Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.488 – 500

RESEARCH ARTICLE

A SECURE AND TRUSTED ROUTING SCHEME FOR WIRELESS MESH NETWORKS

Pushpender Sarao

Computer Science & Engg.

Shri Venkateshwara University

Amroha (UP), India

Pushpendrasarao@gmail.com

Prof.(Dr.) Sohan Garg

Computer Science &Engg.

C.C.S. University

Meerut(UP), India

sohangarg@rediffmail.com

Abstract- In this paper, we propose a secure and reliable routing technique based on fuzzy logic (SRRT) for finding a secure and reliable path in wireless mesh networks. In this technique for each node we find out two variables, trust value and hop count value, to determine the lifetime of the routes. The trust level that is used to choose a reliable and secure route between the communicating nodes is not a predefined value. Therefore to facilitate the evaluation of trust levels, a fuzzy logic based approach has been also implemented. To assign trust levels to nodes of wireless mesh networks, a fuzzy trust evaluation mechanism receives information about the behavior history of wireless mesh network nodes. Three types of misbehaving nodes are considered in this paper. These include dropping the packets by the node, packets forwarding in a wrong direction and delay the packet regularly. Every node along route discovery records the trust value and hop count value in RREQ packet. In the destination with the aid of fuzzy logic, a new parameter is generated from inputs trust value and hop count value of each route which is called "Route". The path with more route value is selected as a secure and reliable route from source to destination. Simulation results show that SRRT has significant performance and reliability enhancement in comparison with other traditional existing on-demand routing algorithms.

Keywords-Wireless Mesh Networks, Reliability, Trust Value, Packet Dropped, Fuzzy Logic, SRRT

I. INTRODUCTION

Wireless mesh networks (WMNs) are self-configurable and, self-healing wireless networks. Access point (AP), gateways, mesh clients, mobile nodes, mesh routers are the main components of a wireless mesh networks. In WMNs data is transferred hop by hop. And to forward a packet from source to destination, a number of hops may have to be visited. As the small network is extended to a large network, the chances of degradation of performance and reliability of routing process are more. Mostly several routing protocols used for MANETs are also used for WMNs. But when the size of a WMN is extended to a large, the performance in such a network is going to through poor. In the last few years, a number of routing algorithms for wireless mesh networks has been proposed. But most of the algorithms are designed taking into consideration that all the nodes into network will take full cooperation in routing the packets form source to destination. Also some traditional already existing protocols such as DSR and AODV only takes one parameter 'minimum hop count' for routing decisions. Also there are several limitations in the existing protocols. But several other parameters must have to be considered such as signal power, mobility of the node, buffer occupancy, trust level, and maliciously and selfishly of a node on a wireless network. But, the fact that all the nodes in the wireless network will not compulsory full cooperates in routing the packets from source to destination. Some nodes may refuse to forward packets as expected and due to this reason the reliability and performance of the network may be degraded. To enhance a secure and reliable routing, a new enhanced routing protocol must have to be designed for wireless mesh networks. Due to the selfishly and maliciously behavior of the nodes in the WMNs, a new trust level based routing algorithm to eliminate the effects of such nodes in the network have to be required. Utilizing the fuzzy inference system, a scheme to establish trust relationship between nodes is proposed. The proposed scheme uses the trust level of the route and number of hops form source to destination in routing decision purposes. In this proposed research work, trust level of each node is calculated based on multiple parameters in a fuzzy trust evaluation technique is developed using fuzzy logic toolbox of MATLab 7.0. This technique takes into account the information about the behavior history of the WMN node. The trust levels and number of hop counts are then used by the routing protocol in an attempt to select the most secure and reliable route between source and the destination.

To achieve a more reliable and secure route, the remainder of this paper is partitioned into five sections. The related work of fuzzy based routing protocols is presented in section 2. In section3, a detailed description of the proposed fuzzy model based on trust level and hop count is illustrated. The simulation work and result discussion with various scenarios used in this research work are presented in section 4. And the section 5 concludes this research article.

II. LITERATURE SURVEY

In[1] H.Hallani et al proposed an reliable routing protocol based on trust level between nodes. A trust evaluation model is proposed in this work. This model uses four variables packet-dropping, wrong-forwarding, fabrication, and replay-attack for evaluation of trust level. Each route has a trust level. The proposed Fuzzy Trust Algorithm (FTA) is compared with AODV routing protocol. MATLab and OPNET simulators have been used for simulation purposes.

