International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(4):1170-1179

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i04.01440

# TS-AODV: Leveraging Trust for Secure Routing in Manets

K Lokeshwaran[1]*, Jayanthi Arumugam[2], Komal Kumar Napa[1], Senthil Murugan Janakiraman[3], Balamurugan AG[4]

[1]Department of Computer Science and Engineering (Data Science), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India, [2]Department of Computer Science and Engineering, Velammal Engineering College, Chennai, India, [3]Department of Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, India, [4]Department of Computer Science & Engineering, Vel Tech Rangarajan Dr. Sakunthala R&D Institute of Science and Technology, Chennai, India. *Corresponding Author's Email: k.lokeshwaran@gmail.com

## Abstract

Mobile Ad-hoc Networks (MANETs) offer on-the-fly connectivity for devices without fixed infrastructure, but their decentralized nature makes them vulnerable to malicious nodes that disrupt communication. Existing routing protocols struggle to guarantee reliable data transmission in such environments. This paper introduces Trusted Ad hoc On-Demand Distance Vector (TS-AODV), a novel secure routing protocol for MANETs that leverages trust mechanisms to bolster network security. TS-AODV establishes a trust management system, assigning trust values to each node based on past behavior in forwarding packets. This value reflects a node's reliability and cooperation. When selecting routes, TS-AODV considers both hop count (distance) and the trust values of involved nodes. Nodes with higher trust ratings are prioritized, effectively isolating malicious nodes with low trust from participating in critical data paths. Additionally, TS-AODV incorporates packet weighting, where more crucial data packets are directed through paths with the highest cumulative trust values. The trust value of a node is estimated by considering three factors: 1. the total number of packets sent, 2. the number of packets successfully delivered, and 3. the relevance of the information carried. This comprehensive approach helps identify nodes engaged in malicious activities like packet dropping or forwarding irrelevant data. Extensive simulations conducted in the NS2 network simulator demonstrate the effectiveness of TS-AODV in identifying malicious nodes and resisting various attacks. These results highlight TS-AODV's potential to secure data transmission and foster trust in MANETs, paving the way for more reliable and secure communication in dynamic wireless networks.

**Keywords:** Malicious Nodes, Mobile Adhoc Networks, Network Security, Routing Protocol, Wireless Networks.

## Introduction

MANET comprises a group of mobile nodes that form an infrastructure wireless network. In this network, each node is considered as a host and an acting router to forward packets from the source to the destination. Tactical operations, law enforcement, virtual classrooms, search and rescue operations, and other applications are among the many uses of MANET. When contrasting MANET with cellular and wireline networks, it has the following unique qualities: a) absence of pre-existing infrastructure, b) ability to support fast node mobility, and c) decentralized and self-organized communications by insider nodes in a limited area spatial across the bandwidth-constrained wireless medium (1). The flexibility and independent infrastructure of MANET enable the network to be used in several environments such as disaster rescue operations and military battlefields. In recent years, many researchers (2, 3) have been concentrating on trusted secure routing algorithms to enhance the security and performance of the ad-hoc wireless network (4). The secure communication among directly connected wireless devices of wireless ad-hoc networks is protected by a cryptographic protocol and it mainly focuses on threat identification and attacks of MANET systems (5). The type of attack in a network is classified as a passive attack and an active attack. The passive attack does not disturb the function of the network but it tries to eavesdrop on the information in the communications (6). This type of attack is tedious to detect and causes minor damage to security mechanisms. Active attacks are further classified into insider attacks and outsider attacks. The compromised node initiates an insider attack and it holds the primary key materials in the MANET communication system whereas the outsider

(Received 26th June 2024; Accepted 17th October 2024; Published 30th October 2024)

attack doesn't carry the primary key materials. Authorized access people cause most of the attacks in the network, not only hackers. Most of the insider threats come from users who are fully authorized people to use the accessing systems. It is tough to detect malicious use by authorized users and Cybersecurity can't able to stop them. By comparing with outsider threats, insider threats cause more damage to the MANETs. Communication within these networks may be forbidden from these attacks.

In Mobile Ad-hoc Networks (MANETs), traditional routing protocols like Ad hoc On-demand Distance Vector (AODV) (7), Dynamic Source Routing (DSR) (8), and Temporally Ordered Routing Algorithm (TORA) (9) operate under the assumption of cooperative behavior from all nodes. However, this idealistic scenario proves difficult to maintain in dynamic environments where malicious nodes can disrupt communication. To address this challenge and enhance security and reliability, researchers are increasingly focusing on trust mechanisms within MANET routing protocols (10).

Several trust-based routing approaches have emerged, offering diverse techniques. Lightweight Trusted Routing prioritizes efficient trust estimation using local information and Intrusion Detection Systems (IDS) to minimize overhead (11). This method seamlessly integrates with existing protocols like AODV. Friendship Metric introduces a trust-based approach to secure AODV. The source node evaluates potential routes based on factors like node reputation before sending data, fostering secure communication. An On-demand Trust-based Multi-path Routing (AOTMDV) builds upon traditional models with new trust mechanisms and secure routing information (12). It utilizes Message Authentication Codes (MAC) to secure trust information within routing packets and proposes a path trust update mechanism to handle frequent route changes inherent to MANETs (13). Trusted-DSR and similar trust-based extensions of DSR consider trust values along the entire path for data forwarding (14). Trust values increase for nodes that successfully deliver packets and decrease for those that don't. However, pinpointing the exact culprit for dropped packets remains a challenge (14). Dynamic Trust Evaluation proposes evaluating trust dynamically for transmission paths and offers various route selection strategies, further enhancing adaptability in MANETs (15).

