International Journal on Emerging Technologies **11**(3): 1204-1211(2020)

**ISSN No. (Print): 0975-8364**
**ISSN No. (Online): 2249-3255**

# Analyzing Trust based Routing in Secure MANET Using TAODV, TACO and FUZZY_FPSO Algorithms

***K. Ranjithsingh[1] and D. Maruthanayagam[2]***
*[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.*
*[2] Head/Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.*

*(Corresponding author: K. Ranjithsingh)*
*(Received 08 April 2020, Revised 14 May 2020, Accepted 22 June 2020)*
*(Published by Research Trend, Website: www.researchtrend.net)*

**ABSTRACT: The trusted secure path is one of the mainly essential processes which become the play important role in MANET Environment. Trusted Secure routing approaches has been recognized to be a key issue for routing optimization MANET. There are different methods to secure routing and the threads which make them up. Also, Secure Routing is major active research fields, where the researchers work to enhance the performance of the trusted secured routing operation in MANET Environment. In existing methods, some efficient factors related to better PDR, high throughput and malicious node detection rate not been considered in the routing operation. The lack of such factors in the trusted secure routing process has mechanically decreased the performance. To overcome such drawbacks in the old techniques, new efficient optimization algorithms have been emerged in the field of MANET. In this paper, the comprehensive comparative analyses of the four trust based pre-existing algorithms namely TDSR, TAODV, TOLSR and TACO are done. The efficiency of these algorithms has been evaluated on different scenarios using performance metrics. The investigation of routing presentation tested and the results are evaluated and symbolize graphically.**

**Keywords:** Mobile Ad Hoc Network, malicious node detection, Trust based Security, Dynamic Source Routing, Ad hoc On-Demand Distance Vector, Ant Colony Optimization, Fuzzy PSO

**Abbreviations:** AODV; Ad-Hoc On demand Distance-Vector, DSR; Dynamic Source Routing, PDR; Packet Delivery Ratio, TACO; Trusted Ant Colony Optimization , FPSO; Firefly integrated Particle Swarm Optimization

## I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are advanced wireless communication networks which operate with no fixed infrastructure. It allows for users to enter and exit any time, while seamlessly maintaining communication between other nodes. MANET is a self configuring network of interconnected mobile devices. MANET has distinct characteristics, which make them very difficult to secure. Much kind of characteristics contain: the lack of network infrastructure; no pre-existing relationships; unreliable multi-hop communication channels; Network devices limitation; and node mobility. Users cannot rely on an external innermost authority, like a trusted third party or certificate authority to carry out security and network tasks. The major challenge in designing such a self-organized network is the exposure of the routing attacks and failures. The fixed adding of many attacking nodes will strictly corrupt the routing performance. The attacking nodes try and confirm the detection and eliminated effectively to improve the routine of the network. Another significant difficulty of wireless communication over infrastructure-less networks is the unpredictable node mobility. The node mobility leads to frequent link disasters in single path routing, ensuing in negative network throughput. Thus, to stability the speed of the network as well as dependable data delivery, it is necessary to consist of the majority reliable multipath routing and an environment friendly trust evaluation model in adversarial environments. The important area of research has been using the idea for mitigate security threats [1]. The model of "Trust" at first derives from social sciences and is distinct as the quantity of one-sided confidence about the behaviors of an exacting entity [2]. The trust based routing is one approach to frame collaboration among nodes for setting up an effective routing between nodes. Trust esteem assumes a urgent function in the entirety of the organization exercises. The trust computation is, however, demanding task because of random node mobility and the lack of central authority. The surveys of trust management in MANET [3-5] give an outline of a variety of method for trust oriented network calculations.

The most important challenges of the trust routing of MANET are deliberated below.

- Routing in MANETs is have an effect on, which is explain using the QoS factor, and the direction-finding process is vulnerable to security problem happen by the altering network topology. The decisive factor is firm on the requirement for the security-aware techniques for routing [6].
- The decision concerning with admin of the nodes regarding their selection of the routing lane depend on the source and the destination nodes is a challenge [7].
- The communication of the nodes among each other causes the misbehavior of the nodes and sometimes, the self-centeredness of the nodes led to be short of their participation in the routing activities. The result of the overall performance state over of the nodes have an effect on the energy and trust in revealing the trustful data, which on the whole affected the performance of MANET [8].
- To allow the faith in the nodes and because the security of the direction-finding relies on the

reliability of the nodes concerned in routing, that is necessary to know the dependability of the nodes. Thus, MANET's behaved in a compassionate fashion and suffers from the cruel attacks [9].

*A. Trust Based Security in MANET*

The traditional security schemes that provide authentication and data privacy do not detect when an internal node provides false routing information, or where a node does not support by the other nodes to save its resources. There should be another layer of security that detects such misbehavior. This layer is situated on trust concept. This concept was first proposed in the early 80's. It is depend on the way that human beings trust each other. When a person wants to verify another person, he usually asks his friends about this person. He also request this person to contribute him with the list of mention people who will be asked if he is to be trusted. In the similar way, step, S requests recommendations from the list of trusted entities (friends). This request involve a question to each entity in the list around the identity of D. Each entity answers yes (trusted) or no (un-trusted). Any entity that does not find D in its friends list forwards the request to its trusted entities list (Recommendation list). If any entity of the friends list or the recommendation list knows D and trusts him, information about D is sent back to S. In the next step, node S will ask D about the references, i.e. other entities with which he has communicated before. When S receives D references, he asks his friends list if they know these references and trusts them. S also may ask the references for references. In references also proposed to use the trust concept to evaluate the nodes in MANET.

