Asian Journal of Information Technology 15 (11): 1739-1745, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

OTSIR: An Optimal Trust Based Swarm Intelligent Routing in Manet

[1]S.P. Manikandan and [2]R. Manimegalai
[1]Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering,
Sriperumbudur tlk, 602117 Chennai, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Park College of Engineering and Technology,
Kaniyur, Karumathampatti, 641659 Coimbatore, Tamil Nadu, India

Abstract: Mobile Ad Hoc Network (MANET) is a network of low cost, small, mobile and self-configuring devices which have no fixed infrastructure and centralized administrative control. Openness of the communication channel and mobility of nodes makes it vulnerable for intruder nodes in the network. Therefore, efficient trust based routing protocols are required for MANETs in order to provide better security. This research proposes an Ant Colony Optimization (ACO), Optimal Trust based Swarm Intelligent Routing (OTSIR), to select the best path with trusted nodes. The proposed ACO based algorithm is implemented and its performance is compared with the conventional on-demand Dynamic Source Routing (DSR) protocol. The performance of the proposed algorithm is analyzed by measuring parameters such as packet delivery ratio, packet loss ratio and end-to-end delay. The experimental results obtained show that the proposed OTSIR for routing gives better performance than the on-demand DSR routing.

Key words: MANET, dynamic source routing, trust based routing, ant colony optimization, swarm intelligence

INTRODUCTION

Mobile Ad hoc Network (MANET) is a kind of infrastructure-less wireless network. It has a small group of self-configured mobile nodes connected by wireless links with no base station. In MANETs, each host can act as a router and all nodes communicate by wireless links. MANETs are said to be dynamic as nodes in the network are mobile (Kumar and Mishra, 2012). In MANETs, communication between nodes use multi hop paths. Density and deployment of nodes in MANET depend on the application which uses the MANET. Some of the challenges in MANET are listed below (Ramanathan and Redi, 2002):

- The communication medium is unprotected from outside signal
- Wireless medium is unreliable when compared to the wired medium
- Hidden terminal and expose terminal phenomenon may occur

Traditional TCP/IP protocol architecture is used by MANET nodes for end-to-end communication. As MANET has mobile nodes and each node has limited resources, TCP/IP layer functionality should be appropriately modified for efficient routing operations. Routing protocols by Abolhasan *et al*. (2004) used for MANETs can be classified into three types, namely, proactive, reactive and hybrid routing algorithms. In proactive algorithms, routes are assigned to all destination nodes at the starting period and updated periodically. Reactive protocols use route discovery process whenever a source wants to start a communication. Hybrid routing protocols combine features of both proactive and reactive protocols. Different types of applications and users may expect different Quality of Service (QoS) from MANET. Some of the applications of MANET include military communication in battle fields, remote weather monitoring using sensors, monitoring earth activities, disaster recovery, earthquakes, crowd control and commando operations, virtual class and conference rooms, multi-user games, robo pets, automatic call forwarding, advertise location specific services and location dependent travel guide.

Subjective logic is one of the trust models that consider beliefs of real world as opinion. An opinion can be represented as a probability measure which represents uncertainty about the real world things (Josang, 2001).

Corresponding Author: S.P. Manikandan, Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering, Sriperumbudur tlk, 602117 Chennai, Tamil Nadu, India

Two types of trusts, namely node trust and route trust are used in trust model (Li *et al*., 2004). For each route in the routing table, trust is calculated by measuring the reliability when a data can be sent to a destination using the route. Node trust is calculated at each node for its neighbor nodes. Node trust helps the node by suggesting the route through its neighbors. As the topology of MANET is dynamic, the trust values in each node should be updated regularly.

Swarm intelligence based routing is inspired from the behaviour of insect groups such as ants and bees. They search for food and find the shortest possible path between food and nest. During forward movement, these insects release a special hormone called pheromone. This special hormone, i.e., pheromone is sensed by other insects in order to find the shortest path between food and nest. In this study, a novel trust based routing algorithm, Optimal Trust based Swarm Intelligent Routing (OTSIR) which employs Ant Colony Optimization (ACO) is proposed.

