



Enhancing IoT Security with Trust-Based Mechanism for Mitigating Black Hole Attacks

Mahalakshmi Govindaraj^{1*}, Suresh Arumugam²

¹ Department of Computer Science, Periyar University, Salem 636011, Tamil Nadu, India

² Department of Computer Science, Sona College of Arts and Science, Salem 636011, Tamil Nadu, India

Corresponding Author Email: priyamahamga@gmail.com



<https://doi.org/10.18280/ijssse.130515>

ABSTRACT

Received: 30 April 2023

Revised: 24 August 2023

Accepted: 13 September 2023

Available online: 10 November 2023

Keywords:

routing, Mobile Ad Hoc Network (MANET), Ad hoc On-demand Multipath Distance Vector (AOMDV), IoT, intrusion detection

This study focuses on enhancing both security and network performance in Mobile Ad Hoc Networks (MANETs) by integrating a trust model with the Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. The inherent structure of MANETs, characterized by dynamic, wireless connections between mobile nodes and a lack of centralized supervision, makes these networks particularly susceptible to security threats. Traditional security solutions designed for fixed networks prove inadequate for the unique challenges posed by ad hoc networks. We explore the benefits of multipath routing, which establishes multiple paths between source and destination nodes, thereby improving the reliability of data transmission and achieving load balancing. However, these benefits are undermined without a robust security framework. To this end, we introduce a trust model as a key mechanism for enhancing security. Trust is not only crucial for decision-making but also vital for the design and analysis of secure distribution systems. By assessing the trustworthiness of nodes, we aim to enhance both security and routing performance. Simulation results suggest that our proposed trust-based routing protocol is effective. Detailed findings will elucidate how this integrated approach can address the pervasive security challenges in MANETs while optimizing network performance.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are rapidly evolving, self-organizing networks that exhibit a remarkable capability for swift deployment. Their adaptability has proven beneficial in numerous real-world applications [1]. With a surge in the number of portable devices and advancements in wireless communication, the popularity of ad hoc networking continues to grow. This networking paradigm's almost infrastructure-less nature allows for its use anytime and anywhere. The applications of MANETs span a wide range, from small, static, power-constrained networks to large, mobile, dynamic networks. As legacy systems adapt to such ad hoc environments, it is expected that the number of devices and applications will increase [2].

The inherent properties of MANETs, such as self-organization and adaptability, require devices within these networks to possess the ability to detect other existing devices. This is essential for performing the necessary setup to facilitate communication, data sharing, and service provision. In addition to maintaining network connections, these devices should be capable of adding and removing devices from the network. The highly mobile nature of the nodes can lead to unpredictable and swift changes in network topology over time. Given the decentralized nature of these networks, the nodes must ensure that both data delivery and network organization are effectively carried out.

In MANETs, users can access and exchange information irrespective of geographical location or the presence of traditional network infrastructure. The absence of a fixed

infrastructure, a unique characteristic distinguishing MANETs from other mobile networks, and dynamic connections lend these networks a distinct advantage in terms of robustness and flexibility [3]. The primary objective of MANETs is to extend this flexibility into self-sustaining, mobile, and wireless domains where nodes can function as both routers and hosts, forming the infrastructure to route the network in an ad hoc manner. The dynamic nature of wireless networks makes routing a significant challenge. An ad hoc network, in a typical setting, is characterized by a set of constantly moving nodes that form a transient network dynamically in the absence of any network infrastructure. Within such a network, mobile nodes coordinate to exchange information for specific durations. Given that these nodes remain mobile during data exchange, networks must continually adapt to establish paths without external support.

Various ad hoc networks have been developed with different routing protocols, which can be categorized based on several conditions. Route discovery forms a critical criterion for categorization. Based on this, routing protocols can be either reactive or proactive. In the former, such as Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector routing (AODV), route requests are initiated on-demand. If a node wishes to establish communication with another, it sends a route request and awaits a response from the destination [4]. Contrarily, proactive protocols such as Optimized Link State Routing (OLSR) continuously update routing information to maintain a comprehensive overview of the network topology.

