International Journal of Computational Methods and Experimental Measurements
Vol. 13, No. 1, March, 2025, pp. 115-123
Journal homepage: http://iieta.org/journals/ijcmem

Comprehensive Approach to Addressing Misbehaving and Unintentional Packet Drops Nodes in MANETs to Improve the Network Performance

Polu Srinivasa Reddy*, Arshad Ahmad Khan Mohammad

Department of CSE, GITAM Deemed to be University, Hyderabad 502329, India

Corresponding Author Email: spolu@gitam.in

https://doi.org/10.18280/ijcmem.130112

Received: 2 February 2025
Revised: 21 March 2025
Accepted: 26 March 2025
Available online: 31 March 2025

Keywords:
MANETs, packet drop, misbehavior node, acknowledgments, performance

ABSTRACT

Mobile Ad Hoc Networks (MANETs) plays an important role in various fields; however, this network unavoidably encounters difficulties at the network layer primarily owing to misbehavior or malicious nodes. Among the issues plaguing MANETs, the deliberate and accidental dropping of packets by intermediate nodes emerges as a noteworthy problem requiring attention. The work proposes a novel routing protocol that aims to mitigate the packet dropping problem in a thorough yet efficient manner by selecting only neighbors with proven stability and integrity during route discovery. The protocol devises a neighbor node election tactic reliant on residual status of energy and buffer so that it can compute stable route and avoid those neighbors in route which are having constrained energy and buffer. Additionally, it deploys counter-based authenticated acknowledgments and promiscuous monitoring to enable integrity in route and counter malicious packet drooping. Simulation results show the protocol's efficacy, consistently outperforming existing algorithms in packet delivery and energy efficiency. In conclusion, this work systematically addresses the complexities introduced packet dropping nodes in infrastructure-less networks.

1. INTRODUCTION

MANETs are dynamic, self-configuring wireless networks consisting of mobile wireless nodes that communicate directly without central administration and fixed infrastructure. It leverages ad hoc routing protocols, allowing nodes to create and maintain network connections spontaneously. This network is characterized by lack of fixed infrastructure, self-organizing ability, dynamic topology, mobility, decentralization without centralized administration, and limitations of nodes' resources. Such distinguishing qualities render MANETs particularly useful in circumstances where conventional infrastructure networks are impractical, unavailable, or non-existent. Situations where conventional, foundation-built systems fail to offer networking and mobile ad hoc solutions serve as a stopgap [1].

MANETs find a great spectrum of uses in several fields. Essential in military operations, they ensure flexible and safe communication on the ground. Further it allows real-time patient monitoring in healthcare, therefore enhancing the effectiveness of medical treatments. Moreover, it helps to improve disaster recovery efforts by preserving communication while conventional infrastructure is disrupted. MANET-based safe and flexible communication is what government organizations rely on, especially when traditional networks are hacked. Furthermore, it increases network-based gaming experiences in civilian sectors [2], enables resource sharing in smart home environments, and offers continuous conferencing.

Nonetheless, MANETs present many challenges. The open wireless media, multi-hop communication, and lack of centralized control make security a major issue since they make one vulnerable to many attacks. Further challenges arise in supervising the changing network topology, resource constraints, and preserving quality of service (QoS). Whether intentional or accidental, packet loss is a significant problem in MANETs [3].

In intentional packet dropping-that is, attacks including the Black Hole Attack Cooperative Black Hole Attack, False Reports, and Partial Dropping, where nodes purposefully drop packets. Collisions, poor transmission power, limited energy resources, buffer overflow, and expiration of time-to-live (TTL) cause unintentional or accidental packet drop. Mitigating packet drop is crucial for reliable networks operations, requiring systems to detect and fix nodes that drop packets [4].

In literature various intrusion detection solutions have been designed for MANETs, however there is a requirement of identifying and mitigating both intentional and unintentional packet-dropping nodes. If ignored, this issue can severely impact overall MANETs performance. The paper aims to design effective solutions to mitigate packet dropping nodes of MANETs by two distinct approaches explained as follows:

1) To mitigate unintentional packet dropping nodes and extend the performance of the network, the work computes the route with nodes which are having sufficient

resources and buffer space. The metric used to select route is resource-rich, uncongested and energy- sufficient nodes path.

2) Counter-based authenticated acknowledgements and indiscriminate monitoring help to reduce malicious packet drops, hence preserving reliability in communication. Data flow is guaranteed dependability via counter-based authenticated acknowledgment and indiscriminate monitoring. This approach directly reduces packet loss, therefore improving network dependability.

To effectively reduce both intentional and inadvertent packet drop, the paper combines the above-described techniques with the existing reactive routing protocol (AODV). Simulation results show the protocol's efficacy, consistently outperforming existing algorithms in packet delivery and energy efficiency. Thus, this work systematically addresses the complexities introduced packet dropping nodes in infrastructureless networks.

2. LITERATURE REVIEW

To address the problems caused by misbehaving nodes in MANETs, great effort has been done. Methodologies based on reputation [5, 6]: Systems of reputation help to reduce intentional packet dropping by intermediate node during communication. These systems comprise nodes that regularly monitor the behaviour of nearby nodes; the monitoring method is categorized as either direct or indirect experience of reputational information. Indirect experience consists of reputation data acquired from the neighbours of nodes with which it interacts, direct experience involves a node's appraisal of its proximal neighbours. While indirect experience helps to validate and strengthen trust, direct experience is more important in its evaluation. The monitoring component of a node determines the degrees of trust most of the times.