Literature review: Routing in MANETs is affected by node misbehaviours. Aravindh *et al*. (2013) have presented a trust based approach for detection and isolation of malicious nodes in MANET. For secure routing, trust values are updated at each node periodically while forwarding a packet. Trust values are calculated by employing direct trust calculation and recommended trust calculation. Each node calculates direct trust for its neighbors based on their behavior. Indirect trust is calculated for a target node by its neighbouring nodes. Based on direct trust and recommended trust, trust handler determines trust count for each node in the network. Each node maintains a trust counter and if the trust value is less than a specified threshold value, then, the corresponding node is marked as malicious node and isolated from the network. Isolating malicious nodes improves the network performance in terms of packet delivery ratio, packet loss ratio and end-to-end delay (Aravindh *et al*., 2013).

Priyadharshini and Arunachalam have presented an efficient genetic algorithm for optimal routing in Ad Hoc networks by. Proactive routing protocols are based on routing tables, whereas, reactive protocols are called as on-demand protocols. Priyadharshini and Arunachalam (2013) study genetic algorithm is used to find the minimum cost path between a source node and a destination node. The fitness function is designed to minimize the cost function and optimize bandwidth metrics in order to select an optimal path between source and destination.

The most challenging task in MANET is finding an efficient and secured routing in spite of mobile and dynamic nodes in MANET. In ACO routing algorithms, artificial ants are used to establish an optimal route between source and destination. One artificial ant could communicate with others indirectly by depositing pheromones. The performance analysis of Ant Colony Optimization (ACO) algorithms for MANETs is presented by Sebastin (2013). The results obtained in have proved that ACO algorithms are suitable for MANETs where nodes are moving mobile and dynamic with frequent topological changes.

Benamar and coauthors have presented an ant-colony based routing algorithm, AntPKI, for MANETs in. ACO routing algorithms use two different types of artificial ants for discovering and establishing routes, namely, Forward ANT (FANT) and Backward Ant (BANT). FANT searches the entire network to find possible routes from source to destination and deposits an artificial pheromone in intermediate nodes. This pheromone values are used by BANT to select a final route. While constructing the solution, pheromone table is updated with new pheromone value. The pheromone values are increased by FANT during its forward movement and decreased by BANT if the route is not optimal. In the proposed algorithm, AntPKI guaranties data confidentiality by establishing session key along with certificate publishing (Kadri *et al*., 2013).

A novel ant-based security alert routing algorithm, ODASARA, for MANET in grid environment is presented by. ODASARA uses ACO to select optimal routes and included security as a negotiable metric to improve the relevance of routes. Trust levels are formed for each node. At the time of route discovery, security information requested by sender node is also attached with RREQ packet. Any node which violates security parameters will not be considered as part of the route to the destination. Experimental results obtained by Rameshkumar and Damodaram (2010) indicate that there is a decrease in the control overheads by 1.27% using the proposed ACO based routing algorithm.

MATERIALS AND METHODS

Trust based routing using ant colony optimization

Trust computation: The trust metrics are measured using the availability of security mechanisms to thwart network and system attacks. The Internal Trust (IT) of the node is computed based on its ability to defend against virus attacks, network attacks and unauthorized resource utilization:

$$IT = \sum \varphi_{Av} + \varphi_{Fw} + _{Aut}$$

$$\varphi_{Av}\begin{bmatrix}0,\text{if antivirus product is not present}\\0.5,\text{if antivirus product is present but not update}\\1,\text{if antivirus is product is present and up to date}\end{bmatrix}$$

$$\varphi_{Av}\begin{bmatrix}0,\text{if firew wall not present}\\2,\text{if firew all is present and not upto date}\\4,\text{if firew all is present and up to date}\end{bmatrix}$$

$$\varphi_{Aut}=\begin{bmatrix}0,\text{if authorization mechanism of any type, not present}\\1,\text{if password based authorization mechanism such present}\\2,\text{if alternetive authorization mechanism such as}\\\text{biometrics is present}\end{bmatrix}$$