The Ad hoc On-demand Distance Vector (AODV) protocol

is among the most commonly utilized within the realm of MANETs. Its distinguishing feature is the on-demand routing mechanism, which is initiated only when paths to other nodes need to be discovered or verified, thereby enhancing the routing efficiency. The two fundamental operations of the AODV protocol are route discovery and route maintenance. Route discovery is initiated when a node intends to communicate with a destination for which it lacks a valid route entry [5]. Route maintenance can be achieved in two ways. One approach involves a node broadcasting connectivity information via local hello messages, enabling nearby nodes to listen to these packets and determine connectivity. An alternative approach utilizes a link or network layer mechanism, such as the IEEE802.11 Media Access Control (MAC) protocol [6].

The Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol represents an evolution from the AODV protocol. This reactive protocol is designed to identify multiple node-disjoint and link-disjoint paths [7], evaluating multiple loop-free paths. A drawback of this approach is the increased message overhead due to extensive flooding during route discovery. As a multipath routing protocol, AOMDV might encounter substantial control overhead due to the necessity for the destination node to respond to multiple Route REQuests (RREQs). This results in the generation of larger overhead packets in response to a single RREQ packet [8].

In recent times, trust-based routing has been considered a promising security solution. To protect the routing protocol, a trust-based scheme is employed. Each network node independently implements a trust model to estimate its trust level in other network nodes, which can then be incorporated into routing decisions. Unlike traditional routing protocols which prioritize establishing the shortest route, trust models aim to establish the most trusted routes [9].

For design and the deployment of the security systems, trust is a crucial factor. Trust evaluation in MANET can be used in trust routing, node authentication and access control. Evaluating the trustworthiness of the related nodes results in enhanced security and also better routing performance. Trust refers to the belief that is held with respect to factors like dependability, reliability, honesty, competence etc. in reference to a particular context.

The evaluation of the direct trust value, which may be either positive or negative, is predicated on the direct experience of the trustor node with the trustee node. In instances where the trustor lacks sufficient trust in the trustee node, the recommendation of a third node may be necessitated. Once both direct and recommendation trust values are acquired by the trustor node, a combination formula may be required to strike a balance between the direct and recommendation trust [10, 11].

This paper proposes an augmentation of the AOMDV protocol with a trust model, aimed at enhancing network performance. The second section provides a review of the relevant literature. The methodology is elucidated in the third section, while the fourth section presents the empirical findings. The paper concludes with the fifth section.

2. RELATED WORK

Wei et al. [12] introduced a novel trust model under which trust values are assessed based on various factors including prior interactions, contextual considerations, and references

from neighboring nodes. This model, when integrated with the Ad hoc On-demand Multipath Distance Vector protocol (AOMDV), forms a new trusted multipath routing protocol, the Trust-based AOMDV (TAOMDV). The TAOMDV protocol offers flexibility by selecting either the shortest path or multiple paths from all trust-satisfied routes, thereby facilitating load balancing. Empirical evidence demonstrates that the TAOMDV protocol not only reduces end-to-end latency but also improves the network loss ratio.

In a further advancement of the AOMDV protocol, Alkhamisi and Buhari [13] proposed a Trust-based Secured Adhoc On-demand Multipath Distance Vector (TS-AOMDV) protocol. This protocol was developed based on nodes' routing behavior with the aim of identifying and mitigating intrusions such as gray hole attacks, black hole attacks, and flooding within Mobile Ad-hoc NETWORKS (MANETs). A comparative analysis was performed using the NS2-based simulation tool between the proposed TS-AOMDV and the existing AOMDV. The performance evaluation revealed that the proposed TS-AOMDV protocol significantly improved throughput by 57.1% compared to AOMDV, particularly in challenging scenarios, thus demonstrating the superiority of TS-AOMDV over the AOMDV routing protocol.

Further enhancing network security, Poornima and Khasim Vali [14] proposed an improved TS-AOMDV strategy, or Trust-based Secured Ad-hoc On-demand Multipath Distance Vector. Unlike the AOMDV Routing protocol, the TS-AOMDV approach integrates an Intrusion Detection System and incorporates a trust-based routing factor, thereby delivering enhanced security and routing performance.

A groundbreaking trust model designed to factor in black hole and gray hole attacks was proposed by Qu et al. [15]. Building upon this model, they presented an extension of the AOMDV, a light-weight trust-based multipath routing protocol named LWT-AOMDV. The principal focus of this proposed work was the establishment of numerous reliable and trusted paths, including the identification of compromised nodes. By employing on-demand route maintenance and incorporating the concept of path error in lieu of route error, the control overhead was reduced. Simulation results via the NS-2 simulator illustrated that the proposed method enhances the packet delivery ratio, albeit at the cost of utilizing additional resources.

