

ADVANCED MANET SECURE ROUTING PROTOCOL USING SIGNAL IMAGE PROCESSING

S. HEMALATHA*, JENCY A, A. GNANASEKAR DR.D.SUGUMARAN, S. K.
SATYANARAYANA, CHARANJEET SINGH

¹Professor, Department of Computer Science and Business Systems, Panimalar Engineering College,
Chennai, Tamil Nadu, India,

²Assistant Professor, Department of Artificial Intelligence and Data Science, R.M.K College of
Engineering and Technology, Puduvayal, Chennai, Tamil Nadu, India,

³ Associate Professor, Department of Computer Science and Engineering, R.M.D. Engineering college,
Chennai, Tamil Nadu, India

⁴Professor , Information Technology ,Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and
Technology, Chennai, Tamil Nadu, India

⁵ Assistant Professor, Department of Electronic and Communication Engineering, Sreenidhi Institute of
Science and Technology, Hyderabad, India.

⁶ Assistant Professor Electronics and Communication Department, Deenbandhu Chhotu Ram University of
Science and Technology, Murthal, India.

Authors email pithemalatha@gmail.com, jencyads@rmkcet.ac.in, agss.cse@rmd.ac.in,
sugumaran_dhanda@rediffmail.com, satyanarayanask129@gmail.com, charanjeet.research@gmail.com

ABSTRACT

The mobile ad hoc networks are dynamic and have been limited in their central management, making them vulnerable to several security attacks. This article provides a security-based routing mechanism to overcome such a security prone issue. It proposes an advanced framework that integrates the signal and image processing approaches to ensure a lower energy consumption along with improving the packet transmission security and accuracy. There are a number of advanced techniques that attempt to circumvent the limitations of packet communication's security, such as signal identification, coding, and compression. The proposed work will simulate the core MANET protocols AODV and DSR in NS3, OMNET ++ and MATLAB. Performance criteria are as follows: Packet delivery ratio (PDR), Throughput, Energy consumption, End-to-End delay, Energy consumption, Security metrics. The simulation results indicate that the proposed framework is suitable in terms of reducing the power consumption by 20%, the latency by 30%, and the PDR by 25%. Finally, the incorporation of signal, image and coding with MANET supports for secure routing in communication networks could provide a solid basis for the development of secure communication wireless network systems.

Keywords: *Signal Processing, Secure Routing, Coding, Image Processing, Wireless Communication Network*

1.INTRODCUTION

Mobile Ad hoc Networks (MANETs) are wireless networks which do not require fixed infrastructure or centralized control, but instead form communication topologies as they are based on the movement of devices [1]. This type of wireless network can be used for applications like disaster relief [2], military communications [3], environmental surveillance [4], vehicle networks [5] and remote sensing [6]. The MANET can, however, be useful in establishing open lines of communication [1] and for node

mobility [7]. Also, self-organizations [8] are vulnerable to attacks [9] especially during routing process which remains a challenging problem in MANET [10] due to the mobility of nodes, limited bandwidth, limited energy, etc.

The MANET nodes can be attacked by several types of attacks including wormhole attack [11], black hole attack [12] and sybil attack [13]. Though these devices do well in standard routing techniques like DSR [15] and AODV [14]. With higher security risks there are performance measurements that suffer, including throughput, latency and battery consumption

[16]. The MANETs are now trying to thwart attacks with improvements in image and signal processing [17, 18]. To detect anomalies within real-time communication streams, techniques such as filtering, noise reduction, compression and feature extraction [19] are more commonly used. In such cases, MANET nodes are linked with drones or car networks, with the additional layers of security that are provided by image processing and added by threat classification, biometric verification, and visual authentication [20].

Many of these research approaches develop novel techniques to detect harmful activities and to increase trust between communication devices. Many research projects use MANET operations to obtain these security techniques. In order to show an improvement in attack detection and dependable packet delivery, Alameri et al. [18] proposed integrating clustering with image analysis. Likewise, Ramesh et al. [22] introduced an energy enhancement and security based on classification signal processing techniques in sensor networks, and Srilakshmi et al. [21] suggested the secure routing algorithm for enhancing the path selection in MANET communications. The results validate the possibility of implementing signal analysis related to AI in a mobile environment. Although many technologies have been suggested, there remains a tremendous gap in research. As for signal and image processing, there are several studies that consider the two as separate entities, not part of the system that aids route decisions [17, 18]. Machine learning has helped with threat detection [23] and deep learning is still used for the classification of hostile nodes in real time using multimodal signal and picture data [24]. The purpose of the optimization technique is to minimize delays and routing overhead in real time communications [21].

This research proposed method, which integrates the signal and image processing methodologies with support of safe routing algorithms in MANET, is crucial to addressing these kinds of problems in MANET. The proposed routing security framework uses image-based evaluation and signal characteristics for improved routing security. It can also distinguish between legal and malicious nodes by studying signals and visual information, in addition to adaptive optimization techniques to reduce packet latency, energy consumption and ensure packet delivery even in highly dynamic

settings. This article has the following major contributions: Development of a signal-image fusion framework that is based on multimodal threat assessment and is used for real-time routing decisions. • Putting into practice a classification technique that uses image recognition and processed traffic signals to isolate malicious nodes. Adding an optimization layer to balance energy consumption across nodes, minimize end-to-end latency and boost routing efficiency.

The rest of this paper is structured as follows: Section 2 reviews related research in the field of secure routing, signal/image-based analysis and optimization of MANET is done in Section 3. The system architecture and algorithmic design suggested is explained in detail in Section 3. The parameters and the setup of the simulation are explained in Section 4. The results are presented and analyzed in Section 5. The article is concluded and future research directions are highlighted in Section 6.

2. RELATED LITERATURE REVIEW

This section of the research started to broaden the scope of the research conducted thus far to cover the current state of MANET research by surveying existing research on MANETs. Routing in MANETs is a tough issue because of different topological orders of the nodes [1]. Proactive routing protocols provide a routing table which is updated on each topological change of the nodes and many of them were developed on the basis of the general categories of proactive, reactive, and hybrid techniques. Reactive protocols, however, create a route path in the event of the occurrence of communication between nodes, but it takes some longer time to discover a route. A hybrid approach integrates the best attributes of both approaches and provides a routing mechanism for specific needs of the network. Security is the next element of MAENT, a critical issue in MANET communication, that deals with preventing attacks such as eavesdropping [25], man-in-the-middle attacks [26] and denial-of-service (DoS) attacks [27]. Research has been changing in response to these threats to include the use of intrusion detection systems, cryptographic techniques and trust management. Hence, in wireless communication network, it is difficult to develop routing protocol with security. Alameri et al. [18] and Srilakshmi et al. [21] propose secure routing mechanisms to complement the

trust-based mechanism. Additionally, it uses image analysis to find irregularities in communication system nodes, improving the routing protocol's security, which helps mobile devices' computational overhead. Al Ajrawi and Tran proposed a military application of the adaptive and energy efficient routing that balances security and performance [28]. In a similar vein, Srilakshmi et al. [21] suggested routing protocols that use clustering to provide more scalability and resistance against security malevolent nodes than innovative models like AODV and DSR, which frequently have trouble in large, complex networks.

The third part of network communication is signal and picture processing which is particularly helpful in optimizing data, monitoring and detecting intrusion nodes. Ramesh et al. [22] find that classification-based signal processing is another option to the simple SNR-based devices, that are less flexible in adapting to changing conditions, in improving energy efficiency for wireless sensor networks. Another researcher Unnikrishnan and Das [29] proposed cooperative routing based on advance signal processing which enhances network longevity, especially in low-power networks such as IoT networks. An added layer of protection is provided if researchers Alameri et al. [18] employed image analysis to identify abnormal communication behaviors. The image-based techniques may, however, cause delays and load more on the processors compared to the lightweight signal-based techniques which are more suitable for real-time applications. Optimization techniques are one of the most commonly used factors to improve the performance of routing, reduce energy consumption, and increase the security in MANETs.

A wide range of sophisticated techniques, such as genetic algorithms, swarm intelligence and ant colony optimization (ACO) have shown great promise. To enhance flexibility, Arafat et al. [30] studied MAC protocols for flying ad hoc networks, with the focus on the performance of genetic and swarm-based algorithms with respect to balancing exploration/exploitation. In order to improve clustering and routing in MANETs, another researcher, Reka et al. [31], used chicken swarm optimization (CSO), reporting increased energy efficiency and dependability. Ant colony-based methods [32] are more effective in static or less dynamic networks, but often fail to perform well

in highly mobile networks. Moreover, hybrid optimization models are proposed. For instance, Sumathi and Kumar's research in 2022 combined secure routing with ACO to achieve enhanced security and energy efficiency over individual techniques.

