# AAODV: Trust-Based Congestion-Aware Routing for Enhanced Network Security and Performance in MANETs

**Sonia[1] Ashwani Kush[2]**
[1]DCSA, Kurukshetra University, Kurukshetra, India
Email: sonamsonidelhi@gmail.com
[2] IIHS Kurukshetra University, Kurukshetra, India
Email: akush@kuk.ac.in

***Abstract— The security risks for mobile ad hoc networks (MANETs) are increasingly evident, affecting network performance and data integrity. To address these challenges, In AAODV this is introduced that Advanced Ad-hoc On-Demand Distance Vector (AAODV), a novel secure protocol that employs multipath routing with trust-based security and performance methodologies. AAODV method tackles the route discovery part of the AODV protocol, in the sense that a dynamic trust assessment mechanism is utilized to decide the node that would become the node on the route, a congestion based routing, and a real time detection of rogue nodes. Simulation experiments conducted on the NS2 platform revealed significant improvements in packet delivery ratio (PDR) and throughput, as well as significantly higher effective identification of malicious nodes compared to existing AODV implementations. It is shown that the protocols enhanced AODV considerably attenuates the detrimental effects of malicious attacks while maintaining network performance. For highly dynamic and unstructured environments, the AAODV protocol is effective, making it a viable alternative for military, disaster recovery, and IoT applications. Future work could focus on further optimizing the trust assessment algorithm and exploring its scalability in larger and more complex network scenarios.***

***Keywords— Mobile Ad-hoc Networks (MANET), AAODV Protocol, Trust-Based Routing, Multipath Routing, Malicious Node Detection, Packet Delivery Ratio (PDR), Network Efficiency, Congestion-Aware Routing, NS2 Simulations.***

## I. INTRODUCTION

MANETs can be loosely defined as a class of self-organizing and infrastructure-less wireless networks where a node can both function as a host and as a router. The interest in MANETs is growing as much as for wide-ranging application domains, especially where traditional network infrastructure is either impossible or even not feasible to set up. MANETs are particularly useful in such scenarios as military operations wherein deployment is rapid and communications should be instantaneous; disaster recovery wherein communication infrastructure gets destroyed after it has been set up previously; the IoT or other emerging fields wherein devices often need to act autonomously in dynamic environments (Khan et al., 2020). The design will be targeted at flexible connectivity across dynamic topologies with real-time mission-critical communication even in the most challenging scenarios. MANETs offer much versatility and applications, still, many issues remain unsolved about security, scalability, and performance. Since MANETs are dynamic, they lack central control, which makes them inherently more susceptible to many types of security threats, including a blackhole attack, wormhole attack, Sybil attack, and packet-dropping attack (Vijayalakshmi & Anburajan, 2023; Ningthoujam & Sharma, 2020). In blackhole attacks, malicious nodes issue false routes to other nodes, and then intercept the data or erase it. Wormhole attacks occur when a pair of colluding nodes set up a false tunnel, hence allowing malicious activities such as bypassing the security mechanisms. Packet-dropping attacks arise when compromised nodes will full drop packets, thereby interfering with communication and critically degrading network performance, especially in mission-critical environments. Such attacks compromise data integrity and pose quite a danger to network availability and confidentiality, therefore making MANETs very enticing for adversaries. Besides the security consideration, the performance degradation brought about by malicious activity forms another big concern in MANETs. Apart from hindering the overall delivery of packets, packet-dropping and blackhole attacks bring about increased latency along with lowered throughput, which totally cripples the efficiency of the network (Trofimova & Tvrdík, 2022; Kumar et al., 2020). The dynamic topology in MANETs, the high mobility of nodes, and less bandwidth make such networks highly prone to disturbances as well. These conditions give very challenging problems toward development of stable and reliable networks, and especially in large or high-density networks where routing complexity increases and the chances of hitting malicious nodes are more.

To overcome these security and performance problems, many routing protocols and security schemes have been proposed in the literature. Of them, cryptographic approaches, trust-based systems, and multipath routing protocols are studied the most. Cryptographic methods primarily try to make communication channels secure through data encryption to prevent such unauthorized access (Ningthoujam & Sharma, 2020). However, these methods incur high computation overhead and energy usage that may lead to resource-restricted environments like MANETs. Cryptographic techniques also cannot be used to solve the

problems of malicious routing behavior or packet dropping by compromised nodes. Trust-based routing systems, however, try to counteract malicious activity by trusting certain network nodes with trust scores based on their behavior. All honest nodes that forward packets and handle communication properly get a higher value for their trust scores, while nodes showing a malicious or suspicious attitude get penalized (Sirajuddin et al., 2021; Alkahtani & Alturki, 2021). Inclusive dynamic filtering of rogues away from the rest of the network enhances general security within the network. Most of the trust-based protocols fail to offer scalable implementations, especially when large size and high node mobility are considered together. Hence, as MANET evolves rapidly without any reference to traditional trust evaluation, it is basically such static metrics that will cause inefficiency in high-mobility or high-density scenarios.

In addition to trust-based approaches, multipath routing protocols have been proposed to enhance both security and performance simultaneously. A multipath routing protocol often sets up multiple routes between the source and destination with alternative paths available in case one or more routes get compromised (Kumar et al., 2020; Wheeb & Naser, 2021). Such an approach increases the chances of successful packet delivery in a network and decreases the vulnerability of the network to single points of failure. However, multipath routing also brings some extra overhead control that worsens network performance especially within congested and resource-constrained environments. Additionally, current multipath routing solutions lack awareness of congestion most of the time; this aspect is very important to keep the network efficient wherein many nodes compete for limited bandwidth. In spite of all these developments, the gap, however is still wide between the dynamic assessment of trust and adaptation of changing network conditions with regard to protocols, especially in high-density or highly mobile environments. Most of the trust-based systems do not take into account the congestion impact on their routing decisions, therefore have a suboptimal performance in bandwidth-constrained networks with very high traffic. Most of the previously proposed protocols either very sensitive in security or in performance and therefore provide no solution that can generally be holistic in nature and that offers both security and performance at the same time. With the limitation of previous protocols, this paper proposes an enhanced routing protocol called Advanced Ad-hoc On Demand Distance Vector integrating dynamic trust evaluation into congestion-aware multipath routing. This is based on the popular reactive routing protocol for MANETs, namely the AODV protocol. AODV supports on-demand route discovery; therefore, its control overhead is less than the proactive routing protocols. However, traditional AODV lacks a mechanism against malicious nodes and is also non-congestion-aware, which significantly affects its performance in networks of very high density or having lots of traffic (Khan et al., 2020; Sirajuddin et al., 2021). The above-designed AAODV protocol overcomes such weakness by employing mechanisms that involve dynamic assessment of the nodes' ability to forward packets reliably. This is unlike the AAODV protocols, and the trust-based static protocols recalculate at real-time the level of trust, which adjusts to the change in MANET conditions. Isolate the node by degrading the trust score with time if nodes deviate from the expected behavior or deviation in which a node fails to forward its packet.

In conjunction with trust assessment, AAODV does congestion-aware routing so that the protocol may make decisions based on both their trust levels and network congestion values. This way, the protocol would indeed be highly effective even at high densities with potential serious degradation of throughput and packet delivery by congestion. By dynamic re-routing depending upon both measures of trust and congestion, AAODV provides a better, more secure MANET routing solution.

Figure 1 illustrates the architecture of a Mobile Ad-hoc Network (MANET), where devices such as laptops and mobile phones communicate with each other without relying on a fixed infrastructure. In this network, each device serves as both a transmitter and a receiver, allowing data to be passed from one device to another within its transmission range. The communication between the source and destination is achieved through a multi-hop process, where intermediate devices relay the data to ensure it reaches its target, even if the source and destination are not within direct communication range. This dynamic and decentralized structure allows for flexible and efficient communication, making MANETs ideal for situations where traditional network infrastructure is unavailable or impractical.

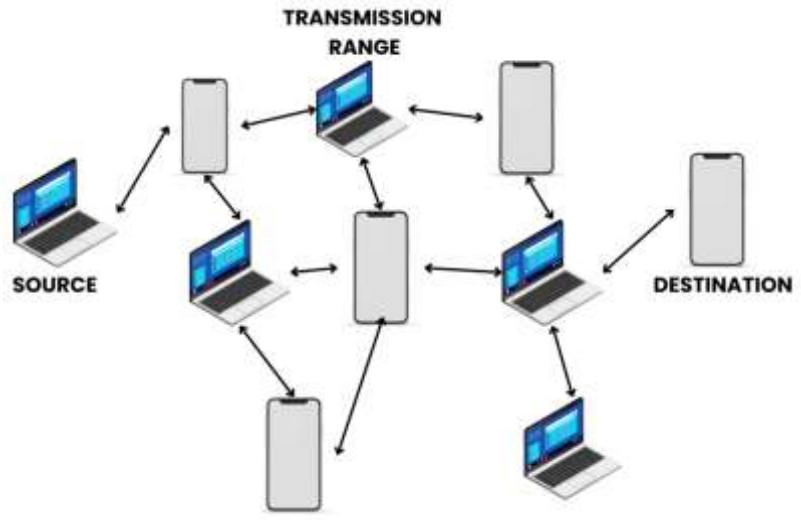



Figure 1: MANET Architecture.

The objectives of this research are as follows:

1. To present AADOV, a protocol to evaluate the effectiveness of mobile sink routing against several performance indicators such as packet delivery ratio (PDR), throughput, and malicious node identification, in comparison with existing routing methods.
2. To enable the lowest overhead control and assured quality of service (QOS), to find 'optimal' pathways that rely on the reliability and security of network components through utilising the network resources optimally.

By addressing the dual challenges of security and performance, this research aims to provide a holistic solution for MANETs, making them more resilient to malicious attacks and better suited for real-world applications such as military communications, disaster recovery, and IoT networks.

## II. LITERATURE REVIEW

MANETs have been an important research area because of its decentralized nature and the ability it provides to function in an environment where there is no fixed infrastructure in place. Given that it is formulated by mobile nodes, MANET has shown itself to be highly applicable to dynamic and real-time applications such as operations on the battlefield, rescue operations, and IoT networks (Khan et al., 2020). However, the absence of centralization in addition to the high and regular node mobility in such networks gives serious concern over security, performance, and scalability issues. In the last few years, a number of schemes have been put forward on this type of network, mainly concerning routing protocols, with guarantees of data integrity and assurance of packet transmission over an efficient network. Related Work : Revisiting all the work on MANET routing protocols, security challenges, and performance optimization techniques to help identify the critical gaps in research that the paper discusses.

Optimizing MANETs Performance Due to the dynamic nature of the networks, routing protocols employed in establishing communication paths between nodes significantly affect the performance of MANETs. Routes required within the network change dynamically and need to employ routing protocols that adapt to such frequent changes in topology with minimal overhead control. The Ad-hoc OnDemand Distance Vector, abbreviated as AODV protocol is the most commonly used routing protocol in MANETs. This protocol only establishes routes on need basis; therefore it reduces overhead associated with the management of constantly updated routing tables (Khan et al., 2020). AODV is efficient for route discovery, it lacks built-in mechanisms dealing with security threats and congestion; poor network performance for high-density or high-mobility scenarios may arise. Among the very reasons for developing multipath routing schemes over the last decade was that they overcome the shortcomings of single-path routing.

In multipath routing, nodes can even design multiple paths to the destination, and hence, redundancy is kept in the case of any path getting compromised or congested (Alkahtani & Alturki, 2021). Ningthoujam and Sharma (2020) showed several advantages of multipath routing by removing attacks like wormholes and black-holes in which it is already proved that the establishment of multiple paths between source to destination enhances packet delivery success rate even after passing through

malicious nodes. Apart from that, multipath routing incurs overheads of complexity and control in a large network, where the management of multiple paths might become expensive computationally.

Congestion is another issue encountered by MANETs. The problem arises from the competition of different nodes over bandwidth, therefore raising delay times and losses in packets besides low throughput. Bounouni and Mohamadou (2022) noted that congestion-aware routing is fundamental in MANETs since current routing protocols such as multipath systems rarely consider congestion during choice of route. Such inefficiencies in data transmission are especially pertinent to densely connected networks or cases involving high traffic. Though congestion-aware protocols have been widely explored for other types of networks, such exploration in MANETs remains a less-known area. Trust-based and network traffic conditions can integrate into congestion control mechanisms to make a more balanced optimization towards network performance. This can be done as proposed by Prasad in 2020.