Comparing to credit-based approaches, reputation-based systems [7] have many advantages. They are suitable for MANETs since they replace the need for centralized electronic payment systems or additional hardware including tamper-proof components at individual nodes. Inside the framework based on reputation, several procedures could be applied [4]. Dynamical trust computation continuously tracks peers' reputation by indiscriminate observation, identifying malicious nodes when their reputation falls below a given level. Real-time monitoring classifies specific neighbours as suspected and guides them to listen in on the communications of perhaps hostile nodes. Reputation-based systems compile, preserve, and distribute reputation data over the network so that nodes with high reputations may access network resources while nodes with low reputations may experience isolation.

Approaches based on acknowledgements [8]: Usually, these strategies help one to manage deliberate packet dropping. These techniques enable the discovery and management of nodes by letting nodes intentionally discard packets by verifying their receipt of packets. Although selective acknowledgment of arriving data packets helps to lower routing overhead, acknowledgment-based solutions locate troublesome nodes rather well.

In this field, two main approaches are Two ACK and AACK. Two ACK signifies data packet recognition and calls for nodes along the path to broadcast confirmations to a specified node two hops away. AACK lowers memory and computational expenses by using multiple acknowledgment methods and switching to other procedures should acknowledgements not be received within designated times frames not be received within specified times frames. Although compared to credit-based or reputation-based methods, acknowledgment-based systems are less expensive, their effectiveness depends on the dependability of acknowledgment packets. EAACK pays costs in crucial agreement and employs adaptive acknowledgements but ignores unintentional misbehaviour.

Through careful monitoring, and safe knowledge-based strategies [9] assist to spot and stop both deliberate and inadvertent misbehaviour of nodes. Every node closely observes the activity of its neighbouring nodes. Should a node above a specified packet loss threshold, further investigation is carried out to find the fundamental causes of these occurrences. This method considers limited energy reserves, insufficient memory, or the expiration of the time-to-live (TTL) value generating packet losses. Should the analysis reveal that resource constraints are not causing packet loss, the node will be tagged as biobehavioural, and a warning will be issued to every other node to stop interaction with the found misbehaving node. This approach makes use of a least hop count-based routing metric, which, considering resource constraints, can result in packet loss. It investigates the factors causing packet loss when a node beyond the specified packet drop threshold, hence generating greater delay and additional routing overhead.

Particularly with regard to energy, energy-aware routing techniques help to lower inadvertent behaviour resulting from limited resources. These methods extend network lifetime by considering the energy condition of nodes in route choice. By matching to the energy levels of nodes and avoiding energy-depleted nodes during route creation, they essentially lower accidental errors. Buffer overflow and typical cause of unintended packet dropping nodes in MANETs are mitigated by buffer management mechanisms. By sorting packets based on criteria including priority and delay sensitivity, the method maximizes node buffer use and hence reduce packet loss resulting from overflow. While buffer management helps to minimize unintended packet dropping, it could not be as successful against intentional packet dropping.

These methods focus is to either mitigate intentional or inadvertent packet dropping, therefore failing to provide a complete solution even if they offer interesting insights and strategies for tackling specific aspects of misconduct in MANETs. While some strategies give security top priority to mitigate intentional misbehaviour, others do not sufficiently examine circumstances limited in resources that lead to unintended misbehaviour. Moreover, some approaches combine advanced cryptographic techniques, which may lead to processing overhead and thereby make less suitable for MANETs with limited resources. Therefore, a comprehensive mechanism is essential for both effectively controlling intentional and unintentional misbehaviour as well as for suitable to the dynamic character of MANETs.

The work proposes a novel routing protocol that aims to mitigate the packet dropping nodes using efficient way of selecting only those neighbours with proven stability and integrity during route discovery. The protocol devises a neighbour node election tactic reliant on residual status of energy and buffer so that it can compute stable route and avoid those neighbours in route which have constrained energy and buffer. Additionally, it deploys counter-based authenticated acknowledgments and promiscuous monitoring to enable

integrity in route and counter malicious packet dropping. Simulation results show the protocol's efficacy, consistently outperforming existing algorithms in packet delivery and energy efficiency. In conclusion, this work systematically addresses the complexities introduced packet dropping nodes in infrastructureless networks.

3. PROPOSED WORK

By resolving packet-dropping problems at the network level generated by malicious activities as well as system failures, Mobile Ad Hoc Networks (MANETs) help to enhance the reliability and efficiency. This paper designs a novel approach to address these problems by following contributions

1). To guard against malicious packet-dropping nodes, it uses advanced security techniques such as counter-based authenticated digested acknowledgements.

2). Moreover, techniques for enhancing packet processing capability of nodes in terms of energy and buffer constraints are presented to minimize the packet drops brought about by system faults.

3). Moreover, adding these features into the Ad Hoc On-Demand Distance Vector (AODV) routing protocol [10] provides trustworthy and safe communication.

Through better reliability and efficiency, this designed mechanism offers MANETs a complete solution.

3.1 Prevention of intentional misbehaving nodes: Optimizing packet processing in multi-hop wireless networks

Improving packet delivery is essential for enabling efficient communication in wireless infrastructureless multi-hop networks as the network is constrained in terms of energy and buffer. The work designs a mechanism of an optimization method that enables intermediate nodes, (I_n), efficient packet processing. Considering energy and buffer limits, the mechanism solves resource constraints and offers techniques to calculate the Optimal Packet Processing Capacity ($OPPC$) of these nodes.

