International Journal of Advanced Technology in Engineering and Science
Vol. No. 10, Issue No. 02, February 2022
www.ijates.com
ijates
ISSN 2348 - 7550

# A TRUST BASED MECHANISM IN MULTIPATH ROUTING FOR MITIGATING BLACK HOLE ATTACKSUSING PARTICLE SWARM-SHUN OPTIMIZATION

**[1]G. Mahalakshmi, [2]Dr. A. Suresh ,**

*[1]Research Scholar, Periyar University, Salem.*

*[2]M.C.A., M.Phil., Ph.D., SET., HOD, Department of Computer Science, Sona College of Arts and Science, Salem.*

*Mail Id: priyamahamga@gmail.comMail Id:* ***asuresh1975@yahoo.com***

**ABSTRACT**

Mobile Ad hoc Network (MANET) has the ad hoc interconnection of a mobile node group with each other without any centralised administration. For ad hoc routing, the implementation of a security mechanism is quite arduous due to its singular network traits. In MANET, blackhole attacks can occur when malicious nodes use a fresh destinate route to attract data packets and then drop the packets. For the mitigation of blackhole attacks, this work has given the proposal for a trust-based routing having a probability of a new packet forwarding. This work's Ad hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol is based on the trust model which will measure the trust of nodes and then will make a decision. Proposal for a novel optimisation technique for the multipath routing's enhancement is dependent on the Particle Swarm Optimisation (PSO)-Shun Optimisation algorithm. It is evident from the simulations that the proposed technique is able to attain better performance through enhancement of the network longevity as well as Packet Delivery Ratio (PDR), and also through reduction of the end-to-end delay.

*Keywords: Mobile Ad hoc Network (MANET), Routing, Attacks, Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing Protocol, Trust, Particle Swarm Optimization (PSO) and Tabu Search (TS).*

## 1 INTRODUCTION

A Multi-Agent System (MAS) will constitute multipleintelligent agents which interact amongst themselves. An individual agent will communicate as well as cooperate with other agents in order to accomplish its objectives. A MobileAd Hoc Network (MANET) will constitute wireless mobile nodes that dynamically form a self-organised MAS,there are nopredefined infrastructures and every node will operate as the host as well as the routers. With message transmission, it is possible to accomplish inter-agent communication in a MANET. Intermediate nodes are required to forward messages for two distinct nodes outside the range ofdirect communication. MANETs are considered to be collaborative since the assumption is that every node can relay packets for the othernodes [1].

Key characteristics of MANET include:ability to work without a central coordinator, quick deployment, self-configurable,multi-hop radio communication, regular link breakage because of mobile nodes,resource (lifetime of the battery, power for computation, bandwidth, and so on) constraints, and very dynamic topology due to all nodes being mobile. Therefore, routing protocols in MANET have to face the following critical challenges:being fully distributed, adaptivity to constant changesin topology, simple computation as well as maintenance, optimal as well as loop-free route, optimal resource utilization, Quality of Service (QoS)capacity, and minimal collisions [2].

Finding a path between the communicatingnodes is quite a daunting task in MANET. Characteristics of this network type are inclusive of thecentralised infrastructure's absence, dynamic topology,energyconstraints, node heterogeneity, multi-hop as well as constrained bandwidth. In MANET, the routing will identify a path between thesource and the destination for forwarding the packets. However, the routing procedure is quite difficult due to its dynamic features, constrained bandwidth, constant changes in topology due to node mobility as well as the MANET's energy usage. The routing protocol must identify theshortest path between the source and the destination as well as be adaptive. Proactive, reactive, andhybrid protocols [3] are the three key categories of routing protocol classification.

Introduction of multipath routing approaches was done for the detection of multiple paths between source-destination pairs. Benefits of multiple routes between a source-destination pair are inclusive of: higher bandwidth utilisation, lower end-to-end delay, higher throughput, higher network longevity, and so on. Moreover, it will apply the network with

load balancing by carrying the traffic via multiple paths. It will also decrease the network congestion as well as offer protection from route failures. Multipath routing's mechanism for path discovery is quite similar to the single path routing in MANET. It will primarily pick disjoint paths to carry forward the traffic between the source and the destination. Link-disjoint and node-disjoint are the two different types of multipaths. Given a source-destination(s-d)pair, the set of link-disjoint routes is made up of paths which have no common links except for the constituent s-d path. Likewise, for the node-disjoint approach, the routes are made up of paths which do not have the presence of any common node (except for the s-d path) in more than a single constituent path. The various numbers of paths between a s-dpair is evaluated within a single route discovery attempt by the MANET multipath on-demand routing protocols. The initiation of an operation of new routediscovery will only occur when there has been failure of every path between a s-dpair [4].

There active routing discovery-based Ad-hoc On-Demand Distance Vector Routing (AODV)protocol employs three distinct message types: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR). Moreover, there is utilisation of the destination sequence numbers to always ensure loop freedom. In the AODV protocol, every source node will identify a new route by the RREQ's limited flooding using ring expansion and will acquire a route to its destination through the RREP. The AOMDV protocol will expand the AODV to a multipath routing protocol where the source node will retain numerous distinct routes from many number of RREPs. Nevertheless, the AOMDV's static route selection is unable to deal with the network's dynamic changes like severe congestion as a result of biased traffic [5].

