ROBUST AND SECURE DATA TRANSMISSION USING ARTIFICIAL INTELLIGENCE TECHNIQUES IN ADHOC NETWORKS

Kavya TM[1], Mohammed Hussain[2]
[1]M. Tech Student, Department of Computer science and engineering, Golden valley integrated campus, Kadiri Road, Angallu Post, Madanapalli, Chittoor, Andhra Pradesh 517326

[2]Assistant Professor, Department of Computer science and engineering, Golden valley integrated campus, Kadiri Road, Angallu Post, Madanapalli, Chittoor, Andhra Pradesh 517326

Abstract Mobile Ad Hoc Networks (MANETs) are decentralized wireless communication networks where mobile nodes communicate dynamically without relying on fixed infrastructure. Due to their open medium, dynamic topology, limited bandwidth, and lack of centralized administration, MANETs are highly vulnerable to security threats such as packet dropping, black hole attacks, wormhole attacks, data interception, and unauthorized access. Ensuring robust and secure data transmission in such environments has become a major challenge in modern wireless communication systems.

This project proposes a robust and secure data transmission model using Artificial Intelligence (AI) techniques in Ad Hoc Networks. The system integrates Machine Learning (ML) and intelligent routing mechanisms to improve network security, reliability, and transmission efficiency. AI algorithms are used to analyze node behavior, detect malicious activities, predict network congestion, and select optimal routing paths dynamically. The proposed approach continuously monitors network traffic patterns and identifies abnormal activities in real time, thereby reducing packet loss and improving secure communication.

The system employs intelligent intrusion detection and trust-based routing techniques to enhance protection against cyberattacks. AI-based decision-making enables the network to adapt quickly to topology changes and node mobility while maintaining stable communication. Encryption mechanisms and authentication protocols are also incorporated to ensure confidentiality, integrity, and secure access to transmitted data.

Experimental analysis demonstrates that the proposed AI-driven approach achieves higher packet delivery ratio, lower transmission delay, improved throughput, and better attack detection accuracy compared to traditional routing methods. The system is scalable, adaptive, and suitable for applications such as military communication, disaster recovery, emergency response systems, and IoT-based wireless environments.

In conclusion, the integration of Artificial Intelligence techniques with Ad Hoc Networks provides an effective solution for achieving robust, reliable, and secure data transmission. The proposed system significantly enhances network performance and security while addressing the challenges associated with dynamic and infrastructure-less wireless communication environments.

1. Introduction

Ad Hoc Networks, commonly known as Mobile Ad Hoc Networks (MANETs), are self-configuring and infrastructure-less wireless communication networks in which mobile devices communicate directly with one another. These networks do not rely on centralized administration, routers, or fixed base stations. Each node in the network acts both as a host and as a router, forwarding data packets to other nodes dynamically. MANETs are widely used in military operations, disaster recovery, emergency communication systems, healthcare monitoring,

vehicular communication, and Internet of Things (IoT) applications due to their flexibility and rapid deployment capabilities.

Despite their advantages, Ad Hoc Networks face several challenges related to security, reliability, routing efficiency, bandwidth limitations, and frequent topology changes. Since the communication medium is wireless and open, the network is highly vulnerable to attacks such as black hole attacks, wormhole attacks, denial of service attacks, packet dropping, and unauthorized access. Additionally, the mobility of nodes causes continuous changes in routing paths, resulting in increased packet loss, transmission delays, and reduced network performance. Traditional routing and security mechanisms are often insufficient to handle these dynamic and complex network environments effectively.

Artificial Intelligence (AI) has emerged as a powerful technology for solving complex networking and cybersecurity problems. AI techniques such as Machine Learning (ML), Deep Learning (DL), Neural Networks, and Intelligent Decision-Making Algorithms can analyze network behavior, predict threats, optimize routing paths, and detect malicious activities in real time. By integrating AI into Ad Hoc Networks, the system can adapt intelligently to changing network conditions and improve overall communication performance and security.

The proposed system focuses on developing a robust and secure data transmission mechanism using Artificial Intelligence techniques in Ad Hoc Networks. The system uses AI-based trust evaluation and intelligent routing algorithms to identify reliable nodes and avoid malicious or unstable nodes during communication. Intrusion detection techniques are incorporated to monitor network traffic continuously and detect abnormal activities automatically. Secure encryption and authentication mechanisms are also implemented to protect the confidentiality and integrity of transmitted data.