H.Hallani and S.A. Shahrestani proposed an approach for wireless ad-hoc networks [2]. This approach is based on fuzzy logic to enhance the performance of security and reliability for wireless ad-hoc networks. The trust level of node is calculated using several parameters i.e. percentage of wrong forwarding messages, percentage of dropped packets, and percentage of replay attacks generated by a particular node. This is mainly centralized to achieve a reliable and secure routing path. Throughput, round trip delay, and packet loss route are the three parameters used for analyzing the effect of presence of a malicious node in the network.

Houssein et al proposed a routing algorithm based on fuzzy logic and trust level. This algorithm works as other on-demand routing protocols such as AODV and DSR. Packet dropped, wrong forwarding, fabrication, replay attack are the fuzzy inputs and trust level is the output variable for the proposed fuzzy rule based algorithm [3].

In [4] Paratha Sarathi Banarjee et al proposed a trust based AODV for mobile ad-hoc network. In this work, trust level is evaluated using five input parameters i.e. reliability, residual energy, buffer occupancy and packet generation rate. And one output parameter 'trust level' is used. Gaussian and Pi Membership functions have been used by fuzzy system.

K.Sasikala et al represent a routing protocol for wireless mesh network [5]. In this research work several parameters are considered such as buffer residency, node energy and hop count to calculate a reliable route on the network. The proposed work is based on tree construction scheme which manages to decreases data overhead-compared to customary ad-hoc routing protocols. Also an auto-configuration protocol is used to provide nodes with topologically correct IP addresses.

Mamam Hussein Mamaum presented a routing technique for MANET. A productive decision is applied by using three input variables link strength (LS), node energy (NE), and number of hopes (NH). Using a fuzzy system, a network broadcast will be continue or not continue is decided. GloMoSim simulator have used for simulation purposes and the proposed work is compared with DSR protocol using the performance metrics route request overhead, packet delivery ratio, average end-to-end delay[6].

Mehdi Karger presented a routing mechanism for ad-hoc networks based on malicious and selfish nodes [7]. The proposed work is designed with LCP (Least Cost Path). It is a reactive routing scheme. After starting of a session, the computation of routing path is taken place only. Route discovery, detecting malicious nodes, data transmission and route discovery are four main parts of the proposed protocol.

Jing Nie et al presented a fuzzy logic based security routing protocol (FLSL) for mobile ad-hoc networks. This work is designed on the basic idea of "local multicast" and security level. In this proposed protocol, security level of each node on the network is evaluated. To evaluate the security level, three parameters length of the security key(l), number of neighbor hosts (n), and the frequency of changing keys (f) are used as input for fuzzy system and one parameter 'security level' is used as output. Here fuzzy sets for output parameter are taken as lowest, low, normal, high, and highest[8].

III. PROPOSED MODEL

In this section we propose our secure and reliable routing technique SRRT which is improved version of our previous work [9].

A. SRRT Mechanism

Trust value and hop count are the two main variables in this technique that make the routing technique more secure and reliable. Before explaining the scheme, trust value estimation mechanism is described below.

Trust Evaluation: The trust level that is used to choose a reliable and secure route between the communicating nodes is not a predefined value. Therefore to facilitate the evaluation of trust levels, a fuzzy logic approach has been implemented here. To assign trust levels to nodes of wireless mesh networks, a fuzzy trust evaluation approach receives information about the behavior history of wireless mesh network nodes. Three types of misbehaving nodes are considered in this paper. These include dropping the packets by the node, packets forwarding in a wrong direction and delay the packet regularly. Trust value of each node is calculated based on the various parameters like packet dropped by node, packet forwarding to the wrong destination. Based on the above parameters trust level of a node i to its neighbor node j can be calculated.

Trust calculation:

To calculate the trust value of each node in the network, Fuzzy Logic has been used. This trust of a node is based on Dropping of packets, delay of packets, and wrong forwarding of messages on the network. The absolute value of each of these variables can take a large range at different points on the wireless mesh network. We have considered the normalized values for each variable.

'Crisp' normalized values have been converted into fuzzy variables. For this, three fuzzy sets have been defined for each variable. The fuzzy sets, Low, Medium and High have been used for the input variables.

The normalized value of each parameter is mapped into the fuzzy sets. Each value will have some grade of membership function for each set.

