sustainability

MDPI

Article

Sustainable Network by Enhancing Attribute-Based Selection Mechanism Using Lagrange Interpolation

Chetna Monga [1], Deepali Gupta [1], Devendra Prasad [2], Sapna Juneja [3], Ghulam Muhammad [4,*] and Zulfiqar Ali [5]

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, Punjab, India; chetna@chitkara.edu.in (C.M.); deepali.gupta@chitkara.edu.in (D.G.)
[2] Department of Computer Science and Engineering, Panipat Institute of Engineering & Technology (PIET), Samalkha, Panipat 132102, Haryana, India; devendra.prasad@chitkara.edu.in
[3] Department of Computer Science, KIET Group of Institutions, Delhi NCR, Ghaziabad 201206, Uttar Pradesh, India; sapnajuneja1983@gmail.com
[4] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[5] School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK; z.ali@essex.ac.uk
* Correspondence: ghulam@ksu.edu.sa

Abstract: The security framework in Ad-hoc Networks (ANET) continues to attract the attention of researchers, although significant work has been accomplished already. Researchers in the last couple of years have shown quite an improvement in Identity Dependent Cryptography (IDC). Security in ANET is hard to attain due to the vulnerability of links (Wireless). IDC encompasses Polynomial Interpolations (PI) such as Lagrange, curve-fitting, and spline to provide security by implementing Integrated Key Management (IKM). The PI structure trusts all the available nodes in the network and randomly picks nodes for the security key generation. This paper presents a solution to the trust issues raised in Lagrange's-PI (LI) utilizing an artificial neural network and attribute-based tree structure. The proposed structure not only improves the trust factor but also enhances the accuracy measures of LI to provide a sustainable network system. Throughput, PDR, noise, and latency have been increased by 47%, 50%, 34%, and 30%, respectively, by using LI and incorporating the aforementioned techniques.

Keywords: Polynomial Interpolations; security; sustainable ad-hoc networks; Lagrange's approach; reliability

Citation: Monga, C.; Gupta, D.; Prasad, D.; Juneja, S.; Muhammad, G.; Ali, Z. Sustainable Network by Enhancing Attribute-Based Selection Mechanism Using Lagrange Interpolation. *Sustainability* **2022**, *14*, 6082. https://doi.org/10.3390/su14106082

Academic Editors: Saqib Iqbal Hakak and Thippa Reddy Gadekallu

Received: 28 March 2022
Accepted: 12 May 2022
Published: 17 May 2022

1. Introduction

Ad-hoc Networks (ANETs) are infrastructure-free, self-contained wireless framework networks that have piqued the interest of both academics and industry professionals. This provides a great opportunity to increase affordability, consistency, reliability, flexibility, anonymity, and compatibility around the world [1]. The security architecture is indispensable considering typecast applications. As the hackers are smart enough to avoid traditional security measures, the previously utilized security systems are no longer sufficient [2]. Dozens of features complicate security design in ANET [3]. These features include the shared medium of wireless topology, the dearth of infrastructure, motile nodes, and limitations of bandwidth [4]. In this paper, our main concern is key management (KM), which is the understructure of the security framework in ANET [5]. There is considerable literature available on Public Key Infrastructure Management (PKIM) presented in [6]. A standard security protocol in PKIM is that a sender transfers an encrypted message to the receiver utilizing a public or secret key, which is shared between them [7]. Following a set of rules, the sender creates a cipher specifically for the receiving node [8]. If there are

p receivers, the sender must generate p different ciphers for the message containing the same body. The multi-receiver scheme substantially reduces the computation cost at the sender rotocolend. This paper focuses on the selection of the receiver node by applying the Attribute-Based Selection Mechanism (ABSM). The ABSM has the edge over PKIM as it achieves one-to-many communications rather than one-to-one communication [9]. Lagrange's Polynomial Interpolation (LI) is integrated into the ABSM for crucial computation.

Remote channel correspondence ensures that the transmitter and beneficiary produce the key from its media. Nonetheless, numerous hindrances in genuine situations make a common estimation pattern of various transceivers that are related to inconsistencies. Along these lines, when estimations can provide a bit sequence, one may see a dazzling bit mismatch rate, and as a result, the ability and security of establishing a security key may be compromised as some data may be revealed during agreement [10]. A good key generation technique should be able to prevent these problems. Curve fitting is now utilized to preprocess estimations during key generation to ensure that the outputs are superior to the initial channel estimation. Now, to reduce bit mismatch, sequences are generated. A shared bit sequence can also be extracted by interactive cascade during information recollection. For privacy amplification, two hashing functions are implemented, and randomness in the shared key is guaranteed [10].

Secret-key generation for any transaction has been an essential task for which the randomness of wireless networks is considered [11]. According to an experiment, two transceivers experience almost the same state of the channel when measured within a consistent time. On the other hand, the channel state becomes inconsistent when the distance is half the wavelength. Now, this results in the involvement of transceivers to use these medium states to generate a secret key. In the mentioned case, it is assumed that there are no limitations to eavesdropping on computational resources. The fundamental factor is variation in the channel, which influences the key generation process as the arbitrariness for the essential generation is considered by the channel variation. The channel variation also affects the reciprocity of the channel measurements. So, the authors in [12] used different statistics to hinder channel states. RSS (Received Signal Strength) is used in many schemes to generate the key. Such schemes are also available in different scenarios such as an increase in the size of the network [13] or mobile, in which many channel variations are assured by the movement of intermediate objects or entities. This means that such solutions are incapable of static scenarios without a considerable channel variation. In addition to all the other ways for key generation, other statistics such as CIR (Channel Impulse Response) and AOA (Arrival Of the Angel) should be investigated. In the case of different schemes, the selection of statistics is done for key generation, and it is dependent upon efficiency, requirements, the environment of the application, and complexity related to implementation. For example, due to its having less channel variation, it is challenging to extract random bits from RSS, whereas in many schemes where channel variation is significant, it guarantees key generation.