The Fuzzy Trusted Dynamic Source Routing (FTDSR) protocol (16) explores a novel approach to evaluating node reliability. It combines fuzzy logic rules prediction and analytic hierarchy process theory to assess trust in a nuanced way. Another approach gaining traction is the Agent-based Trust Dynamic Source Routing protocol (ATDSR) proposed by Islam Tharwat *et al.* in 2018 (17). This method leverages a multi-agent system on each node to monitor and calculate trust values for all participating nodes in the network.

Trust-based routing offers a promising approach. Jayalakshmi *et al.* propose Trust Vector-based Dynamic Source Routing (TV-DSR), which meticulously evaluates node reliability using various factors gleaned from past interactions between nodes (18, 19). The Fuzzy-based Power-aware Trusted Dynamic Source Routing Protocol (FTP-DSR) by (20) incorporates a trust management system that assesses both a node's remaining battery power and trustworthiness using fuzzy logic. This ensures reliable data transmission by considering both a node's capabilities and potential malicious intent. Looking beyond trust-based routing, Mohamed Elhoseny *et al.* proposed a Reliable Data Transmission Model that leverages signcryption to improve confidentiality and efficiency in secure data transmission for MANETs (21, 22). This model combines energy-efficient routing with signcryption, a technique that encrypts data and attaches a digital signature for verification. These advancements showcase the ongoing pursuit of robust and secure communication in MANETs through a combination of trust evaluation, secure routing protocols, and cryptographic techniques. Keerthika *et al.*'s AODV with Artificial Bee Colony (ABC) optimization utilizes an optimization algorithm to detect and remove malicious nodes, enhancing overall network security (23). Traditional routing protocols are also being enhanced for security. Ashish Kumar Jain *et al.* propose Security Enhancement of AODV, a behavior-based evaluation system that identifies secure paths using a threshold value (24).

## Trust Estimation

Ad-hoc networks can benefit from a trust-based routing model to enhance security, as illustrated in Figure 1 using a weighted directed graph where nodes and connections represent trust values. Each node maintains a "trust table" containing the trust values of its neighbors. These trust values are critical for identifying malicious nodes within the network. Calculating a node's trust value involves a multifaceted approach that considers its packet forwarding behavior. Here's a breakdown of the factors involved:

- Packet forwarding percentage: This metric reflects the proportion of received packets the node successfully forwards to others.
- Number of packets forwarded accurately: This focuses on the raw number of packets forwarded correctly, offering a quantitative measure.
- Number of packets received: This takes into account the total volume of packets the node receives, providing context for the forwarding metrics.
- Packet relevance: This factor goes beyond simple packet forwarding by considering the importance or relevance of the information carried by the packets. This helps identify nodes that might be dropping or forwarding irrelevant data, potentially for malicious purposes.

By incorporating these multifaceted aspects of packet forwarding behavior, the trust model aims to create a more comprehensive assessment of a node's trustworthiness, ultimately leading to more secure communication in ad-hoc networks.

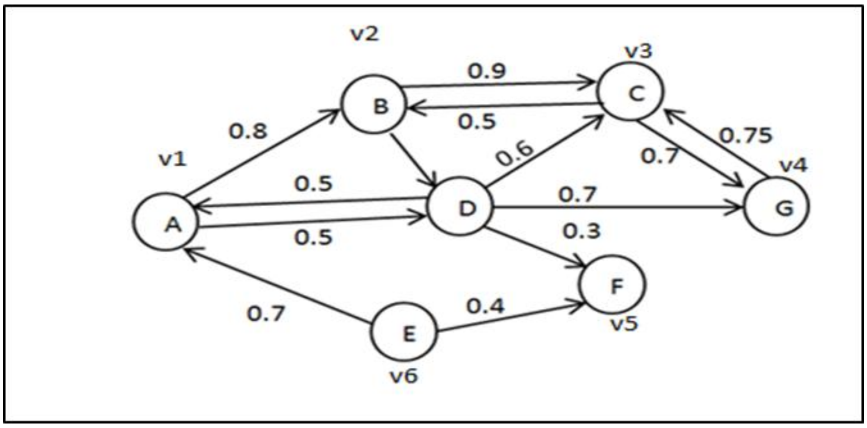

**Figure 1:** A Sample Adhoc Network with Trust Values

The trust value is considered using the following packet forwarding ratio formula:

$$PacketFaowardedRatio = \frac{Numberofpacketscorrectlyforwarded}{Totalnumberofpacketsforwarded}$$

$$TV_{P_i}(t) = \frac{\sum_{i \neq j}^{n} CF_{ij}}{\sum_{i \neq j}^{n} \left(CF_{ij} + NF_{ij}\right)} = \frac{\sum_{i \neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} CF_{jk}}{\sum_{i \neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} CF_{jk} + \sum_{i \neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} NF_{jk}} --- [1]$$

Where $CF_{ij}$ is the number of correctly forwarded packets from Node to Node $_j$. $\delta_{jk}$is the weight of the packet forwarded from Node$_i$ to Node$_j$. j is the node's id, and k is the number of packets.

