International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Optimized Trust Path for Control the Packet Dropping and Collusion Attack using Ant Colony in MANET

S. Sugumaran, P. Venkatesan

Abstract: ***In Wireless communication, Mobile Ad hoc Networks is a self organized structure-less network. MANET can be established easily in any kind of environment. At the same time vulnerable nodes are affected by various kinds of attacks due to changes in topology of the network. Dynamic routing protocols provide a multipath route between movable farthest nodes. In spite of that, malicious nodes in the network perform against the routing protocols. In the previous work of NNT to reduce packet dropping attacks in the node and improve node performance by Neighbor Node Trusted (NNT) concept, malicious and selfish nodes are identified by the time interval between the nodes. The Cluster supported trusting routing protocol(CSTRP) divides the networks into a number of clusters and in turn one of the nodes acts as Cluster-Head(CH) and CH controls the routing activity in the cluster. The CH deliberately monitors node trustworthiness and protects from malicious node and improves reliable security. This paper, proposing swarm intelligent method to select a trust path from different routes between source to destination, is called Trust path Ant Colony optimization (TpACo) algorithm, which serves as the best route and controls the Packet dropping attack and collusion in the network. The results of NS-2 simulator scrutinize the performance of TpACo in various situations. As such the Packet delivery Ratio increased 9.3% than NNT and CSTRP Algorithm. Besides End-to-End delay performance increases to 16%for NNT and 23% for CSTRP and Throughput increased 14.2 % then NNT and CSTRP.***

Keywords **: Mobile Ad-hoc Network, AODV, Packet drop & Collusion Attack, Ant Colony Optimization(ACO), NNT and CSTRP.**

I. INTRODUCTION

The Networks are of two types: wire network and wireless Network. At present, most of us prefer wireless networks because they are user-friendly when compared with wire networks such as secure and fast to upload or download the data. The wireless device in the network can move randomly around and within the area such as laptop, handheld devices, etc., are major advantage of wireless network. In modern technology, wireless network is also classified as infrastructure network and infrastructure-less networks. Infrastructure network has a control unit, which controls every node within the network. Whereas infrastructure-less self-configuring network does not have any control units. Each and every node linking dynamically in the network is termed as Mobile Ad-hoc network (MANET). As MANET has autonomous topology, each and every node is free to move in any direction within the network area and links are dynamically changing between the nodes. Hence, it is considered to have end-to-end connection, self-forming and self healing technology.

The routing protocol creates a route path from sender to receiver through a number of adjacent nodes within the network. Hence Routing protocol form route and effectively deliver the packet to the destination.In MANET, routing protocols are classified into two types: they are Reactive and Proactive (table driven) protocols. In Proactive protocols, every node maintains neighboring node detail in table form and repeatedly updates the changes of neighboring node movement. The Reactive Routing protocol is an on demand routing protocol, and whenever it is required it can be used. It moves to any context to connect with the destination. The Route is created by flooding the route REQ and REP controlling message within the network.

Compared with proactive routing protocol, reactive routing protocol overhead is less on the network. Various types of Reactive protocols are AODV (Ad hoc On-demand Distance Vector), DSR(Dynamic Source Routing), TORA(Transmission-aware Opportunistic Ad hoc Routing Protocol, etc. All the nodes in the networks are providing the best path between source and destination with trust. Whereas in real case, one of the nodes act as malicious. A Malicious node affecting routing performances of the network is known as an [4] attack. Attacks take place due to lack of centralization and dynamic topology of the nodes. They are classified as passive and active attacks, Passive attack does not disrupt the network operation and simply monitors network performance and identification of passive attacks in the network is complicated. Active attacks affect operation of the network such as packet drop by adjacent malicious node, by modifying the packet details and injecting malicious node to confuse the destination position and so on. Collusion attack is more than one number of malicious nodes in the network combined to distract the performances of the network.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
S. Sugumaran*, is Research Scholar in the department of Electronics and Communication Engineering, SCSVMV (Deemed to be University), Kanchipuram, Tamil Nadu, India.
Dr. P. Venkatesan, is Associate Professor in the department of Electronics and Communication Engineering, SCSVMV (Deemed to be University), Kanchipuram, Tamil Nadu, India.

The Neighbor Node Trusted (NNT) Notion [5] algorithm is similar to AODV route finding process by providing additional security to the network. NNT identified two various attacks of selfish and malicious node in the networks.

In this context, a node trusting concept depends on the Packet Forwarding Ratio (PFR). The Cluster Supported Trust Routing Protocol (CSTRP) [6], applied clustering techniques ensures Trust against malicious by two various conditions of Internal and External Trusted conditions.

The Mobile Ad-hoc Network path creation, maintaining the path and security issues is very challenging in high mobility nodes. Trust path selection in the mobile network is implemented in various methods. In this paper, Trust concept deals with the swarm intelligent behavior of Ant Colony Optimization.

In Swarm intelligence method [16], nodes don't have a Centralized control. Nodes created local agent between them and interacted each other with simple rules. Swarm Intelligence provides an optimal path between source to destination with low cast, flexibility and reliable link. Swarm intelligence is a biological system, like ant colony, Bee colony, Particle swarm optimization, etc. In wireless communication[17], ant colony optimization method is suitable for decentralized small area network. The ACO optimized best path in stochastic diffusion, nodes and reduced routing overhead.

