Confidentiality Enhancement Using Spread Spectrum Modulation Technique for Aggregated Data in Wireless Sensor Networks

Trupti Shripad Tagare[1]* and Rajashree Narendra[2]

[1] Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru, 560078, India
[2] Department of Electronics and Communication, Dayananda Sagar University, Bengaluru, 560082, India;
Email: rajashree-ece@dsu.edu.in (R.N.)
*Correspondence: truptitagare-ece@dayanandasagar.edu (T.S.T.)

Abstract—Wireless Sensor Networks (WSN) play a crucial role in transmitting bulk data remotely on Internet of Things (IoT). The data transmitted by the tiny sensor nodes of the network are basically the physical parameters of the environment like temperature, vibration, pressure etc. There exists a huge co-relation in the data sent by the nodes. This bulk data needs to be aggregated in order to conserve the energy of the network and thereby enhance the network lifetime. Although the aggregation might lead to loss of actual data, aggregating helps in reducing energy requirement during transmission which is of primary importance and hence is considered as a suitable method in WSN. Adding confidentiality to aggregated data helps in sending the data more securely. Spread spectrum modulation is a widely used technique to provide confidentiality in communication systems. In this research work, we implement a data aggregation technique and apply the spread spectrum modulation technique to provide confidentiality to the aggregated data that needs to be transmitted from the cluster head node to the gateway. Here, data aggregation process consists of averaging the number of data that are sensed by a sensor node and transmitting only its average value to the gateway. This reduces the amount of data transmission and helps in conserving energy. Further, the spread spectrum technique implements Binary Phase Shift Keying (BPSK) method with Frequency Hopping Spread Spectrum (FHSS) carried out using six different frequencies on MATLAB 2020a. The simulation results evaluate the performance of the system. The graphs are plotted for modulated and demodulated signals, spread and de-spread sequences, Bit Error Rate (BER) of BPSK/FHSS over Rayleigh flat fading channel, Power Spectral Density (PSD) and Fast Fourier Transform (FFT) of frequency hopped signal. The results show that BER value decreases with increase in Signal to Noise Ratio (SNR). The maximum power consumption in the network is 7.518mW at 5MHz frequency, for adding confidentiality to the aggregated data to be transmitted. Thus, the proposed work promises efficient energy consumption, longer network lifetimes with added confidentiality.

Keywords—data aggregation, spread spectrum modulation, frequency hopping, wireless sensor networks, Rayleigh flat fading, power spectral density, fast fourier transform, IoT

I. Introduction

Wireless Sensor Networks (WSNs) consist of several tiny sensor nodes placed in inaccessible areas that need to be monitored. The sensor devices have limited resources like battery energy, storage capacity, network bandwidth etc. [1]. Internet of Things (IoT) is a popular application of WSN today. In an IoT based WSN, the sensor nodes sense the data and transmit it to remote stations over the internet via the gateways of WSN.

The sensor nodes in WSNs sense and transmit large amount of data. The raw data so obtained consists of large number of repetitive values which form a bulk at the gateway. Thus, huge amount of network energy is consumed for this bulk data transmission. This clearly suggests that aggregating the sensed data is necessary as it reduces the number of data packets sent to the gateway. Data aggregation is one of the important techniques used in Wireless Sensor Networks (WSN) to efficiently conserve the energy of the network by reducing the number of data packets that need to be transmitted [2].

However, the data aggregation techniques may degrade the Quality of Service (QoS) of WSN like data accuracy, latency, and fault-tolerance. It increases more vulnerabilities. The node collecting and determining aggregated data might be unethically hacked to reveal the collected data, which attacks confidentiality and integrity of the data. Hence, an efficient data aggregation technique implementation is quite challenging as the designer must find a suitable tradeoff between energy efficiency, data accuracy, data latency, fault-tolerance, and security [3]. We need a good security technique for protecting our sensed data and to maintain authenticity and confidentiality of the data packets delivered to the gateway.

Thus, providing confidentiality to the aggregated data is an important task. Confidentiality helps in securing our data from any kind of breach. Spread spectrum modulation is one such technique which avoids intentional and unintentional interference. Here, a data signal of a particular bandwidth is spread in frequency domain, which results in wider bandwidth signal. The two predominant techniques used are Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread

Manuscript received November 20, 2022; revised December 20, 2022; accepted February 1, 2023.

Spectrum (DSSS). In FHSS, the narrow band signal is made to switch to random narrow bands within a larger bandwidth. While, in DSSS a rapid phase transition is done on the data to widen its bandwidth. FHSS technique is better than DSSS as there are different carrier frequencies involved, it avoids the problem of failing communication which might occur due to fading or a particular interferer. Also, DSSS radios are more complicated and consume greater power than FHSS technique. DSSS systems are more costly than FHSS systems [4].

