International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Routing Selection Policy on Mobile Ad-Hoc Network using Trust based Mechanism Through AODV Routing Protocol

Mrs. Versha Matre *[1], Dr. Pradnya A. Vikhar [2]

Submitted: 06/10/2023 **Revised**: 27/11/2023 **Accepted**: 09/12/2023

Abstract: This research article provides a detailed examination of a new Trust-Aware On-Demand Distance Vector (Proposed_TAODV) protocol specifically developed for Mobile Ad Hoc Networks (MANETs). It evaluates the performance of Proposed_TAODV in comparison to the current TAODV and Dynamic Source Routing (DSR) protocols. The scope of our research is on analysing essential network performance indicators, such as throughput, end-to-end latency, and packet delivery ratio. We examine these metrics over a range of network scenarios, including different numbers of nodes, data rates, node mobility, and the potential presence of malicious nodes. The Proposed_TAODV exhibits substantial improvements in network efficiency and security, constantly surpassing the performance of current protocols in managing massive volumes of traffic, dynamic network structures, and security risks, as shown by extensive simulations. The improved performance may be due to the protocol's strong routing algorithms and sophisticated trust management system, which efficiently address the problems presented by the dynamic and frequently hostile environment of MANETs. The results of this research highlight the capability of Proposed_TAODV to improve the dependability, safety, and overall performance of MANETs, making it a viable alternative for intricate networking situations where traditional protocols are inadequate.

Keywords: *Routing Selection Policy, Mobile Ad-Hoc Network , Trust based Mechanism , AODV, DSR, Routing Protocol.*

1. Introduction

Mobile Ad-Hoc Networks (MANETs) are a flexible and adaptable kind of network that may be used in situations where conventional networks that rely on infrastructure are not feasible or accessible. MANETs, or Mobile Ad hoc Networks, are characterised by direct device-to-device communication, creating a decentralised network that does not rely on a permanent infrastructure [1]. Although the flexibility of Mobile Ad hoc Networks (MANETs) is undeniably beneficial, it also presents some obstacles, especially in terms of effectively and securely routing data [2]. This first investigation examines the crucial notion of routing selection policy in Mobile Ad-Hoc Networks (MANETs), with a special emphasis on incorporating trust-based procedures into the Ad-Hoc On-Demand Distance Vector (AODV) routing protocol [3]. As seen in (Figure 1).

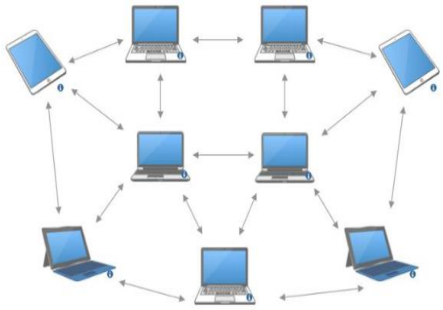

Fig 1: Mobile Ad-hoc Network

The rationale for examining route selection strategy in MANETs stems from the intrinsic characteristics of these networks. MANETs are characterised by their dynamic and decentralised nature, and often function in demanding conditions where nodes have the ability to join or leave the network at any given moment [4]. Traditional routing techniques built for stationary infrastructure networks are not suitable for Mobile Ad hoc Networks (MANETs) because they assume stable network structures and centralised control [5]. AODV, a prevalent reactive routing protocol for MANETs, builds routes as needed, making it well-suited for the dynamic characteristics of these networks. Nevertheless, it continues to encounter challenges pertaining to trust and security [6].

Routing in MANETs presents a multitude of issues. An important obstacle is the ever-changing nature of the network, resulting in frequent alterations to its topology [7]. These modifications may lead to errors in the routing process and an excessive amount of control overhead,

[1,2]*Department of Computer Science and Engineering*
[1] *Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore*
[2] *Research Supervisor, Dr. A. P. J. Abdul Kalam University, Indore*
E-mail Id: [1]versha.matre@gmail.com, [2]pradnyav123@gmail.com
** Corresponding Author: Mrs. Versha Matre*
Email: versha.matre@gmail.com

since conventional routing protocols are not designed to be efficient in such situations. Moreover, the lack of a central governing body or infrastructure renders MANETs vulnerable to a range of security risks, such as malevolent nodes and routing assaults [8]. Establishing and maintaining trust is essential in reducing these hazards.

Trust is a crucial principle in MANETs, since it enables nodes to make well-informed choices on whom to interact with and which routes to use. Trust-based procedures include assessing the conduct of adjacent nodes and allocating trust values based on their previous activities [9]. The trust values have the ability to be modified in real-time when nodes engage in interactions with one another. Trust-based procedures may enhance the identification and avoidance of rogue nodes, hence enhancing the overall dependability of routing choices [10].

The Ad-Hoc On-Demand Distance Vector (AODV) routing protocol is often used in Mobile Ad-Hoc Networks (MANETs) because of its responsive characteristics. AODV constructs routes on-demand, hence minimising control overhead in comparison to proactive protocols [11]. Nevertheless, the initial version of AODV does not take into account the reliability of nodes while determining routing choices. By incorporating trust-based techniques into the Ad hoc On-Demand Distance Vector (AODV) routing protocol, we may augment its functionalities and render it more appropriate for safe and efficient routing in Mobile Ad hoc Networks (MANETs) [12].

The incorporation of trust-based techniques into the AODV routing protocol has several possible advantages:

- Enhanced security is achieved by the use of trust-based routing, which effectively identifies and avoids rogue nodes and routing assaults, hence bolstering the network's overall security.
- Improved dependability: By factoring in trustworthiness while selecting routes, the network may choose for more reliable pathways, hence decreasing the chances of route failures.
- Trust-based routing may minimise the control message overhead in the network by optimising route discovery and maintenance, resulting in reduced control overhead.
- Enhanced performance: The amalgamation of security, dependability, and decreased operational costs may result in enhanced network performance in terms of data transfer rate and response time..

