility of devices. The ideal and maximum value of key entropy is 1. The maximization of the randomness factor reduces the risk of key amplification and provides secured authentication of devices. In this case, the randomness factors are almost identical to those used in existing methods for producing keys.

Discussion: The improved key generation techniques for the physical layer of IoT-based communication devices minimize the number of stages in the generation process while increasing the model's flexibility. The applied langrage's interpolation intercepts the RSS signal and converts it into a multi-bit form, reducing the possibility of error and noise. The applied wavelet transforms decompose the different levels of multi-bit signals into the binary format of key generation. The combination of langrage's and wavelet transform removes the problem of key generation methods such as quantization, formation of bit, and agreements of key for authorized node. The modified key generation methods also reduce the loss of data during the authentication process; hence the BER decreases in the modified key generation process. The modified key generation algorithm is better than the existing algorithm, such as Skyglow (SKG), langrage's interpolation, and wavelet concerning BER and KAR.

9. CONCLUSION

We approach in this paper, as well as a system present a wavelet transform-based efficient key generation process that eliminates the key generation system's pre-processing and error-correcting phases. Wavelet transform and Langrage's interpolation are used in the proposed algorithm. The langrage's interpolation distributes the received signal strength RSSI. The wavelet transforms sampled the RSSI distributed signal and generates the group of random factors. When compared to the existing approach, the proposed algorithm computes faster and has less transmission overhead across approved nodes. The proposed method efficiency evaluation takes place in two simulated environments: indoor and outdoor. That means two scenarios: one is with an obstacle and the other is without an obstacle. According to the results, the proposed method can produce a 128-bit key without any error- correction or pre-processing. The proposed algorithms validate all empirical parameters such as BER, KAR, KLR, and entropy. The maximum values of entropy indicate that the method presented handles high rate of random factors and decreases the possibility of differential time attacks and other signals-based attacks in wireless communication. The time complexity of the suggested method is $nlog(n)$, whereas the time complexity of the existing approach is $O(n^2)$.

References

[1] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[2] A. K. Kamboj, P. Jindal, and P. Verma, "Machine learning-based physical layer security: techniques, open challenges, and applications," *Wireless Networks*, vol. 27, no. 8, pp. 5351–5383, 2021.

[3] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 99–114, 2021.

[4] S. Balaji, K. Nathani, and R. Santhakumar, "Iot technology, applications and challenges: a contemporary survey," *Wireless personal communications*, vol. 108, no. 1, pp. 363–388, 2019.

[5] P. Jindal and B. Singh, "Performance analysis of modified rc4 encryption algorithm," in *International conference on recent advances and innovations in engineering (ICRAIE-2014)*. IEEE, 2014, pp. 1–5.

[6] S. S. Dhanda, B. Singh, and P. Jindal, "Wireless technologies in iot: Research challenges," *Engineering Vibration, Communication and Information Processing*, pp. 229–239, 2019.

[7] P. Jindal and B. Singh, "Analyzing the security-performance tradeoff in block ciphers," in *International conference on computing, communication & automation*. IEEE, 2015, pp. 326–331.

[8] J. Liu, P. Cuff, and S. Verdú, "Secret key generation with one communicator and a one-shot converse via hypercontractivity," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 710–714.

[9] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *Ieee access*, vol. 4, pp. 614–626, 2016.

[10] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2578–2588, 2016.

[11] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual ofdm subcarrier's channel response," in *2015 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2015, pp. 1–6.

[12] W. Sheng, S. Chen, G. Xiao, J. Mao, and Y. Zheng, "A biometric key generation method based on semisupervised data clustering," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 9, pp. 1205–1217, 2015.

[13] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based lte-a networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2424–2434, 2015.

[14] M. F. Haroun and T. A. Gulliver, "Secret key generation using chaotic signals over frequency selective fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1764–1775, 2015.

[15] X. Wang, J. Liu, X. Li, and Y. Li, "Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution," *IEEE Journal of Quantum Electronics*, vol. 51, no. 6, pp. 1–6, 2015.

[16] S. Kakkar, I. S. Makkar, and A. Mohapatra, "Secret key generation

using ofdm samples," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 4, pp. 439–454, 2015.

[17] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "8.7 physically unclonable function for secure key generation with a key error rate of 2e-38 in 45nm smart-card chips," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*. IEEE, 2016, pp. 158–160.