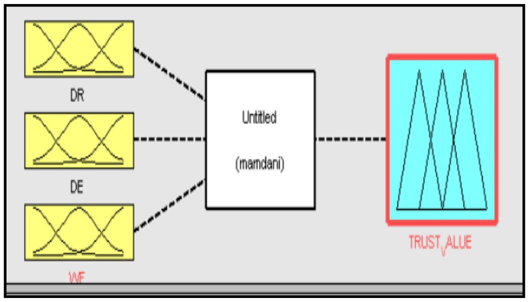

Fig.1: Fuzzy system for trust value evaluation

- In the fuzzy trust evaluation, the trust level of a node is calculated by determining the number of packets dropped, the number of packets delayed, and the number of packets forwarded to the wrong destination. These input variables DR (Dropped packets), DE (Delayed packets), and WF (Wrong forwarding) are characterized by Gaussian membership function.

- The output parameter that indicates the trust level of the node is termed as 'Trust Value'. This parameter has seven fuzzy sets very-very low, very low, medium, high, very high, and very- very high.

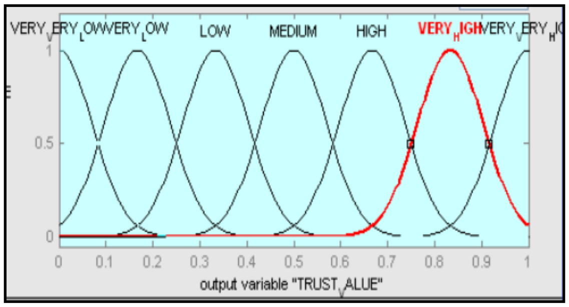

Fig.2: Membership function for output parameter 'Trust Value'

- The trust evaluation system is a 'Mamdani' type with three input variables and one output parameter trust value into the interval (0, 1).
- Fuzzy inputs can then be processed using fuzzy rules in the fuzzy trust value evaluation, a number of rules are derived, but one of them is explained as below:

"If (DR is LOW) and (DE is MEDIUM) and (WF is LOW) then (TRUST_VALUE is VERY_HIGH)".

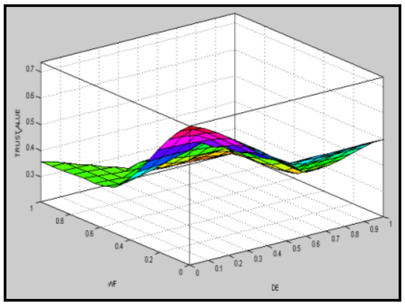

Fig.3 : 'Trust Value' O/P w.r.t. 'WF' and 'DE'

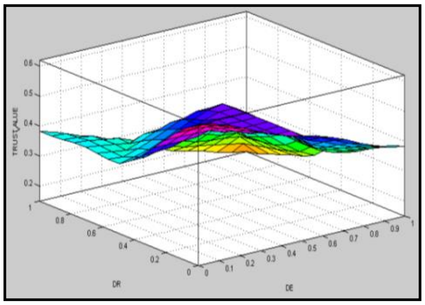

Fig.4 : 'Trust Value' O/P w.r.t. 'DR' and 'DE'

The variation in the trust value of a node , as the dropped of packets, wrong forwarding packets, and delay of packets variables are updated from low to high; is represented in figures. It is clear from these 3D graphs that trust value increases when the values of these variables decreases.

- **THE PROPOSED FUZZY RULE BASED SRRT PROTOCOL**

FuzzyLogic Controller: A useful tool for solving hard optimization problems with potentially conflicting objectives is fuzzy logic. In fuzzy logic, values of different criteria are mapped into linguistic values that characterize the level of satisfaction with the numerical value of the objectives. The numerical values are chosen typically to operate in the interval [0, 1] according to the membership function of each objective.

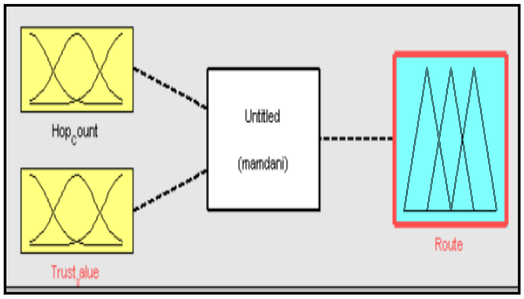

Fig.5: Fuzzy mechanism for SRRT

The proposed fuzzy logic based routing protocol SRRT takes into account of two input parameters, trust value and hop count. For fuzzification process, both input parameters and one output parameter have been assigned three fuzzy sets.