| Neighbor_ID | Trust Value |
|---|---|

**Fig. 1.** Neighbor Table.

| Destination IP | Destination Sequence No | Hop Count | Next Hop | .. | .. | Route Trust |
|---|---|---|---|---|---|---|
| | | | | | | |

**Fig. 2.** Extended Routing Table.

The main aim of the trust model is to give joint solution for preventing malicious activities and consistent resource utilization by load balancing of packets being forwarded. The trust model stands for how to calculate the trust of the routing path by using trust value of individual nodes. The reactive routing protocols of MANET come into view for the routes and are shaped as and while required. When a starting position (source) wants to send to end position (destination), it petition to the route discovery mechanisms to hit upon path to the end position. For example: Ad-Hoc On demand Distance-Vector (AODV), Dynamic MANET On demand (DYMO), and Dynamic Source Routing (DSR). Most Trust security scheme recommended for MANETs have a propensity to build upon a few basic statement concerning the dependability of the participating nodes.

The existing trust based mechanisms of MANETS are Trust AODV (TAODV), Trust Based DSR, Adaptive SAODV (A-SAODV), Friend based Ad hoc routing using Challenges to Establish Security (FACES), Cooperation of Nodes-Fairness in dynamic Ad-hoc Networks(CONFIDANT), Friendship Based AODV (FrAODV), Secure Routing Using-Trust (SRT), Trusted AOMDV and Secure Ad hoc on demand distance vector Routing (SAODV). In this work, compared and evaluated the secure trusted routing performances of existing routing algorithms like TAODV, TACO and Fuzzy_FPSO (Firefly integrated Particle Swarm Optimization). Fuzzy_FPSO algorithm aims to get better result of the throughput performance, increase packet delivery ratio, avoid packet delay and end-to-end delay and then improved resource utilization and minimize energy consumption during trusted secure routing process. The above ( TAODV, TACO and Fuzzy_FPSO) techniques have performed fine with these three factors and also allocated to routing for growing the resource utilization whereas the performances of these techniques are short of in the secure routing process because, such methods have not considered the efficient factors like i) Packet Delivery Ratio` (PDR) ii) Residual Energy (based on Speed) iii) Average End - to - End Delay iv) Detection Rate of Malicious Nodes v) Delay Comparison (based on no. of rounds) vi) Energy Consumption etc during the secured trusted routing process.

## II. RELATED WORKS

Simaremare, *et al.* [10] proposed trust AODV, a trust mechanism to secure the AODV protocol. In adhoc network, black hole attack and active attack like DOS tin can with no trouble happen. These attacks could decrease the performance of routing protocol.

The assessment of this protocol is higher through the use of ant algorithm. When node is trusted the ant agent put fine pheromone. Path communication is based totally on the value of the pheromone. The presentation improves in stipulations of throughput ratio and packet delivery. The perception of disparity routing with hold and agency of an on hand modular security Architecture is influenced and integrated as a end result the disparity routing is finished via adopting the Adhoc On-level Demand Multipath (AOMDV) [11]. To enlarge modular security architecture, have Trust improved Routing Table module to contain the reliability metric. Therefore that route, among the multiple accessible routes to a destination, may be selected and tracked with policy-set parameters. Under the proposal, secure route is the one that will be mapped throughout the trusted (authenticated) nodes with the established SAs, where trustworthy route is the one that will have a high Mean Time among Failure. Reliability and trust as parameters are used with the multiple routes provide the graded routing service – the ability of providing a number of expected courses to objective in a MANET, every one of which might be chosen since its security and dependability measurements coordinate those of the strategy. The four expected evaluations of administration are given in fraded administration like Secure and stable evaluation of administration, Stable reviewed administration, Secure and insecure reviewed administration, Unstable evaluated administration to join courses from both OLSR and AOMDV. Huang [12] proposed a message security scheme to the MANET. By use of trust-based on multipath AOMDV routing collective with the soft-encryption, yielding the so it is called as T-AOMDV scheme. In the event that malicious nodes are clarify in the organization, at that point it is the significant message security issues. For given that validness the message is parts at the source node and afterward scrambled before being steered from side to side different way to the destination. Generate original message by using the decryption approach, it will take

place at recipient end. Various issues happen when malicious networks node is in attendance in the network it causes serious security message anxiety. However, scheme yields the minimal route selection time and the T-AOMDV, is more secure than traditional multipath algorithms and the T-DSR scheme. Pushpa, [13] Create trust primarily based model based on node believe and route trust in AODV protocol. With this least quantity overhead, we can easily remove the malicious node as nicely as we can set up a most superb trusted way between source and destination. Also it makes a protected communication in the surroundings besides any internal attackers. A new information design Neighbor desk is introduced which include of trust really worth and neighbor identity which need to be saved up through each and every node to maintain up track of the progressively altering rundown and its evaluating node trust values. Trust is decided through the regular evaluation of the nodes. The great test is that the network need to provide its kinds of help with no problem through trust primarily based protocols. Supports altered elevated routing protocol. This will supply conversation in secure manner with no any inside attackers. Aggarwal *et al.* [14] proposed a method for Trust Based Secure On Demand Routing Protocol additionally recognised as TSDRP. Adhoc on demand Distance vector (AODV) is modified to advocate TSDRP to save it from a range of attacks such as Black hole attack, Denial of service attack (DOS) etc. This protocol presents security towards DOS and black hole attack. AODV was modified to TSDRP by establish the Node trust table and Packet buffer. Node trust table stores data about every node and the getting out of hand node. Every node has node ID and trust calculation is performed to figure the estimation of trust dependent on packet perception. packet buffer utilizes three diverse PB, for example, PB_DATA, PB_RREQ, and PB_RREP to store control and data packets. Therefore, DoS attack and Black hole attack TSDRP has performed extremely well in approximately all parameters, NRL,PDF and AT as compared to AODV.

