I. J. Computer Network and Information Security, **2013, 12, 27-34**
Published Online October 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.12.04

Fuzzy Membership Function in a Trust Based AODV for MANET

[1]Partha Sarathi Banerjee, [2]J. Paulchoudhury, [3]S. R. Bhadra Chaudhuri
[1,2] Kalyani Government Engineering College, West Bengal India
[3]Bengal Engineering and Science University, Shibpur (BESUS), West Bengal, India
[1] psbanerjee.kgec@gmail.com, [2] jnpc193@yahoo.com, [3]prof.srbc@gmail.com

Abstract — Security issues have been emphasized in MANET due to its vulnerability to unauthorised access and unshielded broadcasting nature of communication. In this paper we present a trust based AODV for MANET. The trust takes into account the eligible neighbours based on reliability, residual energy, and speed. Thus our algorithm provides a reliable, energy efficient routing technique. The multi-criteria trust values are calculated using fuzzy-logic. This algorithm is capable of putting aside the selfish nodes. As only trusted neighbours are selected for packet delivery, energy consumption also diminishes because the transmitting node does not need to deliver packets to the untrusted neighbours. Less number of transmissions renders low energy consumption. Absence of selfish nodes in the selected neighbours at every hop provides better packet delivery and hence better throughput.

Index Terms — MANET, AODV, Trust, Fuzzy Logic, Membership functions

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a kind of wireless network without any centralized authority or fixed infrastructure. Nodes in MANET perform routing by means of route discovery and route maintenance in a self-organized fashion. Though highly explored, routing in MANET still demands for newer approach. Prior research has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment [16]. These may be sufficient for normal day-to-day applications but for applications such as military exercises and disaster relief, a secure and a more reliable communication is a prerequisite. The biggest challenges identified in MANET routing are its ever-changing topology due to mobility of the nodes, limited battery power and existence of malicious nodes. Dynamic topology prevents existence of static path between any source-destination pair. Limited battery power of the nodes inhibits the use of very complicated operations and hence all cryptographic algorithms cannot be used for data security. Malicious nodes in the network apply different tricks to attack the stability of the network .Active attacks can be easily identified by different techniques but passive attacks are more dangerous as the compromised nodes tries to influence the network stability and integrity silently. Conventional security solutions devised for wired network may not be a good choice for use in MANET because of architectural instability and power constraint. Identification of the compromised nodes in MANET is a big challenge. Security solutions for MANET need to be devised keeping in mind the integrity and stability of the network. In section II of this paper a brief literature survey is given. Methodologies and tools used for this work are discussed in section III. In section IV, detailed discussion about the fuzzy based trust calculation method and its application in the proposed protocol is given. A stepwise outline of the proposed protocol is also given there. In section V, simulation results along with graphs are presented.

II. RELATED WORK

Many security solutions for MANET have been provided in literature like secure routing protocols [1], [2], [3], [4], [5] and secure key management protocols [6],[7],[8],[9],[10]. However, these solutions depend on some central authority or trusted third party to issue certificate. Dependency on central authority somehow contradicts the self-organizing dynamic nature of MANET. Information security has been addressed in terms of node-compromise-probability, trust and key management [11], [12], [13]. Secure key management protocols put onus of high computation overhead on the nodes which are power restricted. Our solution is, on the other hand, a secure routing protocol which employs the idea of a trust model so that it can avoid introducing large overheads and influencing the self-organization nature of MANETs. This solution is based on on-demand routing protocols [14]. In this trust-based routing, fuzzy-logic has been used. Different parameters have been fuzzified to get a qualitative measurement of trust. Trust models have found security applications in e-commerce, peer-to-peer networks, and some other distributed systems [15] [16] [17] [18] [19]. In recent years, some research work is conducted to apply trust models into the security solutions of MANETs [20] [21].

