Probabilistic Neural Network based Shared Random Key Generation for Trellis Coded Wireless Cryptosystem

Anusha.T
Department of Computer Science and Engineering
PSG College of Technology,
Coimbatore, Tamil Nadu, India
anusharesearch2015@gmail.com

Venkatesan. R
Department of Computer Science and Engineering
PSG College of Technology
Coimbatore, Tamil Nadu, India
prof.r.venkatesan@gmail.com

Abstract— **Random keys play a vital role in the world of secured digital communication. Wireless networks are prone to more security breaches than wired networks. The majority of security breaches occur due to weak session keys. The Shared Random Key (SRK) used in wireless cryptosystem must be generated, shared, and distributed securely. The objective of this research work is to generate SRK using Mel Frequency Cepstral Coefficients (MFCCs) extracted from audio files, trained Probabilistic Neural Network (PNN), Galois Field (GF), and energy dissipation during transmission and reception of bits for wireless cryptosystem. The Pseudo Random Key Generator (PRKG) generates a sequence of derived keys from the SRK which gets generated from the Initial (IK) formed using GF and matching positions of random sequences. The SRK is mutated to obtain Mutated Shared Random Key (MSRK). Dissipated energy values add randomness to the MSRK. The randomness of MSRK is assessed based on the National Institute of Standards and Technology (NIST) randomness tests. The generated MSRKs are shared securely and used as session keys by the Wireless Nodes (WNs) in our proposed Energy Aware Trellis Coded Wireless Cryptosystems (EATCWC). Data is transmitted in a wireless cryptosystem after eliminating the malicious nodes. The experiments conducted showed that the proposed system improves the security of data transmission.**

Keywords— Cryptosystem, Galois Field, Mel Frequency Cepstral Coefficients, Probabilistic Neural Network, Shared Random Key

I. INTRODUCTION

Data security plays a major role in storing sensitive databases and transmitting data through wired and wireless networks. Wireless networks are more prone to security threats and attacks than wired networks. Data encrypted to another form requires the use of random keys for withstanding cryptanalytic attacks. Though there exist many random key generation methods in the literature, Galois Field (GF) based random key generation is simple and elegant to be used in Wireless Sensor Networks (WSNs). GF finds its application in computing and cryptography. The researchers in paper [1] have surveyed the security breaches that occur in WSNs and the importance of key management in wireless networks. The purpose of our research work is to propose methods to transfer data securely for wireless cryptosystems. Various theorems are designed based on Galois Field (GF). GF helps to form the random sequence of bits, which can be used for the encryption/decryption of data in WSN [2]. For each element in the GF, there exists a corresponding minimal polynomial, whose coefficients can be considered for random key generation. The symmetric key cryptosystem uses the session key both for encryption and decryption of data. Transmitted data gets decrypted by an adversary if the session key gets captured. Hence, there is a need for the secure sharing of keys. The proposed method models novel random key generation using GF (2^n), where 'n' is determined by processing audio files at a node. This fact is used in the process of random number generation from which the Initial Key (IK) is generated. The Mutated Shared Random Key (MSRK) acts as a session key in our proposed Energy Aware Trellis Coded Wireless Cryptosystems (EATCWC), which is generated using GF, Mel Frequency Cepstral Coefficients (MFCCs), and Probabilistic Neural Network (PNN). The MFCCs are associated with audio files and help in the classification of input audio files. Mutation occurs at positions based on the calculated energy value of the transmitter and receiver nodes. The SRK is formed from the IK by extracting the bits at the matched positions of the random sequences generated by the transmitter and the receiver. Length, entropy, efficiency, lifetime, speed, and calculated probability values (p-values) help in ascertaining the randomness of the generated key to be used for cryptographic applications. It acts as a seed value to generate a sequence of derived keys for a Pseudo Random Key Generator (PRKG). The PRKG uses Trellis Codes (TCs) for generating derived keys. TCs are sequences of bits derived from designed state machines. For each input bit, 4 bits are generated using the state machine [3]. Sequences of bits in the derived keys are shuffled using a uniform crossover technique, which is

advantageous over one-point and two-point crossover techniques of the genetic algorithm. The uniform crossover technique does not rely on randomly chosen crossover points, which has some difficulty generating the same key by the receiver for decryption. TCs shuffled by applying a uniform cross-over technique of genetic algorithm are used if it has higher entropy and efficiency values compared to Trellis Codes (TCs). The Trellis Coded Advanced Encryption Standard (TCAES) uses a sequence of keys generated by PRKG. The existence of duplicated link keys makes the nodes malicious and hence made idle before initiating secured transmission of data between the nodes.