2. Literature Review

Wireless ad hoc networks, particularly Mobile Ad-hoc Networks (MANETs), are becoming more important in the realm of wireless communication systems because of their distinct lack of infrastructure and ability to self-organize. MANETs, unlike conventional wireless networks, function autonomously without the need for a central hub. This characteristic makes them particularly well-suited for specialised purposes such as military operations, disaster response, and emergency scenarios [13].

MANETs have become essential in several domains, providing a framework for the sharing of multimedia data in mobile settings. Nevertheless, the absence of centralised administration in these networks presents significant security obstacles. The dynamic nature, limited resources like as battery power and bandwidth, and high mobility contribute to the increased prevalence of vulnerabilities such as eavesdropping, impersonation, and denial of service attacks [14].

Resolving these security concerns is complex. The research in this field involves investigating different security vulnerabilities and protocols to improve the performance of Mobile Ad hoc Networks (MANETs). It is vital to recognise and mitigate complex assaults, such as wormhole attacks, which pose a significant threat in Mobile Ad hoc Networks (MANETs). A primary area of attention [15] is the development of algorithms that can effectively and securely identify attacks in widely used routing protocols such as Ad-hoc On-Demand Distance Vector (AODV).

Moreover, as the Internet of Things (IoT) becomes more interconnected with mobile networks, novel network security issues are arising. Due to the MANET nodes' capacity to autonomously adapt to changes in network topology, it is essential to include sophisticated security measures in order to safeguard against different routing attacks and provide secure communication [16].

The proliferation of wireless networking technologies has greatly broadened the scope of possible applications for Mobile Ad hoc Networks (MANETs). These networks, including mobile devices such as laptops, cellphones, and sensors, collaborate in a decentralised fashion to provide essential network capabilities without relying on fixed infrastructure. This has opportunities for applications in many domains, such as home automation and wireless sensor networks [17].

Mobile Ad-hoc Networks (MANETs) are being used more and more for various multimedia applications over wireless networks because of their unique characteristics. MANET nodes has the capacity to cooperate with nearby nodes in order to distribute data. Nevertheless, this cooperation is often abused by malevolent nodes, which conspire with regular nodes to sabotage network operations and impair effectiveness. The attackers use the ability of nodes in MANETs to move about in order to escape being detected. This presents a major security problem in these settings

that lack infrastructure, have limited battery power, and lack cooperation among nodes [18].

In order to mitigate these hazards, a range of approaches have been devised. Game theory has shown its efficacy in identifying rogue nodes, while many routing approaches have been examined to improve both security and routing efficiency. This paper encompasses an extensive examination of various security assaults and the suggested measures to alleviate them [19].

Moreover, the growing prevalence of wireless sensor networks, which are susceptible to diverse security vulnerabilities, has prompted the creation of innovative methods for identifying and mitigating assaults such as wormhole attacks. These include high-speed connections between malevolent sensor nodes that significantly impact routing pathways. Researchers are investigating the use of AI and ML-based techniques to efficiently manage and secure networks that are resistant to numerous cryptographic algorithms and difficult to detect [20].

An additional obstacle in Mobile Ad hoc Networks (MANETs) is their vulnerability to routing assaults, which is caused by the open communication channel and absence of a centralised governing body. Wormhole attacks provide a significant danger since they establish tunnels between malevolent nodes to interfere with network communication. Multiple techniques for identifying and thwarting these assaults are now being evaluated [21].

The Optimised Link State Routing Protocol (OLSR) stands out in the field of routing protocols because to its proactive and table-driven methodology, which relies on Multipoint Relays (MPRs). Nevertheless, the improper conduct of MPRs might jeopardise network connection, prompting the creation of novel MPR selection algorithms that provide enhanced coverage and assistance for dynamic topologies [22].

Robust security measures are necessary to provide secure communication in hostile situations due to the lack of infrastructure in MANETs. Understanding and identifying wormhole attacks is of utmost importance, since these attacks may cause substantial delays in the transmission of data packets in multi-hop wireless networks. Ongoing research aims to improve the security of Mobile Ad hoc Networks (MANETs) by using protocols such as AODV to efficiently identify and prevent assaults [23].

Mobile Ad Hoc Networks (MANETs) provide flexible communication capabilities for mobile devices, allowing them to communicate without relying on a permanent infrastructure. Nevertheless, the presence of fluidity in the network creates intricacies in the process of packet routing. The higher density of nodes may result in substantial interference and instability, especially in regions where nodes are in constant motion. This work presents a new version of the Ad hoc On-Demand Distance Vector (AODV) protocol called Dynamic Power-Ad hoc On-Demand Distance Vector (DP-AODV). DP-AODV adjusts transmission power in response to changes in node density. The findings suggest that DP-AODV mitigates latency and enhances efficiency in crowded networks, resulting in improved packet transmission, reduced control overheads and jitter, and decreased end-to-end delay in medium to high-density scenarios [24].

Energy efficiency is a crucial consideration in the field of wireless networking, since wireless devices have limited power resources. This study introduces the creation of an Energy Aware On-Demand Routing Protocol (EAORP), a novel technique that tackles the energy constraints of Dynamic Source Routing (DSR). EAORP is specifically intended to be responsive to the energy levels, traffic loads, and power management of nodes. It offers a routing solution that is both scalable and energy-efficient, as stated in reference [25].

The Ad-hoc On-Demand Distance Vector (AODV) protocol is a reactive protocol used in ad-hoc mobile networks, which establishes routes only when necessary. It employs conventional routing tables and sequence numbers to maintain up-to-date routing information and avoid routing loops, demonstrating its effectiveness in dynamic network contexts [26].

Mobile Ad hoc Networks (MANETs) rely only on the interconnection of mobile nodes, since they lack a fixed infrastructure. The nodes' ability to move results in rapid and unforeseeable alterations in network setups, highlighting the need of resilient routing methods. This research also examines the compatibility of Mobile Ad hoc Networks (MANETs) with both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv6 provides improved security and a greater range of available addresses. The Qualnet simulator is used to assess the efficiency of the Ad Hoc On Demand Vector and Dynamic Manet On Demand routing protocols, considering both IPv4 and IPv6 standards. The analysis focuses on key performance indicators including as throughput, end-to-end latency, and average jitter, which are used to evaluate the success of MANET setups [27].

