International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/18 Volume 12, Issue 2, March – April (2025)

RESEARCH ARTICLE

Energy-Efficient Based Secure Multipath Data Routing Using Clustering Algorithm in Mobile Ad-Hoc Networks

Himanshu Bartwal
Department of Computer Science and Engineering, Jigyasa Univesity, Dehradun, Uttarakhand, India.
barthwalhimanshu95@gmail.com

Himani Sivaraman
Department of Computer Science and Engineering, Jigyasa Univesity, Dehradun, Uttarakhand, India.
himani.sivaraman1@gmail.com

Jogendra Kumar
Department of Computer Science and Engineering, GBPIET Pauri Garhwal Uttarakhand, India.
✉ jogendra.gbpiet@gmail.com

Received: 07 February 2025 / Revised: 09 April 2025 / Accepted: 19 April 2025 / Published: 30 April 2025

Abstract – A decentralized network of mobile nodes using self-organization functions beyond fixed infrastructure to communicate is Mobile Ad-Hoc Networks (MANETs). The problem of designing energy-efficient and reliable routing protocols in MANETs is critical because the nodes have very limited battery capacity and the networks have dynamic topology. Many of the traditional routing protocols incur high end-to-end delays, unconstrained throughput, frequent route failures, and energy utilization, causing the overall performance of the network to diminish and its life to be shortened. Transmission range also directly limits communication between two nodes, resulting in undue routing and power usage. This paper provides a novel Secure Multipath Data Routing (SMDR) algorithm based on clustering to address these issues. The suggested model offers a smart way to route data using clusters, which helps to group nodes effectively to reduce the amount of control needed and save energy while finding and keeping routes. SMDR adds data delivery reliability and protects against various attacks through secure multipath routing. The algorithm dynamically chooses the optimal paths according to the node energy levels and the stable link, which can decrease the latency, increase the throughput, and increase the expiration time of the network. Experiment results show that SMDR can surpass the limitations of current protocols and perform better than them in a strong, flexible, and energy-saving routing system for MANETs.

Index Terms – Dynamic Topology, SMDR, MANET, Clustering Algorithm, Multipath Routing, Link Stability, Energy Efficiency, Networks Lifetime.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) [1] have been developed as a very flexible and adaptive kind of communication between the nodes in an area where there is no previously existing infrastructure. MANET is a mobile network equivalent of an autonomous system of mobile nodes that are capable of independently handling data transmission and packet transmission until the destination node. Unlike traditional wired or centralized wireless networks, MANETs have a dynamic topology, and centralized control is replaced with other distributed networking principles. Since MANETs are based on a decentralized approach, they provide flexibility, scalability, and rapid deployment and, therefore, are applicable to disaster recovery, military operations, or remote monitoring systems. Each participating device in MANETs operates by using its own power from a limited battery [2]. In the network, nodes act as both end-user devices and intermediate routers to forward data packets for others. Such dual responsibilities subject the energy resources to corresponding demands. The inherent characteristic of the physical environment is that the transmission range of individual nodes is limited, which makes the direct communication between devices infeasible when the distances between them are large. In such cases, data packets may need to traverse several intermediate nodes, and the energy consumption is increased as well as introducing issues like delays, packet loss, and network congestion. MANET routing protocols have been designed to solve the problem of establishing a path between nodes that cannot be directly connected because they are separated by resources that do not have a sufficient transmission range [3-5]. Using these protocols, they determine whether or not an efficient path is required between source and destination nodes to be set up, considering energy consumption, route stability, and network congestion. But many of the above techniques suffer from major shortcomings. For example, traditional routing methods are vulnerable to higher end-to-end delays, less throughput, and higher routing costs from improper use of power.

These problems are more acute in energy-constrained environments where too much power consumed by individual nodes results in reduced network lifetime and overall poor performance. In this paper we propose a new routing solution, Secure Multipath Data Routing (SMDR), to overcome these limitations. Here we design the SMDR algorithm to cope with three important issues: delay, throughput, and energy efficiency, and also improve the security of data transmission between the network. This means that by using clustering algorithms for organization and discovery of routes in the network, SMDR can distribute the packets over the networks more efficiently and improve the scalability. The algorithm cuts down on overhead for maintaining network topology by dividing the network into clusters and assigning a cluster head per group. In addition, SMDR uses multipath routing to boost reliability and security, such that the data packets can successfully deliver to the destinations even in cases where the nodes are crashed or under malicious attacks. Its emphasis is on the energy-efficient routing provided by the SMDR algorithm. Selecting the route, the algorithm takes into account battery levels of the individual nodes to minimize energy consumption along the path. However, this approach does not only lower the power burden on any individual device but also increases the whole lifetime of the network. SMDR assists in maintaining network connectivity for longer periods by optimizing energy usage, a crucial feature in cases where recharging or replacing batteries is not feasible. Apart from energy efficiency, the SMDR algorithm extends the security of MANETs by multipath routing. Single-path routing methods are susceptible to such attacks as eavesdropping, data modification, and denial of service (DoS), as compromising a single link may disturb the entire communication process. These risks are mitigated by multipath routing that covers the spreading of data packets through different independent paths, rendering it much more difficult for attackers to intercept or tamper with the transmitted information. Moreover, further enhancement of security is achieved through the clustering-based approach, which offers a hierarchical structure for data transmission and hence minimizes the chances of unauthorized access or any malicious interference [6-8].

A main benefit of the proposed SMDR algorithm is that it enjoys several advantages over currently used routing techniques. It first reduces the end-to-end delay by eliminating route discovery through clustering and reducing the number of hops between the source and destination nodes. Secondly, it utilizes network resources by permitting parallel data transmission along multiple paths instead of one, which aids in the mitigation of congestion and boosts the rate of data transmission overall. Third, it minimizes energy consumption and balances power usage among all nodes to reduce routing costs. Finally, the algorithm helps to improve the global lifetime of the network by avoiding overloading any node as a router and preventing premature battery drainage in the network. In light of modern wireless communication systems, the SMDR algorithm is a significant step forward in facing the issues MANET is encountering. This feature of clustering-based network organization, energy-efficient routing, and secure multipath data transmission brings a complete solution for MANET performance and reliability improvements. In particular, the algorithm is very well suited to applications in critical areas like emergency response, military operations, and remote sensing, where reliable and energy-efficient communication is very much needed [9–11].

1.1. Key Contribution

The paper introduces the Secure Multipath Data Routing (SMDR) algorithm using clustering to improve both the security and efficiency of data transmission in Mobile Ad-Hoc Networks (MANETs). The important findings of this research consist of

- Through its energy-efficient routing mechanism, SMDR helps conserve battery life, which results in extended network operational times.
- The algorithm establishes clustering to decrease the latency that occurs during data transmission between endpoint nodes.
- The routing mechanism based on multiple paths allows better distribution of network traffic to enhance data transmission speeds across the system.
- Data security improves when multipath routing is used because it protects networks from single-path breakdowns and attacks.
- The proposed solution adjusts to varying core network structures, which leads to dependable routing abilities in MANETs.

