Fuzzy-Based Trusted Ant Routing (FTAR) Protocol in Mobile Ad Hoc Networks

Srinivas Sethi[1] and Siba K. Udgata[2]

[1] Department of CSE,
IGIT, Saranag, Orissa
srinivas_sethi@igitsarang.ac.in
[2] Department of Computer & Information Sciences,
University of Hyderabad, Hyderabad, 500046
udgatacs@uohyd.ernet.in

Abstract. This paper proposes a novel approach called Fuzzy-based Trusted Ant Routing (FTAR) using fuzzy logic and swarm intelligence to select optimal path by considering optimization of multiple objectives. It retains the advantages of swarm intelligence algorithm and ensures trusted routing protocol by implementing fuzzy logic. It uses trust-evaluation scheme using dropped packet and Time-Ratio parameters which calculate trust values for nodes in MANETs to distinguish between healthy and malicious nodes. FTAR considers not only shortest path but also the trusted level of neighbors or intermediate nodes.

Keywords: MANET, Routing Protocol, Fuzzy, Antnet.

1 Introduction

A mobile ad hoc network (MANET) is becoming popular day to day due to its easy deployability, low cost infrastructure special purpose applications etc.. It is a self-organized network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Since, nodes in MANET can move in an arbitrarily manner, the network topology may change rapidly and unpredictably.

Each node acts as a router and takes part in discovery and maintenance of routes to other nodes in the network. So router has different activities at the same time. To support robust and efficient operations in mobile wireless networks, routing functionality is included in mobile nodes along with tests for trusted nodes as well.

The proposed protocols can be grouped into three different categories: table-driven/ pro-active, on-demand/ reactive, and hybrid [1]. However, due to security vulnerabilities of the routing protocols, mobile ad-hoc network is unprotected to attacks by the malicious nodes. So, it has to address new kinds of security issues which require new evaluation schemes to protect the network from different attacks of malicious nodes. The different attacks are blackhole attack [2], grayhole attack [3], Selective Existence attack [4], etc.

C. Sombattheera et al. (Eds.): MIWAI 2011, LNAI 7080, pp. 112–123, 2011.

In blackhole attack, malicious nodes never send true control messages. To carry out a blackhole attack, when the malicious node receives a route request (RREQ) message, without checking its routing table, immediately sends a false route reply (RREP) message assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. So, requesting nodes assume that route discovery process is successfully completed and ignore other RREP messages and begin to send packets over malicious node. In this way malicious node attacks all RREQ messages and packets are dropped without forwarding anywhere. Blackhole attack affects the whole network if it is in central place of network.

In the grayhole attack of malicious node initially forward the packets and then fails to do so. Initially the node replays true RREP messages to nodes that initiate RREQ message and it takes over the sending packets. Afterwards, the node just drops the packets to launch a denial of service. This is known as routing misbehavior.

The node is not participating in the network operations but, use the network for its advantage to enhance performance and save its own resources such as power. These types of selfish node behaviors are known as selective existence attacks [3]. It does not send any HELLO messages and drop all packets. In this paper, we introduce a trust-evaluation scheme which calculates trust values for nodes in MANET to successfully distinguish between healthy and malicious nodes.

The rest of the paper is organized as; section 2 discusses related works. Section 3 describes the method for detection of trusted node using fuzzy logic. New proposed routing protocol is described in section 4. Simulation environment is discussed in section 5 followed by performance evaluation parameters in section 6. Section 7 discusses results of routing protocol followed by conclusions in section 8.

2 Related Works

The basic idea of the ant colony optimization (ACO) [5] meta-heuristic is taken from the food searching behavior of real ants. It often gives better results for hard combinatorial optimization problems. The study of ant's behavior exhibits the capability of finding the shortest path from the ant's nest to the food source. In AntNet[6][7], ants explore the network building paths from source to destination nodes using a stochastic policy dependent on the past and current network states and collect on-line information on the network status. The disadvantage of AntNet is that it is intrinsically slow.