Similarly, $CF_{2j}, CF_{3j}$.... calculated.

$NF_{ij}$ are some packets that are not forwarded or not correctly transmitted to node $_j$ from node $_i$.

$\delta_{jk}$ is the weightage of the packet forwarded from node$_j$ to node$_i$ . The weightage of the packets is assigned as shown in Table 1.

**Table 1:** Packets Weight

| S.No. | Importance | Value |
|---|---|---|
| **1.** | Rare/ Important | >=0.6 |
| **2.** | Control packets | >=0.4 to <0.6 |
| **3.** | Unwanted | <0.4 |

Existing trust models in the literature typically focus on direct trust, which refers to the level of trust established between two neighboring nodes based on their past interactions. This approach involves analyzing how these nodes have interacted in the past, such as how reliably they have forwarded packets to each other. By examining these interactions, the model estimates the likelihood of a node acting cooperatively in the future. This focus on direct trust lays the groundwork for more complex trust assessments within ad-hoc networks. Many researches overlook the various interaction intervals that could produce various affects when calculating the direct trust evaluation. TS-AODV methodology separates the several effects of each interaction period to determine the node's precise trust value.

If the system addresses dynamic fluctuations in trust, it incorporates adaptive trust mechanisms to adjust trust values based on changes in network conditions or node behavior. This can help to prevent trust degradation or excessively punitive measures. Here, each interaction interval is analyzed by the timestamp mechanism, set as $\Delta t$ = 15 seconds up to current time T, there are *n* intervals from time 0 such that the total elapsed time is T[$t_1$, $t_2$, ..., $t_n$]. The trust value of the node $V_i$ is estimated using the following equation (2) for the k$^{th}$ interaction interval.

$$TV_{P_i}(t_k) = \frac{\sum_{i\neq j}^{n} CF_{ij}}{\sum_{i\neq j}^{n} \left(CF_{ij} + NF_{ij}\right)} \frac{\sum_{i\neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} CF_{jk}}{\sum_{i\neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} CF_{jk} + \sum_{i\neq j}^{n} \sum_{j=1,k=1}^{n,m} \delta_{jk} NF_{jk}} - - - [2]$$

$$TV_{P_i}(t) = \frac{\sum_{k=1}^{n} TV_{P_i}(t_k) \times a_k}{\sum_{k=1}^{n} a_k} - - - [3]$$

$TV_{P_i}(t_k)$ represents the current trust value of a node at time interval $t_k$. The node's character will not be reflected by the current trust value, which can be ascertained only from its behavioral history. The past trust values aggregated.

The aggregated trust value of node$_i$ is calculated according to the history of interactions through the above equation [3]. In eq. [3], $a_k = e^{-(N-n)}, 0 < e^{-(N-n)} < 1, 1 \leq k \leq n$, and the attenuation factor is represented as the base coefficient $e^{-(N-n)}$.

## Methodology

In TS-AODV, trust values are calculated based on a node's historical behavior in forwarding packets. The following factors are typically considered:

- The percentage of packets a node successfully forwards compared to the total received.
- The percentage of packets delivered correctly to their intended destinations.
- The alignment of forwarded packets with the network's purpose and goals.
- The promptness with which packets are forwarded, considering network dynamics.

A weighted average is used to combine these factors into a single trust value. The weights are adjusted dynamically based on network conditions and the specific requirements of the application. Trust values are updated periodically based on a node's recent behavior. This can be done using a sliding window approach, where only the most recent interactions are considered. Alternatively, a decay function is used to reduce the impact of older interactions over time.

When a node exhibits positive behavior, such as successfully forwarding packets or providing accurate routing information, its trust value is increased. Conversely, negative behavior, such as dropping packets or forwarding them to incorrect destinations, leads to a decrease in trust value. The magnitude of the adjustment is based on the severity of the event and the node's historical behavior.

Trust values are typically stored locally on each node, allowing for decentralized management. Nodes periodically exchange trust information with their neighbors to maintain an up-to-date view of the network's trust landscape. Trust thresholds are defined to categorize nodes as trustworthy, untrustworthy, or suspicious. Routing decisions are made based on these thresholds. For example, packets may be preferentially routed through nodes with high trust values, while nodes with low trust values may be avoided.

To avoid forgery of trust values by malevolent nodes reputation system is used to aggregate trust information from multiple sources. This can help to make it more difficult for malicious nodes to manipulate trust values, as they would need to corrupt the reputation of multiple nodes.

The trustworthiness of new nodes upon their integration into the network is evaluated by assigning initial trust value based on their reputation or credentials. For example, nodes belonging to trusted organizations or individuals might be assigned higher initial trust values. The network observes the behavior of new nodes over a while to assess their trustworthiness. This could involve monitoring their packet forwarding behavior, their compliance with network protocols, and their interactions with other nodes. By following this comprehensive methodology, we were able to provide a rigorous evaluation of TS-AODV's performance and demonstrate its advantages over existing secure routing protocols for MANETs. The findings of this evaluation contribute to the advancement of secure communication in dynamic and challenging network environments.

