Design of a Radio Repeater System to Counter Jamming Using the Channel Hopping Technique

M. Nanak Zakaria[1], Ahmad Wilda Yulianto[1], Yoyok Heru P.I[1], Achmad Setiawan[2]

[1]Department of Telecommunication Engineering,
State Polytechnic of Malang (POLINEMA), Malang, Indonesia
[2]Department of Electronic Engineering,
Gajayana University, Malang, Indonesia

Abstract. A Radio Repeater System (RPU) aims to establish communication between transmitters and receivers when obstacles are present. The primary issue faced by the Repeater System is the problem of frequent jamming disturbances in its input section. Jamming disruptions can lead to communication breakdowns, ultimately disrupting the entire communication process. The Anti-Jamming research method employed uses the Channel Hopping algorithm. With this algorithm in place, whenever the input system of the Radio Repeater encounters jamming interference, the controller unit responds by shifting the input channel to a new one that is free from interference. In addition to channel switching, the controller system also provides synchronization signals to user devices to adjust their channels according to the changes in the CH channel as a Repeater, ensuring smooth communication between transmitters and receivers. The primary findings and implications of this anti-jamming research in communication systems provide significant benefits for the security, efficiency, and reliability of modern communication systems. By countering jamming attacks, communication systems can operate more effectively and remain protected from security threats.

Keywords: Repeater, Anti-Jamming, Channel Hopping.

1 Introduction

Modern communication systems have become the backbone of the ever-evolving global society. The use of wireless technology and digital networks is on the rise, connecting people and devices worldwide. However, the increasing complexity of communication infrastructure also brings new challenges, including a diverse and serious range of security threats. One of the primary threats in the context of communication systems is jamming attacks [1]. Jamming is an attack aimed at disrupting or damaging signal transmissions in a communication system by flooding the communication channels with unauthorized signals or interference [2]. Such attacks can lead to communication disruptions, system failures, and can even be utilized by malicious parties to obstruct critical communications or steal sensitive information.

R. Andrie Asmara et al. (eds.), *Proceedings of the 5th Annual Advanced Technology, Applied Science, and Engineering Conference (ATASEC) 2023*, Advances in Engineering Research 229,
https://doi.org/10.2991/978-94-6463-358-0_13

Anti-jamming communication systems are designed to prevent or counter jamming attacks, which are a subset of denial-of-service (DoS) attacks where malicious nodes disrupt legitimate communication by intentionally causing interference in wireless networks [3]. There are several techniques and approaches used to implement anti-jamming communication systems, including: Frequency Hopping (FH), This technique involves rapidly switching between different frequencies to evade jammers. Proactive FH and Reactive FH are commonly used techniques to combat jamming [4]. Spread Spectrum Technique, It involves the use of spread spectrum techniques that do not require shared secrets to counter jamming attacks [5] [2]. Proactive and Reactive Frequency Hopping, Anti-jamming techniques can be classified into Proactive FH, which involves pre-shared keys for channel selection, and Reactive FH, which dynamically changes frequencies in response to jamming attacks [4], Intelligent Anti-Jamming Communication: Some research focuses on the use of intelligent algorithms, such as modified Q-learning and deep reinforcement learning, to optimize channel selection and counter jamming attacks [6] [7]. Jamming-resistant Broadcast Communication: Techniques have been developed to enable broadcast communication without the need for shared keys, making it more resistant to jamming attacks [5].

The effectiveness of anti-jamming techniques may vary depending on the specific communication system and the sophistication of jamming attacks. It is recommended to implement a combination of techniques and continually update and adapt anti-jamming strategies.

The objective of the research on Anti-Jamming in Communication Systems is to identify, analyze, and develop effective methods to counter and mitigate jamming attacks in wireless communication systems. This research aims to enhance the security and resilience of communication infrastructure against jamming attacks, which can disrupt or damage the communication process and lead to system failures. An important gap analysis involves the synchronization between the Repeater and Users. To ensure the success of the Channel Hopping technique, precise synchronization between the Repeater system and user devices is essential [3]. The analysis should consider potential synchronization issues, such as synchronization failures leading to users losing communication channels or channel conflicts during transitions. Reliability of synchronization should be a focal point and continually improved. Proper synchronization between the Repeater system and user devices is necessary for the Channel Hopping approach to succeed. Synchronization issues that may arise, such as synchronization failures resulting in users losing communication channels or channel conflicts during updates, should be considered during the study. Synchronization reliability should be a focus and enhanced [6].

