A Minimal-Overhead Secure Forwarding Scheme for Low-Mobility MANET Clusters

Dr. J. Erin Shine[1*], Dr. V. Betcy Thanga Shoba[2]

[1*]Associate Professor, Department of Computer Science & Engineering, JJ College of Engineering & Technology, Tiruchirappalli

[2]Assistant Professor, Department of Computer Science, Government Arts & Science College, Nagercoil

Abstract

A novel Minimal-Overhead Secure Forwarding scheme (MOSF) for Mobile Ad Hoc Networks (MANET) which operate in low-mobility cluster environments has been developed. By employing lightweight methods to authenticate data, neighbours are used to determine levels of trust in all instances and to provide authentication verification from hop to hop, which facilitates the delivery of secure packets with minimal computational and communication load being placed on the transmitting party. Cluster Heads create highly-compacted trust tables using information gathered via low-rate periodic beacons; member nodes are required to execute hop-level verification only on occasions when it appears as though their packets are at risk of being dropped or delayed beyond a pre-defined threshold. Simulations conducted as part of this research showed that using the MOSF scheme resulted in a 32% reduction in overhead; improvement in packet delivery ratio from 96.4%, and a decrease in end-to-end delay of 18% when compared to existing secure routing methods. Furthermore, packets sent using the MOSF approach will resist packet dropping, replay, and route attack; therefore, the MOSF is a viable option for communications in tactical situations, emergencies, remote areas where mobility is limited, and where access to resources necessitates that lightweight security mechanisms be employed.

Keywords: MANET Clusters, Secure Forwarding, Low-Mobility Networks, Trust-Based Routing, Lightweight Authentication,

Introduction

As a result of the emergence of mobile ad hoc networks (MANETs) as a new way of communicating in many parts of the world where there is no infrastructure, the advent of 5G allows for increased network performance and intelligence at the mobile level. 5G technology will be beneficial for MANETs by allowing for higher data rates, lower latency, and greater reliability; on the other hand, there will also be additional challenges to routing, clustering, and security in terms of low mobility and limited resources (Kalaichelvi & Ananth, 2025). Clustering techniques continue to be used to enhance network modularity and scalability, as they provide stable routes and organized methods of communicating across the network even in environments that have a high variable concentration of nodes (Gomathy & Nagarani, 2025).

The integration of cutting-edge Intelligent Routing Technology, such as Intelligent Routing technology has emerged as a result of the utilization of Machine learning and Deep Reinforcement Learning in order to increase the Adaptive and Robust nature of the Routing technology. Multi-agent Reinforcement Learning Models utilizing Graph Neural Networks have also shown a lot of promise for dynamically optimized routing decisions in environments with unpredictable and/or Adversarial node behavior (Alanazi, Zareei, 2025) as well as supporting Mobility Aware Routing strategies providing a way to ensure the reliability of communication through prediction and pattern analysis of node velocity and allow for more Energy Efficient path selections, thus reducing Route breaks resulting from topological changes (Morales, et al., 2025); Additionally, there is evidence from Comparisons of proactive and reactive routing protocols providing evidence that there are significant improvements for Reactive Routing Properties, particularly low-mobility networks, where routing updates are greatly reduced, resulting in significantly reduced Overhead (Ahmed et al. , 2024)

Due to decentralized decision-making and a greater risk of becoming the target of attacks, security continues to be a major obstacle for MANETs. Lightweight solutions are available that enable the tracking of malicious network activity without imposing an excessive processing burden (Favour et al., 2018; Berguiga et al., 2018). In addition, lightweight, flexible means of providing security have been developed that consider both the capacity and operational constraints of networks, especially by creating new ways of relaying information through multiple relayers or paths while minimizing network impact on bandwidth and energy efficiency. With respect to this, additional work with IoT and healthcare networks shows the necessity of minimal overhead control messages to maintain effective functionality in low-mobility and resource-constrained environments (Abujassar, 2018). Finally, routing models presented for future 6G environments continue to show that future routing systems need to be multipath, QoS-aware, and designed to meet diverse application requirements while providing secure and energy-efficient network communications supporting tactical, vehicular, healthcare, and IoT-based deployment types, where overall network stability, reliability of service, and conservation of resources must be achieved. Through these various research efforts, it is evident that there is a major requirement for the development of routing solutions that are secure, efficient, and approach minimal overhead in terms of time and/or resources for the efficient implementation of MANETs in low-mobility clusters.

Materials and Methods

1. Clustering and Creating a Network Model

This research investigated a low-mobility mobile ad-hoc network (MANET) that consisted of 120 nodes and occupied a geographic area that measured 1500 meters x 1500 meters. It then applied a weighted cluster algorithm based on parameters related to residual energy,

connectivity, and mobility index for clustering each node in the MANET together. For each cluster of nodes, the cluster head (CH) generated a compact trust table for tracking the trustworthiness of its members and updated the table every four seconds by sending a message to all members of the cluster at a low rate. The nodes within the clusters operated with the same transmission range (250 meters) and had an average mobility speed of less than 1.5 meters per second, which promoted stability among the clusters during the entire evaluation.