In ACO, the different ants are starting to search for food from ant-hills in different directions. Moving ant is depositing the pheromone on the way up to destination. This deposition in the trail path is useful for ants in the future. When the moving ants are following the path, a pheromone deposit of this travel path is increased by ants along the path. This pheromone is a devious accumulation, exchange between the respective ants. Pheromone deposition of the shortest path ants movement is higher than longest path. The longest path pheromone content evaporates due to distance and delay. So, future ants are also attracted by shortest path pheromone from the ant-hill to food for quick establishment. These basic concepts of ACO can be used to recognize the Trust node in Mobile ad-hoc network to reduce the packet dropping by attack and collusion with the help of trusted nodes.

TpACo provides the security in the reactive routing protocol by trust path selection using Ant Colony optimization. Trust path is addressed by the following conditions.

- Path discovery process provides various direction routes to source and destination by the ant's agent.
- Probability of best path selection is provided by time delays and pheromone deviation in the path. Time delay changes with respect to distance and pheromone deviation is inversely varied with respect to time.
- Trust path is maintained by the probability of path and less hop count from source to destination and percentage deviation of the battery.
- After selection of best path, the Probability for less hop count is reduced effect from the attack and collusion in the network and utilizing the less amount of energy.
- Less battery deviation is able to survive for long duration and prevented from selfish attack. So less battery deviation of the nodes is preferred in the path.

The Rest of the Paper is prearranged as detailed here. Section II focuses on the Literature Review. Section III Deals with proposed Ant Colony Algorithm. Section IV Contains the simulation results with analysis and finally, Section V Concludes the dissertation work.

II. LITERATURE REVIEW

The security issues play a vital role in MANET-AODV routing protocols. The route is protected by various techniques, whereas route protection is concentrated with the biological swarm intelligent method. Trust path Ant Colony optimization (TpACo) having some inspiration for developing secure routing algorithm is based on chemical substance of ant and used to design steady routing in Reactive protocol of Ad hoc on-demand distance vector and dynamic source routing protocol.

Saleem, K. Fishal [2], proposed BIOSARP as relevant to ACO supported routing protocol. This method uses only two concepts of search and data ANT to control the traffic overhead in the network. A search ANT has discovered the path with pheromone density and a Data ANT takes out the data packets from source to destination for viewing different hop. BIOSARP performance reduces retort and inference of the route. Preethi and Sumathi [3], Proposed ODVA algorithm which avoids the packet drop in the network with the help of neighbor node table update. Before sending the packet, Hello control message flood surrounds the area within the network and updates the neighbors detail – to -neighbors adjacent node. The result is not satisfactory to control void/hole (various attacks) in the network by increasing the nodes within the network or by adding more hop between senders and receivers.

Kashif Saleem, Abdelouahid Derhab [1], the authors proposed Analyzing Ant colony optimization based routing protocol against the holes problem of enhancing user connectivity experience. ACO based routing protocol is used against holes. Holes affect the user connectivity in the wireless sensor network. This result in better battery life to each node reduces the delivery ratio and increases the delay.

Sharvani. G. S, et. all [7]., propose Swarm Intelligent Systems for MANET for repairing the failure route using Lagrange's Interpolation formula. In failed node, swarm intelligence method is used to repair the fault itself and discover new paths to the destination. In practical cases, local repair in failure node is impossible for all conditions. The author uses new path finding from failure node. However, the result produces less overhead. Surrender. S, Prakash. S [8], the authors propose to improve the Quality of Service in Fault Tolerant routing with Ant colony optimization. Generally misbehaving nodes affectthe route discovery and maintenance condition. The best path is preferred by pheromone deposition on the link. In such a case, the result is better than the other existing systems. Thenode throughput slightly reduces as the condition of large and malicious are added to the network.

NishithaTaraka, AmarnathEmani, [9], propose Routing in Ad Hoc networks using Ant Colony Optimization condition. When the results are compared with AODV and DSR, AntHoc Net produces better data rates at large mobile networks. AntHoc Net is not possible to maintain possible path to all destinations from sources. But it is creating a route path on demand. Suparna Biswas, Priyanka Deay and Sarmistha Neogy[10], the authors propose Trusted check pointing Based on Ant Colony Optimization in MANET. Trust module is evaluated by Ant Colony methods in each and every node in the cluster network. Trust condition is based only on node configuration and various attacks on the node, otherwise cryptography Technique is not considered. Trust value calculations are done with preference value. So in the real case minute rate of packet loss occurs due to interference of malicious node which is unavoidable in the network.

Y.Li, P. Yung, Z. Jianpeng [11], propose Trust Cluster Head Election algorithm based on Ant Colony Systems. Cluster head trusted by energy level and energy consumption of the node doesnot consider other constrains. When the security level is poor, theroute easily fails in the network.