2 Research Methodology

The method employed is the Channel Hopping technique, which is a signal transmission technique resilient against disruptions such as noise and jamming. This technique is utilized to address interference issues in the process of transmitting information from the sender to the receiver. Frequency Hopping Spread Spectrum (FHSS) is a method of transmitting information signals that hop within a frequency spectrum either randomly or according to a specific pattern [8].

2.1 Radio Repeater

The Radio Repeater System supports the use of the Channel Hopping algorithm, as illustrated in the diagram in Figure 1 below:

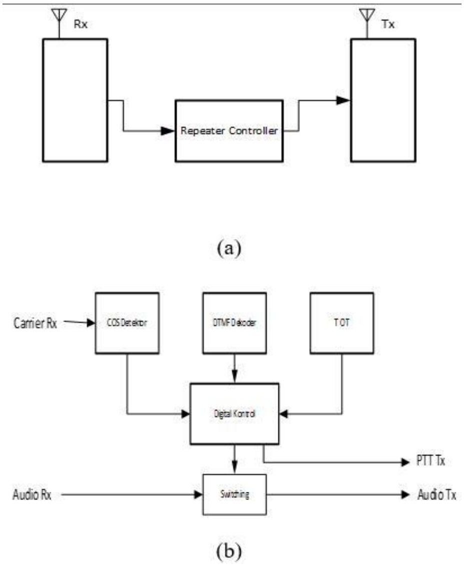


Fig. 1. Repeater System (a) General Repeater Diagram (b) Details of the Controller Unit in the Repeater

From Figure 1a, it can be observed that the Repeater system consists of 3 (three) main units: the Receiver unit (Rx), which is responsible for receiving information from User 1 on channel f1 (Up-Link) and then retransmitting it (using the Transmitter unit (Tx)) to User 2 on channel f2 (Down Link). The Repeater Controller unit is responsible for detecting the Up-Link signal (COS Detector) and processing it digitally to make a decision on whether the signal from the Up-Link needs to be routed to the Down-Link channel or not. The controller unit is also equipped with a DTMF Encoder unit and a TOT unit. The DTMF Encoder unit is used as a means of synchronization between the Repeater system and user devices. The TOT unit is used to limit the occupancy time of the Up-Link channel by the user while also serving as a means to detect Jamming signals.

2.2 Channel Hopping

The Channel Hopping technique involves the periodic rotation of channels within a communication system [9]. Transmitter and receiver devices communicate by changing the channel used at regular intervals. Channel switching is done randomly to reduce predictability in the rotation pattern, making it more difficult for malicious parties attempting to disrupt communication. For this technique to be successful, precise synchronization among all involved devices is required [10] [11]. This ensures that transmitter and receiver devices can switch to the same channel simultaneously. The frequency of channel rotation can be adjusted as needed and based on the level of threat. The more frequent channel changes occur, the more challenging it becomes for jamming attacks to identify and disrupt communication. Advantages of the Channel Hopping Technique [12]:

- Reducing Interference Probability: By randomly switching channels, this technique reduces the likelihood of interference from jamming attacks on a specific channel.
- Enhancing Security: Channel rotation diminishes the chances of jamming attacks causing system failures or gaining unauthorized access to sensitive data.
- Efficiency and Resilience: Channel Hopping can improve resource utilization efficiency and resilience against jamming attacks by avoiding traffic concentration on a single channel.
- Adaptability: This technique can be adapted to changing communication environments and varying network conditions.