AntHocNet [8], a meta-heuristic ant based routing protocol for routing in mobile ad hoc networks, which has been designed after the Ant Colony Optimization (ACO) framework and its general architecture shares strong similarities with the architectures of typical ACO implementations for network routing. It is a hybrid protocol consists of both reactive and proactive components.

ANT-E [9] is a novel meta-heuristic on-demand routing protocol using the Blocking Expanding Ring Search (Blocking-ERS) to control the overhead and local retransmission to improve the reliability in term of packet delivery ratio (PDR).

Ant-Colony-Based Routing Protocol (ARA) [10], has been described as on-demand routing protocols for MANET. In [11] the authors correlate different route selection parameters that affect the network performance is captured by fuzzy ant technology and the results show that fuzzy ant colony based routing protocol is very promising to take care of various uncertainties of MANET effectively. In [12], authors have presented a self-healing technique based on Fuzzy concepts for mobile Ad hoc networks. The basic idea is to modify the entries of the neighbor table and the time-stamp of the entry each based on the fuzzy system. The performance of Dynamic Source Routing (DSR) is improved by adding a congestion level of each mobile node, together with number of hops, as a mixed metric that will be considered during route selection decision in source node using fuzzy logic [13].

The authors investigate the development of protocols which are resilient to Byzantine Attacks in [14] and presented a Byzantine Secure Link State routing protocol for wired environments. In [15], the On-Demand Secure Byzantine Routing (ODSBR) routing protocol was proposed for MANETs. The ODSBR is secure against known outsider attacks due to presence of cryptographic mechanisms. In [3], [16] proposed several passive methods to monitor the behavior of neighboring nodes in order to determine whether they are acting in a faulty manner. In these works, if the neighbor is deemed to be misbehaving, the monitoring node suggests or carries out a path reroute around the faulty neighboring node.

3 A Fuzzy-Based Trusted Node

3.1 Fuzzy Logic

Fuzzy logic is used to approximate functions and can be used to model any continuous function or system. The advantages of fuzzy logic are easy to understand, flexible, tolerant of imprecise data and can model nonlinear functions of arbitrary complexity. The fuzzy logic has been used to solve several routing protocols and handover problems efficiently in wireless networks [18] [19].

3.2 Design of Fuzzy Interface System

Fuzzy inference is the process of formulating the mapping from a given input to an output using fuzzy logic and the mapping provides a basis from which decisions can be made, or patterns recognized. The process of fuzzy inference involves all of the pieces: membership functions, if-then rules etc.

In this paper, neighbor nodes are evaluated for their Trustfulness using a fuzzy logic approach and compare its performance with that of the Ant-U. The inputs to the fuzzy controller for routing are: (i) Time-ratio and (ii) Dropped packet. These two selection parameters make the node's ability to trust deliver network packets. Fig.-1 shows the generalized block diagram of fuzzy system for trusted node.

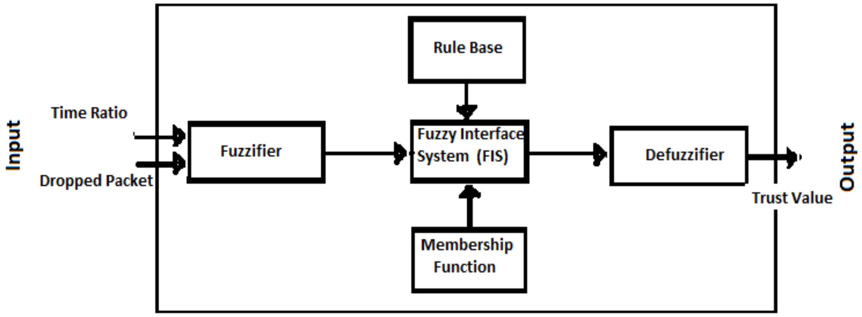


Fig. 1. Generalized Block Diagram of fuzzy system for trusted node

The basic functions of the different components of fuzzy interface system design in the scheme are described as follows.

3.2.1 Fuzzification

The fuzzifier performs the fuzzification process that converts two types of input data and one output which are needed in the inference system. The input to the fuzzifier 'time-ratio' is the ratio between route reply time and time-to-live whereas, dropped packets is numbers of packet dropped at the node. These two parameters are used to measure the trusted node where trusted value of node is output.