## Experimental Setup

To evaluate TS-AODV's performance, we have utilized the NS-2 network simulator and ran simulations under varying conditions. The first scenario mimicked a network of 100 nodes scattered randomly across a 2000 meter by 2000 meter rectangular area. Each node possessed a fixed transmission radius of 200 meters, restricting communication to immediate neighbors. Node mobility was modeled using the random waypoint model, where nodes travel at random speeds following similar movement patterns. Packets could be transferred between nodes as they change locations. Constant bit rate traffic was used in the simulations. This means that the nodes generated a constant amount of traffic, regardless of the network conditions. By setting the maximum node speed to zero, the network became static. Table 2 details the specific simulation parameters employed for this initial evaluation.

**Table 2:** Simulation Parameters

| Parameter | Value |
|---|---|
| Simulation time | 200 s |
| Topology Size | 2000 ×2000 m |
| Number of nodes | 100 |
| Mobility model | Random Way Point (RWP) |
| Traffic type | Constant bit rate |
| Packet size | 512 bytes |
| Transmission radius | 200 m |
| Connection rate | 2 pkts/s |
| Pause time | 2 s |

TS-AODV routing protocol using the following metrics to evaluate the performance of the routing protocol

- Packet Delivery Ratio (PDR): The percentage of packets that are successfully delivered to their destination.
- End-to-End Delay: The average time it takes for a packet to be delivered from its source to its destination.
- Routing Overhead: The amount of control traffic generated by the routing protocol.

The PDR measures the protocol's ability to deliver data reliably, while the end-to-end delay measures its efficiency. The routing overhead measures the protocol's overhead in terms of resource consumption. In addition to these metrics, it also evaluates the performance of TS-AODV in terms of its ability to detect and isolate malicious nodes. This is done by comparing the number of malicious nodes detected by TS-AODV to the number of malicious nodes that are present in the network.

## Results and Discussion

This paper proposes a novel routing protocol for Mobile Ad-hoc Networks (MANETs) termed Trusted Ad hoc On-Demand Distance Vector (TS-AODV). Building upon the well-established AODV protocol, TS-AODV prioritizes enhanced security. It achieves this by integrating a trust mechanism, enabling the network to assess node trustworthiness and favor routes that bypass malicious actors. Notably, TS-AODV preserves the core functionalities of AODV while mitigating attacks from misbehaving nodes through trust-based routing. To assess its effectiveness, we have conducted comprehensive tests using the NS-2 network simulator, comparing its performance against the original AODV. This evaluation will determine if TS-AODV offers significant improvements in security and reliability for MANETs.

### Scenario 1: Varying Node Speeds

The first test compared TS-AODV and AODV by varying node speeds from 0 to 30 m/s (meters per second). As illustrated in Figure 2, the packet delivery ratio of TS-AODV increased significantly as speed increased, while AODV's performance (measured by Packet Delivery Ratio or PDR) gradually declined. This difference became more pronounced at higher speeds. The key factor behind this disparity lies in how each protocol handles malicious nodes. AODV's traditional routing process cannot detect malicious nodes, leading to a decrease in packet delivery ratio. In contrast, TS-AODV's trust mechanism allows it to obtain more accurate trust values for nodes. This translates to a higher probability of successful packet delivery because TS-AODV can favor routes that bypass malicious actors.

Figure 3 illustrates the average end-to-end delay experienced by packets in both protocols. As node speeds increase, route entries in nodes become less reliable due to frequent movement. The comparison shows that AODV suffers from higher average delays at the maximum speed of 30 m/s compared to TS-AODV. This difference can be attributed to TS-AODV's ability to detect and avoid malicious nodes. By selecting routes that bypass these malicious actors, TS-AODV reduces the need to resend packets due to failed routing attempts. This ultimately leads to lower overall delays for packet delivery.