In this research work, we will be implementing a data aggregation technique with frequency hop spread spectrum to add confidentiality. The data aggregation technique proposed here involves averaging the incoming data from node and sending only the averaged value to the gateway. Further, the spread spectrum modulation technique proposed here is Binary Phase Shift Keying (BPSK) which is further spread with frequency hopping technique using six different frequencies in the spread code. Here, we present the research work by providing an overview of the literature survey in Section II. Section III defines the problem statement and solution while Section IV provides the detailed approach by presenting the methodology and flow chart. Further, Section V presents the Results and Discussion. Finally, we conclude the work in Section VI.

II. Literature Survey

WSNs provide a great scope for researchers especially in the domain of energy efficient WSNs. Data aggregation is a technique used to reduce the energy requirement in the network and security to the data is very essential. Many researchers have proposed various aggregation techniques and security methods. Tabha and Althunibat [5] proposed the Chirp Spread Spectrum (CSS) modulation wherein the security is introduced by keying in a secret frequency shift in the transmitted chirp. The technique provided good confidentiality against eavesdropping. Qiu and Zhao et al. [6] also used the CSS approach but used the doppler frequency shifts into linear chirps. Next, in Othman and Bahattab et al. [7] a symmetric key homomorphic encryption technique was implemented to achieve data confidentiality. The results showed improved confidentiality at very low power consumption and prolonged network lifetime. Veeramallu, Sahitya, and LavanyaSusanna [8] proposed sensor network encryption protocol for maintaining authenticity and confidentiality of the transmitted data. In Chaitali and Pawar [9], a survey of digital watermarking technique was implemented to provide security and copyright to the data. Further, in Boubiche and Boubiche et al. [10], a watermarking technique was implemented without encryption. It provided authenticity and integrity for the data sensed at the same time saved network energy. Gao, Feng, and Han [11] implemented reversible watermarking schemes in WSN for implementing security with very less computational cost. Sharma and Richa [12] presented the different spread spectrum techniques and implemented them in MATLAB and the simulation results were compared. Yadav and Neelakanta [13] and Xu and Wang et al. [14] implemented frequency hop spread spectrum modulation (FHSSM) technique in MATLAB and calculated its performance in different frequency bands by evaluating the Bit-Error Rate (BER). Further, Badiger and Nagaraja [15] implemented the FHSSM with Additive White Gaussian Noise (AWGN). The results showed the recovery of data and estimated BER. Mohankumar, Selvi, and Sakethmanukonda [16] implemented a transmitter using FHSSM techniques with Binary Phase Shift Keying (BPSK) modulation in VHDL. It showed that FHSS technique provides better security than DSSS. In this research works, we implement FHSS technique with BPSK modulation technique on aggregated data using MATLAB. BER is estimated to evaluate the performance of the network.

III. Problem Statement and Solution

WSN are resource restrained. The energy of the network is a very important resource that needs to be efficiently utilized. Sensor nodes sense data in bulk and transmit it to the base station via cluster heads using hierarchical clustering technique. Here lot of data similarity exists in the transmitted data. Thus, it consumes more network energy which reduces lifetime of the network. Also, data sent to the gateway requires confidentiality as data breach can occur. In this research work, we follow a two-fold path to address the problem. First and foremost, we efficiently utilize the network energy by aggregating the data which reduces the number of transmission packets and thereby reducing the amount of energy required in transmission of bulk data. Next, to overcome the interference problem, we propose a Binary Phase shift keying modulation scheme with Frequency Hopping Spread Spectrum (FHSS) technique to encode and decode the signal. This increases the confidentiality of the data.

IV. Methodology and Flow Chart

In this research work, we propose a technique to achieve confidentiality to the aggregated data. Fig. 1 shows an overview of the scenario under consideration.

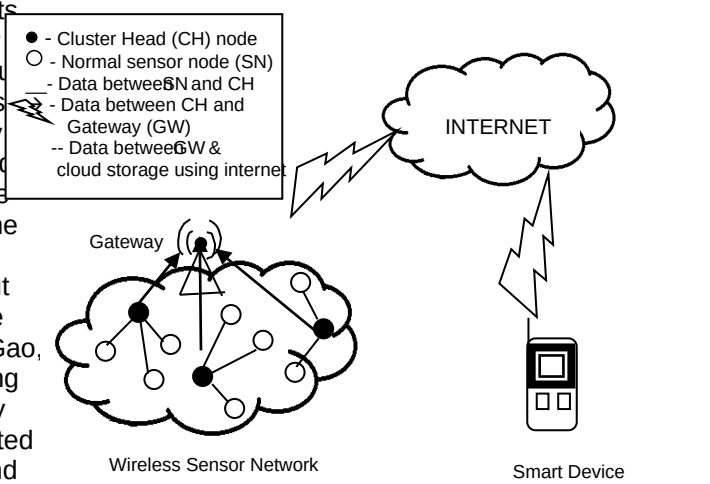

Figure 1. A WSN with data aggregation and confidentiality carried out in cluster heads and transmitted on IoT via gateway.