Our main focus is on on-demand routing protocols [14], in which a node attempts to discover a route to some destination, if and only if has a packet to send to that destination. The source must wait until a route has been discovered, but the traffic overhead is less than table-driven algorithms [14] where many of the updates are for the unused paths. This reduced overhead affects bandwidth utilization, throughput as well as power usage. No prior advertisement is done, which makes the on-demand routing protocols covert in nature. However, this property is alone not enough to stop a malicious user to access the routing information and initiate directed attacks at the source, destination or any other intermediate node in the network, thus effectively disrupting or even bring down the network.

In this literature we have proposed a trust based AODV protocol which is able to bypass the misbehaving nodes during the route discovery process. This filtering is done using the trust value associated with each of the neighbors of all the nodes; those have been discovered during the multi-hop communication from the source.

III. METHODOLOGY

A. *AODV*

The Ad hoc On Demand Distance Vector (AODV) Routing protocol is a very popular protocol in MANET. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. This route discovery and route maintenance are the two major phases proposed in AODV. It maintains these routes as long as they are needed by the sources. This algorithm provides a loop-free, self-starting efficient routing algorithm typically devised for MANET. AODV finds routes using a route request (RREQ) /route reply (RREP) query cycle. Whenever a source node requires a route to a destination node which is not enlisted in the source node’s routing table, it broadcasts a RREQ message. Intermediate nodes between source and destination receive this RREQ message sent by the source. On receiving this packet, these nodes update themselves with the information about the source node.

In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source nodes are aware of. A node, on receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source node, it set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a better option in terms of RREP containing a greater sequence number or a smaller hop-count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will timeout and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery. AODV is chosen because of the inherent security in the protocol. Notice that one of the differences between AODV and DSR is that, DSR requires every packet to carry the routing information, whereas, in AODV, once the route is established, the data packets just carry the flow-ID. So, in DSR, we’ve to encrypt the routing information in every single data packet which is, not impossible, but not desired.

B. *Fuzzy Logic*

In fuzzy logic, unlike standard conditional logic, the truth of any statement is a matter of degree. The notion central to fuzzy systems is that the truth values (in fuzzy logic) or membership values (in fuzzy sets) are indicated by a value on the range [0.0, 1.0], with 0.0 representing absolute False and 1.0 representing absolute Truth. The minimum value is 0 and the maximum value is 1. The value in between the range can be decided by the membership function.

Gaussian Membership Function

A Gaussian membership function is defined by (1), where the parameters m and σ control the centre and width of the membership function.

$$G\,(u{:}\ m,\sigma) = e^{[-\{(u-m)/\sqrt{2\sigma}\}]} \tag{1}$$

Triangular membership function

A triangular membership function is defined by (2). Here the triangular curve is a function of a vector x and depends on three scalar parameters a, b and c as follows

$$F(x;\, a,\, b,\, c) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right) \tag{2}$$

PI-membership function

PI-membership function is represented by the following (3). It is so named because of its π-shape. In the following equation parameters a and d denote the feet of the function and b and c denote the shoulder of it.

$$\begin{aligned} f(x;a,b,c,d) &= 0, & x \le a \\ &= 2\left(\frac{x-a}{b-a}\right)^2, & a \le x \le \frac{a+b}{2} \\ &= 1 - 2\left(\frac{x-b}{b-a}\right)^2, & \frac{a+b}{2} \le x \le b \\ &= 1\ , & b \le x \le c \end{aligned}$$

$$\begin{aligned} &=1-2\left(\frac{x-c}{d-c}\right)^2, \quad c \le x \le \frac{c+d}{2} \\ &=2\left(\frac{x-d}{d-c}\right)^2, \quad \frac{c+d}{2} \le x \le d \\ &=0 \quad , \quad x \ge d \end{aligned} \qquad (3)$$

C. Ad Hoc Network Parameters considered for Trust calculation

a) *Reliability*:

Reliability of a mobile node in MANET is considered to be the ratio of number of packet it has forwarded to the number of packet it has received. This ratio may be regarded as a measure for selfishness of a node. The more packets a node forwards, more reliability is achieved by that node. The node will be considered selfish if the ratio falls below a threshold. A high value of reliability of a node results in greater trustworthiness.

