Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/120322

Trusted and Optimized Routing in Mobile Ad-Hoc Networks Emphasizing Quality of Service

S. Sridhar [1], *V. Nagaraju* [2,*], *B. R. Tapas Bapu*[3], *R. Shankar* [1] and *R. Anitha* [1]

[1] Department of Computer Applications, S.A.Engneering College, Chennai, India
[2] Department of Electronics and Communication Enginrrting, Rajalakshmi Institute of Technology. Chennai, India
[3] Department of Electronics and Communication Engineering, S.A.Engneering College, Chennai, India

Received: 15 Feb. 2018, Revised: 25 Apr. 2018, Accepted: 28 Apr. 2018
Published online: 1 May 2018

Abstract: Mobile ad-hoc network (MANET) has got more focus because of its pragmatic applications and inevitability of communication in mobile devices. MANET is a wireless network, self-configuring and nodes communicate between them without any centralized supervision. Vibrant nature of MANET demands end to end quality of service. Nodes Trust is the most challenging apprehension in routing protocol for MANETs. The trust based routing is one way to form assistance among nodes for performing an competent routing. To optimize the routing mechanism a bio inspired metaheuristics technique, Ant colony optimization is used. It simulates ant behavior to solve complex combinatorial problems. ACO algorithms include the method of optimization, strengthening learning and also decentralized, robust and flexible. The proposed work Trust and ANT Based Routing (TABR) defines an Ant based routing algorithm incorporated with trust values to identify efficient, trusted and optimized routes in MANET. The work is implemented and simulated on NS-2. The proposed TABR is compared with traditional AODV, DSR and ANT based HOPNET routing protocols. The simulation results show the proposed TABR has increase in PDR and throughput and decrease in Delay, packet loss and Jitter compared with traditional AODV, DSR and ANT based HOPNET.

Keywords: ACO, MANET, QoS, TABR, Trust.

1 Introduction

A Mobile Adhoc Network [1] is a self-organizing dynamic network composed of mobile nodes. The absence of a fixed infrastructure increases the challenges to the research community for implementing an ad hoc network. Its characteristics are dynamic topology, bandwidth and variable link scope, self-configuring, multi-hop communications and limited security. Each node can move in an arbitrary manner and forwarding packet communication between each other to find or establish the communication route to the destination node. Due to the node mobility, MANET topology may change rapidly and unpredictably. QoS is usually defined as a set of services that should be sustained during packet transmission. A QoS enabled protocol is expected to sustain several metrics like Throughput, Hindrance (or Latency), Jitter, Packet delivery ratio etc. Therefore, when it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met [2]. Routing protocols in MANETs are generally classified as proactive and reactive [3]. Trust plays a vital role in MANET routing in providing reliable and efficient routing. The idea of using trust to mitigate security threats has been an important area of research [4]. The concept of Trust originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [5]. The trust based routing is one way to form cooperation among nodes for establishing an efficient routing between nodes. Continuous evaluation of nodes performance is used to calculate the trust of this node. Nodes are included for routing only if their trust values are meeting the threshold value. Swarm Intelligence involves systems that are classically made up of a population of simple agents communicating with one another within the current environment. The agents follow very simple rules during the progression of communication [6,7]. Ant Colony Optimization (ACO) is a meta-heuristic loom for solving optimization difficulties. The stirring source of ACO is

* Corresponding author e-mail: vankadarinagaraju@ritchennai.edu.in

the foraging behavior of real ants that consents to find shortest paths between food sources and the shell. Ants release a chemical substance (the pheromone) on the floor, and the way chosen by the following ants is the path marked by a stronger pheromone concentration. Ants on reaching the destination; start a new route backward towards the source shell by following the same path and biases the path by depositing more pheromone on the shortest path. As time progresses, the pheromone on non-optimal paths fade while the pheromone on near-optimal paths is resistant. The fundamental values pouring this system can be applied to many combinatorial optimization difficulties like routing in data networks [8]. The ACO algorithm has been productively used in the routing difficulty commonly by using two sets of synchronized mobile agents, called FANTs and BANTs [9]. Both types of agents have the same structure, but they can sense diverse inputs and produce diverse free outputs [10]. For the application of ACO to network routing, the quandary can be abridged to finding the shortest path between the nodes in a network as the resource and target nodes much like in conservative distance-vector or link state routing protocols [11]. Control information can be transmitted in the network easily along with the data packets when compared to traditional routing packets which could only carry Tables with them [12]. ACO based routing algorithms have ability to produce a good suboptimal path based on many recital parameters for QoS like link quality, congestion or other cost metrics [13]. A trusted and optimized routing protocol will be capable of meeting the challenges in MANET routing. Therefore, a trust and ACO based routing protocol (TABR) is proposed that performs well in the dynamic nature of MANET and also provides good quality of service.

