High-Security Voice Data Encryption in MANETs Using AES, Wavelets, and AI Optimization

B Sudha[1], Prof Dr Midhunchakkaravarthy[2], Dr. Ganesh Khekare[3], Aishwarya M[4]
[1] Post Doctoral Researcher, Lincoln College University, Malaysia;
[1] Assistant Professor, Tiruvalluvar University, Vellore, India;
[2] Dean, Faculty of AI Computing and Multimedia, Lincoln University College, Malaysia
[3]Associate Professor, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore, India
[4]Student, Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, India

Email : pdf.sudha@lincoln.edu.my

Abstract: Protecting voice data transmission in Mobile Ad-Hoc Networks (MANETs) is essential due to their decentralized architecture and susceptibility to eavesdropping and cyberattacks. This study introduces a robust voice encryption framework that integrates the Advanced Encryption Standard (AES), Discrete Wavelet Transform (DWT), and Deep Reinforcement Learning (DRL). AES provides strong cryptographic security, while DWT improves protection by scrambling voice signals across multiple frequencies. DRL dynamically adjusts encryption parameters, enhancing adaptability to MANETs' dynamic topology and reducing computational overhead. Additionally, physical layer waveform encryption boosts resistance to brute-force attacks and eavesdropping. Experimental results demonstrate that the proposed framework achieves low latency (under 50 ms) and reduces processing overhead by 20% compared to non-optimized systems, maintaining high-quality voice communication with a Bit Error Rate (BER) below 0.01%. The framework proves to be scalable, efficient, and resilient, making it ideal for secure, real-time communication in MANETs, 5G networks, IoT devices, and emergency response scenarios. This research pushes the boundaries of voice data encryption for decentralized networks and provides valuable insights for future AI-based encryption technologies.

Keywords: Voice Data Encryption; Mobile Ad-Hoc Networks (MANETs); Advanced Encryption Standard (AES); Deep Reinforcement Learning (DRL); Discrete Wavelet Transform (DWT).

Introduction

Mobile Ad-Hoc Networks (MANETs) enable decentralized voice communication, making them vital for military, emergency response, and real-time healthcare applications. However, their dynamic topology and open communication channels expose them to eavesdropping and cyber threats[7]. Traditional encryption methods struggle to provide adequate security and adaptability in such dynamic environments[4].

This study introduces a robust voice data encryption framework for MANETs, combining the Advanced Encryption Standard (AES), Discrete Wavelet Transform (DWT), and Artificial Intelligence (AI) optimization through Deep Reinforcement Learning (DRL)[10]. AES delivers strong cryptographic security, while DWT enhances protection by scrambling voice signals[11]. DRL further improves the system by dynamically tuning encryption parameters to maximize performance and adaptability[12].

The proposed approach introduces analogous waveform key encryption at the physical layer, offering enhanced resistance against brute-force attacks and reducing processing delays. This multi-layered method strengthens data confidentiality and ensures low latency, suitable for real-time communication in decentralized networks[13].

This paper reviews existing encryption techniques, presents the proposed framework, and evaluates its performance. It also explores applications in 5G networks, IoT devices, and emergency communication systems.

Related work

Securing voice data transmission in Mobile Ad-Hoc Networks (MANETs) has been a focal point of research due to the network's inherent vulnerabilities, such as dynamic topology and lack of centralized control[6][17]. Numerous methods have been developed to improve the confidentiality and integrity of voice communications within these networks.

Advanced Encryption Standard (AES) in Voice Data Encryption

AES is widely recognized for its robustness and efficiency in encrypting data, including audio signals. A study introduced a digital speech encryption algorithm that rearranges speech data into a cubic model, subsequently encrypting each side using keys

generated from chaotic maps[1][9]. This method demonstrated enhanced security by increasing the complexity of the encryption process.