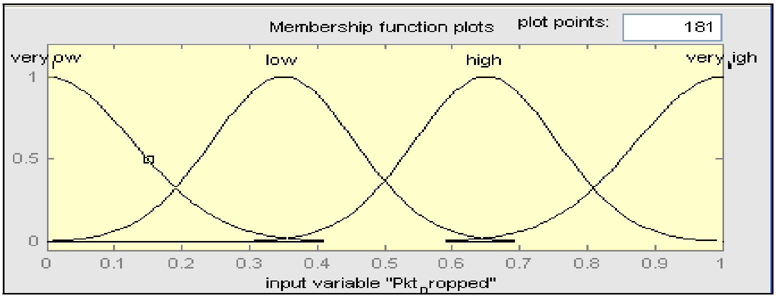


Fig. 2. Dropped Packets fuzzy set

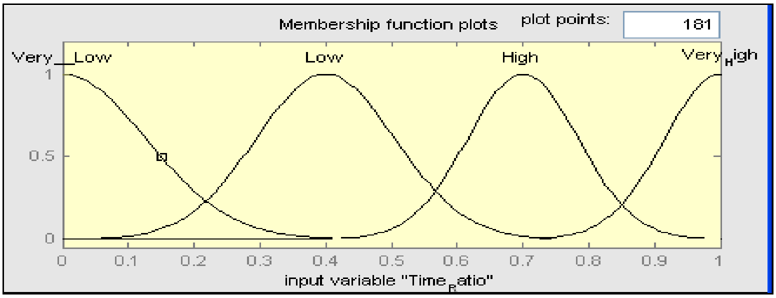


Fig. 3. Time-Ratio fuzzy set

Fuzzification of inputs: It obtains inputs and determines the degree to which they belong to each of the appropriate fuzzy sets via membership functions. It may be a table lookup or a function evaluation. Trusty node performs the node evaluation process in order to determine the trustworthiness of a neighbor node after establishing the route. The trust-value of a node evaluated through two inputs. They are dropped packet and Time-ratio, which get fuzzified in order to give a step-less indication as Fig-2 and Fig-3 respectively.

Fuzzification of outputs: After creating fuzzy sets from all inputs, output fuzzy sets are evaluated by rule evaluation where, the rule evaluation consists of "if-then"-statements that give evidence of how to proceed with a node with certain fuzzy-sets. The fuzzy sets as in Fig.-4, are used to appraise each constraint as being Very Low, Low, Medium, High or Very High, assigning each a value between {0,1}. These evaluations are passed to a fuzzy inference system that applies a set of fuzzy rules that determines the node is trusted or not.

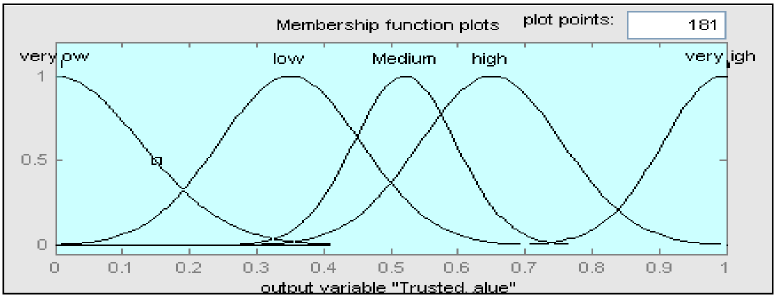
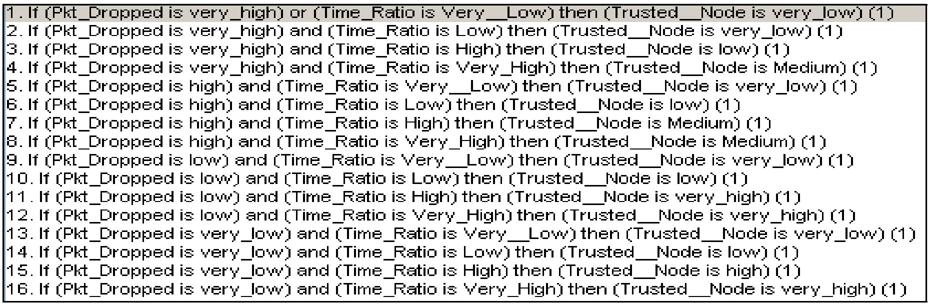