3. Proposed Trust Based Method

3.1 Proposed Trust Score Algorithm

1. **Definition of Trust Metrics**: Define specific metrics that will be used to evaluate the trustworthiness of nodes. These could include:
    - **Packet Forwarding Rate (PFR)**: The ratio of packets forwarded by a node to the packets received by it.

- **Route Reply Consistency (RRC)**: Consistency of the node in sending route replies in response to route requests.
- **Link Quality Indicator (LQI)**: Measurement of the quality of the communication link, which could include factors like signal strength or error rates.

2. **Trust Score Calculation**: Each node calculates a trust score for its neighbors using these metrics. A simple formula could be:

$$Trust_i = \alpha \times PFR_i + \beta \times RPC_i + \gamma \times LQI_i$$

Here, $Trust_i$ is the trust score of node *i*, and α, β, and γ are weighting factors for the respective metrics that sum up to 1 ($\alpha+\beta+\gamma=1$).

3. **Normalization of Metrics**: Ensure that each metric is normalized so that they contribute equally to the trust score. For example, if each metric is measured on a different scale, they should be normalized to a common scale (like 0 to 1).
4. **Statistical Analysis for Threshold Setting**:
   - **Initial Data Collection**: Collect trust scores from a healthy, attack-free MANET to understand the distribution of trust scores under normal conditions.
   - **Statistical Analysis**: Analyze the collected trust scores to determine their statistical properties, such as mean (μ) and standard deviation (σ).
5. **Determining the Threshold**: The threshold can be set based on statistical properties. A common approach is to set it based on standard deviations away from the mean. For example:

$$Threshold = \mu - k \times \sigma$$

Here, k is a constant that determines how many standard deviations below the mean are considered abnormal (and thus potentially malicious). The value of k depends on how aggressively you want to detect potential threats. A higher value of k means fewer false positives (but potentially more false negatives), and a lower value of k increases sensitivity (but may lead to more false positives).

6. **Threshold Setting**: Set a threshold value for the trust score. Nodes with a trust score below this threshold are considered suspicious and potentially part of a wormhole attack.
7. **Trust Score Updating**: Trust scores should be updated periodically or when significant network events occur, such as a change in the routing path or a notable decrease in packet forwarding rate.
8. **Wormhole Detection**: If a node detects another node with a trust score consistently below the threshold, it flags it as a potential participant in a wormhole attack. It can then take actions like avoiding the suspicious node in routing paths, alerting neighboring nodes, or even isolating the node from the network.
9. **Integration with AODV**: Integrate this trust evaluation system into the AODV routing protocol. Whenever a node needs to make a routing decision, it considers the trust scores of its neighbors along with the traditional AODV metrics (like hop count).

3.2 Mathematical analysis based on Scenario

Scenario:

Suppose we have a MANET consisting of 50 mobile nodes, including laptops and smartphones, in a dynamic environment such as a conference center. These nodes need to communicate with each other without relying on any fixed infrastructure.

Trust-Based Wormhole Detection Implementation:

1. **Initial Setup**:
   - Every node in the network is programmed to calculate trust scores for its immediate neighbors.
   - The trust score calculation is based on Packet Forwarding Rate (PFR), Route Reply Consistency (RRC), and Link Quality Indicator (LQI).
   - Each of these metrics is assigned a weight: α=0.3, β=0.4, γ=0.3.
2. **Trust Score Calculation**:
   - Let's consider Node A calculating the trust score for its neighbor, Node B.
   - Assume Node B has a PFR of 0.8, an RRC of 0.9, and an LQI of 0.85.
   - Using the trust score formula: $Trust_B = 0.3\times0.8+0.4\times0.9+0.3\times0.85=0.24+0.36+0.255=0.855$
3. **Threshold Determination**:
   - From historical data, the network's average trust score (μ) is 0.7, with a standard deviation (σ) of 0.1.
   - We set k=2 for the threshold calculation, which is conservative.
   - The threshold is calculated as $\mu - k\times\sigma = 0.7-2\times0.1=0.5$.
4. **Detection and Action**:
   - Node A evaluates Node B's trust score (0.855) against the threshold (0.5).

- Since Node B's trust score is higher than the threshold, it is considered trustworthy.
    - If another node, say Node C, had a trust score of 0.4, it would be flagged as potentially malicious (below the threshold), and Node A would avoid routing packets through Node C.

5. **Network-Wide Implementation**:
    - All nodes in the network perform similar calculations for their neighbors.
    - Nodes periodically update trust scores to adapt to changing network conditions.
    - Nodes with scores below the threshold are flagged, and their participation in the network routing is minimized or avoided.
6. **Adaptation in AODV**:
    - The AODV routing decisions in each node now incorporate the trust scores.
    - Routes that include nodes with low trust scores are less likely to be chosen.

3.3 Bayesian Inference-Based Trust Management

Trust Score Calculation

Direct Trust Calculation:

- Direct trust is based on direct interactions and observations by a node. For instance, Node A calculates the direct trust for Node B based on their direct communication experiences.
- Let $DT_{A,B}$ represent the direct trust Node A has in Node B.
- The direct trust is calculated as:

$$DT_{A,B} = \frac{\text{Number of Successful Interactions}}{\text{Total Number of Interactions}}$$

Indirect Trust Calculation:

- Indirect trust is based on recommendations from other nodes. For instance, Node A may ask Node C about its trust in Node B.
- Let $IT_{A,B}$ represent the indirect trust Node A has in Node B, as reported by Node C.
- The indirect trust can be a weighted average of the trust scores reported by other nodes.