C. V. Anchugam, K. Thangadurai [13], the authors proposed the ACO concept in Mobile Adhoc network and identifies black hole attack. Thisattack misguides the node and drops the packet in the network. This attack is controlled by the ACO optimization method to improve the PDF, throughput and time delay performance, by providing security for blackhole attack. Harris.S, Abdelhafid, Riri.F[14], proposes Performance analysis of optimized Trust AODV using an ant algorithm, In AODV, routing protocol is vulnerable by various attacks. Theauthors proposed ant algorithm and put a positive pheromone when the node is trusted. Trust evaluated by trust gobal and trust local method does not have a significant effect on the performance of the end to end delay. Devarajan JinilErsis, T.Paul Robert[15], authors review ad-hoc on-demand distance vector protocol and its swarm intelligent variants for Mobile Ad-hoc Network. The Route designs are based on efficiency, reliability and scalability of the MANET. The QoSis considered by delay, cost and hop distance of the network. The Swarm intelligent method is used to identify the shortest path in AODV protocol. In this Routing protocol time delay, packet delivery ratio and throughput are affected by various interferences in the network while route is existing. Swarm intelligent algorithms originate to solvethe route optimization problem in MANET. In the previous work, Stay Away From Packet Dropping Attack in MANET using Neighbor Node Trusted Notion Technique is proposed to control the packet dropping and selfish node in the network and prearranged security to AODV routing protocol[5]. This method detected the selfish node subsequently isolated from the network and identified the malicious node with the help of the neighbor node Trusted notion is then protected from packet drop and allotted neighbor nodes by malicious warning. However, packets are simply forwarded through the trusted node. In the second paper, the security of the network was improved by Attacks Reduction in MANET with Cluster Supported, Trusted Routing Protocol [6] Mechanism, Trust node concepts were implemented with the help of cluster group within the network. As a result, overall Packet delivery Ratio, Throughput and End-to End delay results are getting better than AODV and DSR. Once again we improve the trusted node concept in AODV with Ant Colony Optimization Algorithm. Already ACO has been proposed in MANET for various kinds of application. Whereas security based route protection and trusted notion implementation work is less in this area of research.

III. TRUST PATH ANT COLONY OPTIMIZATION

The Trust path Ant Colony optimization (TpACo) is a metaheuristic approach. The behavior is related to real ants and TpACo which provides the safest route for source to destination. The ant found the shortest path from ant-hill to food with the help of Chemical spray (pheromone) spread by ants along the path. It is used to find a path to the following ants in this path to reach the food. Actually ants are starting to move from the ant-hill in different directions. Whereas the food identified by ants on the shortest path earlier is compared with ants on the longest path. After collecting the food, ants started to move in the same path in backward direction. The path is identified by pheromone on the way. However the pheromone density is high in the shortest path compared to the longest path. The Pheromone deposition density of the path is based on a time interval. If the time elongates then pheromone density will evaporate on the path due to sublimation process. In due course the route is hidden in longest path and other ants will move in the shortest path from the ant-hill to food. These ACO concepts are used in various swarm intelligent optimization problems. TpACo method is an indirect technique to trace the correct path from sender to receiver. The ants are acting as control packets. They are collecting possible sample route in the network. Ants collect substance almost entire route to the direction and use this for corroborative to movement to the end. Ants deposit pheromone on the path which is useful for future ant moving in the same path. In Trust path Ant Colony Optimization (TpACo) algorithm, trust node from the sender to destination implemented with ant colony algorithm, consists of three various stages, namely (1) Discovered possible path (2) Path selection and updating and (3) Trust path selection. In NNT[5] Algorithm, trust value of hop node is calculated by receiving control packet value of hop node with a control packet value of that same hop in the neighbor node register. In CSTRP[6], Trust value calculated by comparative result of Threshold value for Packet delivery ratio(PDR) of each and every Cluster Head(CH) within the network cluster group. In this paper, The Trust value is evaluated by selecting possible path between source and destination, Number of Hop count and Battery deviation of the nodes in Percentage.

A. Discovered Possible Path

Initially sources don't have any route to destination, source requested message is started by ant's agent and spread to all neighboring nodes within the network. When Forward ANT reaches the neighbor node, which is not a destination, then Forward ANT moves to the next hop with updated detail of adjacent node, Otherwise Forward ants requests are destroyed by Destination and Backward ANT replay is given to the sources. At this moment, ant pheromone density is deposited on the paths. If pheromone value is less than that of threshold values then this path is not suitable for data transmission and it can be cancelled. Path connectivity is considered by the density of pheromone between source to destination and each adjacent node.

If Ants reached the destination, then retrace the path to sources and updated the pheromone level in every adjacent node within the network. If the retraced path hasn't reached the sources at correct time due to long distance, link breakage or malicious node, after some time interval pheromone density is set to zero and updated details are with node register.

B. Path selection and Route update

The path selected from sender (x) to receiver(y) is based upon pheromone density on the route and Probability of time delay between the paths. Time interval indirectly indicates the distance of the path. So one of the major parameters selects the correct path within the network. Usually forward ANTs are moving in all angles of node from sources. The forward Ants deposit is pheromone and updates the pheromone level in each and every node. Ant colony concept produces more

