Isolating Packet Dropping Misbehavior in VANET using Ant Colony Optimization

Kishan N. Patel
Department of Computer Engineering / IT
SVM Institute of Technology
Bharuch 392-001, Gujarat, India

Rutvij H. Jhaveri
Department of Computer Engineering / IT
SVM Institute of Technology
Bharuch 392-001, Gujarat, India

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are special type of decentralized wireless networks among the various mobile nodes. In VANET decision of forwarding the data packets from one node to other node is dynamic and based on the network connectivity. So efficient, optimized and secure techniques are required for secure transmission of data packets and tracking the changing topology of the network. We propose an ACO based Routing Algorithm in which data packets are forwarded based on the trustworthiness of the neighbor node. The nodes exchanges the Ants (agents) between source and destination deposit the pheromone based on the best path between the source and destination. In this proposed scheme we have projected Ant colony algorithm to defense against malicious attack. It also isolates various attacks and provides secure as well as optimize route from source to destination. We have also analyzed the performance metrics such as packet delivery ratio, end-to-end delay, routing overhead and energy consumption. Simulation result shows that our approach is efficient and reliable.

Keywords

VANET, Trust, AODV, T-ACO, Ant Algorithms

1. INTRODUCTION

Traditional wired networks have mechanism for protection by various means of defense like gateways, firewalls etc Vehicular Ad Hoc Networks (VANETs) [1] are those networks which do not require any infrastructural support for communication among the nodes. Due to high mobility and dynamic nature of the networks it is very difficult to find an optimal path from source to destination in VANET. When the packets travels path from source to destination within the network, the problems such as delay, Jitter and packet loss may occur which directly affects the performance of the network. VANETs has an risk of various misbehaviors like tampering of messages, spamming etc due to lack of centralized administration. VANETs applications support the real time communication and it deals with life critical information in order to do it correctly and effectively, it must follow the security requirements such as integrity, confidentiality, privacy and authentication to protect against attackers and malicious vehicular nodes. Routing [2] is the central theme of the research problems. It is very difficult to give a accurate definition of any algorithm, because the definition may vary according to the authors and its uses.

Ant colony optimization (ACO) [3] is the widely used technique for solving many complex engineering problems. It is the study of Ant's actions to find out the food from nest to food and food to nest vice versa by natural ant. The biological ants in the ant colony form a collective behavior.

One important aspect of a network is its capability to withstand failures and fluctuations in the operation of its nodes and links. Failure may occur in the network in many different ways, it depends on the systems complexity. A network is robust if their function is not affected by the attacks to nodes or links, which can be done by malicious node. Thus, the robustness of networks is to guarantee the security of network systems.

In a packet dropping attack, the malicious nodes always reply positively to route request whether it may not have valid route and send the reply with higher sequence number to sender. So all traffic is diverted towards malicious nodes which drops the packet. Therefore, the security as well as optimization of network structures is needed. The newly approach avoids the inclusion of misbehaving node during route establishments and finds the secure and optimized route the by using the trust metrics and ant algorithm and also improves the network performance which is one of the major requirement of security schemes for complex networks like VANETs.

This paper is organized as follows. Section-II highlights the theoretical background. Related work is discussed in section-III. Section-IV discusses the proposed solution. Evaluation of our mechanism with simulation results is presented in section-V. Section-VI concludes the paper.

2. THEORETICAL BACKGROUND

2.1 Overview of Ant Colony Optimization

The ant colony optimization (ACO) [4] is a probabilistic technique which is used for solving computational problems and helps to find good path. As shown in below figure ants find the shortest path while searching for their food to nest vice versa.

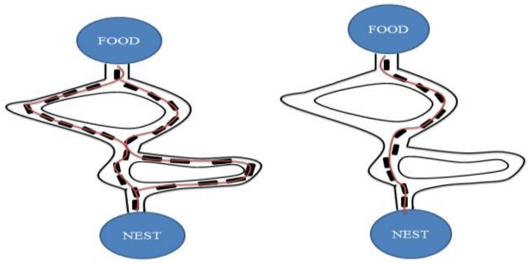

Fig 1: ANT Mechanism [5]

This algorithm is a member of swarm intelligence methods, and it contains some metaheuristic techniques. It is based on the behavior of ants finding the shortest path between their colony and the food.