b) Residual Energy:

Every transmitted or received packet consumes power. Energy consumption due to transmission is greater than that of reception of packets. So, reliable and active nodes are subject to more power consumption as these nodes are more trusted for packet forwarding compared to their less reliable peers. Therefore, it is found that reliability and residual energy are inversely related to each other. Greater residual energy leads to high trust value.

c) Buffer occupancy:

All the nodes in MANET are equipped with queues which are called buffer. When a packet reaches a node, it is queued there for a while for the sake of synchronization with and availability of the next level of neighbours. Greater is the buffer-occupancy, greater the probability of packet loss.

d) Packet Generation Rate:

This parameter depicts the behaviour of the node. A high value of packet generation rate may indicate malicious behaviour of the node. This is a kind of attack in which the malicious node tries to jam the network by generating spurious packets.

e) Speed:

Nodes are mobile in MANET. But high speed nodes are less probable of forming an ad hoc network.

D. Performance Metrics:

1. *Packet Delivery Ratio (pdr)*:

This parameter is measured as the ratio of the number of successfully received packets to the number of packets transmitted in the network. As the number of nodes increases, the size of the network increases and hence pdr decreases as a result of increased hop count for every packet delivery.

2. *Average end-to-end delay:*

Every packet in the network requires a minimum amount of time to reach the destination node. This time is called end-to-end delay. This parameter is considered as a QoS parameter for MANET.

IV. IMPLEMENTATION

Design Goals:

The main aim is to send packets through a wireless path which is energy efficient and void of malicious node.

Trust calculation:

In the proposed protocol Fuzzy Logic has been used for trust value calculation. This trust of a node is based on Reliability (ratio of packets forwarded to packet received by the node concerned), Residual Energy, Buffer Occupancy, Packet Generation rate and Speed of the node. The absolute value of each of these parameters can take a large range at different points on the network. We have considered the normalized values for each parameter.

'Crisp' normalized values have been converted into fuzzy variables. For this, three fuzzy sets have been defined for each variable. The fuzzy sets, low (from 0 to 0.4), medium (from 0.2 to 0.8) and high (from 0.6 to 1.0) 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. The memberships that have been defined for each of the fuzzy set for any particular input variable vary in shape depending on the characteristic of the membership function used. In Fig. 1 and Fig. 2 it is shown that the variation of input parameters reliability (fwd/recv) and residual energy according to the Gaussian-membership function and triangular membership respectively. All the input parameters will have the similar kind of characteristics with respect to the fuzzy membership function used.

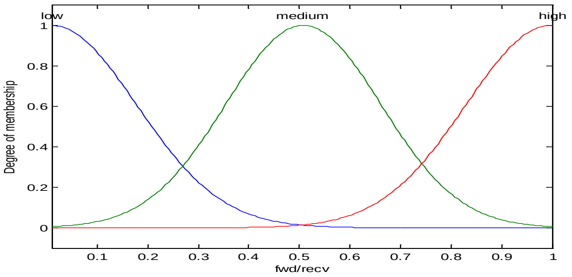


Figure 1. Fuzzy membership of Reliability (fwd/recv) according to Gaussian-membership function

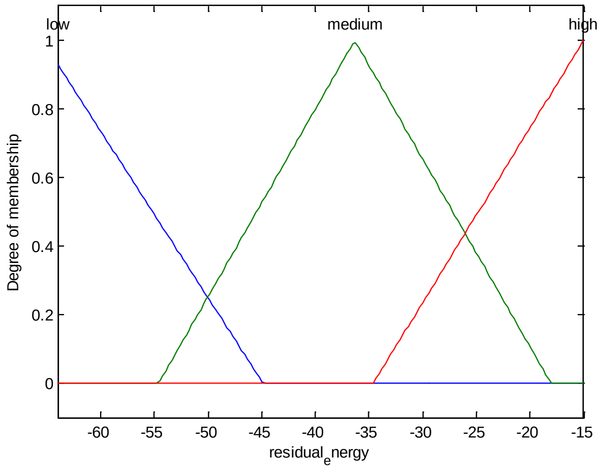


Figure 2. Fuzzy membership of residual energy (triangular membership function)