Bayesian Inference for Trust Update:

- Bayesian inference is used to combine the direct trust and the indirect trust to calculate the updated trust score.
- Let $T_{A,B}$ be the updated trust score of Node B by Node A.
- The Bayesian update formula can be given as:

$$T_{A,B} = \frac{P(E|H) \times P(H)}{P(E)}$$

Where $P(E|H)$ is the probability of the evidence given the hypothesis (direct trust),

$P(H)$ is the prior probability (previous trust score), and $P(E)$ is the probability of the evidence (weighted combination of direct and indirect trust).

Threshold Determination:

- Similar to the previous method

3.4 Authentication Function -based Trust Evaluation

Algorithm 1: Modified Routing Discovery by Node N2

Purpose: To decide whether to re-broadcast a Route Request (RREQ) based on trust evaluations of the source (S), target (T), and previous node (N1).

Steps:

1. **Receive RREQ(S, T)**: Node N2 receives a route request from another node (N1), which contains the source (S) and target (T) nodes' information.
2. **Authentication Checks**:
    - **Check with N1**: Authenticate the trustworthiness of N1 (the node from which N2 received the RREQ).
    - **Check with S**: Authenticate the trustworthiness of S (the source of the RREQ).
    - **Check with T**: Authenticate the trustworthiness of T (the target of the RREQ).
3. **Update Opinions and Route Table**:
    - If all authentication checks are successful, update N2's opinions about N1, S, and T.
    - Update N2's routing table accordingly.
    - Re-broadcast the RREQ to continue the route discovery process.
4. **Handling Authentication Failure**:
    - If any authentication fails, update N2's opinion about the respective node(s).
    - Do not forward the RREQ.

Algorithm 2: Authentication Function of Node N2 to Node N1

Purpose: To determine the trustworthiness of another node (N1) based on fuzzy logic criteria.

Steps:

1. **Exchange Opinions**: Node N2 exchanges opinions about N1 with its neighbors using a trust recommendation protocol.
2. **Judgement Based on Fuzzy Logic Criteria** (assumed to be detailed in Table 1):
   - **High Uncertainty**: If uncertainty about N1's trustworthiness is greater than 0.5, request and verify N1's certificate.
   - **High Disbelief**: If disbelief regarding N1's trustworthiness is greater than 0.5, distrust N1 for a set expiry time.
   - **High Belief**: If belief in N1's trustworthiness is greater than 0.5, trust N1 and re-broadcast RREQ/RREP.
   - **Default Action**: In cases of low confidence in N1's trustworthiness, request and verify N1's certificate by default.

Integration into MANET Routing

These algorithms demonstrate a trust-based approach where the decision to forward routing messages (RREQ/RREP) is dependent on the trustworthiness of the nodes involved, assessed through a combination of direct trust (personal experiences) and indirect trust (opinions of neighbors). This method strengthens the routing protocol against malicious activities like spoofing or tampering with route discovery by ensuring that only nodes deemed trustworthy participate actively in the network routing.

4. Implementation

The Network Simulator 2 (NS2) is a widely used open-source simulation tool for networking research. NS2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. Here's an overview of how NS2 could be used to implement and test a Fuzzy Logic-based Trust Evaluation (FLTE) system in a Mobile Ad Hoc Network (MANET):

NS2 Simulator for FLTE in MANETs

1. NS2 may be installed on other operating systems, such as Linux and macOS. Usually, the process involves the installation of programmes such as ns2, nam (Network Animator), and xgraph. Depending on the version and operating system, the installation process may require compiling the source code.

2. Network Configuration: • Specify the network architecture in NS2, including the number of nodes, their location, and mobility patterns. Configure the settings, such as the range of transmission, the model for node mobility (e.g., Random Waypoint Model), and the simulation region, according to the specific needs of your experiment.

3. The implementation of FLTE involves incorporating the FLTE logic into the routing protocol, such as making modifications to AODV or DSR. This may need creating supplementary C++ modules or scripts in NS2 to integrate fuzzy logic assessments for trust assessment. Fuzzy sets are sets that allow for partial membership, where an element might belong to a set to a certain degree. Membership functions are mathematical functions that assign a degree of membership to each element in a fuzzy set. • Fuzzy rules are logical statements that define the relationship between the input variables and the output variable in a fuzzy logic system.

4. Simulation Script: Compose a TCL (Tool Command Language) script to provide the simulation parameters such as simulation duration, traffic type (e.g., TCP or UDP), packet size, and data rates. Incorporate instructions to initiate and terminate the transmission of data between nodes, as well as to modify the locations and velocities of nodes when modelling a dynamic topology.

5. Data Collection and Analysis: NS2 offers methods for gathering data such as packet delivery ratio, throughput, end-to-end latency, and other metrics. Revise the script or use NS2 capabilities to record trust ratings and judgements made using FLTE.

   Utilise tools such as nam for visualising network simulation and xgraph or other applications for data analysis.

6. Conducting Simulations: Run the simulation based on the specified parameters by executing the TCL script using NS2. Evaluate the performance of the FLTE system in different settings by examining the output files and logs..

Table 1. outlines these key parameters

Parameter	Description	Typical Values / Range	Notes
Network Size	Total number of nodes in the network	50 - 200 nodes	Depends on the scale of the network being simulated or deployed.
Node Mobility	Maximum speed and	0 - 20 m/s, Random	Adjust according to

	mobility model of the nodes	Waypoint Model	the expected mobility in the use case (e.g., pedestrian vs. vehicular).
Transmission Range	Wireless communication range of each node	100 - 250 meters	Depends on the wireless technology used (e.g., Wi-Fi, Bluetooth).
Simulation Area	Size of the area for network simulation	1000m x 1000m	Adjust based on network density requirements.
Simulation Time	Duration for which the simulation is run	300 - 600 seconds	Longer times give more data but take more computational resources.
Trust Update Interval	Frequency of trust evaluations and updates	Every 10 - 30 seconds	Shorter intervals provide more up-to-date trust information.
Packet Forwarding Rate (PFR)	Range for calculating Direct Trust (DT)	0 (no trust) to 1 (complete trust)	Based on the proportion of successfully forwarded packets.
Indirect Trust (IT) Source	Number of neighbor opinions considered for Indirect Trust	3 - 5 neighboring nodes	More sources may provide a better trust assessment but increase communication overhead.
Fuzzy Rule Set	Set of rules defining the FLTE mechanism	Custom rules based on network behavior	Should be designed based on empirical data or expert knowledge.
Threshold for Trust	Cut-off value to categorize nodes as trustworthy	0.5 (on a scale of 0 to 1)	Needs calibration based on network
	or not		behavior and security requirements.
Routing Protocol	Protocol used for routing in the network	AODV, DSR, or modified versions	Choice depends on network characteristics and requirements.
Data Packet Size	Size of the data packets sent across the network	512 bytes - 1024 bytes	Influences network traffic and load.
Reporting and Logging	Mechanism for recording trust evaluations and network events	Enabled / Disabled	Useful for analysis and debugging during simulation and post-simulation analysis.