## III. METHODOLOGIES

In this section we discuss about various trusts based secure ad hoc routing schemes.

**A) Trusted Ant Colony Optimization (TACO)**

The Trusted Ant Colony Optimization (TACO) is a metaheuristic approach. The conduct is recognized with actual ants and TACO which gives the most secure direction to source to destination [15]. The subterranean insect discovered the briefest way from ant colony to meals with the help of Chemical shower (pheromone) unfold through ants alongside the way. It is utilized to find out a way to the accompanying ants in this way to arrive at the food. All matters regarded ants are establishing to move from the ant colony in a number methods even though the meals diagnosed through ants on the most restricted way earlier than is contrasted and ants on the longest way. Subsequent to gathering the food, ants started to move in a comparable way in reverse heading. The way is exotic by way of pheromone in transit. Anyway the pheromone thickness is excessive in the most limited path contrasted with the longest path.

The Pheromone oath thickness of the way relies upon a period stretch. If the time extends, by then pheromone thickness will disappear on the path as a result of sublimation measure. At the suitable time the course is concealed in longest way and various subterranean insects will move in the briefest path from the ant colony to state to food. These ACO thoughts are used in various huge number savvy improvement issues. TACO methodology is an underhanded technique to follow the correct path from sender to receiver. The ants are going about as control packets. They are gathering possible model course in the organization. Ants gather accumulate substance for all intents and purposes entire course to the heading and use this for confirming to improvement quite far ants store the pheromone on the path which is important for future underground creepy crawly moving in a comparative way. In Trusted Ant Colony Optimization (TACO) count, trust hub from the sender to objective realized with underground bug state estimation, involves three distinct stages, to be explicit (1) Discovered conceivable way (2) Path choice and refreshing and (3) Trust way determination. TACO gives the security in the responsive coordinating show by trust way decision using Ant Colony advancement. Trust way is tended to by the going with conditions.

**Path discovery process provides** diverse going to source and objective by the underground subterranean ants subject matter expert.

**Probability of best path determination** deferrals and pheromone deviation in the manner. Time concedes changes concerning division and pheromone deviation is oppositely moved in regards to time

**Trust path is kept** up by the probability of way and less bounce count from source to objective and rate deviation of the battery.

**After determination of best path,** the Probability for less bounce check is reduced effect from the assault and conspiracy in the organization and utilizing the less proportion of energy.

**Less battery deviation** can get by for long haul and kept from egotistical assault. So less battery deviation of the hubs is supported in the way.

**Discovered Possible Path:** At first sources don't have any course to objective, source referenced message is started by insect's representative and spread to all adjoining hubs inside the association. When Forward ANT shows up at the neighbor hub, which isn't an objective, by then Forward ANT moves to the accompanying hop with revived detail of bordering hub, regardless Forward subterranean insect's requesting are crushed by objective and Backward ANT replay is given to the sources. Right now, insect pheromone thickness is saved on the ways. In the event that pheromone esteem is not as much as that of limit esteems, at that point this way isn't appropriate for information transmission and it very well may be dropped. Way accessibility is considered by the thickness of pheromone between source to objective and each adjoining node.

1. **Path selection and Route update:** The path browsed from sender (s) to receiver(r) relies upon pheromone thickness on the course and Probability of time delay between the ways. Best way determination is considered by Probability of most limited ways and pheromone deviation on the path.

$$P_{sr} = \frac{d_{sr}}{P(t)_{sr}} \quad \ldots (1)$$

Where P_sr the best is chosen path from s to r, ⟦P(t)⟧_sr address Probability of briefest paths to arrive at s to r and d_sr is the pheromone deviation. The pheromone thickness increments from s to r when r distinguishes the Forward ANT from s and getting an answer of r. At that point Pheromone thickness expanded to q_sr=q_sr+∆q_sr. On the off chance that r doesn't distinguish any neighbor node

to communicate the Forward ANT, the pheromone deviation happens the factor of ρ.

$$d_{sr} = (1-\rho)d_{sr} \quad \ldots(2)$$

Where ρ is the estimation of 1 to 0. On the off chance that not having any development of ants in the path, the pheromone esteem is set to zero..

$$P(t)_{sr} = \frac{\tau(X)_{sr}}{\sum_{sr=1}^{n}\tau(X)_{sr}} \quad \ldots(3)$$

Where ⟦P(t)⟧_sr is a likelihood of the briefest path from source to destination.

$$\tau(X)_{sr} = \sum_{sr}(T_a + T_b) \quad \ldots(4)$$

Where, T_a is the Time postponement of ith hub and T_b = Total time deferral of the way from sender node to receiver node. The likelihood of additional Time postpone way lies among sender and receiver.