2 Literature Survey

The Ant Colony Optimization (ACO) approach is used for the optimal selection of cluster heads. Proposed algorithm [14] optimizes communication workload, node lifetime, and mobility. The cluster structure is optimized by the defined probability function for clusters. The probability function is calculated by using the parameters such as residual energy, energy drain rate and mobility factor. Node that has the maximum value for the probability function will select as a cluster head. The overall communication workload is calculated periodically. If its value is high, then cluster head is reassigned. The advantage of this algorithm is that it can better balance the energy consumption of the nodes and increase the stability of the node. Experiment results show that our proposed work results in more energy efficient and stabilized clusters. A new trust mechanism to secure the AODV routing protocol called Trust AODV [15] is proposed where the performance of the proposed secure protocol is increased by using an ant algorithm. Ant agent put a positive pheromone when the node is trusted. Path communication is chosen based on pheromone value. Evaluation and comparison of the performance of proposed protocol is carried out before and after using ant algorithm under DOS/DDOS attack. The simulation result shows the performance of proposed protocol increases while using ant algorithm in term of PDR and throughput. However in terms of delay there is no significant effect to the performance. Trust and Reputation would serve as a major solution to problems existing in MANET. Learning the network characteristics and choosing right routing decisions at right times would be a significant solution. Thus a QoS constrained fault tolerant ant look ahead routing algorithm [16] is proposed which attempts to identify valid route and look-ahead route pairs which might help in choosing the alternate path in case of valid route failure. The results prove that the proposed algorithm takes better routing decisions with 20-30 percent improvement compared with existing ant colony algorithms. The authors propose an ant based multipath backbone routing [17] for load balancing in MANET. When the source wants to transmit data towards destination, it selects the multiple routes with maximum path preference probability using swarm based ant colony optimization technique. The path preference probability is estimated based on next hop availability, delay and bandwidth. During route discovery, the nodes subjected to faults are found and the relevant path is skipped. Then the network load on the routes is balanced by an index by each backbone node to distribute the data traffic equally on the links from source to destination. By simulation results, the authors show that proposed technique reduces the network load. Wireless ad hoc network makes available multiple paths for data transmission, but it is necessary to choose most efficient path and provide better Quality of Service (QoS). A new protocol QAMR [18] is introduced based on ant colony optimization algorithm which provides plausible path out of multiple paths for data transmission. This algorithm is scalable, adaptive and efficient and the performance is evaluated using network simulator which shows good improvement. A hybridization of the Ant Colony Optimization (ACO) and the Firefly, swarming algorithm (FA) for Ad-Hoc On Demand Distance Vectoring (AODV) routing protocol [19] is proposed to increase the efficiency in the transmission of the signals in a MANET system. This protocol is intended to substantially reduce the losses, so incurred using solely the AODV Routing Protocol and overcome drawbacks of ACO based AODV. Comparative studies on the proposed hybrid algorithm with the existing routing algorithms (AODV and ACO based AODV) are done thereby ensuring reduction of network load by avoiding re-discovery attempts between the nodes A Hybrid Ant Colony Optimization based routing algorithm [20] is proposed that generates routes dynamically, following the concept of equal load distribution in the network. The local search component of ACO is modified using Simulated Annealing to provide an effective and energy efficient node selection mechanism. Experiments show that the algorithm exhibits effective load distributions and also provides dynamic random paths.

3 Proposed Work

The biggest challenge in Mobile ad hoc network is routing due to the dynamic nature of nodes. In spite of this vibrant topology nodes communicate with each other and exchange data on the network. Ant colony optimization is used to optimize the routes selected for routing and along with trust which provides more efficient routing.. The various phases of proposed TABR and its algorithm are described in the following sections.

3.1 Phases of TABR

In the proposed TABR for MANETs, the network agents (ants) are only transmitted on demand and are flooded through the entire network in a similar process as AODV. The routing table entries stores pheromone concentrations, which are transformed into probabilities later on. TABR works in three phases which are discussed in the following section.

3.2 Phase 1: Route Discovery

In the first phase, Route Discovery Phase, new paths are discovered. The creation of new routes requires the use of a FANT which establishes the pheromone track to the source node, and a BANT, which establishes the track to the destination node. FANTs are broadcasted by the sender to all its neighbors. Each FANT has a unique sequence number to avoid duplicates. A node receiving a FANT for the first time creates a record (destination address, next hop, pheromone value, trust value) in its routing Table.