The primary objective of this project is to enhance data transmission reliability, minimize packet loss, reduce network congestion, and improve security against cyber threats in MANET environments. The proposed AI-driven approach aims to achieve efficient routing, faster decision-making, and adaptive communication while maintaining high throughput and low delay.

In conclusion, the integration of Artificial Intelligence with Ad Hoc Networks provides a smart and efficient solution for secure wireless communication. The proposed system enhances network performance, strengthens security, and ensures reliable data transmission in highly dynamic and decentralized networking environments.

2. Literature Reviews

S. Corson and J. Macker The authors discussed the importance of secure routing mechanisms in Mobile Ad Hoc Networks (MANETs). Their research highlighted the challenges of dynamic topology, node mobility, and security vulnerabilities in wireless communication. The study emphasized intelligent routing techniques for improving packet delivery and reducing malicious attacks in decentralized networks.

Y. Zhang and W. Lee This research proposed a Machine Learning-based intrusion detection system for detecting abnormal activities in wireless ad hoc networks. The authors used classification algorithms to identify malicious nodes and unauthorized access attempts. Their approach improved attack detection accuracy and reduced false-positive rates in network monitoring.

3. Existing system

The existing system in Ad Hoc Networks mainly relies on traditional routing protocols and conventional security mechanisms for data transmission. Common routing protocols such as AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and DSDV (Destination Sequenced Distance Vector) are widely used to establish communication paths between mobile nodes. These protocols focus primarily on route discovery and packet forwarding without incorporating intelligent decision-making capabilities.

In traditional MANET systems, security is generally implemented using basic encryption techniques, authentication methods, and predefined routing rules. The network nodes communicate dynamically without centralized control, making it difficult to continuously monitor malicious activities or detect abnormal node behavior effectively. Existing systems lack the ability to analyze network traffic patterns intelligently and respond automatically to security threats.

Most conventional approaches use static or rule-based intrusion detection systems that cannot adapt efficiently to changing network conditions. These systems are unable to accurately identify sophisticated attacks such as black hole attacks, wormhole attacks, Sybil attacks, packet dropping, and denial-of-service attacks in real time. As a result, network performance decreases due to packet loss, increased delay, congestion, and unreliable routing paths.

Additionally, the existing systems do not provide efficient trust management among network nodes. Routing decisions are often made without evaluating the reliability or behavior of participating nodes, which increases the possibility of malicious nodes entering the communication path. Frequent topology changes caused by node mobility further reduce the effectiveness of traditional routing mechanisms.

4. Proposed system

The proposed system introduces a robust and secure data transmission framework using Artificial Intelligence (AI) techniques in Ad Hoc Networks (MANETs). The system is designed to improve network security, routing efficiency, reliability, and overall communication performance in highly dynamic wireless environments.

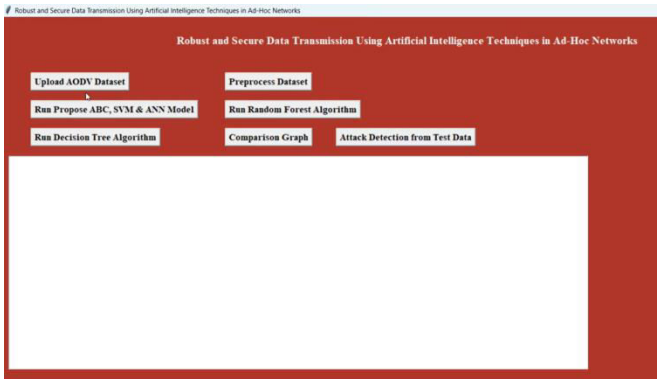
In the proposed approach, Artificial Intelligence and Machine Learning algorithms are integrated with routing protocols to provide intelligent decision-making capabilities. The system continuously monitors network traffic, analyzes node behavior, and identifies malicious or suspicious activities in real time. AI-based intrusion detection mechanisms are used to detect attacks such as black hole attacks, wormhole attacks, packet dropping, and unauthorized access attempts.