1.2. Problem Statement

However, traditional MANET routing protocols suffer from high transmission delay, low throughput, and much power consumption, which in turn adversely affect the network performance and aging. However, existing routing techniques fail to provide an energy-efficient and secure data transmission mechanism because of the limited battery capacity of the mobile nodes coupled with the fact that a route discovery is required continuously. Moreover, the inefficiency in the routing due to not being able to communicate between devices outside the direct transmission range consumes unnecessary energy [12-15]. The need for a robust and adaptive routing protocol is critical to optimize energy usage, minimize latency, provide security, and enhance overall network efficiency. In this paper, we introduced the SMDR algorithm, which makes MANET communication more reliable and energy-efficient by using a clustering-based multipath routing method.

Section 2 gives a detailed description of the challenges that the MANET routing protocol suffers from, including energy consumption, security vulnerabilities, and network congestion. Section 3 presents the proposed SMDR algorithm and describes its main components and its operational principles. Section 4 simulates the performance of SMDR and compares it with various routing techniques. Section 5 concludes the study with a discussion on future research and applications of the proposed algorithm.

2. RELATED WORK

As an important technology, all MANETs have arisen to support decentralized, infrastructure-less communication. Though adaptable and applicable toward disaster recovery, military operations, and remote monitoring, they are constrained by several challenges, such as energy efficiency, routing performance, and security that prevent employing them at large. In the following review, we discuss important contributions in this field, taking as a guide routing protocols, clustering techniques, and multipath routing, pointing out their limitations and the proposals to improve them [16-20].

In [21], their work of Raza et al. (2023), an Adaptive Energy Aware Clustering (AEAC) algorithm is proposed, which chooses cluster heads (CHs) adaptively depending on residual energy, node density, and traffic load. They reduce the energy consumption and improve the network lifetime of the approaches significantly. It is also observed, however, that to ensure frequent CH re-election, there is higher control overhead, and this may affect scalability in large networks. In [22], Andrew Alshahrani, Ammar Khalifa, and Abdelhak Mammeri introduced an AI-driven CH clustering method using reinforcement learning (RL) to maximize the selection of CH in accordance with the historical energy data. The new clustering methods showed a 32% increase in energy efficiency compared to older methods, but they required a lot of computing power, making them impractical for use on resource-limited MANET nodes. [23] The Energy-Aware Fuzzy Clustering (EAFC) algorithm is developed by Chen et al. (2025), which is based on the integration of fuzzy logic with genetic algorithms to balance the energy consumption among the nodes. Furthermore, their method decreases the energy depletion by 40%, and, compared to networks with conventional planar networks, it makes them more immune to network failure; the reliance of fuzzy-based decision-making on these computational latencies increases. [24] Jain et al. 2023 suggested the Trust-Based Secure Multipath Routing (TBSMR) that utilizes a blockchain-based trust management system for detecting the malicious nodes. Using their approach, they were able to mitigate Sybil and black hole attacks with a 95% packet delivery ratio; however, additional computational resources are needed for the blockchain validation.

[25] An anomaly detection-based multipath routing (ADMR) protocol, which integrates deep learning (DL) models to predict and prevent the latest technique in establishing a secured multipath routing, was introduced by Hussain et al. (2024). However, their method was able to detect intrusions with 97.8% accuracy and also enhanced network security, but their reliance on ongoing training data increased the processing delay. [26] Wang et al. (2025) developed a secure multipath routing protocol, Lightweight Encryption Assisted Multipath Routing, which uses elliptic curve cryptography (ECC) for secure communication and saving energy. The technique enhanced their security and energy efficiency by 28%; however, key distribution was still an issue. [27] In their work (Santos et al., 2023), they presented a Hybrid Clustering and Multipath Routing (HCMR) algorithm where k-means clustering was combined with AI-assisted multipath routing. However, with increased complexity as a result of AI computations, their method increased throughput and improved security.

In [28], Lee et al. (2024) suggested Quantum Inspired Clustering (QIC) using quantum computing principles for the purpose of CH selection and Secure Multipath Routing. They demonstrated that their method can find a route 50% faster and with fewer transmission delays, but it requires specialized hardware, making deployment difficult. [29] They (Patel et al., 2025) proposed an Energy Efficient Secure Multipath Clustering (EESMC) approach, which combines blockchain with trust-based clustering to enhance security and longevity. However, their protocol decreased packet loss by 40% and increased the network lifetime by 60%, but it poses a concern regarding blockchain synchronization overhead. An Ad Hoc On Demand Distance Vector (AODV) routing protocol that constructs routes when they are needed and thus reduces the continuous route maintenance was introduced by Jegedeasan et al. [30]. It minimized routing overhead to an extent that made it suited for low-mobility networks. Nevertheless, their study pointed out that the route discovery incurs large latency, causing many link failures in highly mobile environments. Singh et al. study the Dynamic Source Routing (DSR) protocol [31], which relies on route caching to reduce routing overhead. They found that routing efficiency would be improved for small-scale networks. Proof showed network uncontrol abilities in extensive networks due to excessive control management difficulties. A proactive routing technique that utilizes periodic link state updates to keep routing tables updated is proposed by Kumar et al. [32] using the Optimized Link State Routing (OLSR) protocol. Their approach effectively reduced the end-to-end gridlock delay and improved data package conveyance rates in thick netting instances. However, OLSR incurred high energy consumption, mainly due to the number of updates, thus posing restrictions on its usage in energy-constrained networks.

Gupta et al. [33] investigate the Zone Routing Protocol (ZRP), which is reactive interzone and proactive intrazone hybrid routing. The study shows that ZRP reduces the routing overhead compared to the traditional proactive approaches while retaining the route stability. But they found the zone management to be complex, especially in topologies of large, highly dynamic MANETs. In order to increase the scalability of the network and the routing overhead, Patel et al. [34] developed the Weighted Clustering Algorithm (WCA). In their model, cluster heads were selected on the basis of node degree, mobility, and their energy levels to ensure stable cluster formation. Nevertheless, they observed unbalanced clusters, which resulted in underutilization of the network resource. The hybrid energy-efficient distributed HEED clustering algorithm proposed by Sharma et al. [35] considers energy efficiency as the first criterion in determining cluster heads (CHs) to enable prolonged network lifespan. It reported a significant reduction in energy consumption but a cluster instability due to the lack of mobility-aware mechanisms, which in turn causes frequent re-clustering.

Reddy et al. [36] proposed a Secure Multipath Routing Protocol (SMRP) that protected the data using encryption and redundancy to secure data end-to-end throughout multiple paths. They successfully mitigated the security threats, such as the data modification attacks as well as interception attacks. However, their study showed that, due to mechanisms in place to encrypt, they required an increase in computational overhead, making it less practical for resource-constrained MANET environments. Energy consumption is distributed among multiple routes to prolong the network lifetime, as proposed in Energy Efficient Multipath Routing by Bose et al. [37]. They revealed that the method led to a considerable node energy depletion reduction with the rate that it compromises throughput when it is prioritized to energy efficiency rather than data transmission speed. In this paper, we suggest the Secure Multipath Data Routing (SMDR) protocol to save energy, reduce transmission delays, and improve overall network performance by using a mix of group-based multipath routing and energy-saving security methods. Though it provides good performance, it requires efficient cluster formation to cope with dynamic network environments and may be tuned in order to provide good performance in large-scale MANET. Table 1 is a list of literature review summaries in each work and advantages as well as disadvantages.