A MANET is only able to exist as well as effectively operate with the cooperative behaviour of the network nodes. Even so, MANETs frequently get attacked by malicious or selfish nodes like selective forwarding (grey-hole) attacks ,and packet dropping (blackhole)attacks, due to its open working environment. It is possible to mitigate the damage from malicious nodes through careful selection of dependable paths in MANET. Thus, for a MANET [1], it is a critical to design adependable routing protocol.

For the network's basic functionality, the security in MANET is paramount. With the satisfactory resolution of security issues, it is possible to accomplish the network service availability, and the data's integrity as well as confidentiality. Usually, MANET has to confront various attacks on security due to its traits such as the lack of a clear defense

mechanism, absence of central surveillance as well as management, cooperative algorithms, dynamic changes to its topology and open medium. Such factors have made it awar-like situation for the MANET in confronting threats to security [6].

A vital role is served by the trust computation in exploitation of the agents' trust when the network has the presence of malicious nodes. The trust model's key function is to collect, disseminate as well as accumulate the feedback of the earlier participant nodes. While the trust is defined as the relationship between a network's two distinct nodes, the trust computation will categorise the nodes into non-trusted and trusted nodes. Quantification of the value of trust computation will be within the limit 1 to -1, in which +1 represents the trusted nodes,0 represents the unknown nodes, and -1 represents the non-trusted nodes. Direct, indirect, recent, and historic are the four chosen trust computations for the prediction of the trusted source as well as the destination nodes [7].

- **Direct trust**: Also termed the local trust,direct trust will represent the trust portion, wherein a node will compute from its self-experience with regards to the target nodes.
- **Indirect trust**: Also termed the recommendation, the indirect trust will compute from the neighbouring nodes' experience with regards to the target node.
- **Recent trust**: Being an of the direct as well as the indirect trust, the recent trust will take into account the target node's recent behaviours.
- **Historical trust**: Evaluation of the historical trust is done by taking into account the past experiences as well as the long-term behavioural pattern of the target node.

In MANET, there is utilization of swarm optimisation techniques for detection of the best and optimal solution from all possible outcomes. The application of numerous optimisation techniques in MANET have offered a high performance as well as better outcomes. These techniques are primarily focused on the optimisation approaches that would make the network more effective as well as reliable without any loss of the original link during the transfer of data. Utilisation of these optimisation techniques will make it easier to detect the eligible solution from every outcomes. It is possible to detect the optimal and best solution using numerous optimisation approaches. For the purpose of optimisation, biologically influenced algorithms refers to the category of algorithms which have similar

performance as that of nature. These algorithms' benefits facilitate the resolution of diverse problems: First, in order to arrive at a solution, it does not have to follow any mathematical approaches. Second, the results can be acquired very quickly and also are accurate [8].

In this work, proposes the PSO-Shun (i.e. PSO-Tabu Search (TS)) algorithm for multipath routing in MANETs. The remaining part of the investigation is organized into the following sections. Section two discusses related works in literature. Section three explains various methods used in the work. Section four discusses experimental results and section five concludes the work.

## 2 RELATED WORKS

Narmadha [9] had proposed a Winnow Trust based Multipath Route Discovery (WT-MRD) mechanism. This mechanism involved the construction of multiple paths from the source to the destination with less amount of time as well as higher security. At first, the Neighbour Node-based Trust Calculation (NN-TC) Model would evaluate every node's trust value on the basis of the node cooperative count, data packet forwarding rate as well as packet drop rate. This was followed by the nodes' classificationby the Winnow Linear Multiplicative Classification (WLMC) Algorithm into malicious or normal categories. With the assistance of normal nodes, the WT-MRD Mechanism would send two control messages: RREQ and RREP, to identify multipath from the source to the destination.

Alkhamisi et al., [10] had developed an extension of the AOMDV routing protocol known as the Integrated Incentive and Trust-based optimal path identification in AOMDV (IIT-AOMDV) for MANET. This proposed protocol had involved the integration of an Intrusion Detection System (IDS) together with the Bayesian Network (BN) based trust and payment model. The IDS would employ the BN's empirical first-hand as well as second-hand trust information, and would underpin the Cuckoo Search (CS) algorithm in mapping the QoS as well as the trust value into one fitness metric, which was tuned as per the malicious nodes' presence of. It was evident from the simulation outcomes that, in comparison to the present AOMDV integrated with the IDS (AID), the IIT-AOMDV had improvements of 20% in detection accuracy as well as 16.6% in throughput.

Panda & Pattanayak [11] had addressed security through the utilisation of diverse algorithms, and had found that the evolutionary technique-based algorithms were the most

efficient amongst them. For optimisation, one of the renowned evolutionary algorithm was the Ant Colony Optimisation (ACO). A comprehensive review of the ACO-based secure MANET routing protocols was done to aid researchers in developing secure routing protocols, particular utilising the ACO algorithm, to address the MANET's issues of security.