- The input fuzzy parameter "Trust Value" has three fuzzy sets-low, medium, and high. The membership function for trust value is illustrated in fig.
  - ➢ Low (from 0.0 to 0.4).
  - ➢ Medium (from 0.2 to 0.8).
  - ➢ High (from 0.6 to 1.0).
- The input fuzzy parameter "Hop Count" has three fuzzy sets-low, medium, and high. The membership function for trust value is illustrated in fig.
  - ➢ Low (from 0.0 to 0.4).
  - ➢ Medium (from 0.2 to 0.8).
  - ➢ High (from 0.6 to 1.0).

- The output fuzzy parameter “Route” has five fuzzy sets- very low, low, medium, high, and very high. The membership function for trust value is illustrated in fig.

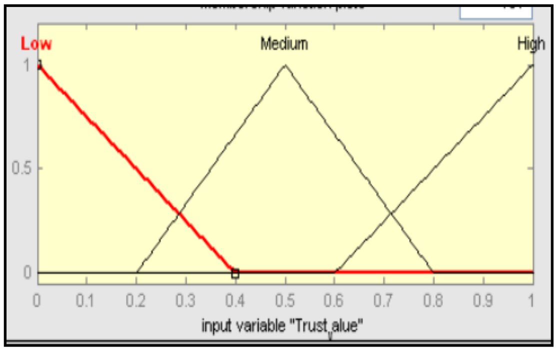

Fig.6: Membership function for input variable ‘Trust_Value’

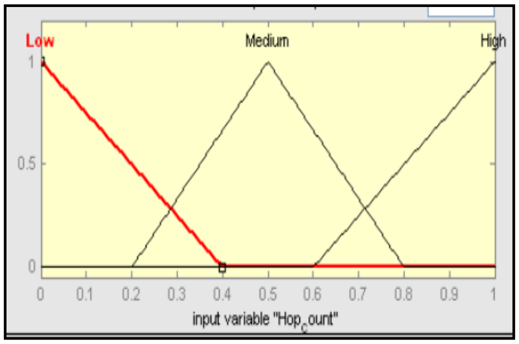

Fig.7: Membership function for input variable ‘Hop Count’

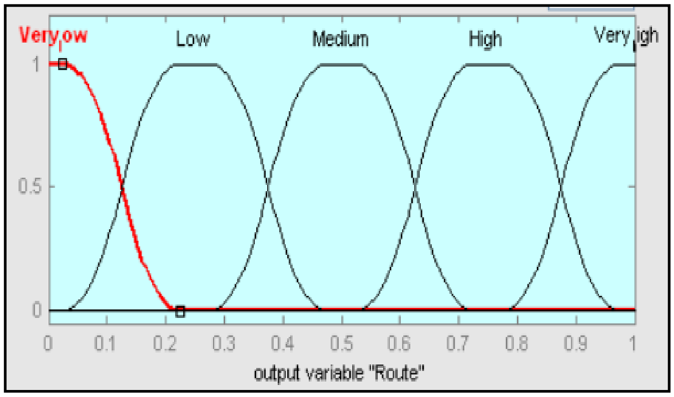

Fig.8: Membership function for ‘Route’

Route Evaluation: Route parameter take different values based on nine fuzzy inference rules that dependent upon varied input variable values i.e. hop count and trust values .A fuzzy logic system calculates for each two input values which values appear in output. The fuzzy logic system with product inference engine, singleton fuzzifier and center average defuzzifier are of the following form:

$$f(x) = \frac{\sum_{i=1}^{6} \bar{y}^{l}\left(\prod_{i=1}^{2} \mu_{A_i^l}(x_i)\right)}{\sum_{i=1}^{6}\left(\prod_{i=1}^{2} \mu_{A_i^l}(x_i)\right)}$$

In Eq.1 , x_i represents crisp input ith (hop count or trust values), $\mu_{A_i^l}(x_i)$ represents fuzzy membership function for input ith , and $\overline{y}^l$ is center average of output fuzzy set Ith . The fuzzy rules are as follows:

Rule1: If (Trust_ Value is Low) and (Hop Count value is Low) then (Route is Medium).

Rule2: If (Trust_ Value is Medium) and (Hop Count value is Low) then (Route is Low).