❖ Application of Ant Colony Optimization:

a) Network Optimization
b) Scheduling problem
c) Vehicle routing problem

d) Assignment problem
e) Device Sizing Problem in Nanoelectronics
f) Image Processing

2.2 Ant Colony Optimization Mecanism

The foraging behavior of ants has more unique ability to find the shortest path from their nests to a food source. Some experiments which are done on the certain ants' shows the communication occurs by depositing a substance called pheromone along the path. It also deposits the pheromone with higher concentration where there is shortest route which is known as Ant Colony Optimization (ACO) [6]. ACO has highly dynamic parameters. Most ant have very limited or no vision.

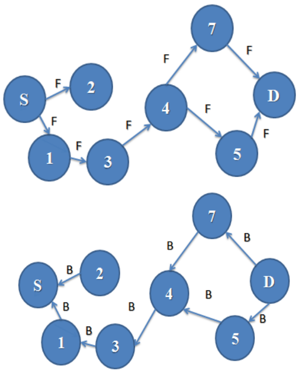

Fig.2: FANT and BANT Agent [7]

As shown in Figure 2 there are two types of agents in routing algorithm: forward ant agents (FANT) which is from source to destination, in its going to destination process to collect information about the quality of path; backward ant agents (BANT) which is from destination to source. The creation of new routes requires the use of a forward ant (FANT) and a backward ant (BANT). A FANT is an agent which establishes the pheromone track to the source node. In contrast, a BANT establishes the pheromone track to the destination node. The FANT is a small packet which has its unique sequence number. Nodes are able to differentiate duplicate packets on the basis of the sequence number and the source address of the FANT. Ants decide on which path they would follow based on the pheromone concentration deposited on each particular path. Those paths which have greater pheromone concentration will have higher probability of selection. Therefore, the selection among the paths is biased toward the shortest path. Each ant search for route in the network, it can according to routing information to choose path, and then can modify the routing table value, look for good path.

2.3 Packet Dropping Attack

In this section we discuss the working of packet dropping attack along with the outline of AODV routing protocol. Packet dropping attacks are widespread DoS attacks on Ad hoc networks.

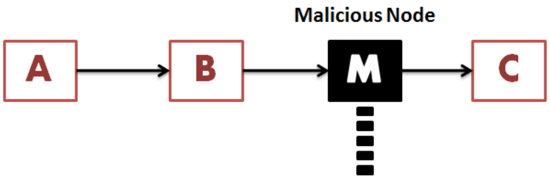

Fig.3: Packet dropper behavior

Packet dropper AODV or Packet dropping attack is the AODV under malicious attack. As shown in Figure 3 behavior of the attacker M that drops the packets sent by source A towards destination C. In this packet dropping attack the malicious nodes allows only 70% of packets and drops 30% of packets.

3. RELATED WORK

Gianni et al. [8] compared the behavior of other five shortest paths routing algorithms. Also considered heavy traffic conditions for some representative temporal and spatial traffic distributions for a real network instance. It showed always a robust behavior and able to reach a good stable level in performances.

Marwaha et al. [9] proposed the ANT AODV. It is combination of the on-demand routing capability of Ad Hoc On-Demand Distance Vector (AODV) routing protocol with ant-like mobile agents. It reduces latency and the end-to-end delay by providing high connectivity without any cost of extra processing of the ant messages also it does not affect to the packet delivery.

Kaur et al. [10] proposed an Ant Colony Optimization (ACO) technique in conjunction with linear programming approach for minimizing the overall delay which are used for exploring the optimum route from source of food. The algorithm has been able to cope with all dynamic networks also it has ability to improve the link performance. It can achieve optimum route performance with reduced link delay.