2. **Trusted path Selection:** Different characters are used for trust path choice and ejection of weakness. In this method, connecting node are trusted by three factors most limited route path, least hop count among sender and receiver and deviation of battery level in rates. When in doubt, the most concise course way is picked by Probability of the most ideal way condition (1). Chosen way trust by less number of skips is differentiated and the other directional course and deviation of the battery. The two states of jump and battery deviation are giving a protected correspondence way and lessening parcel drop and extremist assault on account of defenseless (malevolent) nodes in the association. Underneath conveyed the condition for trust path,

$$\text{Trusted}_{path} = \frac{P(t)_{sr}}{\sum_{sr}(E_{sr}+\%B_{dv})} \quad \ldots(5)$$

Where, battery level of their deviations communicated as,

$$\%B_{dv} = \frac{\text{Actual battery level difference}}{\text{Actual battery level}} \times 100 \ \ldots (6)$$

The Secured correspondence is depicted by pheromone deviation, Hop check and Battery deviation of every single node is inside the network.

**Algorithm 3: Route Discovery Process**

**Initialize:** $E_s = \text{Source Node}$, $E_r$= Destination Node, $E_{sx}$ = Adjacent Sender Node, $E_{sy}$= Adjacent Receiver Node, $\tau(X)_{sr}$=Probability for less time delay

**Procedure**

$E_s$ Send Forward_Ant to $E_{sy}$
If $E_{sy}$ != $E_r$= then
$E_{sy}$ Set $E_{sx}$
$E_{sx}$ Send Forward_Ant to $E_{sy}$
$\tau(X)_{sr} = \sum_{sr}(T_a + T_b)$
$E_{sx}$=1+$E_{sx}$
$q_{sr} = q_{sr} + \Delta q_{sr}$
Else
Set Backward_Ant =0
Backward_Ant.Path=Forward_Ant(Reverse Path)
Register($E_s$) updated by Backward_Ant.Path
End Procedure

**Algorithm 4: Trusted Path Selection**

**Initialize:** $P(t)_{sr}$=Probability of shortest path, $Pt_{sr}$ = Best path, i=number of path, $E_{th}$=Threshold level, $\%B_{dv}$=Battery deviation of the nodes,
$\text{Trusted}_{path}$= Trust node path

Procedure
If ($q_{sr}$ != 0) then
$P(t)_{sr}$ Set by $\tau(X)_{sr}$
$Pt_{sr}$=Selected best path
Else
$Pt_{sr}$= Malicious path
If ($E_{sr} \le E_{th}$) && ($B_{dv} < \%B_{th}$)
If % $B_{dv}$ > 60 % then
$\text{Trusted}_{path}$ = Partially Trusted
Else
$\text{Trusted}_{path}$= Trusted path
Else
$\text{Trusted}_{path}$=Malicious

The Route Discovery measure is tried in Algorithm 3. The source node (E_s) sends Forward Ant (Forward_Ant) to after that Adjacent node (E_sy). On the off chance that E_sy isn't an destination, Forward Ant moves to next node with updation of time delay (⟦τ(X)⟧_sr), hop count and Pheromone level (q_sr). In any case E_sy will send Backward Ant (Backward_Ant) to Reverse way of Forward_Ant. The most brief and confided in way choice technique is given in Algorithm 4. At the point when the Pheromone deviation(q_sr ) of the course from source to destination isn't equivalent to nothing, the source hub tracking down the most brief way ⟦P(t)⟧_sr by time postpone ⟦τ(X)⟧_srof the different course get the best way Pt_sr in the organization. In any case Pt_sr will get noxious. Then, the confided in way (Trusted_path) is recognized from the jump tally (E_sr) and battery deviation of the node in the course. In the event that both are not exactly the edge, Trusted_path is trusted or in part trusted by battery deviation. Something else, Trusted_path is malignant.

**B) Trusted Ad hoc On-Demand Distance Vector (TAODV)**

Believed AODV is a routing algorithm that broadens the AODV protocol by adding a trust boundary for the routing messages [16]. The trust an incentive for some node N is determined from the neighbor node trust estimations of the relative multitude of neighbors of the node. Two novel fields are added to the routing table containing trust data and neighbor list. route trust can be registered relying upon number of bundles sent and number of bundles got by objective or some other organization boundaries. The network chooses the TREPs with the best trust o esteem and chooses that way for communication.

**Algorithm :**

1. Source node broadcast RREQ control packets to its all neighbors
2. Neighbor nodes check its Routing Table access for the desired destination and also check the corresponding route freshness.
3. If fresh route entry exits, then originate RREP control packets to the source node
4. Else rebroadcast RREQ packets to its neighbors (add its IP address in RREQ before rebroadcast)
5. Source waits for more than one RREP (max 4 numbers) from its neighbors
6. Calculate RT value using below equation:

RT = (Hop Count x w1) + (Route Trust x w2) where, w1= 40%, w2 =

60% Hop count, Route Trust accessed from RREP control packets.

7. Sort RREP in ascending order based on RT value
8. Choose first three RREP packets
9. For ( i =0; i < 3; i++)

Extract Neighbor List from selected RREP packets
Source node originates TREQ packets to all the neighbors in the

Neighbor List. Avoid the route through the RREP originator node to reach the neighbors.