After the input parameters are fuzzified into three fuzzy sets vide LOW, MEDIUM and HIGH; the rules of inference have been written. Initially total 225 rules are devised. The crisp value of input variable is given and a defuzzified crisp value for selected variable is calculated. An output linguistic variable is used to represent the trust. The trust is classified into six fuzzy sets vide **lowest** (0.06 to 0.21), **very low** (0.2 to 0.37), **low** (0.3 to 0.53), **moderate** (0.5 to 0.68), **good** (0.65 to 0.84), **best** (0.8 to 1.0). as shown in Fig. 3. This figure is shown for the Gaussian-membership function only. The same fuzzy sets have been used for triangular function and PI-membership function also.

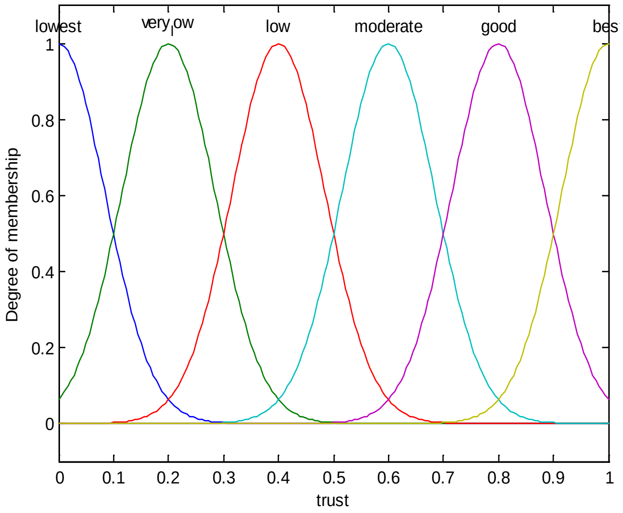


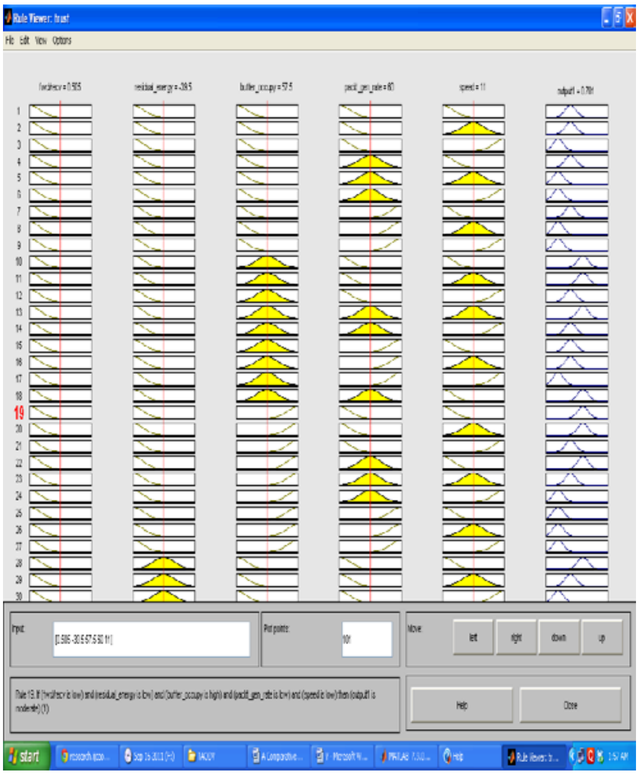
Figure 3. Fuzzy membership function (in case of Gaussian membership function) of the output 'trust'

An exhaustive rule set has been formed. Some of the fuzzy rules are depicted in table 1.