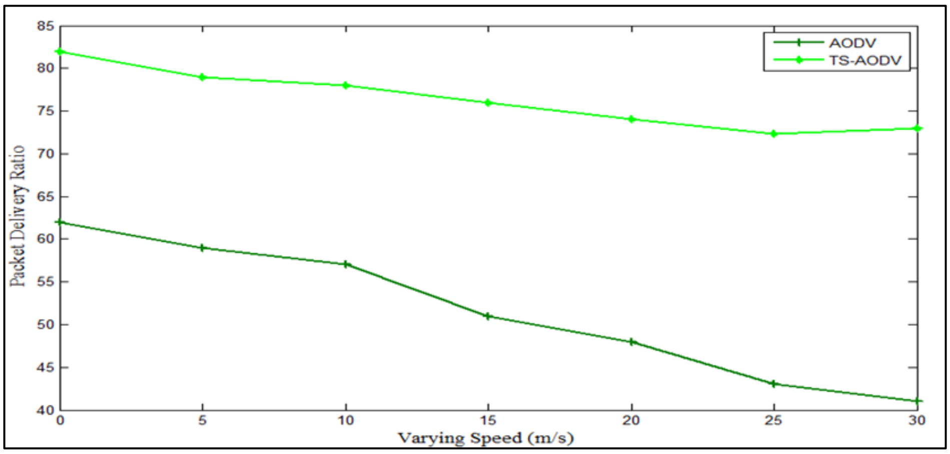

**Figure 2:** Packet Delivery Ratio (PDR) versus Different Node Mobility Speed

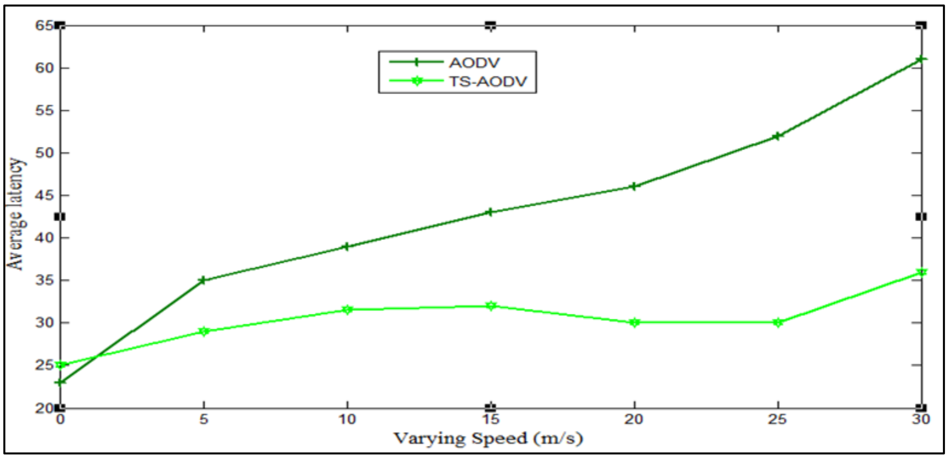

**Figure 3:** Average Latency versus Varying Mobility Speed (m/s)

Figure 4 compares the routing overhead generated by TS-AODV and AODV. At lower node speeds (under 15 m/s), AODV exhibits lower overhead due to its simpler routing process without trust considerations. However, this advantage disappears as speed increases. TS-AODV requires more routing packets (Route Request - RREQ and Route Reply - RREP) initially to discover reliable routes that meet its trust requirements. This is because nodes move quickly, leading to a greater number of intermediate nodes involved and more RREQs being initiated. However, this investment pays off in the long run. As TS-AODV avoids nodes with low trust values during route discovery, it reduces overall routing overhead in the future. In contrast, AODV's lack of trust estimation becomes a liability at higher speeds. With frequent route disruptions due to unreliable nodes, AODV is forced to send more route request and maintenance packets to find alternative paths. This significantly increases its routing overhead compared to TS-AODV.

## Scenario 2: Varying Number of Malicious Nodes

We tested the TS-AODV protocol against malicious nodes represented in Figure 5, there were only a few malicious actors in the network, both AODV and TS-AODV performed well, with a packet loss of just 4%. However, as the number of malicious nodes increased, packet delivery rates suffered significantly. With roughly 10 malicious nodes present, the AODV delivery ratio dropped dramatically, going from 96% down to only 38%. This clearly demonstrates the disruptive influence of malicious nodes in the network.