Shabut et al. [16] investigated the potential of trust in determining the optimal path between two nodes. They proposed identifying the most trustworthy route based on a multidimensional mechanism for calculating trust, which includes the number of hubs, trust opinion, confidence in providing trust, and the energy contained by the nodes in the route. The model went beyond merely considering the nodes' trustworthiness along the route and incorporated route optimization for selecting the path from source to sink. Experimental results substantiated the robustness and accuracy of the trust model within MANETs.

In a subsequent study, Shabut et al. [17] introduced a friendship-based trust model for securing the routing protocol from source to destination within MANETs. This model incorporated several levels of friendships to determine the trustworthiness of the nodes. The nodes' behavior was likened to human patterns to illustrate the complexity of trust and provide diverse perspectives. This approach addressed the limitation of previous models that neglected the social behavior of nodes during trustworthiness evaluations. Experimental analyses demonstrated the enhanced robustness

and accuracy of the trust model in dynamic MANETs.

Jain and Baras [18] proposed a straightforward approach for applying point-to-point trust metrics derived from various techniques to secure routing. The primary advantage of the proposed method lies in its compatibility with existing on-demand routing protocols with minimal alterations, and its ability to employ both link trust and additional node trust. The authors emphasized scenarios that underscore the need for associating trust with both the node and the link. The security features of the proposed scheme in ad-hoc networks were validated through simulation.

Marchang and Datta [19] suggested a light-weight trust-based routing protocol, in which limited computational resources are consumed to estimate the trust a node has in another, using the Intrusion Detection System (IDS). The use of local information ensures scalability. This technique can be incorporated into any routing protocol that has used AODV as the base routing protocol for evaluating the proposed method and presenting performance analysis.

Thanigaivel et al. [20] proposed TRUNCMAN, a trust-based routing mechanism. As a trust-based routing protocol, TRUNCMAN encourages non-cooperation against corrupted nodes. This information is relayed to all other network nodes, ensuring security. The simulation of the protocol across the seven layers would be particularly intriguing. Thus, the non-cooperative movement would be used to segregate the compromised nodes, and the proposed method also assured trust among the network nodes.

Halim et al. [21] introduced a novel protocol based on self-monitoring (agent-based) and following the DSR algorithm, named Agent-Based Trusted DSR (ATDSR) Protocol for MANETs. A novel and more practical model for evaluating trust has been incorporated, factoring in the number and size of relayed packets to reflect the "selective forwarding" node behavior. The superiority of the proposed protocol over the trusted DSR was demonstrated through simulation evaluation of protocol performance. Various environmental conditions such as movement rates, malicious nodes, and host density were used for conducting the simulations.

Li et al. [22] proposed a reactive routing protocol utilizing a trust model, capable of identifying more than one trusted route during discovery to meet the dependability requirements of data packets. The framework offered a feasible approach for selecting the shortest route, which was evidenced to improve the packet delivery ratio.

Jassim et al. [23] introduced a security-enhanced AODV routing protocol known as R-AODV (Reliant Ad hoc On-demand Distance Vector Routing). This protocol incorporates a modified trust mechanism - Direct and Recommendations trust model - which is then integrated into AODV. This modification enables AODV not only to identify the shortest path, but also the most trusted one. Simulation results demonstrated that R-AODV provides enhanced data transfer reliability compared to standard AODV, particularly when compromised nodes exist within the MANET.

Ferdous and Muthukkumarasamy [24] conducted an analysis and comparison of three protocols: OLSR, DSR, and AODV. The metrics employed included throughput, packet delivery ratio, and delay, and the Network Simulator (NS2) served as the experimental tool. The power consumption of two trust-based models, TLEACH and Node-based Trust Management (NTM), were compared with the performance analysis of these protocols. Simulation outcomes revealed superior performance of OLSR compared to AODV and DSR.

3. METHODOLOGY

In the context of Mobile Ad hoc Networks (MANETs), blackhole attacks manifest when data packets are enticed by malicious nodes through the utilization of fresh routes, followed by the abandonment of these packets [7]. This work introduces a proposal for a trust-based routing method intended to mitigate blackhole attacks.