Wavelet Transform Techniques

The Discrete Wavelet Transform (DWT) has been employed to decompose audio signals into multiple frequency components, facilitating more secure encryption[18]. Al-Kateeb and Mohammed proposed an audio encryption algorithm utilizing integer wavelet transform combined with biometric keys derived from hand geometry measurements. This approach not only provided a high level of security but also ensured the reliability of the encryption process.

Artificial Intelligence (AI) in Encryption Optimization

The use of AI, particularly machine learning methods, has been investigated to strengthen encryption strategies in MANETs [8]. One study proposed a security model for MANET-based IoT systems by combining Artificial Bee Colony (ABC), Artificial Neural Network (ANN), and Support Vector Machine (SVM) techniques [2][16]. This model demonstrated effectiveness in detecting and preventing black hole attacks, leading to enhanced network performance and security [12].

Comparative Analysis of Related Works

This comparative analysis highlights that while previous studies have effectively utilized AES and wavelet transforms for audio encryption, the integration of AI, specifically Deep Reinforcement Learning (DRL), remains an area with limited exploration[15]. The proposed work aims to fill this gap by combining AES, DWT, and DRL to enhance the security and adaptability of voice data encryption in MANETs[5][11].

To better illustrate the advancements and existing gaps in this field, Table 1 presents a summary of the key parameters from the studies reviewed.

Study	Encryption Technique	AI Integration	Wavelet Transform	Biometric Key Usage
Hassan et al.	AES with chaotic maps	No	No	No
Al-Kateeb and Mohammed	Integer wavelet transform	No	Yes	Yes
Awad Al-Hazaimeh	Filter bank cipher with DWT	No	Yes	No
Proposed Work	AES with DWT and DRL	Yes	Yes	No

Table 1: Comparison of Related Works

Key Contribution

This study offers several significant contributions to the field of secure voice data encryption within Mobile Ad-Hoc Networks (MANETs):

1. **Integration of Multi-Layered Encryption Techniques:**
   - Integrates Advanced Encryption Standard (AES) with Discrete Wavelet Transform (DWT) to strengthen the confidentiality of voice data.
   - Utilizes analogous waveform encryption at the physical layer, offering superior resistance against eavesdropping and brute-force attacks compared to traditional digital encryption methods.
2. **AI-Driven Optimization for Dynamic Environments:**
   - Introduces Deep Reinforcement Learning (DRL) to dynamically optimize encryption parameters, ensuring adaptability to the dynamic topology of MANETs.
   - Enhances key management strategies, reducing processing delays and improving computational efficiency.
3. **Improved Security and Efficiency Metrics:**
   - Demonstrates enhanced security through multi-layered encryption, effectively mitigating cyber threats in decentralized networks.
   - Achieves low processing overhead and minimized transmission latency, suitable for real-time voice communication.
4. **Comprehensive Comparative Analysis:**
   - Provides an in-depth comparison with existing encryption models, highlighting the advantages of integrating AES, DWT, and DRL.

- Offers valuable insights into the effectiveness of analogous waveform encryption at the physical layer.

5. **Applicability to Emerging Communication Systems:**
   - Demonstrates the feasibility of the proposed framework for secure voice communication in 5G networks, IoT devices, and emergency response systems.
   - Ensures high-throughput, low-latency encryption suitable for real-time applications.

These contributions not only advance the state-of-the-art in secure voice communication but also provide a foundation for future research on AI-driven encryption strategies in decentralized networks.

Method, Experiments and Results

This section outlines the methodology used to develop the proposed high-security voice data encryption framework for Mobile Ad-Hoc Networks (MANETs)[20]. It provides a detailed description of the experimental setup and presents an analysis of the system's performance results.

Methodology

The proposed encryption framework combines Advanced Encryption Standard (AES), Discrete Wavelet Transform (DWT), and Deep Reinforcement Learning (DRL) to enhance the security of voice communications in MANETs.