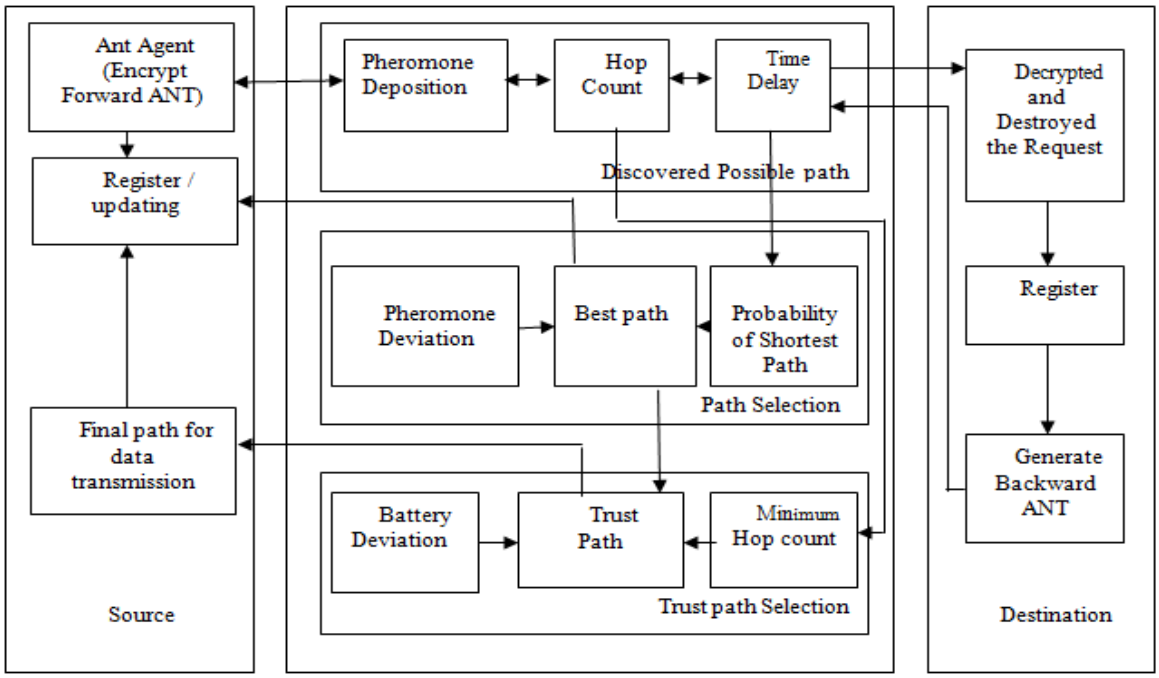

Fig.1 Block Diagram of TpAco Algorithm

than one number of paths from sender to receiver. Best path selection is considered by Probability of shortest paths and pheromone deviation on the path.

$$Pt_{xy} = \frac{q_{xy}}{P(t)_{xy}} \quad (1)$$

Where $Pt_{x,y}$is the Best selected path from x to y,$P(t)_{xy}$ represent Probability of shortest paths to reach x to y and q_{xy} is the pheromone deviation.

Source IP
Destination IP
Insisted Time
Unique sequence no
Pheromone density

(a)

Destination IP
Source IP
Hop Count
Time Delay
Pheromone density

(b)

Fig.2. (a) Forward ANT Control Packet Format (b) Backward ANT control Packet Format

The pheromone density increases from x to y when y detects the Forward ANT from x and getting a reply of y. Then Pheromone density increased to $q_{xy} = q_{xy} + \Delta q_{xy}$. Like vice a path is creating from x to the destination. Initially, Pheromone value (q_{xy}) is equal to zero. If y doesn't detect any neighbor node to transmit the Forward ANT, the pheromone deviation takes place the factor of ρ.

$$q_{xy} = (1 - \rho) q_{xy} \quad (2)$$

Where ρ is the value of 1 to 0. If not having any movement of ants in the path, then the pheromone value is set to zero.

$$P(t)_{xy} = \frac{\tau(D)_{xy}}{\sum_{xy=1}^{n} \tau(D)_{xy}} \quad (3)$$

Where P $(t)_{xy}$is a probability of the shortest path from source to destination.

$$\tau(D)_{xy} = \sum_{xy} (T_i + T_j) \quad (4)$$

Where, T_i is the Time delay of 'i^{th} node and T_j = Total time delay of the path from sender node to receiver node. The probability of more Time delay path lies between sender and receiver.

If malicious nodes are dropped, then ant agent forwards packets which are dropped by vulnerable node and reduced pheromone density is set as zero and time delay will increase. Even then they partially forward the packet to the next hop and then the pheromone density is reduced between the two adjacent nodes which is less than another path density level. So, malicious nodes are identified easily within the network.

C. Trusted path Selection

Various identities are used for trust path selection and removal of uncertainty. In the proposed method, adjacent nodes are trusted by three factors: shortest route path, lowest hop count between sender and receiver and deviation of battery level in percentages. Usually, the shortest route path is selected by Probability of the best path equation (1). Selected path trust by less number of hop is compared with the other directional route and deviation of the battery. Both conditions of hop and battery deviation are providing a secure communication path and reducing packet drop and selfish attack due to vulnerable(malicious) nodes in the network. Below expressed the condition for trust path,

$$T_{Path} = \frac{Pt_{xy}}{\sum_{xy}(H_{xy}+\%Bat_{devi})} \quad (5)$$

Where, battery percentage of their deviations expressed as,

$$\%Bat_{devi} = \frac{\text{Difference from actual batterry level}}{\text{actual battery level}} x\ 100 \quad (6)$$

The Secured communication is described by pheromone deviation, Hop count and Battery deviation of each and every node is within the network. In this paper, expected to secure communication is obtained, when the pheromone deviation is less than 40 %, Hop count is less than that of Threshold from the total node in the network and Battery deviation of each and every node is below 50 %.