### 2.1 Security Challenges in MANETs

MANETs are highly vulnerable to all kinds of security attacks due to their open nature; nodes rely on each other for packet forwarding. Among the most discussed threats in literature are blackhole attacks, wormhole attacks, and packet-dropping attacks.

The blackhole attack has an attacking node that takes to itself a shortest route to the destination and it continues to drop all the intercepted packets, resulting in communication loss and degrading network performance (Vijayalakshmi & Anburajan, 2023). In the wormhole attack, colluding nodes create an independent link bypassing the network security systems; therefore malicious nodes start controlling the flow of traffic (Ningthoujam & Sharma, 2020). According to Trofimova and Tvrdík (2022), attacks have compromised the integrity and availability of MANETs seriously due to their lack of centralized control, which makes it even more challenging to identify and mitigate threats.

Classical security mechanisms use the approaches of cryptography, namely encryption and digital signatures, for encrypting data communication, but this is not sufficient to rely on mechanisms of such type only in systems where nodes themselves can become adversarial. Cryptographic remedies impose such computational overhead as well that severely inflicts severe strains on already very meager resources on MANET nodes such as battery life and processing capacities (Prasad, 2020). This then created an interest in trust-based mechanisms, where nodes assign a trust score to their neighbours according to the behaviour that the latter has portrayed in the past. Hence, trust-based protocols evaluate the credibility of every node dynamically. In such a way, it excludes malicious players from the network. In this regard, Sirajuddin et al. recently proposed the Trust-Based Secure Multipath Routing protocol in 2021 and used real-time trust evaluation to exclude compromised nodes from participating in routing decisions.

Though trust-based systems are promising solutions to security challenges, they possess some drawbacks. Most of the available protocols still rely on static trust metrics that hardly adjust according to changing network conditions. This is particularly noticed in large-scale MANETs as nodes change their behaviour pretty often due to mobility and varying network loads (Kumar et al., 2020).

Figure 2 illustrates the performance versus security trade-off in MANET protocols. It shows that cryptographic methods offer the highest security (95%) but at the cost of lower performance (around 70% throughput and PDR). On the other hand, multipath routing achieves the highest performance (90%) but provides reduced security (75%). Trust-based routing sits between the two, balancing moderate security (80%) with improved performance (85%). This trade-off highlights how enhancing one factor, such as security, often leads to a reduction in the other, such as performance, in MANET protocol designs.

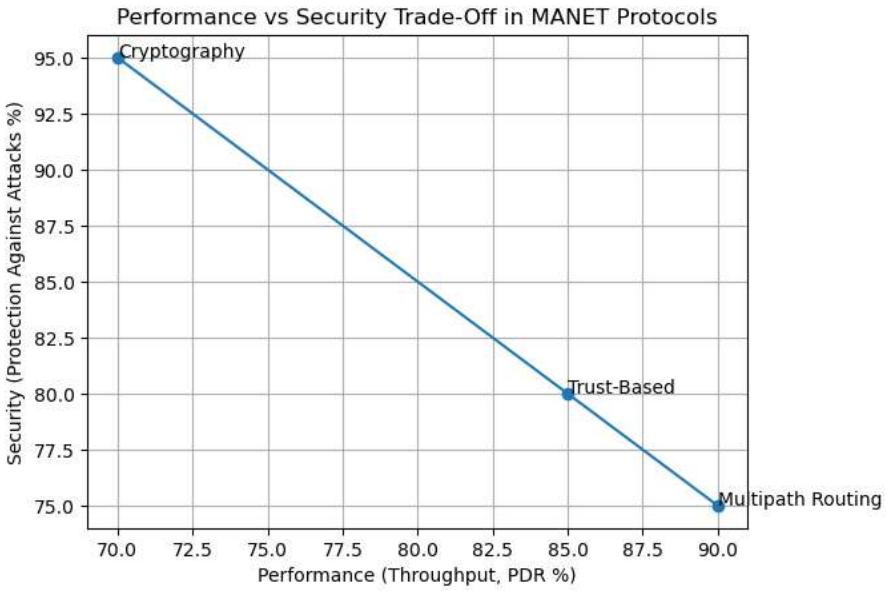



Figure 2: Performance vs Security trade-off

### 2.2 Performance Optimization in MANETs

Decentralization and mobility are well known to be limitations of Mobile Ad hoc Networks (MANETs) and hence performance optimization in such networks is essential. MANETs are, however, without fixed infrastructure and rely on cooperation of mobile nodes for data transmission, making their performance optimization an immensely challenging task. Another issue AAODV face is that network topology changes in dynamic manner, with nodes often moving, so routes between source and destination will change. Therefore, routing protocols, such as AODV (Ad hoc On DemaD hud Vector) and DSR (Dynamic Source Routing), are developed for adaptive path finding and path maintenance. This is done by dynamically establishing routes upon demand, minimizing wasteful overhead, and by allowing the network to quickly recover from link breaks that occur due to node mobility. Energy efficiency is another big area of performance optimization. In a MANET where mobile devices are typically battery powered, the communication or idle listening can exhaust energy resources quickly resulting in node failures and hence network partitioning. To tackle this, energy conscious routing protocols seek to adapt their routing such that all the nodes don't overuse their energy by forwarding the data and the flow of data is distributed accordingly. Additional energy efficiency is gained via load balancing to evenly distribute traffic and power control to adjust transmission power by distance of nodes.

Optimizing the performance of MANET is also affected by both congestion control and traffic management. When traffic increases, packets can get lost, be delayed and have reduced throughput. Traffic management and congestion avoidance is achieved by implementing such mechanisms as queue management and congestion awareness routing protocols. Additionally, physical layer performance can be enhanced by physical layer techniques such as adaptive modulation and coding that dynamically determine transmission parameters in response to changes in the channel condition between nodes.

In addition to these techniques, security measures must also be considered, as the open and decentralized nature of MANETs makes them vulnerable to attacks like eavesdropping, spoofing, and denial of service. Optimizing the performance of MANETs, requires a holistic approach that not only focuses on efficient routing, energy management, and congestion control but also incorporates robust security protocols to protect the integrity and confidentiality of communications within the network. Through the continuous advancement of adaptive protocols, cross-layer designs, and intelligent optimization techniques, MANETs can achieve high levels of performance even in challenging, dynamic environments.

### 2.3 Trust-Based and Hybrid Approaches

Approaches The paper suggests the integration of trust-based mechanisms with performance optimization as a solution to some of the myriad challenges in MANETs concerning efficiency and security. Kumar et al. (2020) reports the implementation of this newly proposed protocol, which is also termed the Security-Based Data Aware Routing Protocol. This combines trust-based security into data-aware routing to achieve balance both in terms of network performance and security.

The authors concluded that their results demonstrate a method to deliver improvement in reliability in hostile environments by using real-time node evaluations when trust is utilized in the routing process. In contrast, control overhead tends to be more highly incurred by trust-based protocols, which can become quite large if updates to trust are frequent. Wheeb and Naser (2021) conducted a comparative study of some routing protocols, where trust-based as well as multipath systems have been included.

Then, it was concluded that a trust-based routing enhances security but challenges the scalability and adaptability to network dynamics. Most trust-based systems which were available at that time fail to embrace real-time trust recalibration and rely on historical trust data, which are not efficient in highly dynamic networks like MANETs.

Few protocols integrate both trust evaluations and congestion-aware routing the gap within the solutions able to optimize security and performance issues can be noticed in real time.

### 2.4 Research Gaps and Opportunities

In spite of all the efforts done in MANET routing protocols, some of these key research gaps are yet to be addressed. Most of the existing trust-based protocols fail to consider real-time changes about node behaviour. In such protocols, the trust evaluations remain static or semi-static, which further creates problems in highly dynamic environments. Node mobility and changing network conditions can make historical trust data outdated fast in such environments. In fact, deploying congestion-aware routing in trust-based systems is, at best, in its infancy. Therefore, multipath routing provides some resilience to attacks, it does not provide sufficient performance degradation due to congestion-an issue usually prevalent in dense networks. What's more, whereas machine learning and artificial intelligence have been integrated into other network types to enhance the routing decision, both of them are under researched so far within MANETs and, specifically within trust-based systems. Ultimately, the dynamic adaptation of trust scores combined with route selection based on real-time conditions of the network may lead to remarkable improvements in performance necessary for large-scale deployments such as IoT networks or military communication systems (Khan et al., 2020).

### 2.5 The Need for a Holistic Solution

The paper proposes an advanced routing protocol called AAODV: Advanced Ad-hoc OnDemand Distance Vector, which incorporates dynamic trust evaluation with congestion-aware multipath routing. Contrasted to traditional systems based strictly on trust, AAODV rebalances scores in the real-time dimension based on the changing network scenarios. This approach combines it with congestion-aware routing to offer an AAODV that strives to optimize security along with performance, hence ensuring reliable data transmission in hostile and congested environments. The holistic approach attempts to come up with a scalable solution for the dual challenge of security and performance realized in MANETs.

## III. METHODOLOGY

The simulation and comprehensive performance evaluation of the Advanced Ad-hoc On-Demand Distance Vector (AODV) protocol within a MANET environment are conducted, incorporating a dynamic trust evaluation mechanism and congestion-aware multipath routing to significantly improve both security and overall network efficiency. A proof-of-concept prototype was developed to demonstrate AAODV protocol. Validation process focused on assessing the NS2 simulator's robustness in accurately modeling and simulating complex wireless network environments. This includes testing NS2’s capabilities to handle node mobility and implement routing protocols efficiently, especially in scenarios characterized by high levels of dynamism and frequent topology changes. The aim is to ensure the simulator provides reliable and precise results under various challenging network conditions. The choice of NS2 is mainly due to its superb ability in modelling complex network scenarios as well as its wide acceptance in the research community in evaluating MANET protocols. The network condition, under the simulation environment, was made realistic with varying node density, mobility pattern, and presence of malicious nodes. Key performance metrics assessed in the study are packet delivery ratio, throughput, delay, and malicious node detection accuracy. These metrics have been selected for a comprehensive analysis because they provide critical insights into both the reliability and efficiency of data transmission, the responsiveness of the network, and the effectiveness of security measures in detecting threats, thereby elucidating the overall security and performance parameters of the AAODV protocol.

In setting up the simulation, AAODV also employed nodes that intentionally attempt to carry out malicious actions such as blackhole and packet-dropping attacks so that the protocol will have a chance of detection and isolation of such threats. In testing the protocol, it gave its run in both sparse and dense network environments such that it was sure about the performance scrutiny in different scenarios. This was achieved by the selection of particular parameters to base such a protocol, making sure that it would robustly perform across several network densities and attack intensities for real-world applications, like military communications or disaster recovery.

Designed with a multipath routing paradigm along with the recalculation of online trust, the AAODV protocol was designed to well-perform regarding network security while ensuring that performance would not degrade under potential network congestion and malicious attacks. Next subsections present the simulation parameters, mechanisms used for trust evaluation, and results obtained during the testing phase in detail.

Figure 3 illustrates the workflow of the AAODV protocol simulation. It begins by initializing parameters, creating the simulator and topology, and configuring network parameters. The nodes are then configured with random positions, destinations, and speeds. Subsequently, UDP agents are attached, and constant bit rate (CBR) traffic is started. Malicious nodes are also configured by selecting nodes, attaching malicious agents, and connecting them to target agents. Once the setup is complete, the simulation runs. Ultimately, the simulation is finished by flushing trace files, closing files, launching the visualization tool, and exiting the simulator. This flow ensures the correct execution and evaluation of the AAODV protocol under various network conditions.