Every intermediate node in MANET, known as I_n, has specified limits on energy (E) joules and buffer capacity (Q) bytes. Maintaining packet processing capability within these constrained limits is vital to mitigate energy depletion and buffer overflow, which cause packet drops from an intermediate node. The total number of packets a node handles cannot exceed its buffer capacity ($Q\ bytes$) and accessible energy (E joules) to prevent packet drop. Addressing this restriction helps to mitigate buffer overload and save energy resources, therefore lowering the possibility of packet drop from an intermediate node.

3.1.1 Enhancing packet processing

The network follows the buffer capacity (Q) and energy reserves (E) of every intermediary node while trying to maximize packet processing. Attaching high packet throughput while keeping to these constraints depends on efficient use of resources. Strategic packet management calls for careful selection of packets for processing given constraints on buffer and energy. For best packet processing, effective congestion control and balance between energy and buffer use are absolutely vital.

Within this paradigm, multi-hop communication depends on intermediary nodes. The intermediary nodes have E joules of energy reserve and buffers capacity of Q bytes. These buffers are momentarily occupied by packets negotiating the network. Consider the following elements to find the Optimal Packet Processing Capacity (OPPC) of nodes.

3.1.2 Energy and buffer optimization

The aim of the algorithm is to process the highest number of packets such that the energy consumption does not beyond the energy capacity (E) of every node. Determining the capacity of packets that can be processed concurrently depends critically on buffer capacity (Q). The method has to improve buffer space efficiency and stop buffer overflow. From the collection $\{p_1, p_2, p_3, \dots, p_n\}$ drawn from multiple sources $\{S_1, S_2, S_3, \dots\}$, the algorithm must choose packets for processing with great care. The aim is to maximize the overall size of selected packets so that their total energy consumption during processing stays within the available energy (E) and that their cumulative sizes do not surpass the buffer capacity (Q).

The optimization technique ensures that, considering energy and buffer constraints, every intermediary node efficiently handles packets. The result is the discovery of the Optimal Packet Processing Capacity ($OPPC$) for every node, so enabling continuous multi-hop communication and so eliminating packet loss related to buffer or energy limitations.

The Energy-Buffer Product (EBP) defined as follows is obtained by computing the energy and buffer required for processing a packet (P_i) at an active intermediate node:

3.1.3 Energy and buffer threshold (ET and QT)

The minimum energy and buffer space required for the node to process the one packets and participate in routing.

$$\boldsymbol{ET} = E_{min}$$
$$\boldsymbol{QT} = Q_{min}$$

3.1.4 Initial energy-buffer product ($EBP_{initial}$)

$$\boldsymbol{EBP_{initial}} = E * Q$$

$\boldsymbol{EBP_{initial}}$ represents the product of the initial energy level (E) in joules and the initial buffer capacity (Q) in bytes of the intermediate node. $E\ and\ Q$ values are greater than threshold values so that they can participate in communication.

3.1.5 After processing one packet ($EBP_{after\_one\_packet}$)

$$\boldsymbol{EBP_{after\_one\_packet}} = (E - E(P_1) * (Q - Q_s(P_1))$$

$EBP\_after\_one\_packet$ signifies the product of the remaining energy $E - E(P_1)$ after processing the first packet (P_1) and the remaining buffer space ($Q - Q_s(P_1)$ after forwarding this packet.

3.1.6 After processing 'n' number of packets ($EBP_{after\_n\_packet}$)

$$\boldsymbol{EBP_{after\_n\_packet}} = (E - \sum(E(P_i)\ for\ i\ in\ 1\ to\ n)) * (Q - \sum(Q_s(P_i)\ for\ i\ in\ 1\ to\ n))$$

$\boldsymbol{EBP_{after\_n\_packet}}$ represents the product of the remaining energy $(E - \sum(E(P_i)\ for\ i\ in\ 1\ to\ n))$ after processing $'n'$ packets and the remaining buffer space $(Q - \sum(Q_s(P_i)\ for\ i\ in\ 1\ to\ n))$ after forwarding these packets.

3.2 Current Residual Condition (CRC)

Crucially for figuring a node's packet processing capacity, Algorithm 1 computes the Current Residual Condition (CRC). Following energy and buffer constraints, it finds the best packet selection for processing using dynamic programming.

Algorithm 1: Calculation of Current Residual Condition (CRC)

Functioncalculate_CRC
$(n, E, P, e, \boldsymbol{EBP_{initial}}, \boldsymbol{EBP_{after\_n\_packet}}, Keep)$
Initialize 2-Dimentional arrays $\boldsymbol{K}[n+1][EBP_{initial}+1]$ and $\boldsymbol{Keep}[n+1][EBP_{initial}+1]$
for i from 0 to n:
for EBP from 0 to $EBP_{initial}$:
$K[i][EBP] = 0$
$Keep[i][EBP] = False$
for i from 1 to n:
for EBP from 0 to $EBP_{initial}$:
if $\boldsymbol{EBP_{after_{n_{packet}}}}[i] <= EBP\ and\ K[i-1][EBP] < K[i-1][EBP - \boldsymbol{EBP_{after_{n_{packet}}}}[i]] + P[i]$
$K[i][EBP] = K[i-1][EBP - EBP_{after\_n\_packet}[i]] + P[i]$
$Keep[i][EBP] = True$
else:
$K[i][EBP] = K[i-1][EBP]$
$EBP = EBP_{initial}$
$selected\_packets = an\ empty\ set$
for i from n down to 1:
if $Keep[i][EBP]$:
add packet i to selected_packets
$EBP = EBP - EBP_{after\_n\_packet}[i]$
return $selected\_packets, K[n][EBP_{initial}]$

The Algorithm 1 initializes two 2-Dimentional arrays, K and Keep, to store intermediate values and track the selection of packets. It uses dynamic programming with a nested loop to calculate CRC values for different scenarios, considering each packet's energy and buffer requirements. It ensures that packets are selected to maximize processing while respecting energy and buffer constraints. Finally, it traces back through Keep to determine the set of selected packets and computes the final CRC value.