The data sensed by the sensor nodes is transmitted to the cluster head present in that cluster. The Cluster Head (CH) performs data aggregation and adds confidentiality to the data. Further, it transmits this data to the Gateway (GW) which routes the data to the smart devices on the internet. Here, we achieve energy efficiency in the WSN by performing data aggregation on the data at the Cluster Head (CH) before it is transmitted to the GW. Also, a spread spectrum technique: Frequency Hop Spread Spectrum (FHSS) technique is implemented on a Binary Phase Shift Keyed signal. This provides confidentiality to the signal.

In the following part we present the proposed data aggregation, confidentiality technique, analytical evaluation parameters and the flow chart.

A. Proposed Data Aggregation Technique

Data aggregation reduces the amount of energy required in transmission of the data to the gateway [17]. There are many data aggregation techniques available like averaging method, data prediction method etc. Each of these techniques will evaluate a value which will be sent to the base station for further processing. Even though these techniques involve a certain amount of error compared to the actual sensed value, the error is negligible as large number of nodes are dispersed in a given area. All the sensor nodes almost sense the same physical value in that environment. So, the value that is chosen depending on the aggregation technique is usually with negligible error. Data prediction algorithms are more complex and energy consuming than averaging method. Hence, the averaging method is chosen in the research work. So, in our proposed data aggregation technique, the process followed is as given below:

- First, we generate digital data randomly which depict the data sensed by the sensor nodes.
- The average value of every 15 random data points is evaluated
- Only the average value is sent to the gateway.

This technique reduces the amount of data sent to the gateway thereby efficiently conserves energy and increases network lifetime.

B. Proposed Confidentiality Technique

Here, the confidentiality of the aggregated data is maintained by performing BPSK modulation on the aggregated data as the message signal. Next, FHSS technique is applied on BPSK signal to spread the signal [4]. Fig. 2 shows the block diagram of BPSK/FHSS technique.

The following steps are carried out:

- At the transmitter side, first we generate NRZ polar format bit pattern for the aggregated data viz., message signal.
- Generate a cosine carrier signal
- Perform BPSK modulation

$$bpsk\_sig = signal \times carrier \quad (1)$$

- Next, for spreading the signal generate 6 new carrier frequencies for the given time durations

$$t1 = 0:2 \times pi/8:2 \times pi \quad (2)$$

$$t2 = 0:2 \times pi/9:2 \times pi; \quad (3)$$

$$t3 = 0:2 \times pi/17:2 \times pi; \quad (4)$$

$$t4 = 0:2 \times pi/35:2 \times pi; \quad (5)$$

$$t5 = 0:2 \times pi/89:2 \times pi; \quad (6)$$

$$t6 = 0:2 \times pi/179:2 \times pi; \quad (7)$$

- Cosine carriers are generated.
- Then BPSK signal generated is hopped to different carrier frequency randomly to spread the signal.

$$freq\_hopped\_sig = bpsk\_sig \times spread\_signal \quad (8)$$

- A Rayleigh flat fading random variables are introduced to evaluate the performance of the system
- At the receiver, we despread and demodulate the signal.