The trust metric contains the following properties [11]:

- Dependency on the context: Only in certain contexts, the trust relationship have a certain meaning.
- Function of uncertainty: Evaluating the possibility whether an entity performs or not is referred to as trust.
- Whether a given entity will perform the action or not is evaluated by Trust.
- Quantitative values: either continuous or discrete numeric values can be used for representing trust.
- Asymmetric: Trust need not be two way process. That is, if AX trusts Y, it is redundant to clutch that Y trusts X.
- Transitive: Trust is transitive, i.e., Suppose node B is trusted by A and node C is trusted by B, then C must also be trusted by A.
- Personalized: The matter of trust is highly subjective and the trustworthiness about the same entity may be evaluated differently by two people.

The suggested trust based ad hoc on demand multipath distance vector protocol is explained in the current section.

3.1 Ad hoc On-demand Multipath Distance Vector

A multipath extension on top of AODV is the ad hoc on demand multipath distance vector routing. For enabling multiple paths, the process of route discovery has been altered. The disjointedness of the links is considered for multiple paths so that the nodes only and not the edges are shared. Also, using the sequence number of the nodes assures loop freedom. Due to the need to address the problems, split the traffic along each path and packet reorder at the destination, a single path is chosen. Another feature that distinguishes the AOMDV is the usage of periodic HELLO messages for detecting the sales path [25].

A list of subsequent hops plus the hop counts for these are included in the routing entries, for keeping a track of multiple paths. Same sequence number is possessed by all the next hops. Hop count that is promoted is defined as the maximum hop count for all the paths. This, in turn, is maintained by a node for every destination. For sending route promotions to the receiving nodes, this is the hop count that is used. Each duplicate route promotion that a node receives defines an alternate path to the destination.

If and only if the hop count for a path is lesser than the promoted one for the destination does a node accept that alternate path. This is to ensure loop freedom. As the greatest value of the hop count is used, the promoted hop count remains the same for the same sequence number [26]. The subsequent hop list along with the advertised hop count will be initialized again when the route promotion is obtained for a destination that has a higher sequence number. For finding node-disjoint or link disjoint routes, AOMDC can be used and for finding node-disjoint routes, the duplicate RREQs are not instantly rejected by every node.

A node- disjoint path is defined by the source with different

neighbor arriving by each RREQ. Any two Route requests arriving at an intermediate node with neighbor distinct from that as the source wouldn't have crossed the same node as the nodes cannot send repeated route requests. For obtaining multiple link-disjoint routes, the sink node sends responses to duplicate Route requests. The response of the destination is to the RREQs that have unique neighbors. The RREPs after the first hop, follow the reverse path, which are both node as well as link disjoint. Even though the trajectories of every RREP may traverse the intermediate node, every RREP takes a distinct reverse path to the source for ensuring link disjointness [27].

The AOMDV, while still choosing the disjoint paths, enables the intermediate nodes to respond to the RREQs and this is the main benefit it offers. AOMDV has a lot of message overheads, as there is increased flooding during route discovery. Also, being multipath routing protocol, the destination responds to the multiple RREQs whose results are in longer overhead.

3.2 Proposed trust model

Trust derivation, its computation and evaluation are performed by the trust model. It is from the packet forwarding ratio that every node derived trust factor. A linear aggregate technique has been used to estimate the trust of the entire node trust as per the trust factors and a path's trust can be evaluated least value method. Trust based discovery of route and its selection are included in the trust application.

The firsthand information for the neighbors is Direct trust which can be easily achieved. Using the history of the direct interactions among the nodes for trust computation, the trust model can be simplified. After obtaining the service of a forwarding node, the procedure of trust evaluation is a routing process which is a remark of the sender. Due to gray hole, black hole attack, heavy traffic and poor wireless communication are the factors for packet dropping. Thus we can say that the quality of forwarding is evaluated using packet forwarding ratio.