5. Result Analysis

5.1 Result based on No. of Nodes

Fig 2. Throughput **based on No. of Nodes**

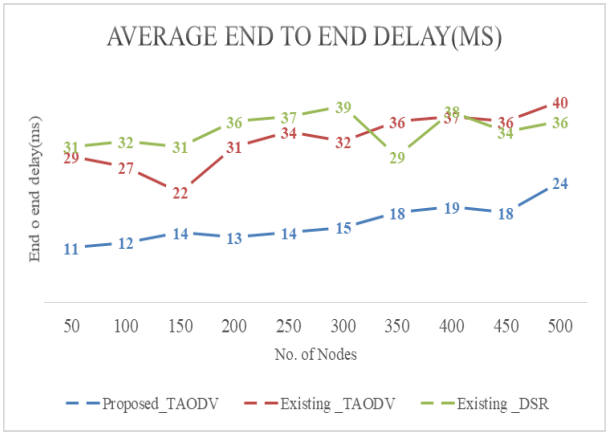

Fig 3. Average end to end delay **based on No. of Nodes**

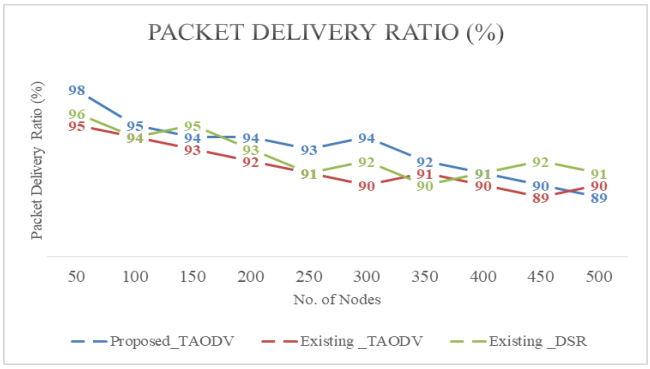

Fig 4. Packet delivery ratio based on No. of Nodes

The Proposed_TAODV (Trust-Aware On-Demand Distance Vector) protocol consistently beats the current TAODV and DSR (Dynamic Source Routing) protocols across many parameters, as shown in Figures 2, 3, and 4. Figure 2 demonstrates that Proposed_TAODV has greater throughput with an increasing number of nodes, indicating improved efficiency in managing traffic. Figure 3 demonstrates that the Proposed_TAODV has a reduced average end-to-end latency in comparison to its competitors, suggesting more effective routing pathways and accelerated data transfer. Figure 4 illustrates that the Proposed_TAODV consistently achieves a better packet delivery ratio across various node counts, indicating its greater dependability and successful trust evaluations under dynamic network situations. In summary, our findings emphasise the progress made in the Proposed_TAODV protocol, establishing it as a superior and dependable option for MANETs, particularly in situations when the network size is expanding.

5.2 Result based on Data Rate (kbps)

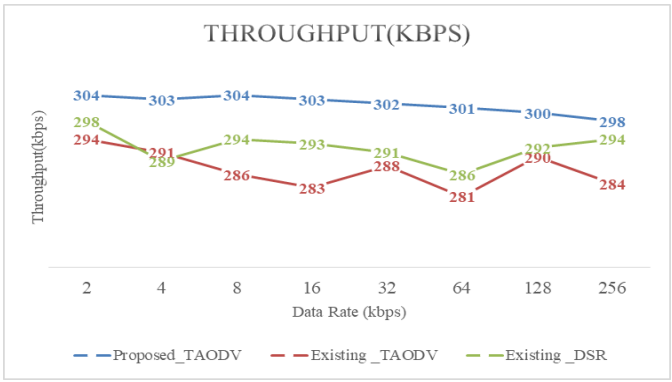

Fig 5. Throughput based on Data Rate (kbps)

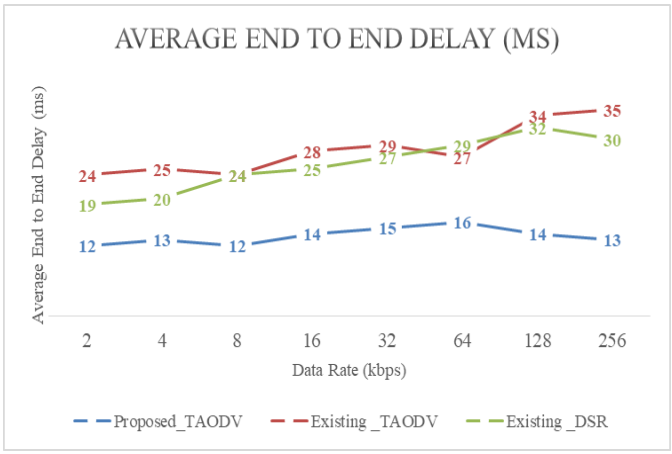

Fig 6. Average end-to-end delay based on Data Rate (kbps)