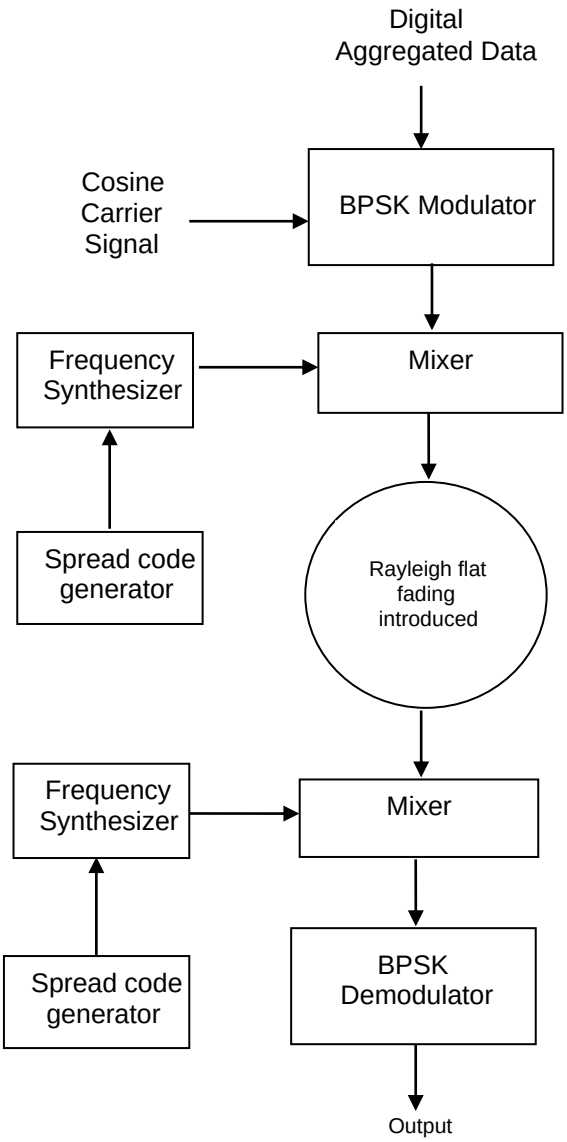

Figure 2. Block diagram for BPSK/FHSS technique.

C. Analytical Evaluation Parameters

For evaluating the performance of the WSN, the following steps are carried out:

- Evaluate BER of BPSK/ FHSS over Rayleigh flat fading random values
- Plot the Power Spectral Density (PSD), FFT of BPSK / FHSS signal as a function of frequency.

D. Flow Chart

Fig. 3 represents the steps carried out in the proposed research work. Two important techniques carried out here are data aggregation and spread spectrum modulation.

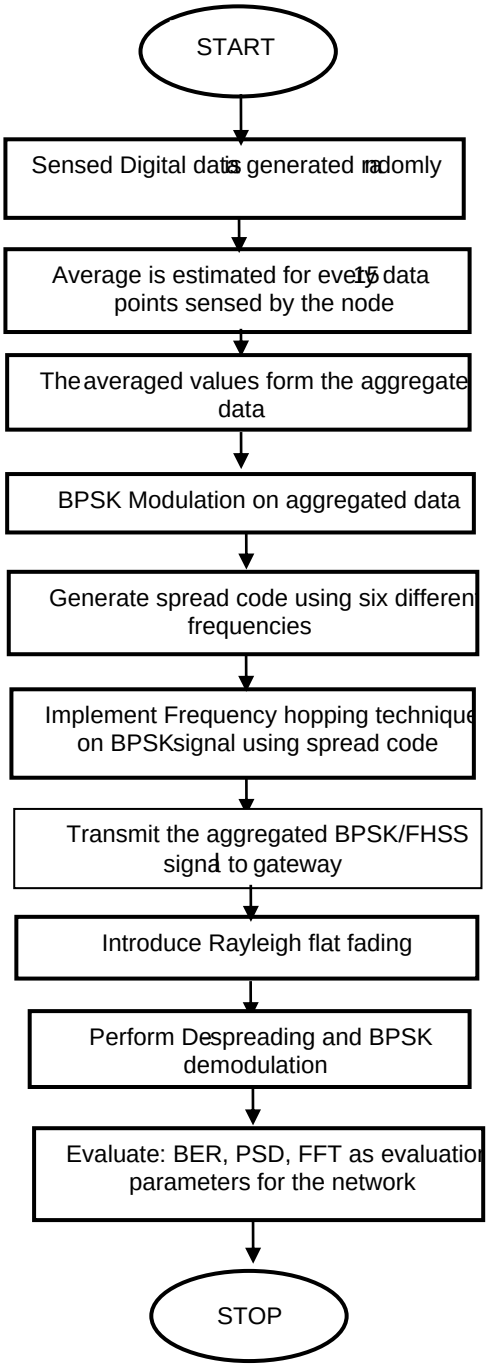

Figure 3. Flow chart depicting the proposed research work

V. Results and Discussion

The data aggregation and confidentiality techniques are implemented using MATLAB 2020a [18, 19]. Figs. 4-8 below show the simulation results carried out on digital data. For data aggregation, we consider randomly generated 3600 bits. On aggregation, the data is reduced to 180 bits. This clearly conserves energy required in transmitting the data to gateway and increases network lifetime.