The cumulative count of accurate forwards is denoted as $N_C(t)$, and the total count of all requests made up to time t is represented as $N_A(t)$. Within a given timeframe from time t_i-w to t_i , the correct forwarding count is calculated as $N_C(t_i) - N_C(t_i-w)$, with w signifying the duration of the time window. The packet forwarding ratio within the i -th window, denoted as $FR(t_i)$, is established according to the following Eq. (1) [28]:

$$FR(t_i) = \begin{cases} \frac{N_C(t_i) - N_C(t_i - w)}{N_A(t_i) - N_A(t_i - w)}, & t_i > w \\ \frac{N_C(t_i)}{N_A(t_i)}, & t_i \leq w \end{cases} \quad (1)$$

where, $i=1,2,3$.

The concept of verifying whether packets dispatched from node j to node k for forwarding have indeed been forwarded by node k is encapsulated by the notion of trust between the two nodes. This trust factor is referred to as the trust of node j towards node k . To ascertain the overall trustworthiness of a specific node, the trust values from two trust factors, namely the Control packet Forwarding Ratio (CFR) and the Data packet Forwarding Ratio (DFR), are assigned relative weights. The direct trust of node j in node k , denoted as T_{jk} , is quantified

using the subsequent Eq. (2):

$$T_{jk}(t_i) = w_1 \times CFR_{jk}(t_i) + w_2 \times DFR_{jk}(t_i) \quad (2)$$

In this equation, $CFR_{jk}(t_i)$ corresponds to the control packet forwarding ratio, and $DFR_{jk}(t_i)$ indicates the data packet forwarding ratio witnessed by node j when forwarding to node k at time t_i . The parameters w_1 symbolize the weights allocated to the Control packet Forwarding Ratio (CFR), while w_2 symbolize the weights assigned to the Data packet Forwarding Ratio (DFR).

Within the phase of route discovery, the RRQ flooding invasion happens. It attacks the packet in route that invalid network destination. An IDS observe the cohort of the packet from the source and the source' trust value is allocated. Initially every node allocates the trust value like one. The original trust value is measured by an IDS; then, as per the route discovery of these nodes, the network is apprised on this by the IDS. When IDS check the trust value for all the neighboring nodes [29]. Every node checks for the source' trust value when the source node sends the route request packets to the neighbors. If the source' trust value <the threshold, the source is thereby dropped, thwarting the attack. In case the source' trust value is distinct from all the nodes, its trust value will be lesser than the threshold because of which it cannot forward the route request to the destination node.

For establishing a trusted routing path, the trust model carries out the following steps [30].

1. Initializing the statistics that are concerned with network trust and that of all the network nodes.
2. After the operations like dropping and forwarding of packets etc. of every node, updating the network statistics related to trust.
3. Broadcasting route request for the destination when it is established.
4. Upon reception of a route request by a destination, a route reply is sent and the route's trust is initialized to 0.
5. The intermediate nodes compute their trust value using network statistics when receiving route reply; this is added to the path's trust in the route reply packet.
6. The source node stores the path when it obtains a reply for the first time. The data packets are sent along that path. The source node, on obtaining many path replies will compare the New Andy received path's trust with that of the current route and the path having the maximum trust is stored.
7. The routing path is updated to the ones with most trust, periodically.

4. RESULTS AND DISCUSSION

During the simulation experiments, a tailored Wireless Sensor Network (WSN) was crafted using MATLAB. This network involved the random deployment of 200 nodes across a two-dimensional space measuring 1000×1000 units. Each node was initially endowed with an energy level of 2J. The size of the data packets 30 bits. Two scenarios were considered: 5% and 10% of nodes in the network were malicious. The conducted experiments aimed to compute several key metrics, including PDR, delay, the count of links to the destination, and

the percentage of malicious nodes identified. The outcomes of these experiments were tabulated in Tables 1 through 4.

Table 1. Packet delivery ratio

Node Pause Time (s)	AOMDV-5% Malicious	AOMDV-10% Malicious	Trust-5% Malicious	Trust-10% Malicious
10	7.8	7.4	5.2	5.8
30	7.1	7	5.2	5.2
50	6.4	6.6	4.4	4.8
70	5.6	5.9	4.7	4.7
90	3.8	4.3	3.4	3

Table 2. Average end to end delay in second

Node Pause Time (s)	AOMDV-5% Malicious	AOMDV-10% Malicious	Trust-5% Malicious	Trust-10% Malicious
10	0.0186	0.0121	0.0086	0.0144
30	0.0057	0.002	0.0014	0.0047
50	0.004	0.0019	0.0014	0.0031
70	0.0019	0.0017	0.0012	0.0014
90	0.0015	0.0014	0.001	0.0012