1. Collect TREP from all the neighbor nodes
2. Node Trust Value is evaluated by the below equation:

NTV ( i node) = [NNT (1)+NNT(2)+ . . + NNT(n)] / n
Where, NTV ( i node) : i th Node Trust Value n : No of neighbors in the Neighbor list NNT : Neighbor Node Trust value about the node

3. Sort RREP in ascending order based on Node Trust Value
4. Choose the first RREP
5. Source node selects this route for communicate the desired destination

At first, broadcasting RREQ message to the entirety of its neighbors. Every node keeps two principle table; Route Table and Neighbor Table. Every node refreshes its Neighbor Table by conveyance HELLO packets in the typical span. Neighbor Table contains Neighbor_ ID and Trust Value fields. Next table on the whole node is Route Table. It deals with the course angle data like Destination IP Address and Sequence Number. Legitimate Destination Sequence Number, Next Hop, Hop Count and Route Trust and so on for every one of the route those are substantial from this node. At the hour of course foundation interaction or packet sending measure, this table is refreshed. Neighbor node check these routing tables whether they are have any route to the ideal destination or not. Assuming it isn't works, hubs conceivable to send a RREP message to source in turned around the back way. Source generally chooses RREP message among other RREPs dependent on two standards, Minimum hop count tally worth to the destination and ongoing arrangement number of the recipient node than source realized objective succession number. In this plan, RREP carries on a significant part in RREP choice cycle. Relies upon huge number of Route Trust step, the RREP is picked for additional route foundation.

**C) Fuzzy_FPSO (Firefly integrated Particle Swarm Optimization)**

The principle objective of this test is to construct a current incredibly secure routing protocol by set up as a regular occurrence trust factor and fluffy relies on Intrusion Detection and Prevention system [17]. This Method consists of the FPSO algorithms are in use for envisaged the safe way in the MANET. In 4 important phases of this policies are list out i) computation trust nodes ii) Detection of Intrusion by rule classifier iii) Path Identification, and iv) Selection of the secured path through the FPSO Algorithm [18]. The aggressors interfering the network can be imagining by utilizing the Intrusion Detection and Prevention strategy with fuzzy guideline alongside trust factors. When the protected nodes are distinguished, the FPSO algorithm assumes the basic part in the most ideal path choice for secure routing. The four main steps in The Intrusion Detection and Prevention method are intrusion detection, path prediction, optimum path selection and ultimately the data transmission. At first, all of the nodes are initialized with trust=1, the intrusion node is detected through using the fuzzy classifier [19]. All the paths among the source destination nodes are anticipated allowing for the trust stage of the nodes. For figuring out the great path among supply and destination, an included FPSO optimization algorithm is hired that predicts the path regarding the ideal fitness function. Then, the data may be despatched through the anticipated optimum path.

The fitness function included in the optimization scheme makes the selections primarily based on the answer quality. The primary intention of the health function of FPSO with distance and have confidence as its goal is to maximize the fitness value. The distance between the nodes taking phase in routing ought to be in minimum for an efficient route. Trust stage is computed between the node and its neighboring nodes for making sure safety in the network. The nodes with the most have confidence stage will be only chosen as the intermediate relied on nodes for facts transmission. The most fitness valued answer is regarded as the most suitable path of a system. The formulation of fitness function is given below,

$$\text{Fitness} = \frac{1}{P}\sum_{k=1}^{P} 0.5\,(T_{path}^{k} + [1 - D_{path}^{k}]) \quad \ldots(7)$$

where, P denotes the considered number of multipath, $T_{path}^{k}$ indicates the Path trust of the $k^{th}$ path, $D_{path}^{k}$ represents the Path distance of the kth path. The path T value need to be most in an fine system; it is calculated primarily based on the trust of the nodes in the suitable path through the use of the below equation (8).

$$T_{path}^{k} = \frac{1}{m^2}\sum_{c=1}^{m-1}\sum_{d=c+1}^{m} T_{c,d} \quad \ldots(8)$$

where, m denotes the complete number of nodes in the specific path, and cT_(c,d) , shows the trust value between cth node and dth node in the path k . The computed path distance value D_path^k need to be in minimal for high quality intrusion detection. T_(c,d) , and D_path^k is calculated by way of using the following equations (9) and (10),

$$T_{c,d} = \frac{1}{4} * \left[T^{direct} + T^{indirect} + T^{recent} + T^{historic}\right] \ldots(9)$$

$$D_{path}^{k} = \frac{1}{m^2}\sum_{c=1}^{m-1}\sum_{d=c+1}^{m} D_{c,d} \quad \ldots(10)$$

Finally, the high-quality condition (optimal solution) is accomplished with the aid of non-stop change of information between its participants. Here each and every node is viewed as a member and the distance and trust stage are the data parameters. This PSO is accelerated to supply better outcomes and solves issues of various variety when some changes are included. In this research, the furnished change for PSO is the integration of PSO with FA.

Let the particle role be H_i (z) at time immediate z , the role of the particle is up to date through including velocity considering the velocity influences the particle position. where, H_i (z+1) is the firefly position at z+1th instant, H_i (z) is the firefly position at zth instant, j and i are the fireflies considered for function update, β_0 is indicated as the attractiveness at r = zero , γis noted as the constant mild absorption coefficient, r is represented as the distance between the two fireflies j and i , αis indicated as the randomization parameter inside the restriction [0,1] and ϵ_iis denoted as the random quantity drawn from Gaussian distribution.

$$H_i(z+1) = \frac{1-\beta_0 e^{-\gamma r^2}}{1-\beta_0 e^{-\gamma r^2}-(1-h_1 s_1 - h_2 s_2)}\,[Fu_i(z) + h_1 s_1 B_l(z) + h_2 s_2 B_g(z) - (\frac{1}{1-\beta_0 e^{-\gamma r^2}})(\beta_0 e^{-\gamma r^2} H_j(z) + \alpha\epsilon_i)_{[1-h_1 s_1 - h_2 s_2]}] \quad \ldots(11)$$

Equation (11) is the in the end got position update equation by the usage of the FPSO algorithm. Using the above equations the choicest 'p' route prediction and the reallocation of nodes in the MANET is finished successfully, for routing.