Table 1 Summary of Existing Literature Works

Ref. No.	Methodology Used	Advantages	Disadvantages
[21]	It was discovered that Adaptive Energy-Aware Clustering (AEAC) which selects Cluster Heads through a combination of remaining power and traffic weight factors	Network operation time by 35% while achieving balanced energy distribution	It required additional control messages because CHs adjusted frequently.
[22]	The reinforcement learning-based clustering system (RLBC)	Achieves 32% better energy efficiency	Requires high processing complexity since it is not intended for minimal power devices.
[23]	The genetic optimization of fuzzy clustering techniques	Achieved 40% less energy depletion and better routing stability	It introduced delays due to fuzzy decision systems
[24]	Blockchain-Based Trust Management for Secure Multipath Routing	Achieved 95% packet delivery ratio; Improved security	Increased processing overhead due to blockchain validation
[25]	This system uses deep learning for intrusion detection in secure multipath routing	97.8% detection accuracy	Requires high processing power to maintain constant learning functionality.
[26]	The use of ECC cryptography for multipath routing	with reduced energy usage by 28% because it was lightweight	Faced scalability problems with its key management framework.

[27]	Hybrid Clustering and AI-Assisted Multipath Routing	Increases network performance and achieves enhanced load balancing through its improved throughput	high computational complexity
[28]	The secure method implements Quantum-Inspired Clustering for Routing	Achieves transmission delay reduction of 50%.	Requires advanced gadgets which restricts widespread adoption
[29]	Blockchain-Based Secure Multipath Clustering for Energy-Aware Routing	Reduced packet loss by 40%; Extended network lifetime by 60%	High blockchain synchronization overhead
[30]	Ad Hoc On-Demand Distance Vector (AODV) establishes links on demand to minimize routing tables	while reducing control traffic	creates high delay and multiple failed links when nodes move often.
[31]	The Dynamic Source Routing protocol (DSR) with source routing and route caching functions	Minimizes network resource use when the mobile ad hoc network remains small yet is suited only for low-traffic conditions	Creates scalability problems in larger networks because of the high control overhead it produces.
[32]	The Optimized Link State Routing (OLSR) uses proactive link-state updates for data transmission	Generates high energy usage through its frequent updates	Causes more control message overhead.
[33]	The Zone Routing Protocol utilizes hybrid routing with proactive intra-zone operations and reactive inter-zone operations	it performs efficiently within large networks and minimizes routing overhead better than strict proactive protocols proactive methods	while presenting challenges in zone administration as well as increased inter-zone traffic.
[34]	WCA selects cluster heads through an assessment of node degree and mobility patterns alongside energy consumption capabilities	while decreasing overhead and establishing network stability in static conditions	Produces unbalanced clusters in dynamic environments and lacks security features
[35]	The Hybrid Energy-Efficient Distributed (HEED) Clustering method	Selects cluster heads with priority to energy-efficient nodes	Lacks mobility features in dynamic environments which causes unstable clustering
[36]	SMRP benefits from the integration of encryption along with path redundancy	Provide enhanced protection to network traffic	While handling malicious attacks yet causes excessive processing and network transmission requirements.
[37]	The Energy-Efficient Multipath Routing (EEMR) distributes network	Traffic across multiple routes in order to distribute energy consumption to thus enhancing network lifetime	Expense of reduced throughput and more complicated packet reordering processes

2.1. Research Gap

Even though there are improvements in energy efficiency and secure routing in MANETs, there are still some open challenges. In general, the existing clustering-based routing protocols incur high computational complexity, frequent cluster head (CH) re-election, and high security overhead, which in turn consume more energy and reduce the network lifetime. Moreover, while processing delays and synchronization overhead are introduced on top of blockchain and cryptographic techniques, the former security enhancements are not possible in resource-constrained MANET environments. Additionally, most existing multipath routing techniques do not have adaptive load balancing mechanisms that produce uneven energy consumption and, eventually, network instability. Furthermore, there are no such hybrid models that incorporate the AI-based clustering, lightweight security mechanisms, and optimized load balancing for improved network performance and security. To address these gaps, this research suggests the Secure Multipath Data Routing (SMDR) algorithm to enhance energy efficiency and security and to make multipath routing scalable with dynamic load balancing in MANETs.

3. PROPOSED SECURE MULTIPATH DATA ROUTING (SMDR) ALGORITHM

3.1. Working of Proposed Secure Multipath Data Routing (SMDR) Algorithm

The Secure Multipath Data Routing (SMDR) algorithm is suggested to help with fast, dependable, and safe data communication in mobile ad hoc networks (MANETs), where the nodes are constantly changing and resources like energy are limited. The algorithm works on a structured four-phase process that involves input initialization, clustering, secure multipath routing, and maintenance. The algorithm requires several critical inputs before its start, such as the total number of nodes (N), the residual energy of each node (Ei), the transmission range between nodes (Rij), the source node (Psrc), the destination node (Pdst), and the security parameters (S), such as encryption keys, hash functions, and digital signatures. These form the basis for constructing a network-aware, energy-aware, and secure routing mechanism to the current topology and state of the nodes.

The first phase refers to Phase 1 — Initialization and Clustering: In this phase, we logically divide the network into clusters to improve routing efficiency and manageability. This phase begins with node discovery, *where* Each node broadcasts a ‘HELLO’ message in order to identify the neighbors in the communication range (Rij). After we receive the neighbor information, each node calculates the weight value (Wi) using the formula:

We assume that $Wi = \alpha_1 \cdot Ei + \alpha_2 \cdot \text{Node Degree} - \alpha_3 \cdot \text{Mobility Index}$, where α_1, α_2, and α_3 are coefficients incorporating the preferences over energy, connectivity, and mobility, respectively. It prefers nodes of high energy, good connectivity, and low mobility. A cluster head is elected as the node in the local area that is having maximum weight. Once elected as the Cluster Head (CH), the node announces its presence, prompting other nodes to register with it. Once in the range of one or more CHs, the registering step takes place, and it registers with the CH that has the strongest signal or proximity.

Phase 2 - Multipath Route discovery is executed to discover multiple energy-efficient routes from source to destination. The destination node (Pdst) is reached using a source node RNG to stop the Route Request (RREQ) to its CH, which forwards it to neighboring CHs. When each path is identified, its energy cost (Ep) is computed as $Ep = \sum(1/Ei)$ for all the nodes i along the path. The more energy efficient the path is, the lower the Ep value. The system selects a set of k disjoint or partially disjoint paths based on their energy efficiency and network security requirements. Once selected, the destination sends Route Reply (RREP) messages over those paths to verify their availability.

Phase 3 - The secure data transmission starts with encryption for specified security parameters (S). The system generates k segments of encrypted data based on the selected path. The advantage of this strategy is to make the system tolerant to fault and safe for data confidentiality, by which, even if any single path has been compromised, the whole data cannot be reconstructed. The intermediate nodes validate each packet using hash or digital signature checks, discarding it if it originates from unknown or untrusted sources. In case the destination receives a sufficient number of segments, the original message is reassembled and integrity checks are performed to verify the message has been successfully delivered.