The contributions of this paper are as follows. Curve fitting and the Fourier transform are used in the proposed method to improve the effectiveness of the key generation process. Additionally, route discovery methods are built, and a node deployment architecture is explained to boost security. This paper is structured in the following manner: Section 2 introduces the ABSM framework. The execution procedures are covered in the same section. Section 3 presents the analysis of the results, and Section 4 concludes the study.

2. Related Work

Authors in [14,15] discussed the feasibility of generating the key. The literature provides the analysis for key generation from theoretical concepts, and according to it, an assumption is made that X, Y would be random variables, and Z would be an adversary. Many schemes are proposed practically to generate the key. Many schemes are proposed to extract secret keys from RSS, as it is supportive for most devices. In [16], a scheme is proposed which suggested two-level execution for generating security bits for this

CIR, and RSS is used to perform validation. Now, the results show the feasibility of this scheme. Authors in [17] suggested an environment scheme for the extraction of secret keys from RSS in a wireless channel. The measurement sequence is divided into blocks, and a two-level quantifier is employed to carry out the plan. Several real-world trials are conducted to guarantee that the suggested plot is approved. The results of the experiments reflected that the scheme produces high entropy bits at an extremely high rate in contrast with different plans. Authors in [18] proposed another scheme for bit extraction in wireless sensors. In the process of key generation, ranking mechanisms and interpolation are executed to remove non-reciprocities that are caused due to different inferences. After this, authors in [19] proposed the technique based on the KLT (Karhunen–Loeve Transform), which is applied for the removal of time-based correlation obtained from the RSS fading signal. In the last stage to produce shared secret bits for transceiver multi-bit, versatile quantization and grey code are utilized. The results show that this approach generates a secret key quickly. The complexity of the key generation increases as KLT is implemented. Aside from these different schemes, which are additionally proposed for secret-key generation from RSS, it is proposed that CSI (channel state information) performs better compared to RSS [20]. Various schemes prefer CSI over RSS for achieving effective key generation. Although both schemes perform efficiently, some devices do not support CSI without modification. Authors in [21] proposed angle-of-arrival for signature key extraction. Elevation angles are additionally utilized for laying out a secret key to expand the proficiency of key generation. Authors in [22] proposed that the chaotic signals are preferred over frequency selective fading channel for key generation. The phase reciprocity uses of multicarrier communication systems resulted in security key generation. Presently, according to experiments conducted in existing schemes, information gathered from transceivers is not indistinguishable and has disparities. Some of these discrepancies cause bit mismatches, and as suggested earlier in the paper, key-generation security and its efficiency are affected by this mismatch. It is suggested that pre-processing of the channel should be performed to reduce the bit mismatch rate. This review has been compiled in Table 1.

Table 1. Technique Used.

Sr. No.	References	Technique Used
1	[14]	RSS
2	[15]	RSS
3	[16]	two-level execution using CIR and RSS
4	[17]	Blocks and a two-level quantifier
5	[18]	Key generation ranking mechanisms and interpolation
6	[19]	Technique based on the KLT (Karhunen-Loeve Transform)
7	[20]	CSI (channel state information)
8	[21]	Angle-of-arrival for signature key extraction
9	[22]	Chaotic signals

3. Building Blocks of ABSM

We first present the definition and model of ABSM.

Definition 1: *ABSM architecture has three algorithms (Tree Setup, Cross-Validation, Node Selection using Interpolation), which are defined by their definitions as follows.*

Tree Setup: This algorithm considers that the nodes of the current network C_n are already secured; hence, validation is required for the request of other relative networks O_n. The demanding node d_n from the O_n requests the sender S_n of C_n. To validate d_n, S_n

builds a tree structure by applying the Zig-Zag rule. The S_n takes the d_n as the first node. S_n identifies the nearby nodes of d_n by applying the distance formula.

$$dist = (x_{s_n} - x_p)^2 + (y_{s_n} - y_p)^2 \quad (1)$$

As per the LI's second-order mechanism, three different nodes are required for verification. For d_n, S_n will follow the Right-Left mechanism. The nearest right node (R_n) of the d_n followed by the nearest node of R_n will be the first consideration. The S_n will ask for the share.

The Fog Server will request three options from any node in the network and choose two at random whenever a node requests data from a server, whether directly or through RSU. Three shares, including the asking node, will be examined in total. The Fog will compute the following using Lagranges' polynomial $S(x)$ having degree $\leq (n-1)$, which requires k number of nodes with coordinates (x_1, $y_1 = f(x_1)$), (x_2, $y_2 = (x_2)$), . . . , (x_n, $y_n = f(x_n)$), which is given by Lagrange polynomial as

$$S(x) = \sum_{j=1}^{n} S_j(x) \quad (2)$$

where

$$S_j(x) = y_j \prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{x - x_k}{j^{x_j - x_k}} \quad (3)$$

If written explicitly for $n = 3$ nodes:

$$S(x) = \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} y_1 + \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} y_2 + \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} y_3 \quad (4)$$

The different polynomial can also be determined, which is known as Lagrange's basic interpolation.

$$S(x_1) = \frac{x_2 \times x_3}{(x-x_2)(x-x_3)} y_1 \text{ for first node} \quad (5)$$

$$S(x_2) = \frac{x_1 \times x_3}{(x_1-x_2)(x_1-x_3)} y_2 \text{ for sec ond node} \quad (6)$$