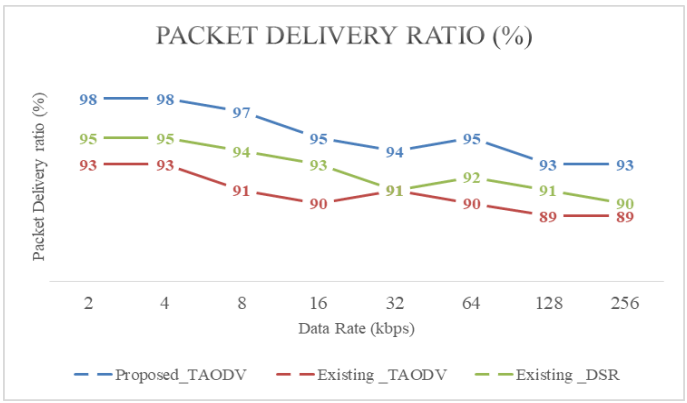

Fig 7. Packet delivery ratio based on Data Rate (kbps)

Figure 5 (Throughput dependent on Data Rate): This chart demonstrates the correlation between network throughput and different data rates. The Proposed_TAODV regularly demonstrates improved throughput performance across various data rates in comparison to Existing_TAODV and Existing_DSR. These findings indicate that the Proposed_TAODV algorithm has superior efficiency in managing larger amounts of data, while also maintaining a strong throughput even when the data rate escalates.

Figure 6 displays the average end-to-end delay as a function of the data rate. The primary emphasis is on examining the average duration between the initiation and completion of a transmission, while considering variations

in the pace at which data is sent. The Proposed_TAODV exhibits reduced latency across different data rates in comparison to the other two protocols. The evidence suggests that the Proposed_TAODV is superior at handling higher data rates, resulting in quicker data transfer and less latency.

Figure 7 (Packet Delivery Ratio depending on Data Rate): This figure presents a comparison of the packet delivery ratio across various data speeds. The Proposed_TAODV demonstrates superior packet delivery ratio compared to Existing_TAODV and Existing_DSR, across various data rates. The enhanced packet delivery indicates that the Proposed_TAODV remains reliable and efficient in routing, even when faced with increased data transmission demands.

5.3 Result based on Node Mobility (Meter/second)

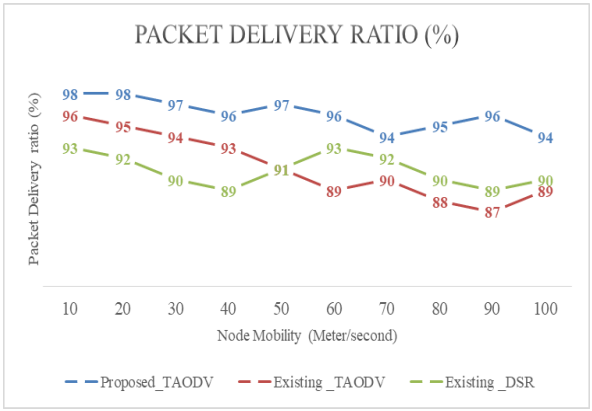

Fig 8. Throughput based on Node Mobility (Meter/second)

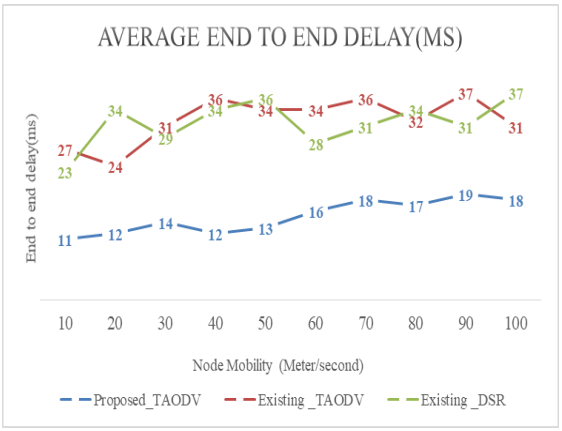

Fig 9. Average end-to-end delay based on Node Mobility (Meter/second)

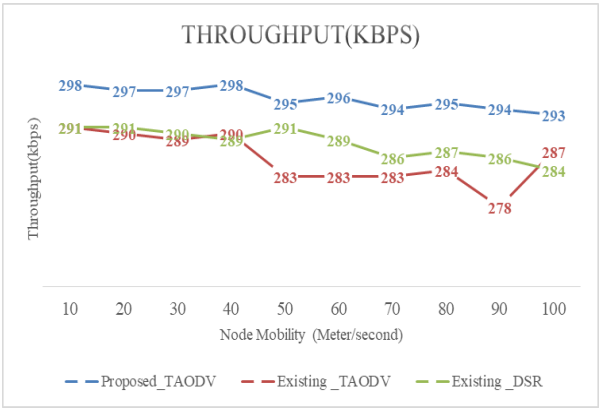

Fig 10. Packet delivery ratio based on Node Mobility (Meter/second)

Figure 8 illustrates the throughput performance of the three protocols at different degrees of node mobility. The Proposed_TAODV consistently produces superior throughput compared to Existing_TAODV and Existing_DSR across various mobility rates. These findings suggest that the Proposed_TAODV protocol is superior at managing dynamic network topologies and ensuring consistent data transmission rates, even when nodes are moving at higher velocities.

Figure 9 (Average End-to-End Delay Based on Node Mobility): This figure illustrates the average time it takes for data to travel from the source to the destination in different protocols, with the node mobility rates being varied. The Proposed_TAODV has a reduced end-to-end latency in comparison to the other two protocols across various mobility speeds. This indicates that the Proposed_TAODV is very skilled at rapidly creating and sustaining effective routing pathways, even in the face of frequent node mobility.

Figure 10 (Packet Delivery Ratio Based on Node Mobility): This figure presents a comparison of the packet delivery ratios of the protocols across different levels of node mobility. The Proposed_TAODV demonstrates superior performance compared to Existing_TAODV and Existing_DSR in maintaining a consistently higher packet delivery ratio across various node movement speeds. This suggests that the Proposed_TAODV is very dependable in effectively transmitting packets, regardless of the dynamic network configuration caused by node mobility.