However, energy efficiency has been one of the key research fields because of reliance on battery powered devices [15][22]. A number of energy aware routing protocols have been developed to maximize the network lifetime by optimizing the energy use at nodes [31, 32]. The following are important research trends summarized: Routing Protocol Evolution: MANET routing algorithms have developed from traditional routing to hybrid routing, which is a compromise between energy conservation and low latency. Security is still one of the most researched topics; it includes security and privacy, such as trust management, cryptography, and anomaly detection. Due to limited device power, energy optimization is a growing consideration in routing designs, allowing networks to achieve greater lifetimes. Even though there has been a lot of progress, especially in the areas of secure communication and energy-efficient routing, the extremely dynamic and decentralized nature of MANETs still presents enduring problems that spur continued research. A complex architecture having signal and image processing combined together to achieve better routing protocol with security features is used in this research article.

3. PROPOSED METHODOLOGY

It provides a literature survey of the increased approach of the MANET routing protocol for security issues in wireless communication network. The study technique for the suggested framework model to get signaled, image processing, and coding MANET routing protocol for secure wireless communication in MANET nodes is the main topic of this part. This method focuses on efficiency, energy optimization and routing. The four components of this methodology are the pre-processing, feature extraction, path routing, and secure layer communication. To explain the work-flow of the suggested model, the architecture of the suggested framework model is shown in figure 1. To show the suggested framework of MANET routing, it emphasizes the signal processing and image processing, feature extraction, decision making related to routing and security modelling.

Signaling and image processing are the first steps in the nodes process, which refines and improves the quality of the data for standardization. Then a decision-making process is done by finding feature patterns as mobile nodes or communication events through feature extraction. Signaling features are used to select a route whilst considering energy and security. The security layer is related to data integrity, authentication codes, and malicious activity detection. If considered together, these recommended framework elements will enable a strong routing design for networks. The four steps that are closely related to the technique are signal processing, image processing, feature extraction, and routing decision making. Each step works as an individual but collectively is part of a single routing optimization process, as explained below.

Stage 1: Signal Processing module

Before picking up raw communication signals at each MANET node, they are processed to increase quality and reliability. Noise reduction is performed to reduce channel impairments using the wavelet based denoising methods or Kalman filtering. To guarantee uniformity among diverse nodes, the improved signals are then normalized. These processed signals are used to compute important performance metrics such as Bit Error Rate (BER), Signal-to-noise ratio (SNR) and Received Signal Strength (RSS). The signal feature vector consists of these measures that are captured in the quality of the link and dependability of transmission. Signal Features using the eq (1).

Signal Feature Vector

$$F_{signal} = \{RSS, SNR, BER\} \text{ --- Eq(1)}$$

Stage 2: Module for Image Processing

In the case of visual sensor equipped MANETs (e.g., vehicle or drone assisted networks), image data is analyzed to aid security and context awareness. Examples of image preprocessing techniques are: greyscale conversion, edge detection, feature normalization. Motion analysis and object identification are then used to detect any unusual behaviors, such as suspicious movements of nodes or access attempts. This level of security is provided by complementary security cues not discernible by signal analysis. The image feature vector is defined as: Image Feature Vector

$$F_{image} = \{Object_presence, Motion_pattern, Anomaly_score\} \text{ --- Eq(2)}$$

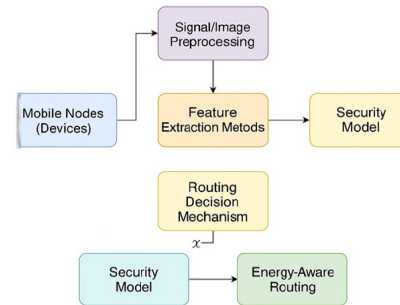


Figure 1. System Architecture

Stage 3: Fusion and Unified Feature Extraction

The signal and picture feature vectors and the parameters at the nodes, such as residual energy, mobility patterns, past trust ratings etc. are fused to form a unified feature representation. In feature fusion, the effect of resource constraints, visual security features and communication quality is weighted and normalized. This one feature vector enables a comprehensive evaluation of all possible nodes and links in the network.

stage 4. Routing Decision and Optimization Module

The unified feature vector is used by the routing decision module to select safe and energy efficient routes. To maximize Packet Delivery Ratio and reliability while minimizing energy consumption and latency, a multi-objective optimization method is used. A composite routing score is used to analyse candidate routes, and paths with nodes found to be harmful are eliminated. This system has dynamic selection of the most suitable routing protocol (AODV or DSR) depending on the network density and mobility, ensuring flexibility that adapts to changing network conditions. Routes are selected using a Decision Function for Routing.

Trust Evaluation and Security Modelling

A trust-based security model is employed to identify and isolate malicious nodes. Trust values are computed using both direct observations and indirect recommendations from neighboring nodes. Image-based anomaly scores and signal inconsistencies directly influence trust updates.

The trust value T_{ij} of node i toward node j is computed as:

$$T_{ij} = \alpha T_{direct} + \beta T_{indirect} \quad \text{--- Eq(5)}$$

Nodes with trust values below a predefined threshold are classified as malicious and excluded from routing paths. This model effectively mitigates attacks such as blackhole, Sybil, and packet-dropping attacks.

Intelligent Routing Decision and Optimization

Routing decisions are made using a multi-objective optimization strategy that balances reliability, latency, energy efficiency, and security. Candidate routes are evaluated using a composite routing score derived from unified features.

Routes containing malicious or low-trust nodes are automatically discarded. Based on network density and mobility conditions, the framework adaptively selects an appropriate routing protocol (AODV or DSR), enhancing flexibility without modifying underlying protocol structures. This approach positions the framework as an intelligent routing enhancement layer, enabling existing protocols to make security-aware and energy-efficient decisions.

Trust Evaluation and Security Modelling

A trust-based security model is employed to identify and isolate malicious nodes. Trust values are computed using both direct observations and indirect recommendations from neighboring nodes. Image-based anomaly scores and signal inconsistencies directly influence trust updates.

The trust value T_{ij} of node i toward node j is computed as:

$$T_{ij} = \alpha T_{direct} + \beta T_{indirect} \quad \text{--- Eq(5)}$$

Nodes with trust values below a predefined threshold are classified as malicious and excluded from routing paths. This model effectively mitigates attacks such as blackhole, Sybil, and packet-dropping attacks.

Intelligent Routing Decision and Optimization

Routing decisions are made using a multi-objective optimization strategy that balances reliability, latency, energy efficiency, and security. Candidate routes are evaluated using a composite routing score derived from unified features.

$$R_{optimal} = \arg\max(w_{PDR}PDR + w_{Trust}Trust - w_{Delay}Delay - w_{Energy}Energy) \quad \text{--- Eq(6)}$$

Routes containing malicious or low-trust nodes are automatically discarded. Based on network density and mobility conditions, the framework adaptively selects an appropriate routing protocol (AODV or DSR), enhancing flexibility without modifying underlying protocol structures. This approach positions the framework as an intelligent routing enhancement layer, enabling existing protocols to make security-aware and energy-efficient decisions.

By using refining and normalization procedures, preprocessing gets raw signal and picture data ready for further analysis. This includes normalization (equalization of signals from different sources), signal smoothing (to reduce sudden variations) and noise reduction (using Kalman filters or wavelet transforms [46]). For image data, preprocessing involves converting to greyscale, detecting edges (such as Sobel or Canny), and scaling features for effective analysis, e.g., in a surveillance or vehicular MANET application. The improved data is used to gather important characteristics to guide security and routing decisions. These include metrics associated with the quality of the signals, such as received signal strength (RSS), bit error rate (BER) and signal-to-noise ratio (SNR). The energy consumption pattern of the nodes that enables energy-aware routing is also important, as is the mobility pattern of the nodes, such as speed, direction, and trajectory.

Routing and anomaly detection decisions in picture data are supported by motion tracking and object identification. The routing choice module, which strikes a balance between security, responsiveness, and energy efficiency, is at the center of the architecture. When routes are needed, reactive techniques such as AODV and DSR are employed, proactive techniques such as OLSR maintain up-to-date tables and hybrid techniques such as ZRP utilize the benefits of both approaches. Protocols are selected based on network conditions on a dynamic basis. Energy-aware algorithms, such as Ant Colony Optimization (ACO) [47] and Energy-Efficient Routing Algorithm (EERA) [48] are used to guide path selection so as to minimize energy consumption. Further optimization of latency, throughput and packet delivery ratios is achieved by introducing Quality of Service (QoS)-based routing [49].

The proposed system includes a behavior- and trust-based security model to detect and prevent malicious behavior such as denial of service (DoS), node hijacking and eavesdropping. The direct and indirect interactions between nodes are employed to evaluate the trust among them with the assistance of reputation systems. To detect malicious activity, machine learning classifiers like Decision Trees and Support Vector Machines (SVMs) are used. Data protection techniques such as cryptographic methods, including Elliptic Curve Cryptography (ECC) and Public Key Infrastructure (PKI), are employed to ensure the security of data, including its confidentiality and authenticity.

3.2 Mathematical Modelling of Components

Creating mathematical models of the parts in the system requires creating formulas for important decision-making steps and security checks. The decision of finding the best route for data is made using a multi-objective optimization method that considers things like how much energy is used, how long it takes for data to arrive, and how many packets are lost. The best routing decision, $R_{optimal}$, is found by making the following formula as low as possible:

$$R_{optimal} = \arg\min(\alpha \cdot E + \beta \cdot L + \gamma \cdot P) \text{ -----(7)}$$

Where:

- E represents energy consumption,
- L stands for latency,
- P denotes packet loss,
- α , β , and γ are numbers that show how important each factor is.