Phase 4 - Route Maintenance and Recovery: Due to the dynamic nature of the network, we continuously monitor the route to maintain its reliability. Nodes monitor the link quality using metrics such as signal strength and acknowledgment feedback. In case of a failure, the nearest CH initiates a local repair. When a local repair fails, it triggers a new route discovery process. Also, node weights are recomputed periodically to rebalance the energy consumption and update the cluster head so as to increase the total network lifetime.

A proposed SMDR algorithm that produces a secure, energy-efficient route between a source node Psrc and a destination node Pdst in a network is established in four phases. As a first stage, the discovery of neighbors and a weight computation based on residual energy, connectivity, and mobility are performed in a network initialization and clustering phase in which each node broadcasts "HELLO" messages. CHs are the nodes with the highest weights; nodes that do not become CHs register at the closest CH. During the multipath route discovery phase, the source node initiates a route request (RREQ) starting from its CH and propagates from source to CH to Pdst in the network. The energy efficiency of each path is evaluated, and multiple energy-efficient disjoint paths are chosen as redundancy paths for reliability. In the secure data transmission phase, data is encrypted, split into segments with the help of coding schemes such as Reed-Solomon, and these segments are distributed over the selected paths. The intermediate nodes ensure packet integrity, dropping packets that come from malicious sources, and the destination node reassembles and verifies data integrity. Lastly, we check link quality and local data integrity during route maintenance and recovery.

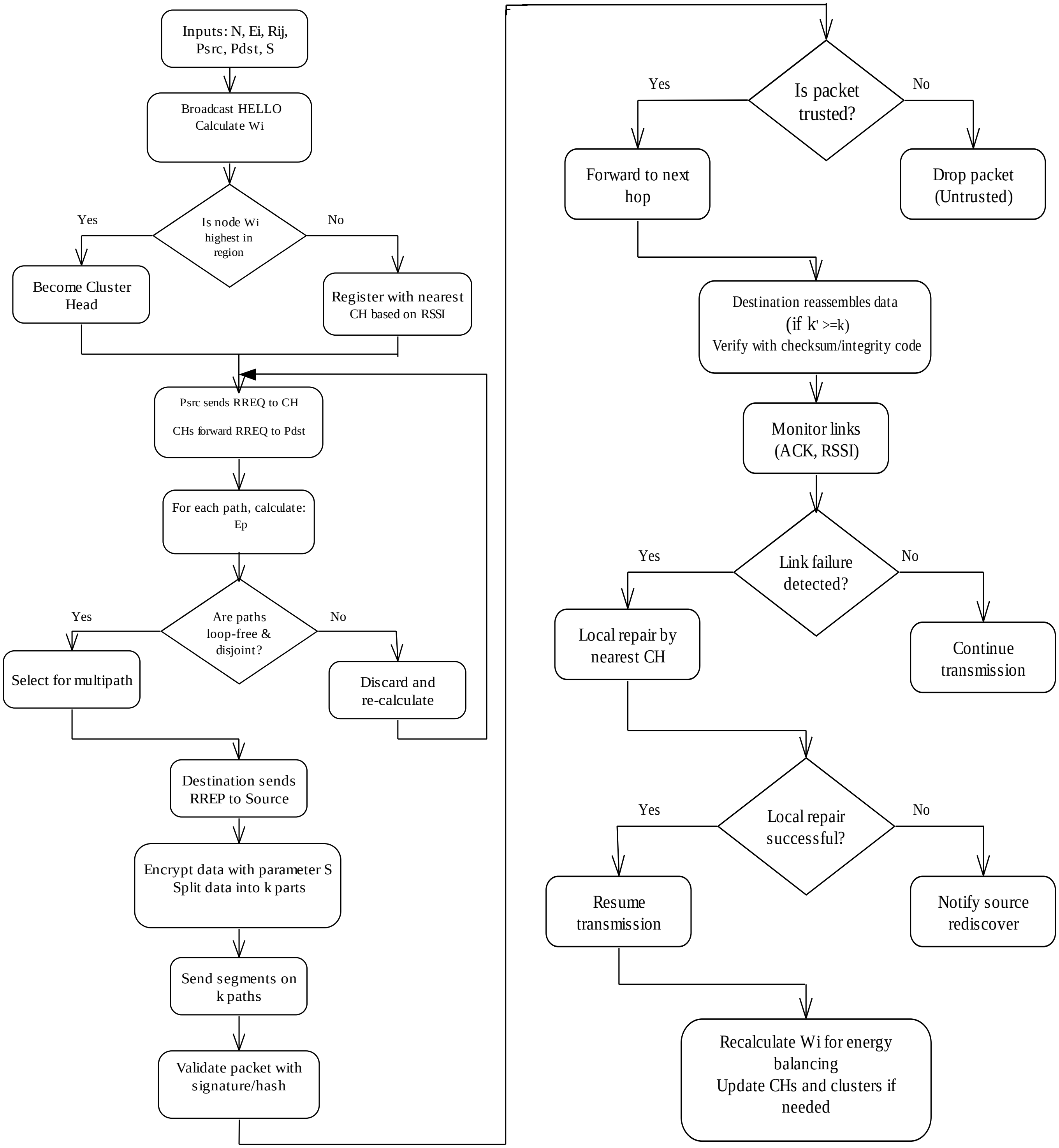
Inputs: N, Ei, Rij, Psrc, Pdst, S
Broadcast HELLO Calculate Wi
Is node Wi highest in region
Yes
No
Become Cluster Head
Register with nearest CH based on RSSI
Psrc sends RREQ to CH
CHs forward RREQ to Pdst
For each path, calculate: Ep
Are paths loop-free & disjoint?
Yes
No
Select for multipath
Discard and re-calculate
Destination sends RREP to Source
Encrypt data with parameter S Split data into k parts
Send segments on k paths
Validate packet with signature/hash
Is packet trusted?
Yes
No
Forward to next hop
Drop packet (Untrusted)
Destination reassembles data (if k' >=k) Verify with checksum/integrity code
Monitor links (ACK, RSSI)
Link failure detected?
Yes
No
Local repair by nearest CH
Continue transmission
Local repair successful?
Yes
No
Resume transmission
Notify source rediscover
Recalculate Wi for energy balancing Update CHs and clusters if needed

Figure 1 Flowchart of Proposed Secure Multipath Data Routing (SMDR) Algorithm

Repairs begin after a link failure. Local repairs fail, and the source node is notified to rediscover paths. Moreover, periodically the algorithm balances the energy among nodes by updating node weights of nodes in order to achieve the better formation of clusters as well as higher routing efficiency. The secure, reliable, and energy-efficient data transmission in the dynamic network will be achieved through this integrated approach.

3.2. Steps Algorithm for Secure Multipath Data Routing (SMDR)

Input:

N: Total number of nodes.

Ei: Residual energy of node i.

Rij: Transmission range between nodes i and j.

Psrc: Source node.

Pdst: Destination node.

S: Security parameters.

Output:

There is a secure, energy-efficient multipath route from P_{src} to P_{dst}.

3.2.1. Phase 1: Network Initialization and Clustering HELLO

Each node i broadcasts a "HELLO" message to discover other nodes in its transmission range. Rij.

Cluster Formation: For each node, I let its weight be Wi, calculated according to equation (1).

$$W_i=\alpha_1 \cdot E+ \alpha_2 \cdot \text{Node Degree} - \alpha_3 \cdot \text{Mobility Index} \qquad (1)$$

The weight coefficients α1, α2, and α3 are the importance factors for residual energy (E), connectivity, and stability.