The node interprets the source address of the FANT as destination address, the address of the previous node as next hop, and computes the pheromone value depending on the number of hops the FANT needed to reach the node. Then the node relays the FANT to its neighbors. When the FANT reaches destination, it is processed in a special way. The destination node extracts the information and then destroys the FANT. A BANT is created and sent towards the source node. In that way, the path is established. Now the selection of optimal trusted path is based on pheromone value and trust value and for every transmission the same procedure is followed and routing tables is updated. The algorithm can be informally described as follows: When a source node s starts a communication session with destination d, first, it would search for this nodes routing table, see whether it has routing information for d available, if has, then would send packets according to highly pheromone probability, else, this node would save packets to buffer, and then launch routing path setup, broadcast Fant to its neighbors, F_{ant} would collect information about routing of networks. When F_{ant} arrives to destination, generates Bant which receives all the information from F_{ant} and then back to source node, in this process, hand overs all the information to the SERVagent, and then, SERVagent updates routing table of this node.

3.3 Phase 2: Route Maintenance

Once the F_{ant}s and Bants have established the pheromone tracks for the source and the destination node, subsequent data packets also increase the pheromone value. Data packets are used to maintain the path, so no overhead is introduced but still nodes have to be checked for updated trust values. Pheromone and trust values keep on changing. When a node relays a data packet toward destination to a neighbor node, it increases the pheromone value for that entry. The same happens in the opposite direction. The evaporation process is simulated by regular decreasing of the pheromone values.

3.4 Phase 3: Route Failure Handling

A route failure is recognized through a missing acknowledgement on the MAC layer and to deactivate that link by resetting the pheromone concentration to 0. Then, the routing table is checked for different links towards the destination and the packet gets relayed accordingly. If a message has to take a long path towards a target it lasts long until the sender is able to realize that the packet was lost. First, an attempt is made to send the packet over an alternate route; otherwise, it is returned to the previous hop expecting that there exists an alternate route in the network.

3.5 TABR - Implementation

The proposed work optimizes the trust based routing using ANT Colony Optimization where nodes are selected for routing based on proposed TABR (Trusted ACO Based Routing) algorithm. Routes are selected which have shortest path and nodes in the selected shortest path have good trust value to perform the routing efficiently. The pheromone value (PH) and trust value (TL), indicating estimated goodness of going from i over neighbor n to destination d are calculated. The ant agent chooses next hop n with the probability PB. The incremental pheromone value is calculated based on delay and hop and reflected in PH.

STEP 1: Each node maintains a routing table RT, each ant agent chooses a fair path based on the information from

RT. The RT shows the probability of choosing the next hop node to the destination. Suppose ant agent is in node i, the RT looks as,

PB N,i	PB N,i+1	PB N,i+2	PB N,D

Where D is the destination, PB is the probability and N is the neighbor node.

STEP 2: The pheromone value, indicating estimated goodness of going from i over neighbor n to destination d is calculated as;

$$PH_{n,d} = \frac{\left(PH^{i}_{n,d}\right)^{\alpha}}{\sum_{j\in N^{i}_{d}}\left(PH^{i}_{n,d}\right)^{\alpha}} \quad (1)$$

Where $\alpha \geq 1$ is the parameter value to control the exploratory behavior of ant agents.

STEP 3: The Trust value, indicating estimated faith of going from i over neighbor n to destination d is calculated as follows. The trust level value calculation is based on the parameters shown in the Table 1. The count field describes about two criteria, success rate (packets delivered successfully) and failure rate (packets lost or not delivered).

Table 1: Ant based trust parameters

Success rate	$qrs(F_{ant})$	$qps(B_{ant})$
Failure rate	$qrf(F_{ant})$	$qpf(B_{ant})$

$$QrFant_{n,d} = \frac{\left(qrs^{1}_{n,d} - qrf^{1}_{n,d}\right)}{\left(qrs^{1}_{n,d} - qrf^{1}_{n,d}\right)} \quad (2)$$

$$QrBant_{n,d} = \frac{\left(qrs^{1}_{n,d} - qrf^{1}_{n,d}\right)}{\left(qrs^{1}_{n,d} + qrf^{1}_{n,d}\right)} \quad (3)$$

$$TL^{1}_{n,d} = \left(QrFant^{1}_{n,d} - QPBant^{1}_{n,d}\right) \quad (4)$$

To select the next hop node the trust value of all neighboring nodes from current source node is calculated and finally a node which has highest value than the threshold is selected as next hop node for the current routing. The nodes which are not selected for the current transmission based on their trust value cannot be tagged as unfit node and can serve as best trusted node for another transmission based on the scenario.