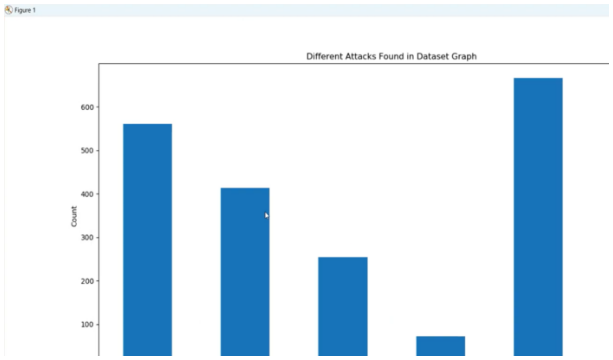
The proposed system employs a trust-based intelligent routing mechanism where each node is evaluated based on its behavior, reliability, and packet forwarding performance. Only trusted and secure nodes are selected for data transmission, which reduces the risk of attacks and improves communication stability. Machine Learning models help predict network congestion and dynamically select the most efficient routing paths.

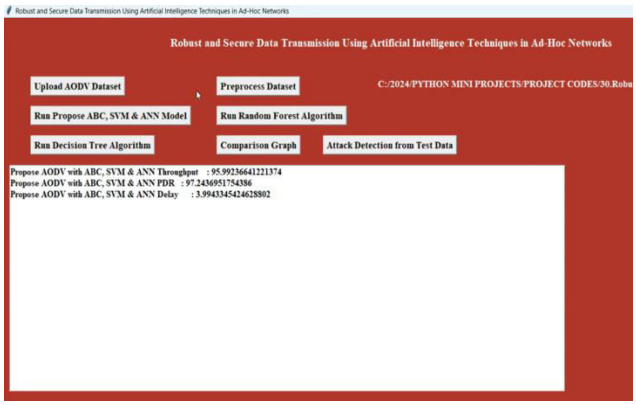
To ensure secure communication, the system incorporates encryption and authentication techniques that protect the confidentiality and integrity of transmitted data. AI algorithms also optimize bandwidth usage, reduce transmission delay, and improve packet delivery ratio by adapting automatically to topology changes and node mobility.

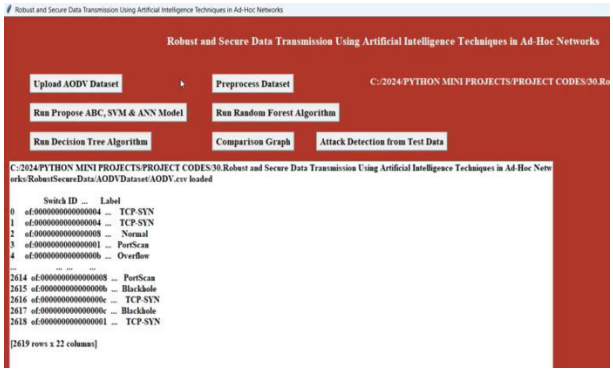
The proposed framework supports real-time monitoring, adaptive routing, and intelligent attack prevention, making the network more scalable and efficient compared to traditional systems. The integration of AI techniques enables the system to respond quickly to changing network conditions and maintain stable communication even in hostile environments. Overall, the proposed system provides a smart, adaptive, and highly secure solution for data transmission in Ad Hoc Networks, improving network performance while ensuring reliable and protected wireless communication.

