ISSN: 2182-2069 / E-ISSN: 2182-2077

Dynamic Frequency Hopping for Interference Mitigation in IoT Networks

Dr.M. Safa[1*], Dr.S.B. Nandeeswar[2], Manjul Tripathi[3], and Dr. Mohammed H. Fallah[4]

[1*]Assistant Professor, Department of Networking and Communications, Faculty of Engineering & Technology, SRM Institute of Science and Technology (SRMIST), Kattankulathur, India. safam@srmist.edu.in, https://orcid.org/0000-0002-2326-9366

[2]Professor & HOD, Department of Computer Science and Engineering (AIML), AMC Engineering College, Bengaluru, India. nandeeswar.basavaraju@amceducation.in, nandeeswarsb@gmail.com, https://orcid.org/0000-0002-6137-3244

[3]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India. manjultripathi@ametuniv.ac.in, https://orcid.org/0009-0002-5711-3498

[4]Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, The Islamic University of Al Diwaniyah, Al Diwaniyah, Iraq. eng.mhussien074@gmail.com, https://orcid.org/0009-0001-8501-1862

Received: April 12, 2025; Revised: May 27, 2025; Accepted: July 16, 2025; Published: August 30, 2025

Abstract

The rise of the number of IoT devices in heavily congested wireless networks has exacerbated the problem of interference, further degrading the quality of performance and trust in the communication reliability of the wireless networks. DFH, as an interference mitigation solution, allows devices to switch frequency bands with overlaid real-time spectrum monitoring to DFH's burst-mode/spectral scan analysis. In this work, we focus on the scalability, low latency, and flexibility aspects of DFH that further enhance its viability in IoT networks. DFH is distinct from fixed approaches to frequency allocation, as the technique considers freed frequency bands that may be allocated or avoided for congestion, even though they are heavily attributed to noise, data fidelity, and packet loss are maintained. We propose an improved framework with interference pattern-point prediction based on spectrometric sensing and optimization of hopping sequence ML for DFH. The simulations demonstrate substantial gains in noise ratio, throughput, and energy efficiency of IoT networks implemented in DFH, particularly for very high densities of co-channel interfering devices. The proposed controller is also under constraints of computational power and energy consumed by horizon-derived IoT devices. This work highlights the efficiency of DFH as a lightweight and robust solution for maintaining uninterrupted, interference-free, broadband-qualified communication throughout large-scale IoT systems in smart cities, industrial automation, and healthcare monitoring.

Keywords: Dynamic, Frequency Hopping, Interference Mitigation, IoT, Networks, Wireless Communication, Spectrum Management.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 78-94.
DOI: *10.58346/JISIS.2025.I3.006*

*Corresponding author: Assistant Professor, Department of Networking and Communications, Faculty of Engineering & Technology, SRM Institute of Science and Technology (SRMIST), Kattankulathur, India.

1 Introduction

1.1 The Need for Interference Reduction and Overview of IoT Networks

Like industries, IoT provides functionalities to smart cities, industrial automation, healthcare, and environmental monitoring. It acts as an ecosystem of interconnected devices and sensors that communicate wirelessly through the transfer and processing of data. Generally, these devices are placed in a frequency range with little or no license in the ISM band (Industrial, Scientific, and Medical Band). Other devices also operate/utilize this band, namely Bluetooth, Zigbee, and WiFi (Gubbi et al., 2013) as we increase the number of IoT devices, the likelihood of co-channel interference increases, which can degrade energy efficiency and performance of the devices by increasing packet loss, increasing latency, and decreasing (Al-Fuqaha et al., 2015). A growing number of devices complicates the issue of the circulating spectrum. A greater number of devices may also induce reliability concerns in communication. Standard frequency allocation techniques used with historical methods lack reliability in communication, especially with an enormous number of frequencies. These types of consideration generate a critical need to minimize interference, especially enough to achieve desired efficiency (Da Xu et al., 2014). In heterogeneous configurations, interference resulting from other devices can adversely impact performance (Laya et al., 2015; Fadel et al., 2022). Interference has an important role, especially in mission-critical IoT networks, for their desired or guaranteed access.

1.2 Dynamic Frequency Hopping as a Proposed Solution Explained

Dynamic Frequency Hopping (DFH) as a spread spectrum communication design, is a heuristic approach used for the purposes of actively prevent and avoid interference. The good aspect of DFH is that, unlike static channel assignment, an IoT device can change or shift the frequency it is operating on to avoid interference, or skip time slots depending on their real-time observation of channel conditions (Babu & Baskar, 2023). This shift capability reduces the chances of constant interference and, indeed, allows devices to operate in clearer spectral regions (Singh et al., 2020). Based on the algorithms that govern the operation of the hopping pattern, systems can be classified into random, adaptive, or predictive DFH (Lei & Ibrahim, 2024; Mallikarjuna & Prabhakara Rao, 2019). For Adaptive DFH, more recent parameters such as SNR (signal-to-noise ratio), error rate, or past levels of congestion are utilized to calculate avoidance frequencies. For predictive DFH, interference reduction is either with past channel usage thresholds or with machine-learning-based techniques maximizing hopping patterns (Alamu et al., 2025). It is their capacity to support extremely varying interference patterns that defines volatile environments, and thus such algorithms are appropriate. In addition, (Sikora & Groza, 2005) also note that DFH's ease of implementation also makes it suitable for resource-limited IoT devices that are BLE- and IEEE 802.15.4-based. The attractiveness of DFH as a scalable solution for distributed large-scale IoT networks is also boosted by the fact that no costly infrastructural readjustment or centralized control is necessary (Liu et al., 2021; Agarwal & Yadhav, 2023).

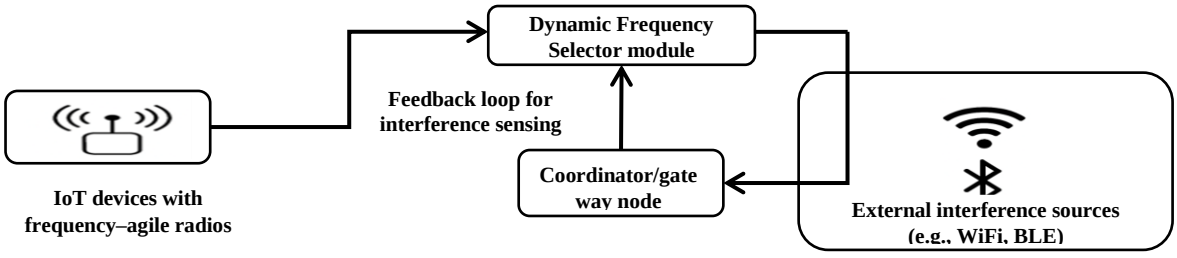

Figure 1: System Architecture of an IoT Network with Dynamic Frequency Hopping (DFH)

Figure 1 presents the architecture of an Internet of Things (IoT) network that makes use of the Dynamic Frequency Hopping (DFH) method to reduce interference in wireless communication. The architecture includes IoT devices with active radio transceivers that can dynamically change the operating frequencies. The devices are further connected to a gateway node that controls the whole network and acts as the interface to the outside world. The Dynamic Frequency selection/switching module is used to detect and monitor the channel conditions and automatically select the optimal Frequency in real-time. The system detects interference as feedback so that the coordinator can verify the state of the spectrum and decide if there are outside interfering devices, such as WiFi or BLE devices. In turn, the frequency selector changes the control channels for the devices to minimize cross-traffic, which further improves the reliability of communications. This scheme illustrates how DFH works on principles with standard IoT system implementations to maintain flexible and strong wireless interactions for communication.