Table 1. Fuzzy Rule Base

Fwd/ recv	residual _ energy	buffer_ occupy	packt_gen _rate	speed	trust
Low	Low	Low	Low	Low	Low
Low	Low	Low	Low	High	Very Low
Low	low)	Medium	Low	Medium	Moderate
Low	Low	Medium	High	High	Very Low
Low	Low	High	High	Medium	Very Low
Low	Medium	Low	Low	Low	Moderate
Medium	High	High	High	High	Moderate
Medium	High	High	Low	High	Moderate
High	Low	Low	Medium	High	Good
High	High	Low	Low	Medium	Best

Fig. 4. shows a snapshot of the fuzzy rule base when input is {fwd/recv=0.505, residual energy=39.5 db, buffer_occupancy=60%, packet_generation_rate=60 kbps, speed=11m/s} and the output (trust) is 0.781.



[0.505 -39.5 57.5 60 11]

101

Rule 19. If (fwd/recv is low) and (residual_energy is low) and (buffer_occupy is high) and (packt_gen_rate is low) and (speed is low) then (output1 is moderate) (1)

Figure 4. Fuzzy Rule viewer for the trust calculation

The fuzzy rule base has been trained and tested with 10 set of values for each of the membership function. Some of the test values are shown in table 2.

Table 2. Test values for fuzzy rule base

	Fwd/ recv	residual _ energy (dB)	buffer _ occupy (%)	packt _gen _rate (kbps)	Speed (m/s)	trust
Gaussian	0.74	-39.5	57.5	60	11	0.77
	0.3	-50.5	60.5	40	5	0.64
	0.9	-15	80.5	70	15	0.8

PI	0.9	-64	90.5	80	20	0.42
	0.62	-64	90.5	70	12	0.51
	0.35	-50	69	38	15	0.54
Triangular	0.9	-15	80.5	70	15	0.72
	0.59	-58	90.5	70	12	0.53
	0.74	-38	59	68	11	0.71

The trust value corresponding to PI-membership function, Gaussian-membership function and Triangular membership function has been calculated using the fuzzy inference system. This trust value associated with each neighbor of a node is used in AODV. The trust based AODV protocol has been discussed in the following paragraph. The protocol has been tested separately with each of the fuzzy membership function under consideration.

Protocol Description:

Step 1:

In this protocol the sender node sends 'HELLO' packet to the neighbors asking for the instantaneous values of the parameters Reliability, Residual Energy, Buffer Occupancy, Packet Generation Rate and Speed. Nodes those are located within the transmission range of the sender are considered as neighbors.

Step 2:

On receiving the response packets, the source sends them to the Fuzzy Rule Based Trust Calculation Module. This module associates trust values with all the neighbors of the source node and recommends the next hop for packet delivery.

Step 3:

The source then forwards the RREQ packet to the trusted neighbors. The neighbors with a trust value less than a threshold are avoided.

Step 4:

Each of the neighbors who receive the RREQ packet from the source, checks the destination address carried by the RREQ to find whether the packet is destined for itself. If it is matched, destination is found at first hop. Otherwise the node will follow the same procedure starting from 'Step 1'.

Step 5:

After the path is found from the source to the destination, RREP (Route Reply) packet, which will follow a unicast path to the source from the destination, will be sent.

Step 6:

After the path is established between source and destination, data are sent through the path which consists of highly trusted nodes

Simulation:

The proposed trust based routing protocol has been simulated in MATLAB. For trust calculation fuzzy-logic toolbox of MATLAB has been used. The simulation parameters are shown in table 3.

Table 3. Simulation Parameters

Simulation parameters	Values
No. of nodes	50
Mobility	Random Waypoint Mobility
Initial Transmission Range	80m
Traffic Type	CBR
Packet Size	100 Bytes
Reliability(packet forwarded/packet received)	Min: 0.01 Max: 1
Residual Energy	Min: -64dB Max:-15 dB
Buffer Occupancy	Min: 20% Max: 95%
Packet Generation Rate	Min: 20 kbps Max:100 kbps
Speed	Min:2m/s Max:20m/s

With the parameters mentioned in Table 3, Fuzzy based Trust-AODV has been implemented. The simulation has been executed 15 times for every set of values of input parameters. The average values of packet-delivery ratio and end-to-end delay has been taken.