Fig. 4. Trust value of node

3.2.2 Inference System with Rule Base and Membership Function

Fuzzy Inference System is the system that simulates human decision-making based on the fuzzy control rules and the related input linguistic parameters. The low-high inference method is used to associate the outputs of the inferential rules [20][21]. The



```
1. If (Pkt_Dropped is very_high) or (Time_Ratio is Very__Low) then (Trusted__Node is very_low) (1)
2. If (Pkt_Dropped is very_high) and (Time_Ratio is Low) then (Trusted__Node is very_low) (1)
3. If (Pkt_Dropped is very_high) and (Time_Ratio is High) then (Trusted__Node is low) (1)
4. If (Pkt_Dropped is very_high) and (Time_Ratio is Very_High) then (Trusted__Node is Medium) (1)
5. If (Pkt_Dropped is high) and (Time_Ratio is Very__Low) then (Trusted__Node is very_low) (1)
6. If (Pkt_Dropped is high) and (Time_Ratio is Low) then (Trusted__Node is low) (1)
7. If (Pkt_Dropped is high) and (Time_Ratio is High) then (Trusted__Node is Medium) (1)
8. If (Pkt_Dropped is high) and (Time_Ratio is Very_High) then (Trusted__Node is Medium) (1)
9. If (Pkt_Dropped is low) and (Time_Ratio is Very__Low) then (Trusted__Node is very_low) (1)
10. If (Pkt_Dropped is low) and (Time_Ratio is Low) then (Trusted__Node is low) (1)
11. If (Pkt_Dropped is low) and (Time_Ratio is High) then (Trusted__Node is very_high) (1)
12. If (Pkt_Dropped is low) and (Time_Ratio is Very_High) then (Trusted__Node is very_high) (1)
13. If (Pkt_Dropped is very_low) and (Time_Ratio is Very__Low) then (Trusted__Node is very_low) (1)
14. If (Pkt_Dropped is very_low) and (Time_Ratio is Low) then (Trusted__Node is low) (1)
15. If (Pkt_Dropped is very_low) and (Time_Ratio is High) then (Trusted__Node is high) (1)
16. If (Pkt_Dropped is very_low) and (Time_Ratio is Very_High) then (Trusted__Node is very_high) (1)
```

Fig. 5. Fuzzy control rules for Trusted value of node

rule base is composed of a set of linguistic control rules and the accompanying control goals. Using the rule-based structure of fuzzy logic, a series of IF-THEN rules are defined for the output response given the input conditions. There are sixteen (4x4) possible logical-product output response conclusions, as shown in Fig.-5.

3.2.3 Defuzzification

The Defuzzification is the process of conversion of fuzzy output set into a single number and the method used for the defuzzification is smallest of minimum (SOM). The input for the defuzzification process is a fuzzy set. The aggregate of a fuzzy set includes a range of output values, and be defuzzified in order to resolve a single output value from the fuzzy set. Defuzzifier adopts the aggregated linguistic values from the inferred fuzzy control action and generates a non-fuzzy control output, which represents the trusted node adapted to node conditions. The defuzzification method is employed to compute the membership function for the aggregated output [20][21].

4 Description of Proposed Protocol

In this section, we discuss the adaptation of the fuzzy based trusted node for ant colony optimization meta-heuristic in MANET and describe the Fuzzy-based Trusted ant Routing (FTAR) protocol.

Data packets and control packets are two different types of packets used in the network. Forward ant (FANT) and a backward ant (BANT) are two classes of control packets used to update the routing tables and distribute information about the traffic load in the network. Apart from the control packets, the neighbor control packets are used to maintain a list of available nodes to which packets can be forwarded. The data packet represents the information which is exchanged among end-users. In ant-routing, data packets use the information stored at routing tables for moving from the source to the destination node. The HELLO messages are broadcasted periodically from each node to all its neighbors to check if the ant has arrived or not, as the destination address will change at every visited node. Birth time of an ant is the time when the ant has been generated and arrival time at the final destination is used to calculate the trip time.