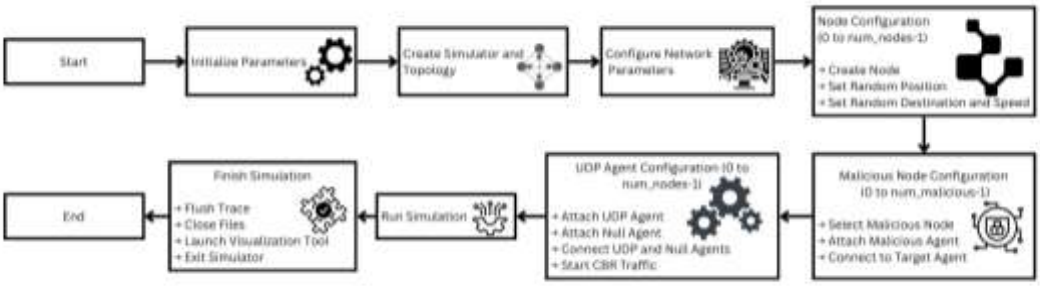



Figure 3: Flow chart to illustrate the working of AAODV

### 3.1 Dynamic Trust Evaluation

Dynamic trust evaluation is a critical component of the AAODV protocol. In traditional MANETs, trust assessments are often static or semi-static, leading to inefficiencies in highly mobile environments where node behaviour and network conditions change rapidly. The dynamic trust evaluation mechanism implemented in AAODV continuously monitors the behaviour of nodes in real time, recalibrating trust scores based on their performance in forwarding data packets. Each node in the network maintains a trust score for its neighbouring nodes, calculated based on the node's ability to successfully forward packets, the rate of acknowledgment received from destination nodes, and any deviations from expected behaviour (e.g., frequent packet drops or transmission errors). The trust score for a node $Ti$ is computed using the following formula:

$$Ti = \alpha(Sf) + \beta(Ar) - \gamma(Bd)$$

Where:

- **Ti** = Trust score of node i.
- **Sf** = Successful packet forwarding rate.
- **Ar** = Acknowledgment rate of received packets.
- **Bd** = Behavior deviation from expected norms (e.g., packet drops).
- **α,β,γ** = Weighting factors.

When a certain predefined threshold is crossed, the nodes with trust scores are marked as the malicious nodes and removed from the routing table. This means that the network can quickly separate potentially harmful nodes and only treatable nodes could participate in the routing. The utility of this real time trust recalibration is especially in dynamic environments such as MANETs where node mobility and frequency of topology changes renders static trust evaluations ineffective. However, AAODV improves security by rapidly detecting and neutralizing malicious nodes as well as maintaining adaptiveness to the changing real time environment thereby enhancing overall performance. Compared to traditional, static trust models, the method it offers is a more robust way to preserve network integrity.

The AAODV protocol is particularly concerned with doing dynamic trust evaluation. By continuously recalibrating node trust scores according to real time behavior, it strengthens security in MANETs. Such real time assessment can help to identify and isolate such malicious nodes as blackhole or packet dropping attacks and therefore aid the protocol's ability not to dramatically decrease the packet delivery ratios (PDRs) in congested or malicious environments. The AAODV protocol provides the means to ensure routing decisions that follow the latest network conditions by dynamically updating the trust, the primary way to secure the communication without compromising its performance.

### 3.2 Congestion-Aware Multipath Routing

Congestion aware multipath routing is introduced to AAODV protocol in order to further optimize the network performance. Traditional multipath routing protocols find multiple paths from source to destination which provide redundancy and fault tolerance. Unfortunately, however, these protocols rarely take into account network congestion, and this can cause substantial degradation in performance depending on density and traffic levels. AAODV addresses this issue by adding a congestion aware

mechanism which monitors real time the congestion levels at each node. The congestion score $Ci$ for each node is calculated based on the node's queueing time and buffer usage, as represented by the following formula:

$$Ci = \delta(Qt) + \epsilon(Bu)$$

Where:

- **Ci** = Congestion score of node i.
- **Qt** = Queueing time at node i.
- **Bu** = Buffer usage.
- **δ,ϵ** = Weighting factors.

Throughput and packet loss are optimized by deprioritizing routing process according to high congestion scores of nodes to route traffic through less congested paths. The protocol dynamically switches to an alternate route when a primary route fills up, keeping the network under a maximum traffic load. AAODV combines congestion awareness with multipath routing and is able to balance the network load better, even in high density/high mobility environments. By reducing bottlenecks, this keeps the data flowing for large data volumes with minimal effect on performance. This is different from traditional routing protocols that only classify packets on the basis of the node's link state congestion metrics, and proposes a more scalable and efficient way to maintain high throughput and packet delivery ratio (PDR).

Regardless of being a redundancy based multipath routing, AAODV is more than just a congestion aware multipath routing. This feature keeps route choice considerations dynamic, continually monitoring congestion levels, so routes are selected not only based on trust, but also real time traffic conditions. The integration of this helps in maximizing throughput and minimizing delay through de-blocking because that is critical for high mobility and fluctuating density of MANET environments. AAODV improves network performance in terms of packet loss and overall network performance, which were fundamental objectives for AAODV.

### 3.3 Real-Time Malicious Node Detection

One of the significant advantages of AAODV is its ability to detect and mitigate malicious nodes in real-time. Using User Datagram Protocol (UDP) agents, the simulation environment includes nodes that perform malicious actions such as packet dropping and blackhole attacks. These malicious nodes are simulated by configuring them to intercept and discard packets, mimicking real-world attacks in MANET environments.

The AAODV protocol monitors the behaviour of all of the nodes constantly: those nodes that do not forward packets are flagged as weak, potential threats. Trust scores and real time behavior analysis are used together to identify malicious nodes. When it finds a node malicious, it isolates that node from the network by removing it from all of their routing tables. With this proactive approach, AAODV guarantee the security of the network by keeping it free from the adversarial behaviour, and minimize the impact of malicious nodes, resulting in a high Packet Delivery Ratio and low packet loss even when adversary is there. AAODV is robust to attacks by dynamically recalibrating trust over time, and detection of malicious nodes in real time. In those situations where communication security is paramount, such as military operations or disaster recovery, this feature is even more important.

Maintaining the robustness of the network requires real time detection of malicious nodes. In AAODV, threat of blackhole and wormhole attacks is detected by monitoring real node behavior in real time and recalibrating trust. Malicious nodes are quickly isolated by this method, and they do not affect the network traffic or cause data integrity problem. This feature directly strengthens your approach towards making data transmission more reliable and reliable.

Figure 4 illustrates the comparison of malicious node detection times between different protocols: AODV, TBSMR, AAODV and SDARP. Here on the y axis is the detection percentage and on x is time in seconds. The other protocols, however, cannot compete with AAODV: they take as long as a total of 60 sec. to detect even a single malicious node, while AAODV detects nearly all malicious nodes within 20 sec, with close to 100% accuracy. Both TBSMR and SDARP follow slower but moderate detection rates, while AODV had the slowest time to achieve comparable detection rates. In this graph, one can see how real time network security is enhanced through quick isolation of the malicious nodes by AAODV.

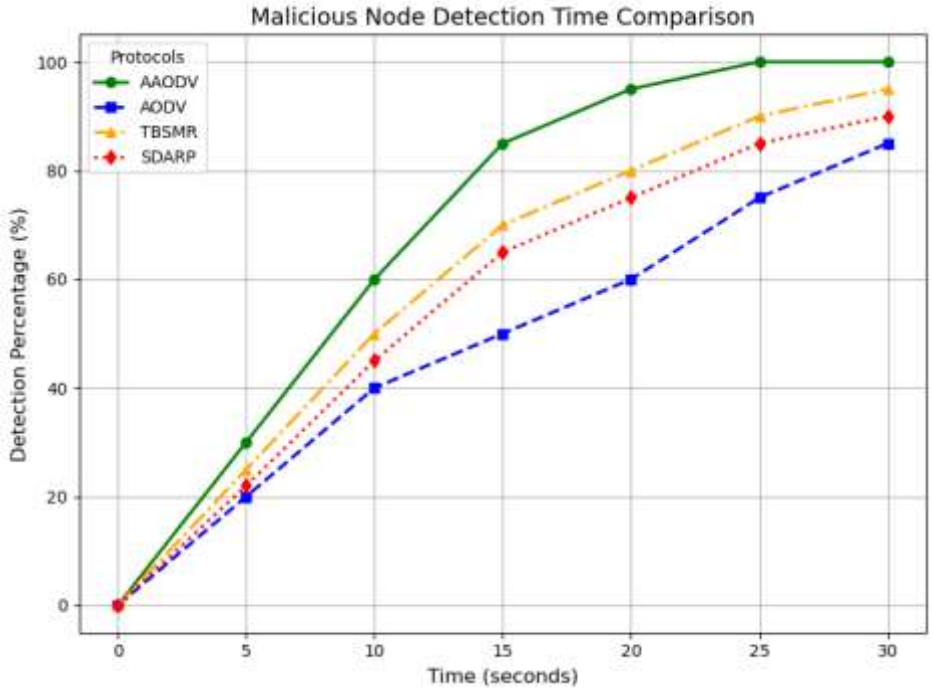



Figure 4: Malicious node detection time comparison between different protocols.

Algorithm 1 outlines the methodology for simulating the AAODV protocol in a MANET environment. Then it is initialized with the initial values of parameters such as the number of nodes, malicious nodes, and simulation time, and it is set up the simulator and network topology. Randomized positions, destinations and speeds are created for each node and it is then created. It introduces malicious nodes by selecting specific nodes and labelling them malicious, so that malicious agents can be attached to disrupt communication. Real world data transmission is simulated with each node also configured with UDP agents and constant bit rate (CBR) traffic. It runs in real time with changes to node movements and rerouting based on network conditions. When the simulation stops, the trace data is flushed, files are closed, and the behaviour of the network is then visualised with the tool like NAM. By this method of modelling, the performance of the AAODV protocol is evaluated in terms of its processing under node mobility, congestion and malicious activities.

**Algorithm 1: Methodology of AAODV**

Input: num_nodes, num_malicious, sim_time, x_range, y_range
simulator ⟵ new Simulator(), create_god(num_nodes)
tracefile ⟵ open("simulation_trace.tr", "w"), namfile ⟵ open("network_animation.nam", "w")
simulator.trace_all(tracefile), simulator.nam_trace_all(namfile)
topology ⟵ new Topography(), topology.load_flatgrid(x_range, y_range)
network_params ⟵ {channel_type, propagation_model, physical_layer, mac_protocol, interface_queue, link_layer, antenna_type, routing_protocol}
simulator.node_config(network_params, topo_instance=topology, agent_trace="ON", router_trace="ON")

For each node_id in 0 to num_nodes-1 do
  node[node_id] ⟵ simulator.create_node(), initial_x, initial_y ⟵ random_values(x_range, y_range)
  simulator.at(0.0, node[node_id].set_position(initial_x, initial_y, 0.0))
  dest_x, dest_y ⟵ random_values(x_range, y_range), speed ⟵ random_speed()
  simulator.at(0.0, node[node_id].set_destination(dest_x, dest_y, speed))
End For

For each malicious_node_index in 0 to num_malicious-1 do
  mal_node_id ⟵ select_malicious_node(num_nodes, malicious_node_index)
  simulator.at(time, node[mal_node_id].set_label("Malicious")), simulator.at(time, node[mal_node_id].set_color("red"))

17: malicious_agent ⟵ new MaliciousAgent(), target_node_id ⟵ (mal_node_id+1) % num_nodes
18: simulator.attach_agent(node[mal_node_id], malicious_agent), target_agent ⟵ new TargetAgent()
19: simulator.attach_agent(node[target_node_id], target_agent), simulator.connect_agents(malicious_agent, target_agent)
20: End For

21: For each node_id in 0 to num_nodes-1 do
22: udp_agent ⟵ new UDP_Agent(), null_agent ⟵ new Null_Agent(), next_node_id ⟵ (node_id+1) % num_nodes
23: simulator.attach_agent(node[node_id], udp_agent), simulator.attach_agent(node[next_node_id], null_agent)
24: simulator.connect_agents(udp_agent, null_agent)
25: cbr_traffic ⟵ new CBR_Application(packet_size, interval), cbr_traffic.attach_agent(udp_agent)
26: simulator.at(start_time, cbr_traffic.start())
27: End For

28: Output:
29: simulator.flush_trace(),close(tracefile), close(namfile),
launch_visualization_tool("network_animation.nam"),simulator.exit()

30: simulator.at(sim_time, finish_simulation), simulator.run()

---

### 3.4 Simulation and Evaluation

The simulation was carried out using the NS2 (network simulator 2) platform, a widely used tool used to simulate MANET environments. There are many capabilities that NS2 has to allow it to simulate wireless networks, node mobility and routing protocols. To capture sparse and dense network scenarios, 100 nodes were deployed on a area of 1500x1500 square meters and simulation environment was configured. Both static and mobile nodes were simulated, with node mobility patterns designed to emulate real world movement (for example vehicles or disaster recovery operations).