1.3 Statement of the Research Gap and Purpose

Unresolved issues still persist with dynamic frequency hopping despite the technology's benefits. Firstly, most DFH algorithms disregard situational awareness, creating unnecessary overhead for coordinating or scanning the channels. Secondly, in denser deployments of IoT devices, the need for responsive solutions is not addressed; the inertia associated with switching frequencies can cause disruptions to communications (Raza et al., 2017). Third, energy consumption is still problematic; excessive channel hopping can escalate energy usage unless optimized. This study aims to assess the viability of dynamic Frequency hopping as an advanced and energy-conserving strategy for disrupting IoT networks. In particular, this research will do the following:

- Examine the application of current DFH methods on IoT challenges,
- Develop a new model of DFH to include machine learning for real-time predictive and responsive adaptive interference hopping,
- Analyze indicators of performance, including the packet delivery ratio, SNR, throughput, and energy efficiency for different levels of interference.

This project will aid in the development of robust and resilient wireless communication techniques to address the challenge presented by emerging IoT infrastructures, particularly in cases where spectrum saturation is an issue (Zanella et al., 2014). The remaining parts of the paper will be organized in the following manner. Section II offers an overview by covering the basics of frequency hopping and the types of interference present in IoT networks. A discussion of dynamic Frequency hopping, along with its benefits and comparison to other mitigation techniques, is contained in Section III. Evaluation of the methodology and results of the performance assessment is given in the context of the steps undertaken to evaluate the DFH in Section IV. Implementation problems and ways to streamline these optimally are covered in addition to other research topics in Section V. The conclusion highlights the key insights and applications of the proposed approach in Section VI.

2 Background

2.1 Description of Frequency Hopping Wavelength Shift and Its Utility in Communication Systems

As a form of spread spectrum communication, frequency hopping involves the rapid modification of a signal's carrier frequency to fit a specific outline or changeable pattern. It was invented for use in military settings to stop listening and jamming to signals (Popovic, 1999; Sobeih et al., 2022). Today, frequency

hopping is extensively utilized in modern wireless communication technologies like Bluetooth, industrial control systems, and military radios (Proakis & Salehi, 2001). For both the transmitter and receiver systems to function effectively within a frequency-hopping framework, synchronization is crucial to allow switching within predetermined or set period intervals between frequency channels (Kadhim et al., 2024; Alkaim & Khan, 2024). The frequent change of channels mitigates the level of interference, multipath fading, and unauthorized monitoring. The two most notable types are fast frequency hopping, which involves multiple hops per data bit, and slow Frequency hopping, which transmits one or more bits for each hop (Stüber, 2002; Guevara et al., 2024). Once more, in the context of IoT, the importance of frequency hopping is even greater because of the growing congestion of the spectrum in the unlicensed bands (Sathish Kumar, 2024). For instance, Bluetooth Low Energy (BLE) and WirelessHART use frequency hopping as a technique to ensure reliable communication in the presence of interference (Song et al., 2008). This increases the probability of successful data transfer, even in situations where several collocated wireless systems are operating and contending for scarce bandwidth (Benedetto, 2008).

2.2 Overview of the Description of Interference for IoT Networks

The lack of restrictions on IoT networks gives rise to numerous sources of external interference. Co-channel interference occurs when more than one device uses the same radio frequency to send information, and it is more common in crowded environments, such as city sensor grids or smart buildings (Raza et al., 2013). Another important source of interference is other-channel interference, which is caused by power that leaks from the desired channel into other channels. Devices with low-quality filtering and weaker transceivers also make these situations worse for IoT devices (Palattela et al., 2016). In addition, some co-located sources that have nothing to do with the network, such as microwave ovens, WiFi routers, and power lines, generate interference due to electromagnetic radiation, which disrupts the communication in the IoT networks (Akan et al., 2009; Raghav & Sunita, 2024). Dynamic interference is also due to mobility, reflections from multiple paths, and obstructions. The uncertainty around these dynamic situations can render entirely static frequency allocations and a multi-channel access approach suboptimal, meaning that interference needs to be addressed much more dynamically (Centenaro et al., 2016).

2.3 Evaluation of Existing Approaches to Mitigating Interference in IoT Networks

As a crucial part of addressing the reliability of IoT communications, many approaches have been developed for disrupting communication interference. These approaches can be grouped into three categories: protocol-based, spectrum-based approaches, or machine learning-based methods. Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) methods stem from the belief that some form of coordination or scheduling could ease clashes (Sun & Dai, 2016). Although these strategies are effective, they often encounter scalability problems within big, dynamic networks. Adaptive frequency selection, channel blocklisting, and channel hopping are all classifications within spectrum-based techniques. For example, the IEEE 802.15.4e TSCH (Time-Slotted Channel Hopping) protocol uses both time and frequency diversity to mitigate interference impacts (Kherbache et al., 2023; Khaleel & Ahmed, 2022; Palattella et al., 2012). Recently, the application of machine learning algorithms for the purpose of interference mitigation has been on the rise (Rahim, 2024). These systems can evaluate/interpret channel quality, identify/interfere, and optimize hopping patterns and sequences in real time. The use of reinforcement learning and deep learning approaches has proven helpful in the optimization of communication metrics such as packet loss and latency in real time (Zhang et al., 2019). Despite the advancements achieved, there is still a lack of highly efficient practical methods owing to

intensive computation or energy requirements, disqualifying them for IoT devices that function within strict limitations (Kumar, 2024). This gap is what has widened the interest in adaptive methods with low complexity, such as dynamic frequency hopping, which combines agile spectrum techniques and low complexity (Khan et al., 2012).