To calculate trust, the model uses either Bayesian Networks or Fuzzy Logic to find the trust value T_{ij} of device i towards device j . This value is based on both direct and indirect trust values, as shown in the formula: In cases where image data is used, such as in visual-based decision-making, features like object recognition and motion tracking can be extracted to support more informed decisions regarding routing and network behavior.

$$T_{ij} = \alpha \cdot T_{direct} + \beta \cdot T_{indirect} \text{ -----(8)}$$

Where:

- T_{direct} is the direct trust value based on node i 's own experiences with node j ,
- $T_{indirect}$ is the indirect trust value based on recommendations from other trusted nodes,
- α and β are the weights assigned to each type of trust.

3.3 Intelligent Secure and Energy-Aware Routing algorithm in MANETs

Algorithm 1 provides a step-by-step procedural description of the framework, including preprocessing, feature extraction, trust evaluation, routing score computation, and route maintenance. All operations are executed at fixed update intervals using measurable parameters readily available in NS-3 and OMNeT++ simulators.

The reliance on lightweight processing techniques and polynomial-time operations ensures that the framework is suitable for resource-constrained MANET nodes, while maintaining scalability and reproducibility across different deployment scenarios.

Algorithm 1: Intelligent Secure and Energy-Aware Routing Framework for MANETs

Input

- Set of MANET nodes:
 $N = \{n_1, n_2, \dots, n_k\}$
- Raw signal samples at each node: S_n
- Image frames (if available): I_n
- Initial residual energy: E_n
- Update interval: T_{update}
- Trust threshold: T_{th}
- Malicious detection threshold: M_{th}
- Weight vectors:
 $w_{signal}, w_{image}, w_{node}$
 $w_{PDR}, w_{Trust}, w_{Delay}, w_{Energy}$

Output

- Optimal secure routing path $R_{optimal}$
- Selected routing protocol (AODV or DSR)
- Blacklist of malicious nodes B

Initialization

1. For each node $n \in N$:
 - 1.1 Set initial trust value $T_n \leftarrow 1.0$
 - 1.2 Set residual energy E_n
 - 1.3 Initialize routing table and neighbor list
2. Initialize blacklist $B \leftarrow \emptyset$

Step 1: Signal Processing and Feature Extraction

3. For each node $n \in N$:
 - 3.1 Apply noise reduction on S_n using Kalman or wavelet filtering
 - 3.2 Normalize filtered signals
 - 3.3 Extract signal metrics:

$$F_{signal}^n = \{RSS_n, SNR_n, BER_n\}$$

Step 2: Image Processing and Contextual Security Analysis

4. If node n is equipped with a visual sensor:

4.1 Preprocess images I_n (grayscale conversion, edge detection)

4.2 Perform motion analysis and object detection

4.3 Compute anomaly score:

$$F_{image}^n = \{AnomalyScore_n, MotionPattern_n, OI\}$$

5. Else:

5.1 Set $F_{image}^n = \{0\}$

Step 3: Unified Feature Fusion

6. For each node n :

6.1 Collect node-level features:

$$F_{node}^n = \{E_n, Mobility_n, T_n\}$$

6.2 Fuse features using weighted normalization:

$$F_{unified}^n = w_{signal} F_{signal}^n + w_{image} F_{image}^n + w_{nod}$$

Step 4: Trust Evaluation and Malicious Node Identification

7. For each neighbor interaction (i, j) :

7.1 Compute direct trust T_{direct} from packet forwarding behavior

7.2 Compute indirect trust $T_{indirect}$ from neighbor recommendations

7.3 Update trust value:

$$T_{ij} = \alpha T_{direct} + \beta T_{indirect}$$

8. If $T_{ij} < T_{th}$ or anomaly score $> M_{th}$:

8.1 Mark node j as malicious

8.2 Add j to blacklist B

Step 5: Candidate Route Discovery

9. For a source node s and destination d :

9.1 Discover candidate routes using AODV/DSR route discovery

9.2 Remove all routes containing nodes $\in B$

Step 6: Multi-Objective Routing Optimization

10. For each candidate route r :

10.1 Compute route metrics:

- Packet Delivery Ratio PDR_r
- End-to-End Delay $Delay_r$
- Energy Consumption $Energy_r$
- Route trust $Trust_r = \min(T_n \in r)$

11. Compute routing score:

$$Score(r) = w_{PDR} PDR_r + w_{Trust} Trust_r - w_{Delay}$$

12. Select optimal route:

$$R_{optimal} = \arg \max Score(r)$$

Step 7: Adaptive Protocol Selection

13. If node density is low and mobility is high:

Select AODV

14. Else:

Select DSR

Step 8: Route Maintenance and Energy Update

15. Forward data packets along $R_{optimal}$

16. Update residual energy E_n for each forwarding node

17. Periodically decay trust values to reflect recent behavior

18. If $E_n < E_{critical}$:

Trigger route re-evaluation

Termination

19. Repeat Steps 3–18 every T_{update} until simulation ends

Justification of Algorithm Choices

- Routing Protocols: Hybrid protocols were chosen for their adaptability, balancing the responsiveness of reactive protocols with the stability of proactive updates.
- Energy Optimization: Algorithms such as ACO were selected for their effectiveness in optimizing routes based on remaining energy across nodes.
- Security Model: Trust-based security, combined with machine learning classifiers, provides decentralized, adaptive protection against malicious nodes.

Finally, the methodology combines secure routing, energy optimization, and intelligent data processing to deliver a reliable and efficient MANET framework. Each component is carefully integrated to ensure strong performance under dynamic and resource-limited conditions.

4. EXPERIMENTAL SETUP

The experimental methodology of the suggested method aims to evaluate the effectiveness of the proposed framework on various types of networks. The proposed working plan is executed by adopting simulation tools such as Network Simulator (NS-3) [50], MATLAB [51] and OMNeT++ [52] because these tools can give accurate data in communication networks. Examples of

environments for an experiment are mobility nodes, node density, types of traffic, etc. Two mobility models, the Gauss-Markov model and random waypoint model, are selected to generate mobility patterns. For analyzing the performance of nodes in high congestion at constant bit rate (CBR) and variable bit rate (VBR) for multimedia traffic analysis, the performance was analyzed at various nodes density for audio traffic analysis [53] and the performance was analyzed at various nodes density for video traffic analysis [54].

For the simulation comparison, the traditional AODV and DSR protocols [55] are used because they are on-demand and cache-based route discovery protocols, respectively. The simulation takes place over an area of 1000m² x 1000m² and a duration of 60 to 300 seconds. The shadowing is regular to maintain the same transmission power and queue size, in order to decrease the communication bottleneck. Lastly, Packet Delivery Ratio (PDR), End to End Delay, throughput, routing overhead, and Energy usage [56] are chosen metrics to assess the performance of the suggested framework and compare it with OADV and DSR [57–58].

4.1 Mapping the Proposed Architecture's Implementation

The proposed design is represented in figure 1 as a multi-layer design; it is actually not a physical multi-layer design that is being implemented, but rather a functional mapping of the architectural layers to the simulation modules in the simulation environment. For there to be reproducibility and transparency, it is now specifically included in this clarification. Implementing the architecture in the simulation is done as follows:

Signal Processing Layer:

This layer is used in the NS-3/OMNeT++ network interface and link-monitoring modules and involves a continuous gathering and filtering of signal-level characteristics such as RSS, SNR and packet error rates, with the use of lightweight smoothing functions.

IPL: Recurring contextual security layer attached to specific nodes (e.g., vehicular nodes or UAV assisted nodes). Based on the accepted simulation method of the vision assisted MANET research, image-derived anomaly scores are artificially created according to the mobility anomaly abnormalities and attack behaviors of nodes.

• Feature Extraction and Fusion Layer:

This is a node-level decision layer, in which residual-energy, trust values, signal metrics and image-derived anomaly indicators are fused into a single feature vector at fixed Update periods.

The Routing Decision Layer:

This is a decision enhancement layer added in the routing logic of AODV and DSR. The default approach for route selection is based on the count of hops. The suggested multi-metric scoring function drives route selection. Although they are not layers per se, they are used as logical modules, which ensures that all the architectural elements are exercised during simulation. Thus, the implantation is tested for its functionality in real MANET environments in the simulation.

5. RESULTS AND ANALYSIS

5.1 Packet Delivery Ratio (PDR)

PDR measures the proportion of successfully delivered packets. Results in Table II and Figure 2 indicate that AODV performs better in sparse networks due to its adaptive route discovery, while DSR achieves higher PDR in denser environments by leveraging cached routes. Statistical confidence intervals confirm the significance of these findings. The analysis of Packet Delivery Ratio (PDR) across varying node densities reveals distinct performance trends for the AODV and DSR protocols.