The rest of the paper is organized as follows: Section II describes the studies that were carried out. Section III discusses the proposed shared random key generation method. The experimental setup and corresponding results are given in Section IV. Section V discusses the time complexity and merits of our proposed shared random key generation method. The future scope of this research work is discussed in section VI. Section VII concludes this research paper.

II. Literature Survey

Generating random numbers based on non-deterministic methods is truly random and is complex compared to deterministic methods of generating random numbers. Also, the cost of generating random numbers using a non-deterministic method is high compared to generating random numbers in a deterministic method. The researchers in the paper [4] surveyed the various energy consumption models in wireless sensor networks and identified various sources of energy consumption at each layer of the network. The researchers in the paper [5] generated an efficient random-bit sequence using chaotic maps. The true random number generation from bioelectrical signals is studied in the paper [6]. The researchers explored different techniques and algorithms used in Quantum key distribution and analyzed the dependence of quantum cryptography on public-key cryptography [7]. The researchers in the paper [8] proposed an energy-efficient routing to improve the networking lifespan of a wireless environment. This study improved the Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm by identifying a reliable Cluster Head (CH). The researchers in the paper [9] analyzed the network resilience and associated overhead by a prior distribution of keys. The researchers in the paper [10] surveyed machine-learning approaches for the automatic detection of voice disorders and identified the role played by MFCC in feature extraction from voice signals. The researchers in the paper [11] generated random numbers using photon detection time non-deterministically and tested the results using the Diehard statistical test and NIST statistical tests. The researchers in the paper [12] proposed a novel technique for improving the security of Wireless Sensor Networks (WSNs) using a random key pre-distribution scheme. The researchers in the paper [13] used the cooperative generation of cryptographic keys in wireless networks using relay nodes. The researcher in the paper [14] proposed a method to recognize insect sounds based on MFCC and PNN. The method used signal parameterization methods and state-of-the-art pattern-matching techniques. This method identified 50 specific sounds of insects. The contribution of quantum cryptography to network security is used in the paper [15]. In quantum cryptography, sharing of keys occurs by sending the sequence of bits in another form to prevent eavesdropping. Bits are transmitted using rectilinear or diagonal polarization and choosing any of the four directions (0^o, 90^o, 45^o, 135^o). The key that is shared between two parties is based on the matched positions of correctly depolarized bits. Bits are transmitted in another form to prevent eavesdropping. The key that is shared between two parties is of variable length. The variable length makes the retrieval of the key by unauthorized users a challenging one and detects any third party. The need for a third party is eliminated in this method. This empirical method is practically infeasible, which paves the way for computational modeling of the method involved in it. Quantum cryptography helps prevent eavesdropping but has some user authentication issues. The complexity inherent in classical cryptography and quantum cryptography is considered. The researchers examined the relationship between speed and secrecy in the paper [16]. Fast calculation of secret keys leads to the security of the key being violated. The researchers in the paper [17] focused their work on generating keys using Euclidean and prime number. The role played by centralized authentication is portrayed vividly, and the maintenance of the group key is analyzed. The issue behind maintaining the group key is that there is a chance for a replay attack when a user leaves the group. The researchers in the paper [18] used a random forest algorithm for classifying speech signals based on extracted MFCC. The researchers in the paper [19] used Shannon-Fano-Elias codes for data encryption and identified that the length of the keys can be reduced substantially and are inversely proportional to the vulnerability of being retrieved. The researchers in the paper [20] developed randomness tests which are standardized by the National Institute of Standards and Technology (NIST) tests. The