Table-I: The notations

Symbol	Description
Pt_{xy}	Best Selected Path between x and y node.
$P(t)_{xy}$	Probability of shortest path between x and y
q_{xy}	Decreasing value of pheromone
P	Constant
$\tau(D)_{xy}$	Probability for less Time delay
T_i	Time delay of i^{th} node
T_j	Total time delay to reach source to destination
T_{path}	Trust Path
H_{xy}	Number of Hop count
H_{th}	Threshold value of the Hop count
$\%Bat_{devi}$	Battery deviation of the nodes in percentage
$\%Bat_{th}$	Threshold value for Battery deviation in Percentage

Table-II: TpACo – Trust node selection

Pt_{xy}	H_{xy}	$\%Bat_{devi}$	T_{path}
If q_{xy}= 0			
Else	$>H_{th}$	Whatever	Malicious
If $q_{xy}\neq 0$	$H_{xy}\leq H_{th}$	Below 50%	Trusted
		Above 50 %	Partially Trusted
		Above Bat_{th}	Malicious

Table - IV: Simulation results of TpACo

S.No	Malicious Node(%)	PDR	Average End-to-End Delay(%)	Throughput (kpbs)
1	10	0.94	60	8.9
2	20	0.86	58	8.8
3	30	0.86	56	8.5
4	40	0.8	40	8.6
5	50	0.78	42	8.4
6	60	0.7	42	8

The trusted node concept provides greatest and viable paths for data transmission. The route protection hypotheses are implemented by an TpACo swarm intelligent algorithm. The deposit pheromone of selected paths is given the best route for data transmission. Where one of the best and shortest routes is selected by source and other routes are stored for future. In MANET more numbers of nodes are possible to enter within the network or leaving the network. Such a case facing delay in transmission collapses the network route and depletes node energy. This problem is averted by frequent path selection probability method and selected best route in the network periodicals. The selected new route path is also affected by malicious or link failure due to collusion; affected node is informed to sender and selected alternative path and periodically monitored the changes in the network which is working or not.

Algorithm 1: Route Discovery Process

Init H_x=Source node,

H_y=Destination node,

H_{xi} = Adjacent Sender node,

H_{xj}=Adjacent Receiver node,

$\tau(D)_{xy}$ = Probability for less time delay,

Procedure H_x send F_ANT to H_{xj}

If H_{xj} != H_y, then

H_{xj} set H_{xi}

H_{xi} send F_ANT to H_{xj}

$\tau(D)_{xy} = \sum_{xy}(T_i+T_j)$

$H_{xi}=1+H_{xi}$

$q_{xy} = q_{xy}+\triangle q_{xy}$

Else

Set B_ANT = 0

B_ANT.path = F_ANT (Reverse Path)

Register(H_x) updated by B_ANT.path

End Procedure

The Route Discovery process is implemented in Algorithm 1. The source node (H_x) sends Forward Ant (F_ANT) to next Adjacent node (H_{xj}). If H_{xj} is not a destination, F_ANT moves to next node with updation of time delay ($\tau(D)_{xy}$), hop count and Pheromone level(q_{xy}). Otherwise H_{xj} will sends Backward ANT (B_ANT) to Reverse path of F_ANT.

Algorithm 2: Path Selection & Trusted

/Source node Finding the Trust Path/

Init $P(t)_{xy}$ = Probability of shortest path,

Pt_{xy} = Best path,

n = number of path,

H_{th} = Threshold level,

$\%Bat_{devi}$= Battery deviation of the nodes

T_{path} = Trust Node Path

Procedure **If** (q_{xy} ! =0) then

$P(t)_{xy}$ set by $\tau(D)_{xy}$

Pt_{xy} = Selected Best Path

Else

Pt_{xy} = Malicious Path

If (H_{xy}<= H_{th}) && (Bat_{devi} < $\%Bat_{th}$)

If $\%Bat_{devi}$ > 50 %, then

T_{path} = Partially Trusted

Else

T_{path}= Trusted Path

Else

T_{path} = Malicious

End Procedure.

The shortest and Trusted path selection procedure is given in Algorithm 2. When the Pheromone deviation(q_{xy}) of the route from source to destination is not equal to zero, the source node finding the shortest path $P(t)_{xy}$ by time delay $\tau(D)_{xy}$ of the various route get the best path Pt_{xy} in the network. Otherwise Pt_{xy} will become malicious. Next, the trusted path (T_{path}) is identified from the hop count (H_{xy}) and battery deviation of the node in the route. If both are less than the threshold, T_{path} is trusted or Partially trusted by battery deviation. Otherwise, T_{path} is malicious.

IV. SIMULATION RESULTS WITH ANALYSIS

The behavior of trusted path Ant Colony Optimization (TpACo) is implemented by ns2 simulation and it analyses the performance with various attacks. The ns2 command coding is very easy to create the various topologies in the network, the mobility of the nodes and make configure between the two nodes. A result of TpACo is compared among AODV, NNT and CSTRP in terms of Packet delivery ratio, throughput and End to End delay by varying the number of malicious in the network.