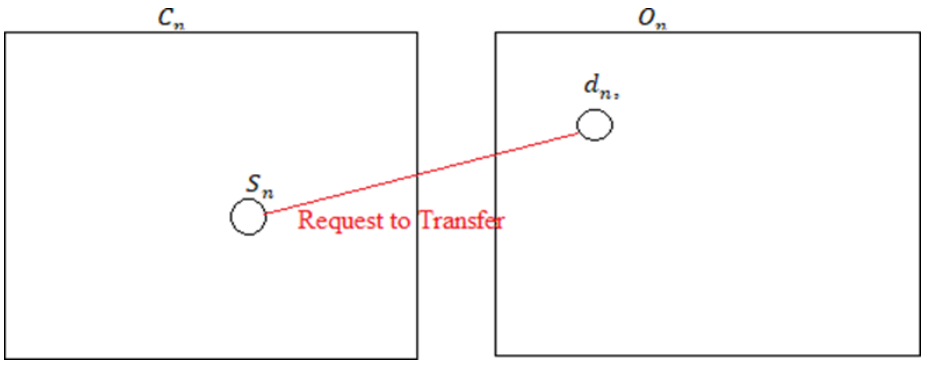
$$S(x_3) = \frac{x_1 \times x_2}{(x_1-x_2)(x_1-x_3)} y_3 \text{ for third node} \quad (7)$$

When the Fog server provides data to the node, only then does G_k match the network key. Second, security at the RSU level is added, making the network more secure. The pseudo-code is also supplied to help demonstrate how this security is constructed.In Figure 1a, d_n is requesting for the shared key from S_n and in Figure 1b, a tree type structure is formed to transfer the shared key from left right nodes.

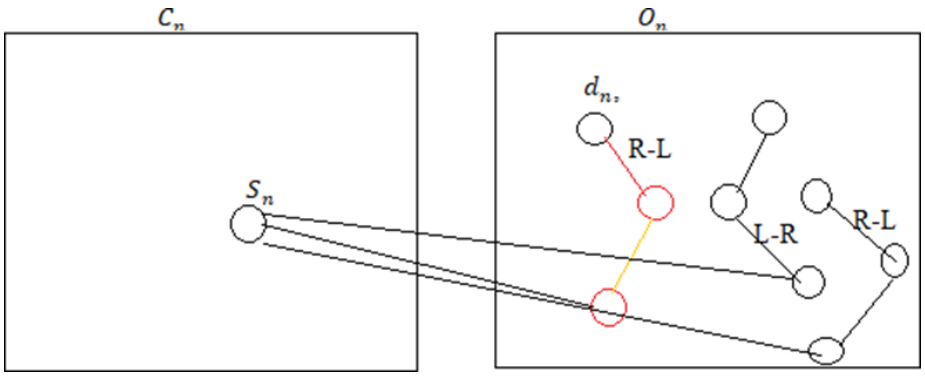
The interpolation order 2 is used in the Algorithm 1. Only three nodes will be chosen for correspondence. Whether or not the nodes will be chosen for the information correspondence rests on the ultimate key outcome, which is determined using Lagrange's approach. A numerator and a denominator are required in one key generation approach. The network id of nodes that are left for iteration determines the numerator. Consider the nodes 45, 53, 61 as an example of the verification nodes. The numerator value (Num) for 45 is thus $53 \times 61 = 3233$. The remaining nodes' network ids are multiplied to obtain the denominator (deno). The deno value for the number 45 is $(45 - 53) \times (45 - 61) \rightarrow (-8) \times (-16) \rightarrow 128$. The verification key would be the result of the shared key of 45 to Num. DenoSharedkey will be calculated in the same way for 53 and 61. The final verification key would be the total of all the produced verification keys.

$$Final_{key} = \sum_{k=0}^{i} My_{value} \quad (8)$$

The corresponding nodes are chosen if the Final key is the same as the network security key. The Lagrange theorem chooses a node for verification at random, although the Lagrange confirmation process works well.



(**a**)



(**b**)

Figure 1. (**a**) d_n requesting to S_n; (**b**) Tree Setup.

Algorithm 1 Share Verification Pseudo Code

(1) Order = 2; // order of Interpolation
(2) My_{VALUE} = [ ] // Empty value be initialized
(3) *For* x = 1: 3 // For 3 nodes
token = 1;
$Current_1 = Node_{ID}I$ // Using the first node as a starting point
(4) for y=1: Nodes;
Current = $Vehicles_j$; // There would be two Rest Nodes for each interpolation.
if $Current_1$~ = Current // If nodes are not equal
Rest(token) = current;
Token = token + 1;
End If
(5) End
(6) For *Deno* = 0
(7) $Deno = Current_1 - Rest_1 * Current_1 - Rest_2$ // The denominator value
(8) Num = $Rest_1 * Rest_2$
(9) $My_{value}[x]$ = Num/ Deno
(10) $Shared_{key} = Share_{Current1} * My_{value}[x]$
(11) End For

4. Curve Fitting

The fundamental purpose of curve fitting is to develop a mathematical function or curve that finds the best match for a given data set. Both interruption and smoothing are curve fitting methods, with interruption concentrating on organizing the approximate fit and smoothing on sorting out the correct fit to the data. Curve fitting is employed to build the effectiveness of key creation in this research, and smoothing is recommended for capturing significant information from the given data set while also reducing noise and distinct variances. According to the analyses, the estimation sequence for multiple transceivers is unequivocally connected, which implies that the essential example in these arrangements is comparative.

However, these sequences also have inconsistencies that are brought about by small variations. Presently, transceivers are independently applied as a similar relieving cycle to these estimations. The exchange of processed aspects brings about an arrangements upgrade as a portion of the errors are diminished. Furthermore, by generating bit sequences for transceivers from these processed measures, the mismatch between sequences is reduced, and data gathering proficiency can be improved. Moving average, smoothing spline, and Savitzky–Golay smoothing are examples of smoothing techniques. Pre-process computing is carried out in the experiments utilizing Fourier series fitting and a simple moving average.

