Secured Wireless Data Transmission using Encryption and Frequency Hopping Technique

S.P.Vijaya Vardan Reddy, T.V.Padmavathy, D.S.Bhargava, B.Raghunatha Rao, T.Jagapathi Babu

Abstract*: This work aims at developing wireless communication medium a mid two nodes by using Encryption and Frequency Hopping techniques. Data Encryption is done by using Cryptography. One of the major challenges in data communication network is security. This issue becomes more critical if there is connectivity during resource sharing. In our paper, we discuss data encryption using RSA algorithm to make certain that data is confidential. Using this algorithm, sender is allowed to generate public keys to encrypt the information and receiver is been shared with a private key using a protected database to decrypt the same. An erroneous private key will decrypt the protected data but to a different form from the actual data. The data we choose for being a key, method of distributing it are vital issues in algorithms. Hence Cryptography is used to convert the message block into a private key and Frequency Hoping is done by using the Spread Spectrum technique. Also the classification of cryptographic algorithms is outlined in this paper.

***Keywords*— Encryption, Cryptography, RSA Algorithm, Frequency Hoping, Spread Spectrum.**

I. INTRODUCTION

This work establishes one-way wireless communication between two nodes, where security is an important stipulation. Explicitly, we look at audio transmission wherein the voice signal is sampled at a practical rate and then the quantized samples are transmitted in digital format. At the receiver end, the signal is reconstructed from the samples.

Transmission of voice over a wireless channel is an important challenge and requires high data rate, whereas wireless transfer of other data, does not involve high bit rate and may be achieved effortlessly.

On the contrary, Real-time voice transmission necessitates the bit generation rate equals the transmission rate. On the usage of speech coding algorithms, data rate of 32 kilobits/sec or 4kilobytes/sec is required. Conventional wireless systems claim to security is solely the encryption of data, transmitted over the wireless channel. A possible adversary who can "hear" the data stream still has the capability to retrieve the individual bits of the encrypted stream. Often, algebraic attacks may be employed to decipher the data. When security infringes is a major issue, there is a need for stronger encryption. We attempt to maintain better security of data through the following:

- Encryption of data by modulo-2 addition (XOR addition) with a fixed random string.
- Implement frequency hopping in a cyclic fashion. The carrier frequency is altered in such a manner that is identified only by the transmitter and receiver. In such cases, thus the possible adversary would not be able to "hear" more than a certain fraction of the input data stream at intermittent intervals of time.

Thus, real-time (Linear Feedback Shift Register) LFSR encryption along with frequency hopping results in a safe and protected communication link.

II. RELATED WORKS

In this paper [2] various techniques of using Digital Frequency Locked Loop (DFLL) in the Frequency-Hopped Spread-Spectrum (FHSS) systems were discussed. The approach used in [2] makes probable to use an exact DFLL instead of RF Local Oscillator (LO) particularly in the fast FHSS systems. A DFLL in position of LO had not been reported for fast FHSS systems due to the reason that type of frequency synthesizer requests relatively long time for accurate frequency measurement and setting. Using prediction algorithm in DFLL provides solution to above mentioned problem. Instead of LO, Predictive Digital Frequency Locked Loop (PDFLL) has been used in fast FH-SS systems which make use of useful spectral properties of the DFLL. [2]

A cryptography technique based on the concept of algorithm hopping is proposed in [4]. In this paper usage of single encryption algorithm in conventional systems to encrypt the plain text has been discussed and also it has been compared with usage of different encryption algorithms to encrypt different sections of plain text. The substantial point in this kind of cryptography is hiding internal parameters, which are actually the encrypting algorithm. In the virtue of pseudo random number the hidden parameters can be determined. The selection of Pseudo random number is similar to the FHSS techniques which selects next hop frequency.