Singh et al. [11] proposed a new ACO based Routing Algorithm(ANTALG). There will be random selection of source and destination nodes and exchanges the Ants between them. And also optimal behavior is not for searching shortest-hop paths but also for the quality of the links which make up those paths. A future packet uses those in a stochastic manner.

Melchor et al. [12] proposed AntTrust, it facilitates a malicious manipulations of data packets. The protocol is for ensuring routing features and for adding some security level to routes and inspired by multi-agent systems by ant colony and their ability to solve complex problems for establishing paths in ad-hoc networks.

Bahaa et al. [13] proposed Agent-Based Trusted Dynamic Source Routing protocol. To overcome the misbehavior of node, the trustworthiness of the network nodes should be considered in the route selection process, this protocol manages trust information locally with minimum overhead. Also Multi agent system is installed. It consists of two types of agents: monitoring agent and routing agent and weighted by both number and size of routed packets to for selective forwarding behavior of a node.

Simaremare et al. [14] proposed a new trust mechanism for security against DOS attacks. And also used ant colony optimization in which ants can move freely to find their destination. It will deposit pheromones if node is trusted. By using ACO throughput and PDR is increased.

Table 1.Shows Comparison of Various Ant Algorithms

Algorithm	**Type of Ants**	**Type of Ants Pheromone evaporation**	**Problem**
Antnet [8]	Forward and backward ants	By forward and backward ants	Long delays in propagating routing information
Ant AODV [9]	Ant agents	By Ant agents	Route Error

Improved Ant routing algorithm [10]	Forward and backward Ants	Single Ant	Overhead of hello packets
ANTALG [11]	Forward Ant, Backward ant	Backward Ant, data packets and proactive forward ants	Less overhead
Ant Trust [12]	Ant agents	By Ant agents	Less Security
ATDSR [13]	Monitoring agent and Routing agent	By Ant agents	Less security
TACO	Forward Route Ant Agent and Backward Route Ant Agent	By FRAA and BRAA	Higher Security and Optimization

4. T-ACO : THE PROPOSED SOLUTION

In this whenever node wish to send the packet it will find the valid route but if valid route is not found then route discovery process is started forward ant is brodcasted to all its neighbour. Ant will calculate the the trust value as well as it will deposite the pheromone. Destination node recieves the ant and again backward ant is created. The backward ant has information regarding the trust of ech node in the route. When the backward ant is received by source node then the shorter and the trustworthy route is selected for sending the data packet. If the route contain the malicious node then that route is neglected and the packet will be send by another route which drops the less number of packet.. If all the route contain the malicious node the packet will be send from route which contain less number of malicious node and which send maximum number of packet.

4.1 Algorithm

Each node participating in the network must install the (multi-agent system) MAS and perform routing.

Step 1: Trust value is calculated by the NEA. This value is updated whenever routing is performed.

R f: no of all packets this not has received and was asked to forward to another node.

H f: no of packets actually forwarded by this node

SR f: The total size of all packets this node has received and was asked to forward to another node.

SH f: The total size of all packets actually forwarded by this node.

C f: total number of control packets generated.

D f: total number of data packets received.

The trust value is calculated by this formula:

$$\mathbf{Tr\ (Ni)} = \alpha\ \frac{\mathbf{Hf\ (Ni)}}{\mathbf{Rf\ (Ni)}} + \beta\ \frac{\mathbf{SHf\ (Ni)}}{\mathbf{SRf\ (Ni)}} + \gamma\ \frac{\mathbf{Cf\ (Ni)}}{\mathbf{Df\ (Ni)}}$$

α, β ,γ are weight factor used for trust calculation.

Step 2: Node wish to send packet it find a valid route in routing table.

Step 3: If valid route is not found it creates RAA Route Ant Agent and broadcast to its entire neighbor. FRAA (Forward Route Ant Agent) is RAA with forward status.