Rule3: If (Trust_ Value is High) and (Hop Count value is Low) then (Route is Very Low).

Rule4: If (Trust_ Value is Low) and (Hop Count value is Medium) then (Route is Very High).

Rule5: If (Trust_ Value is Medium) and (Hop Count value is Medium) then (Route is Medium).

Rule6: If (Trust_ Value is High) and (Hop Count value is Medium) then (Route is Low).

Rule7: If (Trust_ Value is Low) and (Hop Count value is High) then (Route is Very High).

Rule8: If (Trust_ Value is Medium) and (Hop Count value is High) then (Route is High).

Rule9: If (Trust_ Value is High) and (Hop Count value is High) then (Route is Medium).

B. Route discovery procedure

Step1: A source node starts to flood RREQ packets to its neighboring nodes in a wireless mesh network until they arrive at their destination node. Each RREQ consists of source id, destination id, hop count value and trust value of nodes along the path.

Step2: If the intermediate node M receives a RREQ packet and it is not the destination, then the information of node M is added to the RREQ packet which is appended to packet fields. After that, node M re-forwards the packet to all the neighboring nodes of itself.

Step 3: If node M receives a RREQ packet and node M is the destination, it waits a period of time. Therefore, the destination node may receive many different RREQ packets from the source. Then it calculates the value of ‘Route’ for each path from source to the destination using the information in each RREQ packet. Finally, destination node sends a route reply (RREP) packet along the path which has a maximum ‘Route’ value.

IV. SIMULATION AND RESULT DISCUSSION

A detailed analysis of wireless mesh network simulation results after applying the SRRT approach are presented in this section. For simulation purposes, we have used fuzzy logic toolkit of MATLab 7.0.The rule viewer for the SRRT has been shown in figure 9 and figure 10.

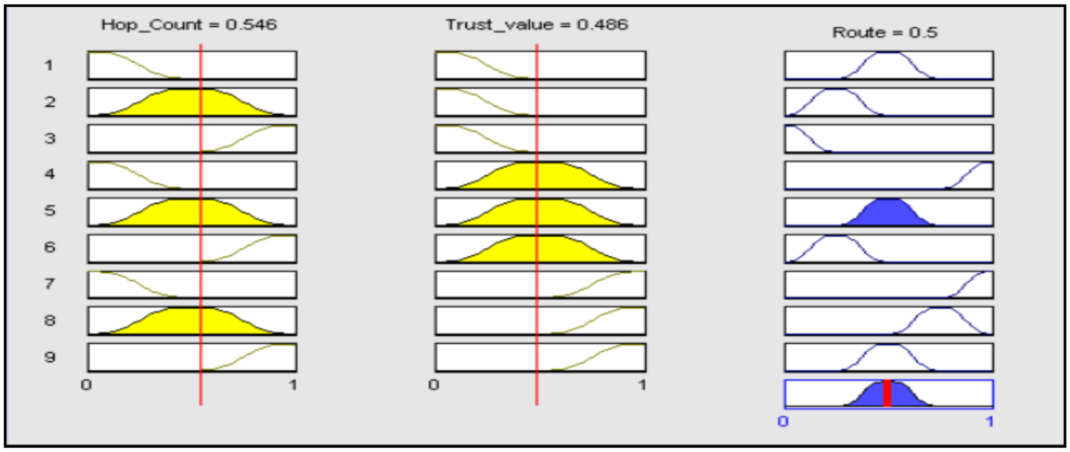

Fig.9: Fuzzy Rule viewer for the Route value calculation

The **figure 9 illustrates** that when hop count is 0.546, trust value is 0.486 then in this condition the route is 0.5.