4.1. Fourier Series Fitting (FST)

For complex exponential functions or the sum of simple sine functions, the Fourier series is used. Authors in [23] define a function *f(a)* on the interval [−l, l], as follows:

$$f(a) = a_0/2 + \Sigma\infty\ n = 1\ an\ cos\ n\Pi a/l + \Sigma\infty\ n = 1\ bn\ sin\ n\Pi a/l \tag{9}$$

The coefficient can be constructed by calculating the integral of Equation (4):

$$a_0 = \frac{1}{1\int_{1-1}^{1} f(x)dx} \tag{10}$$

$$a_n = \frac{1}{1\int_{1-1}^{1} \frac{f(x)cosn\pi x}{1dx}} \tag{11}$$

$$a_n = \frac{1}{1\int_{1-1}^{1} \frac{f(x)sinn\pi x}{1dx}} \tag{12}$$

The constant term in the equation is $a_0/2$, while the others are known as periodic terms. The finite summation is used when the Fourier series is applied to a given function. An equation is given below to calculate the partial sum.

$$\int_{N}(a) = \frac{a_0}{2} + \sum_{n=1}^{N} a_n \frac{cosn\pi x}{1} + \sum_{n=1}^{N} a_n \frac{sinn\pi x}{1} \tag{13}$$

As N grows larger, the fractional total becomes more approximate [13]. When N exceeds, the incomplete sum is transformed into a Fourier series of the function. The partial sum of measure and partial sum reconstruct measure are determined. The secret key for each transceiver is created using the replicated arrangement. The curve of a reconstructed sequence of various transceivers for those with similar variance with various ranges is shown in the results. We focus on the effects of Fourier series fitting mutual data and Spearman correlation coefficients of sequences with varying numbers of words. The Spearman correlation coefficient and the correlation coefficient are crucial. When a smaller number of terms are used to replicate measurements, the exchange is updated. In the instance of the 3-term Fourier series, the Spearman link coefficient and the Fourier series

fitting shared data are both high. The Fourier series is used to eliminate pre-handling metric inconsistencies.

4.1.1. Computation Complexity

For a ($0 \leq n \leq N$) and b ($1 \leq n \leq N$), the equation needs to be computed for further calculation of the partial sum of the given data. According to the DFT (Discrete Fourier Transform) and Fourier series relation, the partial sum is to be calculated.

4.1.2. Randomness

To reduce scale rapid variation, the randomness of the measurement sequence is used. Due to quantization, many small variations are eliminated even though the Fourier series is not used. For the unpredictability of the key, and to produce the mismatch that affects the key's formation, some variables are regarded as worthless. The produced key's unpredictability is ensured through amplification. Even though their dimensions are pre-processed by various curve fitting procedures, the NIST test addresses the fact that the key can secure the correspondence between transceivers.

4.2. Moving Average (Simple)

To calculate multiple series of averages from different subsets of a larger data set, the moving average is one of the most commonly used smoothing techniques. To reduce small-scale changes, a moving average is utilized. The application is used to determine the threshold. Three moving average techniques have been developed: Cumulative Moving Average (CMA), Exponential Moving Average (EMA), and Simple Moving Average (SMA). The SMA of the provided information is computed using [14].

$$\mathrm{SMA} = \mathrm{dM} + \mathrm{dM} - 1 + \ldots\ \mathrm{dM} - (n-1)/n = 1/n\ \Sigma^{\mathrm{n}-1}\ \mathrm{I} = 0\ \mathrm{dm} - \mathrm{I} \tag{14}$$

D ($1 \leq \mathrm{I} \leq n - 1$) Previous n-1 data is denoted by M-i. SMA smoothing is accomplished by swapping components with an average of $n - 1$ neighbors and itself, and it has minimal complexity compared to other moving average approaches. In Equation (9), n denotes the SMA window size.

4.2.1. Computation Intricacy

In Equation (14), the SMA is carried out by computing the series average. In the proposed study, the SMA is utilized for smooth, collected estimations. The computation of N rounds of n-range results in N estimations. The SMA represents a simple moving average, and n stands for average range.

4.2.2. Randomness

The Fourier series is fitting simply in the same way. SMA eliminates small-scale variations of estimations. The privacy amplification ensures the randomness of the secret key. The NIST randomness test produces a secret key that can secure correspondence between transceivers. The exchange can be improved, and channel measurements are handled by Fourier series fitting and simple moving average processes [24].

The proposed work algorithm aims to minimize the network losses through the selection of the appropriate node at the right time of the processing [25]. The interpolation is used to decrease the waste time of the network so that the data are processed more smoothly. The other network model is as follows.

4.2.3. Setup

The setup has been implemented by deploying the nodes, and the nodes' properties have been initialized. The pseudocode for the node deployment and its setup is given as follows:

Pseudocode 1: *Node Setup and its Deployment*
Network_Wisth = 2500 *m*
Network_Length = 2500 *m*
Location Initialization of nodes such as m and n
SetupEnergy = *AssociatedEnergy*
TransmissionDelay = *TransmissionNew Delay*
Packet_Dump = *Setup*
Node Deployment
End

The proposed network setup and deployment of the nodes work in a heterogeneous environment. Thus, different parameters in the network for each node have been assigned with different quantities. Therefore, it is essential to design the network and deploy the nodes by some primary values which work as fuel for them. These values are different for various nodes, and delay has been assumed after some time with the packet dump value. However, the range of communication has been computed and evaluated using Algorithm 2:

Algorithm 2 Communication range prediction (*Nodes*, *m*, *n*, *Nodeid*)

CommunicationPrediction = []
For node 1 *in environment*
For node 2 *in environment*
When node ∂ = *node* 1
$D = \sqrt{}$ [(*node*) − *M*(*node*1)]2 + [*N*(*node*) − *N*(*node*1)]2
Predict the coverage (*node*, *node*1) = $Node_i$(*node*1)
End_For
End_For
End Algorithm 1

The distance between the nodes is computed using the communication range prediction algorithm as described above. The rough model of the Algorithm 2 is given in Figure 2.