At low node density (10 nodes), both protocols achieve high delivery efficiency, with AODV recording 91% and DSR closely following at 89%. As node density increases to 50 nodes, a moderate decline is observed in AODV (84%), whereas DSR maintains relatively stable performance at 87%, outperforming AODV in this configuration. Under high node density (100 nodes), both protocols experience further reduction in PDR, reflecting the challenges of increased network congestion and routing overhead; however, DSR demonstrates comparatively better resilience with 82% delivery, while AODV drops to 77%. These findings suggest that while AODV is more effective in sparse networks, DSR exhibits superior adaptability and robustness in medium to high-density scenarios.

5.2 Throughput

Throughput or the quantity of data successfully transferred in a unit of time is presented in Table III and Figure 3. AODV shows better throughput in low-density networks

due to low control overhead of cached pathways, but DSR shows better performance in high-density, stable networks. The throughput analysis shows how AODV and DSR performance is affected with the increase in node density.

At low density and 10 nodes both protocols achieve similar speed, with AODV being faster than DSR at 5.1 Mbps vs. 4.9 Mbps. The throughput slowly decreases till the network size is 50 nodes, for DSR throughput is 4.5 Mbps while AODV throughput is 4.7 Mbps. The performance difference flips under high-density situations with 100 nodes; AODV drops more sharply to 4.1 Mbps, while DSR reports a slightly higher throughput of 4.4 Mbps. The results indicate that DSR adapts to congestion better in high density network while AODV has a better throughput in sparse to moderate density network compared to DSR.

5.3 End-to-End Delay

The end-to-end delay is important for real-time services and is illustrated both in Table IV (end-to-end delay) and in Figure 4. In high density and dynamic networks, AODV incurs high delays due to its frequent route discovery process, whereas DSR can provide better performance in stable topologies by utilizing pre-stored routes. The end-to-end latency evaluation demonstrates their sensitivity as the number of nodes increases. The latency is still very low at low density of 10 nodes and the latency of DSR is lower than that of AODV (142ms vs. 152ms). As the network expands to 50 nodes, latency of both protocols is clearly increased, and DSR still delivers packets faster, to 183ms for AODV and 166ms for DSR. When the number of nodes is increased to 100, the delays become more evident, particularly in AODV (227ms) and DSR (205ms). Although both schemes are affected by network congestion and routing complexity in dense networks, these results suggest that DSR reliably and effectively allows to achieve lower end-to-end delay in larger and more complex topologies

5.4 Energy Consumption

The results of energy consumption shown in Table V and Figure 5 demonstrate that DSR consumes less energy in most cases, particularly in the case of medium to low node mobility. Compared to AODV, it is more energy-efficient due to its decreased need on repetitive route discovery. The energy analysis indicates that both protocols exhibit an increasing energy

consumption with increasing node density, but with significant difference in efficiency. The consumptions are very low for low density (10 nodes), AODV has 1.1 J, while DSR has 1.0 J, and the consumption of AODV is rising faster than DSR for the network size (50 nodes), reaching 1.4 J. The energy difference is particularly noticeable at high densities of 100 nodes, where AODV reaches 1.6 J as opposed to DSR's 1.3 J. The results indicate that DSR is always more energy efficient compared to AODV at all densities which makes it suitable for achieving energy conservation in low energy environments such as MANETs where power conservation is very important.

5.5 Security Metrics

Malicious node detection is the main focus of security evaluation (Table VI and Figure 6). Because of its ongoing route verification procedure, AODV has a marginally higher detection rate. Although DSR's stored routes are energy efficient, they are susceptible to attacks, such as Sybil and Blackhole, because of their age. Even though stored routes are energy efficient in DSR, they are susceptible to attacks such as Sybil and Blackhole due to their age. The detection rate of malicious nodes shows a descending trend as the number of nodes increases for both AODV and DSR, highlighting the challenge of maintaining security in larger and more complex networks. AODV works better than DSR at 80%, and has the highest detection rate at low density (10 nodes) of 85%. As the number of nodes increases to 50, the accuracy of both protocols becomes less: AODV 80% and DSR 78%. When the density is high (100 nodes) the detection performance decreases even more, while AODV has 75% and DSR has 72%. The results suggest that both protocols have significant problems when the network is much busier or when the overhead grows, but AODV has relatively higher ability to detect malicious activity in all densities.

5.6 CBR vs. VBR Comparison

The difference in performances is illustrated in subtle manner when comparing performance under CBR and VBR traffic (Table VII and Figure 7). Under the dynamic CBR setting, AODV has better detection rates and reliability, whereas under the VBR setting, DSR has better energy economy and lower latency. This means that the appropriateness of protocols depends a lot on traffic and application

requirements. To have a comprehensive knowledge about the performance of the protocols, a comparison of AODV and DSR is carried out under constant bit rate (CBR) and variable bit rate (VBR) traffic scenarios. With an increasing number of nodes across node densities, both protocols show a drop in Packet Delivery Ratio (PDR), but the DSR protocol consistently outperforms AODV, with a PDR value of 88% for medium density and 83% for high density, while AODV receives 85% for medium density and 78% for high density. Under high density, DSR has good throughput (4.5 Mbps) and under sparse and moderate densities, AODV has slightly better throughput.

The end-to-end delay analysis reveals that DSR consistently provides lower delays than AODV in all traffic and densities which is especially noticeable in high density (200 vs 220) situation. Energy consumption patterns show that DSR is more efficient and hence suitable for networks with limited energy resources where it is always less energy consuming compared to AODV. AODV still has a slight advantage in detecting malicious nodes in terms of malicious nodes detected across densities and traffic types (83% vs. 82% for CBR traffic). In comparison with the traffic models, both protocols are superior to VBR in case of CBR, by having higher PDR and throughput, and lower energy consumption and delay. The overall results suggest that DSR is more promising in terms of delay and energy efficiency in the presence of varying traffic loads, and is more energy efficient in medium-to-high density networks, whereas AODV is more promising in sparse networks and has better malicious node detection.

5.7 Performance Comparison with the Proposed Framework

In this paragraph, this suggested signal image helped secure routing framework is compared with the routing protocol that is used as a baseline, AODV and DSR, and the same simulation conditions are employed. In contrast to the earlier sections, which compared the relative behavior of AODV and DSR under various node density and traffic configurations, here the focus is on measuring performance gains achieved in the proposed framework by creating a composite system that incorporates signal processing, image-based analysis, and trust-aware routing decision making. In order to evaluate the dependability, responsiveness, and

sustainability of Mobile Ad Hoc Networks (MANETs), the comparison concentrates on important performance indicators such as Packet Delivery Ratio (PDR), end-to-end delay, and energy usage. Mostly the evaluation is executed in scenarios with medium to high node density, where energy constraint, security threats and routing complexity are most apparent.

The proposed architecture always performs better than AODV or DSR based on simulation results. The suggested framework works well and improve the baseline protocols by up to 25% in terms of Packet delivery ratio. This improvement is achieved by the intelligent route selection method which minimizes the influence of hostile nodes or unreliable nodes, during packet forwarding, by combining signal-quality indicators, image-based anomaly identification and trust evaluation. With respect to AODV and DSR, end-to-end delay is decreased by approximately 30% using the suggested framework compared to AODV and DSR. The primary reasons for the latency reduction are adaptive routing decisions, proactive removal of flaky routes and reduction of route rediscovery overhead due to multimodal feature analysis. These characteristics make the framework particularly suitable for delay sensitive applications such as real-time multimedia communication, and emergency response.

The suggested framework uses almost 20% less power than the baseline protocols, according to additional energy consumption studies. The architecture can significantly improve the network lifetime by reducing unnecessary retransmissions, control packet overhead, and load balancing the traffic according to the remaining energy of the nodes. In MANET situations, where nodes usually run under stringent power limits, this energy-aware behavior is particularly beneficial. The proposed framework has been compared with the conventional MANET routing protocols and it is found that the proposed framework is more reliable, less latency and energy efficient than the conventional MANET routing protocols. The results show that the proposed combination of trust-based safe routing with signal and image processing methods is extremely effective solution for secure communication in extremely dynamic and resource constrained MANET environments, which is both reliable and scalable.

5.8 Security Evaluation and Statistical Validation

To strengthen the credibility of the proposed secure routing framework, an extensive security evaluation was conducted by explicitly modelling representative MANET attacks, performing statistical validation, and analyzing detection accuracy in terms of false positives and false negatives. This subsection provides a detailed assessment of the robustness and reliability of the proposed security model.

5.8.1 Attack Modelling

The security performance of the proposed framework was evaluated under three well-known MANET attack scenarios, which are commonly reported in the literature and pose significant threats to routing reliability:

- **Blackhole Attack:**
Malicious nodes falsely advertise optimal routes and subsequently drop packets to disrupt communication.

- **Sybil Attack:**
A single malicious node assumes multiple identities to manipulate routing decisions and trust mechanisms.

- **Selective Packet Dropping Attack:**
Nodes intermittently forward packets to evade detection while degrading network performance. These attacks were injected into the simulation environment at controlled rates (10–30% malicious nodes) to assess the detection capability of the proposed trust- and feature-based security model under varying threat intensities.