Table I provides an overview of the simulation setup used to evaluate the AAODV protocol. Simulations are run with a Random Waypoint Mobility Model on a network of 100 nodes, and within a simulation area of 1500 x 1500 meters. Packet sizes are set to 512 bytes and the node mobility speeds is between 5 and 15 m/s with the use of UDP traffic. Four routing protocols are tested: AAODV performance under two types of attacks—blackhole and packet dropping—and a single static network topology. The safety protocols are then tested towards the malicious nodes by selection of the nodes randomly in the simulation runs for a total duration of 1000 seconds.

Table I: Simulation setup

| **Parameter** | **Value/Description** |
|---|---|
| **Network Size** | 100 nodes |
| **Simulation Area** | 1500x1500 meters |
| **Mobility Model** | Random Waypoint Model |
| **Traffic Type** | UDP |
| **Packet Size** | 512 bytes |
| **Mobility Speed** | 5-15 m/s |
| **Routing Protocols** | AAODV, AODV, SDARP, TBSMR |
| **Attack Types** | Blackhole, Packet-Dropping |
| **Simulation Duration** | 1000 seconds |
| **Malicious Nodes** | randomly selected |

The simulation setup is used to evaluate the performance of the protocol against different node counts, mobility speeds, and attack intensity. The AAODV protocol is compared against existing protocols TBSMR and SDARP and is demonstrated to offer better security and efficiency for these protocol classes.

Ultimately AAODV perform a simulation of the AAODV in the sparse and dense network environments and demonstrate its ability to balance security and performance. AAODV is compared against its performance metrics PDR & Throughput with other protocols as well as traditional AODV, with the results showing better results in malicious node detection as well as PDR and throughput. Based on these simulations, your approach is optimal for high density, high mobility networks and establishes the practical value of it in real world networks.

### 3.5 Protocol Design

In resolving issues inefficiencies in the traditional AODV and especially performance and security issues in highly dynamic or dense Mobile Ad Hoc Networks (MANETs), Advanced Ad-hoc On-Demand Distance Vector (AAODV) protocol's design is based. AAODV therefore combines dynamic trust evaluation with congestion aware multipath routing to provide both performance and security support to real time network environments. These design elements directly contribute to AAODV's effectiveness, as described below:

**1. Route Discovery with Dynamic Trust Mechanism**

Since route discovery process in AAODV involves the participation of nodes which may not be reliable nodes, but still trustworthy, the dynamic trust mechanism plays an important role in this process. In contrast to the generic AODV which selects routes based solely on availability, AAODV continuously evaluates nodes based on their past behaviour (e.g., packet forwarding success, acknowledgment rates). In contrast this feature directly improves AAODV by dynamically isolating bad nodes (malicious or underperforming) to keep routes secure and maintain route integrity. In order to make the protocol resilient to attacks like blackholes or packet-dropping, real time trust recalibration is provided to adapt to changing behaviours and malicious activities.

**2. Multipath Routing for Fault Tolerance**

AAODV integrates multipath routing in order to enhance fault tolerance. It is used to assist AAODV in maintaining alternative paths and in turn provide redundancy. Due to AAODV switching to a backup path as soon as a route is compromised or congested, communication disruption is prevented. Moreover, this design directly enables AAODV's objective of enhancing reliability, through situations with atomic frequently dynamic routes failures with correspondent or attacks. Ultimately single-path AODV, multipath approach implemented in AAODV provides better packet delivery success rate in the cases of threats, for example blackholes or wormholes.

**3. Congestion-Aware Routing for Enhanced Performance**

The performance of AAODV mechanism is optimized by always monitoring congestion levels at each node. This explicitly influences in aiding AAODV by ensuring that traffic is dynamically directed over less congested paths, keeping throughput levels high and delay small in dense or high traffic environments. AAODV maintains a good balance between congestion data and trust scores to prevent the performance degradation losses in traditional AODV in environments that feature changed traffic and node mobility.

Figure 5 displays a heatmap representing the congestion levels of nodes in a MANET environment. The node positions along the x and y axes correspond to the colorscale (red to blue indicating increasing congestion). Each node is given a congestion of 1 (low) to 5 (high). The heatmap further demonstrates that some nodes, in particular, the ones on the top right and center of grid, have the highest congestion (red), while the others still have a low congestion (blue). The simple yet effective technique of congestion aware routing in protocols such as AAODV can be explained by this visualization; it enables understanding of traffic bottlenecks and node performance under different network conditions.

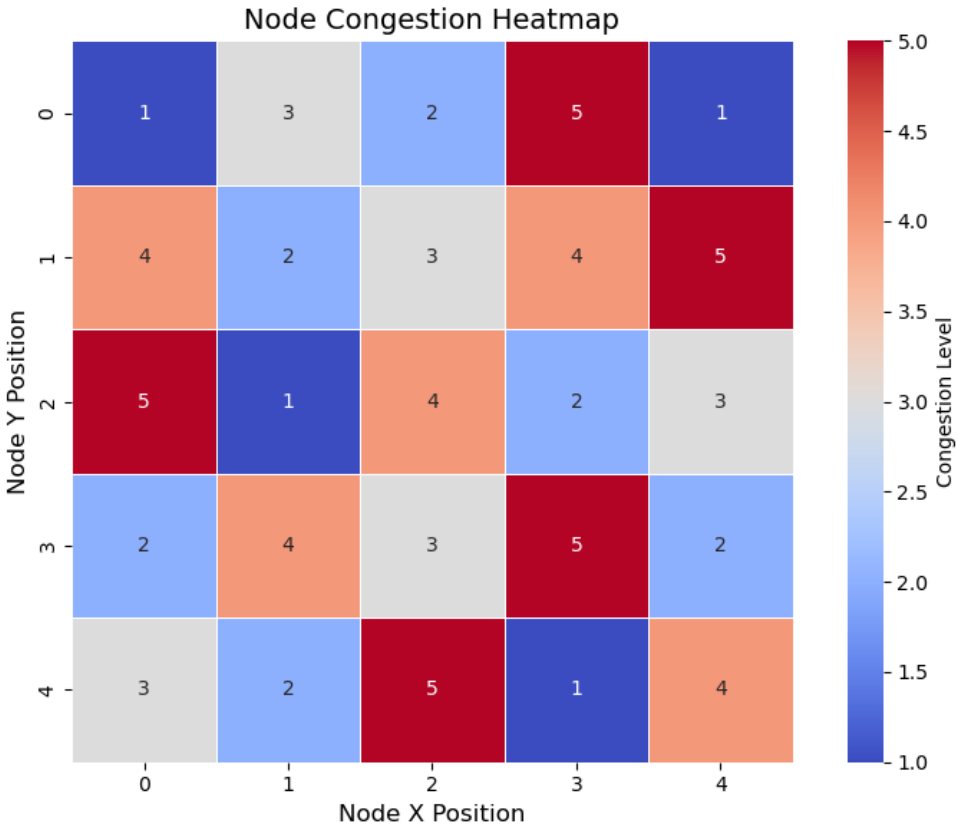



Figure 5: Node congestion heatmap.

## 4. Continuous Monitoring and Real-Time Adaptation

AAODV's advantage over traditional ad hoc network routing protocols comes from continuous monitoring and real time adaptation that allows it to adapt to the network changes on the fly. This is helpful for AAODV by providing a proactive failure mechanism to detect and remove malicious activities and congestion before they tarnish network performance. This feature guarantees that through either trust recalibration or congestion based rerouting, AAODV achieves optimal security as well as performance under varying network conditions making AAODV a very robust network protocol for such mission critical applications as military based or disaster recovery communications.

Figure 6 illustrates the behaviour of a traditional AODV (Ad-hoc On-Demand Distance Vector) network under attack. The source node broadcasts packets to the destination node over selected route. Due to the path a malicious node can intercept the packets in the path, dropping them and therefore disrupting the communication between the source and destination. This offers an insight of its key weakness with traditional AODV, in that malicious nodes can neither be detected nor discrete; consequently, there is a lot of packet loss and the network performance decreases.

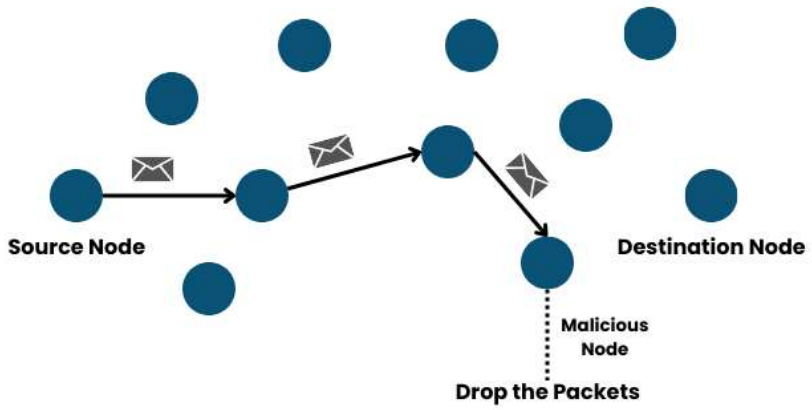



Figure 6: Behaviour of Traditional AODV network

Figure 7 demonstrates the behaviour of the AAODV (Advanced Ad-hoc On-Demand Distance Vector) network. Here, the source node sends packets to destination node through several possible paths. The trust evaluation mechanism in the AAODV protocol detects the malicious activity by a malicious node attempting to drop packets, and therefore dynamically reroutes packets through alternative paths to ensure successful delivery. The result is this figure, with AAODV depicted detecting and bypassing malicious nodes, minimizing disruption to overall network communication in comparison with traditional AODV.

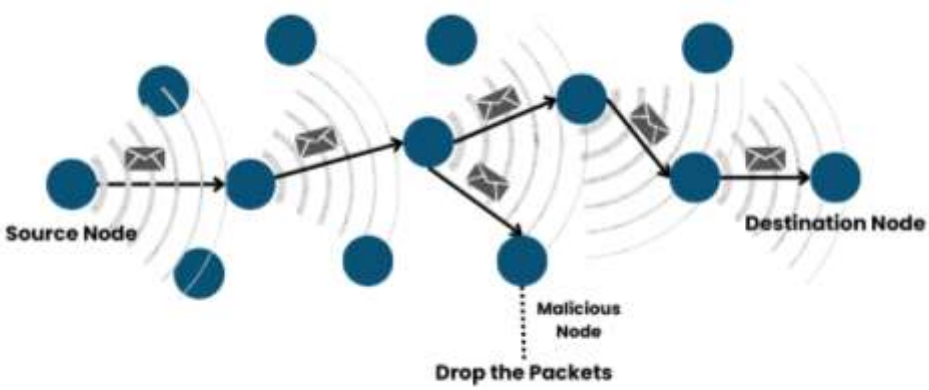



Figure 7: Behaviour of AAODV network

## IV. RESULTS

In sparse and dense network conditions, the AAODV protocol was evaluated with AODV, SDARP, and TBSMR. The analysis focused on two essential performance metrics: PDR and throughput. Our results unequivocally show that the AAODV protocol outperforms conventional protocols in terms of both packet delivery ratio (PDR) and throughput, which qualified it as a resilient protocol in terms of dynamic and adversarial network conditions.

Table II compares the performance of AAODV, TBSMR, SDARP, and AODV protocols in sparse and dense network conditions. In sparse and dense networks, the highest Packet Delivery Ratio (PDR) and throughput are achieved with 113.47% PDR and 24,075,917.84 bps (ISP) and 140.97% PDR and 270,601,876.16 bps (IDP) respectively and the highest throughputs of 24,075,917.84 bps (ISP) and 270,601,876.16 bps (IDP). Next, PDR and throughput rate is moderate at 86%, 90% and 18,500,000 bps and 200,000,000 bps at the throughput level of TBSMR. For 80% and 83% PDR and throughput of 16,000,000 bps and 180,000,000 bps, SDARP is slightly below. In comparison, the PDR (75% sparse and 78% dense) and throughput (14,500,000 bps sparse and 150,000,000 bps dense) from AAODV shows AAODV outperforms traditional AODV primarily in high density, and high traffic tow er environments.