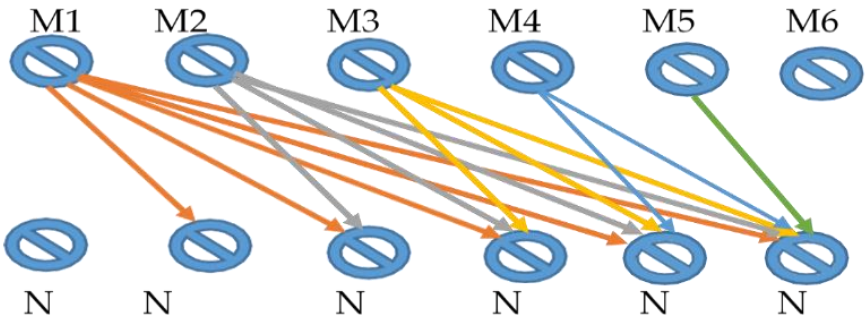


Figure 2. Communication between nodes.

4.2.4. Route Discovery

The architecture of routing is made by different nodes. Algorithm 3 demonstrates the functioning of the route discovery.

Algorithm 3 Route Dicovery

Input: Source at Transmission and Destination at Receiving end
Send Message = Send ('Hi')
For each responder of Send Message
Compute Requirements of the route = ();
Choose Node (*Hi*);
If reply comes back then
Add Route
EndIF
Repeat the step until destination dose not found
EndFor
End Algorithm

Algorithm 3 sends the Hi message in the network and waits for the response. The nodes respond to this message only, which goes under the correspondence range as assessed by the above algorithm. Subsequently, this paper presents an answer to the route discovery system and node correspondence in the network.

5. Results and Discussion

The results and comments are presented in this section, in which various attributes such as throughput, Noise (Jitter), Packet Delivery Ratio (PDR), and delay have been considered to determine the adequacy of the proposed structure.

- **Throughput:** Throughput is known as the ratio of total packets received at the destination end per unit time. In mathematical terms, it is written as follows:

$$\text{Throughput} = \frac{\text{Total packets at the destination}}{\text{time}}$$

- **PDR:** defined as the ratio of the total number of packets received from targets to packets generated by source nodes on the transmission side, the PDR is calculated using the following mathematical formula:

$$\text{PDR} = \frac{\text{Data packet received from the targets}}{\text{Data packet from the source end}}$$

Noise and disruption have an impact on the network's performance. It is effectively the ratio of total generated delay to spectrum value fluctuation.

Table 2 lists the throughput of the proposed work with LI and without LI. Primarily, it is observed that the average throughput with LI is 22,860 and without LI, it is 12,000. The range of throughput with LI lies between 22,000 to 23,800. However, without LI, it lies between 11,000 to 13,000.

Table 2. Computation of Throughput.

Number of Iterations	Throughput without LI	Throughput with LI
50	11,000	22,000
100	11,500	22,500
150	12,000	23,000
200	12,500	23,500
250	13,000	23,800

Figure 3 illustrates that the throughput rate of the proposed technique with LI is better than without LI. Thus, the overall throughput rate has been improved by 47% when Lagrange has been incorporated into the proposed architecture. However, curve fitting and Fourier series transform help enhance the throughput by computing the required parameters for the proposed work. In addition, the increased throughput rate shows that

the PDR is also high, and there is low fuel consumption, which enhances the performance of the network [26].

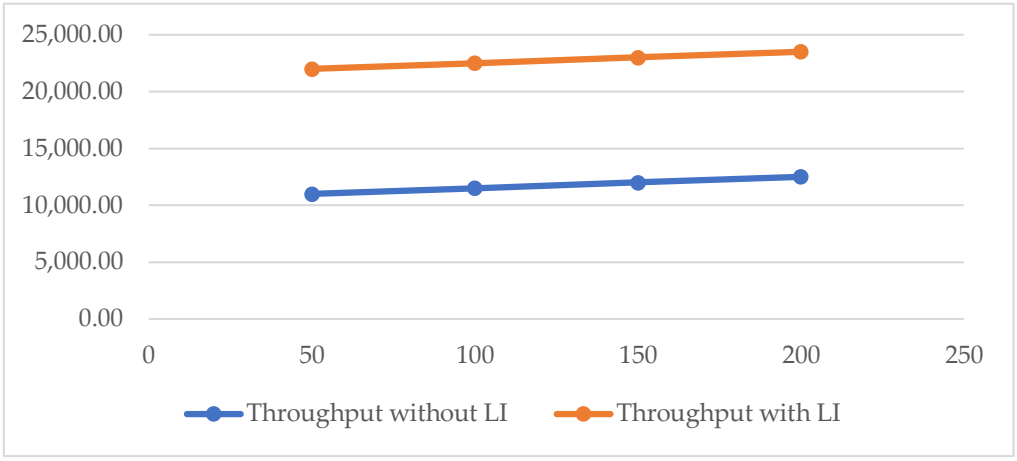


Figure 3. Throughput rate.

The PDR of the proposed work with Lagrange and without Interpolation architecture is shown in Table 3. The results show that the average PDR without LI comes in the range of 0.34 to 0.4. However, the PDR lies in the range of 0.71 to 0.79 with LI. Thus, the average computed PDR with Interpolation architecture is 0.74 and without LI, it is 0.37. Thus, improved results have been obtained through the proposed work without LI.

Table 3. PDR.

Total Number of Iterations	PDR without LI	PDR with LI
50	0.34	0.71
100	0.36	0.72
150	0.38	0.74
200	0.41	0.76
250	0.4	0.79

Figure 4 depicts the PDR performance over different iterations. The proposed work has been compared without Interpolation architecture [27,28]. The PDR with LI remains constant for 50 to 100 simulations. It rises to 0.8 for 100 to 250 iterations. However, the PDR without LI is 0.37 for 50 to 100 simulations, but then it remains constant from 150 to 250 simulations. Thus, overall improved results have been attained and the PDR has been revamped by 50% in comparison to when it is without Interpolation architecture.