Table 3. Average number of hops to destination

Node Pause Time (s)	AOMDV-5% Malicious	AOMDV-10% Malicious	Trust-5% Malicious	Trust-10% Malicious
10	0.6272	0.6111	0.739	0.7221
30	0.681	0.673	0.8325	0.7895
50	0.7079	0.6876	0.8598	0.8401
70	0.7242	0.7003	0.862	0.8421
90	0.7865	0.7386	0.8871	0.8101

Table 4. Percentage of malicious node detected

	Trust-5%	Trust-10%
Percentage	84	86

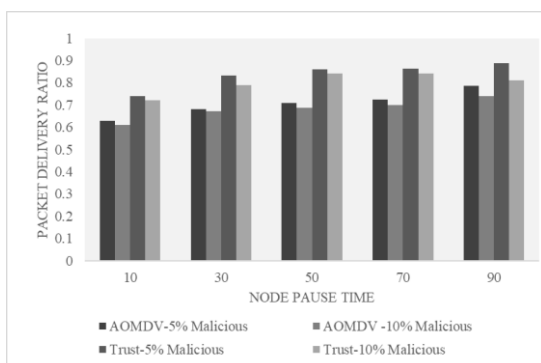


Figure 1. Packet delivery ratio

Figure 1 clearly indicates that the introduced trust model exhibited noteworthy enhancements in packet delivery ratio when subjected to scenarios involving malicious nodes. Specifically, the proposed trust model demonstrated a remarkable 20.02% enhancement in packet delivery ratio compared to the AOMDV protocol under the influence of 5% malicious nodes, with a node pause time of 30 seconds. Moreover, when confronted with 10% malicious nodes and a

node pause time of 50 seconds, the proposed trust model showcased a substantial 19.96% improvement in packet delivery ratio compared to the AOMDV protocol. Figure 2 shows the delay analysis.

Figure 3 proved that the proposed trust model achieves better performance than the other conventional models.

It can be observed from the Figure 4 that the proposed trust model with 10% of malicious nodes improved the percentage of malicious nodes detected by 2.35% than trust model with 5% of malicious nodes.

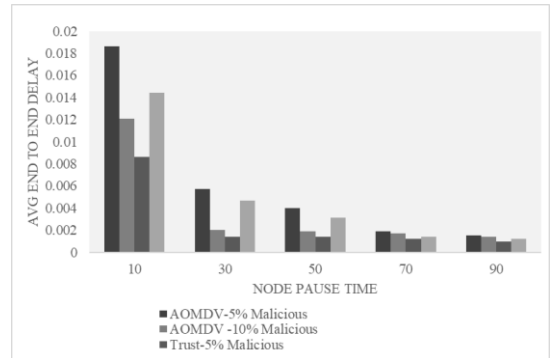


Figure 2. Average End to End Delay in second

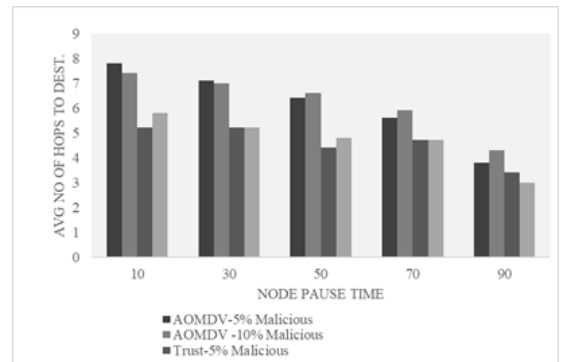


Figure 3. Average number of hops to destination

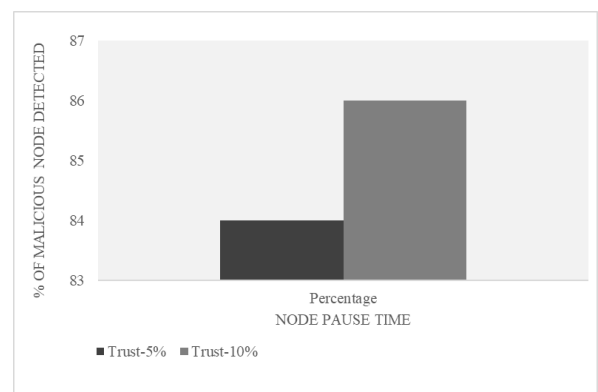


Figure 4. Percentage of malicious node detected

5. CONCLUSION

The concept of trust is intricate and abstract, influenced by various factors including circumstances and many other elements, creating a complex psychological cognitive process. This study presents a trust-based ad hoc on-demand multi-path distance vector (AOMDV) routing protocol designed for