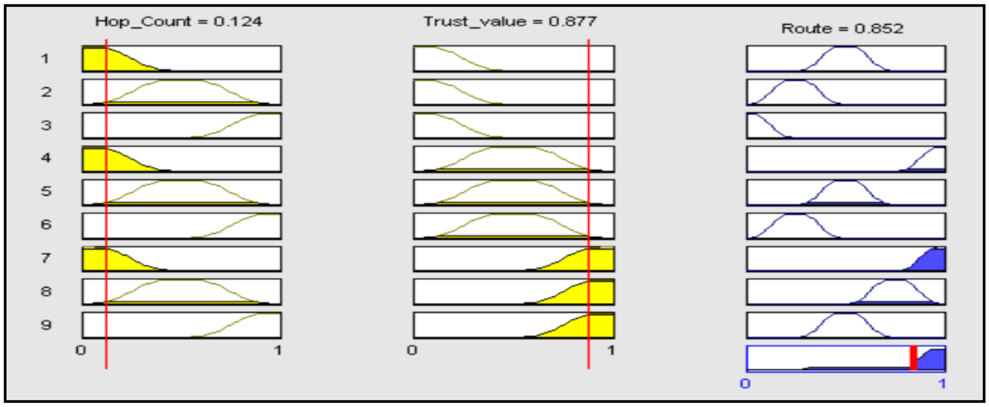

Fig.10: Fuzzy Rule viewer for the Route calculation

The **figure 10 indicates** that when hop count is low 0.124, trust value is high (0.877) and bandwidth is then in this condition the route is reliable (0.852).

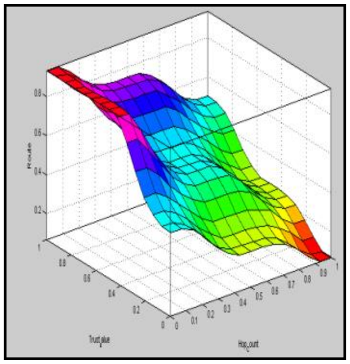

Fig.11 : 'Route' O/P w.r.t. 'Trust Value' and 'Hop Count'

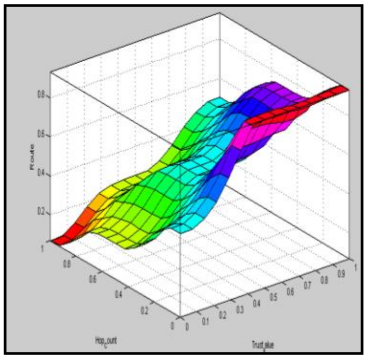

Fig.12: 'Route' O/P w.r.t. 'Hop Count' and 'Trust Value'

In **figure 11** the inputs of the protocol (hop count and trust value) are on the horizontal axes and the output (route) is on the vertical axis. In **figure 12** hop -count and trust value are the fuzzy input parameter for the proposed routing protocol which lies on the horizontal axes and route is the output parameter which has been shown on the vertical axis.

A number of test cases have been conducted for the proposed routing protocol SRRT. Some of them have been explained in the table 1. The table represents several input values of hop count and trust value and also their respected outputs.

Table 1: Test cases conducted for SRRT

Test Case No.	Hop Count	Trust Value	Route
Test case no.1	0.83 (high)	0.914 (high)	0.545
Test case no.2	0.0688 (high)	0.0682 (low)	0.5
Test case no.3	0.243 (low)	0.277 (low)	0.528
Test case no.4	0.546 (medium)	0.489 (medium)	0.5
Test case no.5	0.683 (high)	0.614 (high)	0.455
Test case no.6	0.794 (high)	0.759 (high)	0.473
Test case no.7	0.894 (high)	0.841 (high)	0.47
Test case no.8	0.977 (high)	0.941 (high)	0.5
Test case no.9	0.702 (high)	0.877 (high)	0.845
Test case no.10	0.28 (low)	0.877 (high)	0.755
Test case no.11	0.124 (low)	0.877 (high)	0.852
Test case no.12	0.0413 (low)	0.95 (high)	0.934
Test case no.13	0.0413 (low)	0.659 (high)	0.931
Test case no.14	0.0413 (low)	0.477 (medium)	0.934
Test case no.15	0.0413 (low)	0.332 (low)	0.777
Test case no.16	0.0413 (low)	0.186 (low)	0.568
Test case no.17	0.0229 (low)	0.986 (high)	0.934

- The simulation results indicates that at low hop count and when value of trust is low, route is medium i.e. reliability and security of route is medium. But at constant trust value, when increasing the value of hop count from low to medium and then high, the reliability of the route is go to very -very poor stage.

- At medium trust value, but lowest number of hop count, at this condition, the route will be at highest reliability point. But at constant trust value, when increasing the hop count, again the route goes to at lowest reliability point.
- At high trust value and low hop count, the route is at highest point of security and reliability, but when increasing the value of hop count, the reliability of route goes to medium stage.
- At last, the simulation results indicate that proposed SRRT routing protocol works well at high number of hop counts even though when trust value must be high. Also the proposed SRRT protocol works well at low trust value even though when hop count must be very low.