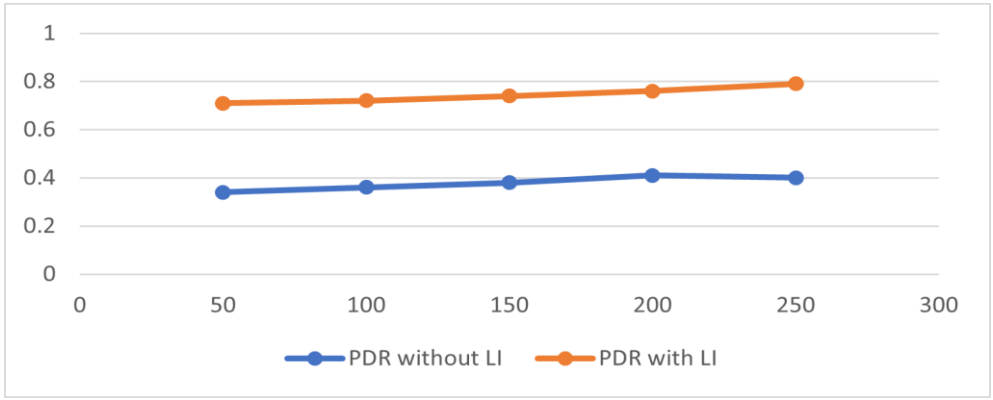


Figure 4. PDR vs. the number of iterations.

Table 4 shows the incidence of disturbance and noise in the heterogeneous environment. The noise has been computed in seconds [29]. Noise for 50 to 250 simulations lies in the range of 0.26 to 0.39. However, in the case of the proposed structure, it lies in the range of 0.16 to 0.27 s. Similarly, for 300 to 450 simulations without LI structure, it rises to 0.42 s. In the case of the proposed framework with LI, it reduces to 0.21. The average jitter without LI is 0.35 and with LI, it is 0.23. Thus, the performance of the proposed framework has been improved by incorporating LI.

Table 4. Noise occurrence.

Total Number of Simulations	Noise without LI	Noise with Proposed Methodology Incorporating LI
50	0.26	0.16
100	0.25	0.22
150	0.31	0.24
200	0.36	0.26
250	0.39	0.27
300	0.4	0.27
350	0.41	0.23
400	0.42	0.21
450	0.42	0.21

Figure 5 illustrates the incidence of the noise of the proposed work with LI and without LI. The performance of the proposed work has been improved by 34%. The average jitter increases over different simulations without LI. However, the proposed framework shows that noise increases from 50 to 300 simulations, and then further falls from 300 to 450 simulations. Thus, noise falls in the range of 0.16 to 0.21.

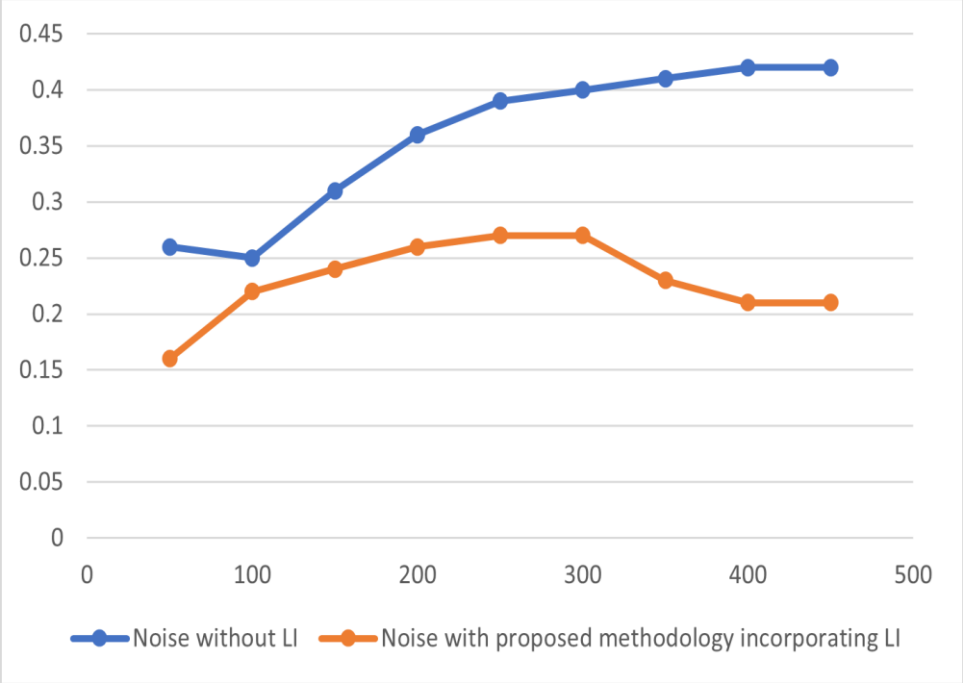


Figure 5. Noise vs. the number of iterations.

Table 5 depicts the delay that is introduced into the network. The delay reduces the performance of the system and hampers the network lifetime. The delay [30] imposed in the proposed work with Interpolation architecture has been minimized, and it now ranges from 0.34 to 0.3 s. However, without LI, the delay has been increased [31] over different

simulations. The delay occurs in the range of 0.42 to 0.55 s, and the average delay is 0.46, and with LI, it is 0.32 s.

Table 5. Delay.

Iterations	Delay without LI (Seconds)	Delay with LI (Seconds)
50	0.42	0.34
100	0.43	0.33
150	0.44	0.33
200	0.55	0.32
250	0.44	0.31
300	0.5	0.3

Figure 6 shows that the delay without LI and delay with LI varies. The proposed approach appears to perform better than the architecture without interpolation [32–34]. This framework shows that the delay decreases from 50 to 300 simulations with LI, and it increases with interations without LI [35–37].