Step 4: If neighbor node is intermediate node then deposit pheromone value and set trust value which is minimum of RAA and NEA.

Pheromone Decrement formula:

$$\mathbf{PRD} = \frac{\mathbf{1}}{\mathbf{Maximum\ no\ of\ hops}}$$

Step 5: Check the trust value and pheromone value Trust value is less then threshold and pheromone value is zero then node is malicious go to step 3.

Step 6: Neighbor node is destination node then create BRAA (Backward Route Ant Agent) is RAA with backward status and send it to source node.

Step 7: Source node receive the BRAA and wait for timeout if it is timeout then BRAA is destroyed route is invalidated.

Step 8: BRAA is received with reverse info then check the route quality.

$$\mathbf{Q\ (Rj\ ) = \mu\ Tr + (1 - \mu)\ Pj\ (Nn)}$$

μ is the trust/performance weight factor.

The route with the maximum quality is selected for delivering the packet and routes with lower trust and pheromone value of are avoided.

4.2 Flow Charts

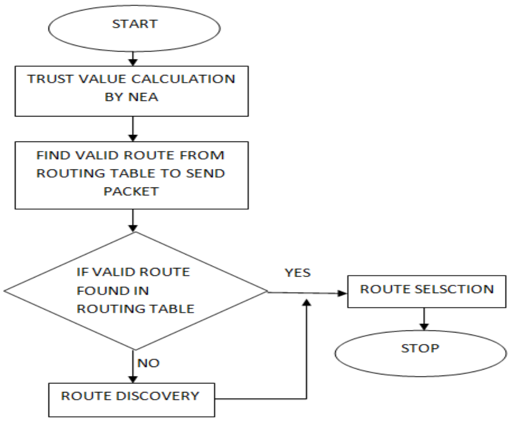
START
TRUST VALUE CALCULATION BY NEA
FIND VALID ROUTE FROM ROUTING TABLE TO SEND PACKET
IF VALID ROUTE FOUND IN ROUTING TABLE
YES
ROUTE SELSCTION
STOP
NO
ROUTE DISCOVERY

Fig.4: Routing process

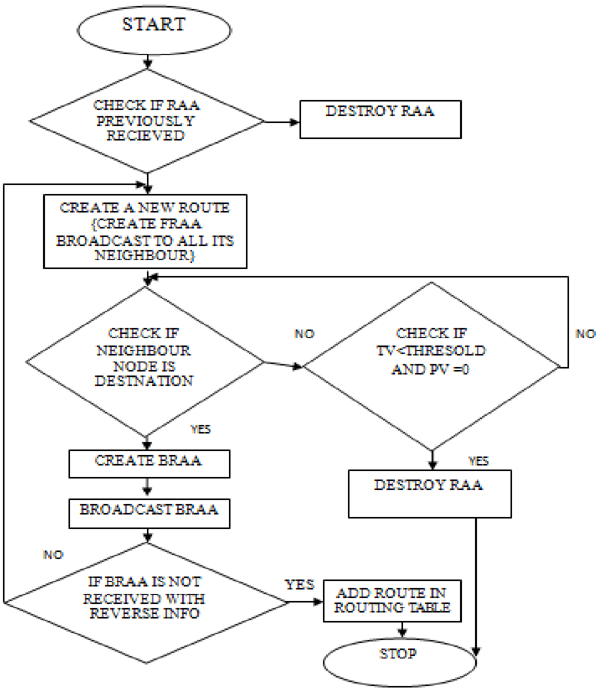
START
CHECK IF RAA PREVIOUSLY RECIEVED
DESTROY RAA
CREATE A NEW ROUTE {CREATE FRAA BROADCAST TO ALL ITS NEIGHBOUR}
CHECK IF NEIGHBOUR NODE IS DESTNATION
NO
CHECK IF TV<THRESOLD AND PV =0
NO
YES
CREATE BRAA
BROADCAST BRAA
YES
DESTROY RAA
NO
IF BRAA IS NOT RECEIVED WITH REVERSE INFO
YES
ADD ROUTE IN ROUTING TABLE
STOP