A. Simulation setup for performance comparison

The main technique of evaluating the performance of WMNs is simulation. The simulation work for comparison of proposed protocol SRRT with AODV routing protocol is done in MATLAB 7.0. The network is taken as 100X100 square kilometers. The performance is recorded taking different number of nodes. The nodes are placed randomly in the network. The packet size is taken as 512 bytes and the traffic type is Constant bit rate (CBR). The parameters taken for simulation are listed below in the Table 2. Here, we designed and implemented our test bed using MATLAB 7.0 to test the performance of both Routing protocols. The data transmission rate is 4packets/sec. The total simulation time is 100 second.

Table 2: Simulation Parameters

Parameter	Value
Simulator	MATLAB (R2008b)
Area	100 Km X 100 Km
No. of Nodes	20, 40, 60, 80 and so on up to 300
Packet Size	512 bytes
Traffic Type	CBR
Simulation Duration	100s
Mobility Speed	10(m/s)
Mobility Model	Randomly
Transmission Range	250m
Packet rate	4 packets/s
Number of CBR connections	8

B. Performance Measuring matrices

The performance is measured on the basis of some matrices which are described as follows:

Packet Delivery Ratio (PDR) - Packet delivery ratio is defined as the number of packets actually delivered to the destination to the number of data packets supposed to be received. The better the packet delivery ratio, the more complete and correct is the routing protocol.

***PDR=No.** of packets delivered/No. of packets received*

End-to-end delay (EED)- Average end-to-end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time. This metric is useful in understanding the delay caused while discovering path from source to destination.

Throughput- Throughput is the ratio of number of packets sent and total number of packets. It describes the average rate of successful message delivery over a communication channel. Throughput measures the efficiency of the system.

***Throughput= No.** of packets sent/Total no. of packets*

C. Results and Analysis

The simulation results indicate the characteristics of SRRT and AODV routing protocols. The analysis of the simulation of SRRT and AODV routing protocol is done on the basis of performance matrices which is as following:

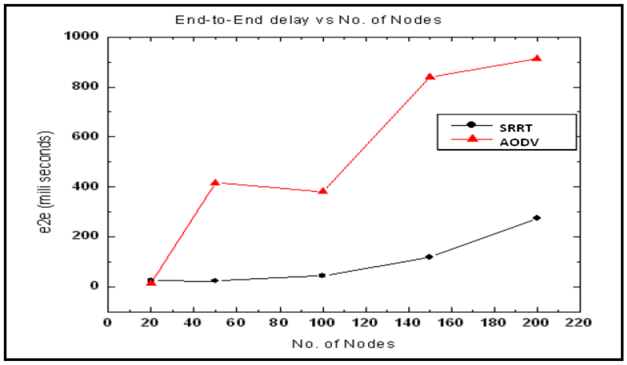

Fig.13: End-to-End Delay v/s No. of Nodes

Fig. 13 shows that as the number of node increases end to end delay in AODV increases rapidly as compared with SRRT. Reason behind the reduction in end to end delay is because of the selective processing of packets.

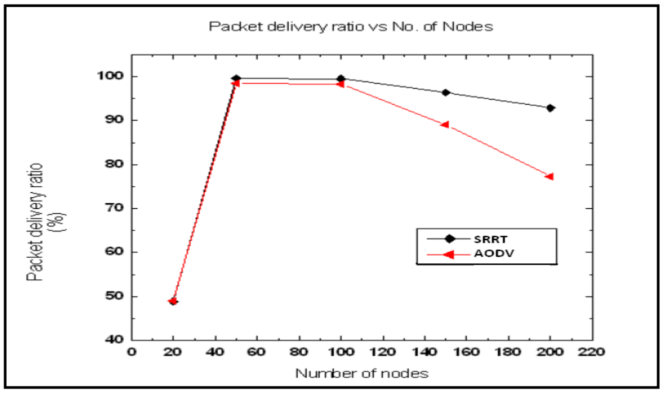

Fig.14: Packet Delivery Ratio v/s No. of Nodes

Fig. 14 shows that as the number of nodes increases routing overhead also increases, SRRT avoid unreliable and unsecure nodes from the route, it requires less rerouting and leads to less control overhead so in large network SRRT perform better than AODV.

