International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:8, 2015

An Enhanced Associativity Based Routing with Fuzzy Based Trust to Mitigate Network Attacks

K. Geetha, P. Thangaraj

***Abstract*—**Mobile Ad Hoc Networks (MANETs) is a collection of mobile devices forming a communication network without infrastructure. MANET is vulnerable to security threats due to network's limited security, dynamic topology, scalability and the lack of central management. The Quality of Service (QoS) routing in such networks is limited by network breakage caused by node mobility or nodes energy depletions. The impact of node mobility on trust establishment is considered and its use to propagate trust through a network is investigated in this paper. This work proposes an enhanced Associativity Based Routing (ABR) with Fuzzy based Trust (Fuzzy- ABR) routing protocol for MANET to improve QoS and to mitigate network attacks.

***Keywords*—**Mobile Ad hoc Networks (MANET), Associativity Based Routing (ABR), Fuzzy based Computed Trust.

I. Introduction

MANETs are a prevalent research area in recent years due to challenges poses to the related protocols. MANET is an emerging technology enabling users to communicate without any infrastructure, regardless of geographical location and hence it is also called an infrastructure less network. Increase of cheaper, small and powerful devices makes MANET the fastest growing network [1]. MANET is more vulnerable than wired networks due to mobile nodes, threats from compromised nodes within the network limited security, dynamic topology, scalability and the lack of central management. MANETs due to these vulnerabilities are prone to malicious attacks [2]. MANET communication is through the use of multi-hop paths.

MANET nodes share a wireless medium and network topology changes erratically and dynamically. Communication breakdown in MANET is frequent, as nodes freely move anywhere. Node density and number depend on applications which use MANETs [3]. MANETs applications are diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks limited power sources. Mobile nodes dynamically self-organize in a temporary network topology [4]. MANET security needs authentication, key establishment and distribution and encryption. Routing protocols assume pre-existence/pre-sharing of public/secret keys for initial members. The protocols neglect key exchange and authentication, important in MANETs [16].

Trust is important as an attack which has already taken place could make an adversary try to destroy relief operations by compromising first responder system [5]. A Trust based packet forwarding in MANETs is sans a centralized infrastructure. It uses trust values to favour the packet forwarding by maintaining trust counter for nodes. A node is punished/rewarded by decreasing/increasing a trust counter [6].

Trust value is calculated for a node based on its success/failure transmission rates. The trust value identifies whether a node is reliable to perform routing or unreliable for the current transmission. Trust based routing identifies and eliminates misbehaving MANET nodes performing efficient and effective routing [7]. So, trust is adopted in routing protocols to secure nodes and data transmission. Different trust based routing protocols provide security in MANET by securing routing path nodes [8]. A drawback in locating a route based trust is route discovery efficiency. A network node stores other node's trust values. A node's trust value is computed/updated by trust agents residing in network nodes [9]. The MANET environment trust model is hard to assess due to many uncertainties.

The fuzzy logic theory extends mathematical research ontology to be a composite leveraging quality/quantity and having some fuzziness. Introducing fuzzy logic into trust management research combines collaborative filtering, to solve issues connected to MANET trust management uncertainty [10]. In this model, a passive acknowledgment (monitored node's packet forwarding ratio) is a single observable factor to assess trust [11].

Quality of Service (QoS) refers to network aspects that allow transport of traffic with special requirements. QoS guarantees are important when network capacity is insufficient, especially for real-time streaming multimedia applications, as these needs fixed bit rate and are delay sensitive and networks with the limited resource capacity [12]. QoS routing strategies are split into source routing, distributed routing, and hierarchical routing.

QoS based routing is challenging in MANETs, as nodes should update link status information. Also, due to MANETs' dynamic nature, maintaining precise link state information is difficult. QoS routing should locate a feasible new route to recover service [13]. Most protocols provide QoS support for a given path's available bandwidth requirement.

This is because bandwidth is a critical MANET application parameter due to this resource scarcity in a wireless environment [14]. QoS routing requires finding a route from source to a destination which satisfies end-to-end QoS requirement, given regarding bandwidth or delay. QoS is harder to guarantee in adhoc networks than in other networks,

Dr.P.Thangaraj, HOD, is with the Dept. of. CSE, Bannari Amman Institute of Technology, Tamil Nadu, India.

Mrs. K. Geetha, Assistant Professor, is with the Dept. of. IT, Excel Engineering College, Tamil Nadu, India (e-mail: geetharajsri@gmail.com).

as wireless bandwidth is shared by adjacent nodes and network topology changes as nodes move [15].

This paper used a fuzzy trust approach to improve QoS in MANET. The rest of this paper is summarized as follows: Section II discusses related work. Section III explains the methodology. Section IV discusses the experimental results, and Section V concludes the paper.