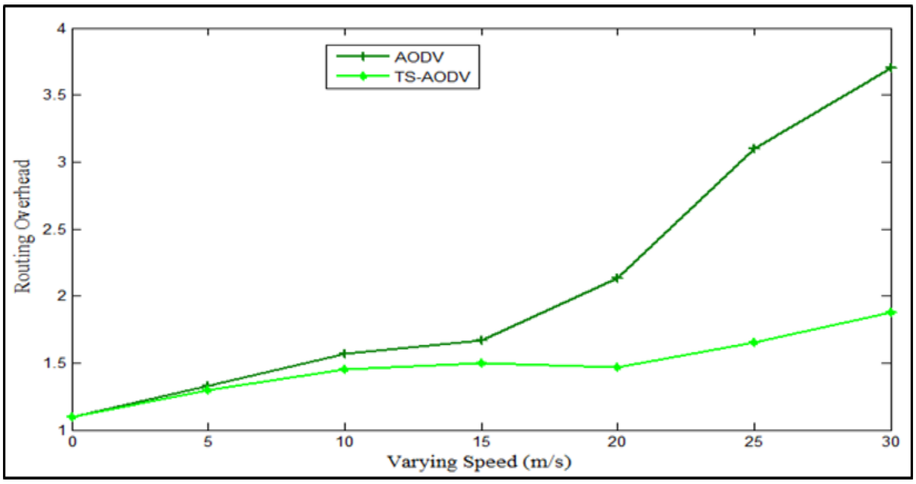

**Figure 4:** Routing Overhead versus Varying Mobility Speed

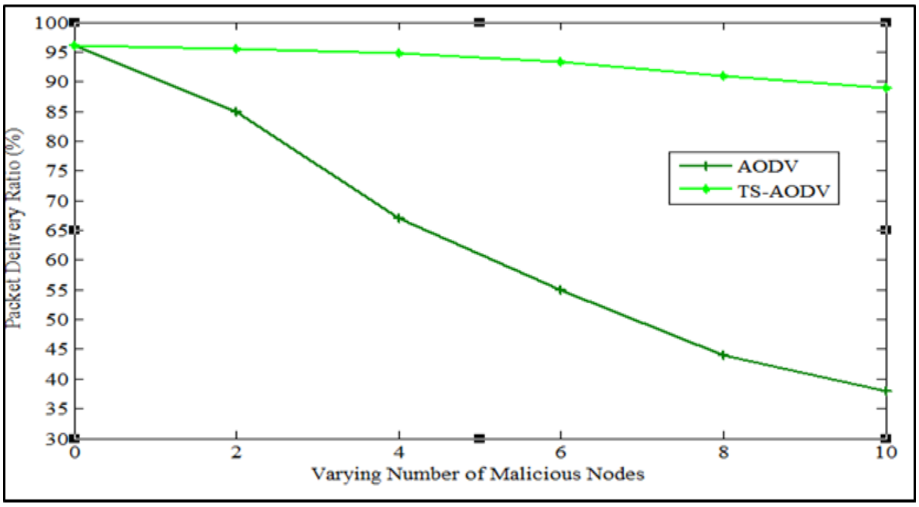

**Figure 5:** Malicious Nodes versus Packet Delivery Ratio (PDR)

Figure 6 highlights a key advantage of TS-AODV over AODV reduced delay. While AODV suffers from a significant increase in average delay, TS-AODV experiences a decrease. This difference is attributed to how each protocol handles queuing and retransmission, two major contributors to overall delay. TS-AODV likely experiences less queuing delay, and its superior ability to identify malicious nodes leads to fewer retransmissions, further reducing delay. This advantage stems from TS-AODV's core functionalities: prioritizing reliable routes for data transmission, effectively identifying and avoiding malicious nodes, and minimizing retransmissions. Overall, TS-AODV achieves a significant reduction in end-to-end delay compared to AODV.

Both AODV and TS-AODV exhibit increased routing overhead as the number of malicious nodes grows, but in contrasting ways. Figure 7 showcases this difference. When malicious nodes are scarce (less than 5), TS-AODV initially incurs a higher overhead compared to AODV. This is likely due to its use of additional control packets (RREQ and RREP) for trustworthiness verification during route discovery. However, the trend reverses as malicious nodes become more widespread (over 5, or 20% of total nodes). In such scenarios, AODV's overhead skyrockets, exceeding TS-AODV's. This dramatic rise in AODV's overhead is likely caused by the significant data packet loss occurring on paths containing malicious nodes. AODV's reactive nature forces frequent route rediscovery due to these losses, leading to a surge in control packets. In essence, TS-AODV's proactive approach to identifying trustworthy routes incurs a slightly higher upfront overhead, but this investment pays off when malicious nodes become more prevalent as it avoids the substantial overhead associated with AODV's reactive route rediscovery.