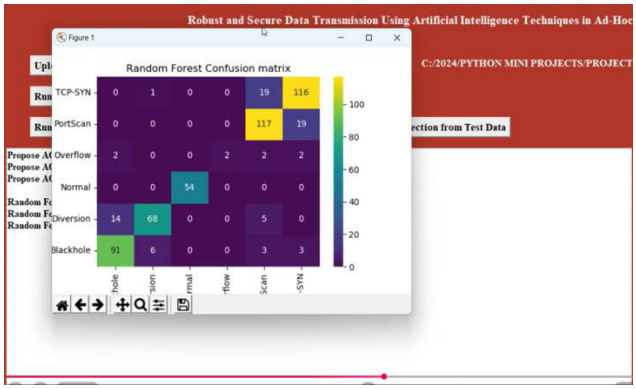
5. Results and analysis

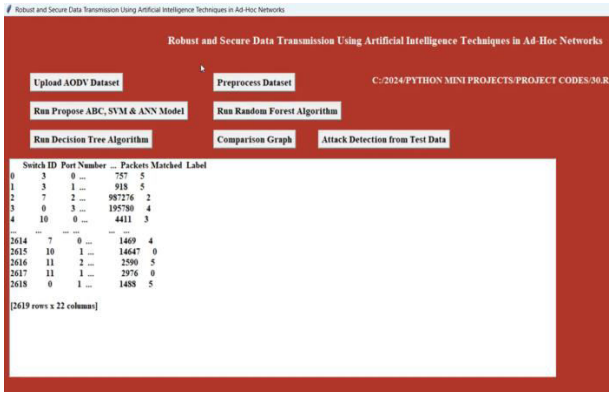


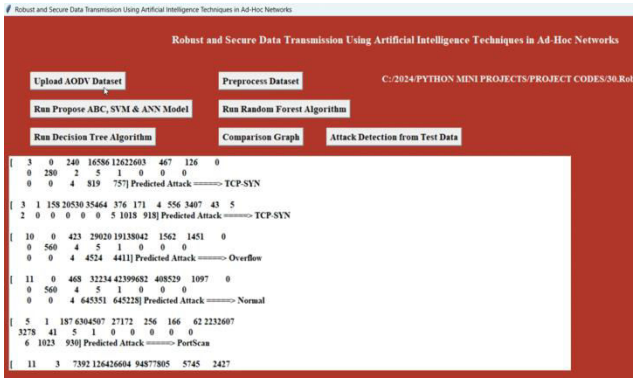


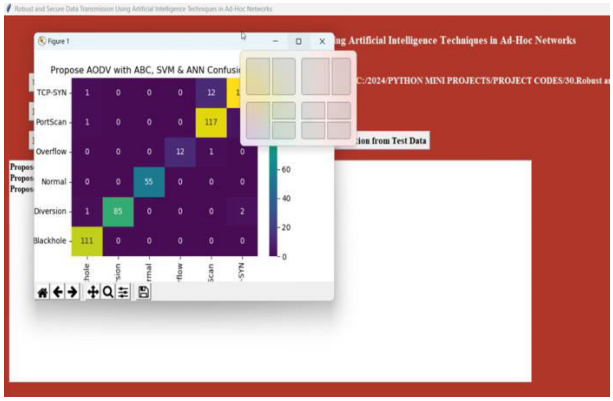












6. Conclusions

The proposed system for robust and secure data transmission using Artificial Intelligence techniques in Ad Hoc Networks provides an efficient solution to the major challenges faced in traditional MANET environments. The integration of Artificial Intelligence and Machine Learning techniques enhances network security, routing efficiency, and communication reliability in dynamic wireless networks.

The system successfully implements intelligent routing mechanisms, trust-based node evaluation, intrusion detection, and secure encryption techniques to protect data transmission from various network attacks such as black hole attacks, wormhole attacks, packet dropping, and unauthorized access. AI-based decision-making enables the network to adapt dynamically to topology changes, node mobility, and traffic variations while maintaining stable communication.

The proposed approach improves important network performance parameters such as packet delivery ratio, throughput, transmission speed, and attack detection accuracy while reducing packet loss, delay, and network congestion. Real-time monitoring and intelligent analysis help identify malicious activities quickly and ensure secure communication between network nodes.

The implementation results demonstrate that the AI-driven system performs better than traditional routing and security methods in terms of reliability, adaptability, and scalability. The proposed framework is highly suitable for real-world applications such as military communication systems, disaster recovery operations, emergency services, IoT networks, and wireless sensor networks.

In conclusion, the integration of Artificial Intelligence with Ad Hoc Networks provides a smart, adaptive, and secure communication environment that enhances both network performance and data security. The proposed system offers an effective and future-oriented solution for secure wireless communication in decentralized and dynamic network infrastructures.

References

1. S. Corson and J. Macker, “Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,” IEEE Publications, 1999.
2. C. Perkins, “Ad Hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, IEEE Network Publications, 2003.
3. D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing Journal, 1996.
4. Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” ACM International Conference Proceedings, 2000.
5. S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” ACM MOBICOM, 2000.
6. L. Buttyan and J. Hubaux, “Security and Cooperation in Wireless Networks,” Cambridge University Press, 2007.
7. A. Mishra and K. Nadkarni, “Security in Wireless Ad Hoc Networks,” Handbook of Wireless Networks and Mobile Computing, 2002.
8. E. Royer and C. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, 1999.
9. D. E. Denning, “An Intrusion Detection Model,” IEEE Transactions on Software Engineering, 1987.
10. I. Goodfellow, Y. Bengio, and A. Courville, “Deep Learning,” MIT Press, 2016.
11. R. Shanmugavadivu and N. Nagarajan, “Secure Data Transmission in MANET using Intelligent Techniques,” International Journal of Computer Applications, 2011.
12. P. Gupta and P. R. Kumar, “The Capacity of Wireless Networks,” IEEE Transactions on Information Theory, 2000.