For message transmission to multiple nodes, an efficient routing scheme is the multicast routing. However, it is essential to fulfil multiple QoS assurances for these applications. Singh et al., [12] had made a presentation for the Genetic oriented QoS Multicast Routing (GA-QMR) algorithm. This effective algorithm was used to detect the optimal multicast tree which could fulfil multiple QoS parameters than the other two algorithms. Moreover, it could simultaneously explore various paths from a single node,pick the best path on the basis of the parameters' quality, and also accomplish global convergence. It was essential that the routes could fulfil the bandwidth, packet success rate, packet loss rate, jitter, end-to-end delay, and so on.

Dixit & Singhai [13] had presented the PSO algorithm to pick the favourablevalues for the AODV routing protocol's parameters in order to boost the QoS in MANET. Resolution of the routing problem involved the PSO'smetaphorical usage of agents such as insect community entities . Routing-based swarm agents had described a collection of rules to be followed by the participating nodes. For successful completion of the swarm agents' assigned tasks, they had done effective as well as adaptive exchange of information related to their behaviour. PSO algorithm would employ the maximum flow objective to give preference for the swarm agents' best locations during every step of network operation. Utilisation of the PSO along with the aid of parameters for QoS such as average delay, throughput, and jitter, was able to boost the AODV's performance.

## 3 METHODOLOGY

In this section, the AOMDV protocol, PSO, TS and PSO-Shun methods are discussed.

### 3.1 Adhoc on-Demand Multipath Distance Vector Routing (AOMDV) Protocol

The AODV protocol will begin the route discovery procedure by sending a Route REQuest (RREQ) to the destination across the network. Upon receipt of a non-duplicate RREQ, the intermediate node will record the earlier hop as well as check for a new and valid route entry to the destination. The node will send the source a Route REPly (RREP) together with a

unique sequence number. Upon update of the route information, there will be the route reply'spropagation as well as acquisition of additional RREPs if a RREP has either found a shorter route or has a bigger destination sequence number (newer). The AOMDV's development from the AODV, a unipath path on-demand routing protocol, could eliminatefrequent link failures as well as route breakages from occurring in highly dynamic ad hoc networks. The two stages involved in the AOMDV protocol's detection of multiple paths: a route update rule to establish as well as maintain multiple loop-free paths at every node, and a distributed protocol for the link-disjoint paths' [14] detection.

The AOMDV protocol would identify link-disjoint or node-disjoint routes between the source and the destination. The occurrence of link failures could be due to collision of packets, traffic congestion, failure of the nodes, mobility of the nodes, etc. For the detection of node-disjoint routes, the duplicate RREQs do not get rejected right away by each node. There is an acquisition of a node-disjoint path by every RREQ which arrives from the source's diverse neighbours since the nodes are unable to broadcast the duplicate RREQs. Any two RREQs that arrive at an intermediate node via the source's diverse neighbours would not have travelled over a common node. For the acquisition of multiple link-disjoint routes, the destination will send RREP to the duplicate RREQs irrespective of their first hop. In order to ensure the link-disjointness in the RREP's first hop, the destination will only reply to RREQs that arrive via unique neighbours. The RREPs would follow reverse paths, that are node-disjoint and hence, link-disjoint after the first hop. In order to ensure link-disjointness, every RREP would only intersect at an intermediate node, and also would take a different reverse path towards the source.

The multipath routing's underlying idea is to seek multiple routes to a host in order to avoid any active attacks. There may be numerous reasons to do this as it will minimise the end-to-end delay in a transfer between two nodes prior to the disappearance of their employed link. The AOMDV protocol's [15] benefits include: ability to establish route on demand, ability to yield loop-free nodes,ability to maintain the connectivity,and swift as well as effective failure recovery. Drawback of the AOMDV protocol's utilisation is it having more message overheads at the time of route discovery because ofan increase in flooding, and due to it being a multipath routing protocol, the destination would reply to the various RREQs,resulting in the formation of longer overhead packets in response to a single RREQ packet,which in turn, can cause heavy control overhead.

### 3.2 Particle Swarm Optimisation (PSO) Algorithm

A point within an n-dimensional solution space will indicate a solution of the problem in the PSO algorithm. The PSO's operation involves the random motion of a number of particles across the space. At every iteration, the fitness values of the individual particle as well as its neighbours are noted. These particles will try to mimic its successful neighbours by shifting towards their direction. Diverse scheme are used to compute the grouping particles, wherein all the particles are part of a one global flock or there is utilization of semi-independent flocks. In 995, inspired by the research on bird flocking behaviour, Kennedy and Eberhart had devised the PSO [16].