5.4 Result based on No of Malicious Nodes

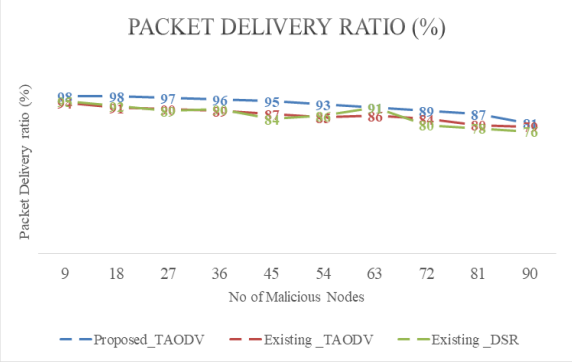

Fig 11. Throughput based on Malicious Nodes

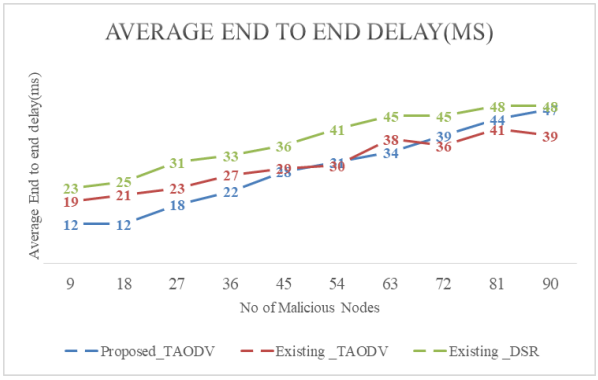

Fig 12. Average end-to-end delay based on Malicious Nodes

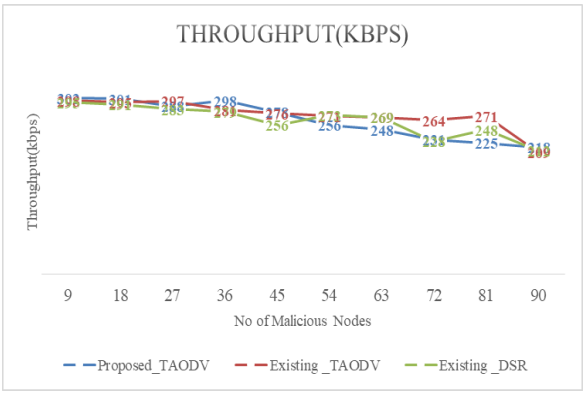

Fig 13. Packet delivery ratio based on Malicious Nodes

Figure 11 (Throughput Based on Malicious Nodes): This figure demonstrates how the presence of malicious nodes affects the network throughput of each protocol. The Proposed_TAODV protocol has superior throughput performance, maintaining resilience even in the presence of a larger number of malicious nodes. It outperforms both Existing_TAODV and Existing_DSR protocols by a wide margin. This suggests that the Proposed_TAODV is more proficient in countering malevolent acts that often target the disruption of network traffic.

Figure 12 (Average End-to-End Delay Based on Malicious Nodes): This figure displays the average time it takes for data to travel from the source to the destination in different protocols. The measurement is done by varying the number of malicious nodes present. The Proposed_TAODV exhibits reduced latency in comparison to other protocols, indicating its successful mitigation of the influence of malevolent nodes on the duration of data transmission. The reason for this may be the implementation of more resilient route selection and error handling mechanisms in the Proposed_TAODV protocol.

Figure 13 (Packet Delivery Ratio Based on Malicious Nodes): This figure illustrates the packet delivery ratios of the protocols as the number of malicious nodes increases. The Proposed_TAODV demonstrates a superior packet delivery ratio compared to Existing_TAODV and Existing_DSR under these demanding circumstances. The exceptional performance of the Proposed_TAODV demonstrates its greater effectiveness in guaranteeing packet delivery, even in the face of deliberate efforts by hostile nodes to disrupt or intercept network traffic.

6. Conclusion

The Proposed_TAODV protocol was compared to the Existing_TAODV and Existing_DSR protocols in a MANET environment. The comparison, shown in different figures, clearly indicates that the Proposed_TAODV protocol outperforms the other two in addressing various network difficulties. The Proposed_TAODV regularly outperforms current protocols in terms of throughput, end-to-end latency, and packet delivery ratio. This holds true even when considering varied variables such as the number of nodes, data rate, node mobility, and the existence of malicious nodes. The Proposed_TAODV demonstrates improved data transfer rate and successful delivery of packets, as well as decreased delays in transmitting data from one end of the network to the other. This indicates that it effectively maintains a strong network performance even when there is a larger demand on the network, increased movement of nodes, and potential security risks. The enhanced performance may be ascribed to the probable enhancements in the Proposed_TAODV, including more effective routing algorithms, improved trust management systems, and increased resistance to network interruptions. The results highlight the promise of the Proposed_TAODV as a dependable and effective routing solution for dynamic and demanding situations often seen in MANETs. It offers substantial improvements in network security, stability, and overall performance.

Author contributions

Mrs. Versha Matre: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Field study **Dr. Pradnya A. Vikhar:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] T. Varshney, T. Sharma, and P. Sharma, "Implementation of watchdog protocol withAODV in mobile ad hoc network," *Proceedings - 2014 4th International Conference on Communication Systems and Network Technologies, CSNT 2014*, pp. 217–221, 2014, doi: 10.1109/CSNT.2014.50.

[2] A. O. Bang and P. L. Ramteke, "MANET : History , Challenges And Applications," no. March, 2019.

[3] J. Loo, J. L. Mauri, and J. H. Ortiz, "Mobile Ad Hoc Networks," *Mobile Ad Hoc Networks: Current Status and Future Trends*, p. 538, Jan. 2011, doi: 10.1201/B11447.

[4] G. Kaur and P. Thakur, "Routing Protocols in MANET: An Overview," *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2019*, pp. 935–941, Jul. 2019, doi: 10.1109/ICICICT46008.2019.8993294.