One of the challenges in radio networks, particularly in radio networks employing radio repeaters, is the issue of Jamming interference. Typically, Jamming attacks involve emitting noise signals on the Uplink channel of the Repeater [13]. Radio repeaters lacking Anti-Jamming devices will amplify these Jamming signals and transmit them across the network through the Downlink channel. Since Downlink signals are usually high-power signals, all communication utilizing the Downlink channel will be disrupted. To address such Jamming attacks, various methods have been proposed. Specifically, for radio communication based on Analog-FM modulation, the Channel Hopping method is a reliable approach to implement [2] [14].

2.2.1. Channel Hopping Concept.

Channel Hopping is one of the Anti-Jamming techniques where periodically, the Transmitter device changes the communication channel in such a way that attackers cannot Jam the channel in use. Conceptually, it can be expressed as follows: the Transmitter device provides a set of channels to be used, denoted as L, expressed as { f1, f2, f3, ..., fL }. Then periodically, the controller of the transmitter changes the communication channel in a random pattern and occupies each channel for TH seconds. The pattern of channel occupation or hopping can be illustrated as shown in Figure 2 below [15] [4] [8]:

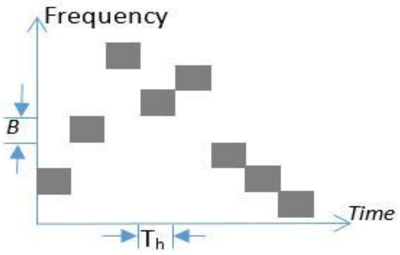
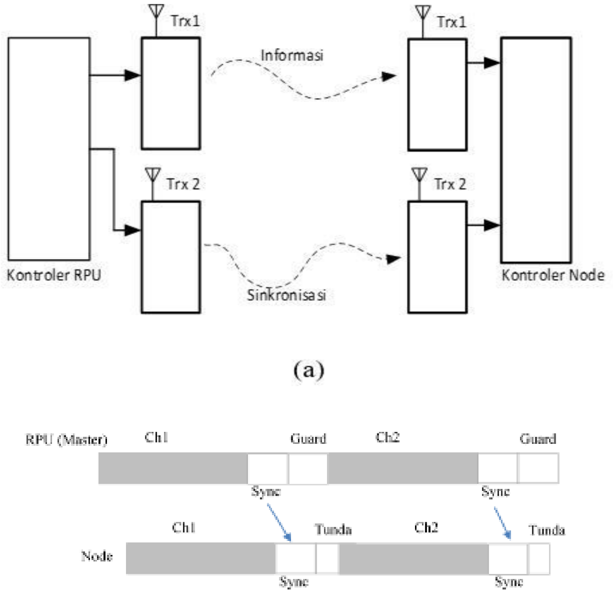


Fig. 2. Hopping Pattern in the Channel Hopping Technique

2.2.2. Synchronization in the Channel Hopping Technique.

The biggest challenge in employing the Channel Hopping technique in a Radio Repeater system is the issue of synchronization between users and the Radio Repeater system [5] [10] [11]. Generally, synchronization can be achieved using 2 (two) synchronization techniques, namely: using a dedicated channel to convey Synchronization signals or embedding Synchronization signals in the Downlink channel.



(a)

(b)

Fig. 3. Synchronization Methods (a) Using a dedicated Synchronization channel (b) Embedding Synchronization signals in the Downlink channel

Referring to Figure 3a, it can be seen that the synchronization technique using a dedicated channel requires additional transmitter devices on the Repeater side to convey synchronization signals to the User side (inefficient) [15] [16] [17]. Figure 3b illustrates an alternative method for conveying information signals from the Repeater side to the User side. In this figure, it can be observed that Synchronization signals are embedded in the communication channel after the channel-switching process. The method depicted in Figure 3b is more efficient than the method in Figure 3a as it does not require additional transmitter devices to convey Synchronization signals.