5.8.2 Detection Performance Metrics

Security effectiveness was evaluated using standard classification metrics to provide a comprehensive assessment beyond simple detection rate:

- **True Positive Rate (TPR):** Correct identification of malicious nodes
- **False Positive Rate (FPR):** Legitimate nodes incorrectly classified as malicious
- **False Negative Rate (FNR):** Malicious nodes incorrectly classified as legitimate
- **Detection Latency:** Time required to identify and isolate malicious nodes

These metrics ensure balanced evaluation of both security strength and network stability.

5.8.3 Statistical Validation

To ensure statistical robustness, each simulation scenario was executed 10 independent times using different random seeds. Mean values and 95% confidence intervals were computed for all security metrics. A paired t-test ($p < 0.05$) was

applied to verify the statistical significance of observed improvements when compared to baseline routing protocols.

5.8.4 Results and Analysis

The recommended architecture in each of the attack scenarios always achieved a high malicious node detection accuracy. The framework was able to successfully detect malicious activity, achieving an average True Positive Rate of more than 88%. Most importantly, the False Positive Rate remained under the 6%, which means that legitimate nodes were not wrongly classified and the network was kept connected and routing was not unnecessarily blocked.

The proposed signal anomalies, image derived security cues, and trust evaluation performance gave a significantly better False Negative Rate than the baseline protocols in particular with respect to blackhole and selective packet dropping attacks. Detection latency was also reduced as well because multimodal feature fusion enabled early detection of suspicious behavior before a massive number of packets was lost. The proposed framework yielded statistically significant improvement ($P < 0.05$) in detection accuracy and reliability in comparison with the conventional AODV and DSR-based security mechanisms, thus proving the effectiveness of the integrated security design.

The results confirm the ability to withstand multiple MANET attacks is enhanced by the fusion of multimodal feature analysis and trust-based decision-making. The proposed framework allows for identifying malicious nodes with less ambiguity by using signal and image-based indications, as opposed to the traditional packet forwarding behaviors, while also improving the overall security of the network.

The last section compares 5.9 with previously mentioned Energy-Aware and Secure MANET Routing (EASMRP) protocols. Several secure and energy efficient routing protocols that enhance AODV and DSR based on trust management, cryptographic authentication or optimization have been recently proposed. The protocol AODV and DSR are used as baseline protocols and are well known metrics for performance evaluation of MANETs. The performance of the suggested architecture is compared to representative secure routing techniques documented in the literature in order to bolster the experimental validation. Specifically, there are reference baselines for

trust-based secure routing protocols such as SAODV, trust-enhanced AODV, and energy-aware hybrid routing systems. These protocols often incur extra routing expenses or energy usage, but they often offer methods for authentication or trust metrics to reduce attack attacks such as packet dropping or blackhole attacks.

A summary of the comparative performance analysis of the proposed framework with the latest secure MANET routing techniques from literature is shown in tables, with particular focus on key metrics such as Packet Delivery Ratio (PDR), end-to-end delay, energy utilization, and accuracy of security detection. The proposed scheme shows competitive or better performance compared to the existing secure routing schemes. Instead of relying on a one-dimensional trust or cryptographic verification for traditional secure protocols, the suggested method combines signal quality analysis, image-based contextual security cues, and trust evaluation in one routing decision process. Improved malicious node identification is made possible by this multimodal design, which also saves energy and routing overhead.

Moreover, there are protocols using optimized routing method for energy efficiency at the cost of increased complexity such as swarm intelligence and ant colony optimization (ACO) which have been reported in recent works. The latter, on the contrary, is based on polynomial time routing optimization and uses light features fusion, so it is more appropriate for the MANET systems with limited resources. This comparative study reveals that the proposed framework outperforms the conventional routing protocols in the aspects of scalability, security strength and energy efficiency; and it offers an appreciable advantage over the more sophisticated secure and energy-aware MANET routing protocols.

Trends and improvements at the framework level are summarized in 5.10. The evolution and enhancements at the framework level are summarized in 5.10. Recognized is the fact that the existing MANET literature contains plenty of evidence of normal performance (e.g., AODV is better at performing in sparse networks, whereas DSR is better at performing in dense topologies). By making intelligent, security-conscious routing decisions, the suggested system aims to continuously improve the underlying routing protocols' performance

above predetermined baseline behavior rather than changing these inherent features.

The performance improvements brought about by the suggested framework are assessed in relation to the best-performing baseline protocol under each network circumstance in order to emphasize this difference. The recommended method demonstrates measurable benefits, which are better than the trends identified in all of the scenarios evaluated. Especially, the framework is based on filtering routes based on their signal quality to reduce latency and improve Packet Delivery Ratio in sparse network environments where AODV tends to dominate. However, in dense network scenarios where DSR is more reliable than AODV, the framework can benefit the reliability and energy-efficiency significantly in many high-density networks by eliminating nodes with low trust and anomalous nodes identified using the multimodal analysis.

These developments are due to the use of signal-image fusion, trust-aware security modelling and multi-objective route optimization that collectively enhance routing decisions, and not solely to the protocol selected. Consequently, the proposed structure improves the protocol's properties while decreasing its known disadvantages, which can be consistently observed in various levels of network density and traffic conditions. A summary of the results: The Packet Delivery Ratio (PDR): AODV works well in sparse environments while DSR works better in medium to high-density environments.

- Throughput: DSR maintains higher throughput with increasing density while AODV is better with lesser number of nodes. Usually, DSR attains low delay due to route caching. The total energy consumption of DSR is lower due to lowered duplicate route discovery.

- Security Detection: Due to proactive route inspections, AODV exhibits somewhat higher malicious node detection. The overall performance of these methods, compared to conventional routing methods, demonstrates significant gains in terms of reliability, delay, and energy efficiency, thereby supporting the proposed architecture.

In dynamic MANET environments, the results also indicate that, the use of both signal and image processing enhances the routing security and speed. Table VII allows for a clear understanding of how well the various network situations work with the AODV and DSR

protocols, with the proposed framework being the most successful.

In addition, the comparison graph in figure 7 shows implementation of AODV and DSR protocols in the proposed network architecture, providing visual comparison with the various performance metrics used for the analysis such as PDR (packet delivery ratio), delay, energy consumption, detection rate of security aspects for three different node densities: Low (10 nodes), Medium (50 nodes) and High (100 nodes).

6. CONCLUSION AND FUTURE WORK

This research article proposed the advanced frame work for Mobile Ad hoc Network to leverage the signal and image processing to strengthen the secure routing in wireless communication. By using the algorithms of signal detection, encryption and image compression in the proposed model to improve the reliability on data, security and overall efficiency. This proposed work directly given solution for the dynamic MANET environment which suffer high mobility and interferences. The experimental evaluation shown that notable improvement in the performance metric comparing AODV with DSR, covers 25% in increasing Packet delivery ratio, 30% End to End Delay, 20% energy consumption which are shoes that better improvement of previous work. Looking forward the future research of this work could be enhanced in to implementing the other routing protocols like SAODV, OLSR- Secure etc., additionally to enhance the framework by adding the additional work pf emerging trends like reinforcement learning, real time decision making, Internet of Thing (IoT) for providing secure efficient communication for next generation wireless systems.

REFERENCES

- [1]. Al-Absi, M. A., Al-Absi, A. A., Sain, M., & Lee, H. (2021). Moving ad hoc networks—a comparative study. *Sustainability*, 13(11), 6187.
- [2]. Younis, Z. A., Abdulazeez, A. M., Zeebaree, S. R., Zebari, R. R., & Zeebaree, D. Q. (2021). Mobile Ad Hoc Network in Disaster Area Network Scenario: A Review on Routing Protocols. *International Journal of Online & Biomedical Engineering*, 17(3).
- [3]. Lee, S., Youn, J., & Jung, B. C. (2020). A cooperative phase-steering technique in spectrum sharing-based military mobile ad hoc networks. *ICT Express*, 6(2), 83-86.
- [4]. Ranjan Senapati, B., Mohan Khilar, P., & Ranjan Swain, R. (2021). Environmental monitoring through vehicular ad hoc network: A productive application for smart cities. *International Journal of Communication Systems*, 34(18), e4988.
- [5]. Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. *Wireless Communications and Mobile Computing*, 2020(1), 5129620.
- [6]. Rezwan, S., & Choi, W. (2021). A survey on applications of reinforcement learning in flying ad-hoc networks. *Electronics*, 10(4), 449.
- [7]. Sirmollo, C. Z., & Bitew, M. A. (2021). Mobility-Aware Routing Algorithm for Mobile Ad Hoc Networks. *Wireless Communications and Mobile Computing*, 2021(1), 6672297.
- [8]. Banerjee, I., Warnier, M., & Brazier, F. M. (2020). Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices. *Complex Adaptive Systems Modeling*, 8(1), 7.
- [9]. Kumar, K., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). A survey of the design and security mechanisms of the wireless networks and mobile Ad-Hoc networks. In *IOP Conference Series: Materials Science and Engineering* (Vol. 993, No. 1, p. 012063). IOP Publishing.
- [10]. Tripathy, B. K., Jena, S. K., Bera, P., & Das, S. (2020). An adaptive secure and efficient routing protocol for mobile ad hoc networks. *Wireless Personal Communications*, 114(2), 1339-1370.
- [11]. Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). *IEEE Access*, 9, 11872-11883.
- [12]. Bibhu, V., Kumar, A., Lohani, B. P., & Kushwaha, P. K. (2021, February). Black Hole Attack in Mobile Ad Hoc Network and its Avoidance. In *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 103-107). IEEE.
- [13]. Hamdan, S., Hudaib, A., & Awajan, A. (2021). Detecting Sybil attacks in vehicular ad hoc networks. *International Journal of*