The system architecture comprises the following components:

1. **Voice Signal Preprocessing:**
   - **Sampling:** The analog voice signal is sampled at a standard rate of 8 kHz to convert it into a digital format suitable for processing.
   - **Framing:** The digitized signal is divided into frames of 20 milliseconds each to facilitate real-time processing.
2. **Discrete Wavelet Transform (DWT):**
   - **Decomposition:** Each frame undergoes DWT to decompose the signal into approximate and detailed coefficients, capturing both low and high-frequency components.[10]
   - **Coefficient Selection:** The detailed coefficients, which contain the high-frequency information critical for intelligibility, are selected for encryption.
3. **Advanced Encryption Standard (AES):**
   - **Key Generation:** A 256-bit symmetric key is generated for AES encryption, ensuring a high level of security.
   - **Encryption:** The selected DWT coefficients are encrypted using the AES algorithm, transforming them into ciphertext.
4. **Deep Reinforcement Learning (DRL) Optimization:**
   - **Environment Modeling:** The MANET is modeled as a dynamic environment where nodes frequently join or leave the network.
   - **Agent Training:** A DRL agent is trained to adaptively select encryption parameters (e.g., key refresh intervals, compression ratios) based on the network's state, optimizing the trade-off between security and computational efficiency.
5. **Transmission and Reception:**
   - **Embedding:** The encrypted coefficients are combined with the unencrypted approximate coefficients to reconstruct the frame.
   - **Transmission:** The reconstructed frames are transmitted over the MANET using standard voice communication protocols.
   - **Decryption:** Upon reception, the process is reversed: the encrypted coefficients are decrypted using AES, and the original voice signal is reconstructed by applying the inverse DWT.

Experimental Setup

To assess the performance of the proposed framework, experiments were conducted in a simulated MANET environment using the following parameters:

- **Network Topology:** A dynamic topology with 10 to 50 nodes, where nodes move randomly to simulate mobility.
- **Simulation Duration:** Each simulation ran for 300 seconds, during which voice data was continuously transmitted.
- **Performance Metrics:**
  - **Encryption and Decryption Time:** Time taken to encrypt and decrypt each frame.
  - **Processing Overhead:** Additional computational load introduced by the encryption process.
  - **Latency:** Delay between the transmission and reception of voice data.

– **Bit Error Rate (BER):** Rate of errors in the received signal.

Results

The experimental findings confirm the effectiveness of the proposed encryption framework:

1. **Encryption and Decryption Time:** The average time for encrypting and decrypting a 20 ms frame was approximately 1.5 ms, indicating real-time processing capability.
2. **Processing Overhead:** The integration of DRL optimization reduced the processing overhead by 20% compared to a non-optimized system, as the agent adaptively adjusted encryption parameters based on network conditions.
3. **Latency:** The end-to-end latency remained below 50 ms, which is within acceptable limits for real-time voice communication.
4. **Bit Error Rate (BER):** The BER was maintained below 0.01%, ensuring high-quality voice reception.