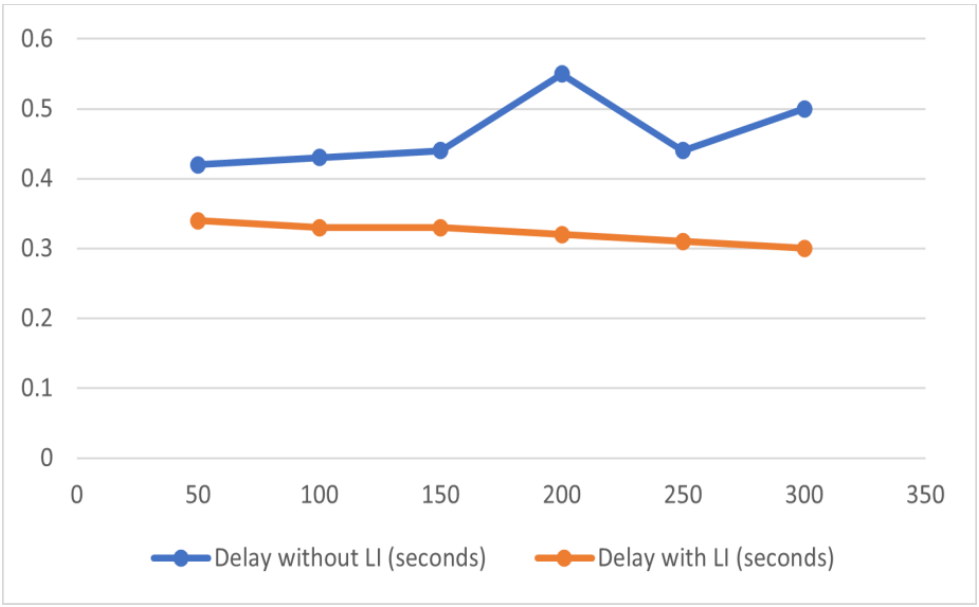


Figure 6. Delay.

In comparison to the work conducted without LI architecture, the total performance of the proposed work has improved by 30%. Thus, effective results have been attained by incorporating the Interpolation architecture in the proposed work.

6. Limitation and Future Directions

However, the proposed work has a built-in computational overhead. The associated storage and processing cost in a typical ABSE method varies linearly with the number of attributes possessed by a user. Sometimes, due to resource constraints, devices should not perform computationally complex tasks such as those included in a conventional ABSE scheme on their own, instead of relying on other technologies such as blockchain technology, which can enhance both flexibility and system overhead [28]. It also reduces processing overhead as the task of system initialization is not the duty of a single entity in the blockchain-assisted searchable encryption system [29]. Decentralization improves system reliability and eliminates the possibility of a single point of failure [30]. Specific and

specialized learning models created expressly for security objectives are also required. In the future, new learning techniques for detecting new network threats can be developed.

7. Conclusions

This study proposes a resilient system that uses the Lagrange Interpolation architecture to improve security in the ANET by producing security keys. To optimize the effectiveness of the key generation process, the suggested method utilizes curve fitting and the Fourier transform. In addition, route discovery methods are constructed, and a node deployment architecture is developed to improve security. In terms of throughput, latency, jitter, and PDR, the suggested framework outperforms the architecture without interpolation, according to the testing results. The high throughput indicates a high PDR, which not only improves network security but also increases speed and feasibility. Throughput, PDR, noise, and delay have all been improved by 47%, 50%, 34%, and 30%, respectively. The regular ABSE scheme can be amalgamated with Blockchain technology systems to enhance its benefits.

Author Contributions: Conceptualization, C.M., D.G. and D.P.; methodology, C.M. and S.J.; software, S.J. and G.M.; validation, C.M., D.G. and D.G.; formal analysis, C.M., S.J., G.M. and Z.A.; investigation, S.J. and G.M.; resources, S.J. and G.M.; data curation, Z.A.; writing—original draft preparation, C.M., D.G. and D.P.; writing—review and editing, G.M. and Z.A.; supervision, S.J. and Z.A.; project administration, G.M.; funding acquisition, G.M. All authors have read and agreed to the published version of the manuscript.

Funding: The work is funded by Researchers Supporting Project number (RSP-2021/34), King Saud University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their appreciation to Researchers Supporting Project number (RSP-2021/34), King Saud University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Badawy, A.; Khattab, T.; El-Fouly, T.; Mohamed, A.; Trinchero, D.; Chiasserini, C.-F. Secret Key Generation Based on AoA Estimation for Low SNR Conditions. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, Scotland, 11–14 May 2015; pp. 1–7.
2. Muhammad, G.; Hossain, M.S. Deep-Reinforcement-Learning-Based Sustainable Energy Distribution for Wireless Communication. *IEEE Wirel. Commun.* **2021**, *28*, 42–48. [CrossRef]
3. Balaji, N.A.; Sukumar, R.; Parvathy, M. Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network. *Comput. Electr. Eng.* **2019**, *76*, 94–110. [CrossRef]
4. Muhammad, G.; Alhussein, M. Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. *IEEE Consum. Electron. Mag.* 2022; *Early Access*. [CrossRef]
5. Cho, J.H.; Chen, R.; Chan, K.S. Trust threshold based public key management in mobile ad hoc networks. *Ad Hoc Netw.* **2016**, *44*, 58–75. [CrossRef]
6. Cui, H.; Deng, R.H.; Wang, G. An attribute-based framework for secure communications in vehicular ad hoc networks. *IEEE/ACM Trans. Netw.* **2019**, *27*, 721–733. [CrossRef]
7. Das, A.K.; Kumari, S.; Odelu, V.; Li, X.; Wu, F.; Huang, X. Provably secure user authentication and key agreement scheme for wireless sensor networks. *Secur. Commun. Netw.* **2016**, *9*, 3670–3687. [CrossRef]
8. Datta, P.; Sharma, B. A Survey on IoT Architectures, Protocols, Security and Smart City Based Applications. In Proceedings of the 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 3–5 July 2017; pp. 1–5.
9. Yuliana, M. A simple secret key generation by using a combination of pre-processing method with a multilevel quantization. *Entropy* **2019**, *21*, 192. [CrossRef]
10. Alshehri, F.; Muhammad, G. A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. *IEEE Access* **2021**, *9*, 3660–3678. [CrossRef]