Mobile Ad hoc Networks (MANETs) as an extension of the AOMDV protocol. The proposed protocol introduces a mechanism for identifying malicious nodes and its effectiveness is assessed through extensive experiments. The trust model influences the decision-making for selecting next hops or forward paths in the routing strategy. The empirical analysis highlights significant enhancements achieved by the suggested trust-based approach across various performance metrics, including packet delivery ratio, end-to-end delay, the number of hops to the destination, and the percentage of malicious nodes detected. Notably, the proposed trust model demonstrated a substantial 20.02% improvement in packet delivery ratio compared to the AOMDV protocol in scenarios involving 5% malicious nodes, alongside a node pause time of 30 seconds. Similarly, with 10% malicious nodes and a node pause time of 50 seconds, the proposed trust model exhibited a notable 19.96% enhancement in packet delivery ratio compared to the AOMDV protocols.

REFERENCES

- [1] AlRubaieci, M., sh Jassim, H., Sharef, B.T., Safdar, S., Sharef, Z.T., Malallah, F.L. (2020). Current vulnerabilities, challenges and attacks on routing protocols for mobile ad hoc network: A review. *Swarm Intelligence for Resource Management in Internet of Things*, 109-129. <https://doi.org/10.1016/B978-0-12-818287-1.00012-7>
- [2] Valaboju, Y. (2018). Routing and Vulnerabilities in MANETS. *International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)*, 1(2).
- [3] Alo, R.U., Stanly, N.I., Onwe, N.F. (2018). Mobile Ad Hoc Network (MANET): Applications, benefits and performance issues in a global positioning system. *International Research Journal of Engineering and Technology (IRJET)*, 5(11).
- [4] Yi, J., Adnane, A., David, S., Parrein, B. (2011). Multipath optimized link state routing for mobile ad hoc networks. *Ad Hoc Networks*, 9(1): 28-47. <https://doi.org/10.1016/j.adhoc.2010.04.007>
- [5] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, 110(4): 1637-1658. <https://doi.org/10.1007/s11277-019-06788-y>
- [6] Hassnawi, L.A., Ahmad, R.B., Yahya, A., Aljunid, S.A., Elshaikh, M. (2012). Performance analysis of various routing protocols for motorway surveillance system cameras' network. *International Journal of Computer Science Issues*, 9(2): 7-21.
- [7] Mesleh, A. (2018). Black hole attack evaluation for AODV and AOMDV routing protocols. *International Journal of Electronic Security and Digital Forensics*, 10(3): 207-227. <https://doi.org/10.1504/IJESDF.2018.092994>
- [8] Aggarwal, I., Garg, E.P. (2013). AOMDV Protocols in MANETS: A review. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)*, 32: 32-34.
- [9] Salari-Moghaddam, S., Taheri, H., Karimi, A. (2019). Trust based routing algorithm to improve quality of service in DSR protocol. *Wireless Personal Communications*, 109(1): 1-16. <https://doi.org/10.1007/s11277-019-06546-0>
- [10] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H., Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, 105(1): 1475-1490. <https://doi.org/10.1007/s11277-019-06155-x>
- [11] Kaneria, J., Diwanji, H. (2014). A Survey on Trust Models in MANET. *International Journal of Engineering Development and Research*, 2(1): 678-682.
- [12] Wei, D., Cao, H., Liu, Z. (2016). Trust-based Ad hoc On-demand Multipath Distance Vector routing in MANETS. In 2016 16th International Symposium on Communications and Information Technologies (ISCIT), Qingdao, China, pp. 210-215. <https://doi.org/10.1109/ISCIT.2016.7751623>
- [13] Alkhamisi, A.O., Buhari, S.M. (2016). Trusted secure Adhoc on-demand multipath distance vector routing in MANET. In 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, pp. 212-219. <https://doi.org/10.1109/AINA.2016.105>
- [14] Poornima, S., Khasim Vali, D. (2017). A survey on TS-AOMDV routing protocol in MANET. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCCE)*, 6(4): 614-615. <https://doi.org/10.17148/IJARCCCE.2017.64115>
- [15] Qu, C., Ju, L., Jia, Z., Xu, H., Zheng, L. (2013). Light-weight trust-based on-demand multipath routing protocol for mobile ad hoc networks. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, pp. 42-49. <https://doi.org/10.1109/TrustCom.2013.9>
- [16] Shabut, A.M., Dahal, K., Awan, I., Pervez, Z. (2015). Route optimasation based on multidimensional trust evaluation model in mobile ad hoc networks. In 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, pp. 28-34. <https://doi.org/10.1109/InfoSec.2015.7435502>
- [17] Shabut, A.M., Dahal, K., Awan, I. (2014). Friendship based trust model to secure routing protocols in mobile ad hoc networks. In 2014 International Conference on Future Internet of Things and Cloud, Barcelona, Spain, pp. 280-287. <https://doi.org/10.1109/FiCloud.2014.51>
- [18] Jain, S., Baras, J.S. (2013). Distributed trust based routing in mobile ad-hoc networks. In 2013 IEEE Military Communications Conference, pp. 1801-1807. <https://doi.org/10.1109/MILCOM.2013.304>
- [19] Marchang, N., Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. *IET Information Security*, 6(2): 77-83. <https://doi.org/10.1049/iet-ifs.2010.0160>
- [20] Thanigaivel, G., Kumar, N.A., Yogesh, P. (2012). TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network. In 2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), Bangkok, Thailand, pp. 261-266. <https://doi.org/10.1109/DICTAP.2012.6215430>
- [21] Halim, I.T.A., Fahmy, H.M., El-Din, A.M.B., El-Shafey, M.H. (2010). Agent-based trusted on-demand routing