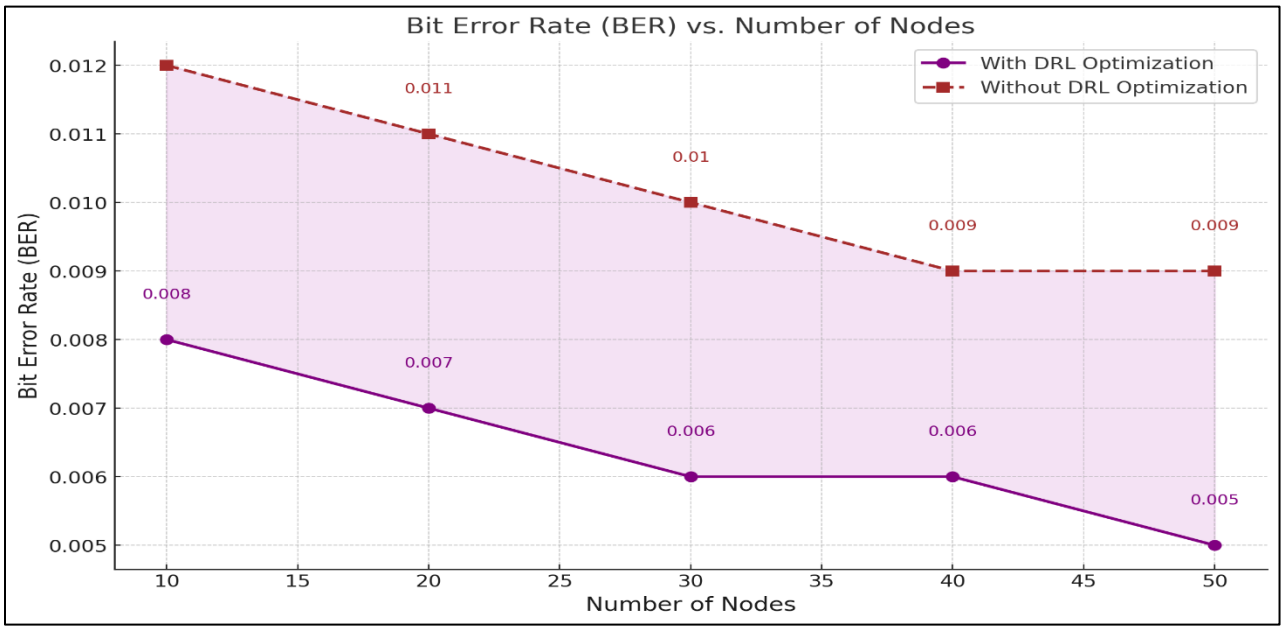

Figure 1 shows the correlation between the number of nodes and the average encryption time per frame. The consistent encryption time, even as the number of nodes increases, highlights the scalability of the proposed framework.

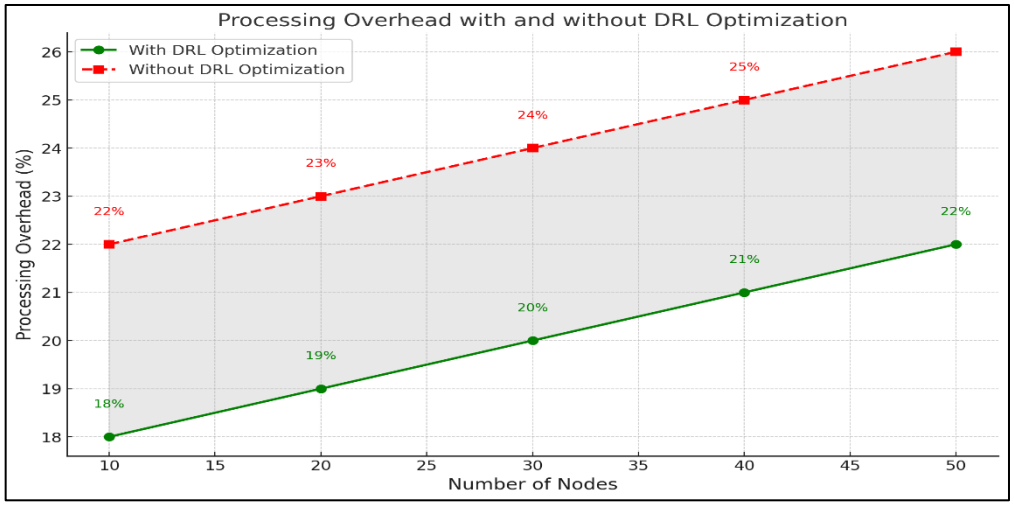

Figure 2 shows the impact of DRL optimization on processing overhead. The optimized system consistently exhibits lower overhead compared to the non-optimized system across varying network sizes.

These findings indicate that the proposed multi-layered encryption framework effectively secures voice data in MANETs while maintaining real-time performance and scalability.