The proposed Trust Correlation Score (TCS) between two nodes U and V is given by:

$$TCS_{uv}=a.\sum\frac{(u_{IT}-v_{IT})}{(u_{IT}-v_{IT})^2}+\frac{P_{dv}}{P_{sv}}$$

where:

U = The node which originates a request and
V = The node which forwards the request
u_{IT} and v_{IT} = are the internal trust of nodes
U and V = A is the trust level required
P_{dv} = The total packet delivered by
v P_{sv} = The total packet sent to v

Proposed optimal trust based swarm intelligent routing (otsir): Ant Colony Optimization (ACO) algorithm (Chicco, 2011) is one of the stochastic search procedures which uses a parameterized probabilistic model called pheromone model. The ACO algorithm is an iterative process and in each iteration M artificial ants search the solution space in parallel. In each iteration, the pheromone value is updated in order to reach an optimal solution during consecutive iterations.

Basic_ACO_Algorithm ( ):

{ 1. Create m number of global ants.
2. Evaluate their fitness using end-to-end delay and PDR.
3. Update the value of pheromone locally.
4. Check whether fitness is improved.
5. Move local ants to better regions.
6. If not improved, select a new search direction in randomly manner, go to step2.
7. If termination condition met (all ants moved towards optimal path).
Update ant's pheromone globally. }

ACO algorithms (Wang *et al*., 2007) are characterized by the following parameters:

- Probabilistic transition rule which is used to identify the moving direction of each ant and
- Pheromone update mechanism which impacts quality of the solution.

ACO algorithms are used for local search or global search in order to select best regions that contain optimal solution. The ACO algorithm for optimization problems is shown above. In this research, the optimal paths are chosen based on the trust value, end to end delay and packet delivery ratio. The trust values are computed for each node as discussed in the previous section. Thus, the objective of the proposed OTSIR is formulated as:

$$\text{Objective}=\alpha TCS_{uv}+\beta e^{\left(\frac{\text{end-to-end delay}}{\text{packet delivery ratio}}\right)^2}$$

where: α and β are constants and $\alpha + \beta = 1$. In this research, the weightage is given more for security, thus, α and β are assigned values 0.7 and 0.3.

Local ants can move to the latent region where the best solution is available, according to the probability of transition $P_i(t)$ of region i which is computed using the formula given as follows:

$$P_i(t)=\frac{\tau_i(t)}{\sum_{j=1}^{g}\tau_j(t)} \quad (1)$$

Equation 1, $\tau_i(t)$ is the total pheromone of region i during time t, and g represents the total number of global ants. The proposed ACO algorithm uses two rules for updating the pheromone:

- Local pheromone update rule which is used while constructing solutions
- Global pheromone updating rule is applied after all the ants construct a solution

In ACO algorithm, the local pheromone update rule is based on trust values of one hop nodes, whereas, the global pheromone updating is based on trust values of all intermediate nodes in the route to destination.

An ACO algorithm has two important mechanisms, namely, trail evaporation and daemon actions (Salami, 2009). Trails of longer paths evaporate in order to avoid accumulation of trails after some duration. Centralized actions that are performed by daemon operations invoke local optimization and update global optimization procedures to eliminate bias in the optimization. Steps involved in the proposed trust based ACO algorithm are shown in Fig. 1. In this research, each node evaluates the trust factor of its neighbouring nodes. Neighbour nodes are identified in the search list and ant agents are generated accordingly. The ACO algorithm is used to achieve the best possible solution. If termination condition is met, then optimal route is generated between