3.3 Procedure for decision-making

Algorithm 2 plays a crucial role to decide the node's participation regarding routing based on computed Current Residual Condition (CRC) value. It compares CRC with CRC -threshold values to determine whether the node to participates in routing or acts as a backup node or does not participate in routing.

Algorithm 2: Procedure for Decision Making

function decide_residual_status $(CRC, CRC_{min}, CRC_{max})$

$participating\_nodes\_counter = 0$
if $CR > CRC_{max}$
$participating\_nodes\_counter += 1$
return "Node participate in routing"
else $CR > CRC_{min}$ && $CR < CRC_{max}$
return "backup node"
else if $CR < CRC_{min}$
return "Node is not participates in routing"
$if\ participating\_nodes\_counter == 0$
return "Backup node considered for routing"

This algorithm decides the node's routing participation based on its CRC, which reflects its packet processing capability in terms of its energy and buffer. Further The CRC threshold values CRC_{min} and CRC_{max} are computed using the following equations (1&2). The routing status of the node is determined by comparing its CRC with the computed $CRC_{threshold}$ values.

$$CRC_{min} = \alpha * \frac{EBP_{initial}}{EBP_{initial} + Q_{initial}} \quad (1)$$

$$CRC_{max} = \beta * (EBP_{residual} + \gamma EBP_{initial}) \quad (2)$$

where,

$$EBP_{residual} = \left(E_{initial} - \sum_{i=1}^{n} E(p_i)\right) * \left(Q_{initial - \sum_{i=1}^{n} Q_s(p_i)}\right)$$

$$CRC_{threshold} = \begin{cases} CRC_{max}, if\ CRC > CRC_{min} \\ CRC_{min}, otherwise \end{cases}$$

By allowing intermediary nodes in a multi-hop wireless network to make informed decisions on packet processing, Algorithm 1 and Algorithm 2 help to maximize efficiency while nevertheless allowing energy and buffer constraints. These techniques are crucial to ensure reliable multi-hop communication and as well as to reduce the probability of packet drops happened due to energy and buffer constraints.

4. PREVENTION OF INTENTIONAL MISBEHAVING NODES: COUNTER-BASED DIGESTED ACK

Resilient security measures are needed in Mobile Ad Hoc Networks (MANETs) to reduce false reporting, partial packet-dropping events, and intentional packet-dropping by hostile nodes. When network security and data integrity are absolutely crucial, the next technological security steps are judged to be absolutely necessary to create a strategy that effectively counters intentional packet-dropping nodes.

4.1 Counter-based authenticated acknowledgments

By use of counter-based validated acknowledgments, this system ensures the dependability of data flow. A destination node creates acknowledgments including a counter value upon receiving data packets. As a separate identity for acknowledgments, the counter rises with every received packet. This maintains data delivery integrity and helps against rogue node counterfeit acknowledgment messages.

Systems of Processed Recognition

Digested acknowledgements in this method enhance security. The destination node guarantees receipt of packets during designated intervals. It combines message digest (MD5) computations and a safe session key agreement using the accepted technique employing chaotic maps [11, 12] into one crucial security mechanism. Data integrity is guaranteed via the MD5 cryptographic hash methods Should an aggressor try to change an acknowledgement, the digest value will be changed, therefore informing the source and destination nodes.

Unrestricted Monitoring

This method stresses on the identification and reduction of packet-dropping nodes. Every MANET node engages in promiscuous monitoring of the one-hop neighbors. Key metrics under observation are packet count received (P_r) and packet count sent (P_t). This method generates suspicions of malicious conduct if P_r and and P_t do not match or the difference beyond a given level.

Control packet distribution

Broadcasting Control packets are distributed to inform other nodes upon the discovery of hostile conduct by promiscuous monitoring. Among the important information these control packets contain are packet type, monitoring node ID, misbehaving node ID, broadcast ID, lifetime, and timestamp. This information distribution ensures that other nodes know the presence and identify of the problematic node, therefore allowing them to carry out appropriate responses. Together, these security elements create a strong plan to offset deliberate packet-dropping brought on by hostile actors, false reporting, and nodes that only partially drop packets, hence improving data integrity and security inside MANETs. This is especially important in circumstances when security is of great relevance.

Algorithm-3 for the identification and mitigating of purposeful misbehaving nodes in MANETs combines a wide spectrum of security aspects to improve network security and data integrity. Counter-based authenticated acknowledgements use incrementing counters to guarantee data transmission dependability; a digested acknowledgment mechanism uses cryptographic hash and safe session key agreement to improve security; promiscuous monitoring examines packet reception and forwarding statistics to identify and alert on packet-dropping nodes; and control packet broadcasting distributes packets. Essential in data-sensitive environments, the program protects MANET data by following these procedures and isolating troublesome nodes.

Algorithm:3 Detection and Mitigation of Intentional Misbehaving Nodes in MANETs

***Initialization*:**

- Set predefined time interval τ for tracking received packets.
- Initialize tracking counter S_τ to 0.
- Create an empty cache for monitoring neighboring nodes.