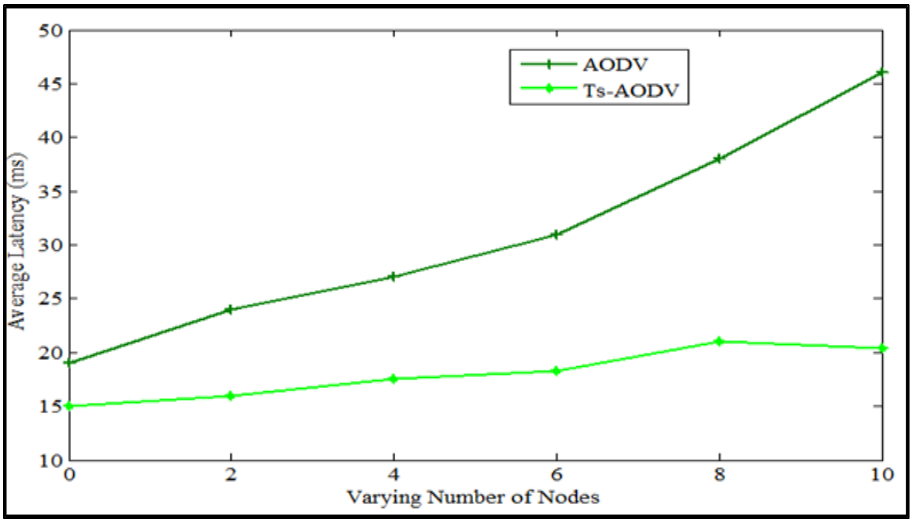

**Figure 6:** Average Latency versus Different Malicious Nodes

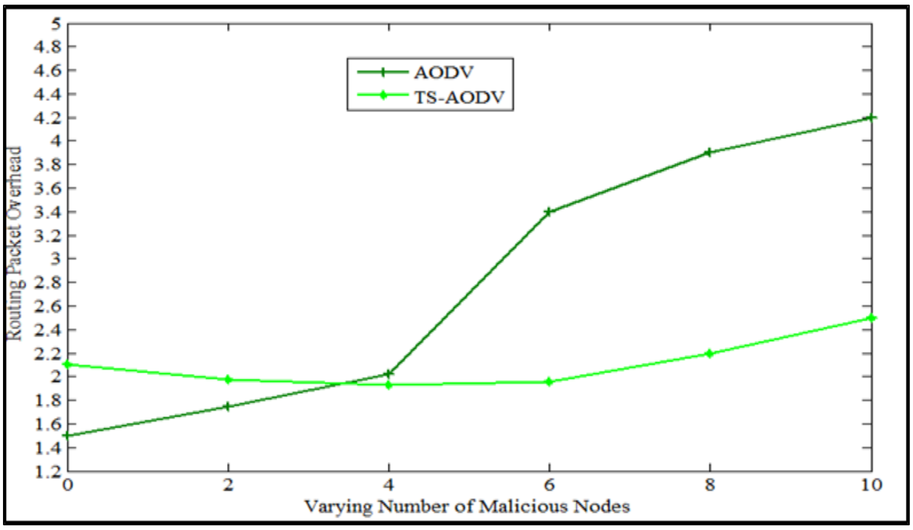

**Figure 7:** Routing Packet Overhead versus Varying Number of Malicious Nodes

## False Positive and False Negative Detection Rates in TS-AODV

A simulated MANET with 100 nodes, including 10 malicious nodes. Malicious nodes engage in various attacks, such as packet dropping, forwarding packets to incorrect destinations, and generating false routing information. The following metrics were used for the simulation:

- False Positive Rate: Number of benign nodes incorrectly identified as malicious / Total number of benign nodes

- False Negative Rate: Number of malicious nodes not identified as malicious / Total number of malicious nodes

Figure 8 showcases that TS-ADOV protocol exhibits a relatively low false positive rate, indicating that it is generally effective in avoiding misidentifying benign nodes as malicious. The false negative rate shows some variation, with occasional spikes. This suggests that the protocol might miss some malicious nodes, particularly when they employ sophisticated evasion techniques. Overall, the protocol demonstrates good accuracy in detecting malicious nodes. However, there is room for improvement in reducing false negatives to enhance security.

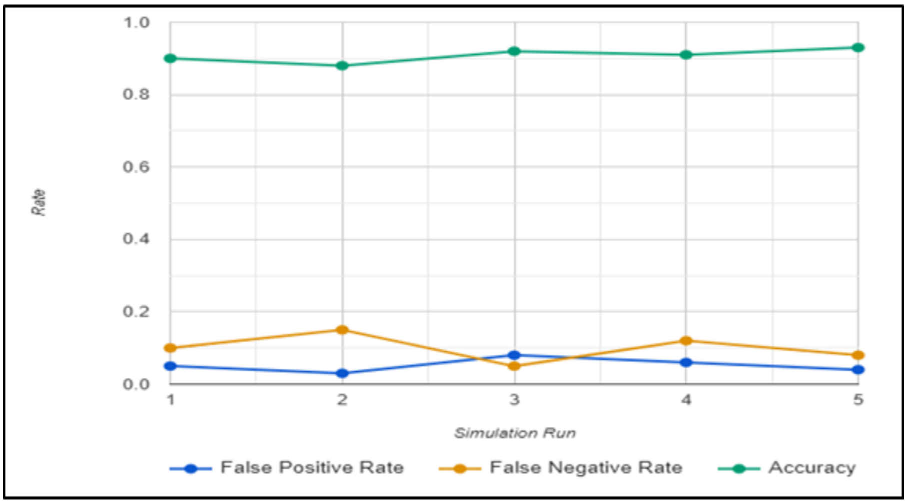

**Figure 8:** False Positive and False Negative Detection Rates in TS-AODV

## Energy Consumption

Overall, the energy consumption of TS-AODV compared to conventional AODV is based on the following factors:

- TS-AODV uses a trust-based routing mechanism that prioritizes routes with nodes that have higher trust values. This potentially reduces the number of routes that need to be explored, which could lead to lower energy consumption.
- TS-AODV can detect and isolate malicious nodes, which leads to lower energy consumption. This is because malicious nodes can waste energy by generating unnecessary traffic or by dropping packets.

The experiments across various scenarios conclusively demonstrate the superiority of TS-AODV over AODV in mobile ad-hoc networks (MANETs). TS-AODV shines in three key aspects: it achieves a higher delivery ratio, ensuring data reaches its destination; it enhances network throughput, allowing for smoother information flow; and it boasts a superior detection ratio for malicious nodes, promoting network security. These combined advantages position TS-AODV as a promising protocol for reliable and secure communication in MANETs, particularly when dealing with malicious actors.

# Conclusion

Driven by their diverse and critical applications, Mobile Ad-Hoc Networks (MANETs) have captured significant research interest. However, the inherent lack of centralized infrastructure and dynamic nature of these networks make them susceptible to a wide range of security attacks. Consequently, securing communication in MANETs remains a crucial challenge. This paper addresses this issue by proposing TS-AODV, a trusted secure routing protocol built upon the Ad-hoc On-demand Distance Vector (AODV) protocol with enhanced trust features. The protocol leverages trust values based on a node's packet forwarding behavior to improve security. Simulation results demonstrate TS-AODV's superiority over the baseline AODV protocol. Future research should focus on achieving a stable routing scheme that considers factors like node mobility, channel bandwidth limitations, link load, and resource constraints within MANETs.

## Abbreviations

ABC: Artificial Bee Colony, AODV: Adhoc On-demand Distance Vector Protocol, AOTMDV: An on-demand trust-based multi-path distance vector protocol, ATDSR: Agent-based trust dynamic source routing protocol, DSR: Dynamic Source

Routing, FTDSR: Fuzzy Trusted Dynamic Source Routing, FTP-DSR: Fuzzy-based Power-aware Trusted Dynamic Source Routing Protocol, IDS: Intrusion Detection System ,MANET: Mobile Ad hoc Networks, MAC: Message Authentication Code, PDR: Performance development review, RREQ: Route Request Packet, RREP: Route reply packet, TS-AODV: Trusted Security-Enhanced-Adhoc On-demand Distance Vector Protocol, TORA: Temporally Ordered Routing Algorithm.