11. Robinson, Y.H.; Julie, E.G. MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks. *Wirel. Pers. Commun.* **2019**, *109*, 739–760. [CrossRef]
12. Haroun, M.F.; Gulliver, T.A. Secret key generation using chaotic signals over frequency selective fading channels. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1764–1775. [CrossRef]
13. Hassan, M.U.; Shahzaib, M.; Shaukat, K.; Hussain, S.N.; Mubashir, M.; Karim, S.; Shabir, M.A. DEAR-2: An energy-aware routing protocol with guaranteed delivery in wireless ad-hoc networks. In *Recent Trends and Advances in Wireless and IoT-Enabled Networks*; Springer: Cham, Switzerland, 2019; pp. 215–224.
14. Huang, Y.; Jin, L.; Wei, H.; Zhong, Z.; Zhang, S. Fast secret key generation based on dynamic private pilot from static wireless channels. *China Commun.* **2018**, *15*, 171–183. [CrossRef]
15. Alam, T.M.; Shaukat, K.; Hameed, I.A.; Khan, W.A.; Sarwar, M.U.; Iqbal, F.; Luo, S. A novel framework for prognostic factors identification of malignant mesothelioma through association rule mining. *Biomed. Signal Process. Control* **2021**, *68*, 102726. [CrossRef]
16. Javed, I.; Tang, X.; Shaukat, K.; Sarwar, M.U.; Alam, T.M.; Hameed, I.A.; Saleem, M.A. V2X-based mobile localization in 3D wireless sensor network. *Secur. Commun. Netw.* **2021**, *2021*, 6677896. [CrossRef]
17. Jose, R.T.; Poulose, S.L. Ontology Based Privacy Preservation over Encrypted Data using Attribute-Based Encryption Technique. *Adv. Sci. Technol. Eng. Syst. J.* **2021**, *6*, 378–386. [CrossRef]
18. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 33–39. [CrossRef]
19. Muhammad, G.; Alshehri, F.; Karray, F.; El Saddik, A.; Alsulaiman, M.; Falk, T.H. A comprehensive survey on multimodal medical signals fusion for smart healthcare systems. *Inf. Fusion* **2021**, *76*, 355–375. [CrossRef]
20. Moara-Nkwe, K.; Shi, Q.; Lee, G.M.; Eiza, M.H. A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. *IEEE Access* **2018**, *6*, 11374–11387. [CrossRef]
21. Rathore, S.; Agrawal, J.; Sharma, S.; Sahu, S. Efficient Decentralized Key Management Approach for Vehicular Ad Hoc Network. In *Data, Engineering and Applications*; Springer: Singapore, 2019; pp. 147–161.
22. Shaukat, K.; Luo, S.; Chen, S.; Liu, D. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Norfolk, VA, USA, 12–13 March 2020; pp. 1–6.
23. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Chen, S.; Liu, D.; Li, J. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
24. Shehadeh, Y.E.H.; Hogrefe, D. A survey on secret key generation mechanisms on the physical layer in wireless networks. *Secur. Commun. Netw.* **2015**, *8*, 332–341. [CrossRef]
25. Strauss, M.A.; Yahil, A.; Davis, M.; Huchra, J.P.; Fisher, K. A redshift survey of IRAS galaxies. V-The acceleration on the Local Group. *Astrophys. J.* **1992**, *397*, 395–419. [CrossRef]
26. Wang, T.; Liu, Y.; Vasilakos, A.V. Survey on channel reciprocity based key establishment techniques for wireless systems. *Wirel. Netw.* **2015**, *21*, 1835–1846. [CrossRef]
27. Xiao, S.; Guo, Y.; Huang, K.; Jin, L. Cooperative group secret key generation based on secure network coding. *IEEE Commun. Lett.* **2018**, *22*, 1466–1469. [CrossRef]
28. Zaman, S.; Chakraborty, C.; Mehajabin, N.; Mamun-Or-Rashid, M.; Razzaque, M.A. A Deep Learning based device authentication scheme using channel state information. In Proceedings of the 2018 International Conference on Innovation in Engineering and Technology (ICIET), Dhaka, Bangladesh, 27–28 December 2018; pp. 1–5.
29. Zhan, F.; Yao, N. On the using of discrete wavelet transform for physical layer key generation. *Ad Hoc Netw.* **2017**, *64*, 22–31. [CrossRef]
30. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. [CrossRef] [PubMed]
31. Kanwal, S.; Rashid, J.; Kim, J.; Juneja, S.; Dhiman, G.; Hussain, A. Mitigating the Coexistence Technique in Wireless Body Area Networks by Using Superframe Interleaving. *IETE J. Res.* **2022**, 1–15. [CrossRef]
32. Shao, C.; Yang, Y.; Juneja, S.; Gseetharam, T. IoT data visualization for business intelligence in corporate finance. *Inf. Process. Manag.* **2022**, *59*, 102736. [CrossRef]
33. Upadhyay, H.K.; Juneja, S.; Maggu, S.; Dhingra, G.; Juneja, A. Multi-criteria analysis of social isolation barriers amid COVID-19 using fuzzy AHP. *World J. Eng.* **2022**, *19*, 195–203. [CrossRef]
34. Roy, A.K.; Nath, K.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Privacy Preserving Multi-Party Key Exchange Protocol for Wireless Mesh Networks. *Sensors* **2022**, *22*, 1958. [CrossRef]
35. Dev, K.; Maddikunta, P.K.R.; Gadekallu, T.R.; Bhattacharya, S.; Hegde, P.; Singh, S. Energy Optimization for Green Communication in IoT Using Harris Hawks Optimization. *IEEE Trans. Green Commun. Netw.* **2022**. [CrossRef]

36. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. *IEEE Trans. Ind. Inform.* **2022**. [CrossRef]
37. Juneja, A.; Juneja, S.; Bali, V.; Mahajan, S. Multi-Criterion Decision Making for Wireless Communication Technologies Adoption in IoT. *Int. J. Syst. Dyn. Appl.* **2020**, *10*, 1–15. [CrossRef]