***Counter-Based Authenticated Acknowledgments*:**

- On data transmission from source to destination, increment S_τ for each received packet at the destination.

***Generating Acknowledgment*:**

- Create an acknowledgment packet $\{(\tau, S_\tau)\}$.
- Add the session key from the authenticated key agreement using chaotic maps.

***Computing the Message Digest*:**

- Calculate m by XORing the acknowledgment packet and session key.
- Compute the digested message $(d) = H(m)$

***Sending Acknowledgment*:**

- Send the acknowledgment packet and digested message to the source node through the reverse route.

***Verification at Source Node*:**

- Upon receiving the acknowledgment, calculate m^1 by XORing the acknowledgment packet and the source's session key.
- Compute the digested message $(d^1) = H(m^1)$.
- If d^1 equals d, communication proceeds; otherwise, an intentional misbehaving node is detected, and further actions are initiated.

***Promiscuous Monitoring*:**

- For each communication session, activate the monitoring interval.
- For each communication session i, monitor the number of packets received $(p_r)$and forwarded (p_t).
- Compare (p_r) and (p_t), and if a mismatch or difference exceeding the threshold is detected, mark the neighbor node as a misbehaving node.

***Control Packet Broadcasting*:**

- If a misbehaving node is detected, broadcast a control packet to notify all nodes. The control packet includes relevant information such as packet type, monitoring node ID, misbehaving node ID, broadcast ID, lifetime, and timestamp.

***Isolation and Prevention*:**

- Other nodes maintain a table of misbehaving nodes, ensuring that detected misbehaving nodes are not allowed to participate in further communication.

This algorithm is a complete system meant to find and reduce intentional misbehaviour in Mobile Ad Hoc Networks (MANETs). It ensures reliable communication by incorporating multiple security components. A prime component is the Counter-Based Authenticated Acknowledgments, which assign different counters to data packets so complicating the duplicate acknowledgment messages by malicious nodes and so preserving the dependability of data delivery.

The approach uses a Digested Acknowledgment Mechanism to improve security using cryptographic mechanisms and Promiscuous Monitoring to monitor neighbouring nodes for signs of misbehaviour, therefore raising questions upon the discovery of anomalies. The Control Packet Broadcasting feature helps to distribute information about errant nodes around the network so that others may apply appropriate actions. Especially in critical situations, this method improves the integrity and security of MANET data by means of combined implementation of several protections and isolation of packet dropping nodes. This system detects and reduces deliberate node misbehaviour, hence improving MANET data integrity and security.

5. ROUTING TO MITIGATE PACKET DROPPING

In this section we present a new MANET routing

mechanism addressing packet-dropping. Reactive routing methods and misbehaviour avoidance strategies help it to handle purposeful and inadvertent packet dropping. The protocol chooses resource-adequate neighbours depending on residual energy and buffer status to prevent congested or energy-constrained nodes and enhance network efficiency.

To guarantee dependable connectivity and stop malicious packet drops, it additionally employs promiscuous monitoring and counter-based authenticated acknowledgments. Renowned MANET routing system AODV is a reactive routing mechanism identified for effective route finding. We can apply the following changes to improve AODV with the suggested mechanisms for identifying and reducing deliberate misbehaviour nodes and improving packet processing:

Counter-Based Authenticated Acknowledgements: Extend AODV to include a mechanism creating counter-based authenticated acknowledgements for data packets. Every acknowledgment packet will have a counter that rises with every effectively received data packet. Using a mechanism to compute a message digest (e.g., MD5) for acknowledgment packets and then link it to the acknowledgment is the digested acknowledgment mechanism. This guarantees the integrity of messages of acknowledgement.

Constant observation: promiscuous Boost AODV by use of promiscuous monitoring features. Every node joining the network will keep an eye on its one-hop neighbours. For every session of correspondence: One makes up a monitoring interval while activating it. Track the packets received from surrounding nodes, p_r. Track the packet forwarding (p_t) by surrounding nodes. To find any differences, compare (p_r) with (p_t). Mark the nearby node as a possible misbehavioring node if the difference between (p_r) and (p_t) surpasses a preset threshold.

Control packet distribution: Promiscuous monitoring detects a possible misbehaving node; the monitoring node then starts a control packet for broadcast to every other node. Information like packet type, monitoring node ID, misbehaving node ID, broadcast ID, lifetime, and timestamp ought to be part of the control packet. Incorporate a neighbour node selection method grounded on residual energy and buffer condition. This method avoids congested or energy-constrained nodes, improves network efficiency, and helps to select resource-adequate neighbours.

Energy-Aware Routing: Improve AODV with energy-aware routing to take node energy condition into account during route choosing into account. Steer clear of routing over energy-limited nodes to lower the chance of inadvertent misbehaviour. Considering the energy and buffer limitations of intermediary nodes, apply systems for maximizing packet processing inside the network. This enhancement guarantees effective packet processing and helps to stop energy depletion and buffer overflow.

6. PERFORMANCE ANALYSIS

We utilized the NS2.34 simulator [13] in our performance assessment to evaluate the effectiveness of our proposed routing protocol. We analysed a dynamic scenario in which the number of participating nodes varies. We employed the random waypoint mobility model for node mobility, integrating a halt time of 20m/s, which allowed nodes to navigate the network autonomously [14]. Each node possesses an initial energy reserve of 20 joules, and a specified radio transmission range of 250 meters has been established. All nodes were equipped with IEEE 802.11 MAC cards operating at a data rate of 2Mbps. The receiving power and transmission power of nodes initially are 300mW, 600mW respectively. We generated Constant Bit Rate (CBR) traffic for our source nodes with packets size 512-byte. The simulation runed for 1000 seconds, and we consolidated the results from three distinct situations to ensure reliability.