FANT and BANT are used to discover the route in route discovery phase. A FANT is an agent which establishes the pheromone track to the source node and it gathers information about the state of network. Similarly, a BANT establishes the pheromone track to the destination node and use the collected information to adapt the routing tables on their path. The FANT is a small packet with a unique sequence number and the sequence number is used to distinguish duplicate packets. It creates a set of routing agents called FANT to search for the destination host. The source node would initiate a route discovery mechanism when a path to destination needs to be established and disseminate FANT to all its one-hop neighbors. While the destination is still not found, the neighbor would keep forwarding the FANTs to their own neighbors and so on. This process continues until a route to the destination is found using Blocking-ERS [22]; otherwise it sends a reply message to the source node. To prevent cycles, each node stores recently forwarded route request in a buffer.

The node interprets the source address of the FANT as destination address of BANT. The address of the previous node as the next hop and computes the pheromone value depending on the number of hops the FANT needs to reach the node. The node then relays the FANT to its neighbors. When the FANT reaches the destination node, the destination node extracts the information of the FANT and destroys it. Afterward, it creates a BANT and sends it to the source node. If any malicious node is available in the network, the above process may be deviated by black hole attack or gray hole attack or selective attack. To avoid this problem, we propose to check the fuzzy trust value of node in the network. The trusted neighbor nodes will be selected and the ant will be forwarded to it.ïWhen the sender receives the BANT from the proper destination node, the path is established from source and destination and data packets can be sent.

Once the FANT and BANT have established the pheromone tracks for the source and destination nodes, subsequent data packets are used to maintain the path and strengthen the path during the communication. When a node relays a data packet towards the destination node, it increases the pheromone value of the entry, to strengthen the route to the destinations by the data packets as per following equation.

$$P_{new} = P_{id} + \Phi P_{id} \tag{1}$$

Where, P_{new} is the new updated value, by P_{id} which is the previous pheromone value before reinforcement and Φ is a scaling factor.

All pheromone values in the routing table decreases over time. It shows the utilization rate of a route in the network. When the pheromone entry reaches a minimum threshold, it is considered a stale route and will be discarded from the routing table. The evaporation function is defined as:

$$P_{new} = P_{id} - \delta P_{id} \tag{2}$$

Where, δ is the evaporation scaling factor. This helps the ant to find out the maximum probability of an ant to choose the path at time $t+1$.

FTAR recognizes a route failure through a missing acknowledgment within predefined time-to-live and a node gets a route error (RERR) message for a certain link, it deactivates this link by setting the pheromone value to 0. Then the node searches for an alternative link in its routing table and it sends the packet via this alternate path, if there exist one; otherwise the node informs its neighbors, to relay the packet. If the packet does not reach the destination, the source has to initiate a new route discovery phase. By using trusted value of the node in the network the proposed routing protocol FTAR is more secure or trust than Ant routing with unsafe or malicious nodes.

5 Simulation

We implemented these protocols in the discrete time network simulator (NS-2)[23], which offers high fidelity in wireless ad hoc network. NS-2 is used under Linux platform to evaluate the performance of proposed routing protocol. Simulations have been carried out using the parameters given table-1 for different mobility rate, area size and number of nodes. Random waypoint mobility model is used for modeling the mobility of nodes.

Table 1. Parameter values of FTAR and Ant-U for simulation

S. No	Parameters	Values
1	Area size	700x700 m.
2	Transmission range	250 m.
3	Number of Nodes	50, 100, 150, 200 Nos.
4	Simulation time	900 s.
5	Nodes Mobility	1,5,10,15,20 m/s.
6	Pause times	10 s.
7	Data rate	1 Kbps.
8	No. Of experiments	5 times.