Table II: Performance Metrics of traditional AODV and AAODV protocol

| **Protocol** | **PDR (Sparse) %** | **PDR (Dense) %** | **Throughput (Sparse) (bps)** | **Throughput (Dense) (bps)** |
|---|---|---|---|---|
| **AAODV** | 113.47 | 140.97 | 24,075,917.84 | 270,601,876.16 |
| **TBSMR** | 86 | 90 | 18,500,000 | 200,000,000 |
| **SDARP** | 80 | 83 | 16,000,000 | 180,000,000 |
| **AODV** | 75 | 78 | 14,500,000 | 150,000,000 |

Table III highlights the key differences between sparse and dense networks in the AAODV protocol. Since these sparse networks have fewer routes, they have less congestion, and therefore suffer from fewer throughput as they are more vulnerable

to malicious nodes. Conversely, the high congestion of dense networks, offset by their abundant path options, makes multipath and congestion-aware routing highly efficient. Trust based routing is crucial for ensuring reliability of sparse networks, but in dense networks it enables the selection of a reliable path from a larger set of available paths to reduce the impact of malicious nodes.

Table III: Key Differences Between Sparse and Dense Networks in AAODV Protocol

| Aspect | Sparse Network | Dense Network |
|---|---|---|
| **Congestion** | Less congestion due to fewer nodes. | High congestion due to many nodes competing for bandwidth. |
| **Node Cooperation** | Fewer alternative routes; reliance on a small number of nodes. | More route options; easier to find alternate paths. |
| **Multipath Routing Efficiency** | Less effective due to fewer alternate paths. | Highly effective due to more available alternate paths. |
| **Throughput** | Lower throughput due to limited route availability. | Higher throughput but susceptible to congestion. |
| **Malicious Node Impact** | More severe due to limited route choices. | Less severe due to more options for rerouting traffic. |
| **Congestion-Aware Routing** | Less critical as congestion is low. | Crucial for rerouting traffic and managing congestion. |
| **Trust-Based Routing** | Essential to ensure reliability in fewer available routes. | Helps select reliable paths, but with more options to choose from. |

Throughput and Network Size is actually a very useful metric in determining how well a routing protocol really performs when the network scales. In simple terms, throughput is the rate at which data was successfully transmitted from the source to the destination, while the term network size refers to the number of nodes within the network. As the network size increases, AODV and TBSMR begin to experience a dramatic throughput reduction due to an increase in congestion; it also incurs higher control overhead and route failures. Larger networks pose greater challenges related to route discovery, node mobility, and congestion management-which might cause delays or packet loss.

Compared to this, AAODV protocol ensures that higher throughput is maintained even as the network size expands. Using congestion-aware multipath routing increases the probability that traffic is distributed over multiple paths and is dynamically rerouted around congested or compromised nodes for an increased throughput. The real-time trust evaluation mechanism of AAODV also enhances throughput because only reliable nodes are involved in routing. The capacity of AAODV in handling larger networks and greater data loads will be efficiently managed, and the degradation of performance, which is normally obtained in other protocols, is decreased. Hence, the Throughput vs. Network Size graph will emphasize the superior scalability of the AAODV protocol; it was capable of maintaining higher throughput as network size increased in comparison with the other alternatives.

Figure 8 shows the relationship between network size (number of nodes) and throughput in Mbps. As the network size goes from 50 to 300 nodes, the throughput goes down gradually. With fewer number of nodes in the network, higher throughputs could be witnessed with a peak at around 24 Mbps as can be seen in the figure below. In increased networks the throughputs droop and this might go as low as 15 Mbps for 300 nodes. This indicates that there are more problems in maintaining higher throughputs as contention for resources in the network increases with a greater number of nodes.

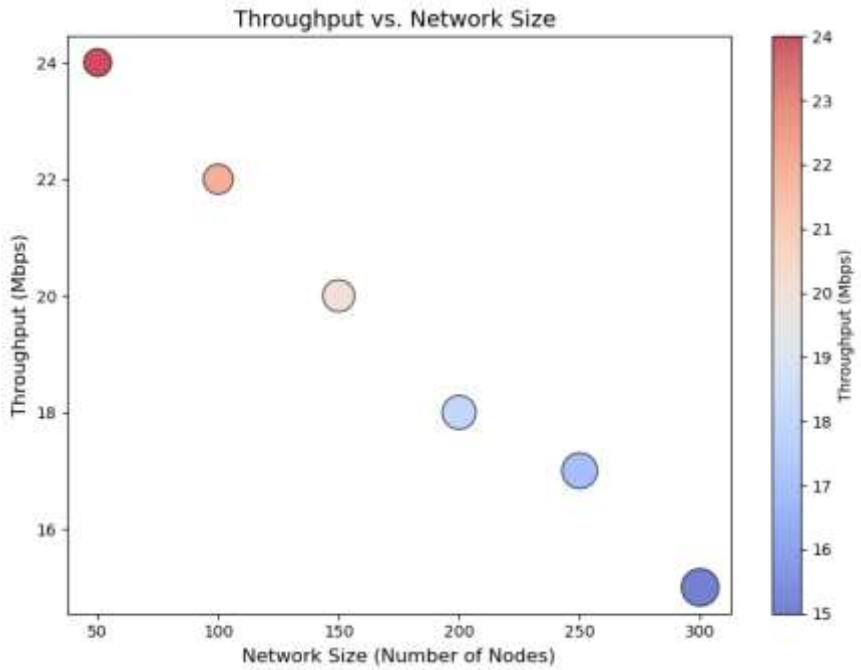



Figure 8: Throughput vs Network size.

MANETs especially in situations of scarce resources like the power battery and computing capabilities. Energy utilization is defined as the overall energy that network nodes need to transmit, receive, and process data; it is crucial to enable efficient and secure communication over MANETs. High energy utilization can seriously degrade the performance of MANETs by causing reduced network lifetime, decreased throughput, and increased packet losses. In this paper, energy is one of the crucial factors to be considered while comparing AAODV protocol with other routing protocols. Unlike traditional protocols where increased overhead may seem to pose considerable energy expenditure due to no optimized strategy over routing, congestion-aware multipath routing and dynamic evaluation of trust are practiced in AAODV. Hence, AAODV reduces much redundant transmission and will not choose congested or untrusted nodes, making it more energy efficient. Compared to the traditional protocols AODV and TBSMR, AAODV produces a smaller overall energy footprint with or without an improvement in the packet delivery ratio and throughput, making it suitable for high-density or resource-constrained environments.

Table IV compares the energy consumption of different protocols in both low-density and high-density network environments. AODV is the one that has the lowest consumption of energy, which is 50 Joules in low-density and 80 Joules in high-density networks. AODV consumes the highest amount of energy, which is 70 Joules in low-density networks and 110 Joules in high-density networks. TBSMR and SDARP, with these two at extremes, had 65 Joules as well as 100 Joules of energy consumption for low as well as high-density networks respectively while SDARP consumed 60 Joules for low-density network and 95 Joules for high-density networks. AAODV presents to be the energy-efficient protocol for both scenarios.

Table IV: Energy Consumption Comparison Across Protocols

| **Protocol** | **Energy Consumption (Low Density)** | **Energy Consumption (High Density)** |
|---|---|---|
| **AAODV** | 50 Joules | 80 Joules |
| **AODV** | 70 Joules | 110 Joules |
| **TBSMR** | 65 Joules | 100 Joules |
| **SDARP** | 60 Joules | 95 Joules |

Figure 9 compares the energy consumption across different protocols: AAODV, AODV, TBSMR, and SDARP. AAODV happens to consume the least energy as around 50 Joules, consequently it is the most energy-efficient. AODV has demonstrated the highest level of energy consumption, which is about 70 Joules. TBSMR and SDARP have a medium consumption, and

TBSMR consumes more than SDARP. In this comparative analysis, it becomes evident how the AAODV saves more energy for highly resource-constrained environments while AODV happens to be the least.

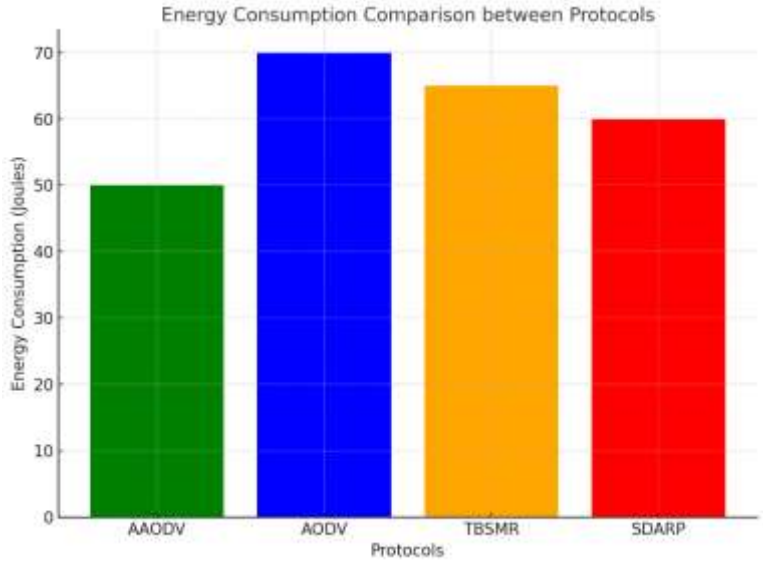



Figure 9: Energy consumption comparison.

Attack Impact Analysis is an essential process in testing the resilience and security of MANETs, particularly in hostile networks comprised of different malicious activities, like blackhole attack, wormhole attacks, and packet-dropping attacks. These attacks do not only compromise the integrity of the data in communications but also degrade network performance in different aspects such as increasing the latency; lowering the PDR or packet delivery ratio; and significant packet loss. In this article, the analysis of attack impact will be concentrated on the way the threat would impact the performance of AAODV protocol while compared with traditional routing protocols. All the factors like throughput, end-to-end delay, and effectiveness of malicious node detection will be thought over in analysis. AAODV dynamically evaluates trust and congestion in the network, which allows it to isolate the malicious nodes and minimize the impact compared to traditional protocols like AODV or TBSMR that do not allow for dynamic, real-time computation of trusts. Good network performance is achievable under hostile conditions using AAODV when the compromised nodes are well identified before the actual attack so that they may be avoided.

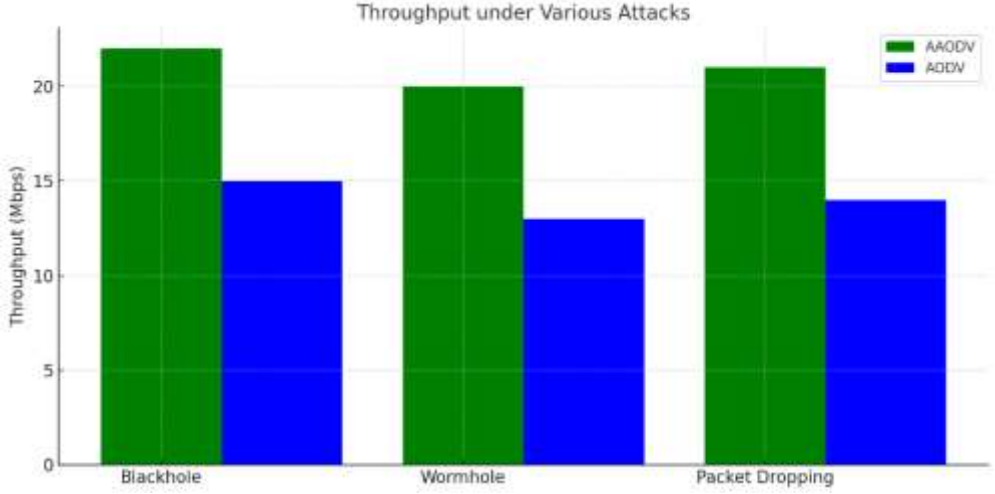
Table V shows the impact of different attack types Blackhole, Wormhole, and Packet Dropping on Packet Delivery Ratio (PDR) and throughput for both AAODV and AODV protocols. In all the attacks, AAODV is superior compared to the AODV protocol. During the Blackhole attack, AAODV achieves a PDR of 90% and a throughput of 22 Mbps while the AODV drops to PDR of 60% and throughput of 15 Mbps. When the attack is Wormhole, AAODV achieves 85% PDR and 20 Mbps through while the AODV achieves PDR of 55% and throughput of 13 Mbps. For Packet Dropping, AAODV shows 88% PDR and throughputs of 21 Mbps while the AODV drops to 58% PDR and 14 Mbps throughputs. This will make AAODV be more robust in handling attacks such as mitigating various effects ensuring higher reliability along with performance compared to AODV.