STEP 4: Therefore, $TL_{n,d}$ is the Trust value and $PH_{n,d}$ is the pheromone value, indicating estimated faith and goodness of going from i over neighbor n to destination d respectively, the ant agent chooses next hop n with the probability $PB_{n,d}$.

$$PB_{n,d} = \frac{\left(PH^{i}_{n,d}\right)^{\alpha}}{\sum_{j\in N^{i}_{d}}\left(PH^{i}_{n,d}\right)^{\alpha}} + \frac{\left(TL^{i}_{n,d}\right)}{\sum_{j\in N^{i}_{d}}\left(TL^{i}_{n,d}\right)} \quad (5)$$

Where $\alpha \geq 1$ is the parameter value to control the exploratory behavior of ant agents, i.e set of neighboring nodes over which the path to destination is reached) and TL is the trust value calculated for each node.

STEP 5: If F_{ant} arrived an intermediate node where information is available in RT to reach destination it can choose next hop based on PB of RT. Else F_{ant} broadcasts, where an intermediate node or destination could receive several F_{ant} from same F_{ant} (duplicates), only number of hops and good travel time are received and others are discarded.

STEP 6: (a) F_{ant} will keep a stack ST of nodes information it has visited from source to destination.

$$ST = \left\{ \begin{matrix} \left(s, d_{s,j1}, 0, TLs\right), \left(j1, d_{j1,j2}, h1, TLj1\right), \cdots \\ \left(jk, d_{jkd}, hk, TLjK\right) \end{matrix} \right\} \quad (6)$$

Where $s, j1, j2, \cdots jk$ are nodes sequence number, $TLs, TLj1, \cdots TLjk$ are trust values of respective nodes $(s, j1, \cdots jk)$, is the delay from node $j1$ to its neighbor $j2$ and hk is the hop. 6(b) In the node, S_{agent} records time F_{ant} arrive and leave. If cycle detected, all the cycles nodes are popped from ant agents stack. F_{ant} would choose next hop from RT randomly in order to avoid getting cycle again.

STEP 7: When F_{ant} arrives destination it is converted to B_{ant} which has all information F_{ant} collected. B_{ant} travels back to source. In each intermediate node, B_{ant} reads delay that form this node i to $j1$ and hops hk, from this node to destination. Now it computes delay from this node i over neighbor $j1$ to destination.

$$d_{j1,d} = d_{i,j1} + d_{j1,j2} + d_{jk,d} \quad (7)$$

STEP 8: The delay calculated in Eq. (3.11) is given to S_{agent} to compute increase of information (Incremental Pheromone, IPH).

$$IPH_{j1}{}^{i} = \left[\frac{d_{j1}{}^{i} + hT_{hop}}{2}\right]^{\beta} * e^{-\gamma t} \quad (8)$$

Where IPH is the incremental pheromone value going from i to next hop j1 till destination d. Thop represents time to take one hop. $\beta \leq -1$ to adjust speed of pheromone increment. $e^{-\gamma t}$ available ratio of ant agent release, in the beginning, has the most available

pheromone, along with elapse of time, the valid information for release is less and less and t time and γ control parameter representing available pheromone.
STEP 9: Therefore Updated pheromone value is,

$$PH^{i}_{j1,d} = (1-dr) * PH^{i}_{j1,d} + IPH^{i}_{j1} \tag{9}$$

Where dr is the decay ratio , value ranges from 0 to1. Finally Eq. (9) is reflected in Eq. (4) to update RT.

4 Experimental Results

Optimization helps search packets or data packets to favorably move towards the destination by improving the pheromone concentration on the trusted paths. However, it reduces the pheromone concentration on the paths which are not on the way towards destination node. With optimization introduced this algorithm is assigned a new name as TABR, i.e., Trust and ANT Based Routing in MANETs. The simulation parameters used for TABR implementation are shown in Table 2. The simulation results obtained from the execution of TABR is compared with the simulation results obtained from the execution of AODV, DSR and an Ant based protocol HOPNET. The experiments results were obtained against different number of nodes and different pause time. The proposed TABR shows good improvement in Qos metrics. PDR and Throughput are higher, delay and packet loss are reduced compared with general AODV, DSR and HOPNET.