Manuscript published on November 30, 2019.
* Correspondence Author

S.P.Vijaya Vardan Reddy*, ECE, R.M.K. Engineering College, Chennai, India. Email: spr.ece@rmkec.ac.in

T.V.Padmavathy, ECE, R.M.K. Engineering College, Chennai, India. Email: tvp.ece@rmkec.ac.in

D.S.Bhargava, ECE, R.M.K. Engineering College, Chennai, India. Email: dsb.ece@rmkec.ac.in

B. Raghunatha Rao, Department of Electronics and Communication Engineering, R.M.K. Engineering College, Affiliated to Anna University Chennai,

T. Jagapathi Babu, Department of Electronics and Communication Engineering, R.M.K. Engineering College, Affiliated to Anna University Chennai,

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

In [4] to evaluate the system, non-exhaustive Boolean functions are chosen as encryption algorithm, where the pseudorandom number helps in identifying the next Boolean function which will encrypt further sections of the plain text, and so the next parameter. Also the advantages of Boolean functions and its implementation using hardware components as well as software have been presented [4]. The algorithm hopping cryptography encryption and decryption speed is comparatively high than traditional algorithms due to the reason logic gates are used to implement Boolean functions whereas in traditional systems it uses decimal number system calculation. This algorithm hopping cryptography method can also be further enhanced/extended and used as asymmetric analysis of codes/ciphers to support public keys.

Wireless Sensor Network (WSN) is a group of thousands sensor nodes with wireless communication, minimal computation and sensing capabilities [3] [6]. Due to paucity of tamper resistant packaging and the unsure nature & design of Wireless Communication (WC) channels and/or systems, these networks are susceptible to internal and external attacks. The routing protocols which are already prevailing are application specific and moreover do not satisfy security requirements of WSN, Further more if in case any device lies within the frequency range can get access to transmitting data which may affect the transmission. In this paper [6], the frequency hopping simulation proves to be a better approach which provides security for WSN is presented.

Spread Spectrum is a modulation technique in which bandwidth is spread in terms of its frequency domain, transfers the actual information signal with wide bandwidth than the original frequency spectrum. In FHSS the carrier frequency does not remain fixed instead changes from one frequency to the other for some instant of time. (Thousand times/second). The spreading of bandwidth is possible by selecting different carrier frequencies for information signal along with hopping sequence. Amongst the range of FHSS merits, one is transmission security. In [11] paper, enhancement of transmission security using hopping sequence and its compliment in FHSS is presented.

In this paper [1] Data Encryption Algorithm is been developed and its performance has been analyzed for various security metrics and the results of algorithm developed are prominently better than Rivest–Shamir–Adleman (RSA), SKIPJACK, Data Encryption Standard (DES1 and 3DES). This was implemented in a web based learning system for addressing security issues like confidentiality and integrity.

To combat noise jamming and reception of undesired signals, FHSS technique has been used in [8]. Vulnerability of Linear Feedback Shift Register (LFSR) codes has been analyzed and hidden frequency hopping method had been applied over spreading codes to get better security of FHSS. The results demonstrate that this method is highly reliable.

In [7] source and channel encryption techniques has been analyzed for WSN enhanced Security. The source information bits are encrypted with the implementation of honey encryption. Inclusion of Gaussian Frequency Shift Keying (GFSK) for the encrypted data leads to FHSS (as a channel encryption). The output is further propagated out with the support of Frequency Hopping Multiple Access (FHMA) in WSN. Henceforth, it is not viable to break in the channel by hackers and moreover the possibilities of detecting and/or decoding the source information by Brute force attack are not feasible. The method discussed in [7] provides dual security to source information.

In this paper [10], comparison of ten different encryption (symmetric and asymmetric key) algorithms had been carried out and its performance on various parameters to select the better data encryption algorithm has been analyzed.

III. PROPOSED SYSTEM MODEL

A. RSA Algorithm

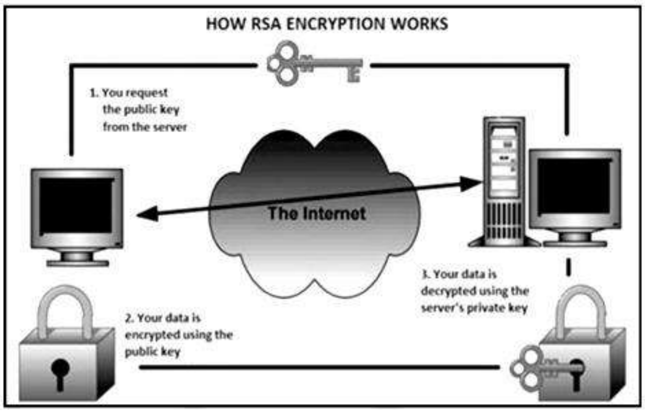

HOW RSA ENCRYPTION WORKS
1. You request the public key from the server
The Internet
2. Your data is encrypted using the public key
3. Your data is decrypted using the server's private key