- Fig. 4 shows the simulation results of (i) digital information, (ii) NRZ polar format of (i), (iii) BPSK modulated signal, (iv) Spreading code with 6 frequencies, (v) Frequency Hopped Spread Spectrum Signal. Here, any random digital information is considered as the parameter sensed by the sensor node. The simulation generates 3600 bits and for clarity (i) represents a small part of 20 bits. In (ii) the NRZ polar format representation of the digital data is plotted. Using (ii) as message signal and cosine carrier signal BPSK modulation is performed and the resulting wave is plotted in (iii). Next, 6 different frequencies are randomly picked and spread code is generated and plotted in (iv). Finally, the BPSK wave is spread using (iv) and frequency hopped SSM wave is plotted in (v). In this approach, the sampling frequency of 3600 bits/sec ie 3.6KHz for the initial random sensor values is considered. However, the work can be carried out for higher frequencies too. To restrict the number of samples and illustrate the behavior of each bit in spread spectrum frequency hopping technique, the study chooses this value.
- Fig. 5 shows the simulation results of (vi) demodulated BPSK signal, (vii) demodulated binary signal and (viii) BER of BPSK/FHSS over Rayleigh flat fading channel. Now, at the receiver side, the introduction of Rayleigh Flat Fading to the BPSK/FHSS signal is also considered. We next perform BPSK demodulation in (vi) and obtain the demodulated binary signal in (vii) which is same as the original signal. The plot in (viii) shows the BER estimation. The simulation and theoretical values shown in Fig.8 are very close to each other which confirms the robustness of the technique implemented. Here, the BER value decreases from 10^{-1} to 10^{-4} as we increase the SNR. With further increase in SNR, the BER reduces
- Fig. 6 shows the Power Spectral Density (PSD) of BPSK / FHSS signal as a function of frequency. The PSD of a signal represents the amount of power present in the signal per unit frequency. Here, we get 7.518 mW at 5MHz of power as the maximum power consumed. Thus, the technique is energy efficient.
- Fig. 7 shows the Frequency Hopped Spread Spectrum Signal and its Fast Fourier Transform (FFT). FFT is used to process data in WSNs to calculate the different frequency components and to reconstruct the original signal from them. The FFT gives the frequency information about the BPSK/FHSS

modulated wave. Here, the frequencies present in the vibrations range from 0 to 822MHz and 2544 to 3593 MHz ranges.

x BER Analysis: We plot the theoretical and practical Bit error for each bit. The results show that the difference in these BER values becomes zero as the SNR increases as shown in Fig. 8. The results show very low BER values of the order 10^{-1} to 10^{-3} as SNR increases from 0 to 25 dB. The results conclude that when SNR is low there is one error bit for every 10 bits transmitted and when is SNR is increased there is one error bit for every 1000 bits transmitted.

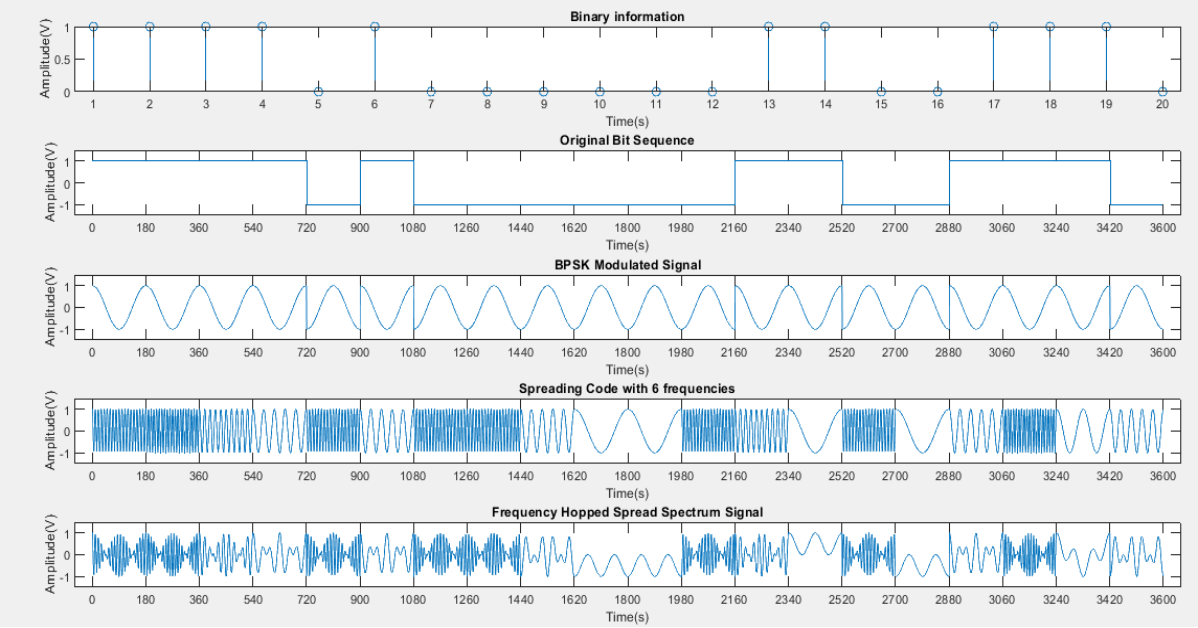

Figure4. Simulation results of (i) digital information, (ii) NRZ polar format of (i), (iii) BPSK modulated signal, (iv) Spreading code with 6 frequencies, (v) Frequency Hopped Spread Spectrum Signal