researchers in the paper [21] identified the usage of primitive polynomials over Galois Field GF (2) in the generation of cryptographic keys. The researchers in the paper [22] proposed random key generation using the phases involved in genetic algorithms and evaluated the key based on the fitness function. Fitness function-based random key selections are not tested using NIST tests. The researchers in the paper [23] proposed a hybrid mathematical model for evaluating the trust of cloud services by combining opinions based on performance, agility, finance, security, and usability criteria. The researchers in the paper [24] used the Sharing Session Key Component (SSKC) for achieving end-to-end security and non-repudiation service in a cellular wireless network. The security of the shared key is ensured by storing it in a distributed manner. One issue with this method is that there is a chance of the key being spoofed by masqueraders. The researchers presented Password-Based Authenticated Key Exchange (PAKE) protocols using lattices in paper [25] and this method is unresistant to hacking. The researchers in the paper [26] proposed a Hamming code and a block cipher mechanism to ensure the secure transmission of a key. The researchers in the paper [27] proposed a model for energy consumption based on an event trigger mechanism.

III. Proposed Shared Random Key Generation Method

Audio files are high-entropy sources that can be used to generate random keys for cryptographic applications. The initial Key(IK) is generated by concatenating the list of minimal polynomials generated for the Galois Field (GF(2n)). The list of minimal polynomials is fixed for a constant ‘n’. The PNN is trained with MFCCs of audio files. A wireless node that should send data selects an audio file randomly and the 'n’ value is generated based on the matching of MFCCs with the trained PNN. The value of 'n' varies the list of generated minimal polynomials. The key that is shared between the nodes Node 1 and Node 2 can further be used for the secured transmission of data. The average energy at the transmitter node and receiver node is calculated to identify the bit positions that are to be mutated in the generated SRK. The inversion of bits at the identified position is used as a mutation operator. Fig. 1 shows the proposed random key generation method. The PNN is a multilayer feed-forward network that is used for the classification problem. In this work, PNN is trained using MFCCs generated from audio files. It is then used for generating the random number 'n' based on matched MFCCs to the MFCCs derived from the input audio file.

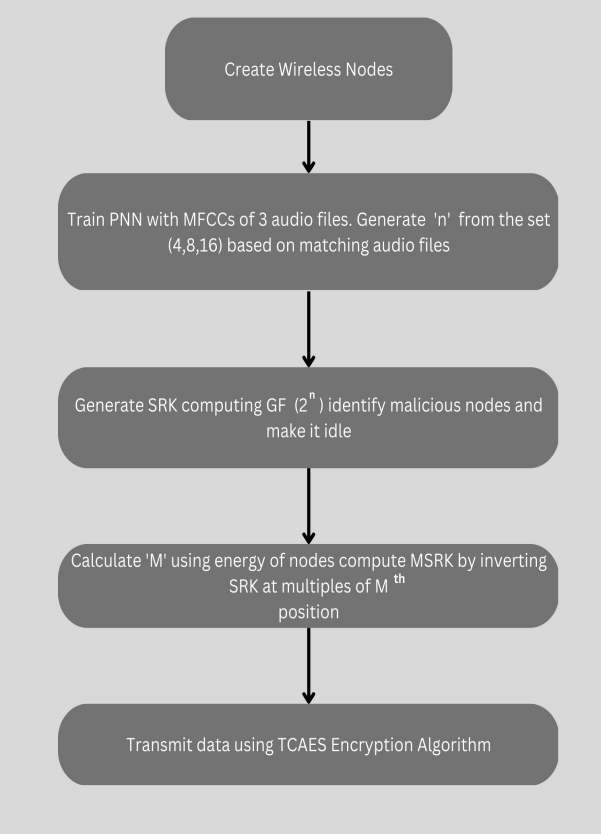

Fig. 1. Energy Aware Trellis Coded Wireless Cryptosystem

The significance of PNN lies in its simple design compared to other neural network models. The PNN can be easily trained and can further be used for matching. WNs are created in random locations. The MFCCs are extracted by processing ‘n’ audio files. The PNN uses a supervised training set to develop distributed functions within a pattern layer. There are 3 layers in the PNN viz., the input layer, middle layer, and output layer. The MFCCs of audio files are given as input to the PNN. The learning function simply selects the first untrained processing element in the correct output class and modifies its weight to match the training vector. The middle layer operates competitively, where only the highest match to output prevails and generates an output.

$$\mathbf{En1n2} = (\mathbf{En1} + \mathbf{En2})/2$$

$$\mathbf{M} = \mathbf{floor}(\mathbf{En1n2} / 10)$$

$$\eta = \mathbf{sumtotal} /11$$

The average energy of the transmitter and receiver nodes is calculated using (1). M is calculated using (2) to identify the bit positions to get inverted and efficiency is calculated using (3) where sumtotal is the number of NIST tests in which p-value$\geq$ 0.01. The SRK is generated by identifying

the positions that are matched between Node 1 and Node 2 generated random positions. Every M^{th} position of SRK gets inverted MSRK. MSRK is used as a session key for secured data transmission between Nodes 1 and Node 2 after checking for randomness using entropy and efficiency values.