In our simulation, we classified nodes into three categories:

I) Reputed nodes that adhere to the defined routing protocol standards.

II) Deliberately disruptive nodes expose network integrity by purposefully dropping the packets due to malicious actions.

III) Unintentional misbehaving nodes that induce packet loss due to buffer overflow and energy constraints.

This comprehensive methodology allowed us to assess the effectiveness of our proposed routing protocol under realistic and challenging conditions, considering both intentional and unintentional packet loss. The performance metrics utilized to evaluate the proposed work include Throughput, Packet Delivery Fraction, and Energy Efficiency:

The performance evaluation compares the proposed routing protocol with designed protocols across multiple scenarios, including networks with both intentional and unintentional packet-dropping nodes, as well as reliable nodes. The subsequent are the primary scenarios:

Misbehaving Nodes Scenario: This scenario involves networks comprising both inadvertent and deliberate misbehaving nodes in conjunction with trustworthy ones. Unintentional misbehaving nodes discard packets due to buffer overflow or energy constraints, but intentional misbehaving nodes reject all incoming packets and broadcast fraudulent reports to the source. This scenario assesses the effectiveness of the proposed solution about these erroneous nodes.

Variable Node Count: Performance is evaluated utilizing various node amounts and multi-hop communication between entities.

Variation in Simulation Duration: Performance is assessed utilizing various simulation durations and varied amounts of nodes.

Energy Consumption Analysis: The examination of energy consumption is performed with varying numbers of nodes to evaluate the impact of node failure due to battery depletion.

7. PERFORMANCE RESULTS

The performance results of the designed routing technique are compared with those of existing routing systems in several network environments. Figures 1-6 show particular results from simulations in Table 1. Graphically depicted to show the performance of the proposed routing protocol relative to existing protocols, including the Secure Knowledge Algorithm (SKA), the Acknowledgment-Based Algorithm (EAACK), and a basic reactive routing protocol (AODV-NM), the results generally comprise metrics for throughput, Packet Delivery Fraction, and energy economy.

An important performance measure gauging the effectiveness of data flow within the network is throughput. Regarding throughput, our analysis shows that the proposed protocol frequently beats SKA, EAACK, and AODV-NM.

This mainly shows itself when the network's node count increases. Incorporating energy-aware routing and buffer management tools into the suggested protocol helps it to achieve outstanding throughput by effective use of network resources. Applications needing fast and effective data transmission depend on the higher throughput.

Table 1. Existing packet dropping mitigation mechanisms and their characteristics

Approach	Mechanism	Advantages	Disadvantages	Effectiveness Against Malicious Nodes	Impact on Network Performance	Computational Complexity
Reputation-Based Systems	Monitors and evaluates node behavior based on direct/indirect experiences and assigns trust scores	Effectively reduces malicious node impact, enhances trust without requiring central control	High overhead due to continuous monitoring and trust computations	High (Detects and isolates misbehaving nodes effectively)	Moderate (Increases trust but adds processing overhead)	High (Frequent reputation calculations and data dissemination)
Acknowledgment-Based Systems	Uses packet acknowledgment to detect and penalize misbehaving nodes	Provides a lightweight mechanism to detect packet dropping, reducing routing overhead	Highly dependent on reliable acknowledgments, vulnerable to false negatives	Moderate (Detects but depends on acknowledgment reliability)	High (Efficient detection with minimal computational cost)	Low (Only requires acknowledgment checking)
Knowledge-Based Monitoring	Analyzes packet loss patterns and investigates reasons before isolating nodes	Differentiates between intentional and unintentional misbehavior, ensuring fair evaluation	Increases routing overhead and decision delays due to extensive monitoring	High (Thorough analysis before isolation, reduces false positives)	Moderate (Ensures fair assessment but increases processing time)	High (Continuous monitoring and analysis increase processing demands)
Energy-Aware Routing	Selects routes by considering energy levels to extend network lifetime and avoid failures	Prevents route failures due to energy depletion, increasing overall network lifespan	Does not address deliberate malicious behavior or security threats	Low (Does not specifically address malicious behavior)	High (Extends network lifespan and reduces failures)	Low (Only considers energy levels during route selection)
Buffer Management Mechanisms	Manages buffer to prioritize packets and prevent loss due to overflow	Reduces unintentional packet loss, ensuring higher buffer utilization efficiency	Only effective against buffer overflow but ineffective against intentional attacks	Low (Does not prevent deliberate packet dropping)	Moderate (Prevents congestion but may not improve security)	Moderate (Sorting and buffer management require some processing power)

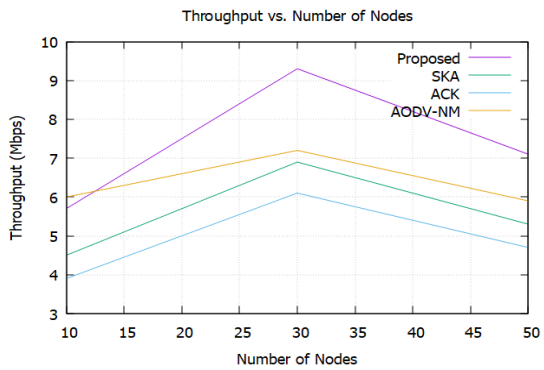

Figure 1. Throughput performance comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to varying number of nodes

Packet Distribution Fraction-defined as the ratio of properly delivered packets to the overall packet count-defines network reliability. Our simulations show that the Proposed protocol routinely sends more packets than SKA, EAACK, and AODV-NM. Both deliberate and inadvertent node misbehaviour in the proposed approach reduces the risk of packet delivery. Packet delivery is improved by counter-based authenticated acknowledgements and indiscriminate monitoring, therefore guaranteeing consistent data transport.