PSO will commence with a randomparticle group. Afterwards, it will search for the optimal solution by updating the generations, wherein the update of every particle will occur using the *pbest* and the *gbest* values. *pbest* is the best solution (fitness). On the other hand, *gbest* is known as the global best. This value is trackedby the PSO and it will be the best value attained so far by any particle in thepopulation. A portion of the population is taken by the particle as itstopological neighbours, and *lbest* (local best) will be the best value. In mathematical terms, there will be random initialisation of the particle swarm over the search space and this swarm will determine a new solution by traversing the dimensional space. For the $i^{th}$ particle at the $k^{th}$iteration, the velocity will be $V_k^i$ and the position will be $P_K^i$. Thus, using Equation (1) and Equation (2), the $i^{th}$ particle's velocity as well as position at$(k + 1)^{th}$ iteration can be updated as below:

$$V_{k+1}^i = w.V_k^i + C_1.rand_1.(pbest_k^i - P_k^i) + C_2.rand_2.(gbest_k^g - P_k^i) \quad (1)$$

$$P_{k+1}^i = P_k^i + V_{k+1}^i \quad (2)$$

Here,$w$ will indicatethe inertia weight, constants$C_1$and $C_2$will indicate thelearning factors (generally equivalent to 2), while $rand_1$ and $rand_2$ will indicate random numbers between 0 and 1.

Determination of the potential routes'fitness values are made from the neighbouring nodes' length as well as energy. Suppose that the nodes are a, b, … ,and so on.The value of fitness of node 'a' can be determined from the neighbouring node 'b', which in turn is the route's next node in Equation (3).

$$fitness_a(R1) = w\left(\frac{total\ energy_{R1}}{\max.energy}\right) + l\left(\frac{\max.edge\ count}{total\ edge\ count_{R1}}\right) \qquad (3)$$

In this equation, *w* will indicatethe route energy's weight factor, and *l* will indicate the route length's weighting factors. *total energy*$_{R1}$will indicate the node energy level ofroute $R_1$, max. *energy* will indicate the maximumnode energy level of every potential route from the given current node,*total edge count*$_{R1}$will indicate the total number of edgesbetween the neighbour node 'b' to the destination node, and max. *edgecount* will indicate the maximum edge count amongst the neighbournodes.

### 3.3 Tabu Search (TS) Algorithm

As per the Oxford dictionary, the term 'taboo' is defined as a social or religious custom which prohibits or restricts a particular practice or forbidsany association with a specificthing, place, or person. In 1986, Glover and Hansen had described that the TS "is a meta-heuristic superimposed on another heuristic. The overall approach is to avoid entrainment in cycles by forbidding or penalizing moves which take the solution, in the next iteration, to points in the solution space previously visited ("hence tabu")". The TS's underlying principle is that it does have some memory of the states already investigated by it, and that it will not revisit these states for a certainperiod of time [17].

The TS aids in two ways: (1) Prevents the search from getting into a loop,that is, to continuously search the same area without making any actual progress, and (2) Assist the search in exploring regions which it may have otherwise not explored.

TS algorithm is given as follows: TS (particle X, number of iterations, tabu size)

1. Consider best to be initially equivalent to particle X.

2. Clear the Tabu List.

3. For 1 to number of iterations:

    i. Consider a null bestmove.

    ii. Consider a null bestpair.

    iii. For every unordered pair (i,j) that is not in the tabu list and enclosed inside the specified range:

a. swapped = swap the $i^{th}$ and $j^{th}$ elements in best.

b. if fitness (swapped) is better than fitness (bestmove), thenbestmove = swapped and bestpair = (i,j).

c. best = bestmove.

d. if cardinality(tabu list) = tabu size, then bestpair will replace the oldest pair; else,append bestpair to tabu list.

4. If fitness(best) is better than fitness(X), return best; else, return X.

### 3.4 Proposed Hybrid PSO-Shun (i.e. PSO-TS) Algorithm

The PSO's key drawbacksare its premature convergence as well as the problem of local optimum. The TS is used as a local search procedure to overcome these constraints.It has been the incorporated to enrich the globalbest solution as well as to utilise the diversification mechanism for guiding the search towardsthe search space's other feasible regions. This was followed by the development of a novel hybrid technique known as the PSO-TS.This technique constitutes strong cooperation amongst PSO as well as TS. It fully takes advantage of the PSO's exploration capability as well as the TS's exploitation capability [18].

Below is the workflow of the PSO-TS (as depicted in Figure 1):

1. After establishing the initialpopulation with the recommended strategy for swarm initialisation,the PSO will modify the particle positions as well as the particle velocities.
2. This is followed by emergence of a new global best solution (gbest*) from improvement done on the current global best solution (gbest) using the TS procedure.
3. There will be termination of the iterative procedureupon reaching a stopping condition.