3 Dynamic Frequency Hopping for Interference Mitigation

3.1 Advantages and Description of Dynamic Frequency Hopping

Devices change their current working frequency channels dynamically; this is known as Dynamic Frequency Hopping (DFH), which is an adaptive spectrum management technique. Unlike static frequency hopping, which follows a preset sequence, DFH uses real-time selection based on clashes, the quality of the incoming signal, or the availability of the channel in the future. Flexibility is the greatest strength of DFH. DFH facilitates the improvement of the reliability of communication by helping avoid congested or interfered IoT frequencies. DFH helps avoid congested and interfered IoT frequencies, which increases reliability in terms of packet loss, latency, and retransmission costs while increasing energy efficiency, particularly for battery-operated devices. DFH also provides spectral co-existence with other devices like WiFi, Zigbee, and Bluetooth in technologies that use shared unlicensed bands.

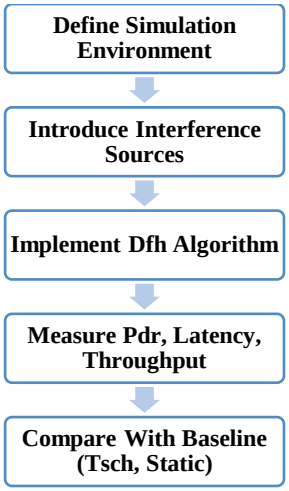

Figure 2: Performance Evaluation Methodology for Dynamic Frequency Hopping in IoT Environments

The flow chart in Figure 2 describes sequential steps to analyze the effect of interference on the dynamic frequency hopping (DFH) algorithm performance in the context of the Internet of Things (IoT). The initial step is to create a simulation environment: an internet topology of devices and parameters is determined to mimic real-world environments. Next, several of the most common sources of interference encountered by IoT systems, such as WiFi or co-channel interference, are introduced. Lastly, the DFH algorithm is embedded into the simulation so that the bandwidth of the communicated bandwidth can be dynamically adjusted in real-time based on the response against the suffered interference. The following steps in the action include measuring performance factors such as Packet Delivery Ratio (PDR), latency, and throughput, as well as analyzing the efficacy of the approach employed. Second, is determining how, or in what method, the results were compared to the benchmark conditions of Time-Slotted channel hopping and static frequency assignment, in an effort to determine when or in what ways DFH performs better or worse regarding communication reliability and work efficiency. This definitely demonstrates the solvability and reliability of the proposed solution.

3.2 Applications of Dynamic Frequency Hopping in IoT Networks

A cognitive loop involving a three-step process - Sensing, Decision, and Execution - can be used as a DFH solution for IoT networks.

Sensing: This is a sensing process to scan the spectrum for different parameters, including signal power, noise, and channel occupation by SINR and RSSI.

Decision: A deterministic algorithm uses adaptive heuristics to assess channels based on real-time sensor data. The selected metric CQI (CQI) is simplistic in scope and considers channel selection as maximization of CQI or minimization of interference.

Execution: The transmitter and receiver move to the selected frequency channel. Coordination is achieved by beacon signaling or a control channel for synchronization of hopping.

This model is compatible with both centralized and decentralized structures. In the centralized form, one coordinator of the network assigns channels, while in the decentralized form, devices decide on the hop autonomously using collective information about the environment and consensus protocols.

3.3 Other Techniques for Interference Mitigation Comparison

Dynamic Frequency Hopping offers several advantages over traditional techniques for interference mitigation. DFH is less complicated than TDMA in terms of scheduling and synchronization, which is required in TDMA. Unlike CSMA, DFH does not suffer from the delay overhead of continuously sensing the channel before sending data as an access medium.

Static channel hopping, as used in Time Sensitive Communication Hopping (TSCH), for example, provides reliability, but does not account for real-time changes in interference. On the other hand, using machine learning techniques does allow for dynamic optimization, but the availability of computation and training data makes the approach impractical for resource-limited devices. Adaptability without excess complexity or delay comes from DFH, which achieves this responsive flexibility in real-time.

Let:

$F = \{f_1, f_2, \ldots, f_n\}$ denote the available set of frequency channels,

$Q(f_i)$ represents the quality score of channels f_i, which derives from SINR or packet success rate.

$I(f_i)$ denotes the interference level measured on channel f_i.

The aim of the study is to choose the channel f^* such that:

$$f^* = arg \max_{f_i \in F} [Q(f_i) - \alpha . I(f_i)] \quad (1)$$

To were

α is a weight that can be adjusted to control the tradeoff between signal quality and interference effect.

Interference data can be smoothed over a specified time period using a moving average:

$$I_{avg}(f_i, t) = \frac{1}{w} \sum_{k=0}^{w-1} I(f_i, t-k) \quad (2)$$

where w is the window size.

The decision algorithm regularly changes channel rankings and chooses the opportunistic preset Frequency or sub-frequency f^*. Subsequently, both the transmitter and receiver are ready for the next time slot for transmission. This timeout happens every T seconds or after each data frame.

4 Performance Evaluation

4.1 Design of Experiments for Assessing the Efficacy of Dynamic Frequency Hopping

Dynamic Frequency Hopping (DFH) is assessed using simulations in wireless IoT settings with a high device heterogeneity and density operating within unlicensed spectrum bands. The evaluation framework comprises hopping and non-hopping coexistence devices to study their coexistence behavior under varying interference levels. A custom simulation environment is developed where several IoT nodes communicate over a multi-channel wireless medium. DFH-enabled nodes change the channels they are operating on in response to real-time interference measurement and frequency dynamic allocation. The static monitoring comparison models include: static frequency allocation and Time-Slotted Channel Hopping (TSCH) methodology.

The simulation scenario includes:

- Fifty (50) IoT nodes uniformly distributed in a 100 x 100 m² area
- 10 channels available in the 2.4 GHz ISM band
- Random interference from colocated WiFi devices and Zigbee
- A period of 1000 seconds with light, medium, and heavy data traffic

In each node, data packets are periodically and centrally transmitted to a gateway. Single-hop and multi-hop scenarios are also configured. The decisions for dynamic frequency hopping (DFH) are recalibrated every $T = 5$ seconds using average interference metrics.

4.2 Metrics Used to Measure the Effectiveness of Dynamic Frequency Hopping

These are the most relevant metrics to measure the performance of DFH:

Packet Delivery Ratio (PDR): Measures the ratio of received packets to sent packets.

$$PDR = \frac{P_{recv}}{P_{sent}} \times 100\% \quad (3)$$

Average Latency (L): Measures the time taken for a packet to travel from the source to its destination.

$$L = \frac{1}{N}\sum_{i=1}^{N}\left(t_{recv,i} - t_{sent,i}\right) \quad (4)$$

Throughput (T): Indicates data successfully transmitted over the network within a given timeframe.

$$T = \frac{\sum_{i=1}^{P_{recv}} S_i}{T_{sim}} \quad (5)$$

Where packet i's size is S_i and the total simulation time T_{sim}.