**Fuzzy_FPSO Algorithm**

- **Input:** Population H
- **Output:** Best Solution $B_g$
- **Parameter:** iteration, maximum iteration max_iteration, global best $B_g$
- Begin
- Initialize the population
- Initialize max_iteration
- For (z < max_iteration)

- Compute fitness value using equation 7
- Update $H_i(z+1)$ with the FPSO position update using equation 11
- Generate new set of solutions
- Compute the fitness value for the new solutions using equations 7
- Determine the best solution based on the fitness
- Z=z+1
- End for
- Return $B_g$
- Terminate

## VI. EXPERIMENTAL RESULTS

This section presents only comparison of results among the TADOV, TACO and the Fuzzy_FPSO algorithms and then find out which one is efficient than others. The Fuzzy_FPSO algorithm immediately in contrast the present methods like TAODV, and TACO. The implementation of surroundings used for simulation tool is NS2. The simulation outcomes consisting of end to quit delay, packet delivery, routing overhead, Energy Consumption and throughput are used to analyze the TACO algorithm with TAODV and Fuzzy_FPSO. This work carried out our simulations in a 1000 X 1000 $m^2$ location and employed IEEE 802.11 MAC. The type nodes have been allotted randomly all through the network which employs the algorithms. Randomly located nodes execute a range of packet forwarding misbehaviors relies upon on the adversary model.

**Table 1: Summary of Simulation Setup.**

| Parameter | Value |
|---|---|
| Number of Nodes | 100 |
| Simulation Time | 250s |
| Map Size | 1000 X 1000 $m^2$ |
| Mobility Model | Random Way Point |
| Traffic Type | CBR (Constant Bit Rate) |
| Transmission Radius | 275 m |
| Pause Time | 5s |
| Misbehaving Nodes | 0-40% |
| Energy of Each Node | 125 joule |
| Packet Size | 512 Bytes |

**A. Average End To End Delay:** The time taken by any packet to go from source to destination is called the end to end delay. The average of these end to end delays of all the received packets is called average end to end delay. Fuzzy_FPSO outperforms TAODV and TACO in delay as shown in Fig. 3 and Fig. 4. The key reason for this is the trust and energy calculation to be carried out by TACO at different pause time. Still Fuzzy_FPSO delay is less than TACO and always better than TAODV.

**Table 2: Different nodes delay.**

| No. of Nodes | Delay | TACO | TAODV | Fuzzy_FPSO |
|---|---|---|---|---|
| 20 | 0.5 | 0.81 | 0.77 | 0.47 |
| 40 | 1.0 | 1.84 | 1.68 | 0.85 |
| 60 | 1.5 | 2.15 | 1.93 | 1.12 |
| 80 | 2.0 | 2.59 | 2.44 | 1.37 |
| 100 | 2.5 | 2.77 | 2.61 | 1.78 |

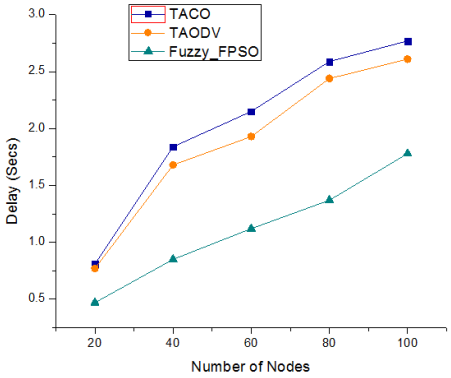


**Fig. 3.** Delay for different nodes.

**Table 3: Delay for different pause time.**

| No. of nodes | TACO | TAODV | Fuzzy_FPSO |
|---|---|---|---|
| 20 | 1.34 | 1.19 | 0.88 |
| 40 | 1.18 | 0.89 | 0.77 |
| 60 | 0.94 | 0.76 | 0.45 |
| 80 | 0.40 | 0.34 | 0.21 |
| 100 | 0.36 | 0.18 | 0.09 |

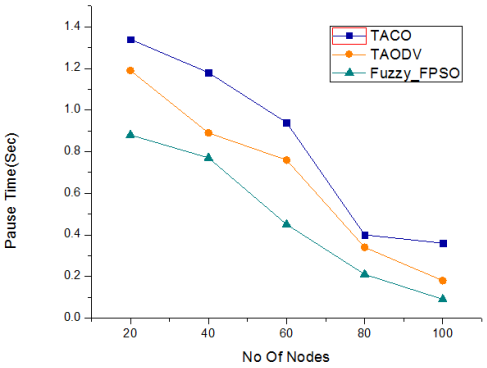


**Fig. 4.** Delay for different pause time.

**B. Throughput:** The measure of total size of correct received packets by the destination for each second called as throughput. The performance analysis of throughput against with the No. of malicious nodes. The Comparison graph for TACO, TAODV, Fuzzy_FPSO shown in Fig. 5. The Fig. 5 describes the relationship between throughput with the number of malicious nodes for TACO, TAODV and Fuzzy_FPSO methods. With the increase of malicious nodes, the effective separation of malicious behavior from the faulty behavior by the Fuzzy_FPSO algorithm provided the high throughput compared to TAODV and TACO.