[18] N. Kannouf, M. Labbi, Y. Chahid, M. Benabdellah, and A. Azizi, "A key establishment attempt based on genetic algorithms applied to rfid technologies," *International Journal of Information Security and Privacy (IJISP)*, vol. 15, no. 3, pp. 33–47, 2021.

[19] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, 2016, pp. 1–12.

[20] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "Rss-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32–38, 2016.

[21] G. Panchal and D. Samanta, "Comparable features and same cryptography key generation using biometric fingerprint image," in *2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*. IEEE, 2016, pp. 691–695.

[22] G. Revadigar, C. Javali, W. Xu, W. Hu, and S. Jha, "Secure key generation and distribution protocol for wearable devices," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, 2016, pp. 1–4.

[23] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Gait-key: A gait-based shared secret key generation protocol for wearable devices," *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 1, pp. 1–27, 2017.

[24] M. A. Bahnasawi, K. Ibrahim, A. Mohamed, M. K. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail, and H. Mostafa, "Asic-oriented comparative review of hardware security algorithms for internet of things applications," in *2016 28th International Conference on Microelectronics (ICM)*. IEEE, 2016, pp. 285–288.

[25] J. Wan, A. Lopez, and M. A. A. Faruque, "Physical layer key generation: Securing wireless communication in automotive cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 2, pp. 1–26, 2018.

[26] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the internet of things from the layered context," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e3935, 2022.

[27] S. Gautam, A. Malik, N. Singh, and S. Kumar, "Recent advances and countermeasures against various attacks in iot environment," in *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*. IEEE, 2019, pp. 315–319.

[28] H. Abunahla, D. Shehada, C. Y. Yeun, B. Mohammad, and M. A. Jaoude, "Novel secret key generation techniques using memristor devices," *AIP Advances*, vol. 6, no. 2, p. 025107, 2016.

[29] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6213–6237, 2015.

[30] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for tdd-ofdm systems over fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176–5186, 2017.

[31] J. Huang and T. Jiang, "Secret key generation exploiting ultra-wideband indoor wireless channel characteristics," *Security and Communication Networks*, vol. 8, no. 13, pp. 2329–2337, 2015.

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

[33] K. Shankar and P. Eswaran, "An efficient image encryption technique based on optimized key generation in ecc using genetic algorithm," in *Artificial intelligence and evolutionary computations in engineering systems*. Springer, 2016, pp. 705–714.

[34] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, and C.-F. Chiasserini, "Secret key generation based on aoa estimation for low snr conditions," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–7.

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

Poonam Jindal Poonam Jindal received B.E degree in Electronics and Communication Engineering from Punjab Technical University, Punjab in 2003, M.E degree in Electronics and Communication Engineeringfrom Thapar University, Patiala in 2005 (India). She is working as Assistant Professor with Electronics and Communication Engineering Department, National Institute of Technology, Kurukshetra, India and completed her Doctoral Degree at National Institute of Technology, Kurukshetra, India. She has published 50 research papers in International/National journals andconferences. Her research interests include security algorithms for wireless networks and mobile communication. She is a member of IEEE

Brahmjit Sigh Brahmjit Singh as completed Bachelor of Engineering in Electronics Engineering from Malaviya National Institute of Technology, Jaipur, Master of Engineering with specialization in Microwave and Radar from Indian Institute of Technology, Roorkee and Ph.D. degree from GGS Indraprastha University, Delhi. He is with the Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra working as Professor having 24 years of teaching and research experience. He is currently serving as Dean PD and Regional Coordinator, Regional Academic Centre for Space at NIT Kurukshetra.He has held several administrative and academic positions in NIT Kurukshetra which include Chairman ECE Department, Chairman Computer Engineering Department, Professor in-Charge Centre of Computing and Networking, and Member Planning and Development Board. He was also incharge of Siemens Centre of Excellence at NIT Kurukshetra. He has published 100 research papers in International/National Journals and conferences, organized several conferences and short term courses. His current research interests include Wireless Sensor Networks, Cognitive Radio, and Security Algorithms for Wireless Networks and Mobility Management in wireless networks and planning designing of Mobile Cellular Networks. He has been awarded The Best Research Paper Award on behalf of 'The Institution of Engineers (India)'. He is the member of IEEE, Life member of IETE, and Life Member of ISTE.