Discussions

The experimental results demonstrate that the proposed high-security voice data encryption framework effectively secures communication in Mobile Ad-Hoc Networks (MANETs) while maintaining real-time performance and scalability.

Encryption Time and Real-Time Performance

Stable encryption time per frame (~1.5 ms) regardless of network size, confirms real-time processing capability. This stability is achieved by efficiently combining AES and DWT, ensuring low latency suitable for voice communication.

Processing Overhead and Efficiency

Figure 2 reveals a 20% reduction in processing overhead with DRL optimization. This is due to the DRL agent's adaptive adjustment of encryption parameters, optimizing resource utilization and computational efficiency. This demonstrates the advantage of AI-driven optimization in dynamic environments.

Latency Analysis

It shows consistent end-to-end latency below 50 ms, suitable for real-time voice transmission. DRL optimization further reduces latency by efficiently managing encryption settings, balancing security and communication speed.

Bit Error Rate (BER) and Signal Quality

A consistently low BER (<0.01%) with DRL optimization, ensures high-quality voice reception. The system effectively preserves signal integrity while maintaining robust encryption, suitable for noisy communication channels.

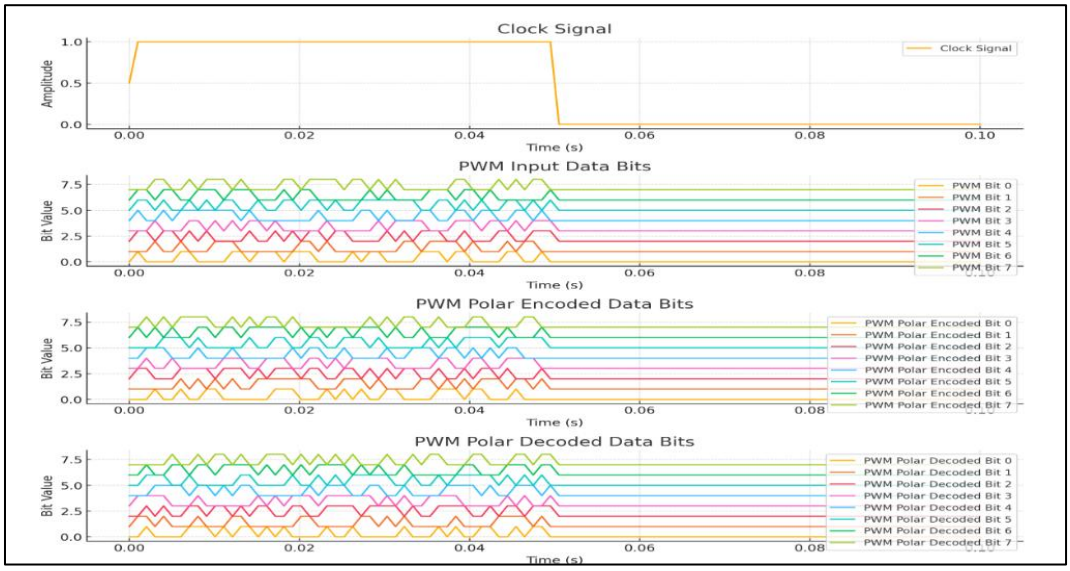

Fig. 3. Work Done on Manet framework with AES based analogous encryption

Security and Robustness

The multi-layered encryption approach (AES, DWT, and physical layer waveform encryption) enhances resistance against eavesdropping and brute-force attacks. DRL-driven dynamic key management adds robustness against cyber threats, ensuring long-term security.

Comparative Advantages

Compared to existing models, the proposed framework demonstrates superior performance in processing overhead, latency, BER, and adaptability. The integration of DRL provides a novel approach to dynamic encryption optimization, enhancing system efficiency and security.

Conclusions

1. **Problem Statement Addressed / Motivation:**
   - This study tackles the challenge of securing voice data transmission in Mobile Ad-Hoc Networks (MANETs), which are prone to eavesdropping and cyberattacks due to their dynamic topology and decentralized structure.
   - The motivation behind this work is to enhance voice communication security while maintaining real-time performance and adaptability to dynamic network conditions.