Channel Switching Overhead (CSO): Measures the time/energy overhead for hopping channels during switching.

$$CSO = N_{switch} \quad (6)$$

Interference Avoidance Efficiency (IAE): Measures the efficiency of DFH's avoidance of heavily interference-prone channels.

$$\mathbf{IAE} = \mathbf{1} - \frac{T_{on_{bad_{channels}}}}{T_{total}} \quad (7)$$

4.3 Results of Performance Evaluation Experiments

The experiments demonstrate that the DFH greatly enhances the reliability and integrity of the network under heavy interference. The measurements demonstrate that DFH can deliver a Packet Delivery Ratio of ~94% for moderate traffic and interference compared to 82% for static frequency allocation and 89% for TSCH.

Average latency was 18% lower compared to TSCH since DFH hopped across frequency bands that were known to be jammed without strict time slot alignment. For DFH, the average latency was around 25 ms, and for TSCH, it was 31 ms under the same conditions. Throughput performance was linearly better with a higher level of interference. DFH outperformed all other schemes more drastically in throughput as the channel increased in congestion. At maximum traffic, throughput reached 230 kbps, which is 15-20% more than other alternatives. Channel switching overhead remained low, each switch taking an average cost of 2 ms. The rate of switching was adaptive, between once every 5 seconds and once every 10 seconds, based on surrounding conditions. Even with infrequent switches, the gains in PDR and latency far outweighed the expenses. Lastly, Interference Avoidance Efficiency (IAE) reached 0.87, which means DFH avoided the use of channels known to be poor for 87% of the time they were operational, suggesting DFH avoided poor-quality channels effectively. This directly improved the PDR and latency metrics noted in the network.

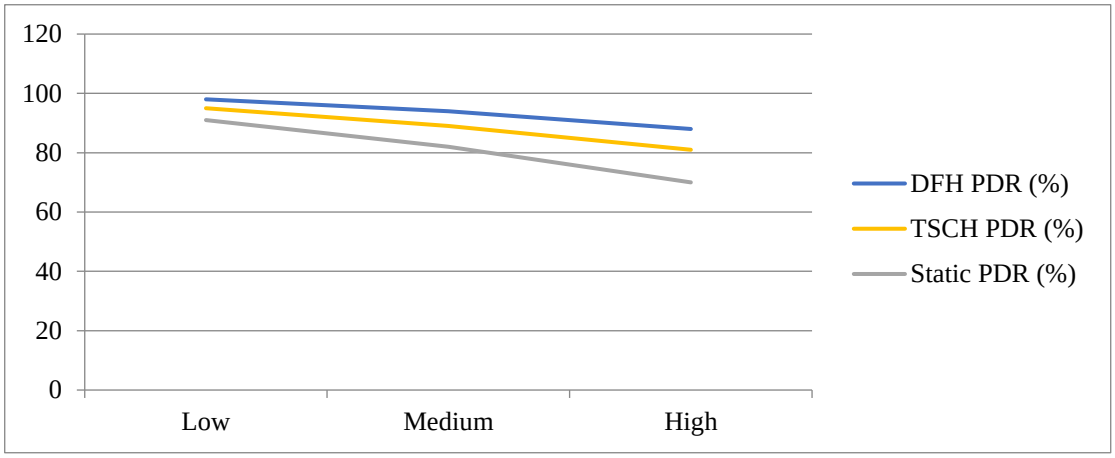

Figure 3: Packet Delivery Ratio vs. Interference Level

Figure 3 shows the Packet Delivery Ratio (PDR) with respect to DFH, TSCH, and Static schemes, which represent different frequency allocation strategies, with increasing levels of interference (low, medium, and high). As interference increases, all three schemes exhibit a drop in delivery ratio. DFH's outperformance of other methods is clear, as he achieved 98% PDR under low interference and a reasonably high rate of 88% even under heavy interference. In comparison, TSCH and Static's performance severely declines under the same conditions; TSCH drops to 81%, and Static drops significantly to 70%. This shows that DFH demonstrated worse adaptability by not adjusting to low-interfering situations, but was able to avoid heavily congested or noisy frequencies, which helped retain communication reliability in boisterous environments.

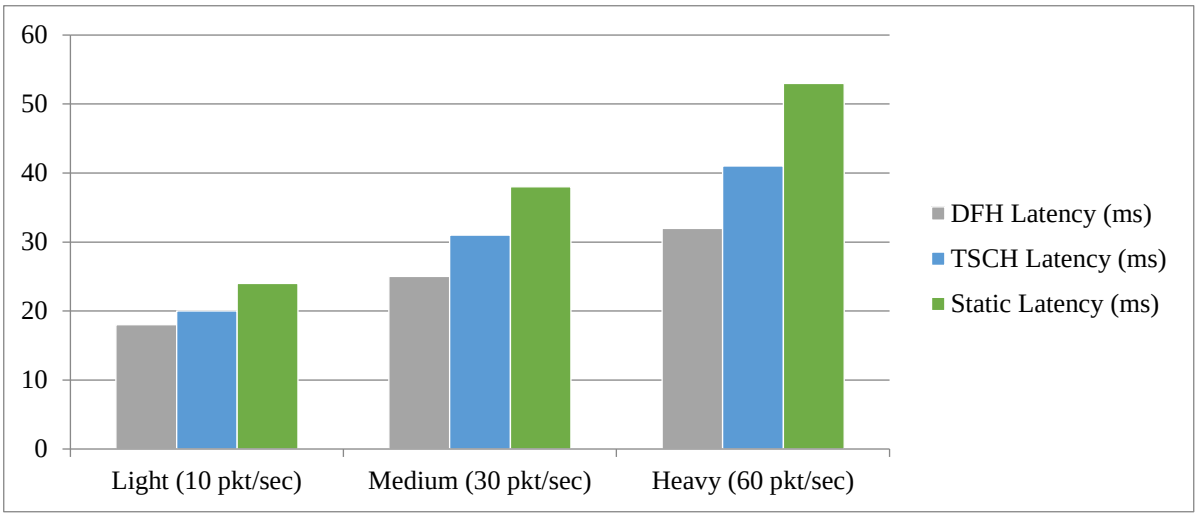

Figure 4: Average Latency vs. Network Load

Figure 4 illustrates the mean packet latency for each scheme, DFH, TSCH, and Static Frequency, with respect to a growing network load and congestion. As expected, latency tends to grow as traffic load increases from light to heavy. DFH has the lowest latency across all loads, starting from 18 ms under light load and rising moderately to 32 ms during heavy traffic. TSCH latency varies from 20 ms to 41 ms, while Static latency significantly worsens from 24 ms to 53 ms. The lower latency in DFH is due to the adaptive channel switching that avoids congested frequencies without the coordination overhead of slot-based schemes such as TSCH.