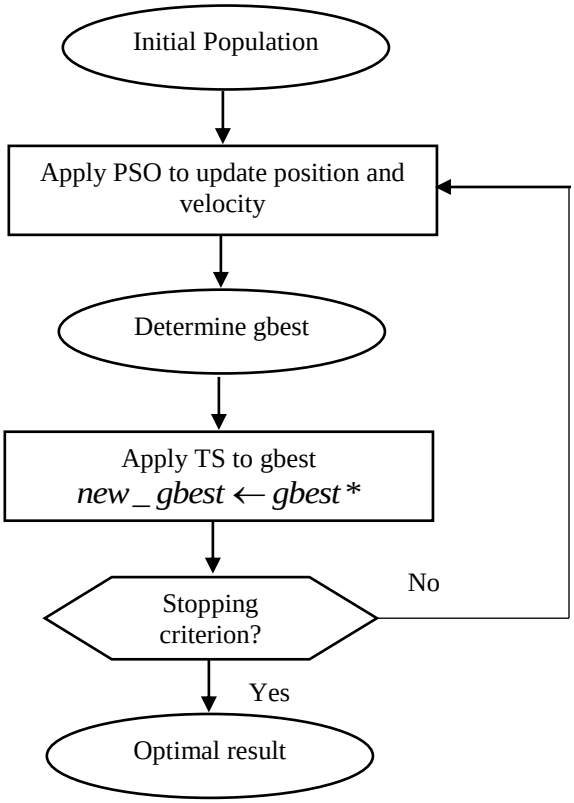


**Figure 1 Flowchart for Proposed Hybrid PSO-TS Algorithm**

## 4 RESULTS AND DISCUSSION

In this section, the PSO-AOMDV 5% malicious, PSO-AOMDV 10% malicious, PSO-Shun AOMDV 5% malicious and PSO-Shun AOMDV 10% malicious methods are used. Experiments are carried out using 10 to 90 node pause time. The Packet Delivery Ratio (PDR), average end to end delay, average number of hops to sink and percentage of malicious nodes detected as shown in tables 1 to 4 and figures 2 to 5.

**Table 1Packet Delivery Ratio for PSO-Shun AOMDV 5% Malicious**

| Node Pause time (s) | PSO-AOMDV 5% Malicious | PSO-AOMDV 10% Malicious | PSO_Shun-AOMDV 5% Malicious | PSO_Shun-AOMDV 10% Malicious |
|---|---|---|---|---|
| 10 | 0.7528 | 0.7593 | 0.7721 | 0.7664 |
| 30 | 0.8591 | 0.8046 | 0.8773 | 0.8359 |
| 50 | 0.8993 | 0.8679 | 0.9127 | 0.8827 |
| 70 | 0.9 | 0.8697 | 0.9217 | 0.8955 |
| 90 | 0.9158 | 0.8474 | 0.9357 | 0.8631 |

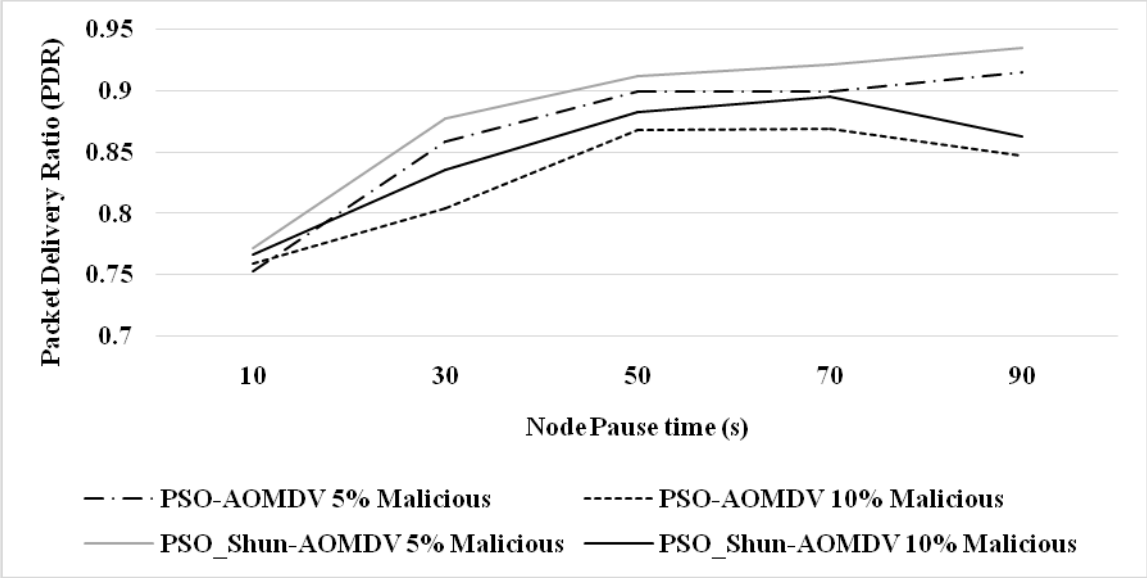


**Figure 2Packet Delivery Ratiofor PSO-Shun AOMDV 5% Malicious**

From the figure 2, it can be observed that the PSO-Shun AOMDV 5% malicious has higher PDR by 2.53%, 1.67% &0.74% for 10 node pause time, by 2.09%, 8.64% &4.83% for 30 node pause time, by 1.47%, 5.03% & 3.34% for 50 node pause time, by2.38%, 5.8% &2.88% for 70 node pause time and by 2.14%, 9.9% & 8.07% for 90node pause timewhen compared with PSO-AOMDV 5% malicious, PSO-AOMDV 10% malicious, PSO-Shun AOMDV 10% maliciousrespectively.