The simulation is implemented with 60 mobile nodes within the region of 140m x140m. Mobile nodes are randomly moving in a rectangular area. The results show the performance of TpACo Algorithm and improvement of packet dropping attacks and collusion control. The CBR (Continuous bit rate) traffic model is used to connect the randomly moving source and destination. The MAC layers protocol of IEEE 802.11 in the module. Further simulation parameters are shown below.

The performance of the Trust algorithm is considered by pheromone level and the battery deviation of the node in the path. When the trust value of a node which is based on pheromone level q_{xy} on the path, if $q_{xy}$is increased then the trust value of the path is decreased. Pheromone is usually affected by time delay of the path. As the time delay increases, the Pheromone deviation too increases in the network (Fig.3).Time delay occurs due to malicious nodes on the path; so malicious nodes affect the trust level of the path.

Table- III: Simulation parameters range

Simulation Parameters	Range / Value
Each node Coverage area	250m
MAC protocol	IEEE 802.11
Data Transferred method	CBR with 50 bytes
Area for simulation	140m x 140m
Simulation time	300s
Nodes	60
Node moving Direction	unsystematic Direction
Node changing speed(m/s)	0 to 10
Path loss rate	3- 20

Likewise, trust node is based on battery deviation and number of hop count between the path. If the node battery deviation increases, the trust value will decrease (Fig.4).When the hop count increases, the trust value decreases, because both are inversely proportional to trust(Fig.5).

Packet Delivery Ratio is defined by the ratio of total number of receiving packets to original packet sent by the sources. The Simulation result of Packet delivery ratio of TpACo when compared to NNT, CSTRP and AODV routing protocol is observed, performance increased with increasing the nodes in the network. The AODV, NNT and CSTRP performances are degraded by malicious. But TpACo performance widely increases 24% than AODV and approximately 9.3% increased than that NNT and CSTRP routing protocols (Fig.6).

End-to-End Delay is a time to transfer the packet across the network form sources to destination. The simulation shows that performance of End to End delay changes with respect to the speed of the nodes in the network. High mobility nodes in the network increases the end-to-end delay (Fig.7).The compared result of TpACo produces 65.4% then AODV and 16%, 23% of results get better than NNT, CSTRP respectively. The simulation result in various speeds with the malicious node of the TpACo algorithm is analyzed and there is some improvement over the other routing protocol.

The throughput is based on network connectivity, Defined as the (number of delivered packets * packet size) to total time duration. The simulation of throughput result of TpACo swarm intelligent algorithm which is better than the comparative performance of NNT, CSTRP and AODV under malicious(Fig.8). It is observed that there is a 20.2% increase in AODV and approximately 14.2% increase than NNT and CSTRP. In NS2 Simulation, after modification of aodv.cc and aodv.h source file, Attacker nodes are introduced in AODV routing protocols. 10 % Attacker nodes are created out of 60 nodes. Then the result of packet delivery ratio, End-to-End delay and Throughput are checked. Next, attacker nodes gradually increased 20%, 30%, 40%, 50% and 60% out of 60 nodes and checked that results for PDR, End-to-End delay and Throughput with TpACo **algorithm in AODV. The created attacker nodes are partially dropped and they forward lesser packet to next hop when selecting the next hop in route selection. As a result, the PDR gradually** decreases due to malicious node and also performances of End-to-End delay and Throughput inversely decreased with respect to malicious node. If the node of 1000 numbers increases within the same area of simulation with 60% of malicious, a better result of PDR, End-to-End delay and Throughput are obtained due to the high node density of the simulation area of 140m X 140m.

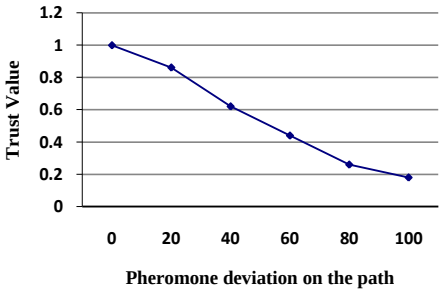

Fig.3 Pheromone density of path Vs Trust Value

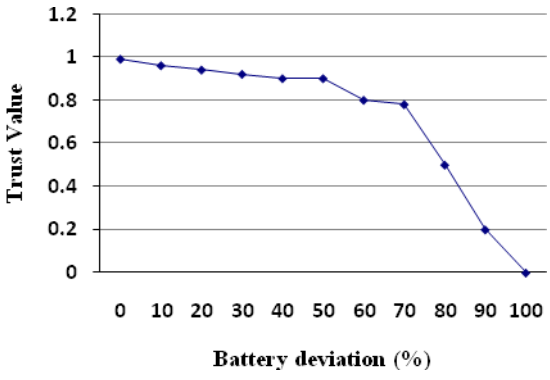

Fig 4 Battery Energy Level in Percentage Vs Trust Value

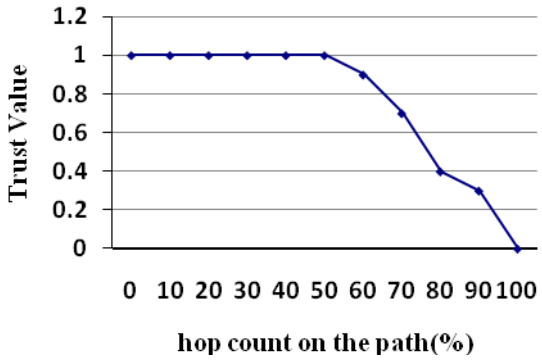

Fig 5. Hop count Vs Trust value

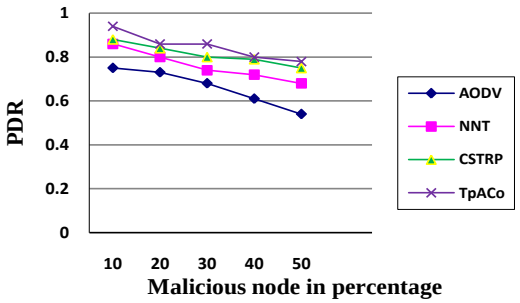

Fig 6. Malicious node in Percentage Vs Packet Delivery Ration(PDR)