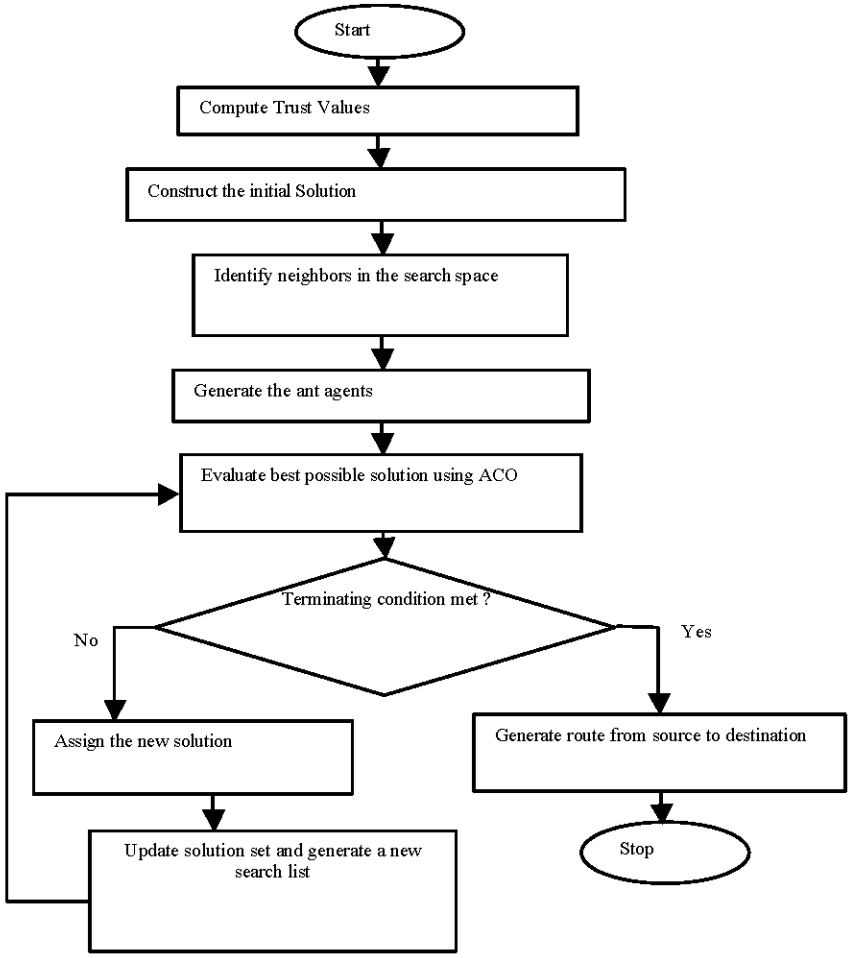

Fig. 1: Steps involved in the proposed trust based aco routing

source to destination. Otherwise, a new search list is generated with a new solution set and the evaluation process is repeated till termination condition is met. Thus, the proposed trust based ACO algorithm uses values of trust to find optimal path which consists of trusted nodes between source and destination.

A trust based mechanism to mitigate black hole attack in MANETs is proposed in. When a source node wants to transmit data packet to a destination node, it broadcasts ants to find the optimal route. Ants move forward to neighbouring nodes updating the pheromone table based on trust values of neighbouring nodes. Computation of trust values is presented elaborately in (Manikandan and Manimegalai, 2013) and summarized in the previous subsection. Ants are either unicasted or broadcasted depending on information of whether or not the node has route for destination. If a route to destination is not available, then, ants are broadcasted else unicasted along the route to destination. Ants move towards the destination by continuously updating the pheromone table. On reaching the destination, a route reply packet with the trust values is sent back to the source node. The best route to the destination with high trust value is chosen to transmit the data.

RESULTS AND DISCUSSION

Simulations are conducted with 80 nodes with varying number of malicious nodes introduced in the network. Performance of the proposed algorithm is analyzed by measuring the following parameters:

- Packet Delivery Ratio (PDR)
- End-to-end delay in milliseconds and
- Packet loss ratio

Two routing algorithms, namely, DSR and the proposed ACO based algorithm, OTSIR, are used in simulation.