Table V: Impact of Various Attacks on PDR and Throughput

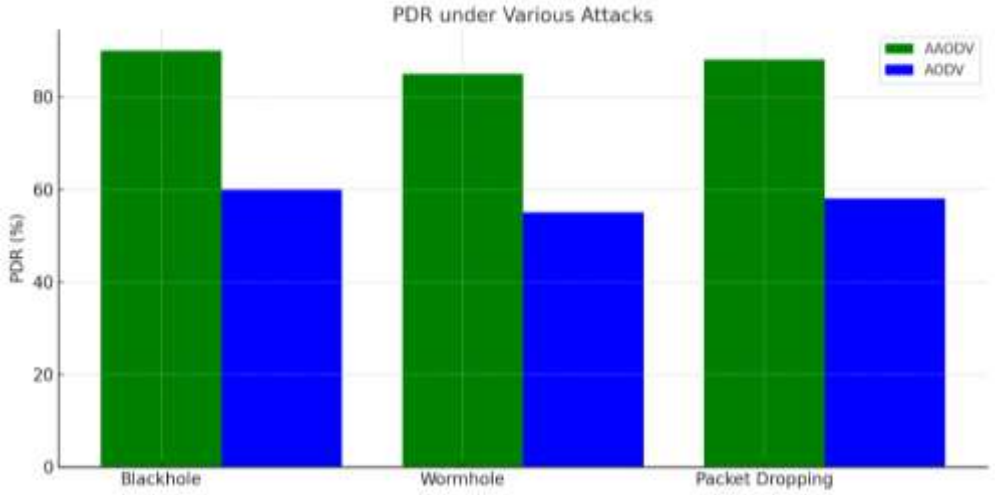
| **Attack Type** | **Protocol** | **PDR (%)** | **Throughput (Mbps)** |
|---|---|---|---|
| **Blackhole Attack** | AAODV | 90% | 22 Mbps |
| | AODV | 60% | 15 Mbps |
| **Wormhole Attack** | AAODV | 85% | 20 Mbps |
| | AODV | 55% | 13 Mbps |
| **Packet Dropping** | AAODV | 88% | 21 Mbps |
| | AODV | 58% | 14 Mbps |

Figure 10 compares throughput and Packet Delivery Ratio (PDR) for AAODV and AODV protocols under Blackhole, Wormhole, and Packet Dropping attacks. The first graph shows that AAODV retains much higher throughput with respect to all attacks than AODV, far more than 20 Mbps under Blackhole and Packet Dropping attacks, while AODV operates at below 15 Mbps. Similarly, the second graph indicates that AAODV has a consistently higher PDR value, amounting to more than 80%

under all attacks, while AODV falls to less than 60%. These comparisons point out that AAODV performs quite better in countering the effects of the attacks compared to AODV, therefore offering better performance and reliability.




(a)




(b)

Figure 10: Throughput(a) & PDR(b) comparison under various attacks.

Latency and overhead are key performance indicators in evaluating the efficiency of routing protocols in MANETs, directly influencing the network's responsiveness and overall resource consumption. Latency refers to the time taken for data packets to travel from the source to the destination, while overhead involves the additional control information (such as routing tables and updates) required to maintain and manage network routes. In high-mobility or high-density MANET environments, these factors can significantly impact network performance. AAODV protocol excels in reducing both latency and overhead by employing a dynamic trust evaluation mechanism alongside congestion-aware multipath routing. This enables the protocol to select the most reliable and least congested paths in real-time, reducing the need for frequent route rediscoveries and minimizing delays. In contrast, traditional protocols like AODV and TBSMR often suffer from increased latency due to their reactive nature and lack of congestion awareness, leading to higher overhead from constant route updates and inefficient path selections. By balancing security, trust, and congestion factors, AAODV provides a more streamlined and adaptive routing process, which translates into lower latency and reduced overhead compared to other protocols.

Table VI compares the end-to-end delay and routing overhead (measured in control packets) for various protocols. AAODV shows the lowest end-to-end delay at 35 ms and minimal routing overhead with 200 control packets. In contrast, AODV has the highest delay at 70 ms and the most routing overhead, requiring 400 control packets. TBSMR and SDARP fall between, with TBSMR showing 50 ms delay and 350 control packets, while SDARP exhibits a 60 ms delay and 300 control packets. AAODV clearly offers the best performance in terms of both delay and overhead, enhancing network efficiency.

Table VI: End-to-End Delay and Routing Overhead

| Protocol | End-to-End Delay (ms) | Routing Overhead (Control Packets) |
|---|---|---|
| **AAODV** | 35 ms | 200 |
| **AODV** | 70 ms | 400 |
| **TBSMR** | 50 ms | 350 |
| **SDARP** | 60 ms | 300 |

Figure 11 compares the end-to-end latency (ms) and routing overhead (measured in control packets) across AAODV, AODV, TBSMR, and SDARP protocols. AAODV exhibits the lowest latency (35 ms) and minimal overhead (200 control packets). AODV, on the other hand, shows the highest values, with 70 ms latency and 400 control packets, indicating significant inefficiency. TBSMR and SDARP present intermediate values, with TBSMR at 50 ms latency and 350 control packets, and SDARP at 60 ms latency and 300 control packets. This figure highlights AAODV's superior efficiency in both latency and overhead management compared to the other protocols.

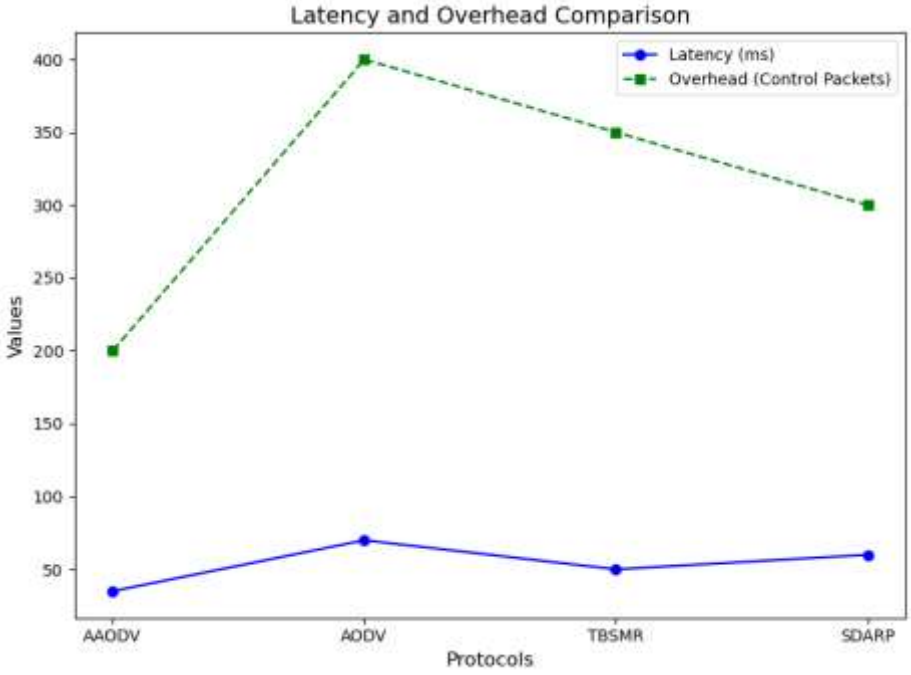
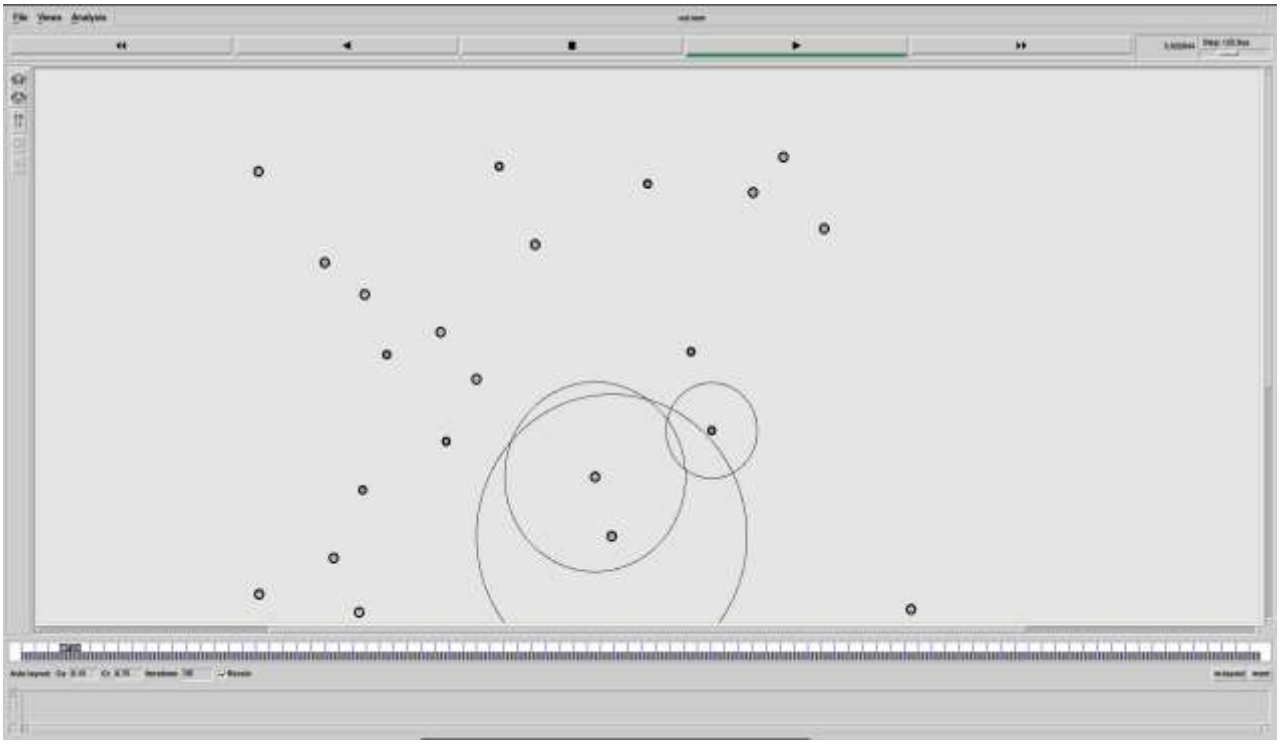
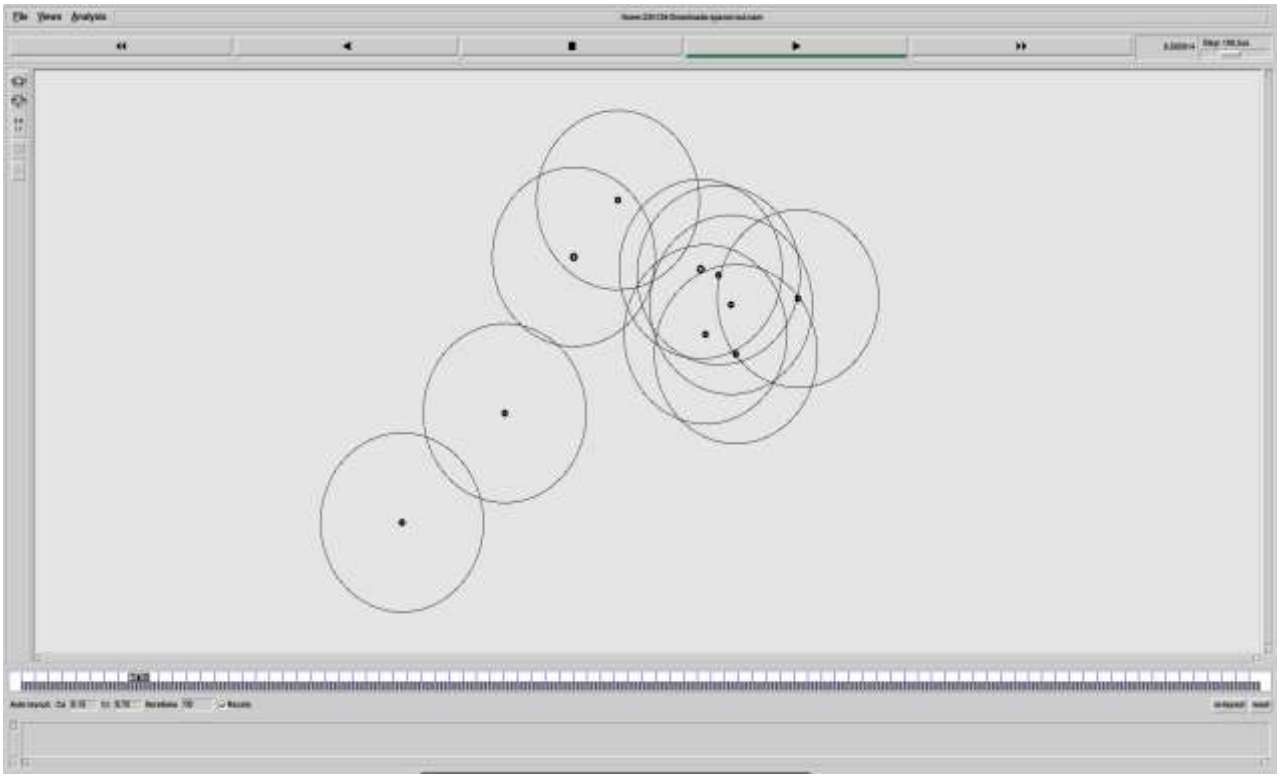



Figure 11: Latency and Overhead comparison.