The MSRK is generated by inverting the M^{th} bit of SRK generated by calculating the energy of the transmitter and receiver nodes. The sequence of keys is derived using PRKG and fed to the Trellis Coded Advanced Encryption Standard (TCAES) algorithm. During the encryption process, the sequence of keys is derived from MSRK using a Trellis Coded State Machine (TCSM) and is applied in reverse during the decryption process. The MSRK acts as a session key. The uniform cross-over technique is applied over TC and gets selected if its randomness is more than the generated Code from TCSM. Generated bit sequences are used as random keys based on length, entropy, efficiency, lifetime, and calculated probability value (p-value). The encryption process accepts a sequence of binary bits. It is XORed with Round Key 1. Round 2 of the encryption process uses the steps- Substitute Bytes, Shift Rows, Mix Columns and Add Round Key of AES. Decryption accepts encrypted bits. Round 1 uses the steps- Add Round Key, Inverse Mix Columns, Inverse Shift Rows, and Inverse Sub Bytes. The output of Round 1 is XORed with Round Key 1 in Round 2. A communication link between any 2 nodes is established using SRK, which, which acts as a link key. The test for malicious nodes is done based on the existence of duplicate link keys. If identical keys exist between nodes, such nodes are considered malicious nodes, and no communication link is established between them. Nodes with unique link keys within a set get communicated. When the distance between nodes (node x, node y) becomes less than the threshold value, there is a chance of capturing sensitive data between (node x, other nodes) and (node y, other nodes). At this juncture, renewing link keys between (node x, other nodes) and (node y, other nodes) must be performed. Since the nodes are mobile in wireless networks, renewing link keys is to be done when the nodes turn malicious. Periodic renewal of link keys can help alleviate this problem. Periodic detection of duplicate link keys and their renewal help in checking the authenticity of a node in a wireless cryptosystem. Malicious nodes are eliminated from the wireless cryptosystems before data transmission.

IV. Experiments and Results

Experiments were carried out by setting up 10 Wireless Nodes (WNs). The PNN is used to determine 'n' for generating polynomials using GF thereby sequence of bits gets generated. In our experimental setup, we have trained PNN with 3 audio files, one of which gets matched for any input audio file. Considering the set {4, 8, 16}, if the MFCC of the input file matches with the MFCC of the first audio file, 'n' is assigned the value 4. If the MFCC of the input file matches with the MFCC of the second audio file, n is assigned the value 8. If the MFCC of the input file matches with the MFCC of the third audio file 'n' is assigned the value 16. The average energy of the Node 1 and Node 2 is used for determining 'M' which is used for identifying the bits that are to be inverted based on their position. Data gets encrypted and decrypted using the TCAES algorithm. TABLE I shows the location of WSN nodes (X-Longitude, Y-Latitude), their state, transmitting node, receiving node, and the energy of the transmitting and receiving node. TABLE II lists the NIST tests used in our proposed system.

TABLE I. Wireless Nodes

S. No.	X	Y	State	Transmitter/Receiver
1	1.17	2.00	Active	
2	5.33	6.42	Active	
3	9.01	6.01	Idle	
4	2.85	4.60	Idle	
5	6.07	8.08	Idle	
6	2.88	3.08	Active	
7	8.40	2.00	Active	Transmitter
8	3.97	8.70	Active	Receiver
9	5.99	3.04	Idle	
10	6.55	8.32	Idle	

TABLE II. NIST Tests For Randomness

S. No.	Test No.	Tests for Randomness
1	T1	Frequency test
2	T2	Frequency block test
3	T3	Longest runs test
4	T4	Spectral test
5	T5	Non-overlapping template matching test
6	T6	Overlapping template matching test
7	T7	Approximate entropy test
8	T8	Binary matrix rank test
9	T9	Runs test
10	T10,T11	Serial test