**Table 2Average End to End Delay for PSO-Shun AOMDV 5% Malicious**

| Node Pause time (s) | PSO-AOMDV 5% Malicious | PSO-AOMDV 10% Malicious | PSO_Shun-AOMDV 5% Malicious | PSO_Shun-AOMDV 10% Malicious |
|---|---|---|---|---|
| 10 | 0.0077 | 0.0132 | 0.0073 | 0.0129 |
| 30 | 0.0012 | 0.0043 | 0.0012 | 0.0041 |
| 50 | 0.0013 | 0.0029 | 0.0013 | 0.0027 |
| 70 | 0.001 | 0.0013 | 0.001 | 0.0012 |
| 90 | 0.0009 | 0.0011 | 0.0009 | 0.0011 |

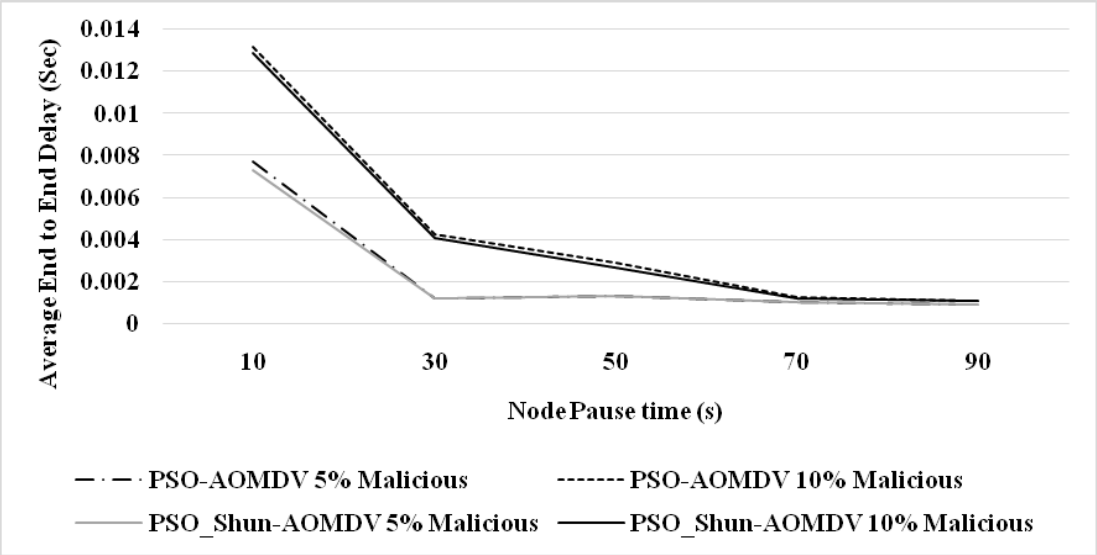


**Figure 3Average End to End Delay for PSO-Shun AOMDV 5% Malicious**

From the figure 3, it can be observed that the PSO-Shun AOMDV 5% malicious has lower average end to end delay by 5.33%, 57.56% &55.44% for 10 node pause time, by no change, 112.72% &109.43% for 30 node pause time, by no change, 76.19% &70% for 50 node pause time, by no change, 26.08% &18.18% for 70 node pause time and by no change, 20% & 20% for 90 node pause time when compared with PSO-AOMDV 5% malicious, PSO-AOMDV 10% malicious, PSO-Shun AOMDV 10% malicious respectively.

**Table 3Average Number of Hops to Sink for PSO-Shun AOMDV 5% Malicious**

| Node Pause time (s) | PSO-AOMDV 5% Malicious | PSO-AOMDV 10% Malicious | PSO_Shun-AOMDV 5% Malicious | PSO_Shun-AOMDV 10% Malicious |
|---|---|---|---|---|
| 10 | 5.4 | 6 | 5.7 | 6.2 |
| 30 | 5.4 | 5.5 | 5.5 | 5.5 |
| 50 | 4.6 | 5 | 4.7 | 5 |
| 70 | 4.9 | 4.8 | 4.9 | 5 |
| 90 | 3.5 | 3.1 | 3.6 | 3.2 |