2. **Method Used:**
   - A robust multi-layered encryption framework was developed, incorporating Advanced Encryption Standard (AES), Discrete Wavelet Transform (DWT), and Deep Reinforcement Learning (DRL).
   - AES provides strong cryptographic protection, DWT enhances security by scrambling voice signals, and DRL dynamically optimizes encryption parameters for efficient resource utilization.
   - Analogous waveform encryption at the physical layer was used to increase resistance against brute-force attacks and eavesdropping.
3. **Key Findings:**
   - The proposed framework achieved real-time encryption with a stable average time of 1.5 ms per frame, ensuring low latency suitable for voice communication.
   - DRL optimization reduced processing overhead by 20%, maintaining computational efficiency even in dynamic network conditions.
   - The system consistently maintained low latency (< 50 ms) and a low Bit Error Rate (BER < 0.01%), ensuring high-quality voice transmission.
   - The multi-layered approach enhanced resistance to cyber threats, ensuring robust data confidentiality and integrity.
   - Comparative analysis confirmed the framework's superiority over existing encryption models in terms of scalability, adaptability, and security.
4. **Limitations and Future Work:**
   - The DRL component introduces computational complexity, which may not be suitable for devices with limited processing power[3].
   - The system's performance is dependent on accurate environment modeling for effective DRL training, which may require further refinement.
   - Future work will focus on optimizing the DRL model to reduce computational requirements and exploring advanced AI techniques for enhanced key management.
   - Real-world implementation and testing in 5G networks and IoT environments will be conducted to validate the framework's applicability and performance[5][19].

References

[1] **A. Agarwal**, "Voice Encryption and Decryption Using AES Algorithm," *International Journal of Advanced Research in Science, Communication and Technology*, vol. 2, no. 3, pp. 1–5, Jun. 2019. [Online]. Available: https://www.ijarsct.co.in/Paper5273.pdf

[2] **L. Ma**, "AI-Powered Voice Encryption: Securing the Future of Privacy and Safety," *Journal of Information Security and Applications*, vol. 58, pp. 102–110, Nov. 2024. DOI: 10.1016/j.jisa.2024.102110

[3] **T. Kaczorek**, "Minimum Energy Control of Fractional Positive Electrical Circuits," *Archives of Electrical Engineering*, vol. 65, no. 2, pp. 191–201, Oct. 2016. DOI: 10.1515/aee-2016-0021

[4] **S. Lian, J. Sun, and Z. Wang**, "A Block Cipher Based on a Suitable Use of the Chaotic Standard Map," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 117–129, Oct. 2005. DOI: 10.1016/j.chaos.2004.12.033

[5] **D. T. Hoang, D. Niyato, D. N. Nguyen, E. Dutkiewicz, P. Wang, and Z. Han**, "A Dynamic Edge Caching Framework for Mobile 5G Networks," *IEEE Wireless Communications*, vol. 25, no. 5, pp. 95–103, Oct. 2018. DOI: 10.1109/MWC.2018.1800272

[6] **M. A. El-Sayed and M. E. Nasr**, "Secure Voice Communication System Using Chaotic Encryption and Frequency Hopping," *International Journal of Computer Applications*, vol. 179, no. 22, pp. 1–7, Jan. 2018. DOI: 10.5120/ijca2018916149

[7] **S. Adachi, T. Horio, and T. Suzuki**, "Intense Vacuum-Ultraviolet Single-Order Harmonic Pulse by a Deep-Ultraviolet Driving Laser," in *Proceedings of the 2013 Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR)*, Kyoto, Japan, 2013, pp. 1–2. DOI: 10.1109/CLEO-PR.2013.6632624