2.3 Implementation of the Channel Hopping Technique in the Radio Repeater System

The block diagram of the proposed Radio Repeater controller system can be illustrated as shown in Figure 4 below:

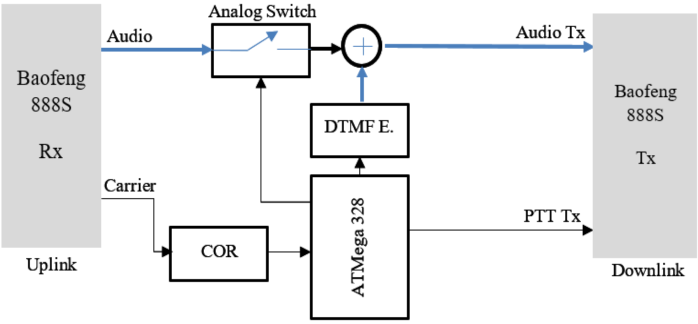


Fig. 4. Block Diagram of the Proposed Repeater Controller System

The controller system structure of the Repeater consists of 4 (four) components: COR (Carrier Operated Relay), DTMF Encoder [18] [19] [20], Analog Switch, and uC ATMega328. The COR unit is used to detect the presence of a Carrier signal on the input side of the Repeater (Up-Link channel). The DTMF Encoder serves as a means of synchronization between the Repeater and user devices, while the Analog Switch unit is used to disconnect the audio connection from the Rx unit (Up-Link) to the Tx unit (Down-Link). The uC ATMega328 unit integrates these components using a control algorithm as depicted in the following flowchart:

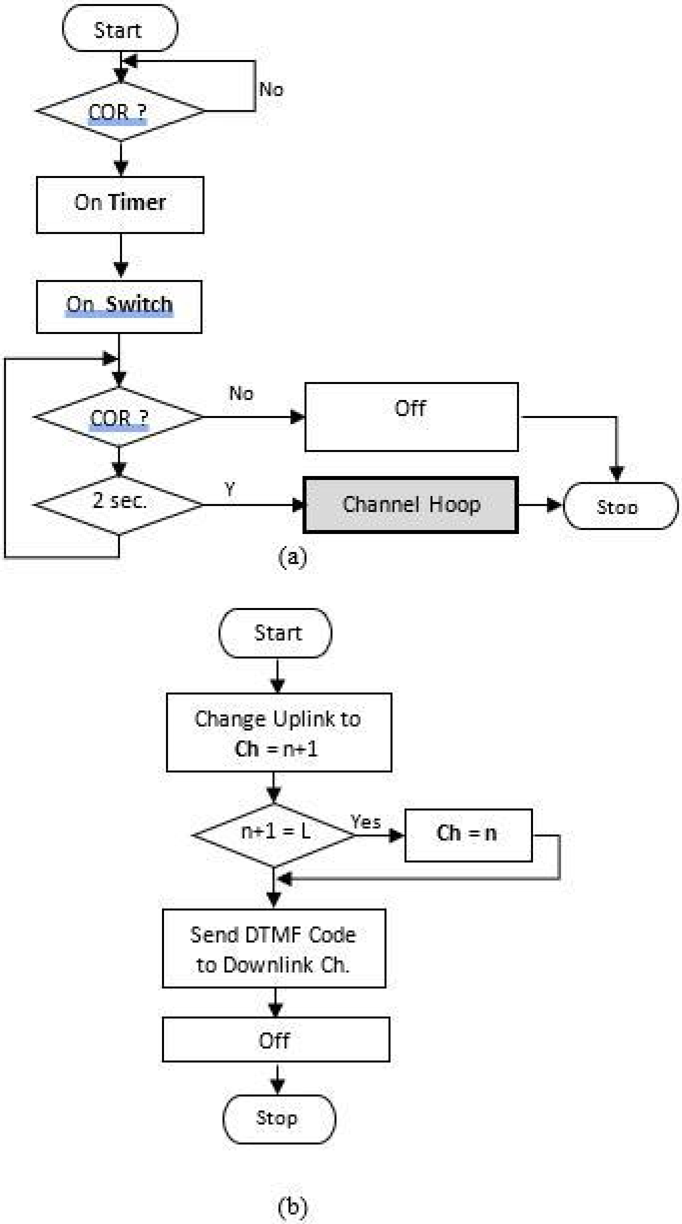


Fig. 5. (a) Control Flowchart of the Repeater Controller (b). Channel Hopping Flowchart