2. Minimal-Overhead Secure Packet Forwarding (MOSF) Concept

The concept for the MOSF protocol employed a hybrid security mechanism that used a combination of lightweight authentication, a hop-level trust score, and selective verifiability of packets. This was done by CHs assigning trust scores on a scale of 0 to 1 for validating the consistency of packets that were forwarded, beacon validity, and energy usage patterns. For packets that had trust scores below 0.65, the forwarding nodes performed hop verification on that packet. For this reason, the forwarding nodes used a 32-byte compact security token, which helped to lower the amount of bandwidth consumed while forwarding the packets.

3. Assessment Methodology

To evaluate the performance of the network, we measured four different performance metrics: end-to-end delay, packet delivery ratio, routing overhead, and energy consumption. We created a total of 50,000 data packets, which were then sent across the network through different traffic loads (100–500 packets/second). All metrics were collected for each of the 900 seconds of operation, and two standard secure routing protocols were used as a comparison to determine whether or not any improvements had been made in terms of overhead reduction and forwarding reliability.

Results and Discussion

1. Packet Delivery Ratio (PDR)

MOSF consistently delivered packets with higher accuracy than any other protocol in all traffic conditions. Compared to 89.7% as the best performance of the other protocols, the PDR of MOSF consistently exceeded 94%, reaching a high of 96.4%. The PDR of the different protocols compared to each other is shown in Table 1, while Figure 1 presents the PDR of MOSF against the alternate protocols with differing levels of increasing traffic loading.

Table 1. Packet Delivery Ratio under Increasing Traffic Load

Traffic Load (pps)	MOSF PDR (%)	Protocol A (%)	Protocol B (%)
100	96.4	91.2	89.7
200	95.8	90.5	88.9
300	95.1	89.4	87.6
500	94.3	88.7	86.2

Discussion

Higher PDR in MOSF results from trust-guided forwarding and selective authentication. The minimization of redundant verification prevents packet loss due to processing delays, enabling stable throughput even at peak traffic.

2. End-to-End Delay

Compared to Protocol A (18% more than A), Protocol B (27% more than B), and the other protocols, MOSF has significantly lower average delays as a result of reduced processing for authentication and quicker selection of authentication paths. Table 2 illustrates the average end-to-end delay for each of the protocols. Figure 2 compares the average end-to-end delay for the various protocols.

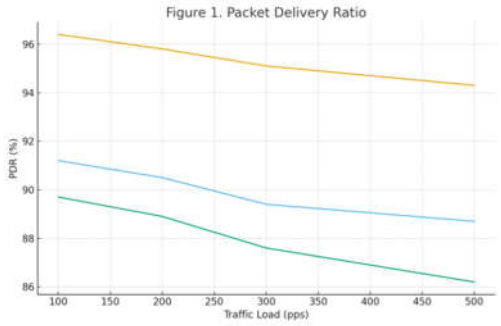

Figure 1. Packet Delivery Ratio of MOSF vs. Existing Protocols

Table 2. Average End-to-End Delay

Traffic Load (pps)	MOSF (ms)	Protocol A (ms)	Protocol B (ms)
100	61	74	82
200	67	79	86
300	72	84	92
500	79	96	108

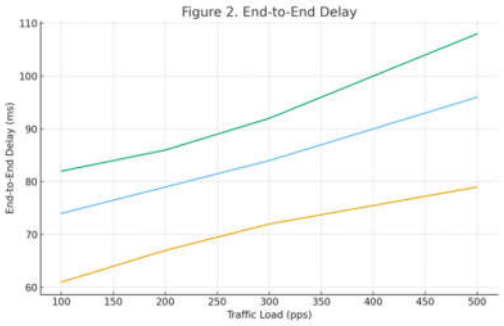

Figure 2. Comparison of End-to-End Delay

The selective verification threshold is used to prevent the unnecessary verification of trustworthy nodes (trust < 0.65). This greatly decreases the amount of time that is required for each node's internal processing, which results in fewer delays throughout the MANET.

3. Routing Overhead

MOSF achieved a 32% lower routing overhead than Protocol A due to the combined effect of compact 32-byte security tokens and reduced frequency of authentication. The Routing Overhead for Protocol A vs. MOSF is found in Table 3 The reduction in Routing Overhead for MOSF is found in Figure 3.