## Acknowledgement

Nil.

## Author Contributions

All authors equally contributed.

## Conflict of Interest

The authors declare no conflicts of interest.

## Ethics Approval

Not applicable.

## Funding

None.

# References

1. Vijaya I, Rath AK, Puthal B, Mishra D, Satapathy S. Performance Analysis of QoS Parameters of MANET on Mobility and Energy based Model with Different MANET Routing Protocols. Indian Journal of Science and Technology. 2016 Oct;9(37):1-4.
2. Griffiths N, Jhumka A, Dawson A, Myers R. A simple trust model for on-demand routing in mobile ad-hoc networks. In Intelligent Distributed Computing, Systems and Applications: Proceedings of the 2nd International Symposium on Intelligent Distributed Computing–IDC, Catania, Italy. 2008:105-114.
3. Pirzada AA, McDonald C, Datta A. Performance comparison of trust-based reactive routing protocols. IEEE transactions on mobile computing. 2006 Apr 24;5(6):695-710.
4. Hughes T, Denny J, Muckelbauer PA, Etzl J. Dynamic trust applied to ad hoc network resources. In Autonomous Agents and Multi-Agent Systems Conference, Melbourne, Australia. 2003.
5. Vijayakumar K, Somasundaram K. Study on reliable and secure routing protocols on manet. Indian Journal of Science and Technology. 2016 Apr;9(14):1-10.
6. Lu R, Li X, Liang X, Shen X, Lin X. GRS: The green, reliability, and security of emerging machine to machine communications. IEEE communications magazine. 2011 Apr 5;49(4):28-35
7. Perkins CE, Royer EM. Ad-hoc on-demand distance vector routing. Proceedings WMCSA&#39;99. Second IEEE Workshop on Mobile Computing Systems and Applications. 2002 Aug 06: 90-100
8. Johnson DB, Maltz DA. Dynamic source routing in ad hoc wireless networks. Mobile computing. The Kluwer International Series in Engineering and Computer Science. 1996 Feb 29; 353: 153-81.
9. Royer EM, Toh CK. A review of current routing protocols for ad hoc mobile wireless networks. IEEE personal communications. 1999 Apr;6(2):46-55.
10. Eissa T, Abdul Razak S, Khokhar RH, Samian N. Trust-based routing mechanism in MANET: Design and implementation. Mobile Networks and Applications. 2013 Oct;18:666-77.
11. Marchang N, Datta R. Light-weight trust-based routing protocol for mobile ad hoc networks. IET information security. 2012 Jun 1;6(2):77-83.
12. Xia H, Jia Z, Li X, Ju L, Sha EH. Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks. 2013 Sep 1;11(7):2096-114.
13. Deb N, Chaki N. TIDS: trust-based intrusion detection system for wireless ad-hoc networks. In Computer Information Systems and Industrial Management: 11th IFIP TC 8 International Conference, CISIM 2012, Venice, Italy. 2012:80-91.
14. Jensen CD, Connell PO. Trust-based route selection in dynamic source routing. In the International conference on trust management. 2006 May 16:150-163.
15. Wei G, Zhongwei X, Zhitang L. Dynamic trust evaluation based routing model for ad hoc networks. InProceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing. 2005 Sep 26;2:727-730.
16. Xia H, Jia Z, Ju L, Zhu Y. Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory. IET wireless sensor systems. 2011 Dec 1;1(4):248-66.
17. Halim IT, Fahmy HM, El-Din AM, El-Shafey MH. Agent-based trusted on-demand routing protocol for mobile ad hoc networks. In2010 Fourth International Conference on Network and System Security. 2010 Sep 1:255-262.
18. Jayalakshmi V, Razak TA. Trust based power aware secure source routing protocol using fuzzy logic for mobile adhoc networks. IAENG International Journal of Computer Science. 2016 Feb 1;43(1):98-107.
19. Jayalakshmi V, Razak TA. Energy based trusted source routing protocol for mobile adhoc networks. ARPN Journal of Engineering and Applied Sciences. 2015 Oct;18(2):108-119.
20. Jayalakshmi V, Razak TA. Trust based power aware secure source routing protocol using fuzzy logic for mobile adhoc networks. IAENG International Journal of Computer Science. 2016 Feb 1;43(1):98-107.
21. Suseendran G, Sasi Kumar A. Secure intrusion-detection system in mobile adhoc networks. Indian journal of Science and Technology. 2016 May;9(19):1-6.
22. Elhoseny M, Shankar K. Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE transactions on reliability. 2019 Jun 6;69(3):1077-86.
23. Keerthika V, Malarvizhi N. Enhanced AODV protocol to secure routing in MANET with optimization techniques [J]. International Journal of Engineering & Technology. 2018;7(2):75-9.
24. Jain AK, Choorasiya A. Security enhancement of AODV routing protocol in mobile ad hoc network. In the 2nd International Conference on Communication and Electronics Systems (ICCES). 2017 Oct 19:958-964.