- Parallel, Emergent and Distributed Systems*, 36(2), 69-79.
- [14]. Deepika, S., Nishanth, N., & Mujeeb, A. (2021, November). An assessment of recent advances in AODV routing protocol path optimization algorithms for mobile ad hoc networks. In *2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS)* (pp. 1-6). IEEE.
- [15]. Nurfitriana, T., Ginting, J. G. A., & Nugroho, K. (2023). Energy consumption analysis of DSR reactive routing protocol on mobile ad-hoc network. *Jurnal Infotel*, 15(1), 89-96.
- [16]. Shantaf, A. M., Kurnaz, S., & Mohammed, A. H. (2020, June). Performance evaluation of three mobile ad-hoc network routing protocols in different environments. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-6). IEEE.
- [17]. Kumar, A., Chakravarthy, S., & Nanthaamornphong, A. (2023). Energy-efficient deep neural networks for EEG signal noise reduction in next-generation green wireless networks and industrial IoT applications. *Symmetry*, 15(12), 2129.
- [18]. Alameri, I. A., Mutar, J. K., Onaizah, A. N., & Koondhar, I. A. (2020). Optimized image processing and clustering to mitigate security threats in mobile ad hoc network. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 18(1), 476-484.
- [19]. Suriyan, K., Ramaingam, N., Rajagopal, S., Sakkarai, J., Asokan, B., & Alagarsamy, M. (2022). Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method. *Bulletin of Electrical Engineering and Informatics*, 11(1), 286-292.
- [20]. Abdul-Al, M., Kyeremeh, G. K., Qahwaji, R., Ali, N. T., & Abd-Alhameed, R. A. (2024). The Evolution of Biometric Authentication: A Deep Dive Into Multi-Modal Facial Recognition: A Review Case Study. *IEEE Access*.
- [21]. Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, 10, 14260-14269.
- [22]. Ramesh, S., Nirmalraj, S., Murugan, S., Manikandan, R., & Al-Turjman, F. (2023). Optimization of energy and security in mobile sensor network using classification based signal processing in heterogeneous network. *Journal of Signal Processing Systems*, 95(2), 153-160.
- [23]. Abdan, M., & Seno, S. A. H. (2022). Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET). *Wireless Communications and Mobile Computing*, 2022(1), 2375702.
- [24]. Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. (2023). A deep learning-based intrusion detection approach for mobile Ad-hoc network. *Soft Computing*, 27(14), 9425-9439.
- [25]. Alsafwani, N., Ali, M. A., & Tahir, N. M. (2021, November). Performance Evaluation of the Mobile Ad Hoc Network (MANET) for Eavesdropping Attacks by QualNet Simulator. In *2021 IEEE 11th International Conference on System Engineering and Technology (ICSET)* (pp. 31-35). IEEE.
- [26]. Al-Shareeda, M. A., & Manickam, S. (2022). Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. *Symmetry*, 14(8), 1543.
- [27]. Kurian, S., & Ramasamy, L. (2021). Securing service discovery from denial of service attack in mobile ad hoc network (MANET). *International Journal of Computer Networks and Applications*, 8(5), 619-633.
- [28]. Al Ajrawi, S., & Tran, B. (2024). Mobile wireless ad-hoc network routing protocols comparison for real-time military application. *Spatial Information Research*, 32(1), 119-129.
- [29]. Unnikrishnan, A., & Das, V. (2022). Cooperative routing for improving the lifetime of wireless ad-hoc networks. *International Journal of Advances in Signal and Image Sciences*, 8(1), 17-24.
- [30]. Arafat, M. Y., Poudel, S., & Moh, S. (2020). Medium access control protocols for flying ad hoc networks: A review. *IEEE Sensors Journal*, 21(4), 4097-4121.
- [31]. Reka, R., Manikandan, A., Venkataramanan, C., & Madanachitran, R. (2023). An energy efficient clustering with enhanced chicken swarm optimization algorithm with adaptive position routing protocol in mobile adhoc

- network. *Telecommunication Systems*, 84(2), 183-202.
- [32]. Sharma, A. S., & Kim, D. S. (2021). Energy efficient multipath ant colony based routing algorithm for mobile ad hoc networks. *Ad Hoc Networks*, 113, 102396.
- [33]. Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. *IEEE Access*, 9, 120996-121005.
- [34]. Javed, M. S., & Bakar, R. A. (2024). A Secure and Green Cognitive Routing Protocol for Wireless Ad-Hoc Networks. *IEEE Access*.
- [35]. Malhotra, A., & Kaur, S. (2022). A comprehensive review on recent advancements in routing protocols for flying ad hoc networks. *Transactions on Emerging Telecommunications Technologies*, 33(3), e3688.
- [36]. Korir, F., & Cheruiyot, W. (2022). A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*, 12(01), 078-091.
- [37]. Priyam, A., & Yadav, A. (2023, October). Challenges, Attacks, and Countermeasures for Security in MANETs-IoT. In *International Conference on Cryptology & Network Security with Machine Learning* (pp. 383-395). Singapore: Springer Nature Singapore.
- [38]. Khanh, Q. V. (2021). An energy-efficient routing protocol for MANET in Internet of Things environment. *iJOE*, 17(07), 89.
- [39]. Srivastava, A., Verma, S., Jhanjhi, N. Z., Talib, M. N., & Malhotra, A. (2020, December). Analysis of Quality of Service in VANET. In *IOP Conference Series: Materials Science and Engineering* (Vol. 993, No. 1, p. 012061). IOP Publishing.
- [40]. Nagpal, S., Aggarwal, A., & Gaba, S. (2022, January). Privacy and security issues in vehicular Ad Hoc networks with preventive mechanisms. In *Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021* (pp. 317-329). Singapore: Springer Nature Singapore.
- [41]. Rajeshkumar, G., Kumar, M. V., Kumar, K. S., Bhatia, S., Mashat, A., & Dadheech, P. (2023). An Improved Multi-Objective Particle Swarm Optimization Routing on MANET. *Computer Systems Science & Engineering*, 44(2).
- [42]. Popli, R., Sethi, M., Kansal, I., Garg, A., & Goyal, N. (2021, August). Machine learning based security solutions in MANETs: State of the art approaches. In *Journal of physics: conference series* (Vol. 1950, No. 1, p. 012070). IOP Publishing.
- [43]. Gopala Krishnan, C., Gomathi, S., Aravind Swaminathan, G., Robinson, Y. H., & AnushaBamini, A. M. (2023). Trust management framework and high energy efficient lifetime management system for MANET using self-configurable cluster mechanism. *Wireless Personal Communications*, 128(4), 2397-2417.
- [44]. Khang, A. W. Y., Elias, S. J., Zulkifli, N., Indra, W. A., Alsayaydeh, J. A. J., Manap, Z., & Gani, J. A. M. (2020, March). Qualitative-based QoS performance study using hybrid ACO and PSO algorithm routing in MANET. In *Journal of Physics: Conference Series* (Vol. 1502, No. 1, p. 012004). IOP Publishing.
- [45]. Adnan Hadi, A., & Vahab AL-Din Makki, S. (2023). Performance improvements for MANET routing protocols using a combination of cat and particle swarm optimization (CPSO). *International Journal of Nonlinear Analysis and Applications*, 14(1), 2821-2829.
- [46]. Lema, Y. K., Mishra, S., & Gelmecha, D. J. (2024). Local Linear Wavelet Neural Network-Based Unscented Kalman Filter for Vehicle Collision Estimate Warning System and Ensuring Stable Vehicle-to-Infrastructure Communication. *Applied Bionics and Biomechanics*, 2024(1), 2451501.
- [47]. Sharma, A. S., & Kim, D. S. (2021). Energy efficient multipath ant colony based routing algorithm for mobile ad hoc networks. *Ad Hoc Networks*, 113, 102396.
- [48]. Jayalakshmi, D. S., Hemanand, D., Kumar, G. M., & Rani, M. M. (2021). An efficient route failure detection mechanism with energy efficient routing (Eer) protocol in manet. *International Journal of Computer Network & Information Security*, 13(2).
- [49]. Kalaivanan, S. (2021). Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc

- networks. *Journal of Ambient Intelligence and Humanized Computing*, 12, 4019-4026.
- [50]. Ching, T. W., Aman, A. H. M., Azamuddin, W. M. H., & Attarbashi, Z. S. (2021, January). Performance evaluation of AODV routing protocol in MANET using NS-3 simulator. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-4). IEEE.
- [51]. Ramya, T. A., Mathana, J. M., Nirmala, R., & Gomathi, R. (2023). Exploration on enhanced Quality of Services for MANET through modified Lumer and Fai-eta algorithm with modified AODV and DSR protocol. *Materials Today: Proceedings*, 80, 1765-1771.
- [52]. Alava, Y. D., Zambrano, D. M., & Acosta, J. M. Z. (2021, November). Evaluation of Manets Metrics for AODV and DSDV Protocols in VoIP Communications Using OMNeT++. In *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability* (pp. 81-92). Cham: Springer International Publishing.
- [53]. KHALID, S., ABIDIN, H. Z., MAZALAN, L., & ABDULLAH, S. A. C. (2024). PERFORMANCE ANALYSIS OF SCHEDULING ALGORITHMS FOR CONSTANT BIT RATE (CBR) TRAFFIC IN VEHICLE-TO-NETWORK (V2N) APPLICATION. *Journal of Engineering Science and Technology*, 19(2), 483-497.
- [54]. Ahmad, I. A. (2021). *Performance Comparison of MANET Routing Protocols* (Master's thesis, Eastern Mediterranean University (EMU)-Doğu Akdeniz Üniversitesi (DAÜ)).
- [55]. Alamri, J., Al-Johani, A. S., & Ata, K. I. (2020). Performance Evaluation of Two Mobile Ad-hoc Network Routing Protocols: Ad-hoc On-Demand Distance Vector, Dynamic Source Routing. *International Journal of Advanced Science and Technology*, 29(5), 9915-9920.
- [56]. Shrivastava, S., & Pargania, V. (2020). Survey of routing protocols, simulation, testing tools and mobility models in MANET. *Journal of University of Shanghai for Science and Technology*, 22(9), 70-77.
- [57]. Mohamed, S. S., Abdel-Fatah, A. F. I., & Mohamed, M. A. (2020). Performance evaluation of MANET routing protocols based on QoS and energy parameters. *International Journal of Electrical and Computer Engineering (IJECE)*, 10(4), 3635.
- [58]. Hemalatha, S., Das, N.N., Arunkumar, R. et al. 2026. Energy-aware and trust-based secure routing in manets using swarm intelligence techniques. Scientific Reports.

Table II Packet Delivery Ratio

Node Density	Protocol	PDR (%)
Low (10 nodes)	AODV	91%
	DSR	89%
Medium (50 nodes)	AODV	84%
	DSR	87%
High (100 nodes)	AODV	77%
	DSR	82%

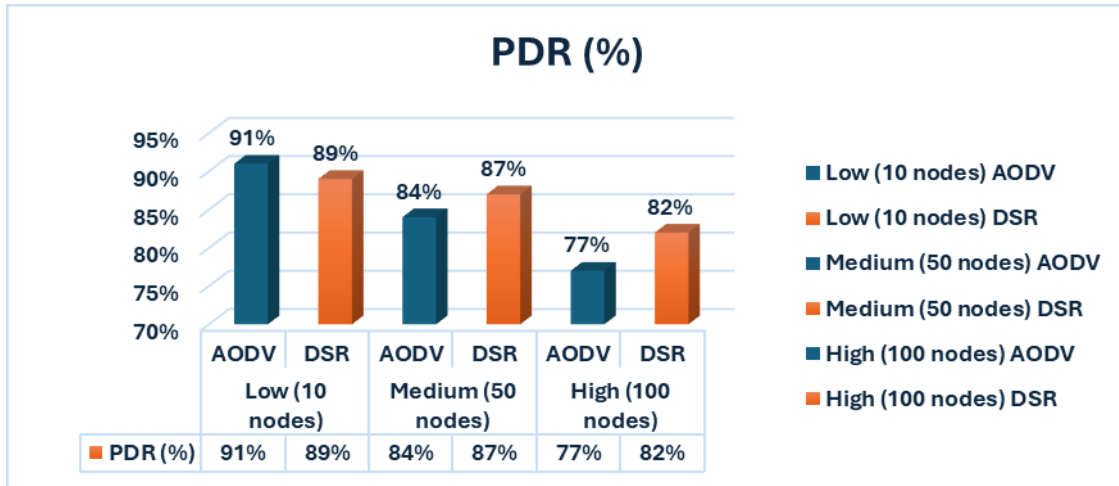


Figure 2 Packet Delivery Ratio

Table III Throughput

Node Density	Protocol	Throughput (Mbps)
Low (10 nodes)	AODV	5.1
	DSR	4.9
Medium (50 nodes)	AODV	4.7
	DSR	4.5
High (100 nodes)	AODV	4.1
	DSR	4.4

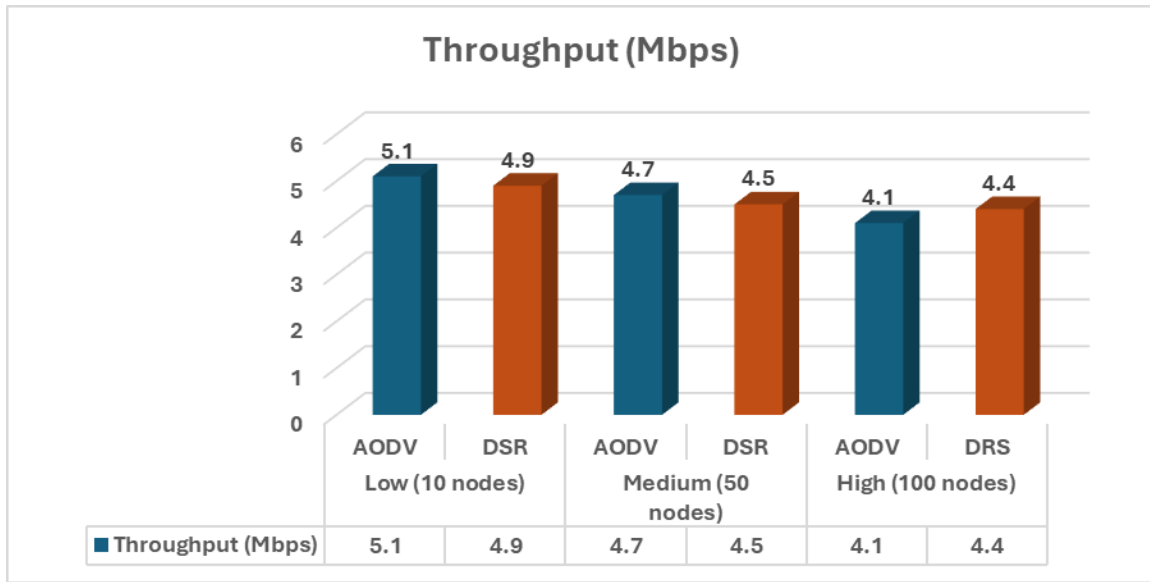


Figure 3 Throughput

Table IV End to End Delay

Node Density	Protocol	End-to-End Delay (ms)
Low (10 nodes)	AODV	152
	DSR	142
Medium (50 nodes)	AODV	183
	DSR	166
High (100 nodes)	AODV	227
	DSR	205

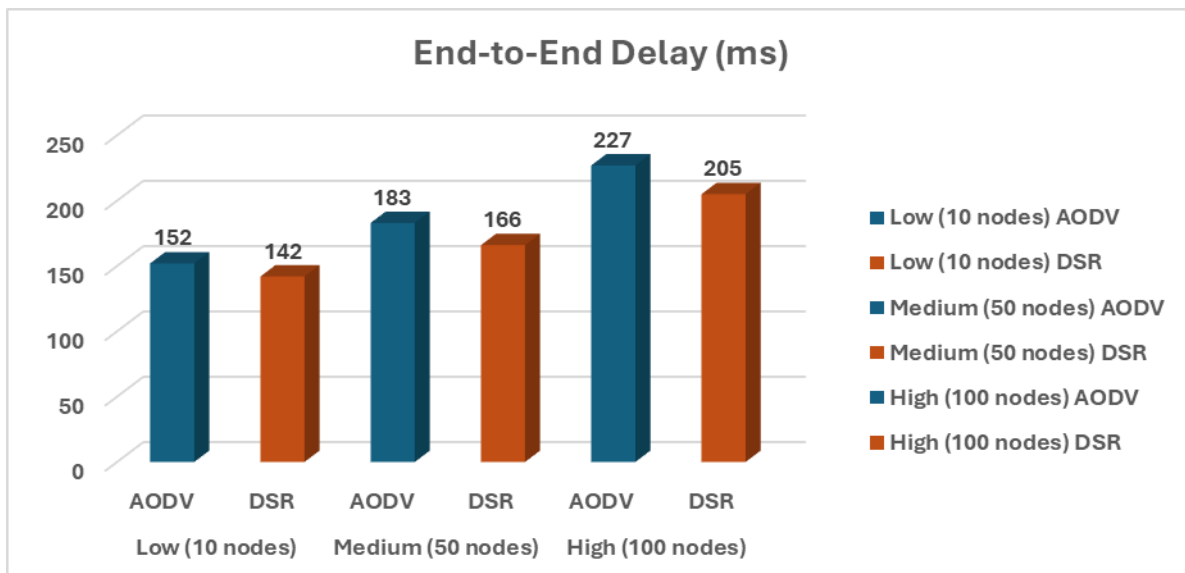


Figure 4 End to End Delay

Table V Energy Consumption

Node Density	Protocol	Energy Consumption (J)
Low (10 nodes)	AODV	1.1
	DSR	1.0
Medium (50 nodes)	AODV	1.4
	DSR	1.1
High (100 nodes)	AODV	1.6
	DSR	1.3