Fig.1. Encryption using RSA

Cryptographic algorithms can be categorized into many different ways; but for the security purposes (for encryption and decryption [1]) based on the fact, number of keys, it has been put into three major types as follows

- ***Secret Key Cryptography (SKC):*** SKC uses only one key for encryption as well as decryption, which are widely known as stream or block ciphers. The major difference between Stream ciphers and Block cipher is that former operates on single bit at a time while the later encrypts one complete data block at a time. The major pitfall of SKC is error propagation due to distortion. Despite the fact that stream ciphers don't proliferate transmission errors, the key may repeat due to periodicity in nature and it results in requirement of digital signature mechanisms [9]
- ***Public Key Cryptography (PKC):*** PKC (two-key crypto system), uses different keys for encryption and decryption. One of the keys is public key and it may be advertised over the network whereas another key is private key, never shared with anyone. RSA is one of the first and foremost PKC implementations that have been used widely till date for key exchange or digital signatures. The prime advantage is administration of keys over a network requires the existence of functionally trusted TTP [9]
- ***Hash Functions (HF):*** The HF uses mathematical transformation to encrypt data. Unlike the above mentioned two methods, this algorithm does not use any keys for either encryption or decryption, rather uses a fixed-length hash value. It is difficult to recover the contents or length of plain text. These algorithms are widely used to provide digital fingerprint, to make certain that the file has not been affected or damaged by an intruder or virus, to encrypt passwords for maintaining data integrity. [9]

B. Frequency Hopping Spread Spectrum

Along with the clear, undistorted and noise-free transmission, it is also required that the communication must be well secure interception by the unauthorized users in commercial and defense communication as well. In SS transmission, a signal occupies larger bandwidth than of minimum necessary bandwidth to send the information. The spreading of bandwidth or generating larger bandwidth is able by means of spreading sequence, especially for the establishment of secure communication. Actually SS transmission was initiated and used by the military in order to reduce jamming and eavesdropping. It takes digital signal or data packets of signal and expands/spread it to look like random noise rather than data signal transmission using often FSK, PSK or QAM as a coding scheme. [2] [7]

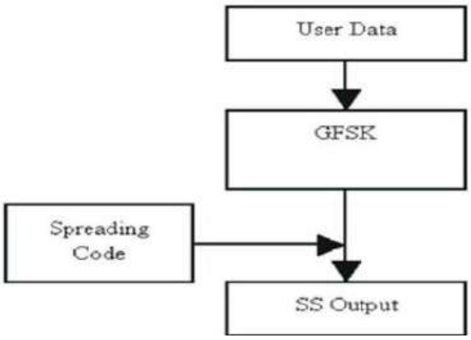


Fig. 2. Spread Spectrum Procedure [11]

FHSS [5] utilizes the coexistence of multiple networks or device which uses multiple access methods in the same location. According to IEEE 802.11 standards, in FH PHY systems hopping takes place over 79 frequency channels in USA and Europe, whereas in Japan its 23 frequency channels with 1 MHz channel spacing [11]. FHSS uses multiple carrier frequencies for modulation of information signal, in every time slot different carrier frequency is modulated using either linear/sequential or random selection methods. This results in increased bandwidth than the actual bandwidth.

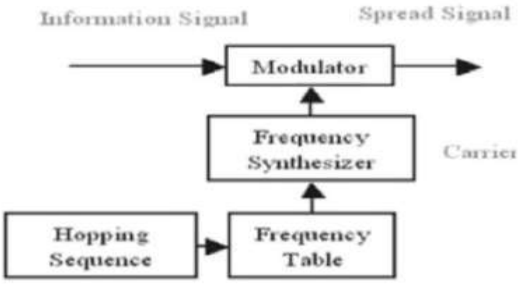


Fig. 3. FHSS General Layout and Procedure [5]

- *FHSS Transmitter and Receiver:*

The FHSS transmitter and receiver should be synchronized to the same hop sequence and also on various other aspects like correlation intervals, SS Generation and Carrier Synchronization etc. This synchronization is essential in order to retrieve the transmitted signals at the receiver end & also to enhance the transmission security and in addition to overcome the signal jamming problems and fading effects. The block diagram of FHSS transceiver shown in Fig 4 illustrates that the system works with the help of frequency synthesizer using frequency table with spreading sequences. This leads to hopping to different frequencies at the different time slots thereby achieving signal spreading. [2]