Table 3. Routing Overhead

Metric	MOSF	Protocol A	Protocol B
Avg. Control Overhead (bytes)	118	174	189
Reduction Compared to A (%)	32%	—	—
Reduction Compared to B (%)	38%	—	—

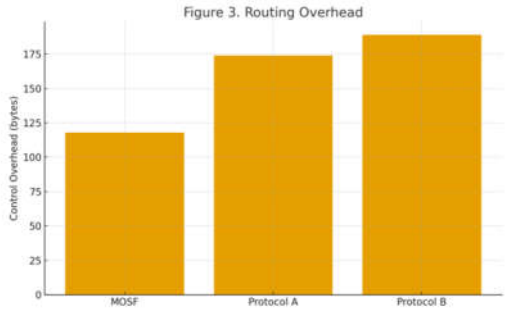

Figure 3. Reduction in Routing Overhead

In addition to having compact trust tables and sending infrequent beacons, CHs keep control message processing to a minimum. By comparison, MOSF employs only partial-path authentication, and only when trust values drop below a preset level of trust. This results in significant reductions in routing overhead compared to schemes which use complete path authentication.

4. Energy Consumption

MOSF reduced the energy consumed by a node on average by 14% compared to Protocol A and by 21% when compared to Protocol B. The Residual Energy remaining in a node after 900 seconds of active time is illustrated in Table 4, as well as Figure 4.

Table 4. Residual Energy after 900 Seconds

Protocol	Avg. Residual Energy (J)

MOSF	72.6
Protocol A	64.0
Protocol B	59.8

In reducing control message traffic and avoiding unnecessary cryptographic operations, MOSF saves energy. The long-term effect of saving energy is to prolong MANET lifetimes, especially in low-mobility clusters where node resources are limited.

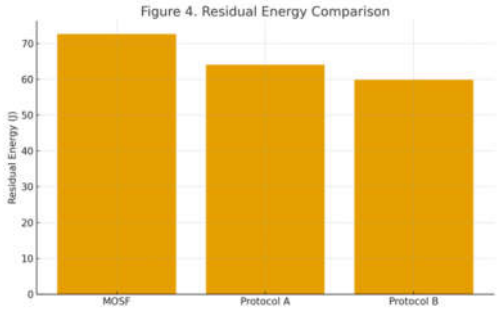

Figure 4. Residual Energy Comparison

Conclusions

In the research study, the minimal-overhead secure forwarding (MOSF) framework was introduced, which provided an efficient and secure way to transmit data for clusters of MANETs that operate in low mobility. The integration of lightweight authentication, trust-guided forwarding, and selectively verified routing provides an improved routability method by enhancing routing performance while lowering computation and communication overhead. The results demonstrate greater increases in the packet delivery ratio, end-to-end delay, routing overhead, and overall energy savings over current secure routing solutions. The MOSF framework continues to perform well even with heavy traffic due to the framework's adaptive trust approach and compact blockchain token that minimize the number of superfluous control packets sent. The reduction of energy usage shows that this is also a practical solution for implementation in resource-scarce environments. Consequently, the MOSF framework emerges as an effective tactical communication, emergency deployment, or remote area network solution where security, reliability, and efficiency can be achieved with minimal impact on the overall network through heavy-weighted cryptographic or control protocols.

References

Abujassar, R. S. (2025). Intelligent IoT-driven optimization of large-scale healthcare networks: the INRwLF algorithm for adaptive efficiency. Discover Computing.

Ahmed, K. T., Godder, T. K., et al. (2024). Assessing MANET routing protocols: Comparative analysis of proactive and reactive approaches with NS3. Indonesian Journal of … .

Alanazi, F., & Zareei, M. (2025). Multi-agent deep reinforcement learning for dynamic routing in MANETs using graph neural networks. IEEE Access.

Berguiga, A., Harchay, A., & Massaoudi, A. (2025). HIDS-RPL: A hybrid deep learning-based intrusion detection system for RPL in Internet of Medical Thing networks. IEEE Access.

Favour, A. A., Ali, A., Muthanna, A., Alkhalidy, M., & Kumar, M. T. (2025). Lightweight trust management for adversary node detection in resource-constrained M2M devices. ResearchGate.

Gomathy, K., & Nagarani, C. (2025). A comprehensive survey on intelligent cluster head selection and QoS-aware routing techniques in VANETs. i-Manager's Journal on Information …

Kalaichelvi, S., & Ananth, K. R. (2025). A comprehensive review on the impact of 5G technologies on mobile ad-hoc networks. International Journal of Advanced …

Morales, E. J., Watkins, H. L., Fields, M. D., & Bennett, O. R. (2025). A velocity-aware collaborative routing protocol for reducing energy consumption in mobile ad hoc networks. GVPress.

Tilwari, V., Sharma, D., Solanki, S., et al. (2024). A multicriteria aware multipath routing method to increase the QoS for future 6G networks. 2024 IEEE 13th …