6 Performance Evaluation Parameters

The standard performance metrics like packet delivery ratio (PDR), overhead and delay are used for evaluating the performance of routing protocols are chosen.

The packet delivery ratio in this simulation is defined as the percentage of the ratio between the number of packets sent by constant bit rate sources and the number of received packets by sink/ destination. This performance evaluation parameter measures the delivery reliability, effectiveness and efficiency of the routing protocol.

$$PDR = \frac{\sum P_d}{\sum P_s} * 100 \tag{3}$$

where, P_d =Number of packets sent at destinations,

and P_s = number of received packets at sources.

Average End-to-end Delay is used to measure as the time elapsed from the time when a data packet is originated from a source and it is successfully received by receiver. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queuing transmission delays at MAC, and propagation and transfer times of data packets. This is the average overall delay for a packet to traverse from a source node to a destination node. So,

$$Avg.End - to - end - Delay = \frac{\sum e}{P} \tag{4}$$

where, $e = T_d - T_s$,

T_d =Time when packet received at destination,

T_s =Time when packet created by source,

and P =Total Generated Packet.

Overhead is the total number of routing packets transmitted during simulation. It is important to compare the adoption to low-bandwidth environments and its efficiency in relation to node battery power (in that sending more routing packets consumes more power). Sending more routing packets also increases the probability of packet collision and can delay data packets in the queues.

7 Result and Discussion

In this paper, trusted value of the node is calculated by using fuzzy logic to make the protocol more secure. At the same time it also improves the PDR which denotes the efficiency, reliability and effectiveness of proposed routing protocol. It also reduces the total routing overhead by checking the malicious node in the network. It is able to control the overhead by detecting blackhole attack, grayhole attack and selective existence attack of malicious or unsafe node in the network.

Fig.-6 shows, the PDR of FTAR is more than other Ant-U with malicious or unsafe node in respect all mobility rate. Similarly from Fig.-7, it is observed that PDR of FTAR is more than Ant-U with any unsafe node in the network in respect to numbers of node. It shows improved reliability, effectiveness and efficiency of FTAR in comparison to Ant-U.