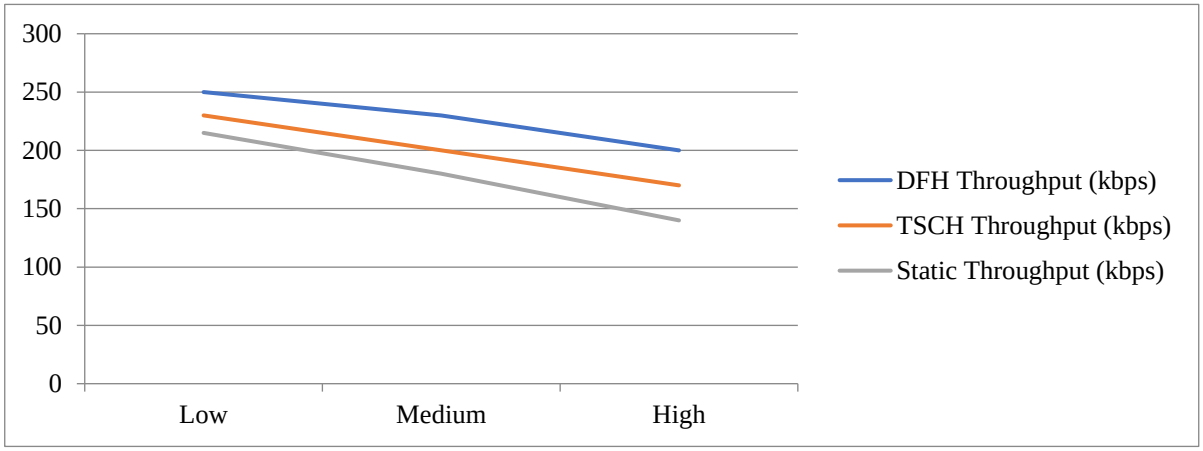

Figure 5: Throughput vs. Interference Level

This line chart (Figure 5) looks at the throughput performance of DFH, TSCH, and Static schemes under different levels of interference. It is evident from the figure that DFH has the highest throughput in all the scenarios, which is 250 kbps in low interference, and it reduces to 200 kbps in high interference. Static and TSCH come behind DFH, while Static has the highest drop in performance, reducing to 140 kbps under high interference. The higher throughput in DFH is an indicator of the scheme's ability to avoid unsuccessful transmissions by changing the chosen channels in the intervals between transmissions, which underlinesTable

DFH's ability to maintain data rate and reliability in volatile spectrum environments.

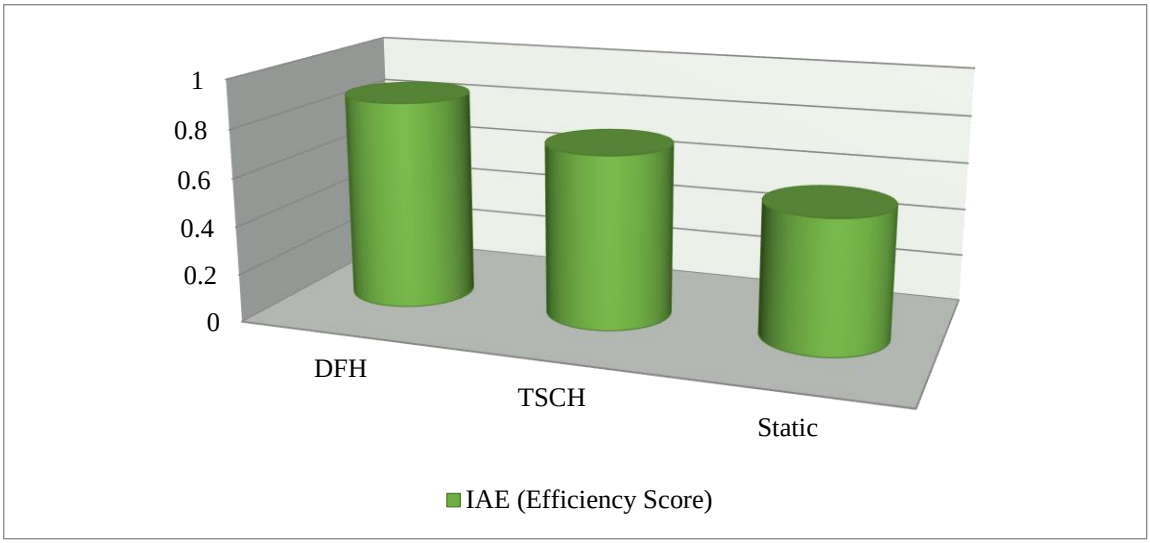

Figure 6: Interference Avoidance Efficiency vs. Scheme

Figure 6 shows the Interference Avoidance Efficiency (IAE) for the three schemes rated on their ability to perform in either an interference-free or low noise channel. DFH achieved the highest rating of 0.87, which indicates that it avoids poor quality channels about 87% of the time. TSCH has rated a moderate efficiency of 0.72, which is better than static's low 0.55. This suggests that DFH's real-time channel testing, paired with adaptive hopping, allows it to properly avoid interference, unlike the static and time-slotted methods, which are hindered by design limits.

4.4 Security-Driven Performance Metrics

In addition to traditional performance metrics such as latency, throughput, and Packet Delivery Ratio (PDR), security resilience of the Dynamic Frequency Hopping (DFH) scheme in the IoT networks should also be taken into consideration. To gain a better understanding of the contributions of DFH to communication security, we will suggest a set of security-related performance metrics according to the context. One, encryption overhead, measures the computational overhead of hopping sequence encryption in DFH, and it measures how much the cryptographic techniques affect system performance and objectively measures the tradeoff between system efficiency and security. The second important measure is jamming resistance, which assesses the ability of DFH to sustain communications, unbroken, when the attackers are deliberately jamming the frequency bands. Another significant measure is the latency of attack detection, which is a measure of the time taken to detect a security violation, such as jamming or eavesdropping attacks. A low detection latency is a guarantee that the system will be able to effectively protect itself by responding to the threat and changing the frequency hopping sequence, if needed, to ensure secure communication. Finally, another significant parameter of security is data integrity, which examines how safe the data remains while in transit, provided by DFH, without alterations, especially when sharing frequencies. By adding these security measures to the traditional performance measures, we will be able to evaluate to an even deeper degree how effectively DFH is able to maximize the network performance as well as increase security in communication in an IoT context. These processes demonstrate the resiliency of DFH in all things security and how well it can deal with attacks that include jamming, eavesdropping, and frequency spoofing, and continue to communicate successfully.