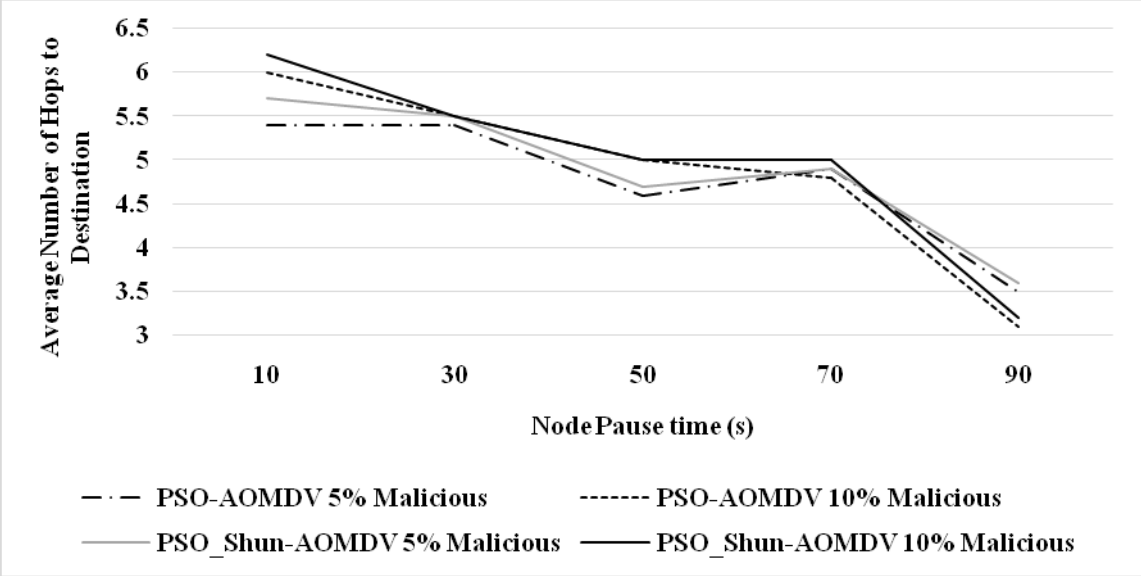


**Figure 4Average Number of Hops to Sink for PSO-Shun AOMDV 5% Malicious**

From the figure 4, it can be observed that the PSO-Shun AOMDV 5% malicious has lower average number of hops to sink by 5.4%, 5.12% &8.4% for 10 node pause time, by 1.83%, no change&no change for 30 node pause time, by 2.15%, 6.18% & 6.18% for 50 node pause time, by no change, 2.06% &2.02% for 70 node pause time and by 2.81%, 14.92% &11.76% for 90 node pause time when compared with PSO-AOMDV 5% malicious, PSO-AOMDV 10% malicious, PSO-Shun AOMDV 10% malicious respectively.

**Table 4Percentage of Malicious Node Detected for PSO-Shun AOMDV 5% Malicious**

| | PSO-AOMDV 5% Malicious | PSO-AOMDV 10% Malicious | PSO_Shun-AOMDV 5% Malicious | PSO_Shun-AOMDV 10% Malicious |
|---|---|---|---|---|
| Percentage | 82 | 85 | 85 | 86 |

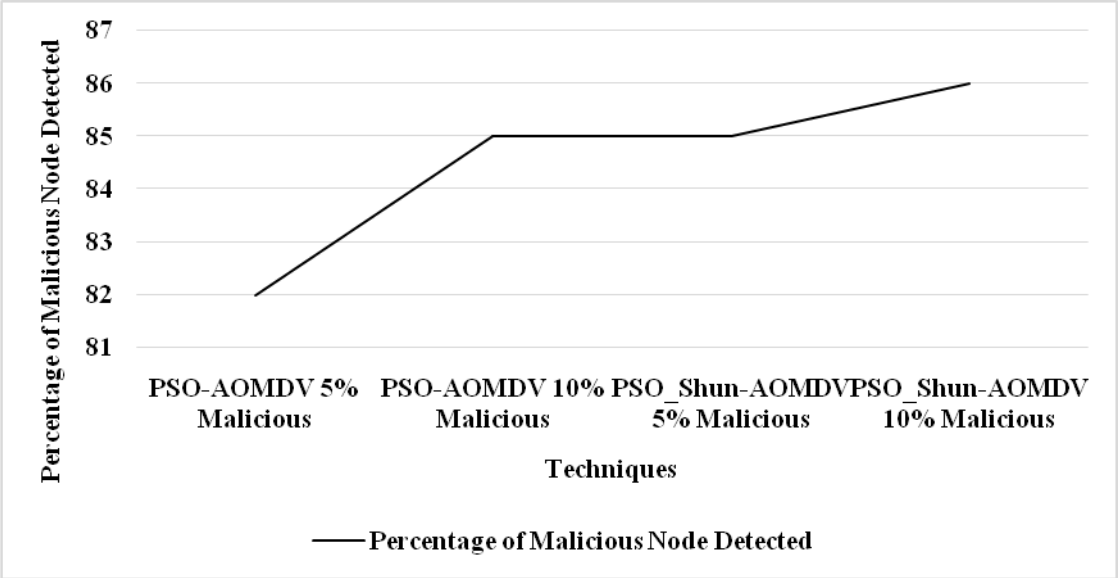


**Figure 5Percentage of Malicious Node Detected for PSO-Shun AOMDV 5% Malicious**

From the figure 5, it can be observed that the PSO-Shun AOMDV 10% malicious has higher percentage of malicious node detected by 4.76% forPSO-AOMDV 5% malicious, by for 1.17% PSO-AOMDV 10% malicious and by 1.17% for PSO-Shun AOMDV 5% malicious respectively.