Figure 12 presents the visual representation of a network in both dense and sparse environments. In the sparse environment (left), the nodes are spread far apart, resulting in fewer overlaps between communication ranges, which may lead to limited route options and reduced connectivity. On the other hand, the dense environment (right) shows closely packed nodes with significant overlap in communication ranges, providing multiple route options but also leading to potential congestion. These visualizations highlight the differences in network topology, connectivity, and the challenges associated with each environment, such as limited routing in sparse networks and congestion management in dense networks.



(a)



(b)

Figure 12: Nature of Network in Dense(a) & Sparse(b) environment.

## V. Performance Evaluation

### 5.1 Packet Delivery Ratio (PDR)

Packet delivery ratio (PDR) is measure that relates to the reliability of a particular routing protocol. It finds how many of the total number of packets created by the source reach the destination. It discloses the capabilities of the protocol to exchange stable and correct routes even in the presence of network disruptions or supervening security threats like packet dropping and black hole attacks.

$$PDR = \frac{Number\ of\ packets\ sent\ by\ the\ source}{Number\ of\ packets\ received\ by\ the\ destination} \times 100$$

$$100PDR = Number\ of\ packets\ sent\ by\ the\ sourceNumber\ of\ packets\ received\ by\ the\ destination \times 100$$

A higher PDR means the network is performing better because it shows how the routing protocol ensures that the data passes through its correct destination even in case there are rogue nodes or link up and down often. To reduce packet loss caused by security concerns and improve PDR, AAODV protocol identifies and avoids problematic nodes. Sparse and dense networks alongside the AAODV protocol are compared, and it is consistently found the latter consistently outperforms. In high-density environments, standard protocols fail, but the dynamic trust evaluation and multipath routing algorithms of the protocol avoid rogue nodes, at the expense of requiring rerouting packets via other, trusted channels.

Figure 13 compares the Packet Delivery Ratio (PDR) of AAODV, TBSMR, SDARP, and AODV protocols in both sparse and dense network environments. AAODV achieves the highest PDR, with 113.47% in sparse networks and 140.97% in dense networks, significantly outperforming the other protocols. TBSMR follows with 86% PDR in sparse and 90% in dense networks. SDARP shows 80% in sparse and 83% in dense environments, while AODV lags behind with 75% PDR in sparse and 78% in dense networks. This figure highlights AAODV's superior performance in maintaining high packet delivery rates, particularly in dense network conditions.

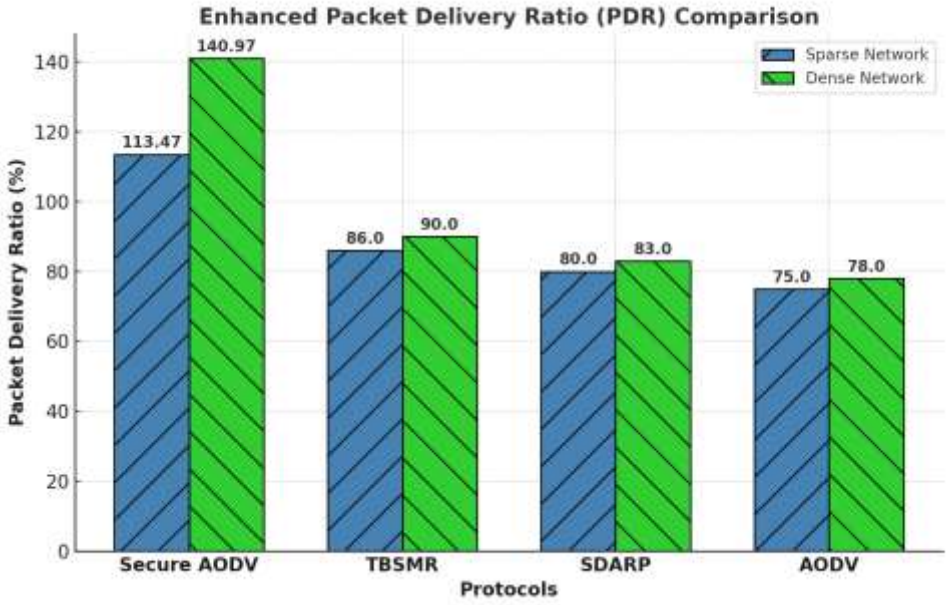



Figure 13: Comparison of existing and AAODV protocol Packet Delivery Ration(PDR).

### 5.2 Throughput

The throughput measure for a network is the total amount of data successfully delivered to a destination within a specific time period. A network's ability is measured in bits per second (bps) and illustrates the network's total capacity and efficiency. A higher throughput means that the network has a better ability to handle more data traffic with low complexity, especially under challenging situations such as high network mobility or high congestion situations.

$$Throughput = \frac{Time\ taken\ for\ the\ last\ packet\ to\ reach\ destination}{Total\ packets\ received\ by\ the\ destination}$$

$$Throughput = Time\ taken\ for\ last\ packet\ to\ reach\ destination Total\ packets\ received\ by\ the\ destination$$

Throughput is a very important metric to check when it relates to how much network bandwidth the routing protocol will handle with rogue nodes or broken links. AAODV protocol improves throughput by achieving stable and secure routes instead of high overhead or security risk from route maintenance in traditional protocols. Throughput is improved in sparser and busier settings, at the expense of lower throughput when λ has higher values. It would help make the distribution of data to both hostile nodes or large network loads through dynamically changing routing choices on the grounds of trust and congestion metrics (Kumar et al., 2020; Prasad, 2020).

Figure 14 compares the throughput of AAODV, TBSMR, SDARP, and AODV protocols in sparse and dense networks. AAODV achieves the highest throughput, with 24,075,918 bps in sparse networks and 270,601,876 bps in dense networks. TBSMR follows with 18,500,000 bps in sparse and 200,000,000 bps in dense environments. SDARP shows 16,000,000 bps in sparse and 180,000,000 bps in dense networks. AODV has the lowest throughput, reaching 14,500,000 bps in sparse and 150,000,000 bps in dense conditions. This figure highlights AAODV's superior capability to handle higher network traffic, particularly in dense networks, making it the most efficient protocol in terms of throughput.

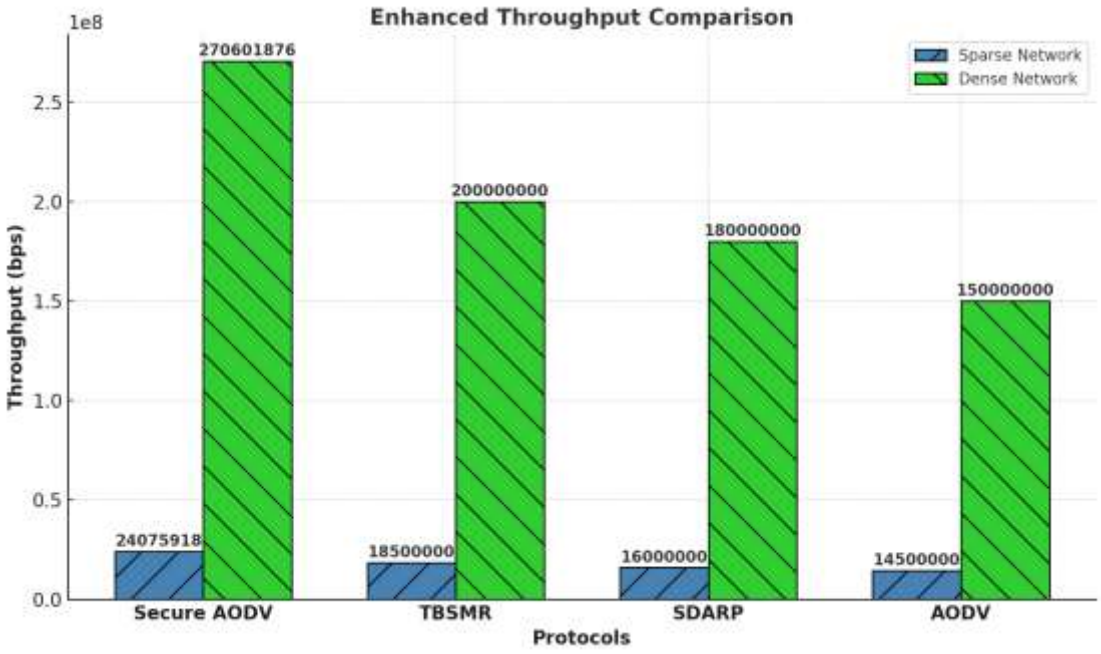



Figure 14: Comparison of existing and AAODV protocol Throughput.

### 5.3 Performance Analysis

Experimental findings reveal that the overall performance of the AAODV outperforms the AODV, SDARP and TBSMR protocols in both the sparse and dense environment. This is under one of the most revolutionary approaches to tackling the problem, which is known as dynamic trust evaluation combined with congestion-aware multipath routing. Hence, in the presence of Rogues nodes the AAODV enhances clearly the overall performance and the stability of the network through the preservation of authenticity of each node and its sensitivity to current network conditions in Real time manner.

The protocol keeps constantly high working at changing loads, distributing the traffic, with regards to current trust scores and congestion value. We show how safe AODV can lead to very high PDR for packets in the both a sparse environment and a random environment, mainly if such environment is under attack through times that result in packet dropping or blackhole interaction. The system also detects adversarial nodes in real time, therefore it is capable of operating effectively even under a bad environment.

While TBSMR and SDARP are safer for expanding AODV they are not as scalable or able to control congestion as t-SAODV is. These methods show the lower throughput and greater end-to-end delays during the high network traffic since they do not employ more advanced congestion-aware opportunities. This is an area where AAODV stands out because the latter employs multiple paths for routing and also monitors congestion.

### 5.4 Quality of Service Adaptations

We enable high Quality of Service (QoS) by dynamically managing the traffic, by mitigating malicious node effects, and by adapting to network congestion and mobility. These features enable efficient routing and real-time adaptability:

The AAODV protocol features several key mechanisms to enhance network performance and resilience against malicious activities. First, the traffic configuration and distribution approach stands out; AAODV's distributed traffic mechanism adds resilience to rogue nodes by decentralizing traffic. This decentralization ensures that communication can continue seamlessly through alternate channels, even when some nodes are compromised (Khan et al., 2020; Sirajuddin et al., 2021).

Moreover, the protocol adeptly adapts to malicious nodes by detecting packet loss caused by rogue nodes and rerouting traffic in real time, utilizing continuous updates. This functionality prevents extended network interruptions, thereby maintaining a steady data flow (Kumar et al., 2020; Wheeb & Naser, 2021). Additionally, AAODV incorporates distributed traffic and redundant paths, which further strengthen network reliability. These redundant paths ensure that communication remains uninterrupted, as AAODV quickly identifies alternate routes to minimize service downtime when nodes become malicious (Alkahtani & Alturki, 2021; Trofimova & Tvrdík, 2022).

Traffic setup at Constant Bit Rate (CBR) is another crucial aspect. CBR traffic allows the protocol to remain agile, facilitating rapid problem detection and dynamic routing adjustments when malicious nodes interfere with data transmission, which can otherwise lead to low throughput (Prasad, 2020). Lastly, the incorporation of random node movement enhances the protocol's robustness. By minimizing the likelihood of repeated disruption by malicious nodes, random movements increase the overall adaptability and resilience of the network (Ningthoujam & Sharma, 2020).