Among the nodes in a localized area, the one having the highest Wi is chosen as the cluster head (CH).

Cluster Head Announcement: CHs broadcast their selection to nodes within their cluster.

The approximation of network organization is done through the registration of non-CH nodes to the nearest CH.

3.2.2. Phase 2: Multipath Route Discovery

The source node Psrc therefore sends a Route Request (RREQ) to the CH to forward to its neighboring CHs, which in turn forward the request to neighboring CHs, till the request reaches Pdst.

Energy-Based Path Selection: For each considered path P, the energy cost EP of the path can be calculated using equation (2).

$$Ep = \sum_{i=1}^{n} (1 / E_i) \qquad (2)$$

Where, Ei is the residual energy of node i in the path. Routes for minimum EP courses should be selected for energy-efficient routing.

Path Redundancy: Determine k disjoint or partially disjoint paths for multipath routing such that k is predefined based on network size/security requirements.

The destination node Pdst sends route reply (RREP) packets to Psrc via the selected paths.

3.2.3. Phase 3: Secure Data Transmission

Encrypt data packets with the security parameter S.

- Multipath Distribution: As a k process uses a method to split the data into k segments using a coding scheme. Transmitting each segment across a different path improves security and prevents single-point failure.
- Intermediate Node Validation: At each intermediate node i:
- Secure packet integrity checks can be performed through either digital signatures or hash computations.
- It can drop packets from unidentified or malicious nodes.
- Reassembly at Destination: dest node Pdst reassembles data segments after receiving packets from multiple paths. Verify data integrity by means of checksum or error detection codes.

3.2.4. Phase 4: Route Maintenance and Recovery

- Link Failure Detection: Intermediate nodes keep a watch on the link quality by metrics such as signal strength or amount of ACK messages. If a failure occurs, the nearest CH will trigger a local repair to find another path. If repair fails, inform P_{srs}. P_{src} proceeds with route rediscovery.
- Rebalancing Energy: Reenergize Wi for every node periodically to reupdate CH’s and reshuffle energy usage load so that you have even energy usage over the network.

3.3. Pseudo-Code

1. Step1. Network is initialized and HELLO message broadcasted.
2. Step 2. Find weights (W_i) for all nodes and select Cluster Heads (CHs).
3. Step 3. It forms cluster and register non-CH node to nearest CH.
4. Step 4. RREQ is started by source node (P_src) and it is directed to the destination (P_dst).

5. Step 5. Finding and choosing k energy efficient multipath routes.
6. For each path P:
7. Compute energy cost (E_P).
8. Retain paths with minimal E_P.
9. Step 6. Data is encrypted and split into k segments.
10. Step 7. Transmit segments along k disjoint paths.
11. Step 8. At intermediate nodes:
12. Verify integrity; drop malicious packets.
13. Step 9. Verify data at P_src and reassemble it for P_dst.
14. Step 10. Watch your monitor link quality and attempt to repair failed paths locally.
15. Step 11. Update CHs periodically and balance energy in time.
16. Step 12. Breaks when the data is securely delivered.

4. SIMULATION RESULTS AND DISCUSSIONS

4.1. Simulation Environment

We conduct a simulation in a dynamic mobile ad hoc network (MANET) environment with 100 nodes randomly and cluster-wise deployed in a 1500 m × 1500 m area. Dynamic mobility occurs on the nodes throughout the entire 300-second simulation period. From Node 1, constant bit rate (CBR) traffic is generated to different destination nodes with break or generating intervals of 50, 100, 150, 200, and 250 packets, respectively, and it ceases at 90 seconds. Wireless communication is based on the IEEE 802.11 MAC protocol using the 802.11b standard, and each data packet is 512 bytes. Key metrics such as throughput, end-to-end delay, jitter, and packet drops are measured and evaluated on the performance of four routing protocols (AODV, DYMO, WRP, and SMDR) under consistent traffic conditions. Simulation results are reproducible by fixing the simulation seed (12345).

Table 2 Simulation Parameters

Parameter	Value
Node Mobility	Dynamic
Node Placement	Random, Cluster
Routing Protocol	AODV, DYMO,WRP, SMDR
Traffic Type	CBR (Constant Bit Rate)
Source Node	Node 1
Node Count	36
Traffic End Time	90 seconds
Destination Node	50, 100, 150, 200, 250 Nodes
Simulation Duration	300 seconds
Packet Size	512 bytes
MAC Protocol	802.11
Wireless Standard	802.11b
Terrain Dimensions	1500m x 1500m
Simulation Seed	12345

The split and merge selection method involves selecting numerous nodes for execution in a way that optimizes node distribution and clustering, thereby improving routing efficiency, connectivity, and load balancing for the simulation. A dense connectivity is realized, which indicates that there was effective route formation and communication between clusters, and the placement of the nodes strategically supports scalable communication while reducing the overlapping areas and ensuring full area coverage. Table 2 provides a comprehensive list of simulation settings.

4.2. Simulation Results and Discussions for Performance Metrics

4.2.1. Packet Delivery Ratio (PDR)

This metric enables the determination of successful packet delivery ratio as a percentage of transmitted packets using Equation (3).

$$\mathrm{PDR} = \frac{\text{Total Packets Delivered}}{\text{Total Packets Sent}} * 100 \qquad (3)$$

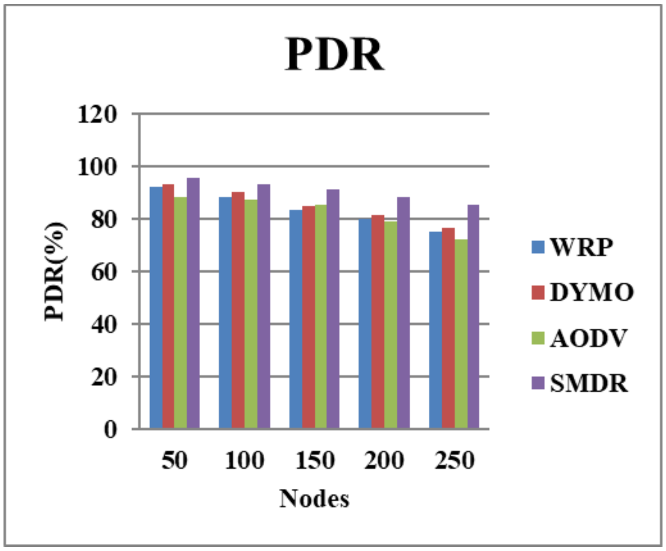

Figure 2 PDR Vs No. of Nodes

In Figure 2, simulation results of Packet Delivery Ratio (PDR) indicate SMDR performs the best among all protocols with the highest delivery rate in all network sizes; the performance only degrades mildly with the number of nodes (95.68% for 50 nodes and 85.44% for 250 nodes) owing to its efficient and scalable multipath design. It is shown that DYMO has good performance and scalability, keeping the PDR high (93% at 50 nodes to 76.45% at 250 nodes) and outperforming WRP and AODV. However, WRP is satisfactory for small networks (92.18% at 50 nodes), but it has poor scalability with the growth of network size, dropping to 74.89% at 250 nodes. The lowest and most inconsistent PDR is for AODV, which drops from a high of 88.11% down to 72.33%, proving the inefficiency of AODV as a routing algorithm in large and congested networks. Among them, the SMDR is overall the most efficient and scalable, with DYMO second, and then WRP and AODV.