- protocol for mobile ad hoc networks. *Wireless Network*, 21: 467-483. <https://doi.org/10.1007/s11276-014-0793-z>
- [22] Li, X., Jia, Z., Zhang, P., Wang, H. (2010). A trust-based multipath routing framework for Mobile Ad hoc NETWORKS. In *Seventh International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2010, Yantai, Shandong, China*, pp. 773-777. <https://doi.org/10.1109/FSKD.2010.5569349>
- [23] Jassim, H.S., Yussof, S., Kiong, T.S., Koh, S.P., Ismail, R. (2009). A routing protocol based on trusted and shortest path selection for mobile ad hoc network. In *2009 IEEE 9th Malaysia International Conference on Communications (MICC), Kuala Lumpur, Malaysia*, pp. 547-554. <https://doi.org/10.1109/MICC.2009.5431438>
- [24] Ferdous, R., Muthukumarasamy, V. (2016). A comparative performance analysis of MANETs routing protocols in trust-based models. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA*, pp. 880-885. <https://doi.org/10.1109/CSCI.2016.0171>
- [25] Kaur, R., Mahajan, R., Singh, A. (2013). A survey on multipath routing protocols for MANETS. *International Journal of Emerging Trends and Technology in Computer Science*, 2(2): 42-45.
- [26] Mueller, S., Tsang, R., Ghosal, D. (2004). Multipath routing in mobile ad hoc networks: Issues and challenges. *Performance Tools and Applications to Networked Systems*, Springer, Berlin, Heidelberg, 209-234. https://doi.org/10.1007/978-3-540-24663-3_10
- [27] Barange, M.Y., Sapkal, A.K., Bhonge, S. (2016). Analysis of single path AODV Vs multipath AOMDV in MANET. *International Journal of Innovative Research in Computer and Communication Engineering*, 4(5): 8582-8588.
- [28] Li, X., Jia, Z., Zhang, P., Zhang, R., Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET information security*, 4(4): 212-232. <https://doi.org/10.1049/iet-ifs.2009.0140>
- [29] Praveena, A., Sangeetha, R., Prem, P.E. (2017). Efficient trusted secure ad-hoc on-demand multipath distance vector in MANET. *International Journal of Engineering Development and Research*, 5(2): 1614-1620.
- [30] Patel, V.H., Zaveri, M.A., Rath, H.K. (2015). Trust based routing in mobile ad-hoc networks. *Lecture Notes on Software Engineering*, 3(4): 318-324.