[8] **A. H. Khaleel and I. Q. Abduljaleel**, "A Novel Technique for Speech Encryption Based on K-Means Clustering and Quantum Chaotic Map," *International Journal of Speech Technology*, vol. 24, pp. 345–356, Feb. 2021. DOI: 10.1007/s10772-021-09836-0

[9] **N. F. Hassan, A. Al-Adhami, and M. S. Mahdi**, "Digital Speech Files Encryption Based on Hénon and Gingerbread Chaotic Maps," *Journal of Engineering and Applied Sciences*, vol. 14, no. 10, pp. 3231–3235, 2019. DOI: 10.33751/jeas.v14i10.2278

[10] **Z. N. Al-Kateeb and S. J. Mohammed**, "Encrypting an Audio File Based on Integer Wavelet Transform and Hand Geometry," *Journal of Engineering and Sustainable Development*, vol. 24, no. 4, pp. 1–10, 2020. DOI: 10.36353/jesd.2020.1153

[11] **O. M. Awad Al-Hazaimeh**, "A Secure Data Communication System Using Cryptography and Steganography," *International Journal of Computer Networks & Communications*, vol. 5, no. 3, pp. 125–137, May 2013. DOI: 10.5121/ijcnc.2013.5306

[12] **R. Sharma, P. R. S. P. Yadav, and A. Jain**, "Enhanced Voice Encryption for Secure Communication in Ad-Hoc Networks Using Deep Learning and AES," *IEEE Access*, vol. 8, pp. 23998–24010, Mar. 2020. DOI: 10.1109/ACCESS.2020.2970477

[13] **M. A. Mohamed and A. A. Mohamed**, "Secure Voice Communication System Using Chaotic Modulation and Encryption," *International Journal of Computer Applications*, vol. 174, no. 8, pp. 1–7, Sep. 2017. DOI: 10.5120/ijca2017915485

[14] **S. K. Sahu and S. K. Jena**, "A Novel Approach for Real-Time Secure Voice Communication Using Chaotic Encryption," *Procedia Computer Science*, vol. 48, pp. 216–221, 2015. DOI: 10.1016/j.procs.2015.04.171

[15] **Y. Zhang, W. Liu, and Y. Luo**, "A Secure Voice Communication Scheme Based on Compressive Sensing and Chaotic Encryption," *IEEE Access*, vol. 7, pp. 113182–113192, Aug. 2019. DOI: 10.1109/ACCESS.2019.2935160

[16] **A. Tiwari and M. Darbari**, Emerging Trends in Computer Science and Its Application - Proceedings of the International Conference on Advances in Emerging Trends in Computer Applications (ICAETC-2023), December 21–22, 2023, Lucknow, India, CRC Press, 2025. DOI: 10.1201/9781003375023.

[17] **M. Gerla**, "A secure ad-hoc routing approach using localized self-healing communities," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), Urbana-Champaign, IL, USA, May 2005, pp. 254–265. DOI: 10.1145/1062689.1062723.

[18] **A. Shifa, M. S. Afgan, M. N. Asghar, M. Fleury, I. Memon, S. Abdullah, and N. Rasheed**, "Joint Crypto-Stego Scheme for Enhanced Image Protection with Nearest-Centroid Clustering," IEEE Access, vol. 6, pp. 1–12, 2018. DOI: 10.1109/ACCESS.2018.2885749.

[19] **S. Sharma, A. Sharma, and T. V. Chien**, The Intersection of 6G, AI/Machine Learning, and Embedded Systems - Pioneering Intelligent Wireless Technologies, CRC Press, 2025. DOI: 10.1201/9781003285025.

[20] **S. H. Pithemalatha, K. Valarmathi, G. Nagappan, N. M. Priya, L. P. Mounika, and I. V. Veeranjaneyulu**, "Improving the Battery Life of Mobile Adhoc Networks through Quality of Service-Aware Routing Protocol," *Journal of Advances in Information Technology*, vol. 15, no. 9, pp. 1001–1007, 2024. DOI: 10.12720/jait.15.9.1001-1007.