Fig.5: Route discovery process

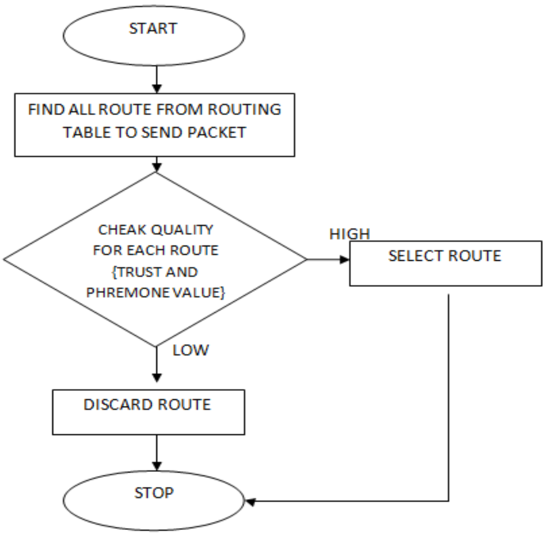
START
FIND ALL ROUTE FROM ROUTING TABLE TO SEND PACKET
CHEAK QUALITY FOR EACH ROUTE {TRUST AND PHREMONE VALUE}
HIGH
SELECT ROUTE
LOW
DISCARD ROUTE
STOP

Fig.6: Route selection process

5. EVALUATION OF T-ACO

This section shows the performance evaluation of our solution T-ACO under different metrics with various network parameters with simulation environment described as follows.

5.1 Simulation Environment

Simulations are performed using ns-2 network simulator which is the network simulation tools that provides implementations of a variety of routing protocols. We move 10 to 50 nodes in the area of 800m x 800m for the simulation time of 600 seconds. Transmission range of each node is 500m. We use UDP at the transport layer. We vary following network parameters in our simulations.

Table 2. Simulation Parameters

Parameter	Value
Simulator	NS-2 (ver.-2.34), SUMO (ver.-0.12.3)
Area	800 x 800
Number of Nodes	10,20,30,40,50
Malicious Nodes	3,6,9,12,15
Number of Connection	3,5,7
Simulation Time	600 sec
Traffic Type	Constant Bit Rate (CBR)/UDP
Protocol	AODV, Packet Dropping Attack, T-ACO
Maximum Speed	40 m/sec

5.2 Perfomance Metrics

To evaluate the performance of our solution, we use the following metrics:

5.2.1 Packet Delivery Ratio (PDR)

The ratio of the number of data packets received by the application layer of destination nodes to the number of data packets transmitted by the application layer of source nodes.

5.2.2 Average End-to-End Delay

Average time taken by the transmitted data packets to reach to the corresponding destinations.

5.2.3 Normalized Routing Overhead

The ratio is measured between number of data packets and number of control packets over a communication channel its called Routing overhead.

5.3 Simulation Results and Analysis

5.3.1 Packet Delivery Ratio

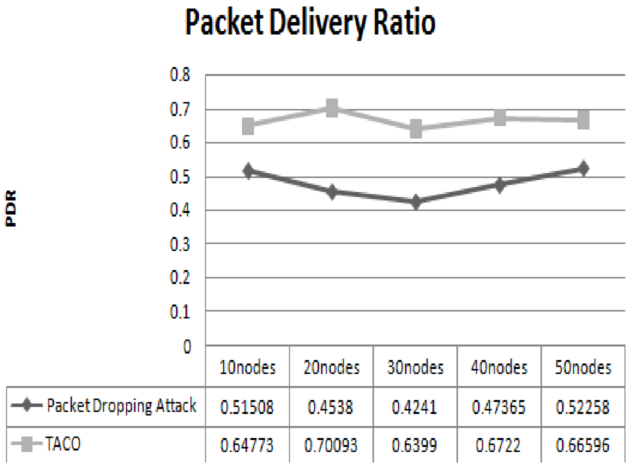

Fig.7: Packet Delivery Ratio

In Figure 7, we compared the Packet dropper AODV with T-ACO protocol. In this, Packet Delivery Ratio is plotted as the number of nodes increases. As we can seen from the graph, with T-ACO running, packet delivery ratio is increases compared to Packet Dropper AODV. Here in simulation we consider 30% misbehaving nodes in network.