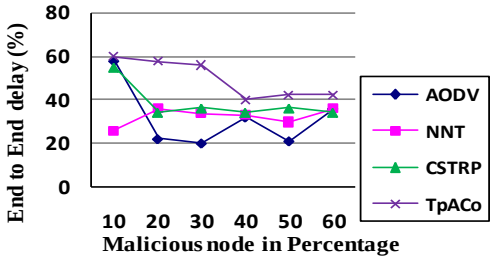

Fig.7 Malicious node in Percentage Vs End to End delay

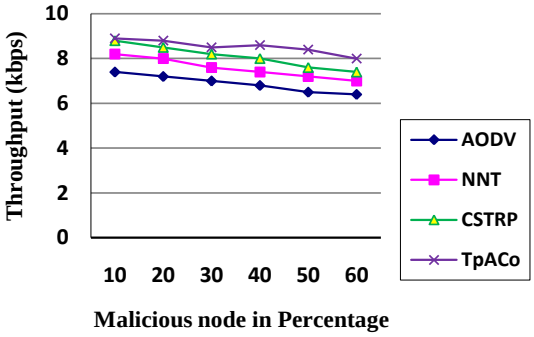

Fig. 8 Malicious node in Percentage Vs Throughput

V. CONCLUSION

In this work, results of Ant colony optimization method provide secured communication route from sender to receiver by trust node are analyzed. . The trust path selection is based on ant pheromone density, number of hop and battery Energy level of the node. The performance is measured with malicious node and collusion in the network and result of a Trust path Ant Colony Optimization algorithm provides better results in Packet delivery ratio, End to End delay and throughput compared with NNT, CSTRP and AODV routing protocol by varying the number of malicious nodes. From the responses, it is observed that the performance of TpACo is better than other methods with respect to performance measures for all the scenarios. It is concluded that the TpACo performs well as compared to AODV, NNT and CSTRP. However End-to-End delay results are better than AODV, NNT and CSTRP, But the overall result in above 50% of malicious node is not satisfactory(Fig 7). In future, the trust node condition will be estimated with cluster mechanism and increased constraints for pheromone value to reduce the End-to-End delay in the Network.