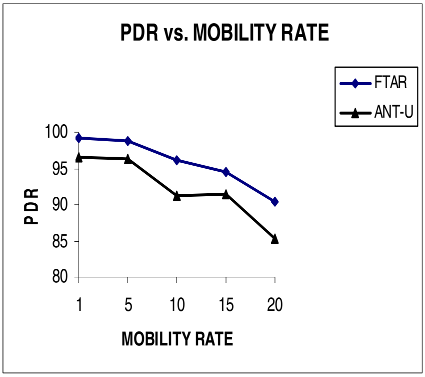


Fig. 6. PDR vs. Mobility Rate at 50 nodes

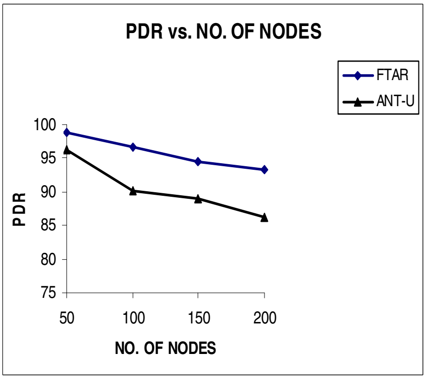


Fig. 7. PDR vs. No. of Nodes at 5 m/s

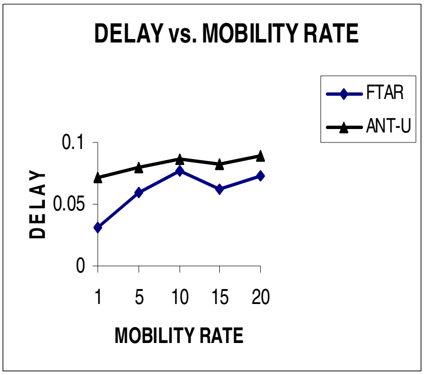


Fig. 8. Delay vs. Mobility Rate at 50 nodes

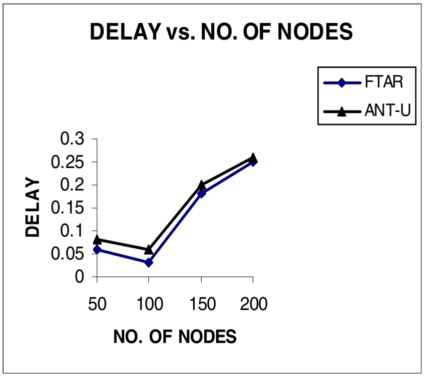


Fig. 9. Delay vs. No. of Nodes at 5 m/s

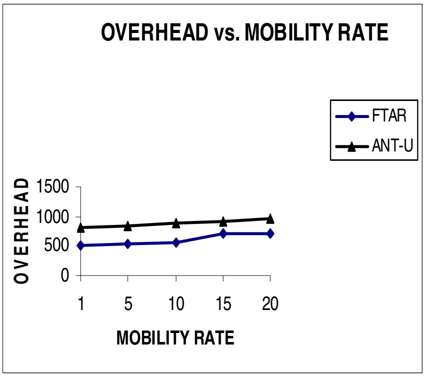


Fig. 10. Overhead vs. Mobility Rate at 50 nodes

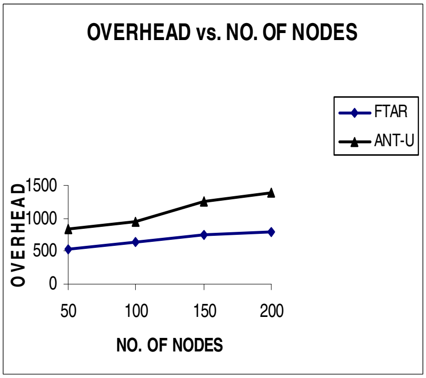


Fig. 11. Overhead vs. No. of Nodes at 5 m/s

In real time application, end-to-end delay is one of the important parameter to measure performance of routing protocol. Now, from Fig.8; it can be concluded that, end-to-end delay for FTAR is less than Ant-U for all mobility rates. Similarly end-to-end delay for FTAR is less than Ant-U for various node sizes as Fig.-9.

The overhead of FTAR is controlled by avoiding blackhole attack, gray hole attack and selective existence attack of malicious or unsafe node in the network. From Fig.-10, it is observed that the total overhead of proposed routing FTAR protocol is better than Ant-U for different mobility rates. Fig.11, show the total overhead of proposed routing FTAR protocol is better than Ant-U for various node sizes.

From the above results, it is observed that, the performance of FTAR is better than Ant-U for all possible combination of mobility rates and node sizes. This shows that the proposed routing protocol FTAR outperforms ANT-U.

8 Conclusions

In this paper, we proposed a Trust-node approach in the MANET based on Fuzzy concepts. The basic idea in this proposed work is to modify the entries of the dropped packets and the time-stamp of each entry based on the fuzzy system. This proposed approach shows an improvement over the Ant-U (with unsafe or malicious node). It avoids different attacks, which try to produce more routing overhead leading to blocking of the network and unnecessary increasing traffic. As trusted nodes are establishing the path from source to destination, it improves the PDR and decrease end-to-end delay and routing overhead. Since trust value of nodes is considered, the proposed routing protocol is highly reliable in real time environments.