5.3.2 End to End delay

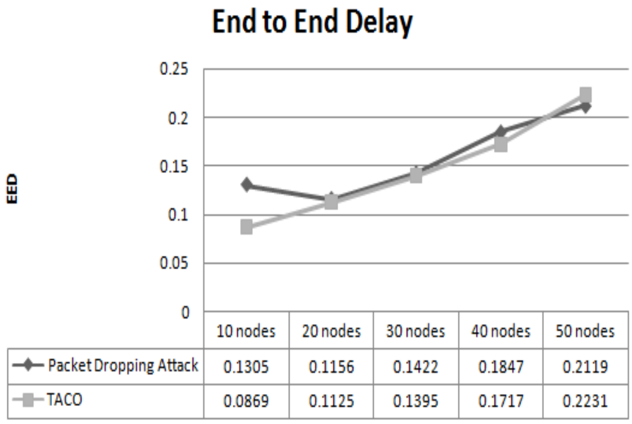

Fig.8: End to End Delay

It measures the average delay time that is taken by data packet from source to destination. The above figure 8 describes the comparison between the proposed scheme and packet dropping attack with respect to end to end delay. In this, the delay of proposed scheme is less than packet dropping attack.

5.3.3 Routing Overhead

Defined graph in the results plots its metric as a percentage of Routing Overhead and number of nodes taken into account. In this, the Routing Overhead of proposed scheme is less than packet dropping attack

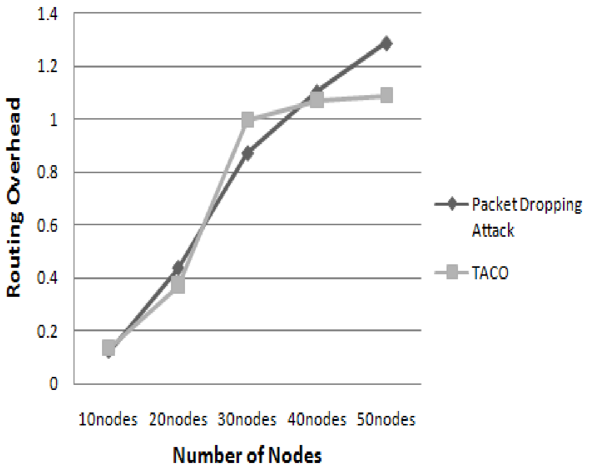

Fig 9: Normalized Routing Overhead

5.3.4 Energy Consumption

It measures the average energy that is consumed by mobile nodes during transmission process. In this, the consumption is increased in packet dropping attack with compare to proposed scheme.