5 Implementation Considerations

5.1 Security Concerns and Vulnerabilities in Dynamic Frequency Hopping

While DFH provides a reasonable defense against the interference threats in IoT networks, it unfortunately grounds out some inherent weaknesses with respect to security. This is due to the frequency cycling and the necessity for real-time spectrum sensing that makes them reliant on insecure features. Such as frequency interference, which attackers can exploit through spoofing or jamming the hopping sequence themselves. For example, a jamming attack is an attack against the use of the shared frequency band between DFH and causes devices to hop at a slower speed. As a result, attacks of this nature reduce the network's forward progress or result in complete communication failure. There is also the man-in-the-middle (MITM) attack if the attacker achieves synchronization with the hopping pattern of the devices so that they can capture or modify aspects of communication between the two devices. The second issue is that there is also the replay attack, where an attacker can reuse a previously stored hopping sequence, which could cause synchronization issues or access. With these known weaknesses documented and understood, DFH ought to be made much more secure if IoT integrity were ever to be guaranteed.

5.2 Proposed Solutions to Enhance DFH Security

The DFH framework can have some solutions to counter such security concerns. Cryptographic protection of hopping sequences may ensure that they are not accessed or modified by the wrong people. Similarly, the frequency hopping sequence may be encrypted with the help of public key cryptography in a way that the attacker will never be able to intercept or guess the frequency switching. Authenticity of the communication can also be verified through message authentication techniques like digital signatures or hash-based message authentication codes (HMAC) to offer a safeguard against MITM attacks. DFH can be used to detect anomalies. Such systems can use machine learning methods to identify abnormal switching behavior of spoofing or jamming attacks. With the application of anomaly detection, the system can automatically control the sequence of hopping or even shift to a secure frequency band. In addition, the replay attacks can be circumvented with the help of secure synchronization protocols, and time-based encryption keys must be re-refreshed in such a way that the hopping pattern employed to carry out the interception can be employed in subsequent requests. These systems are also integrated, such as Intrusion Detection and Prevention Systems (IDPS), and the network is scanned for any malicious activity that tries to attack DFH, and preventive security measures are taken. Lastly, pre-emphasizing interference patterns and hopping sequence optimization to avoid congestion or malicious interference can be optimized through the inclusion of AI-based cognitive models to enhance DFH.

5.3 Integration of Advanced Machine Learning for Security Enhancements

Dynamic Frequency Hopping (DFH) would also be enhanced to further enhance the security of IoT networks by implementing machine learning (ML) tools in order to detect the likely vulnerabilities to security and dynamically adjust the frequency hopping technique. Since DFH is highly agile and adaptive to the dynamic interference patterns, AI-based models could be incorporated so that it can respond to likely attacks in real-time. For example, supervised learning algorithms could be trained to classify standard attack patterns, such as jamming or eavesdropping attacks, from a number of network parameters in past network data. The foregoing models would be applicable in forecasting future occurrences of the interference or attacks and prior rearranging of the hopping sequence in such a manner

as to avoid the interfered frequencies. This may be supplemented with reinforcement learning so that the system learns repeatedly and enhances its defense controls depending on the past discoveries of attacks, and modifies the hopping algorithm to restrict vulnerability the next time an attack occurs. It would considerably enhance the capability of DFH to develop an attack-resistant communication despite the attacks or network failure to provide a smoother and responsive service in a real-time IoT scenario. Machine learning not only makes DFH more resilient but also helps the firm to make dynamic decisions that remain relevant to the changing threat environment.

5.4 The Ills and Limitations of Implementing Dynamic Frequency Hopping in IoT Networks

Their value is in IoT networks, but would likely be highly uncontrollable, particularly in the regulation of the implementation of Dynamic Frequency Hopping (DFH) because of its numerous technical and functional problems. One of the most important problems is synchronization. Effective communication would mean that the transmitter and the receiver are both available in the same channel at the same frequency. This can only be made possible by a standard time reference or control channel, which does not always happen in the case of decentralized or resource-limited IoT networks. The other implementation constraint is the capability at the hardware level. Low-cost, simple IoT devices are based on simple transceivers that do not support multi-channel functionality. The devices under consideration might lack the necessary dexterity to scan a set of channels, measure the level of interference, and adjust frequencies on time. Simultaneously, multiple channel switches may consume power resources, which is negative towards low-power design goals often found in IoT applications. Other issues that are of greater concern include slow frequency selection decision-making. The use of real-time sensing in combination with adaptive algorithms presents the risk of added processing overhead, delay, or both. A long sensing interval may become problematic as it results in the algorithm answering too late. On the other hand, if the interval is too short, the algorithm can become excessively reactive and switch too often, creating instability. Also, the DFH's effectiveness can be stated as reduced due to the limited number of channels available for hopping. This problem becomes more critical in areas like cities, which are densely populated, since the resources are contested.

DFH has the potential to make IoT in different industries much more resilient in terms of security. DFH can also be applied in healthcare to safeguard medical devices against interference within hospitals, which is important in the transmission of reliable data to the medical devices, such as patient monitors and implantables. DFH reduces the chances of eavesdropping and jamming by hopping frequencies and facilitating the provision of secure communication of sensitive health information. DFH can enhance the security and reliability of the systems in smart cities because it prevents overload and interference of other wireless systems in terms of managing traffic systems, smart meters, and even surveillance cameras. It guarantees a continuous communication process, avoiding any inconvenience to important infrastructure. DFH assists in ensuring that communication between sensors, actuators, and control systems is safe within smart factories in the industry of automation. DFH minimizes the probability of interference through the dynamic choice of less congested frequencies, so that operation is not disrupted and attacks like signal jamming are avoided in real-time industrial usage.

5.5 Dynamic Frequency Hopping Customization Strategies

Several other methods may also be applied to augment the merits of DFH. In the instance of the former technique, the process of interfacing is not an energy-demanding one; therefore, the mechanism of sense utilized must attempt as much as possible to conserve energy. Network traffic-dependent variable interval sensing can achieve a tradeoff between network traffic-dependent power savings and power

response. As an example, a node can slow the rate of sensing when network traffic is minimal in an attempt to conserve energy. The prediction of patterns of interference by algorithms of the historical data also helps in the process of optimizing frequency choice. The system is able to look into potential future interference and take appropriate measures, like pre-switching channels, unlike a simple response to channel state. Lightweight synchronization methods are essential in mesh topology-based networks. These help in aligning the frequencies with relatively cheap modifications, including the utilization of beacon signals that could also be utilized in aligning other packets. A coordinator node has the ability to mitigate interference in the network in highly centralized IoT installations and therefore control the Frequency without extra information, which makes it more efficient. Software-based DFH frameworks need to be optimized for low-power radio module functionality in order to be able to circumvent hardware restrictions. In the constraints of resource-limited algorithms, this type of software would be practical with minimal primary storage and memory and would run on minimal IoT hardware.