REFERENCES

1. Saleem, K, et. al, "Analyzing ant colony optimization based routing protocol against the hole problem for enhancing user's connectivity experience", *Computers in Human Behavior*, 2015,Volume-*51*, pp.1340-1350.
2. Saleem, K.Fishal, "Enhanced ant colony algorithm for self-optimized data assured routing in wirless sensor networks". In 18th IEEE international conference on networks (ICON), 2012 (PP. 422-427).
3. Preethi, J. D, &Sumathi, R. (2012). "An energy efficient on-demand routing by avoiding voids in wireless sensor network". In Proceedings of the internationalconference on information systems design and intelligent applications 2012. (INDIA 2012) held in Visakhapatnam, India, January 2012.
4. S.Sugumaran, Dr.N. Kumaratharan, "Surveying Various Protocol Attacks and Security Issue in MANET".*International Journal of Advanced Research Trends in Engineering and Technology*-2015.
5. S.Sugumaran, P.Venkatesan,"Stay Away From Packet Dropping Attack in MANET using Neighbor Node Trusted Notion", *Advanced in Natural and Applied Sciences* 2017.
6. S.Sugumaran, P.Venkatesan, "Attacks Reduction in MANET with Cluster Supported Trusted Routing Protocol", *Journal of Advanced Research in Dynamical and Control Systems* 2017.
7. Sharvanig.set.all., "Development of swarm intelligence systems for for MANETS" *International journal on recent trends in engineering & technology*, vol 05, No.01, Mar 2011.
8. Surendar. S, Prakash.S, "An ACO Look-Ahead Approach to Qos Enabled Fault Tolerant Routing in MANET", *China Communication*, August, 2015.
9. NishithaTaraka, AmarnathEmani, "Routing in Ad Hoc Networks using Ant Colony Optimization", 214 *Fifth International on Intelligent Systems, Modelling and Simulation*, 2014 IEEE .
10. SuparnaBiswas, PriyankaDeay and SarmisthaNeogy, "Trusted checkpointing Based onAnt Colony Optimization in MANET", 2012-EAIT, IEEE Conferences.
11. Y.Li,P.Yung, Z. Jianpeng "Trust Cluster Head Electionalgorithm Based on Ant Colony Systems", Computational Science and Optimization (CSO), *Third International Joint Conference* on, Volume:2, 2010 Page(s): 419 – 422.
12. Gurpreet Singh, Neeraj Kumar, Anil Kumar Verma, "Ant Colony Algorithums in MANET: A review", *Journal of Network and Computer Applications, Elsevier journal*-2012.
13. C.V.Anchugam, K.Thangadurai, " Detection of Black Hole Attack in Mobile Ad-HocNetworks using Ant Colony Optimization-Simulation Analysis", *Indian Journal of Science and Technology*, July-2015.
14. Harris Simaremare, AbdelhafidAbouaissa, RiriFitri Sari and Pascal Lorenz, "Performance analysis of optimized Tust AODV using ant Algorithum", *IEEE ICC 2014 – Communications software, Services and Multimedia Applications Symposium*.
15. DevarajanJinilErsis, T.Paul Robert, " Review of ad-hoc on-demand distance vector protocol and its swarm intelligent variants for Mobile Ad-hoc NETwork", The Institution ofEngineering and Technology 2017.
16. A. K. Kordon, ``Swarm intelligence: The benefits of swarms," in *Applying Computational Intelligence*. Berlin, Germany: Springer, 2010, pp. 145_174, doi: https://doi.org/10.1007/978-3-540-69913-2_6.
17. Ant Colony Optimization by Marco Dorigo and Thomas Stutzle, MIT press, 2004. ISBN 0-262-04219-3.
18. M. H. Eiza, T. Owens, and Q. Ni, ``Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 32_45, Jan. 2016.
19. J. Zhou, H. Tan, Y. Deng, L. Cui, and D. D. Liu, ``Ant colony-based energy control routing protocol for mobile ad hoc networks under different node mobility models," *EURASIP Journal*
20. *Of Wireless Commun. Netw.*, vol. 2016, no. 1, p. 105, Dec. 2016, doi:https://doi.org/10.1186/s13638-016-0600-x.
21. P. Vijayalakshmi, S. A. J. Francis, and J. A. Dinakaran, ``A robust energy efficient ant colony optimization routing algorithm for multi-hop ad hoc networks in MANETs," *Wireless Netw*., vol. 22, no. 6, pp. 1_20,2015.
22. P. Memarmoshre_, H. Zhang, and D. Hogrefe, ``Social insect-based sybilattack detection in mobile ad-hoc networks," *in Proc. 8th Int. Conf. Bioin-spired Inf. Commun.Technol*.,2014,pp. 141_148.
23. Karthik, V. S. Ananthanarayana , "A Hybrid Trust Management Scheme for WirelessSensor Networks", *Wireless PersCommun* (2017).
24. Jiang, J., Han, G., Wang, F., Shu, L., &Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 26(5), 1228–1237.
25. Momani, M., Challa, S., &Alhmouz, R. (2010). Bayesian fusion algorithm for inferring trust in wireless sensor networks. *Journal of Networks*, 5(7), 815–822.
26. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in wireless sensor networks: A survey. *Journal of Computer and System Sciences*, 80(3), 602–617.
27. Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", *IEEE Transaction on Mobile Computing*, 2017.
28. M. Matsumoto and T.Nishimura, "Mersenne twister: a 623-dimenionally equidistributeduniform pseudo-random number generator", *ACM Transactions on Modeling and Computer Simuation*(TOMACS), vol. 8, no.1, pp.3-30, 1998.
29. R.H.Jhaveri, S.J. Patel, and D.C. Jinwala, "Dos attacks in Mobile ad hoc networks: A survey," in *Advanced Computing and Communication Technologies (ACCT*), 2012 Second International Conference on. IEEE, 2012, pp.535-541.
30. S.Bhattacharya and T.Basar, "Game-theoretic analysis of an aerial jamming attack on a uavcommunication network", in American Control Conference (ACC). 2010. IEEE,2010, pp.818-823.
31. S.Zhao, R.Kent, and A.Aggarwal, "A Key management and secure routing integrated framework for mobile ad-hoc networks", *Ad hoc network*, vol.11, no.3, pp.1046-1061, 2013.

AUTHORS PROFILE

S.Sugumaran received the Bachelor of Engineering in Electronics and Communication Engineering from Anna University, Tamil Nadu in 2005, the Master of Engineering in Applied Electronics in 2009 from Sathyabama University, Chennai, Tamil Nadu and pursuing Ph.D in the research area of the Mobile Ad-hoc Network Routing Protocols Attacks and Control in SCSVMV (Deemed to be University), Kanchipuram, Tamil Nadu. His publication details include 03 International conferences, 04 International Journals, all these works concerned with Routing Protocol Attacks in MANET. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering, Adhiparasakthi College of Engineering, Kalavai, Vellore District.

Dr. P. Venkatesan, received the Bachelor of Engineering in Electronics and Communication Engineering from University of Madras, Tamil Nadu in 2000 Masters of Engineering in Power Electronics from CEG, Anna University, Tamil Nadu in 2004 Doctor of Philosophy in Signal and Image Processing from SCSVMV (Deemed to be University) Tamil Nadu in 2014. Currently, He is working as Associate Professor in Department of Electronics and Communication Engineering at SCSVMV (Deemed to be University), Kanchipuram, Tamil Nadu. His research interest is in the field of signal & Image processing, wireless communication and Artificial Intelligence He has published more than 35 papers in reputed journals and conferences He is a lifetime member of ISTE, IEEE & IAENG.