Table 2: General parameters used during simulation of TABR implementation

Parameter Name	Parameter Value
Simulation Start Time	0.5 / 10.0 / 15.0 /25.0
Simulation End Time	20 / 100 / 100 /180
Queue Type	Priqueue
Data Packet Type	FTP (Under TCP Class)
Packet size	5000
Number of Nodes	25, 50, 100
Simultaneously Opened Connections	Around 25 to 30 pairs of connections
Dimension of Topology	[1000x1000] [X x Y]
Node Speed	10 m/s to 30 m/s
Mobility Model	Random Way Point

Comparison of QoS metrics with respect to pause time:
A. Throughput

TABR is on middling 12% better than AODV, 20% better than DSR and 7%better than HOPNET in terms of middling throughput as shown in Fig 1. Since the likelihood of finding an efficient route for TABR is higher than that of AODV, DSR and HOPNET

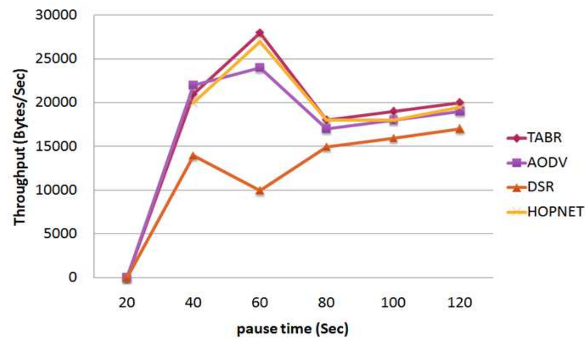

Fig. 1: Throughput for different pause time

B. Packet Delivery Ratio

As shown in Fig. 2, TABR outperforms HOPNET, AODV and DSR. Packet delivery ratio continues to decrease as the pause time goes up with certain fluctuations. The factors that donate to the triumph of TABR are, initiating the route discovery mechanism only when necessary, avoiding the use of stale routes. Routing path is established only with trustable nodes and optimized paths.

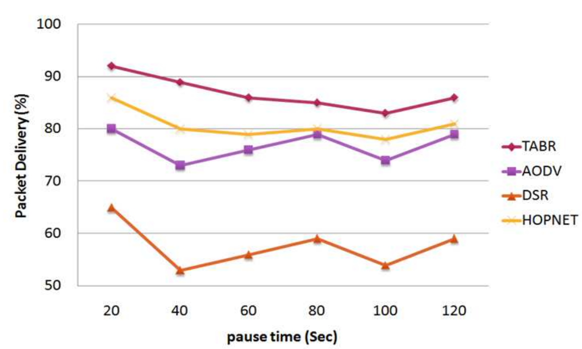

Fig. 2: Packet Delivery Ratio for different pause time

C. Packet Drop:

As a desirable property lesser number of packets should be dropped while communication. Fig. 3 indicates that TABR is better than AODV and DSR. Agents and trust criteria helps our proposed TABR to form a better route with trustable nodes in it there by reducing the packet drop by nodes. HOPNET completely avoids packet loss.

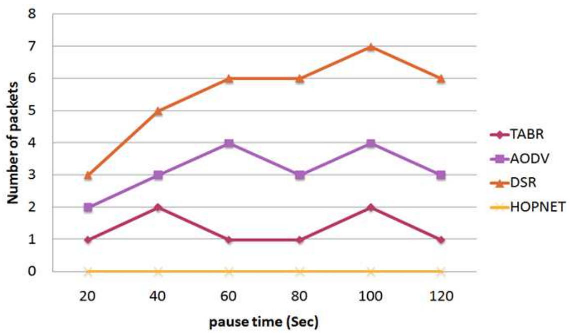

Fig. 3: Packet Drop for different pause time

D. Delay

TABR outperforms AODV and HOPNET in delay as shown in Fig 4. The middling delay for AODV and HOPNET is around 0.18 s and reduces when pause time increases. The key reason for this close delay time is the additional works (trust and ant agents) to be carried out by the proposed TABR.

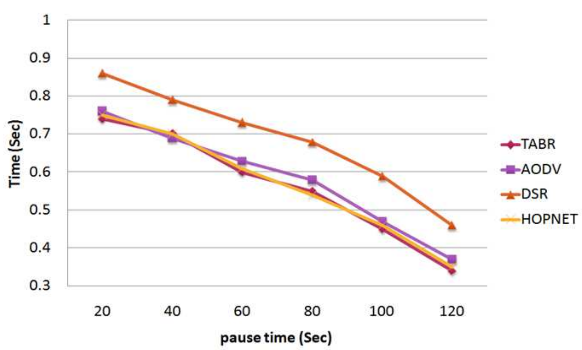

Fig. 4: Delay for different pause time

E. Jitter

Fig 5 clearly shows us that the jitter for TABR is less than AODV and DSR but close to HOPNET.

Comparison of QoS metrics with respect to node count.

A. Packet Delivery Ratio

From Fig 6 prooves packet delivery ratio for TABR is better than HOPNET, AODV and DSR, this is because when the link fails, we have some measures to handle it thereby, the drop packets are reduced and improve PDR.