2.4 User Devices

To utilize the Repeater, User devices must transmit on the Up-Link channel and receive information from other users through the Repeater's Downlink channel. To ensure that User devices can adapt to Repeater channel changes in the event of a Jamming attack, the author proposes a block diagram of the receiver system as shown in Figure 6 below:

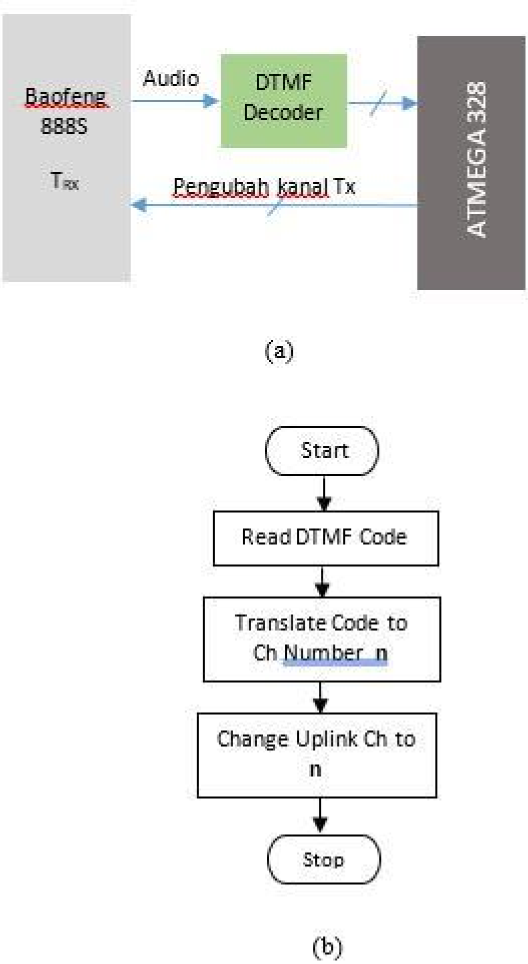


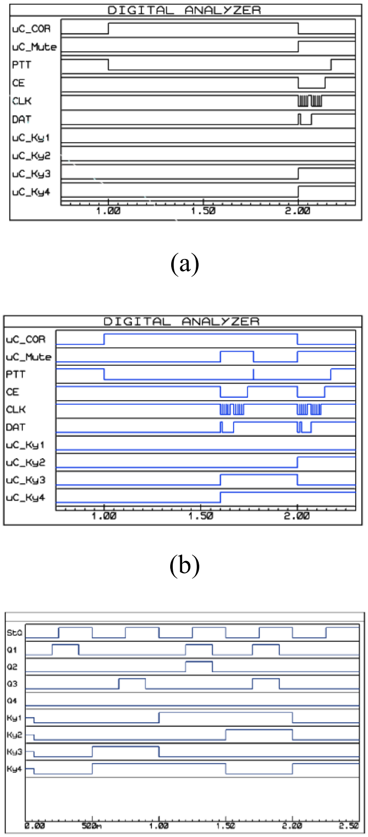
Fig. 6. (a) Block Diagram of the Receiver System (b). Receiver System Control Flowchart

From Figure 6, it can be observed that the proposed receiver system consists of 2 (two) main blocks: the DTMF Decoder unit and the control unit based on uC ATMEGA328. The DTMF Decoder unit is used to detect the appearance of Synchronization signals from the Repeater system. If these signals are detected, the DTMF unit will translate the code and convert it into the Hopping channel number. With the presence of these synchronization signals, User devices will always be able to follow the channel changes on the Repeater WSN due to Jamming interference.

3 Results and Discussion

The fundamental principle of the Channel Hopping technique involves periodic channel changes within a communication system. Transmitter and receiver devices communicate by switching channels at specific time intervals. Channel switching is done randomly to reduce predictability in the rotation pattern and make it more difficult for malicious parties attempting to disrupt communication [14] [21] [22].