In resource-constrained MANETs, energy efficiency is critical and directly affects network sustainability and node lifetime. ERMMN has higher energy economy. It shows a fair use of the energy resources, therefore avoiding early battery depletion of nodes. This is achieved by careful choosing of surrounding nodes based on residual energy and buffer condition. The proposed protocol is suitable for situations where energy economy is vital since it promotes extended network capabilities.

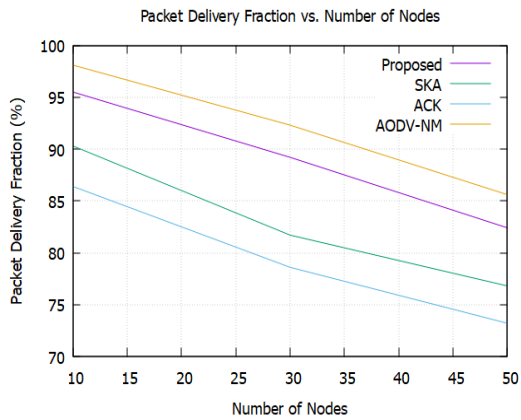

Figure 2. Packet delivery fraction performance comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to varying number of nodes

Over all important criteria-including throughput, packet delivery ratio, overhead, and energy economy-the proposed routing protocol [15] shows improved performance. It deftly addresses the problems raised by both intentional and unintended misbehaviour among MANETs [16, 17]. While SKA and EAACK perform satisfactorily, they may incur more costs and fall short in addressing both kinds of misconduct

completely. Being a basic reactive routing system, AODV-NM [18] performs poorly particularly in cases involving misbehaving nodes. Particularly in important applications where network speed and security are crucial, the suggested protocol is a strong alternative for MANETs [19] because of its efficiency, dependability, and energy-efficient design.

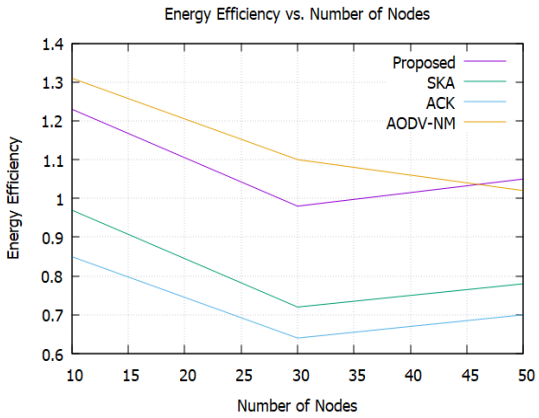

Figure 3. Energy Efficiency comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to varying number of nodes

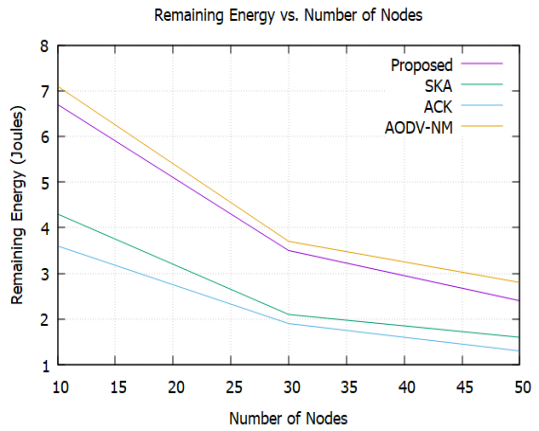

Figure 4. Remaining Energy performance comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to varying number of nodes

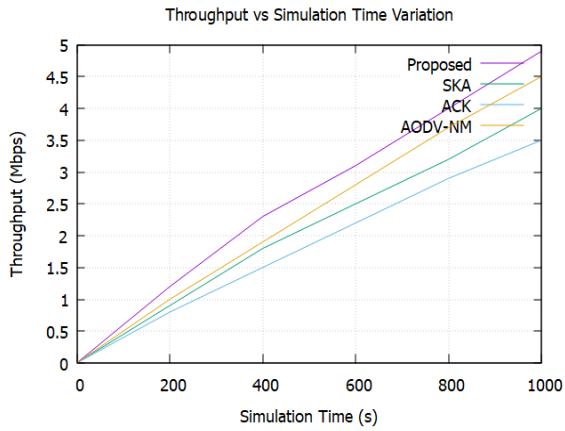

Figure 5. Throughput performance comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to Simulation Time

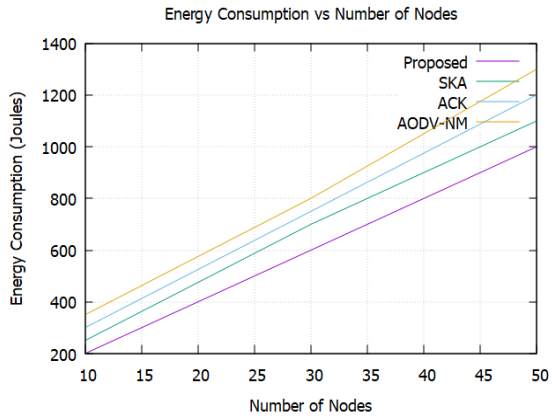

Figure 6. Energy consumption comparison of proposed routing with existing SKA, ACK, and AODV-NM with respect to Simulation Time