Fig's 2-4 show the Packet Delivery Ratio (PDR) by employing DSR routing and the proposed trust based ACO routing with 0, 10 and 20% malicious nodes

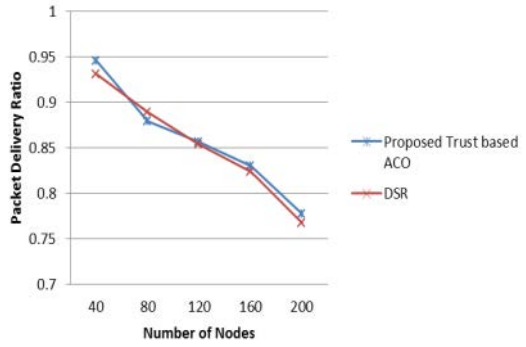

Fig. 2: Packet delivery ratio measured using trust based ACO routing and DSR with 0% malicious nodes

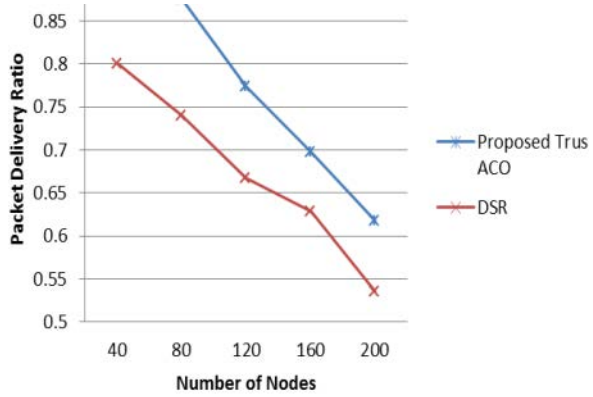

Fig. 3: Packet delivery ratio measured using trust based ACO routing and DSR with 10% malicious nodes

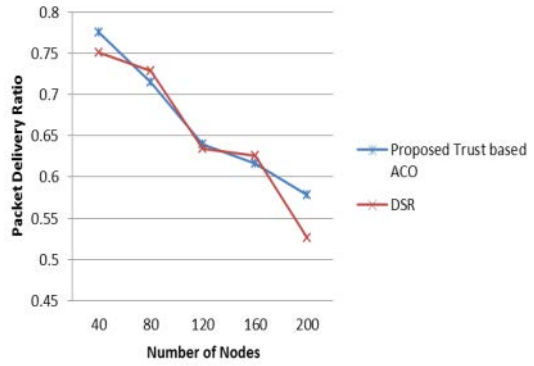

Fig. 4: Packet delivery ratio measured using trust based aco routing and dsr with 20% malicious nodes

network is made up of only trusted nodes (i.e., with 0% malicious nodes) the proposed algorithm, OTSIR, performs slightly better than the classical DSR. As shown in Fig. 2 with 0% malicious nodes in the network, the improvement due to the proposed algorithm is 0.35-1.58%. However, performance of the

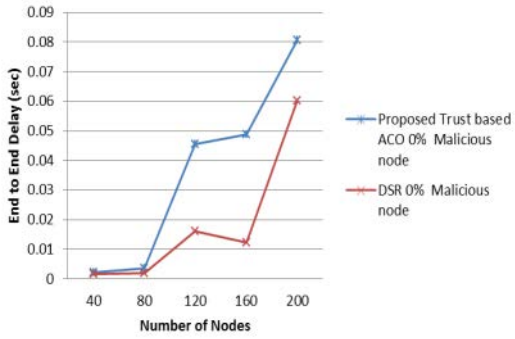

Fig. 5: End-to-end delay measured using trust based aco routing and dsr with 0% malicious nodes

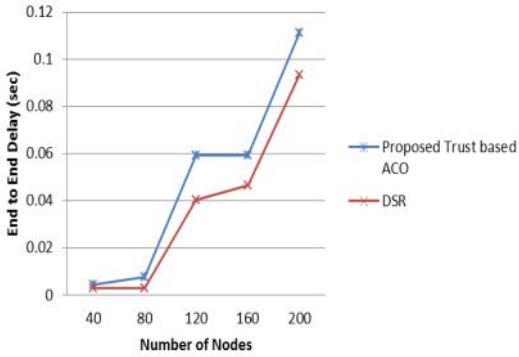

Fig. 6: End-to-end delay measured using trust based ACO Routing and DSR with 10% Malicious nodes

respectively in the network. It is observed that when the proposed algorithm improves over DSR when malicious nodes are introduced in the network. An average of 20% improvement in PDR is observed using the proposed method when compared to DSR with 10% malicious nodes in the network which is shown in Fig. 3. As shown in Fig.4, the proposed trust based ACO routing improves the PDR by 9.99% when compared to the DSR algorithm with 20% malicious nodes in the network.