**Table 4: Throughput vs. Malicious Node Values.**

| No. of. Malicious Nodes | TAODV | TACO | Fuzzy_FPSO |
|---|---|---|---|
| 2 | 9.16 | 11.54 | 16.52 |
| 4 | 8.87 | 10.56 | 15.21 |
| 6 | 8.11 | 9.45 | 13.59 |
| 8 | 7.62 | 9.11 | 10.42 |
| 10 | 7.45 | 8.77 | 9.21 |

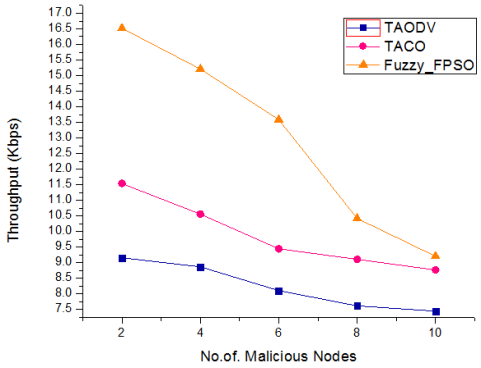


**Fig. 5.** Throughput vs. Malicious Nodes.

**C. Routing Overhead:** As shown in Fig. 6, Routing Overhead of TACO is between 2.3 and 7.8 while that of TAODV is between 4.5 and 7.1 and Fuzzy_FPSO is between 1.6 and 4.7 which are instead better. In the meantime, the Routing Overhead of Fuzzy_FPSO suggests massive development with values. High mobility leads to extra common path failure and route discovery, resulting in greater routing overhead. In Fuzzy_FPSO, the preference of middle nodes is based totally on QoS parameters which would lower the routing overhead.

**Table 5: Table of Routing Overhead against Mobility.**

| Mobility | TAODV | TACO | Fuzzy_FPSO |
|---|---|---|---|
| 4 | 4.53 | 2.36 | 1.61 |
| 8 | 5.51 | 3.55 | 2.33 |
| 12 | 6.24 | 4.94 | 2.42 |
| 16 | 6.95 | 5.82 | 3.52 |
| 20 | 7.12 | 7.81 | 4.73 |

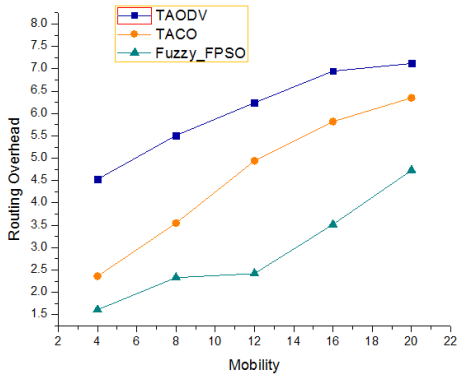


**Fig. 6.** Routing Overhead against Mobility.

**D. Packet Delivery Ratio:** The measure quantity of packets delivered to the destination node alongside the determine of packets produce by way of the source node expression as Packet Delivery Ratio (PDR).

**Table 6: PDR vs. Mean node speed Values.**

| Mean Nodes | TAODV | TACO | Fuzzy_FPSO |
|---|---|---|---|
| 1 | 91.11 | 93.56 | 96.12 |
| 2 | 90.77 | 91.45 | 95.56 |
| 3 | 89.84 | 90.78 | 93.15 |
| 4 | 86.3 | 88.22 | 91.23 |
| 5 | 85.59 | 87.45 | 89.46 |

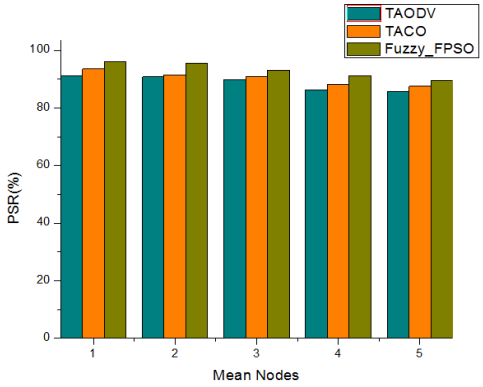


**Fig. 7.** PDR vs. Mean node speed.

The analysis of PDR with the variant of suggest node speed for TAODV, TACO, Fuzzy_FPSO is depicted in Fig. 7. The trust based routing calculation correctly detects the malicious behavior. The Fuzzy_FPSO trust with oblique and direct remark mechanism supplied the excessive PDR in contrast to TAODV and TACO methods.

**E. Residual Energy**

Fig. 8 depicts the energy remaining by different algorithms at different pause times. Fuzzy_FPSO best energy saving compared to TACO and TAODV.