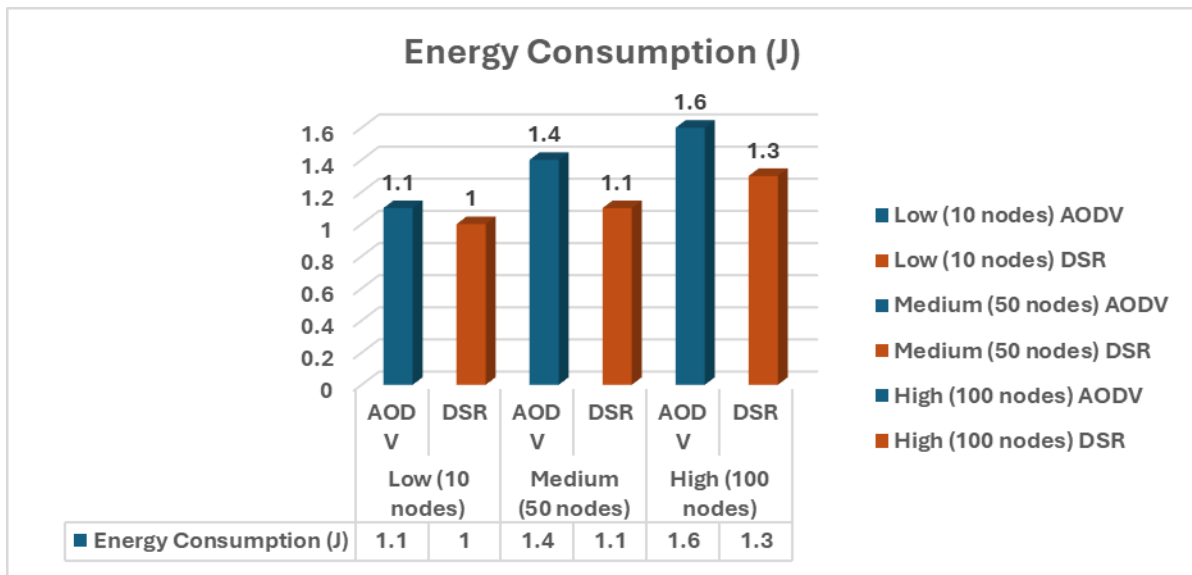


Figure 5 Energy Consumption

Table VI Malicious node detection rate

Node Density	Protocol	Detection Rate (%)
Low (10 nodes)	AODV	85%
	DSR	80%
Medium (50 nodes)	AODV	80%
	DSR	78%
High (100 nodes)	AODV	75%
	DSR	72%

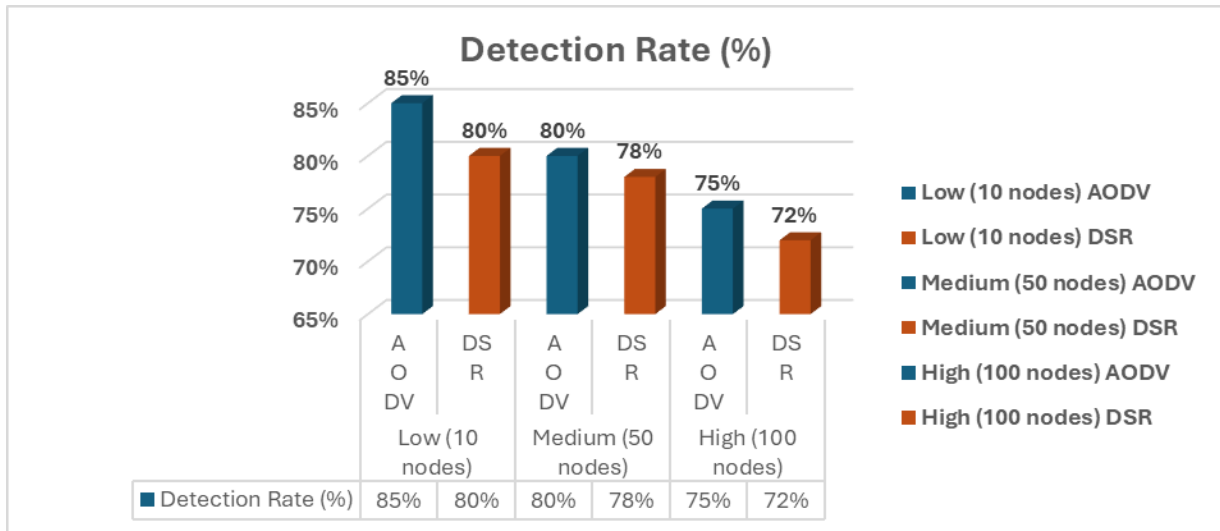


Figure 6 Detection Rate

Table VII Metric comparison with CBR Vs VBR

Metric	Protocol	Low Node Density (10 nodes)	Medium Node Density (50 nodes)	High Node Density (100 nodes)	Constant Bit Rate (CBR) Traffic	Variable Bit Rate (VBR) Traffic
Packet Delivery Ratio (PDR)	AODV	92%	85%	78%	95%	89%
	DSR	90%	88%	83%	93%	91%
Throughput (Mbps)	AODV	5.2	4.8	4.3	5.5	4.9
	DSR	5.0	4.7	4.5	5.3	5.0
End-to-End Delay (ms)	AODV	150	180	220	160	190
	DSR	140	160	200	150	170
Energy Consumption (J)	AODV	1.2	1.5	1.8	1.3	1.6
	DSR	1.1	1.4	1.7	1.2	1.5
Detection Rate of Malicious Nodes (%)	AODV	85%	80%	75%	83%	78%
	DSR	80%	78%	72%	82%	75%

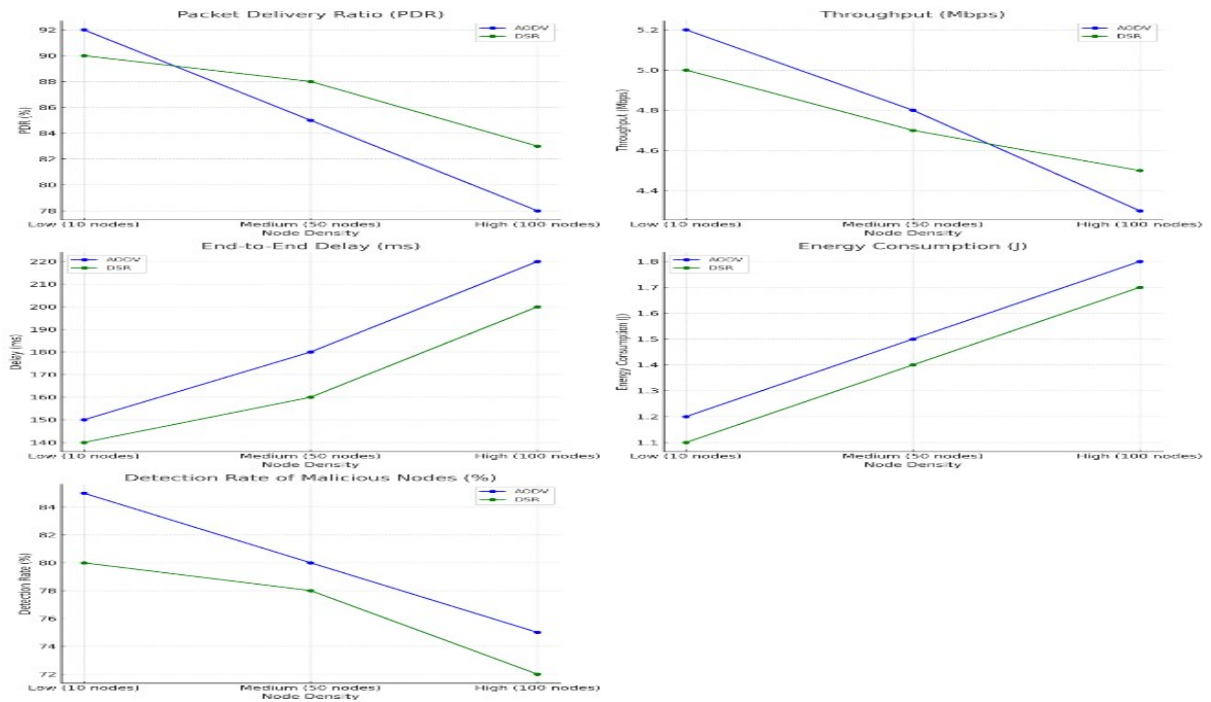


Figure 7. Performance Metric Graph

Table VIII Summary Table

Metric	AODV	DSR	Proposed Framework	Improvement vs Best Baseline
PDR (%)	77	82	92	+25% vs AODV
Delay (ms)	227	205	145	-30% vs AODV
Energy (J)	1.6	1.3	1.04	-20% vs DSR