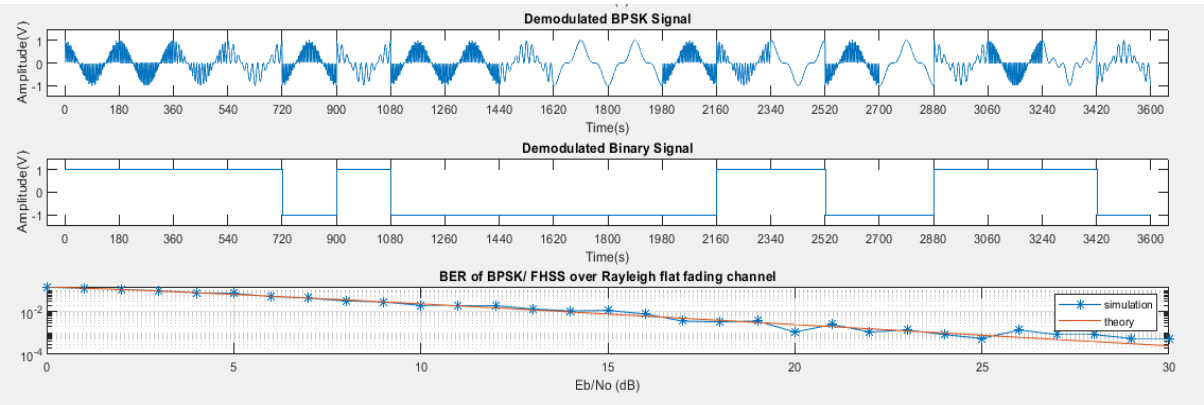

Figure5. Simulation results of (vi) demodulated BPSK signal, (vii) demodulated binary signal and (viii) BER of BPSK/FHSS over Rayleigh fl fading channel

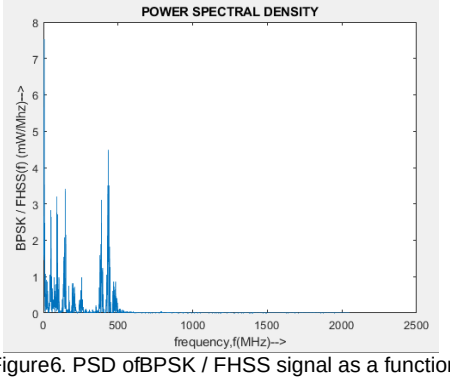

Figure6. PSD of BPSK / FHSS signal as a function of frequency.

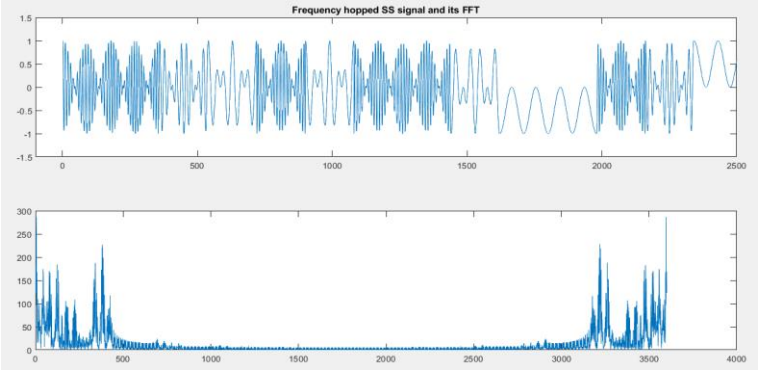

Figure7. Frequency hopped spread spectrum signal and its FFT.

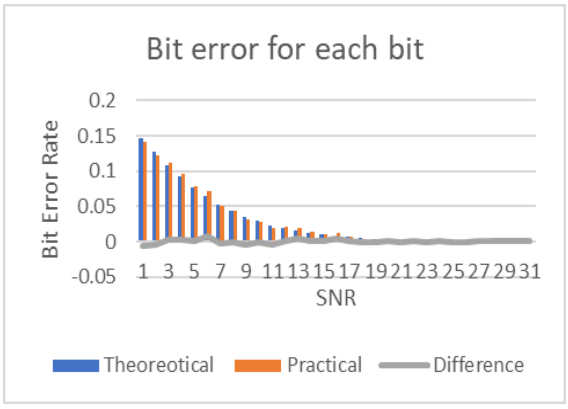

Figure8. Bit error Rate v/s SNR

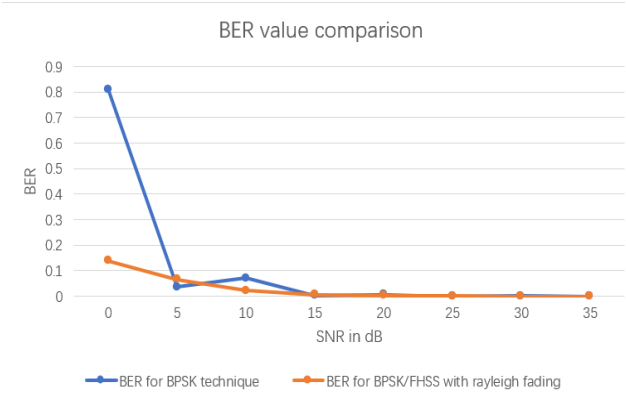

Figure10. Bit error Rate v/s SNR in i. BPSK technique, ii. BPSK/FHSS technique over a Rayleigh fading channel.