## 5 CONCLUSION

A security mechanism's implementation for a blackhole attack in MANET is quite arduous due to its exceptional network traits. This work has offered the proposal for a trust-based routing with a new packet forwarding probability for the mitigation of blackhole attacks.AOMDV protocol, the AODV protocol's extension, is used for the computation of multiple loop-free as well as link disjoint paths.Proposal for a novel optimisation technique which is based on the PSO-Shun optimisation algorithm has been given to boost the multipath routing. Being a meta-heuristic algorithm, the PSO has been extensively used in diverse fields due to its easy implementation as well as conciseness. After the PSO's implementation, the TS is used to make the particles leap out of the local regions. For acceleration of the PSO's convergence, proposal for combining the PSO algorithm with the TS was offered so as to identity a better solution with minimum computation time as well as accuracy. It is evident from the experimental outcomes that, when compared against the PSO-AOMDV 5% malicious, the PSO-Shun AOMDV 5% malicious has higher PDR by 2.53%for 10 node pause time, by 2.09% for 30 node pause time, by 1.47% for 50 node pause time, by

2.38% for 70 node pause time, and by 2.14% for 90 node pause time.In comparison with the PSO-AOMDV 10% malicious, the experimental outcomes show that the PSO-Shun AOMDV 5% malicious has higher PDR by 1.67% for 10 node pause time, by 8.64% for 30 node pause time, by 5.03% for 50 node pause time, by 5.8% for 70 node pause time, and by 9.9% for 90 node pause time. Furthermore, in comparison with the PSO-Shun AOMDV 10% malicious, the experimental outcomes demonstrate that the PSO-Shun AOMDV 5% malicious has higher PDR by 0.74% for 10 node pause time, by 4.83% for 30 node pause time, by 3.34% for 50 node pause time, by 2.88% for 70 node pause time, and by 8.07% for 90 node pause time.

**REFERENCES**

1. 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.
2. Prasad, D. M. S., Niranjan, P., & Swathi, B. (2014). An Effective Method for Load Balancing in MANET. International Journal of Computer Science and Mobile Computing, 3(6), 223-229.
3. Kout, A., Labed, S., & Chikhi, S. (2018). AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks. Wireless Networks, 24(7), 2509-2519.
4. Manohari, P. K., & Ray, N. K. (2015, October). EAOMDV: An energy efficient multipath routing protocol for MANET. In Power, Communication and Information Technology Conference (PCITC), 2015 IEEE (pp. 710-715). IEEE.
5. Balakrishna, R., Rao, U. R., & Geethanjali, N. (2010). Performance issues on AODV and AOMDV for MANETS. International Journal of Computer Science and Information Technologies, 1(2), 38-43.
6. Gupta, K., & Mittal, P. K. (2017). An overview of security in MANET. Int J Adv Res Comput Sci Softw Eng ISSN, 7(6), 151-156.
7. Kondaiah, R., & Sathyanarayana, B. (2018). Trust Factor And Fuzzy-Firefly Integrated Particle Swarm Optimization Based Intrusion Detection And Prevention System For Secure Routing Of MANET. International Journal of Computer Sciences and Engineering, 10(1).

8. Kaur, K., & Pawar, L. (2015). Review of Various Optimization techniques in MANET Routing Protocol. International Journal of Science, Engineering and Technology Research (IJSETR), 4(8).
9. Narmadha, A. S. (2020). Trust-Based Winnow Linear Multiplicative Classification For Secure Multipath Routing In Manet. arXiv preprint arXiv:2006.01404.
10. Alkhamisi, A. O., Buhari, S. M., Tsaramirsis, G., & Basheri, M. (2020). An integrated incentive and trust-based optimal path identification in ad hoc on-demand multipath distance vector routing for MANET. International Journal of Grid and Utility Computing, 11(2), 169-184.
11. Panda, N., & Pattanayak, B. K. (2020). ACO-based secure routing protocols in MANETs. In New Paradigm in Decision Science and Management (pp. 195-206). Springer, Singapore.
12. Singh, S., Koslia, M., & Poonia, R. C. (2018). A GA-QMR: Genetic Algorithm Oriented MANET QoS Multicast Routing. Recent Patents on Computer Science, 11(4), 268-275.
13. Dixit, S., & Singhai, R. (2020). A PSO-Based Approach for Improvement in AODV Routing for Ad Hoc Networks. In Advanced Computing and Intelligent Engineering (pp. 379-389). Springer, Singapore.
14. Brindha, G. S., & Rajeswari, M. (2014). AOMDV-multipath routing protocol in mobile networks to enhance network security. Int. J. Sci. Res, 3(12), 62-66.
15. Aggarwal, I., & Garg, E. P. (2013). AOMDV Protocols in MANETS: A Review. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), 32.
16. Krishna, S. R. K. M., Ramanath, M. B. N. S., & Prasad, V. K. (2018). Optimal reliable routing path selection in MANET through hybrid PSO-GA optimisation algorithm. International Journal of Mobile Network Design and Innovation, 8(4), 195-206.
17. Gamot, R. M., & Mesa, A. (2008). Particle swarm optimization: Tabu search approach to constrained engineering optimization problems. WSEAS Transactions on Mathematics, 7(11), 666-675.
18. Chaabane, L., Khelassi, A., Terziev, A., Andreopoulos, N., de Jesus, M. A., & Estrela, V. V. (2020). Particle Swarm Optimization with Tabu Search Algorithm (PSO-TS)

Applied to Multiple Sequence Alignment Problem. In Advances in Multidisciplinary Medical Technologies─ Engineering, Modeling and Findings (pp. 103-114). Springer, Cham.