TABLE III and TABLE IV shows the generation of IK and round keys. MSRK and round keys are sequences of 0s and 1s which are listed in the hex code for convenience. TABLE V shows the p-values calculated using NIST tests. TABLE VI shows the entropy and efficiency values of MSRK. The threshold value is chosen as 0.5 for both entropy and efficiency values for considering the sequence of bits as MSRK to be used for TCAES encryption TABLE VII shows TCAES encryption results. Plain data P1 and P2 get encrypted using MSRK to get the cipher data C1 and C2. TABLE VIII shows the differential cryptanalysis carried over the results. Since CK1 and CK2 are not equal, we can say that the proposed method withstands differential cryptanalytic attacks.

TABLE III. ENERATION OF IK

n	IK= GF(2^n)
8	'C05C6E3DDB8E7FBB2DB8DEF3FCFEEEA65BD7B8E42F74 DCFE8F9F8DEEEC753F996D8FAF69B8DEF21B1BDFD69B3 FCFFD74787E7CE71B2BEED3763F0D4F0FF31B96CFEC765 EBF9ED377B8E7EF7A9C868F6363BDFD7EB39A6F0E7FE7 CFE8FEBC3D1F030F8BE7E1E735FC6E2E57F3EEF3E9BF9D 8E1FE165D4CE7875FFCD7E37BD96E367F1BB1E2ECB30EB CAFCFBDB4FCEEF1DB8F773F2DBDF3F53D7C8537478DD 8FE6C769BDEC7EB3FFAE1E732BA6FC3871B9FD97CF77C FEA74763FACE787E7D1F0F818BC3D7F17F3E7FE70F659C D7EBFBDC6C6F173095EF7E71DEECB79FD7A6E37F369D8 CFF0F2BF846ECB77D4D8E73E7E1E2EBFF3FCD96BFBD8D CC37B1D96F5F1B699FCAE3777B1F9F17F3B2EF6611DEBD A65777F3FCF7B1DB4DDFE71DBBC763B80'

TABLE IV. MSRK AND SEQUENCE OF ROUND KEYS

n	SRK	Round Key 1 (MSRK)	Round Key 2
8	3CDE9628FEF E9628 CDB41428822 00001	'0001CA938BE FEFD5 6BD849CA9C A9CA93'	00000000000000013 5649CFEFEA9CA93

TABLE V. P-VALUES OF MSRK

p-Values										
T1	*T2*	*T3*	*T4*	*T5*	*T6*	*T7*	*T8*	*T9*	*T10*	*T11*
0.0771	0.0239	0.3944	0.1443	0.0017	0.9968	0.1072	0.3329	0	0.0221	0.0413

TABLE VI. ENTROPY AND EFFICIENCY VALUES

Entropy and Randomness Threshold Value=0.5	Efficiency and Randomness Threshold Value=0.5
0.9823, Random	0.8181, Random

TABLE VII. TCAES ENCRYPTION

Plain Data (P1)	*Cipher Data (C1)*	*Plain Data (P2)*	*Cipher Data (C2)*
'EA04658583 455D	'480A660D806 77E8B	'620465858345 5D95	'460A660D87 677E
965C3398B0 F02D ADC5'	AEEF2621837 774E8'	C3398B0F02D ADC5'	8BA9EF2621 8A777 4E8'