The BER values obtained in the work is compared with [20] as shown in Fig. 9, which works on evaluating BER for BPSK over a Rayleigh fading channel. Table I represents the BER values obtained from graph of [20] for values of SNR (in dB) and Fig. 5 (viii) BER of BPSK/FHSS over Rayleigh flat fading channel of this study.

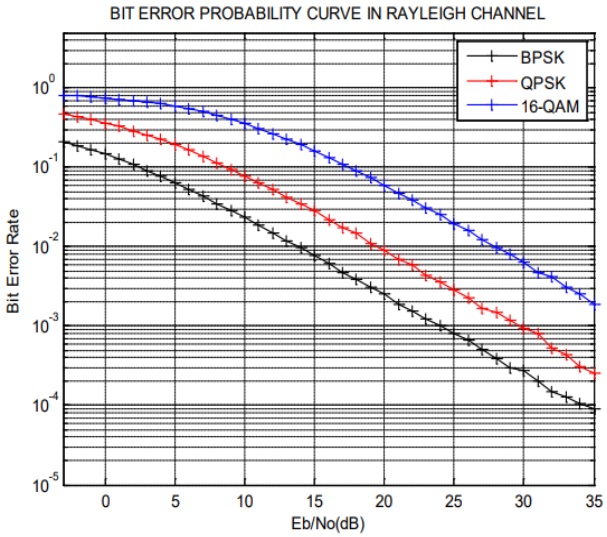

Figure9. Bit error Rate v/s SNR for BPSK over Rayleigh channel. [20]

TABLE I. COMPARISON OF BER VALUE

SNR in dB	BER in [20]	BER in Proposed Technique
0	0.81	0.138889
5	0.036	0.066667
10	0.072	0.0225
15	0.0027	0.006944
20	0.0072	0.003056
25	0.00027	0.001389
30	0.00072	0
35	0.000018	0.000278

Fig. 10 shows that the BER values almost overlap and become negligible as SNR increases in both the techniques.

VI. CONCLUSIONS

WSNs in IoT are instrumental in collecting huge amount of data from the environment [21, 22]. Conserving the energy of WSN is a primary requirement [23, 24]. Thus, a data aggregation technique is implemented in this research work to reduce the number of data points sent to the gateway. This aggregation takes place only at the Cluster Heads and not at every node of the WSN. Further, the aggregated data is secured by adding confidentiality to the same. BPSK/ FHSS technique is implemented in this research work. The technique stands robust against Rayleigh Flat Fading signal and generates the original signal [25]. Here, BER reduces as we increase the SNR (as shown in Fig.7). Also, the simulation results and theoretical values match to a greater extent. The maximum power consumed by the BPSK/FHSS signal is as low as 7.518 mW at 5MHz. Hence, a confidentiality enhanced energy efficient WSN is simulated and presented in this research work which can be implemented on IoT.

CONFLICT OF INTEREST

The authors declare no conflict of interest

AUTHOR CONTRIBUTIONS

Trupti Shripad Tagare conceived the idea on design and development of data aggregation and confidentiality enhancement technique. Rajashree Narendra mentored in the design and simulation of the proposed technique. Further, the authors discussed in detail simulation, comparative analysis and results contributing towards this final manuscript.

REFERENCES

[1] P. P. Kakani, "Data aggregation and gathering transmission in wireless sensor networks: A survey," Thesis work, Master of Electrical Engineering: Specialization in Embedded Systems, Helsinki University of Technology

[2] R. Bista, Y.-K. Kim, and M.-S. Song, "Improving data confidentiality and integrity for data aggregation in wireless sensor networks," IEICE Trans. on Information and Systems, vol. 95, pp. 6777, Jan. 2012.