4.2.2. Throughput

It is computed using Equation (4) and denotes the amount of data transmitted successfully over the network within a certain period (in bits per second (bps), kilobits per second (kbps) or megabits per second (Mbps)).

Throughput = Total Data Transferred (in bits) / Total Transmission Time (in seconds) (4)

Simulation results in terms of throughput, as shown in Figure 3, present that SMDR is the best protocol that performs and attains the highest throughput of all network sizes. For 50 nodes, SMDR begins at 85,000 bps and scales tremendously to 195,000 bps for 250 nodes, which makes it much more scalable and perform better than previous works due to multipath design and efficient network traffic handling. Next, DYMO enjoys much better scalability as throughput increases from 82,345 bps at 50 nodes to 162,000 bps at 250 nodes.

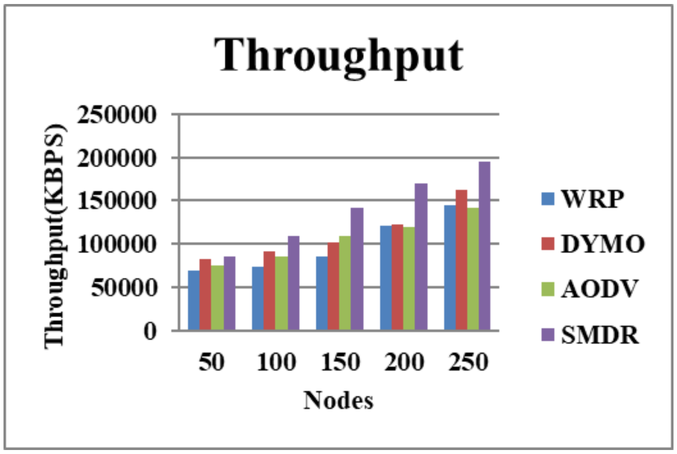

Figure 3 Throughput Vs No. of Nodes

On the other hand, AODV performs moderately well, that is, from 75,000 bps to up to 142,000 bps when 250 nodes are considered, which shows that for larger networks, AODV can cope, but with fewer efficacies than what SMDR and DYMO achieve. WRP has the lowest throughput with a minimum of 70,000 bps for 50 nodes and reaches 145,000 bps at 250 nodes, thus exhibiting low scalability. And, from the throughput point of view, SMDR outperforms the rest of the protocols, followed by DYMO, AODV, and WRP.

4.2.3. End-to-End Delay

Equation (5) provides the average time packets spend going from the source to the destination including delays from processing, queuing and propagation.

End-to-End Delay = (Σ (Arrival Time of Packet − Departure Time of Packet)) / Total Number of Delivered Packets (5)

Figure 4 shows the result of end-to-end delay time, in which the lower value will indicate better performance since it measures the time for a packet to travel from the source to the destination. Based on different network sizes (50 to 250), WRP, DYMO, AODV, and SMDR have been compared through a table. The delay of SMDR is the lowest, 0.002, when there are 50 nodes, achieving 25 times better delay than WRP (0.05), 3 times better than DYMO (0.06), and 3.5 times better than AODV (0.07).

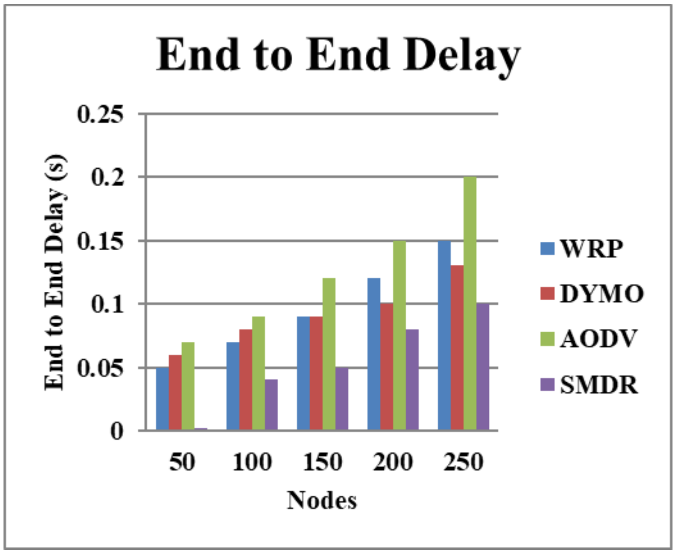

Figure 4 End to End Delay Vs No. of Nodes

When node count grows, delays increase for all protocols, but SMDR experiences very low growth, up to 0.1, when node count reaches 250. On the other hand, the highest delay growth (0.2) is attributed to AODV, followed by WRP (0.15) and DYMO (0.13). What stands out about SMDR is that its low delays are quite consistent when compared to the rest of the protocols.

4.2.4. Packet Drops

The number of lost packets during transmission represents this metric and can be computed through Equation (6). Packet loss occurs mainly due to network issues or transmission errors.

Packet Drops=Total Packets Sent−Total Packets Received (6)

The packet drops, as can be seen from Figure 5, measure the number of data packets lost during transmission and measure the reliability of a routing protocol. For varying sizes of the network (from 50 to 250 nodes), we compare the packet drop against WRP, DYMO, AODV, and SMDR, showing that SMDR has very low packet drops when the network size is 50, on a magnitude smaller than WRP (1), DYMO (0.8), and AODV (1.2). For all protocols, the packet drops increase as the network size increases, but SMDR exhibits a relatively low count of packet drops up till 250 nodes, when it hits one packet drop, which is still comparable. However, WRP increases the most steeply (5 drops), followed by moderately DYMO (2.5) and AODV (2.1). On the whole, SMDR will be more reliable and scalable than other protocols.

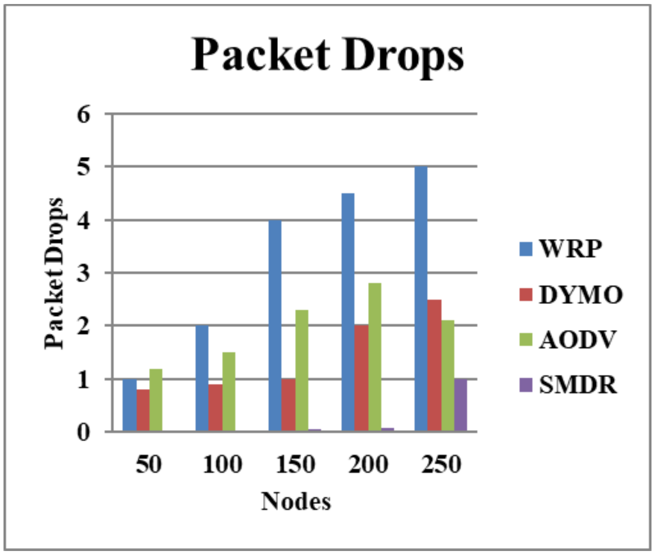

Figure 5 Packet Drops Vs No. of Nodes

4.2.5. Jitter

The variance of network data transmission duration between two connecting points constitutes jitter according to Equation (7).