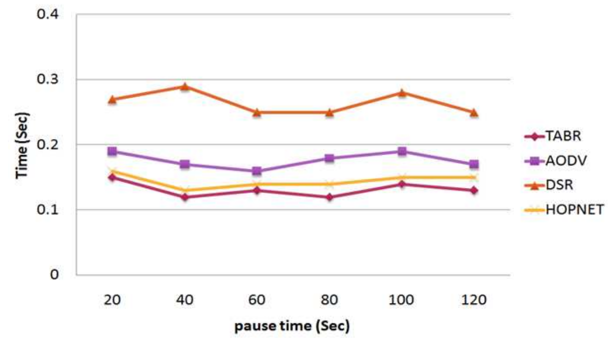

Fig. 5: Jitter for different pause time

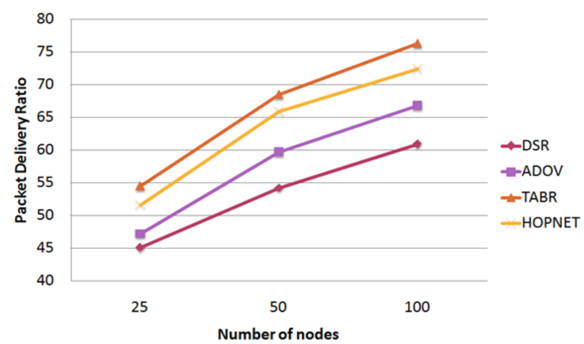

Fig. 6: PDR for different number of nodes

B. Throughput

From Fig. 7, it is proved that the throughput is high for TABR. But in certain conditions, AODV is slightly close to TABR and HOPNET, this is because we add service agents that influence the networks throughput of TABR.

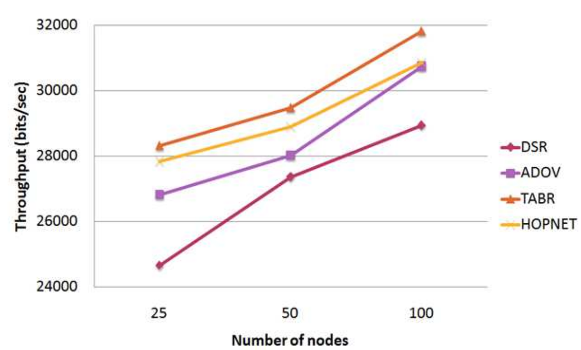

Fig. 7: Throughput for different number of nodes

C. Packet Drop:

As a desirable property lesser number of packets should be dropped while communication. Fig 8 indicates that TABR is better than AODV and DSR. Agents and trust criteria helps TABR to form better route with trustable nodes there by reducing the packet drop. HOPNET completely avoids packet loss.

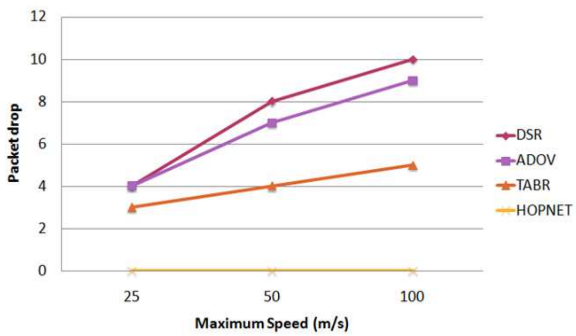

Fig. 8: Packet drop for different number of nodes

D. Delay

From Fig 9, we can see that the delay for TABR is very close to AODV and HOPNET but less than DSR. This is again caused because of the proposed works to be carried out for efficiency by the proposed TABR.

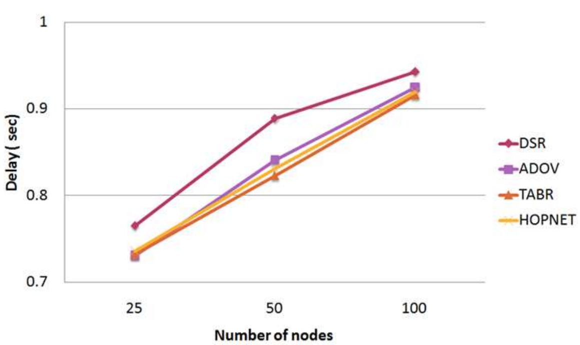

Fig. 9: Delay for different number of nodes

Figure 10 shows the simulation works that detects the untrusted nodes in the path and figure 11 depicts the selection of alternate path as per TABR algorithm.