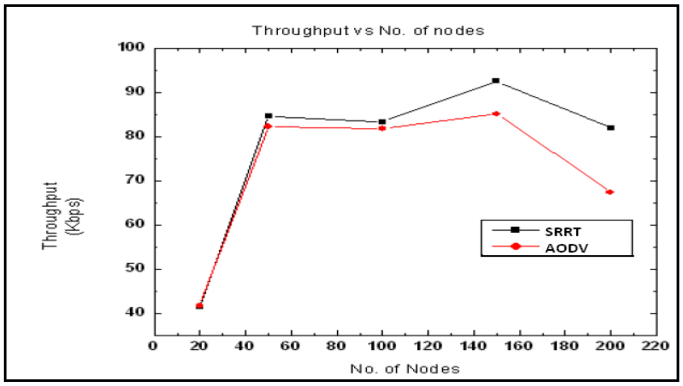

Fig.15: Throughput v/s Number of Nodes

Fig. 15 SRRT selects the most reliable and secure path so number of packet drop is also low as compare to AODV. So the packet delivery ratio is also better than AODV in multi-hop WMNs.

The simulation results of comparison presents that SRRT perform better than AODV as the number of nodes increases.

V. CONCLUSION

Wireless mesh networks are self-configurable, self-healing and data is transferred from source to destination hop by hop. In such an environment, cooperation of each node in the network is most important. If any node behaves like a selfishly or a maliciously node, then performance degradation and security attack of the network is taken place. Hence it is necessary to find a more secure and reliable route that endures a long time. To enhance the performance and reliability of wireless mesh networks in the presence of malicious and selfishly nodes, two fuzzy logic based approaches have been proposed in this paper. In one approach, we find out three variables: trust value, hop count value and route value that are used for finding a secure and stable route from source to destination. At the time of discovery process in the network, every node adds its trust value and hop count value in RREQ packet. At the destination, based on route value, is decided which path or route have to be followed for data communication purposes. The route with more route value is selected to route data packets from source to destination. The simulation results indicate that the proposed routing technique has significant performance and reliability enhancement in comparison with other existing on-demand routing protocols such as AODV.

REFERENCES

[1] H.Hallali and S.A. Shahrestani, "Enhancing the Reliability of Ad-hoc Networks through Fuzzy Trust Evaluation",In 8th International Conference on APPLIED COMPUTER SCIENCE (ACSOP),pp. 93-98.

[2] H.Hallali, S.A. Shahrestani, "Fuzzy Trust Approach for wireless Ad-hoc Networks" ,Communications of the IBIMA,volume 1, 2008,pp. 212-218.

[3] Houssein Hallali and Seyed A. Shahrestani, "Mitigation of the Effects of selfish and Malicious Nodes in Ad-hoc Networks", WSEAS transactions on Computers, issue 2, volume 8, February 2009, pp. 205-221.

[4] Parta Sarathi Banerjee, J.Paulchoudhry, S.R. Bhadra Choudhuri, "Fuzzy Membership Function in a Trust Based AODV for MANET", I.J. Computer Network and Information Security, 2013, pp. 27-34.

[5] K.Sasikala, V.Rajamani, "A Modified Fuzzy logic Routing for Wireless Mesh Network", International Journal of Computer Applications, volume 60-No.2, December 2012, pp. 28-34.

[6] Mamoun Hussein Mamoun, "A proposed Route Selection Technique in DSR Routing Protocol for MANET", International Journal of Engineering &Technology IJET-IJENS vol: 11 No: 02, April, 2011, pp.10-13.

[7] Mehdi Kargar, "Trustful and Secure Routing in Ad-Hoc Networks with Malicious and Selfish Nodes", International Journal of Security and its Applications, vol.3, No.1, January, 2009, pp. 117-128.

[8] Jing Nie, Jiangchua Wen, Ji Luo, Xin He, Zheng Zhou, "An adaptive fuzzy logic based secure routing protocol in mobile ad-hoc networks", Fuzzy sets and Systems 157(2006), pp. 1704-1712.

[9] Er. Pushpender Sarao, Prof.(Dr.) Sohan Garg, "LSA-AODV: A link stability based algorithm using fuzzy logic for multi-hop wireless mesh networks", SHIV SHAKTI International Journal in Multidisciplinary and Academic Research (SSIJMAR) Vol. 2, No. 6, November- December (ISSN 2278 – 5973),Dec,2013,pp. 1-12.