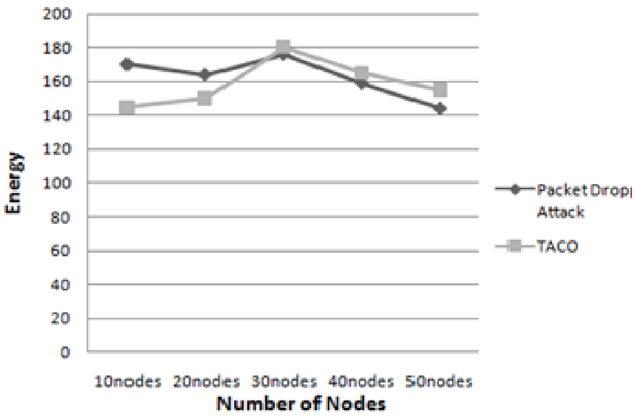

Fig 10: Average Energy Consumption

6. CONCLUSION

In this paper, we provide an improvement in route discovery process to isolate multiple attacks of malicious nodes. Due to presence of the malicious node in the network it might drop some of the data packets so it is not possible to send all the data packets from source to destination in presence of an attacker. As the number of malicious node increases the packet dropping ratio is also increases. Our protocol is efficient in detecting as well as isolating the malicious nodes and provides trustful environment. In this, we analyze the problem of packet dropping attacks in AODV routing protocol. We proposed T-ACO for secure routing by avoiding the packet-dropping attack. We simulate the proposed solution using the SUMO and NS-2.34 simulator. This mechanism provides high packet delivery rate with average end-to-end delay with normal routing overhead and average energy consumption under attack of malicious node.

In future, we can apply different ant algorithm for more accuracy. We can also concentrate on different types of attacks like selfish, worm hole, etc and then compare it with other prevention techniques.

7. REFERENCES

[1] Wang, Yu, and Fan Li. "Vehicular ad hoc networks." Guide to wireless ad hoc networks. Springer London, 2009. 503-525.

[2] Patel, Kishan N., Jhaveri, Rutvij H. "A Survey on Emulation Testbeds for Mobile Ad-hoc Networks." Procedia Computer Science 45 (2015): 581-591.

[3] Nature-Inspired Metaheuristic Algorithms Second Edition.,www.econ.ubbcluj.ro/~rodica.lung/taco/.../Yang_nature_book_part.pdf.

[4] Dorigo, Marco, and Mauro Birattari. "Ant colony optimization." In Encyclopedia of Machine Learning, pp. 36-39. Springer US, 2010I.S.

[5] Adnan, Md Akhtaruzzaman, Mohammd Abdur Razzaque, Ishtiaque Ahmed, and Ismail Fauzi Isnin. "Bio-Mimic Optimization Strategies in Wireless Sensor Networks: A Survey." *Sensors* 14, no. 1 (2013): 299-345.

[6] Jaiswal, Utkarsh, and Shweta Aggarwal. "Ant Colony Optimization." at International Journal of Scientific & EngineeringResearch 2, no. 7 (2011).

[7] Jha, Mrs Smitha, D. K. Mallik, and R. K. Suri. "Balanced Ant Colony Algorithm for Scheduling DAG to Grid Heterogeneous System." *International Journal of Scientific and Engineering Research* 2, no. 6 (2011): 184-193.

[8] Di Caro, Gianni, and Marco Dorigo. "AntNet: Distributed Stigmergetic Control for Communications Networks." *J. Artif. Intell. Res.(JAIR)* 9 (1998): 317-365.

[9] Marwaha, Shivanajay, Chen Khong Tham, and Dipti Srinivasan. "Mobile agents based routing protocol for mobile ad hoc networks." In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, vol. 1, pp. 163-167. IEEE, 2002.

[10] Kaur, Sarbjeet, Ravinder Singh Sawhney, and Rajan Vohra. "MANET link performance parameters using ant colony optimization approach." *International Journal of Computer Applications* 47, no. 8 (2012).

[11] Singh, Gurpreet, Neeraj Kumar, and Anil Kumar Verma. "ANTALG: An Innovative ACO based Routing Algorithm for MANETs." *Journal of Network and Computer Applications* 45 (2014): 151-167.

[12] Melchor, Carlos Aguilar, Boussad Ait Salem, Philippe Gaborit, and Karim Tamine. "AntTrust: A novel ant routing protocol for wireless ad-hoc network based on trust between nodes." In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pp. 1052-1059. IEEE, 2008.

[13] Bahaa-ElDin, Ayman M., Islam Tharwat A. Halim, and Hossam Fahmy. "ATDSR: Trusted On-Demand Routing Protocol based on Agents for Mobile Ad-hoc Networks." *arXiv preprint arXiv:1211.2946* (2012).

[14] Simaremare, Harris, and R. Sari. "Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious attacks." *IJCSNS* 11, no. 6 (2011): 277-287.