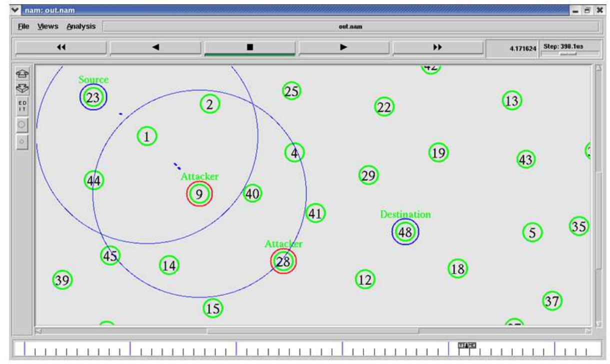

Fig. 10: Identification of untrusted node in the path

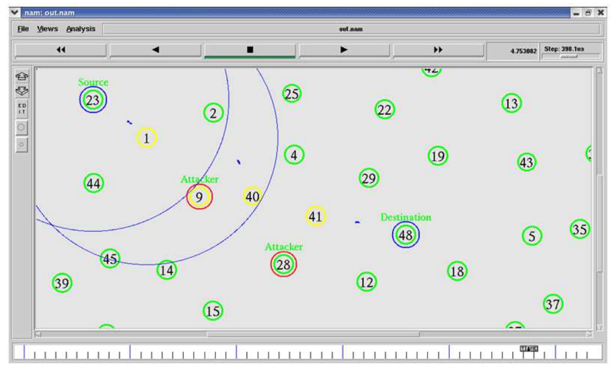

Fig. 11: Selection of alternate path as per TABR

5 Conclusion

The proposed TABR routing is optimized using ANT optimization based on trust. The proposed protocol has shown good improvement over the QoS parameter PDR & Throughput are increased and Delay & Packet loss are decreased. The packet delivery ratio is better in proposed TABR when weighed against AODV & DSR since we provide stable and efficient routes. Only less number of packets is dropped in TABR than AODV and DSR. The proposed scheme is better than the DSR and AODV with respect to Average End to End delay. However, AODV performs slightly closer to TABR just because of trust calculation and agents. The results obtained show that the proposed TABR has better performance as compared to AODV and DSR algorithms and the average jitter in TABR is better than all other approaches in its category. The proposed work can be enhanced by comparing the work with other Ant based protocols and also security mechanisms can be incorporated for more reliable transmission.

References

[1] G. Kortuem, J. Schneider, D. Preuitt, T.G.C. Thompson, S. F'ickas, Z. Segall. Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks, Proceedings of the First International Conference on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001).

[2] V. Alarcon-Aquino, J. M. Ramirez-Cortes, P. Gomez-Gil, O. Starostenko, Y. Garcia-Gonzalez, Network Intrusion Detection Using Self-Recurrent Wavelet Neural Network with Multidimensional Radial Wavelons in Information technology and control, Vol. 43, No.4, pp. 347-358(2014).

[3] Remondo, Tutorial on wireless ad hoc networks in the second international conference in Performance Modeling and Evaluation of heterogeneous networks, (2004).

[4] T. Beth, M. Borcherding and B. Klein, Valuation of trust in open networks, Proceedings of ESORICS (1994).

[5] K. S. Cook. Trust in Society, Russell Sage Foundation Series on Trust, New York, Vol. 2 (2003). **2**, (2003)

[6] S.L.Correia, Celistino Junior, O. Cherkaoui, Mobility-aware Ant Colony Optimization Routing for Vehicular Ad-hoc Networks, IEEE WCNC 2011 Network, pp. 1125-1130(2011).

[7] J. Jain, R. Gupta, T.K. Bandhopadhyay, Ant Colony Algorithm in MANET Local Link Repairing of AODV, Proceedings of third IEEE international conference on Electronics Computer Technology, pp. 270-273(2011).

[8] F. Dressler and O.B. Akan, A Survey on Bio-inspired Networking, International Journal of Computer Networks, Vol. 54, No. 6, pp. 881-900(2010).

[9] P. Deepalakshmi and S. Radhakrishnan, An Ant Colony Based Multi Objective Approach to Source-Initiated QoS Multicasting Method for Ad-hoc Networks, International Journal Advance Soft Computing Applications, Vol. 3, No. 2, pp. 1-18(2011).

[10] M. Lin, X. Yubin, M. Weixiao, An Ant Colony Based Congestion Elusion Routing Scheme for MANET, Proceedings of IEEE Globecom, (2011).

[11] R. Baskaran, P.V. Paul, P. Dhavachelvan, Ant Colony Optimization for Data Cache Technique in MANET, Proceedings of International Conference in Advances in Computing & Advances in Intelligent Systems and Computing, Springer India, Vol. 174, pp. 873-878(2013).