References

1. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: A Review of Routing Protocol for Mobile Ad hoc Networks. Elsevier Ad Hoc Nwtworks Journal 2(1), 1–22 (2004)
2. Deng, H., Li, W., Agrawal, D.: Routing Security in Wireless Ad Hoc Networks. IEEE Communication Magazine, 70–75 (October 2002)
3. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Mobile Computing and Networking (MobiCom 2000), pp. 255–265 (2000)
4. Vigna, G., Gwalani, S., Srinivasan, K.: An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks. In: Proc. of the 20th Annual Computer Security Applications Conference (ACSAC 2004) (2004)
5. Dorigo, M., Gambardella, L.M.: Ant colony system: a cooperative learning approach to the traveling salesman problem. IEEE Transactions on Evolutionary Computation 1(1), 53–66 (1997)
6. Di Caro, G.A., Dorigo, M.: Ant Colonies for Adaptive Routing in Packet-Switched Communications Networks. In: Eiben, A.E., Bäck, T., Schoenauer, M., Schwefel, H.-P. (eds.) PPSN 1998. LNCS, vol. 1498, pp. 673–682. Springer, Heidelberg (1998)
7. Dhillon, S.S., Van Mieghem, P.: Performance Analysis of the AntNet Algorithm. International Journal of Computer Networks, 2104–2125 (2007)
8. Di Caro, G.A., Ducatelle, F., Gambardella, L.M.: AntHocNet: An Ant-Based Hybrid Routing Algorithm for Mobile Ad Hoc Networks. In: Yao, X., Burke, E.K., Lozano, J.A., Smith, J., Merelo-Guervós, J.J., Bullinaria, J.A., Rowe, J.E., Tiňo, P., Kabán, A., Schwefel, H.-P. (eds.) PPSN 2004. LNCS, vol. 3242, pp. 461–470. Springer, Heidelberg (2004)
9. Sethi, S., Udgata, S.K.: The Efficient Ant Routing Protocol for MANET. International Journal on Computer Science and Engineering (IJCSE) 02(07), 2414–2420 (2010)
10. Güneş, M., Sorges, U., Bouazizi, I.: ARA - The Ant-Colony Based Routing Protocol for MANETs. In: International Conference on Parallel Processing Workshops, pp. 1530–2016 (2002)
11. Goswami, M.M., Dharaskar, R.V., Thakare, V.M.: Fuzzy Ant Colony Based Routing Protocol For Mobile Ad Hoc Network. In: International Conference on Computer Engineering and Technology, ICCET 2009, pp. 438–448 (2009)
12. Venkatesh, C., Yadaiah, N., Natarajan, A.M.: Dynamic Source Routing Protocol using Fuzzy Logic Concepts for Ad hoc Network. Accademic Open Internet Journal 15, 1–15 (2005)

13. Wagyana, A., Hendrawan, Rachmana, N.: Performance Improvement of Dynamic Source Routing on Manet using Fuzzy Logic. In: Proceedings of MoMM 2006, pp. 251–258 (2006)
14. Avramopoulos, I., Kobayashi, H., Wang, R., Krishnamurthy, A.: Highly Secure and Efficient Routing. In: INFOCOM 2004 (2004)
15. Awerbuch, B.R., Holmer, D., Nita-Rotaru, C., Rubens, H.: An on-demand secure routing protocol resilient to byzantine failures. In: ACM Workshop on Wireless Security, WiSe (2002)
16. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: A secure on-demand routing protocol for ad hoc networks. In: Hu, Y.-C., Perrig, A. (eds.) Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking, MobiCom 2002 (2002)
17. Belding-Royer, E.M., Parkins, C.E.: Evolution and future directions of the ad hoc on-demand distance vector routing protocol. Ad Hoc Network (Elsevier) 1(1), 125–150 (2003)
18. Wong, Y.F., Wong, W.C.: A fuzzy-decision-based routing protocol for mobile ad hoc networks. In: 10th IEEE International Conference on Network, pp. 317–322 (2002)
19. Raju, G.V.S., Hernandez, G., Zou, Q.: Quality of service routing in ad hoc networks. In: IEEE Wireless Communications and Networking Conference, vol. 1, pp. 263–265 (2000)
20. Pedrycz, W., Gomide, F.: An introduction to fuzzy sets: analysis and design (complex adaptive systems). MIT Press, Cambridge (1998)
21. Buckley, J.J., Eslami, E., Esfandiar, E.: An introduction to fuzzy logic and fuzzy sets (advances in soft computing). Physica Verlag (2002)
22. Park, I., Kim, J., London, I.P.: Blocking Expanding Ring Search Algorithm for Efficient energy Consumption in Mobile Ad Hoc Networks. In: Proceedings of the WONS, Les Menuires, France, pp. 185–190 (2006)
23. NS-2 Manual (2009), `http://www.isi.edu/nsnam/ns/nsdocumentation.htm`