TABLE VIII. DIFFERENTIAL CRYPTANALYSIS

CK2= C1 XOR C2	CK2= C1 XOR C2	Is CK1 =CK2? Yes/No
880000000000000000000 00000000000	0E00000007000000070000 0009000000	No

V. DISCUSSION

For the same GF-based generated random key, different SRK can be generated at different times. Its length is variable at different times, and its lifetime is also short. The lifetime of the key should be short and it must remain unusable after successfully decrypting the cipher values. The speed of key generation is variable as it depends on the length of the key. The SRK is adjusted to get a length of 128 bits and mutated to get MSRK. From the p-values calculated using NIST tests and tabulated in TABLE VII, it is inferred that MSRK is random using NIST tests. The SRK cannot be generated by an adversary on possession of the GF-generated random key and positions generated by Node 1 and Node 2, since the comparison for position matching is done locally by the systems and the adversary is unaware of it. Instead of a comparison function, different functions can be used. Also, the position of mutated bits in SRK to get MSRK remains unpredictable by adversaries. The code generator can act as a trusted third party and make the GF-based key non-accessible to unauthorized users. Also, the key that is shared by two users is not made known to any users or any third party. The uniform crossover technique is preferred for making encryption and decryption possible for the system designed. For other crossover techniques such as one-point crossover and two-point crossover, if the positions are selected randomly by the sender, there is no assurance of selecting the same position by the receiver. Cryptanalysis refers to finding out the key with the gathered information about cryptographic algorithms and cipher data by which plain data can be determined. A brute force attack refers to trying all possible combinations of bits. It fails when the lifetime of the keys is short and the length is variable. Internal keys are of length 128 bits, and an adversary should try for 2^{128} possible ways for finding the round keys for each round and thereby finding the plain data. The best, worst, and average cases of the complexity of the search that is to be performed by the adversary are O(1), O(n), and O(log n) respectively. Linear cryptanalysis refers to forming linear equations portraying the relationship between plain data, cipher data, and encryption key. No linear equation can be

formed since there is no one-to-one relationship between encrypted and decrypted plain data and so linear cryptanalysis fails. Differential cryptanalysis refers to analyzing the difference between cipher data for different plain data and the same encryption key. From TABLE VIII, it is found that no inference regarding the key can be made from the difference in plain data and the corresponding difference in cipher data. The lifetime is short compared to the time of linear searching involved in brute force attacks. In the case of parallel programming of the key search in brute force requires 2^n processing elements are needed to retrieve the key with time complexity O(1), where n is the key length. Since 'n' is variable, the number of processing elements in retrieving the correct key with time complexity O(1) cannot be predicted. The time complexity of malicious node detection is $O(n^2)$. Compromising link keys through brute force, linear cryptanalysis, and differential cryptanalysis can be overcome by renewing the link keys periodically. Messages are sent in an encrypted form from one node to another node, provided both nodes are non-malicious.

VI. Future Scope

The proposed EATCWC cryptosystem withstands differential cryptanalytic attacks of transmitted data. It can be extended using an arbitrary number of rounds for encryption and decryption of the plain data. Increasing the number of rounds increases the execution time, but adds to the security of the data. Further research can be conducted in designing algorithms for data security in Wireless Sensor Networks (WSN) at low energy consumption.

VII. Conclusion

The energy of the transmitted and received nodes acts as a random source. The dynamic nature of energy consumed adds randomness to MSRK. The MSRK is generated based on a randomly considered audio file, an MFCC-trained PNN, and GF. It gets mutated based on the energy of the transmitted and received nodes. If it is random, the sequence of keys is pseudo-randomly generated. The success of the proposed system is based on the unpredictability of MSRK and the sequence of keys, which are generated, shared and distributed securely. The scope of generating, sharing, and distribution of keys finds its usage in wireless networks for secured transmission of data, which lasts forever.

Acknowledgment

We acknowledge the Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India for providing the necessary software for this research work.

References

[1] Amit Kumar Gautam, Rakesh Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," SN Applied Sciences (2021) 3:50.

[2] Kwasi Bash Gyamfi, Emmanuel Akweittey, Matilda Adusei Sarpong, "Galois Fields and some of its Applications," International Journal of Scientific and Research Publications, vol.10, issue 5, May 2020.

[3] Ingemar.J.Cox, Matthew.L.Miller, Jeffrey.A.Bloom, Jessica Fredrich and Tonkalker, "Digital Watermarking and Steganography," Margan Kaufmann Publishers, New York, Chapter 4,2008.

[4] Abo-Zahhad M, Amin O, Farrag M, and Ali A, "Survey on energy consumption models in wireless sensor networks," Open Transaction on Wireless Sensor Network, 1(1):1-4, Dec 2014.

[5] Ahmad M, Doja MN, and Beg MS. "A new chaotic map based secure and efficient pseudo-random bit sequence generation," International symposium on security in computing and communication 2018 Sep 19 (pp. 543-553). Springer, Singapore.

[6] Arslan Tuncer S, and Kaya T, "True random number generation from bioelectrical and physical signals," Computational and mathematical methods in medicine, July 2018.