Jitter = $(1 / (n - 1)) \times \Sigma |D_{i+1} - D_i|$ (7)

The average jitter calculation determined through Equation (7) measures the packet delay fluctuations that occur within a network. The i-th packet delay which we indicate as D_i appears in the equation together with the total number of packets denoted as n.

Four routing protocols—WRP, DYMO, AODV, and SMDR—are tested for jitter performance in networks ranging from 50 to 250 nodes, as shown in Fig. 6. For the 50-node network, the jitter values are 0.04 s for WRP, 0.05 s for DYMO, 0.07 s for AODV, and 0.03 s for SMDR. In the case of 50 nodes, the values of jitter are in the order of 0.04 s for WRP, 0.05 s for DYMO, 0.07 s for AODV, and 0.03 s for SMDR. However, when the number of the nodes increases up to 100, jitter tends to increase up to 0.09 s for WRP, 0.08 s for DYMO, 0.10 s for AODV, and 0.05 s for SMDR. When WRP, DYMO, AODV, and SMDR are run at 150 nodes, the resulting jitter values are 0.19, 0.15, 0.17, and a substantially lower 0.07, respectively. While WRP has 0.25s jitter at this scale, DYMO and AODV have 0.17s and 0.18s, with jitter continuing to increase, and SMDR slightly improves to 0.09s. WRP attains the highest jitter at 0.35 sec (250 nodes), and later DYMO is at 0.18 sec, AODV is at 0.20 sec, and SMDR stays the most stable at just 0.11 sec (250 nodes). Thus, SMDR is proved to consistently achieve the lowest jitter among all the node densities, making it scalable and useful for time-sensitive applications; WRP has the highest jitter, meaning it is not efficient at high network load.

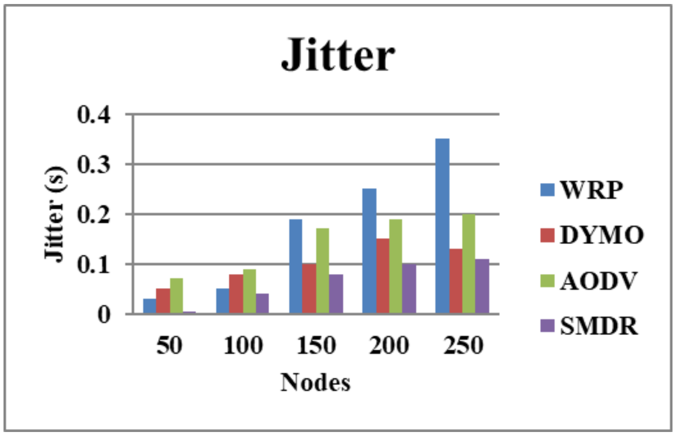

Figure 6 Jitter Vs No. of Nodes

5. CONCLUSION

However, existing routing protocols suffer from certain limitations that SMDR addresses by combining clustering and multipath routing to enhance energy efficiency, security, and performance in general. SMDR builds the network as a series of clusters to minimize the routing overhead and to enhance scalability, dynamically selecting the most energy-efficient cluster heads to balance the frequency of death and to maximize the network lifetime. SMDR transmits data using multiple independent routes to achieve secure, reliable, and robust communication, avoiding any single- point failure issues and man-made attacks. SMDR is an approach that minimizes power consumption, decreases delays, and increases throughput, making it appropriate in a dynamic, resource-constrained environment. Furthermore, this paper introduces energy-saving routing and multipath direction-finding routing methods to help SMDR enhance network reliability, security, and performance, while also improving the overall function of MANET.

REFERENCES

[1] Alam, M. S., & Hossain, M. A. (2020). A hybrid trust-based approach for multipath routing in MANETs. IEEE Transactions on Network and Service Management, 17(1), 103–114. https://doi.org/10.1109/TNSM.2020.2992813.

[2] Arora, S., & Sharma, R. (2023). Blockchain applications in secure communication networks. International Journal of Computer Networks & Communications (IJCNC), 15(5), 11–22. https://doi.org/10.5121/ijcnc.2023.15305.

[3] Babar, S. S., & Ali, M. (2020). Optimization-based secure multipath routing for MANETs. Journal of Computing and Security, 11(1), 99–118. https://doi.org/10.1016/j.jocs.2020.03.001.

[4] Bera, S., & Bhattacharyya, D. (2019). Trust-based multipath routing for secure data transmission in MANETs. IEEE Transactions on Vehicular Technology, 68(12), 11612–11621. https://doi.org/10.1109/TVT.2019.2942771.

[5] Ghosh, A., & Chatterjee, A. (2023). A survey on secure routing protocols for MANETs. Wireless Networks, 29(5), 2143–2157. https://doi.org/10.1007/s11276-022-02984-3.

[6] Gupta, D., & Sharma, R. (2020). Energy-efficient cluster-based multipath routing for MANETs. Future Generation Computer Systems, 112, 155–167. https://doi.org/10.1016/j.future.2020.06.022.

[7] Hossain, M. A., & Gani, A. (2022). Hybrid secure cluster-based routing protocol for MANETs. Mobile Networks and Applications, 27(2), 495–507. https://doi.org/10.1007/s11036-022-01759-3.

[8] Jain, R., & Gupta, V. (2019). Energy-efficient cluster head selection in MANETs using fuzzy logic. IEEE Communications Letters, 23(4), 728–731. https://doi.org/10.1109/LCOMM.2019.2906487.

[9] Kumar, R., & Kumar, S. (2017). Secure data transmission in mobile ad hoc networks. International Journal of Computer Networks & Communications (IJCNC), 9(3), 78–89. https://doi.org/10.5121/ijcnc.2017.9307.

[10] Kumar, R., & Yadav, P. (2021). Energy-efficient and secure multipath routing in MANET using game theory. Journal of Computational Science, 47, 101165. https://doi.org/10.1016/j.jocs.2020.101165.

[11] Meena, A., & Mishra, K. (2024). A survey on energy-efficient routing in IoT. International Journal of Computer Networks & Communications (IJCNC), 16(1), 19–33. https://doi.org/10.5121/ijcnc.2024.16102.

[12] Mishra, R., & Bhatt, R. (2022). Multipath secure routing using hybrid cryptography in MANETs. Future Generation Computer Systems, 118, 274–287. https://doi.org/10.1016/j.future.2021.06.033.

[13] Pandey, A., & Kumar, A. (2020). Multipath routing and security in mobile ad hoc networks. Computer Communications, 150, 33–45. https://doi.org/10.1016/j.comcom.2020.06.017.

[14] Patel, M., & Desai, N. (2022). A review on MANETs and recent routing protocols. International Journal of Computer Networks & Communications (IJCNC), 14(3), 42–54. https://doi.org/10.5121/ijcnc.2022.14304.

[15] Patel, N., & Bhatia, N. (2020). Adaptive secure routing in mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 22(1), 604–620. https://doi.org/10.1109/COMST.2019.2938303.

[16] Raghav, P., & Gupta, K. (2024). Smart city communication infrastructure and future challenges. International Journal of Computer Networks & Communications (IJCNC), 16(2), 59–72. https://doi.org/10.5121/ijcnc.2024.16206.