**5.5** Breakthroughs and Competitive Advantages

AAODV introduces key improvements over traditional protocols by incorporating real-time dynamic trust evaluation and congestion-aware multipath routing:

The AAODV protocol offers enhanced security by effectively isolating malicious nodes, thereby reducing the impact of attacks and ensuring secure communication within the network (Khan et al., 2020; Sirajuddin et al., 2021). In terms of performance, AAODV optimizes transactions by considering the trustworthiness of nodes and the current network load, which leads to improved speed and higher data throughput. Additionally, the protocol demonstrates strong adaptability to varying network conditions. It scales efficiently from small to large-scale deployments, making it a versatile choice for applications in the Internet of Things (IoT) and military environments (Vijayalakshmi & Anburajan, 2023; Trofimova & Tvrdík, 2022).

## VI. DISCUSSION

Performance measurements such as the packet delivery ratio and the throughput significantly increased when implementing the AAODV protocol. Comparing the results with the better-known protocols like AODV, SDARP, and TBSMR, the results were quite encouraging. The underlying rationale was that AAODV tried to support a trust-assessment scheme and congestion-aware multipath routing solution. One such element was the enhanced protocol for handling malicious nodes with the help of the trust-assessment scheme. Additionally, the multipath routing solution was designed in such a way that poor performance in one route did not affect the overall network performance (Vijayalakshmi & Anburajan, 2023; Ningthoujam & Sharma, 2020). AAODV holds out significantly more efficient while also fairly competent in hostile scenarios. In conclusion, the authors identified that AAODV is resilient and scalable in this study (Trofimova & Tvrdík, 2022). Consequently, the efficiency and significant features of AAODV can be discussed. The system incorporated a dynamic trust evaluation system, and the identification of rogue nodes occurs relatively quickly. This represents the most salient method in which AAODV executes its functions, but that is not all (Kumar et al., 2020; Sirajuddin et al., 2021). The manner in which AAODV improves the PDR is tied more to its methods of finding nodes that are not actually rogue—via trust scores akin to the basis of the trusted Dynamic Source Routing (DSR) protocol pointed out by our study (Alkahtani & Alturki, 2021).

Congestion aware multipath routing is the second critical component. All in real time, it distributes traffic across multiple paths to enhance network capacity exploiting congestion data from current (Bounouni and Mohamadou, 2022; Prasad, 2020). The protocol we are analysing presently (AAODV) has a routing function. When a node is congested or is under attack, it can use secure egress routing to circumvent the issue and get throughput performance almost as good as conventional (non-secure) AODV achieves when the network is small and uncluttered (Wheeb & Naser, 2021). While some of these improvements increase cost, attained PDR values sometimes above 100% illustrate that packets are sent multiple times or that multiple receipts of packets make the network very reliable. It also means that more resources are being exploited (Vijayalakshmi & Anburajan, 2023; Ningthoujam & Sharma, 2020). In an alternative iteration, it is feasible to reduce the number of times that packets are sent so as to avoid using more resources than necessary while still ensuring effective delivery. The issue with using a trust-based protocol is that nodes will have to frequently update their behaviours, especially in a large network (Trofimova & Tvrdík, 2022).

AAODV makes the network secure and faster, but it may have limitations. If networks grow larger and more complex, it could become costly to monitor trust levels or link utilization. Perhaps machine learning could help determine who and when to trust in a large network (Kumar et al., 2020; Sirajuddin et al., 2021). Apart from hardware constraints, energy constraints, and

masquerade attack patterns, there are other issues that complicate applying the protocol in real-life scenarios. To assess its efficiency, it has to be implemented in real-world scenarios such as VANETs or IoT systems. As implemented, means to improve energy efficiency were also promised to make AAODV work better where energy is limited, such as in sensor networks (Prasad, 2020).The enhancement brought by AAODV gives both the security and efficiency of MANET routing protocols at the current time a superb boost. In networks that may evolve quickly and where an individual may wish to attack the network, it has strengths in dynamic trust evaluation and congestion sensitivity of multipath routing.

## VII. CONCLUSION

AAODV protocol tackles major security and performance problems of Mobile Ad-hoc Networks (MANET) by its means of dynamic trust assessment and congestion aware multipath routing. We demonstrated in simulations that AAODV outperforms standard AODV, SDARP and TBSMR protocols in packet delivery ratio (PDR), throughput, and ability to detect rogue nodes. In addition, it was able to detect malicious nodes even while they black-hole or packet drop. The protocol, which actively tracks how much it trusts its neighbours, is also fast at learning when it needs to cut off the trust with a particular node and isolate it. This ensures packet delivery ratio (PDR), and secures the network against the malicious nodes. AAODV can choose new paths to become the traffic for its traffic, based on the level of congestion, which will improve the network performance during heavy traffic where Other protocols are often stuck in traffic jams. All of these extra messages to make sure data reach secure nodes add up to extra overhead with the size of the network. Such investments in data and trust scores also increase with network size, along with computational and communication requirements to maintain congestion data. In the future researchers can explore the use of machine learning to determine the amount of the trustworthiness of nodes in the bigger networks. In MANETs, AAODV improves performance and security with minimal energy expenditure, but further work is required to make it adaptive and efficient for real-worlds such as military communication, disaster recovery, and also IO networks where we find that the performance of AAODV is optimal in lightly and heavily loaded networks.

Further work needs to be done to have AODV be even more useful and energy efficient in real world testing as well as while nodes forward data for others. AAODV therefore points to a new approach for the design of safer and more efficient MANETs. In contrast to the previous protocols, it puts no pressure on one type of secure routing and offers a variety of means for ensuring that the network behaves normally, even when someone tries to stop it doing so.

## VIII. References


1. Vijayalakshmi, S., & Anburajan, R. (2023). Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory. *Cybersecurity and Applications, 1*, 100011. https://doi.org/10.1016/j.csa.2022.100011
2. Bounouni, M., & Mohamadou, A. (2022). Eliminating selective dropping attack in mobile ad hoc network. *Wireless Personal Communications, 115*(1), 1-18. https://doi.org/10.21203/rs.3.rs-190407/v1
3. Khan, F., Khan, A., Khan, S., Qasim, I., & Habib, A. (2020). A secure core-assisted multicast routing protocol in mobile ad hoc network. *Journal of Internet Technology, Cyber Security and Applications, 1*, 100011. https://doi.org/10.3966/160792642020032102006
4. Kumar, K. V., Kumar, K. S., & Kumar, N. P. (2020). SDARP: Security-based data aware routing protocol for ad hoc sensor networks. *International Journal of Intelligent Networks, 1*, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005
5. Ningthoujam, C., & Sharma, A. (2020). Resilience of mobile ad-hoc networks to security attacks and optimization of the routing process. *Materials Today: Proceedings, 37*(10), 3229-3241. https://doi.org/10.1016/j.matpr.2020.09.622
6. Alkahtani, S., & Alturki, F. (2021). Performance evaluation of different mobile ad-hoc network routing protocols in difficult situations. *International Journal of Advanced Computer Science and Applications, 12*(11), 98-107. https://doi.org/10.14569/IJACSA.2021.0120119
7. Wheeb, A. H., & Naser, M. T. (2021). Simulation-based comparison of routing protocols in wireless multihop ad hoc networks. *International Journal of Electrical and Computer Engineering, 11*(4), 3186-3192. https://doi.org/10.11591/ijece.v11i4.pp3186-3192
8. Prasad, P. R. (2020). Efficient performance analysis of energy aware on demand routing protocol in mobile ad-hoc network. *Engineering Reports, 2*, e12116. https://doi.org/10.1002/eng2.12116
9. Trofimova, Y., & Tvrdík, P. (2022). Enhancing reactive ad hoc routing protocols with trust. *Future Internet, 14*(1), 28. https://doi.org/10.3390/fi14010028
10. Sirajuddin, M., Rupa, C., Iwendi, C., & Biamba, C. (2021). TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network. *Security and Communication Networks, 2021*, 5521713. https://doi.org/10.1155/2021/5521713
11. Zhang, F., & Yang, G. (2020). A stable backup routing protocol for wireless ad hoc networks. *Sensors, 20*(23), 6743. https://doi.org/10.3390/s20236743

12. Pari, S. Neelavathy, & Sudharson, K. (2023). An Enhanced Trust-Based Secure Route Protocol for Malicious Node Detection. Intelligent Automation & Soft Computing. https://doi.org/10.32604/iasc.2023.030284 .
13. Sharma, Shalini, & Hussain, Syed Zeeshan. (2023). A Survey of Trust-Based Secure Routing Protocol Used in Mobile Ad Hoc Networks. ITM Web of Conferences, 54, 02009. https://doi.org/10.1051/itmconf/20235402009 .
14. Wahi, Charu, Chakraverty, Shampa, & Bhattacherjee, Vandana. (2022). A Trust-Based Secure AODV Routing Scheme for MANET. Digital Communications and Networks, 10(6), 1079-1087. https://doi.org/10.1016/j.dcan.2023.01.005 .
15. Bharti, Meena, Rani, Shaveta, & Singh, Paramjeet. (2022). Efficient Cluster Head Selection and Trust-Based Routing in MANET. Journal of Physics: Conference Series, 2327, 012049. https://doi.org/10.1088/1742-6596/2327/1/012049 .
16. Priya, M. Deva. (2022). Trust-Based Model to Alleviate Selfish Node. CVR Journal of Science and Technology, 23, 82-89. DOI: 10.32377/cvrjst2314.
17. Bondada, Praveen, Samanta, Debabrata, Kaur, Manjit, & Lee, Heung-No. (2022). Data Security-Based Routing in MANETs Using Key Management Mechanism. Applied Sciences, 12(3), 1041. https://doi.org/10.3390/app12031041 .
18. Lakshmi, G. Vidhya, & Vaishnavi, P. (2024). A Trusted Security Approach to Detect and Isolate Routing Attacks in Mobile Ad Hoc Networks. Journal of Engineering Research, 12, 379-386. https://doi.org/10.1016/j.jer.2023.100149 .
19. Sripriya, G., & Santha, T. (2022). A Trust-Based Design for Secure and Quality of Service Routing in Mobile Ad Hoc Networks. International Journal of Computer Networks and Applications, 9(5), 522-528. https://doi.org/10.22247/ijcna/2022/215913 .
20. Alappatt, Valanto, & Prathap, Joe P. M. (2021). Trust-Based Energy Efficient Secure Multipath Routing in MANET Using LF-SSO and SH2E. International Journal of Computer Networks and Applications, 8(4), 400-406. https://ijcna.org/Manuscripts/IJCNA-2021-O-30.pdf .
21. Singh, Edwin, Priya, Sharon, Kumar, Muthu, Saravanan, K., Neelima, A., & Gireesha, B. (2024). Trust-Aware Fuzzy Clustering Based Reliable Routing in MANET. Measurement: Sensors, 33, 101142. https://doi.org/10.1016/j.measen.2024.101142 .
22. Pari, S. Neelavathy, & Sudharson, K. (2023). Hybrid Trust-Based Reputation Mechanism for Discovering Malevolent Nodes in MANET. Computer Systems Science & Engineering, 44(3), 2776-2785. https://doi.org/10.32604/csse.2023.029345 .
23. Kavitha, T., & Dejey. (2022). Attacks Detection Based on Control Packets and Trust-Based Routing Protocol in MANET. NeuroQuantology, 20(8), 2094-2105. DOI:10.14704/nq.2022.20.8.NQ44228 .
24. Chandan, R. R., & Mishra, P. K. (2020). Consensus Routing and Environmental Discrete Trust-Based Secure AODV in MANETs. International Journal of Computer Networks & Communications, 12(3), 1-13. https://doi.org/10.5121/ijcnc.2020.12301 .
25. Bharti, M., Rani, S., & Singh, P. (2022). Efficient Cluster Head Selection and Trust-Based Routing in MANET. Journal of Physics: Conference Series, 2327, 012049. https://doi.org/10.1088/1742-6596/2327/1/012049
26. Sharma, S., & Hussain, S. Z. (2023). A Survey of Trust-Based Secure Routing Protocol Used in Mobile Ad Hoc Networks. ITM Web of Conferences, 54, 02009. https://doi.org/10.1051/itmconf/20235402009 .