8. CONCLUSION

The proposed all-encompassing approach for enhancing security and efficiency in Mobile Ad Hoc Networks (MANETs)offers a complete solution for the packet dropping problems faced by MANETs [20]. Our work essentially guards against malicious packet-dropping nodes and false reporting by including advanced security measures including counter-based authenticated acknowledgements, digested acknowledgements, and novel optimization techniques into the Ad Hoc On- Demand Distance Vector (AODV) routing protocol, so improving packet processing for reliable and safe communication. Furthermore, our neighbour node selection method, based on residual energy and buffer status, maximizes network efficiency and is particularly suitable for uses where data integrity, security, and efficient resource utilization are paramount. Our technologies ensure a significant improvement in the dependability and integrity of wireless communication in a fast-changing environment where MANETs are essential for military operations, emergency response systems, and more. Future research can focus on light-weight security methods and mobility-related challenges to raise data integrity.

REFERENCES

[1] Quadri, S.A., Dapke, P., Nagare, S.M., Bandal, S.B., Baheti, M. (2023). A survey of mobile adhoc network (MANET), its applications, characteristics, and challenges. International Journal for Research in Engineering Application & Management (IJREAM), 9(2): 44-47. http://doi.org/10.35291/2454-9150.2023.0105

[2] Safari, F., Savic, I., Kunze, H., Ernst, J., Gillis, D. (2023). The diverse technology of MANETs: A survey of applications and challenges. International Journal of Future Computer and Communication, 12(2): 37-48. https://doi.org/10.18178/ijfcc.2023.12.2.601

[3] Sivapriya, N., Mohandas, R. (2022). Analysis on essential challenges and attacks on MANET security appraisal. Journal of Algebraic Statistics, 13(3): 2578-2589.

[4] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S.

(2019). Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3): 239-267. https://doi.org/10.1504/IJHI.2019.103580

[5] Thachil, F., Shet, K.C. (2012). A trust based approach for AODV protocol to mitigate black hole attack in MANET. In 2012 International Conference on Computing Sciences, Phagwara, India, pp. 281-285. https://doi.org/10.1109/ICCS.2012.7

[6] Kshirsagar, D., Patil, A. (2013). Blackhole attack detection and prevention by real time monitoring. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, pp. 1-5. https://doi.org/10.1109/ICCCNT.2013.6726597

[7] Saetang, W., Charoenpanyasak, S. (2012). CAODV free blackhole attack in Ad hoc networks. In 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012), Gujarat, India, pp. 63-58.

[8] Atheeq, C., Rabbani, M.M.A. (2021). CACK-A counter based authenticated ACK to mitigate misbehaving Nodes from MANETs. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 14(3): 837-847. https://doi.org/10.2174/2213275912666190809104054

[9] Siddiqua, A., Sridevi, K., Mohammed, A.A.K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, pp. 421-425. https://doi.org/10.1109/SPACES.2015.7058298

[10] Perkins, C., Belding-Royer, E., Das, S. (2003). RFC3561: Ad hoc on-Demand distance vector (AODV) routing. ACM Digital Library. https://doi.org/10.17487/RFC3561

[11] Mohammad, A.A.K., Mirza, A., Vemuru, S. (2016). Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology, 9(26): 1-11. https://doi.org/10.17485/ijst/2016/v9i26/95137

[12] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S. (2018). Providing security towards the MANETs based on chaotic maps and its performance. In Microelectronics, Electromagnetics and Telecommunications: Proceedings of the Fourth ICMEET 2018, Singapore, pp. 145-152. https://doi.org/10.1007/978-981-13-1906-8_16

[13] Issariyakul, T., Hossain, E., Issariyakul, T., Hossain, E. (2009). Introduction to network simulator 2 (NS2). In Introduction to Network Simulator NS2. Springer, Boston, MA, pp. 1-18. https://doi.org/10.1007/978-0-387-71760-9_2

[14] Corson, S., Macker, J. (1999). RFC2501: Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. RFC 2501. https://doi.org/10.17487/RFC2501

[15] Royer, E.M., Toh, C.K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, 6(2): 46-55. https://doi.org/10.1109/98.760423

[16] Kumar, B.R., Bano, F., Sirisha, M., Yalawar, M.S., SK, F., Reddy, P.S. (2024). Brain tumor detection using hybrid deep learning approaches. In 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, pp. 1-5. https://doi.org/10.1109/ICSES63760.2024.10910697

[17] Kaur, R., Singh, P. (2014). Review of black hole and grey hole attack. International Journal of Multimedia and Its Applications (IJMA), 6(6): 35-45. https://doi.org/10.5121/ijma.2014.6603

[18] Pirzada, A.A., McDonald, C. (2005). Circumventing sinkholes and wormholes in wireless sensor networks. In IWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks, Vol. 71.

[19] Hikal, N.A., Shams, M.Y., Salem, H., Eid, M.M. (2021). Detection of black-hole attacks in MANET using Adaboost support vector machine. ournal of Intelligent & Fuzzy Systems, 41(1): 669-682 https://doi.org/10.3233/JIFS-202471

[20] Wu, B., Chen, J., Wu, J., Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security. Springer, Boston, MA, pp. 103-135. https://doi.org/10.1007/978-0-387-33112-6_5