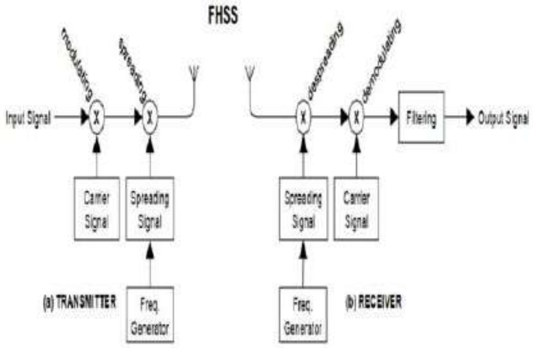
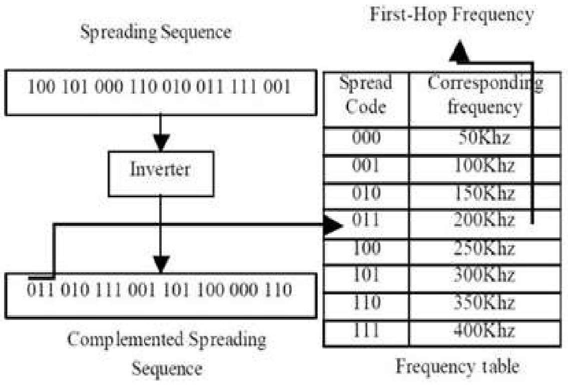


Fig. 4. Block Diagram of FHSS Transceiver [2]

On the other hand at the receiver side, the signal is despread in order to obtain the transmitted signal. To further enhance the transmission security, Complemented Hopping Sequence-Frequency Hopping Spread Spectrum (CHS-FHSS) can be used. One method is CHS-FHSS uses hopping sequence and its compliment as the spreading sequence to select the hop for the incoming information signal and spread the spectrum accordingly. The another method usage of encoding schemes along with hopping sequence and its compliment to accomplish much more secure transmission. The size of spreading sequence and its compliments impacts the transmission security i.e. Larger the size greater the security and vice versa. [11]



Spread Code	Corresponding frequency
000	50Khz
001	100Khz
010	150Khz
011	200Khz
100	250Khz
101	300Khz
110	350Khz
111	400Khz

Fig.5. Complemented Hopping Sequences and Frequency Table [11]

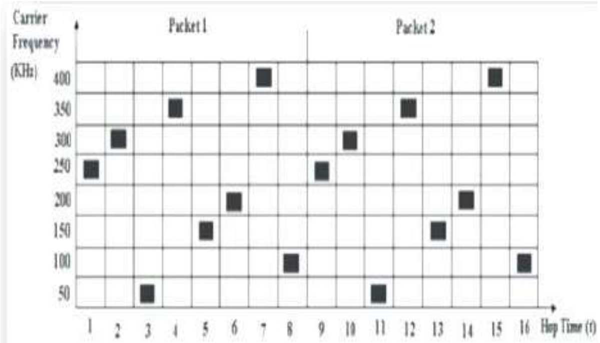


Fig. 6. FHSS Data Packets

Retrieval Number: D9464118419/2019©BEIESP
DOI:10.35940/ijrte.D9464.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. SIMULATED RESULTS