[3] M.-S. Yousefpoor, E.-Yousefpoor, H. Barati, A. Barati, A. Movaghar, And M. Hosseinzadeh, "Secure data aggregation

methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," Journal of Network and Computer Applications, vol. 190, ISSN 1084-8045, 2021
[4] M. Hasan, J. M. Thakur, and P. Podder, "Design and implementation of FHSS and DSSS for secure data transmission," International Journal of Signal Processing Systems, vol. 4, no. 2, pp. 144-149, April 2016.
[5] F.-A. Taha and S Althunibat, "Improving data confidentiality in chirp spread spectrum modulation," presented at IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Oct. 2021.
[6] S. Qiu, D. Zhao, and Y. Wang, "A linear chirp wireless transmission method utilizing Doppler effect," Wireless Personal Communications, vol. 124, pp. 2965-2982, Jan 2022.
[7] O. Soufiene, B. Abdullah, T. Abdelbasset, and Y. Habib, "Confidentiality and integrity for data aggregation in WSN using homomorphic encryption," Wireless Personal Communications, vol. 78, no. 3, Oct. 2014.
[8] B. Veeramallu, S. Sahitya, and C. L. Susanna, "Confidentiality in wireless sensor networks," International Journal of Soft Computing and Engineering (IJSCE), vol. 2, issue 6, pp. 471-474, Jan. 2013.
[9] J. Chaitali and P.-M. Pawar, "Secure data aggregation using watermarking technique for wireless sensor network-a review," International Journal of Computer Application (2250-1797), vol. 7 – no. 3, pp. 80-87, May - June 2017.
[10] D. Boubiche, S. Boubiche, C. H. Toral, A. Pathan, A. Bilami, and S. Athmani, "SDAW: Secure data aggregation watermarking-based scheme in homogeneous WSNs," Telecommunication Systems, April 2015.
[11] G. Gao, Z Feng and T Han, "Data authentication for wireless sensor networks with high detection efficiency based on reversible watermarking," Hindawi Wireless Communications and Mobile Computing, vol. 2021, Article ID 6651137, p. 13, 2021.
[12] V. Sharma and R. Sharma, "Analysis of spread spectrum in MATLAB," International Journal of Scientific & Engineering Research, vol. 5, issue 1, ISSN 2229-5518, Jan 2014.
[13] P. Yadav and U. Neelakantan, "Performance Analysis of FHSS Transceiver Model in MATLAB," International Research Journal of Engineering and Technology (IRJET), vol. 2, issue 2, pp. 349-351, 2015.
[14] X. Xu, W. Wang, L Yi, J. Rong, and A. Wang, "Simulation of frequency hopping communication system based on MATLAB," presented at MATEC Web of Conferences 61, 01019, DOI: 10.1051/matecconf/20166101019, 2016.
[15] R. Badiger, M. Nagaraja, M.-Z Kurian, and I. Rasheed, "Analysis, design and testing of frequency hopping spread spectrum transceiver model using MATLAB – Simulink," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 3, issue 2, pp. 7432-7438, Feb 2014
[16] K. Mohankumar, M. Selvi and Sakethmanukonda, "Development of FHSS transmitter using BPSK modulation in VHDL," Middle-East Journal of Scientific Research 24, ISSN 1990-9233, pp. 101-106, 2016.
[17] T.-S. Tagare and R. Narendra, "Performance analysis and assessment of various energy efficient clustering based Protocols in WSN," in Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies, A. P. Pandian, X. Fernando, W. Haoxiang, eds vol. 117, Springer, Singapore, 2022.
[18] Q. Ali, A. Abdulmaowjod, and H. M. Mohammed, "Simulation and performance study of wireless sensor network (WSN) using MATLAB," Iraqi Journal for Electrical and Electronic Engineering, vol. 7, no. 2, pp. 112-119, December 2011
[19] P.-G. Vispute and R.-S. Kawitkar, "MATLAB implementation of wireless sensor network (WSN) in precision agriculture in rural India," International Journal of Engineering Research & Technology (IJERT), vol. 01, issue 04, June 2012
[20] A. Agarwal and K. Agarwal, "Implementation and performance evaluation of OFDM system in diverse transmission channel using Simulink," American Journal of Electrical and Electronic Engineering, vol. 3, no. 5, 117-123, 2015.
[21] M. Kocakulak and I. Butun, "An overview of Wireless Sensor Networks towards internet of things," in Proc. 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1-6.
[22] T.-S. Tagare, R. Narendra, and T.-C. Manjunath, "A GUI to analyze the energy consumption in case of static and dynamic nodes in WSN," in Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, S. Shakya, R. Bestak, R. Palanisamy, K. A. Kamel, eds, vol. 68, 2022.
[23] N. Zaman, L-T. Jung and M.-M. Yasin, "Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol," Journal of Sensors, Article ID 9278701, p. 16, 2016
[24] T.-S. Tagare and R. Narendra, "Implementation and performance analysis of PEGASIS and MIEEPB Protocols in wireless sensor networks," Lecture Notes in Networks and Systems, vol. 459, pp. 45-54, 2022
[25] V. Nithya, R Balasubramanian, and V. Bhaskar, "BER evaluation of IEEE 802.15.4 compliant wireless sensor networks under various fading channels," Wireless Personal Communications, vol. 77, no. 4, August 2014