The end-to-end delay measured using the proposed OTSIR algorithm and DSR algorithm are shown in Fig. 5-7. End-to-end delay is much higher in the proposed method than the DSR. This is mainly due to the trust calculation between neighboring nodes, which is a time consuming task. Though the proposed method improves the PDR, further investigation is required to reduce the end-to-end delay. Fig. 8-10 show the packet loss ratio of DSR routing and the proposed method with 0, 10 and 20% malicious nodes in the network. When there are no malicious nodes in the network (0% malicious nodes), the packet loss ratio using the proposed algorithm is similar to that of DSR. When there are 10% malicious

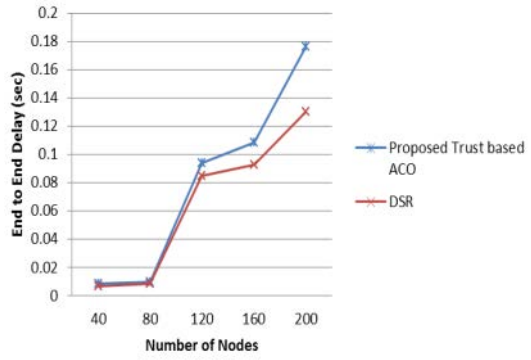

Fig. 7: End-to-end delay measured using trust based ACO routing and DSR with 20% malicious nodes

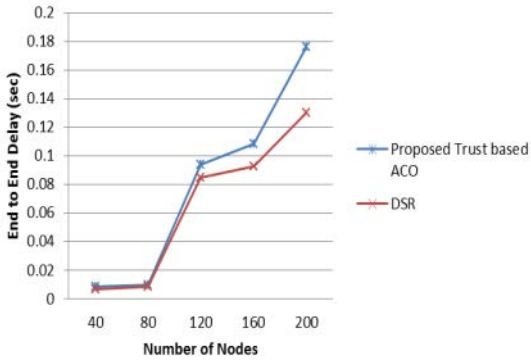

Fig. 8: Packet loss rate measured using trust based ACO routing and DSR with 0% malicious nodes

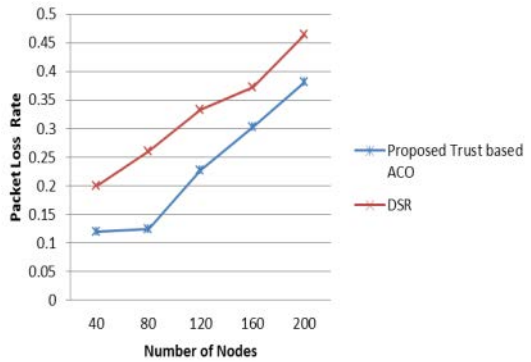

Fig. 9: Packet loss rate measured using trust based aco routing and DSR with 10% malicious nodes

nodes, packet loss ratio is decreased by more than 20%. By selecting nodes with higher trust and delivery capability, the proposed algorithm is able to dynamically adapt to the changing network conditions and decreases the packet drop. With decreased packet drop, the PDR improves and thereby improving overall QOS. When there

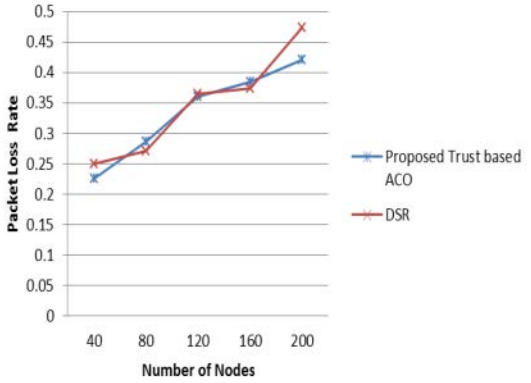

Fig. 10: Packet loss rate measured using trust based ACO routing and DSR with 20% malicious nodes

are 20% malicious modes in the network, the performance of the proposed method degrades as it could not find trusted nodes along the route from source to destination.