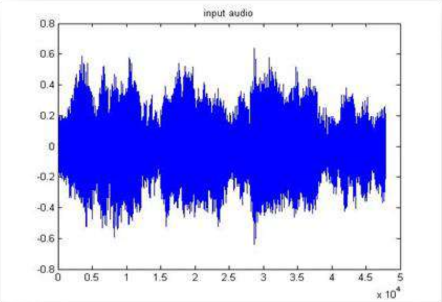


Fig. 7. Input Audio Signal

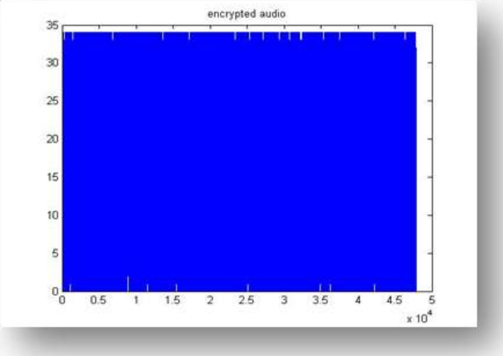


Fig. 8. Encrypted Audio Signal

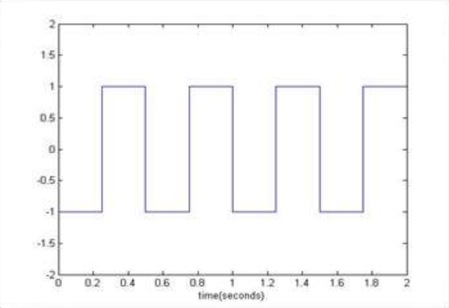


Fig. 9. Square Wave Signal

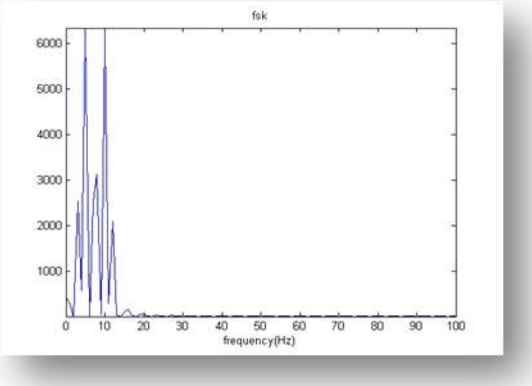


Fig. 10. Pseudo Noise Signal

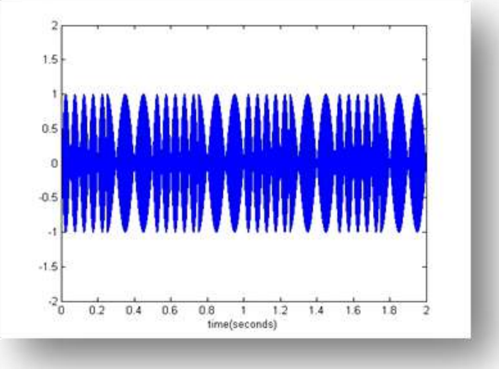


Fig. 11. Pseudo Noise Signal with FSK

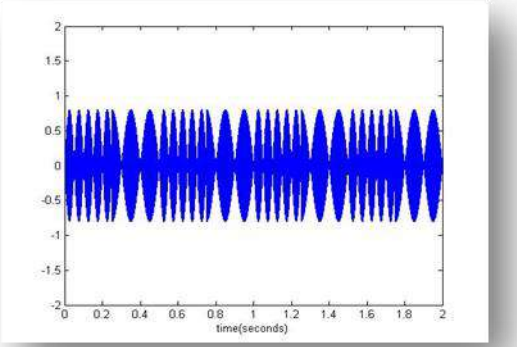


Fig. 12. FSK Modulated Signal

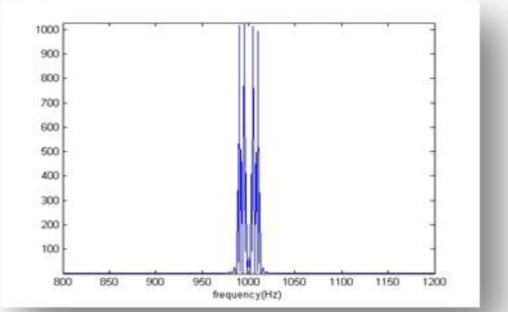


Fig. 13. FIR Filtered Signal

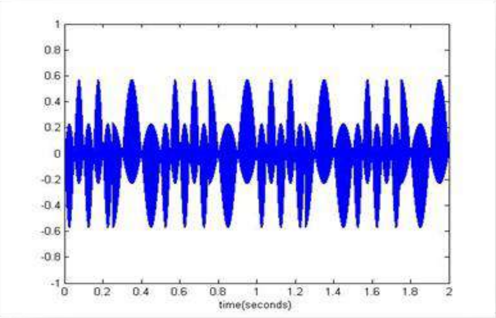


Fig. 14. FSK Demodulated Signal with FIR

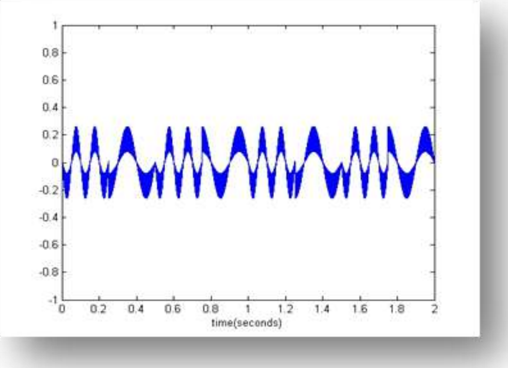


Fig. 15. Recovered FSK Signal

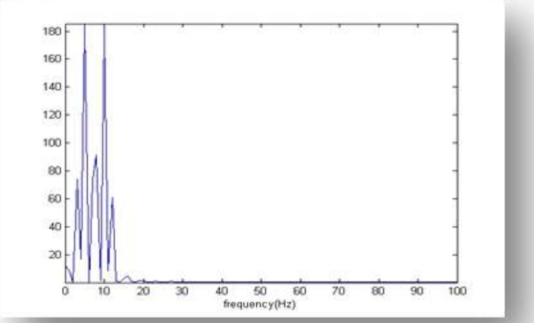


Fig. 16. Recovered Pseudo Noise Signal

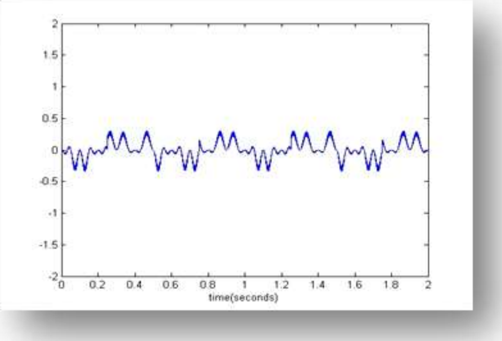


Fig. 17. FHSS Output Signal

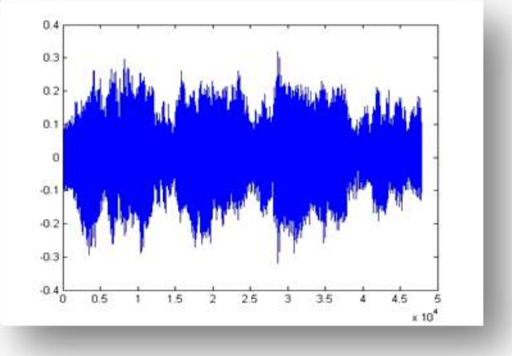


Fig. 18. Decrypted Output Signal

V. CONCLUSION

An RSA public-key cryptosystem has been designed and presented in this paper for efficient communication of audio signals. The significant of security is greatly highlighted and also the system model, its methodology is illustrated in this paper. The system performance is evaluated in terms of audio quality metrics for both encryption and decryption process. The simulation results obtained are presented in previous section which demonstrates that the intelligibility is too low in encrypted audio signal whereas the quality of recovered acoustic signal is good which maintains and confirm the appropriateness, reliability, data security and effectiveness.

REFERENCES

1. Afolabi, A.O and E.R. Adagunodo, *"Implementation of an improved Data Encryption Algorithm in a web based learning system," International Journal of Research and Reviews in Computer Science*, Vol. 3, No. 1. 2012
2. BranislavLojko, *"A Contribution to the Design of a Frequency Synthesizer for Fast Frequency-Hopped Spread-Spectrum Systems,"* Department of Radio and Electronics, Slovak University of Technology.