In Fig. 5 the simulation environment has been shown. It comprises of 50 nodes (green boxes). Path of data delivery is shown from S (source) to D (destination). B, a neighbor of S, is not selected as the next hop because of low level of trust value obtained for B.

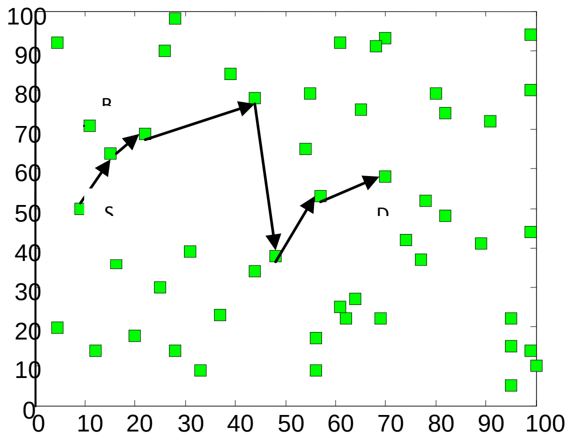


Figure 5: MANET architecture under consideration.

Comparison with respect to packet-delivery-ratio and end-to-end delay has been made among the outputs of the algorithm which is separately tested with the application of Gaussian membership function, PI-membership function and Triangular-membership function. The neighboring node with best trust value is the most likely to be the next hop for data delivery from the source. Neighboring node with lowest trust is not selected as the next hop.

V. RESULTS

The trust based AODV protocol has been tested with three fuzzy-membership functions vide Gaussian-membership function, Triangular-membership function and PI-membership function. The results have been tested with respect to successful packet delivery ratio and average end-to-end delay for each membership functions used for trust calculation. The values obtained for Packet Delivery Ratio (PDR) with respect to increasing number of nodes are presented in Table 4.

Average end-to-end delay with respect to different number of nodes is depicted in table 5. The corresponding plots are shown in Fig. 6 and Fig. 7.

Table 4. Number of nodes vs. Packet Delivery Ratio (PDR)

Membership function ⇨ Number of nodes ⇩	PDR for Gaussian Membership Function	PDR for Triangular Membership Function	PDR for PI Membership Function
40	0.8	0.5	0.2
50	0.7	0.4	0.3
60	0.5	0.4	0.4
70	0.6	0.3	0.2
80	0.6	0.2	0.3
90	0.5	0.2	0.3
100	0.5	0.4	0.2
150	0.2	0.2	0.1

Table 5. End-to-End Delay w.r.t number of nodes

Membership function ⇨ Number of nodes ⇩	End-to-End Delay (ms) for Gaussian Membership Function	End-to-End Delay (ms) for Triangular Membership Function	End-to-End Delay (ms) for PI Membership Function
40	0.0111	0.011	0.013
50	0.0112	0.0129	0.0126
60	0.0115	0.0136	0.012
70	0.0115	0.0138	0.0115
80	0.0133	0.0146	0.011
90	0.014	0.0154	0.0123
100	0.016	0.0163	0.0136

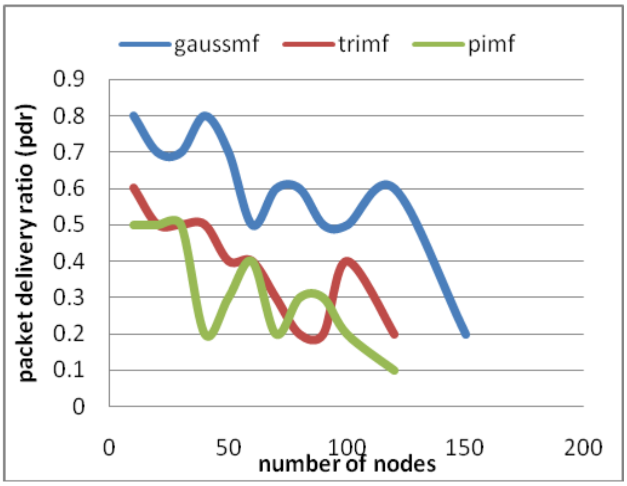


Figure 6. Number of nodes vs. packet delivery ratio (pdr)