Testing was conducted using Proteus to display the internal conditions of the controller unit in the Repeater system. In addition to using Proteus, field tests were also conducted using two user devices, where two devices were functioned as Jammers. Figures 7a and 7b illustrate the internal controller conditions of the Repeater when encountering Jammers.



(a)

(b)

(c)

Fig. 7. Spectrogram of the Controller Unit (a). No Jamming Condition (b). Jamming Condition (c). RX hopping

Figure 7a is a spectrogram depicting the internal controller system conditions when no Jammer signals are present on the Up-Link side of the Repeater. In this research, Jamming signals were detected using the COR signal emitted by the Rx (Up-Link) device. If the COR signal exceeds the Threshold time limit, this condition can be assumed as a Jamming condition. Figure 8b displays the internal controller unit's condition when Jamming has occurred on the Up-Link side. If Jamming occurs, the audio switch is turned off (uC_Mute), and then DTMF codes (CE, CLK, DAT) are transmitted on the Downlink side to inform users of the Jamming and the upcoming change in the Downlink channel.

Field testing using Jamming sources on the Up-Link side can be summarized in the following Table 1:

Table 1. System Testing in the field

Jammer		Repeater		User	
Tx	Era	Rx	Tx	Rx	Tx
Freq. Up-link		Freq. Up-link	Freq. Down-link	Freq. Down-link	Freq. Up-link
Ch 1	2 minutes	Ch1 → Ch 2	Ch 10	Ch 10	Ch1 → Ch2
Ch 2	1 minute	Ch 2	Ch 10	Ch 10	Ch 2
Ch 2 → Ch3	2 minutes	Ch 2 → Ch 3 Ch 3 → Ch 4	Ch 10	Ch 10	Ch 2 → Ch 3 Ch 3 → Ch 4
Ch 4	1.5 minutes	Ch 4	Ch 10	Ch 10	Ch 4

From Table 1, it can be observed that field testing indicates that when Jamming is applied to Ch1 for 2 minutes, the Repeater will change the Up-Link channel from Ch1 to Ch2. Because the synchronization signal is transmitted via the Downlink channel (high-power signal), users can switch channels according to the Repeater's changes. If Jamming is performed with a short duration (less than the Threshold — 2 minutes), the Repeater will not change channels. If Jamming is conducted on channels 2 and 3 simultaneously, the Repeater will require a time equal to 2x the Threshold to change channels (changing from channel 2 to channel 4).

4 Conclusion

Based on the measurement results, it can be concluded that the algorithm implemented in the Repeater controller system can perform channel switching when Jamming attacks occur. The Hopping process occurs when a Jamming attack exceeds the designed Threshold time, which is 2 minutes. For Jamming attacks lasting less than the Threshold time, the system does not perform Hopping. The results of the research on the Channel Hopping technique in Communication Systems are expected to provide an effective solution to counter Jamming attacks and enhance the security and resilience of modern wireless communication systems. By implementing this technique, communication systems can operate more efficiently and be protected from various security threats.