3. Chehri, A., Fortier, P. & Tardif, P.M., *"A Comparison between Different FHSS Techniques for use in a Multiple Access Secure Wireless Sensor Network," IEEE Annual Wireless and Microwave Technology Conference.*
4. Dr. Mohamed Raseen and Dr. Moh'dRadaideh, *"Algorithm Hopping Symmetric Cryptography," International Journal of Computer and Internet Security*, ISSN 0974-2247 Vol. 9, No. 1. 2017
5. Ferreira, C. M. S., Oliveira, R. A. R., Gambini, H. S., &Frery, A. C. *"Characterization of FHSS in Wireless Personal Area Networks," 22nd Wireless and Optical Communication Conference.*
6. Gaurav Sharma, SumanBala, A. K. Verma and Tej Singh, *"Security in Wireless Sensor Networks using Frequency Hopping," International Journal of Computer Applications* (0975 – 8887) Vol. 12, No. 6. 2010
7. M. Rajalakshmi and C. Parthasarathy, *"An Implementation of FHMA for Honey Encrypted Datasets in Wireless Sensor Networks," ARPN Journal of Engineering and Applied Sciences*, Vol. 13, No. 11, June 2018.
8. M. Vembu, S. Navaneethan, *"Security Enhancement of Frequency Hopping Spread Spectrum Based On OQPSK Technique," IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).*
9. Nentawe Y. Goshwe, *"Data Encryption and Decryption using RSA Algorithm in a Network Environment," IJCSNS International Journal of Computer Science and Network Security*, Vol. 14, No. 5. 2014
10. RajdeepBhanot and Rahul Hans, *"A Review and Comparative analysis of various Encryption Algorithms," International Journal of Security and its Applications.*
11. ShahidLatif, Muhammad Kamran, Wasim-ud-Din, RahatUllah and AbouBakarNouman, *"Security Enhancement of FHSS Transmission System using Hopping Sequence and its Compliment (CHS-FHSS)," World Applied Sciences Journal* , ISSN 1818-4952, Vol. 21, No. 6, pp. 920-926, IDOSI Publications, 2013