5.6 Future Dynamic Frequency Hopping Research

The future work in dynamic frequency hopping has broad and comprehensive research directions. The integration of machine learning and reinforcement learning, in order to take advantage of high-level mental processes, is one of the subfields. These models would track the changes in interference over time, thus giving better frequency selection as compared to heuristic approaches due to automation. The other subfield involves cross-layered heuristic optimization as the information on the application, network, and physical layer is provided in the form of a composite to ease hopping choices. This can be done by giving an example of application-level QoS requirements being converted into channel quality parameters to improve end-to-end performance. DFH mechanisms that are more security-oriented have also not been fully exploited. Audio dynamic hopping eavesdropping is more than ever before, but prone to advanced jamming and spoofing attacks. Further studies can be done in the lower half of improving the hopping protocols with increased reliance on sound crypto-practices or with better reliance on anomaly detection. Finally, the non-interoperability and non-standardization will be the final barriers to the broader adoption of the technology. The convergence of divergent IoT ecosystems has a very high possibility of happening without hindrance by open modular DFH protocol research, as well as cross-compatibility of devices within a company, across different manufacturers.

6 Conclusion

This study takes into account the application of Dynamic Frequency Hopping (DFH) as a new method of addressing interference in IoT networks. DFH is better characterized compared to the time-slotted and static channel access scheme since it provides better interference avoidance, greater throughput, greater delivery ratio, lower latency, and better throughput in contrast to the time-slotted and static scheme, since it has a spectrum-responsive mobility. There are a theoretical analysis and simulated experiments that prove that DFH is an effective way to handle the different loads and the level of interference on the network, and the successful communication within the network under different conditions. In spite of these benefits, issues related to synchronization, hardware limitations, and compliance are still present in DFH implementation. Nonetheless, the flexibility and scalability of DFH are promising to be used in the future in IoT systems, particularly in complex, heterogeneous, and dense environments. Its connection to vital IoTs, e.g., smart cities, automation in industries, and environmental monitoring, increases its reliability and energy efficiency and optimizes the quality of services. In the future, more studies can be conducted to facilitate research on the security gap of the available DFH solutions. DFH is best at enhancing the performance of communication; however, it does not give full

attention to security threats that include jamming attacks, eavesdropping, and frequency spoofing. Further research should be done to determine how DFH can be combined with security measures, including secure routing and access control, to enhance the stability of IoT networks. Within the combination of frequent frequency hopping patterns and cryptography, one can prevent unauthorized access and reduce malicious interference. Moreover, machine learning (ML) promises significant opportunities to improve DFH. Further studies may be conducted with malicious interference and network attacks to make predictions based on the ML models in real-time, so that DFH can automatically adjust its hopping patterns in response to the changing security risks. Moreover, the reinforcement learning framework would maximize the frequency hopping in response to continuous threat detection to enhance the capability of DFH to adapt to a high-risk environment. All these innovations would further enable DFH to be a more independent and effective solution to the IoT networks, which would dynamically respond to interference and security attacks in real-time.

References

[1] Agarwal, A., & Yadhav, S. (2023). Structure and Functional Guild Composition of Fish Assemblages in the Matla Estuary, Indian Sundarbans. *Aquatic Ecosystems and Environmental Frontiers*, *1*(1), 16-20.

[2] Akan, O. B., Karli, O. B., & Ergul, O. (2009). Cognitive radio sensor networks. *IEEE network*, *23*(4), 34-40. https://doi.org/10.1109/MNET.2009.5191144

[3] Alamu, O., Olwal, T. O., & Migabo, E. M. (2025). Machine learning applications in energy harvesting internet of things networks: A review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3525263.

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[5] Alkaim, A. F., & Khan, M. (2024). Pharmacist-Led Medication Therapy Management: A Review of Its Effectiveness in Improving Patient Outcomes. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(4), 31-39.

[6] Babu, G. J. S., & Baskar, M. (2023). Location Aware DFS Scheduling Based Improved Quality of Service Maximization with IoT Devices in Cloud. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *14*(1), 37-49. https://doi.org/10.58346/JOWUA.2023.I1.003

[7] Benedetto, D. (2008). *Understanding ultra wide band radio fundamentals*. Pearson Education India.

[8] Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications*, *23*(5), 60-67. https://doi.org/10.1109/MWC.2016.7721743

[9] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243. https://doi.org/10.1109/TII.2014.2300753

[10] Fadel, A., Jaafar, Z., & Salih, H. (2022). The Impact of Accounting Disclosure in the Financial Statements on Investment Efficiency: An Analytical Study of Commercial Banks Listed in the Iraq Stock Exchange. *International Academic Journal of Economics*, *9*(2), 01–14. https://doi.org/10.9756/IAJE/V9I2/IAJE0904

[11] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[12] Guevara, K. G., Guevara, L. A. R., Gonzales, T. V. P., Neyra-Panta, M. J., Galvez, J. F. E., & Saavedra, N. L. C. (2024). Review of Scientific Literature on Social Networks in Organizations. *Indian Journal of Information Sources and Services*, *14*(4), 125-130. https://doi.org/10.51983/ijiss-2024.14.4.19

[13] Kadhim, M. J. H., Alradha, R. M., Jawad, H. K., Al-Dabbagh, B., & Al-Khafaji, Z. (2024). Investigating the Effect of the Yellow Chlorophyll on the Characteristics of Liquid Polyethylene Glycol for Liquid Electrolyte Solar Cells. *Natural and Engineering Sciences*, *9*(2), 244–256. https://doi.org/10.28978/nesciences.1479785

[14] Khaleel, S. A., & Ahmed, M. D. (2022). The Impact of Transformational Leadership Practices in Sustainable Marketing (Applied Research in the General Company for Dairy Products). *International Academic Journal of Business Management, 9*(2), 22–39. https://doi.org/10.9756/IAJBM/V9I2/IAJBM0908

[15] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology* (pp. 257-260). IEEE. https://doi.org/10.1109/FIT.2012.53

[16] Kherbache, M., Sobirov, O., Maimour, M., Rondeau, E., & Benyahia, A. (2023). Decentralized TSCH scheduling protocols and heterogeneous traffic: Overview and performance evaluation. *Internet of Things*, *22*, 100696. https://doi.org/10.1016/j.iot.2023.100696

[17] Kumar, T. S. (2024). Low-power communication protocols for IoT-driven wireless sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 24-27. https://doi.org/10.31838/WSNIOT/01.01.06

[18] Laya, A., Alonso, L., Alonso-Zarate, J., & Dohler, M. (2015). Green MTC, M2M, internet of things. *Green Communications: Principles, Concepts and Practice*, 217-236. https://doi.org/10.1002/9781118759257.ch11

[19] Lei, C., & Ibrahim, M. (2024). Efficient Revenue Management: Classification Model for Hotel Booking Cancellation Prediction. *Global Perspectives in Management*, *2*(1), 12-21.