CONCLUSION

In MANET, open communication channel and mobility of nodes make it easy for intruder nodes to disrupt the functionality of the network. The proposed ACO based routing algorithm uses trust model to identify normal functioning nodes and faulty nodes. Ant colony optimization is used to optimize selection of best path with trusted nodes. Simulations are conducted with 80 nodes with 0, 10 and 20% malicious nodes in the network. The performance of the proposed ACO based algorithm is analyzed by measuring the following parameters:

- Packet delivery ratio
- End to end delay and
- Packet loss ratio

When the network has 10% malicious nodes, the proposed trust based ACO achieves an average of 20% more PDR when compared to conventional DSR protocol, whereas only a slight improvement of PDR is achieved by the proposed method with 20% malicious nodes. When there are 10% malicious nodes in the network, ants are able to identify more trustful nodes which leads to better PDR. But, with increased malicious nodes in the network, the option of finding routes with trusted nodes decreases and therefore, the decreased PDR. The proposed trust based ACO routing algorithm gives 20% increased delay when the number of nodes is >80. This delay is mainly due to checking trust values of all intermediate nodes in the selected path in order to find an optimal route. Further investigation shall be made to reduce end-to-end delay by

checking trust factor of intermediate nodes in the selected path during data transmission. Extending the proposed trust based ACO algorithm to other protocols such as AODV and GRP is an interesting open problem.

REFERENCES

Abolhasan, M., T. Wysocki and E. Dutkiewicz, 2004. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2: 1-22.

Aravindh, S., R.S. Vinoth and R. Vijayan, 2013. A trust based approach for detection and isolation of malicious nodes in MANET. Inter. J. Eng. Technol., 5: 193-199.

Chicco, G., 2011. Ant Colony System-Based Applications To Electrical Distribution System Optimization. INTECH Open Access Publisher, Rijeka, Croatia, ISBN: 9789533071572,.

Josang, A., 2001. A logic for uncertain probabilities. Int. J. Uncertainty Fuzziness Knowl. Based Syst., 9: 279-311.

Kadri, B., D. Moussaoui and M. Feham, 2013. A PKI over Ant colony based routing algorithms for MANETs-AntPKI. Int. J. Network Secur., 15: 42-49.

Kumar, M. and R. Mishra, 2012. An overview of MANET: History, challenges and applications. Indian J. Comput. Sci. Eng., 3: 121-125.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure ad hoc networks. Proceedings of the IEEE Conference on Aerospace, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

Manikandan, S.P. and R. Manimegalai, 2013. Trust based routing to mitigate black hole attack in MANET. Life Sci. J., 10: 490-498.

Priyadharshini, T. and A. Arunachalam, 2013. Efficient genetic algorithm for optimal routing in ad hoc networks. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 364-367.

Ramanathan, R. and J. Redi, 2002. A brief overview of Ad Hoc networks: Challenges and directions. IEEE Commun. Mag., 40: 20-22.

Rameshkumar, R. and A. Damodaram, 2010. ODASARA: A novel on demand ant based security alert routing algorithm for manet in grid environment. Int. J. Comput. Sci. Network Secur., 10: 154-161.

Salami, N.M.A., 2009. Ant colony optimization algorithm. Ubiquitous Commun. Comput. J., 4: 823-826.

Sebastin, E.J., 2013. Performance comparison of ACO algorithms for MANETs. Int. J. Adv. Res. Comput. Eng. Technol., 2: 27-32.

Wang, X., X.Z. Gao and S.J. Ovaska, 2007. A hybrid optimization algorithm based on ant colony and immune principles. Int. J. Comput. Sci. Appl., 4: 30-44.