[7] Charjan S, and Kulkarni DH. "Quantum Key Distribution using Different Techniques and Algorithms," International Journal of Engineering Research & Technology,3(11),2014.

[8] Devika G, Ramesh D, and Karegowda AG " Energy optimized hybrid PSO and wolf search based LEACH," International Journal of Information Technology. 1-2, Jan 2021.

[9] Du W, Deng J, Han YS, Varshney PK, Katz J, and Khalili A, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security (TISSEC),8(2):228-58, May 2005.

[10] Hegde S, Shetty S, Rai S, Dodderi T, "A survey on machine learning approaches for automatic detection of voice disorders. Journal of Voice," 33(6):947-e11,2019.

[11] Khanmohammadi A, Enne R, Hofbauer M, and Zimmermanna H, "A monolithic silicon quantum random number generator based on measurement of photon detection time," IEEE Photonics Journal.,7(5):1-3, Sep 2015.

[12] Krishnappa VK, and Narayanagowda SH, "A Novel Technique for Improving the Security of WSN Using Random Key Pre Distribution Scheme," International Journal of Intelligent Engineering and Systems,12(2):33:41.

[13] Lai L, Liang Y, and Du W "Cooperative key generation in wireless networks. IEEE Journal on Selected Areas in Communications," 30(8):1578-88, Aug 2012.

[14] Le-Qing Z. "Insect sound recognition based on mfcc and pnn," International Conference on Multimedia and Signal Processing, vol. 2, pp. 42-46,2011. IEEE.

[15] Mehrdad SS "Quantum cryptography: An emerging technology in network security," (HST), 2011 IEEE International Conference on Technologies for Homeland Security(HST), pp. 13-19,2011.

[16] Odeh A, Elleithy K, Alshowkan M, and Abdelfattah E. "Quantum key distribution by using public key algorithm (RSA)," Third International Conference on Innovative Computing Technology (INTECH 2013) pp. 83-86, Aug 2013, IEEE.

[17] Ragunathan M, and Vijayavel P, "Design and Implementation of Key Distribution Algorithms of Public Key Cryptography for Group Communication in Grid Computing," Mining Intelligence and Knowledge Exploration 2014 (pp. 417-424). Springer, Cham.

[18] Rao MS, Lakshmi GB, Gowri P, and Chowdary KB. "Random Forest Based Automatic Speaker Recognition System," 12(4), April 2020.

[19] Ruan X, and Katti R. Using improved shannon-fano-elias codes for data encryption, "IEEE International Symposium on Information Theory," 2006 Jul 9 (pp. 1249-1252). IEEE.

[20] Rukhin A, Soto J, Nechvatal J, Smid M, and Barker E., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," April 2010.

[21] Singh I, and Pais AR "A random key generation scheme using primitive polynomials over GF (2). International Symposium on Security in Computing and Communication," 2016 Sep 21 (pp. 42-51). Springer, Singapore.

[22] Soni A, and Agrawal S," Key generation using genetic algorithm for image encryption. International Journal of Computer Science and Mobile Computing (IJCSMC)," 2(6):376-83, June 2013.

[23] Trabay D, Asem A, EI-Henawy, and Gharibi W, "A hybrid technique for evaluating the trust of cloud services. International Journal of Information Technology," 1-9, Jan 2021.

[24] Wu HK, Yang SC, and Lin YT "The sharing session key component (SSKC) algorithm for End-to-End secure wireless communication," Proceedings IEEE 34th Annual 2000 International Carnahan Conference on Security Technology (Cat. No. 00CH37083) 2000 Oct 23 (pp. 242-250). IEEE.

[25] Yin A, Guo Y, Song Y, Qu T, and Fang C, "Two-Round Password-Based Authenticated Key Exchange from Lattices," Wireless Communications and Mobile Computing. Dec 2020.

[26] Zhang Y, Liu X, Ma Y, and Cheng LC, "An optimized DNA-based encryption scheme with enforced secure key distribution," Cluster Computing. 20(4):3119-30.,2017.

[27] Zhou HY, Luo DY, Gao Y, and Zuo DC, "Modeling of node energy consumption for wireless sensor networks," Wireless Sensor Network. 3(1):18, Jan 2011.