**Table 7: Table for Residual Energy.**

| Simulation Time (Sec) | TAODV | TACO | Fuzzy_FPSO |
|---|---|---|---|
| 40 | 92.48 | 94.12 | 97.45 |
| 60 | 90.7 | 92.56 | 95.12 |
| 80 | 88.22 | 91.44 | 92.56 |
| 100 | 87.37 | 89.9 | 90.11 |
| 120 | 86.61 | 88.57 | 89.23 |

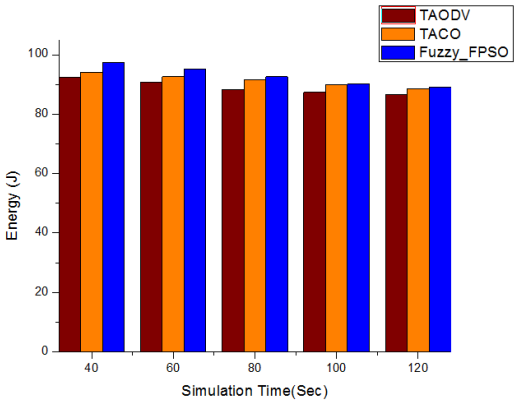


**Fig. 8.** Residual Energy.

## V. CONCLUSION

MANETs are vulnerable to dissimilar kind of attacks such as blackhole, DoS, wormhole, colluding attack etc. due to its infrastructure less property. Trust based algorithms attempt to increase the security of communication in MANETs. a variety of trust based move toward are proposed to avoid such types of attacks and to improve Quality of Services (QoS). In this paper, performance of TACO, TAODV and Fuzzy_FPSO are evaluated under different scenarios. All these four algorithms calculate trust based on the importance of the packet being transmitted. From the given graphs it can be analyzed that the performance

of Fuzzy_FPSO is better in case of average end-to-end delay and throughput. As far as average end-to-end delay is concerned Fuzzy_FPSO outperforms TACO and TAODV due to availability of complete routes in Fuzzy_FPSO cache and large overhead in case of TDSR. The above techniques are achieved throughput; avoid packet delay and optimal solution only if the network remains stable condition otherwise it is unsuccessful. So, another efficient secure routing approach is required to achieve safest path, maximum throughput, good packet delivery ratio, increase % of detection rate of malicious nodes, minimizing energy Consumption, end-to-end delay and also reduce the routing overheads in Mobile Ad hoc Networks.

## REFERENCES


[1]. Beth, T., Borcherding, M., & Klein, B. (1994, November). Valuation of trust in open networks. In *European Symposium on Research in Computer Security* (pp. 1-18). Springer, Berlin, Heidelberg.

[2]. Cook, K. (Ed.). (2001). *Trust in society*. Russell Sage Foundation.

[3]. Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. *IEEE communications surveys & tutorials*, *13*(4), 562-583.

[4]. Menaka, R., & Ranganathan, V. (2013). A survey of trust related routing protocols for mobile ad hoc networks. *International Journal of Emerging Technology and Advanced Engineering*, *3*(4), 903-910.

[5]. Khatri, P., & Mohammed, A. (2013). TDSR: Trust based DSR routing protocol for securing MANET. *International Journal of Networking & Parallel Computing*, *1*(3).

[6]. Guerrero Zapata, M. (2006). Secure ad hoc on-demand distance vector (saodv) routing. *Internet Draft: draft-guerrero-manet-saodv-05. txt*.

[7]. Hu, Y., Perrig, A., & Johnson, D. B. (2002). Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks Proceedings of the 8th An-nual International Conference on Mobile Computing and Networking (MobiCom'02).

[8]. Kaur, R., & Rai, M. K. (2012). A novel review on routing protocols in MANETs. *Undergraduate Academic Research Journal (UARJ)*, *1*(1), 103-108.

[9]. Aggarwal, A., Gandhi, S., Chaubey, N., & Jani, K. A. (2014, February). Trust based secure on demand routing protocol (TSDRP) for MANETs. In *2014 Fourth International Conference on Advanced Computing & Communication Technologies* (pp. 432-438). IEEE.

[10]. Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. (2014, June). Performance analysis of optimized trust AODV using ant algorithm. In *2014 IEEE International Conference on Communications (ICC)* (pp. 1843-1848). IEEE.

[11]. Salmanian, M., & Li, M. (2012, October). Enabling secure and reliable policy-based routing in MANETs. In *MILCOM 2012-2012 IEEE Military Communications Conference* (pp. 1-7). IEEE.

[12]. Huang, J. W., Woungang, I., Chao, H. C., Obaidat, M. S., Chi, T. Y., & Dhurandher, S. K. (2011, December). Multi-path trust-based secure AOMDV routing in ad hoc networks. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011* (pp. 1-5). Ieee.

[13]. Pushpa, A. M. (2009, December). Trust based secure routing in AODV routing protocol. In *2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)* (pp. 1-6). IEEE.

[14]. Aggarwal, A., Gandhi, S., Chaubey, N., & Jani, K. A. (2014, February). Trust based secure on demand routing protocol (TSDRP) for MANETs. In *2014 Fourth International Conference on Advanced Computing & Communication Technologies* (pp. 432-438). IEEE.

[15]. Khatri, P., & Mohammed, A. (2013). TDSR: Trust based DSR routing protocol for securing MANET. *International Journal of Networking & Parallel Computing*, *1*(3).

[16]. 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).

[17]. Robinson, Y. H., & Rajaram, M. (2015). Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks. *The Scientific World Journal*, *2015*.

[18]. Sharma, A., & Johari, P. K. (2017). Eliminating collaborative black-hole attack by using fuzzy logic in mobile ad-hoc network. *International Journal of Computer Sciences and Engineering*, *5*(5), 34-41.

[19]. Rini, D. P., Shamsuddin, S. M., & Yuhaniz, S. S. (2011). Particle swarm optimization: technique, system and challenges. *International journal of computer applications*, *14*(1), 19-26.



**How to cite this article:** Ranjithsingh, K. and Maruthanayagam, D. (2020). Analyzing Trust based Routing in Secure MANET Using TAODV, TACO and FUZZY_FPSO Algorithms. *International Journal on Emerging Technologies*, *11*(3): 1204–1211.