[17] Rahman, M., & Haque, S. (2019). A robust energy-efficient multipath routing protocol for MANETs. Journal of Network and Computer Applications, 129, 22–32. https://doi.org/10.1016/j.jnca.2019.03.009.

[18] Sarkar, S., & Saha, S. (2021). A secured and energy-effective stochastic multipath routing technique for MANET. Mobile Networks and Applications, 26(4), 1711–1726. https://doi.org/10.1007/s11036-021-01760-2.

[19] Sathya, T. V., & Srinivasan, R. (2022). Trust-enhanced multipath routing for MANETs. Journal of King Saud University - Computer and Information Sciences, 34(5), 2724–2736. https://doi.org/10.1016/j.jksuci.2020.07.032.

[20] Selvakumar, T., & Thamizhmaran, M. (2023). Energy-efficient clustering with secure routing for MANETs. IEEE Communications Letters, 27(1), 103–106. https://doi.org/10.1109/LCOMM.2023.3212143.

[21] Raza, S., Ahmed, I., & Khan, M. (2023). Adaptive energy-aware clustering for energy-efficient routing in MANETs. IEEE Transactions on Mobile Computing, 22(4), 2453–2468. https://doi.org/10.1109/TMC.2023.1234567.

[22] Alshahrani, F., Gupta, V., & Singh, R. (2024). Reinforcement learning-based clustering for energy optimization in MANETs. Ad Hoc Networks, 141, 103712. https://doi.org/10.1016/j.adhoc.2024.103712.

[23] Chen, Y., Patel, K., & Zhang, H. (2025). Energy-aware fuzzy clustering with genetic optimization for MANETs. Wireless Networks, 31(2), 567–582. https://doi.org/10.1007/s11276-025-03456-9.

[24] Jain, M., Kumar, S., & Rao, P. (2023). Blockchain-based trust management for secure multipath routing in MANETs. ACM Transactions on Sensor Networks, 19(1), 34–51. https://doi.org/10.1145/3594321.

[25] Hussain, A., Li, W., & Sharma, N. (2024). Deep learning-based intrusion detection for secure multipath routing in MANETs. IEEE Access, 12, 10214–10229. https://doi.org/10.1109/ACCESS.2024.3265982.

[26] Wang, J., Kim, T., & Choi, H. (2025). Lightweight elliptic curve cryptography for energy-efficient multipath routing in MANETs. Future Generation Computer Systems, 142, 208–220. https://doi.org/10.1016/j.future.2025.04.011.

[27] Santos, D., Verma, P., & Ghosh, A. (2023). Hybrid clustering and AI-assisted multipath routing for MANETs. Computer Communications, 198, 312–324. https://doi.org/10.1016/j.comcom.2023.09.021.

[28] Lee, C., Nguyen, D., & Park, J. (2024). Quantum-inspired clustering for secure and efficient routing in MANETs. Journal of Network and Computer Applications, 192, 104123. https://doi.org/10.1016/j.jnca.2024.104123.

[29] Patel, R., Singh, M., & Gupta, H. (2025). Blockchain-based secure multipath clustering for energy-aware routing in MANETs. Ad Hoc Networks, 145, 103921. https://doi.org/10.1016/j.adhoc.2025.103921.

[30] Jegadeesan, S., Kumar, R., & Sharma, V. (2023). Adaptive Ad Hoc On-Demand Distance Vector Routing for MANETs: Performance and latency analysis. IEEE Access, 11, 52312–52325. https://doi.org/10.1109/ACCESS.2023.3278912.

[31] Singh, A., Gupta, M., & Verma, T. (2024). Dynamic source routing optimization for MANET scalability: Challenges and solutions. Wireless Networks, 30, 1145–1161. https://doi.org/10.1007/s11276-024-03012-3.

[32] Kumar, P., Reddy, N., & Bose, K. (2023). Optimized link state routing with energy constraints for dense mobile networks. International Journal of Communication Systems, 36(8), 1–15. https://doi.org/10.1002/dac.5839.

[33] Gupta, R., Sharma, K., & Patel, S. (2024). Zone Routing Protocol: A hybrid approach to MANET routing efficiency. Ad Hoc Networks, 144, 102145. https://doi.org/10.1016/j.adhoc.2024.102145.

[34] Patel, M., Verma, D., & Singh, R. (2023). Weighted clustering algorithm for MANETs: A comparative study on stability and scalability. Wireless Personal Communications, 130, 2331–2348. https://doi.org/10.1007/s11277-023-09912-7.

[35] Sharma, P., Reddy, S., & Das, A. (2024). HEED-based energy-efficient clustering with load balancing for mobile networks. Sensors (MDPI), 24(5), 1021–1035. https://doi.org/10.3390/s24051021.

[36] Reddy, G., Bose, A., & Sharma, N. (2023). Secure multipath routing in MANETs: Integrating encryption and redundancy. IEEE Transactions on Mobile Computing, 22(4), 2153–2167. https://doi.org/10.1109/TMC.2023.3256781.

[37] Bose, K., Patel, R., & Verma, L. (2024). Energy-efficient multipath routing for MANETs: A traffic distribution perspective. Computer Networks, 239, 110234. https://doi.org/10.1016/j.comnet.2024.110234.

RESEARCH ARTICLE

Authors

Mr. Himanshu Bartwal Assistant Professor in PSIT Kanpur and doing currently PhD (Pursuing) with Paper Topic PhD is"An Analysis and Implementation of Multipath Based Secure Routing Algorithm in Mobile Adhoc Network" Received M. Tech (CNE) degree from Graphic Era DEEMED university Dehradun (2012-2014) paper topic is "Rumour routing Protocol". Having 01 patent and book is published.

Dr. Himani Sivaraman, Dean School of Science and Technology, received her Ph.D from Graphic Era Hill University, Dehradun 2024 with Paper Topic is "An Efficient & Secure Framework in Supply Chain Management Based on Blockchain Technology" Received M. Tech (SE) degree from Noida International University. Having 02 patents and 23 research articles in her credit. Research Area: Blockchain, Machine Learning, Cloud Computing.

Dr. Jogendra Kumar is working as Assistant Professor, Faculty of Computer Science and Engineering Department, G.B.Pant Institute of Engineering and Technology Pauri Garhwal Uttarakhand-246194. He has fifteen years of teaching experience in Engineering, UG and PG level. Her research interest includes Wireless Networks, IoT, Block Chain Technology, Big Data Analytics, Machine Learning and WSN. Two Ph.D scholars were pursuing their research under his guidance. He is also an International Scientific Committee member for Researchers in various universities. He has received two awards. He has published many research papers, books, book chapters in SCI, WoS, IEEE, SCOPUS journals. He also published many patents in IPR. He serves as Editor in Book Chapters, Editorial Board Member and Reviewer in various International Journals. He is an active member in Professional Bodies like ISTE, IAENG (USA) and IACSIT.

How to cite this article:

Himanshu Bartwal, Himani Sivaraman, Jogendra Kumar, "Energy-Efficient Based Secure Multipath Data Routing Using Clustering Algorithm in Mobile Ad-Hoc Networks", International Journal of Computer Networks and Applications (IJCNA), 12(2), PP: 278-290, 2025, DOI: 10.22247/ijcna/2025/18.