[20] Liu, Y., Zeng, Q., Zhao, Y., Wu, K., & Hao, Y. (2021). Novel channel-hopping pattern-based wireless IoT networks in smart cities for reducing multi-access interference and jamming attacks. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 152. https://doi.org/10.1186/s13638-021-02029-8

[21] Mallikarjuna, M., & Prabhakara Rao, R. (2019). Classification of Capital Markets by Using Cluster Analysis. *International Academic Journal of Accounting and Financial Management, 6*(1), 11–22. https://doi.org/10.9756/IAJAFM/V6I1/1910002

[22] Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2012). Standardized protocol stack for the internet of (important) things. *IEEE communications surveys & tutorials*, *15*(3), 1389-1406. https://doi.org/10.1109/SURV.2012.111412.00158

[23] Popovic, B. M. (1999). Spreading sequences for multicarrier CDMA systems. *IEEE Transactions on Communications*, *47*(6), 918-926. https://doi.org/10.1109/26.771348

[24] Proakis, J. G., & Salehi, M. (2001). *Digital communications* (Vol. 4, pp. 593-620). New York: McGraw-hill.

[25] Raghav, K., & Sunita, R. (2024). Advanced Material Selection and Structural Design for Sustainable Manufacturing of Automotive Components. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(3), 30-34.

[26] Rahim, R. (2024). Adaptive Algorithms for Power Management in Battery-Powered Embedded Systems. *SCCTS Journal of Embedded Systems Design and Applications*, *1*(1), 20-24. https://doi.org/10.31838/ESA/01.01.05

[27] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks*, *11*(8), 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[28] Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. *ieee communications surveys & tutorials*, *19*(2), 855-873. https://doi.org/10.1109/COMST.2017.2652320

[29] Sathish Kumar, T. M. (2024). Low-power design techniques for Internet of Things (IoT) devices: Current trends and future directions. *Progress in Electronics and Communication Engineering*, *1*(1), 19–25.

[30] Sikora, A., & Groza, V. F. (2005, May). Coexistence of IEEE802. 15.4 with other Systems in the 2.4 GHz-ISM-Band. In *2005 IEEE Instrumentationand Measurement Technology Conference Proceedings* (Vol. 3, pp. 1786-1791). IEEE. https://doi.org/10.1109/IMTC.2005.1604479

[31] Singh, R. K., Berkvens, R., & Weyn, M. (2020). Synchronization and efficient channel hopping for power efficiency in LoRa networks: A comprehensive study. *Internet of Things*, *11*, 100233. https://doi.org/10.1016/j.iot.2020.100233

[32] Sobeih, A. H., Kamel, H. H., & Khaddad, M. T. (2022). The Decision of the Iraqi Parliament and the Criminalization of Normalization with Israel from the Perspective of International Covenants. *International Academic Journal of Humanities*, *9*(1), 24–32. https://doi.org/10.9756/IAJH/V9I1/IAJH0903

[33] Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M., & Pratt, W. (2008, April). WirelessHART: Applying wireless technology in real-time industrial process control. In *2008 IEEE Real-Time and Embedded Technology and Applications Symposium* (pp. 377-386). IEEE. https://doi.org/10.1109/RTAS.2008.15

[34] Stüber, G. L. (2002). Equalization and Interference Cancellation. In: Principles of Mobile Communication. Springer, Boston, MA. https://doi.org/10.1007/0-306-47315-1_7

[35] Sun, X., & Dai, L. (2016). Performance optimization of CSMA networks with a finite retry limit. *IEEE Transactions on Wireless Communications*, *15*(9), 5947-5962. https://doi.org/10.1109/TWC.2016.2574715

[36] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328

[37] Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. *IEEE Communications surveys & tutorials*, *21*(3), 2224-2287. https://doi.org/10.1109/COMST.2019.2916583

Authors Biography

Dr.M. Safa an Assistant Professor in the Department of Networking and Communications at the Faculty of Engineering & Technology, SRM Institute of Science and Technology (SRMIST), Kattankulathur, is a distinguished academic and researcher. Dr. Safa holds a PhD in Computer Science and Engineering from SRMIST (2023) and an M. Tech in Embedded Systems from SASTRA University (2011). Her primary research interests encompass IoT, Wireless and mobile communication, Healthcare projects, Artificial Intelligence, Machine Learning, Deep Learning, Wireless Sensor Networks, Big Data Analytics, and Cloud Computing. She has made significant contributions to her field through various publications and patents, notably focusing on real-time healthcare big data analytics, hybrid AI and IoT systems for cardiovascular patients, and early depression detection using machine learning. She also holds patents for automatic rust detection and environmental monitoring with wireless sensor networks. Before joining SRMIST in June 2013, she served as a Teaching Associate at the National Institute of Technology, Nagaland. Her dedication to research and education has been recognized with a Best Paper award at ICPECTS 2020 and selection for the Visvesvaraya Ph.D. Scheme by MeitY, Government of India. Additionally, she secured a Rs 2,00,000 grant from AICTE-SPICES for the IoT Alliances Club at SRMIST.

Dr.S.B. Nandeeswar is a Professor and Head of the Department of Computer Science & Engineering (AIML) at AMC Engineering College, Bengaluru, and also serves as the Dean and Controller of Examinations. With 23 years of distinguished teaching experience, he is passionate about nurturing technology-driven minds in areas such as core computer science, computer networks, cybersecurity, artificial intelligence, and machine learning. He encourages students to design and develop interdisciplinary projects that create meaningful technological and societal impact. Holding a B.E. and M.Tech in Computer Science & Engineering from VTU, and a Ph.D. in the same discipline from Presidency University with a specialization in AI & ML, he remains dedicated to advancing students' skills and competencies across the evolving landscape of computer science.

Capt Manjul Tripathi did pre sea Training at the Training Ship Rajendra, Bombay (DG Shipping, Govt of India). Thereafter I completed the sea time and apprenticeship with the Indian Ship owners SCINDIA STEAM SHIPPING PROVATE LTD, MUMBAI in the year 1982, Subsequently after passing my Mates COCs of the two levels I did my Master Mariner COC in the year April/1990 at Mumbai. I sailed with various Management companies on all kinds of dry cargo vessels with the main Companies including Barbers, Wilwilhelmsen-Norway, Mol -Tokyo, Dockendale Shipping, Nyk Lines and United Ocean Ship Management Tokyo. I Specialised with Heavy Lift Cargoes When I Worked with Owners Mammoet Shipping, Amsterdam. I stopped sailing in the year 2016. Thereafter I have Been involved with teaching/Training STCW courses at various MTI and involved in teaching Graduates in Naitical Science at Ganpat University and Presently Teaching Nautical Graduates at Academy of Maritime Education and Training.

Dr. Mohammed H. Fallah is a faculty member in the Department of Computer Techniques Engineering at the Islamic University, Najaf, Iraq. His research interests include computer architecture, software engineering, and artificial intelligence applications in technical systems. He has been involved in research addressing advancements in computational modeling, intelligent systems, and emerging engineering technologies.