References

1. W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attack and defense strategies,” IEEE Netw., vol. 20, no. 3, pp. 41–47, 2006, doi: 10.1109/MNET.2006.1637931.
2. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” IEEE Commun. Surv. Tutorials, vol. 11, no. 4, pp. 42–56, 2009, doi: 10.1109/SURV.2009.090404.
3. K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: A survey,” Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014, doi: 10.1504/IJAHUC.2014.066419.
4. B. Gopalakrishnan and M. A. Bhagyaveni, “Anti-jamming communication for body area network using chaotic frequency hopping,” Healthc. Technol. Lett., vol. 4, no. 6, pp. 233–237, 2017, doi: 10.1049/htl.2017.0041.
5. C. Pöpper, M. Strasser, and S. Čapkun, “Jamming-resistant broadcast communication without shared keys,” Proc. 18th USENIX Secur. Symp., pp. 231–247, 2009.
6. C. Han, Y. Niu, T. Pang, and Z. Xia, “Intelligent anti-jamming communication based on the modified Q-learning,” Procedia Comput. Sci., vol. 131, pp. 1023–1031, 2018, doi: 10.1016/j.procs.2018.04.248.
7. G. Han, L. Xiao, and H. V. Poor, “Two-dimensional anti-jamming communication based on deep reinforcement learning,” ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc., pp. 2087–2091, 2017, doi: 10.1109/ICASSP.2017.7952524.
8. A. Cortés-Leal, C. Del-Valle-soto, C. Cardenas, L. J. Valdivia, and J. A. Del Puerto-Flores, “Performance metric analysis for a jamming detection mechanism under collaborative and cooperative schemes in industrial wireless sensor networks,” Sensors, vol. 22, no. 1, 2022, doi: 10.3390/s22010178.
9. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2000-January, no. c, pp. 1–10, 2000.
10. Patricia and RUIZ, “Efficient Communication Protocols for Ad Hoc Networks,” 2013.
11. S. K. Wagle, A. A. Bazilraj, and K. P. Ray, “Energy efficient security solution for attacks on Wireless Sensor Networks,” ACCESS 2021 - Proc. 2021 2nd Int. Conf. Adv. Comput. Commun. Embed. Secur. Syst., vol. 00, no. September, pp. 313–318, 2021, doi: 10.1109/ACCESS51619.2021.9563325.
12. S. Jaitly, H. Malhotra, and B. Bhushan, “Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey,” 2017 Int. Conf. Comput. Commun. Electron. COMPTELIX 2017, pp. 559–564, 2017, doi: 10.1109/COMPTELIX.2017.8004033.
13. L. K. Ketshabetswe, A. M. Zungeru, M. Mangwala, J. M. Chuma, and B. Sigweni, “Communication protocols for wireless sensor networks: A survey and comparison,” Heliyon, vol. 5, no. 5, p. e01591, 2019, doi: 10.1016/j.heliyon.2019.e01591.
14. A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos, “Defending wireless sensor networks from jamming attacks,” IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC, no. c, pp. 0–4, 2007, doi: 10.1109/PIMRC.2007.4394775.

15. Z. Liu et al., “Security cooperation model based on topology control and time synchronization for wireless sensor networks,” J. Commun. Networks, vol. 21, no. 5, pp. 469–480, 2019, doi: 10.1109/JCN.2019.000041.
16. W. Wang, H. Huang, Q. Li, F. He, and C. Sha, “Generalized Intrusion Detection Mechanism for Empowered Intruders in Wireless Sensor Networks,” IEEE Access, vol. 8, pp. 25170–25183, 2020, doi: 10.1109/ACCESS.2020.2970973.
17. S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, “Cryptographic Data Security for Reliable Wireless Sensor Network,” Alexandria Eng. J., vol. 72, pp. 37–50, 2023, doi: 10.1016/j.aej.2023.03.061.
18. T. Joseph, K. Tyagi, and D. R. Kumbhare, “Quantitative Analysis of DTMF Tone Detection using DFT, FFT and Goertzel Algorithm,” 2019 Glob. Conf. Adv. Technol. GCAT 2019, pp. 13–16, 2019, doi: 10.1109/GCAT47503.2019.8978284.
19. S. N. Bhavanam, P. Siddaiah, and P. R. Reddy, “FPGA based efficient DTMF detection using Split Goertzel algorithm with optimized resource sharing approach,” IFIP Int. Conf. Wirel. Opt. Commun. Networks, WOCN, 2014, doi: 10.1109/WOCN.2014.6923072.
20. C. Y. Yeh and S. H. Hwang, “Efficient detection approach for DTMF signal detection,” Appl. Sci., vol. 9, no. 3, 2019, doi: 10.3390/app9030422.
21. R. Alturki et al., “Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks,” IEEE Access, vol. 9, pp. 89344–89359, 2021, doi: 10.1109/ACCESS.2021.3088225.
22. H. Pirayesh and H. Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey,” IEEE Commun. Surv. Tutorials, vol. 24, no. 2, pp. 767–809, 2022, doi: 10.1109/COMST.2022.3159185.