[12] S. Kaur, R.S. Sawhney, R. Vohra, MANET Link Performance Parameters using Ant Colony Optimization Approach, International Journal of Computer Applications, Vol. 47, No. 8, pp. 40-45(2012).

[13] B. Roy, S. Banik, P. Dey N. Chaki, S. Sanyal, Ant Colony Based Routing for Mobile Ad-hoc Networks Towards Improved Quality of Services, Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 1, pp. 10-14(2012).

[14] Jeena John and R. Pushpalakshmi, A reliable optimized clustering in MANET using Ant Colony algorithm, Proceedings of the International Conference on Communication and Signal Processing, pp. 051-055(2014).

[15] S. Vinod and M. Annu, Secure Checkpointing Approach on Ant Colony Optimization in MANET, International journal for research in applied science and Engineering technology Vol. 2, No. 7, pp.127-135(2014).

[16] S. Harris, A. Abdelhafid, S. Riri Fitri, L. Pascal, Performance analysis of optimized trust AODV using ant algorithm, Proceedings of the IEEE International Conference on Communications (ICC), pp. 1843-1848(2014).

[17] S. Surendran and S. Prakash, An ACO look-ahead approach to QOS enabled fault- tolerant routing in MANETs, China Communications, Vol. 12, No.8, pp. 93-110(2015).

[18] F. Pitchaimuthu, A. Selvi, M. Seetharamaiyer, Ant based multipath backbone routing for load balancing in MANET, IET Communications, Vol. 11, No. 1, pp. 136-141(2017)

[19] M. Rajanigandha and A. Sujata, Ant colony optimization algorithm based an intelligent protocol to improve QoS of MANETs, Proceedings of the International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp. 121-125(2014)

[20] N. Subhrapratim, B. Samriddha, S. Amab, K. Subir, Optimizing MANET routing in AODV: An hybridization approach of ACO and firefly algorithm, Proceedings of the Second International Conference on Research in Computational Intelligence and Communication Networks, pp. 122-127(2016).

S. Sridhar received UG degree, B.Sc. Computer Science from the University of Madras, Chennai, India, in 1998, PG degree, Master of Computer Applications (MCA) from University of Madras, Chennai, India, in 2001 and another PG degree Master of Philosophy (M.Phil.) in Computer Science from Periyar University, Salem, Tamil Nadu, India, in 2007. Received Ph.D in Computer Science at Bharathiar University, Coimbatore, Tamil Nadu, India in 2017. Since July 2001 he has been working with Department of Computer Applications (MCA), S.A.Engineering College, Chennai, India and currently Heading the department. He has got more than 18 international publications. His Research interests include Mobile Adhoc networks, Wireless sensor networks and WBAN. He is an Editorial member of 7 International Journals, Reviewer in 13 International journals and has reviewed 54 technical papers for conferences and journals.

V. Nagaraju has completed his Ph.D in Electronics and Communication Engineering department St. Peters University Chennai -54. He is currently working as Professor, in the department of Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Chennai. His area of research is Wireless Sensor Networks. He is also interested in Electronics circuits, microprocessor and Microcontroller, Analog and Digital Communication, Linear Integrated Circuits and control systems.

B. R. Tapas Bapu has completed his Ph.D in Electronics and Communication Engineering department St. Peters University Chennai -54.He is currently working as Professor, Faculty of Electronics and Communication Engineering, S.A.Engineering College, Chennai -77. His area of research is Wireless Sensor Networks. He is also interested in Digital Electronics, Microprocessor and Microcontroller, Analog and Digital Communication, Linear Integrated Circuits and Control Systems.

R. Sankar received UG degree, B.Sc., Mathematics from the University of Madras, Chennai, India, in 2007 and PG degree, Master of Computer Applications (MCA) from Anna University, Chennai, India in 2010. He has been working with Department of Computer Applications (MCA) in S.A. Engineering College, Chennai since 2011. Has got 3 international publications and his research interest includes Wireless Sensor Networks, Mobile Adhoc Networks and WBAN.

R. Anitha , received UG degree B.Com. in 2000 and PG degree Master of Computer Applications in 2003 from the University of Madras, Chennai, India. Completed Master of Philosophy (M.Phil) in Computer Science from Vinakya Mission, Chennai, India in 2009 and Master of Technology (M.Tech) in Computer Science from SRM University, Chennai, India, in 2013 and pursuing Ph.D in Anna University Chennai. She has been working with Department of Computer Applications (MCA) in S.A. Engineering College, Chennai, India since 2006. Has got 6 international publications and her research interest includes Wireless Sensor Networks, Mobile Adhoc Networks, WBAN and Data analytics.