AUTHORS PROFILE

S.P.Vijaya Vardan Reddy, working as Assistant Professor in the Department of Electronics and Communication Engineering, R.M.K. Engineering College has 7 years of experience in Teaching. He received his Bachelor's degree in Electronics and Communication Engineering from SKR Engineering College in the year 2010 & Master's degree in Communication Systems from Rajalakshmi Engineering College, Chennai in the year 2012. He has presented 4 papers in National Conferences and 6 papers in International conferences & has published 2 journals. He is a member in All India Engineers Association and

Indian Society For Technical Education. His research areas include Computer & Wireless Networks and Embedded Systems.

T. V. Padmavathy, Professor, Department of ECE in R.M.K. Engineering College, has 24 years of teaching and research experience in the in the fields of Wireless sensor networks, Under Water Acoustic Sensor Networks and Antenna Design. She has graduated from Institution of Engineers (India), in Electronics and Communication Engineering. She has obtained her Master degree in Control and Instrumentation from College of Engineering, Guindy, Anna University, Chennai and Ph.D. degree from Anna University, Chennai. She has published more than 50 research papers in International and National Journals and conferences in the area of Mobile Ad hoc Networks, Wireless sensor networks, Under Water Acoustic Sensor Networks and Antenna design and she has four Patents in Wireless Sensor Networks. Her current area of research includes security and architecture issues of Mobile ad hoc networks, Wireless sensor networks and Millimeter Wave Antenna design for Wireless Communications. She is a technical paper reviewer for African Journal of Engineering Research and Journal of Engineering and Technology Management. She is recognized as Fellowship member by The Institution of Engineers (India) also she is a member of various professional bodies such as Institute of Electrical and Electronics Engineers (IEEE), Life member of Institution of Electronics and Telecommunication Engineers (IETE), International Association of Engineers (IAENG), ACM, ISSE and Life member of Indian Society for Technical Education ISTE.

D.S. Bhargava, working as Assistant Professor in Electronics and Communication Engineering department of R.M.K Engineering College, has 5 years of teaching experience. He received his Bachelor's degree from J.N.N Institute of Engineering in Electronics and Communication Engineering in the year 2012 and Master's degree in VLSI Design from R.M.K Engineering College in the year 2014. His area of interests includes Cognitive radio networks and VLSI Design technology. He has published 7 research papers in International and National Journals & conferences in the area of VLSI Design, Networking and Cognitive radio networks. He is a professional member of ACM, ISTE, and IAENG.

B. Raghunatha Rao, completed his Bachelor's Degree in the Department of Electronics and Communication Engineering, R.M.K. Engineering College, Affiliated to Anna University Chennai, in the year 2019. He is an active member of various technical forums, during his course of study he has organized technical event like symposiums & also attended Guest Lectures, workshops, seminars and In plant training etc. His area of interests is Networks & Embedded Systems.

T. Jagapathi Babu, completed his Bachelor's Degree in the Department of Electronics and Communication Engineering, R.M.K. Engineering College, Affiliated to Anna University Chennai, in the year 2019. He is an active member of various technical forums, during his course of study he has organized technical event like symposiums & also attended Guest Lectures, workshops, seminars and In plant training etc. His area of interests is Networks & Embedded Systems.