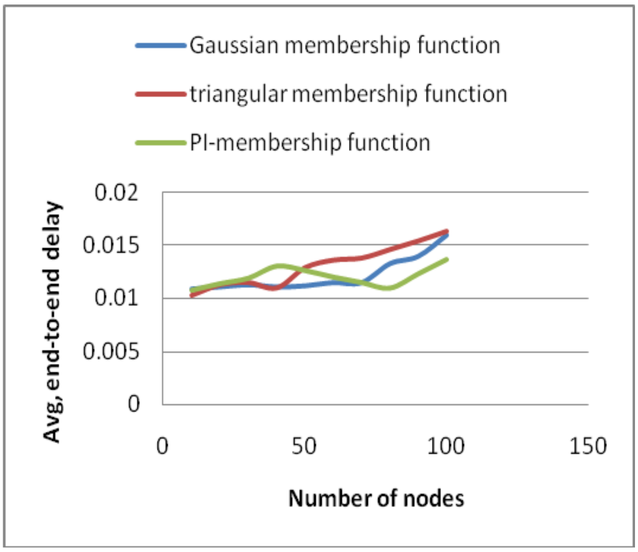


Figure 7. Number of nodes vs. Average End-to-End delay

It has been found that packet delivery ratio (pdr) decreases with increasing number of nodes in case of all three membership functions. Gaussian membership function performs better than the other two membership functions. In case of average end-to-end delay, it is found that the performance of PI-membership function is better compared to the other two membership function.

REFERENCE

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks”, in Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom ’02), Atlanta, USA, September 2002, http://citeseer.nj.nec.com/article/hu02ariadne.html.

[2] M. G. Zapata and N. Asokan, “Securing ad hoc routing protocols,” in Proceedings of ACM Workshop on Wireless Security (WiSe ’02). Atlanta, USA: ACM Press, September 2002, pp. 1–10, http://doi.acm.org/10.1145/570681.570682.

[3] H. Yang, X. Meng, and S. Lu, “Self-organized network layer security in mobile ad hoc networks,” in Proceedings of ACM Workshop on Wireless Security (WiSe’02),Atlanta, USA, September 2002.

[4] Y.-C. Hu, D. B. Johnson, and A. Perrig, “Sead: Secure eficient distance vector routing in mobile wireless ad hoc networks,” in Proceedings of 4thIEEE Workshop on Mobile Computing Systems and Applications (WMCSA ’02), June 2002, pp. 3–13.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, andE. M. Belding Royer, “A secure routing protocol for ad hoc networks,” citeseer.nj.nec.com/551839.html.

[6] L. Zhou and Z. J. Haas, “Securing ad hoc networks,” Journal of IEEE Networks, vol. 13, no. 6, pp. 24–30,1999.

[7] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in Proceedings of IEEE ICNP '01,2001.

[8] J.-P. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), 2001.

[9] S. Capkun, L. Buttyan, and J.-P.Hubaux,"Self-organized public-key management for mobile ad hoc networks," in Proceedings of ACM Workshop on Wireless Security(WiSe '02), Atlanta, USA, September 2002,http://citeseer.nj.nec.com/capkun02selforganized.html.

[10] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self securing ad hoc wireless networks," in Proceedings of IEEE ISCC'02, 2002.

[11] A. Josang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 9, no. 3, pp. 279–311,2001.

[12] "A subjective metric of authentication", in Proceedings of European Symposium on Research in Computer Security (ESORICS'98). LNCS, Springer-Verlag, 1998.

[13] "Prospective for modelling trust in information security," in Proceedings of Australasian Conference on Information Security and Privacy, 1997, pp. 2–13,http://citeseer.nj.nec.com/josang97prospectives.html.