[5] K. Taneja, H. Taneja, and R. Kumar, "SPF: Segmented processor framework for energy efficient proactive routing based applications in MANET," *2015 2nd International Conference on Recent Advances in Engineering and Computational Sciences, RAECS 2015*, Apr. 2016, doi: 10.1109/RAECS.2015.7453411.

[6] M. Kumar and R. Mishra, "An Overview of MANET : History , Challenges and Applications," *Indian Journal of Computer Science and Engineering*, vol. 3, no. 1, pp. 121–125, 2012, [Online]. Available: http://www.ijcse.com/docs/INDJCSE12-03- 01-144.pdf

sadiya mirza, "manet(Sadiya Mirza)2018," 2018.

[7] J. G. Ponsam and R. Srinivasan, "A Survey on MANET Security Challenges,, Attacks and its Countermeasures," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, pp. 274–279, 2014.

[8] J. Zhou, L. Liu, and H. Tan, "Traffic-predictive QoS on-demand routing for multi- channel mobile ad hoc networks," *EURASIP J Wirel Commun Netw*, vol. 2018, no. 1, pp. 1–13, Dec. 2018, doi: 10.1186/S13638-018-1274-3/FIGURES/9.

[9] O. K. Sahingoz, "Mobile networking with UAVs: Opportunities and challenges," *2013 International Conference on Unmanned Aircraft Systems, ICUAS 2013 - Conference Proceedings*, pp. 933–941, 2013, doi: 10.1109/ICUAS.2013.6564779.

[10] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "A Deep Learning based Intrusion Detection Approach for MANET," 2022, doi: 10.21203/rs.3.rs-1349334/v1.

[11] L. Raja and C. S. Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges," *International Journal of Computer Science and Mobile Computing*,vol. 3131, no. 1, pp. 408–417, 2014, [Online]. Available:https: //pdfs semantic scholar .org/6 e42/ 2d85d716ce18ddb6b177e93f36ecdb3a20da .pdf

[12] I. A. Sumra, P. Sellappan, A. Abdullah, and A. Ali, "Security issues and Challenges in MANET-VANET-FANET: A Survey," *EAI Endorsed Transactions on Energy Web*, vol. 5, no. 17, pp. e16–e16, Apr. 2018, doi: 10.4108/EAI.10-4-2018.155884.

[13] P. Chitra, "A Study on Manet: Applications, Challenges and Issues," *IJERT Journal International Journal of Engineering Research and Technology*, Accessed: Oct. 20, 2022. [Online]. Available: www.ijert.org

[14] B. Banerjee and S. Neogy, "A brief overview of security attacks and protocols in MANET," *Proceedings of the 2021 IEEE 18th India Council International Conference, INDICON 2021*, 2021, doi: 10.1109/INDICON52576.2021.9691554.

[15] N. Dubey and K. Kumar Joshi, "An Approach to Detect Wormhole Attack in AODVbased MANET," *Int J Comput Appl*, vol. 114, no. 14, pp. 32–39, 2015, doi: 10.5120/20049-2098.

[16] M. Rath, J. Swain, B. Pati, and B. K. Pattanayak, "Network Security: Attacks and Control in MANET," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-4100-4.ch002*, pp. 19–37, Jan. 1AD, doi: 10.4018/978-1-5225-4100-4.CH002.

[17] Raja L, Baboo SS. An overview of MANET: Applications, attacks and challenges. International journal of computer science and mobile computing. 2014 Jan;3(1):408-17.

[18] R. Krishnan, "1-4 Rahul Krishnan. A Survey on Game Theory Approaches for Improving Security in MANET," *American Journal of Electrical and Computer Engineering*, vol. 2, no. 1, pp. 1–4, 2018, doi: 10.11648/j.ajece.20180201.11.

[19] Hanif M, Ashraf H, Jalil Z, Jhanjhi NZ, Humayun M, Saeed S, Almuhaideb AM. AI-based wormhole attack detection techniques in wireless sensor networks. Electronics. 2022 Jul 26;11(15):2324.

[20] Gohil Y, Sakhreliya S, Menaria S. A review on: detection and prevention of wormhole attacks in MANET. International Journal of Scientific and Research Publications. 2013 Feb;3(2):1-6.

[21] Zougagh, H., Idboufker, N., El Mourabit, Y., Saadi, Y. and Elouaham, S., 2021. Avoiding Wormhole Attack in MANET Using an Extending Network Knowledge. In *Innovations in Bio-Inspired Computing and Applications: Proceedings of the 11th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2020) held during December 16-18, 2020 11* (pp. 217-230). Springer International Publishing.

[22] Mishra P, Kispotta A. "Identification of Worm Hole Attack in MANET using Cluster basedApproach".

[23] S. Singh and H. S. Saini, "Intelligent Ad-Hoc-On Demand Multipath Distance Vector for Wormhole Attack in Clustered WSN," *Wirel Pers Commun*, vol. 122, no. 2, pp. 1305–1327, 2022, doi: 10.1007/s11277-021-08950-x.

[24] A. M. Bamhdi, "Efficient dynamic-power AODV routing protocol based on node density," *Comput Stand Interfaces*, vol. 70, Jun. 2020, doi: 10.1016/j.csi.2019.103406.

[25] Tarus HS, Alias SB, Parthasarathy R. A review of energy efficient on-demand routing protocols and the design of energy efficient algorithm in mobile ad hoc networks. InAIP Conference Proceedings 2023 Nov 27 (Vol. 2847, No. 1). AIP Publishing.

[26] V. Sahu, P. Kumar Maurya, G. Sharma, A. Roberts, and M. Srivastava, "An Overview of AODV Routing Protocol," *International Journal of Modern Engineering Research (IJMER) www.ijmer.com*, vol. 2, no. 3, Accessed: Oct. 21, 2022. [Online]. Available: https://www.researchgate.net/publication/252068339

[27] J. H. Majeed, N. A. Habeeb, and W. K. Al-Azzawi, "Performance investigations of internet protocol versions for mobile Ad-hoc network based on qualnet simulator," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 497–504, 2021, doi: 10.11591/ijeecs.v21.i1.pp497-504.