[14] S.J. Lee, M. Gerla and C.K Toh. A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks, IEEE Network, Jul. 1999.

[15] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molna, "The Eigen trust algorithm for reputation management in p2p networks," in Proceedings of the 12th International World Wide Web Conference (WWW '03), Budapest, Hungary, 2003.

[16] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," in Proceedings of the European Symposium on Research in Computer Security. Brighton, UK: Springer-Verlag, 1994,pp. 3–18.

[17] R. Yahalom, B. Klein, and T. Beth, "Trust relationships in secure systems – a distributed authentication perspective," in Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy (RSP '93),1993, pp. 150–164.

[18] A. Abdul-Rahman and S. Halles, "A distributed trust model," in Proceedings of New Security Paradigms Workshop '97, 1997, pp. 48–60.

[19] Y. Teng, V. V. Phoha, and B. Choi, "Designof trust metrics based on dempster-shafer theory", http://citeseer.nj.nec.com/461538.html.

[20] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen, "Trust propagation in small worlds," in Proceedings of the 1stInternational Conference on Trust Management, 2002,http://citeseer.nj.nec.com/575876.html.

[21] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks", in Proceedings of the Security Protocols Workshop. Cambridge, UK: Springer-Verlag, April 2002,http://citeseer.nj.nec.com/eschenauer02/trust.html.

Partha Sarathi Banerjee obtained his B.Tech in Electronics & Communication Engg. from Kalayni Govt. Engg. College in 2002. He passed M.Tech in Computer Technology from Jadavpur University, Kolkata in 2006. He is currently working as an Assistant Professor in the Department of Information Technology in Kalyani Government Engineering College. He has more than 7 years of experience in research and academics. His current research interest is Soft-computing models, Wireless Communication, Network security. He has 10 research publications in reputed National/International journals and conferences.

Dr. J. Paul Choudhury is an Associate Professor and Head of the department of Information Technology of Kalyani Govt. Engg. College, Nadia, West Bengal. He obtained B.E in Electronics and Telecommunication Engg. From Jadavpur University in 1979. He did his M.Tech form IIT Kharagpur in 1982. He obtained Ph.D (Engg) from Jadavpur University in 2002. He is equipped with an excellent blend of industrial and academic experience of more than 30 years. He has more than 70 research paper published in National/International journals and conferences. His current research areas are soft-computing techniques, optimization techniques, data mining, image processing and networking. He is life member of Institute of Engineers (IE), Computer Society of India (CSI) and IETE.

Dr. Sekhar Ranjan Bhadra Chaudhuri (04/11/1952) is a Professor in the Dept. of Electronics & Telecommunication Engineering, Bengal Engineering & Science University , Shibpur, West Bengal, India. He obtained B.E. Degree and M.E. Degree in Electronics and Telecommunication Engineering from the then B.E.College under Calcutta University in the seventies. He also obtained M.B.A. degree from the Indian Institute of Social Welfare and Business Management under University of Calcutta & Ph.D. Degree in Engineering from Jadavpur University in eighties.

In the earlihood of his career, Dr. Bhadra Chaudhuri was associated with the Telecommunication Industries. Afterwards, he joined with what is now known as Bengal Engineering & Science University (BESU), Shibpur, West Bengal, India, as Faculty Member in the Dept. of Electronics & Telecommunication Engineering (E&TC Engg.) in April,1982 & continuing till date as „Professor „ thereon since 1989. Dr.S.R.Bhadra Chaudhuri was the

Head of the Dept.of E&TC Engg., BESU,Shibpur, during 2008-2010.

His current research areas are Microwave, Communication, Small Antennas & Information Security .He has got 90 research publications in the International / National Journals & Conferences at his credit. He has guided three (3) Ph.D.(Engineering) Research Scholars & at present seven(7) research scholars are pursuing their Ph.D. works under his guidance . He is also the joint inventor of one Indian Patent (Digital Isolation Meter) in which the beneficiary is BESU.