II. Literature Review

Ad hoc Traversal Routing (ATR) to ensure interoperability between different networks was proposed by Fujiwara et al., [17]. With ATR, two nodes in different networks can communicate seamlessly. ATR connects different networks by converted control messages from a network to another and adds a different network node address into routing protocols routing tables. The simulation evaluated ATR performance in a heterogeneous wireless network environment in a vehicle ad hoc network, wireless mesh networks, and a MANET.

Different cooperation, enforcement mechanisms for MANET were proposed by Othman & Weber [18], but most needed a node to maintain the memory of past interactions. This is a major problem in open/large MANETs. The proposed tag-based cooperation, enforcement mechanism ensured cooperation to be enforced in MANET without maintaining memory.

A novel group key agreement scheme for MANET based threshold secret sharing was proposed by Li-Qing & Rong-lin [19]. The key management and agreement are completed by multiple subgroup key managers and group key managers of all MANET users which avoids a single point of failure. All MANET members collaborate to conduct a final group session key through use threshold cryptography. The analysis revealed that the new scheme satisfied key agreement security requirements and were efficient in computation and members storage cost.

The trust based and cryptographic approaches for implementing security in MANET routing was compared by [20]. MANET design issues are in trust based routing protocols. A survey on trust based MANET routing protocols was presented providing directions for future research in trust based MANET routing.

The User-Controllable MultiLayer Secure Algorithm (UMSA) to authenticate MANET nodes before joining existing MANET or new MANET formation using user information, application layer, network layer and the data - link layer was introduced by [21]. Results showed that UMSA enhanced MANET security without negatively impacting the routing algorithm's performance.

A scheme to configure a MANET based on autonomous clustering and P2P overlay network to enhance MANET connectivity was proposed by [22]. Autonomous clustering divides a MANET dynamically into multiple sub networks, called clusters and elects a cluster head for each cluster. In the new scheme, cluster heads exchanges control packets periodically with each other to configure/maintain a P2P overlay network. The simulation proved that the new scheme achieved high connectivity between MANET nodes due to the P2P overlay network and autonomous clustering.

The role of trust overlays and its management is a systematic approach to build a trust overlay in MANET for privacy preservation was schematized by [23]. Increasing trust computing hardware availability of open systems includes portable computers and mobile devices. Tremendous challenges like how to set compatible security policies across administrative domains and how to derive a trust coefficient to build trust in MANET remain.

A subjective trust estimation model that included indicators was represented by intuitionistic fuzzy sets, and subjective trust was measured with intuitionistic fuzzy similarity by [24]. So, a MANET subjective trust based clustering algorithm with intuitionistic fuzzy sets (CAST) was proposed. Results proved that the clustering algorithm is adaptive to MANET and could compensate for defects in other clustering algorithms. The simulation showed that CAST had fewer communication costs and better safety than other clustering algorithms.

Trust concepts and properties derived unique trust characteristics in MANETs, drawing on social trust notions as discussed by [25]. A survey of MANET trust management schemes generally accepted classifications, potential attacks, performance metrics and trust metrics in MANETs. Finally, future research areas in MANET trust management was based on social and cognitive network concepts.

A new novel Improved QoS On-Demand Multicast Routing Protocol (IQoS-ODMRP) by adding two new characteristics to multicast routing protocols with QoS considerations was proposed by [26]. IQoS-ODMRP protocol increased packet delivery ratio and decreased end-to-end delay. The simulation confirmed the proposed protocol's validity.

An efficient QoS-aware routing protocol (QARP) which used a cross-layer communication (CLC) and session admission control (SAC) to provide QoS guarantees regarding network bandwidth was proposed by [27]. QoS-aware route discovery considered the effects of inter and intra-contention during route discovery in QARP. Current periodic message structures are extended to exchange nodes QoS states to reduce the mobility effect in QoS-aware routing method. Also, two methods to handle QoS violations caused due to video traffic and network mobility, dynamic characteristics during data communication were proposed.

An end-to-end QoS guaranteed approach in Cognitive MANETs was proposed by [28]. QoS parameters are a fitness function, and tunable parameters are encoded in the chromosome. This algorithm searched tunable parameter values which optimize QoS parameters. Results showed that approach as being effective and working well during rapid when topology changes.

A MANET routing protocol considering QoS parameters like bandwidth efficiency, link stability and power metric was proposed by [29]. The enhanced route determining process version leads to tremendous QoS improvement. The learning algorithm in current MAODV protocol further enhances QoS in MAODV. The simulation showed that the new system performed better than current systems regarding improving QoS.

A framework, which improved MANET QoS through data replication proposed by [30], aimed to support critical requirement applications based on MANETs like disaster management scenarios where data retrieval is critical to support real time decision making. Many replication techniques to optimize hops needed to retrieve data in MANETs suggested to comprise probabilistic, fuzzy logic and the optimization techniques to achieve an intelligent replica distribution at MANETs nodes.

III. Methodology

This work uses a fuzzy trust approach to improve MANET QoS. Input parameters are specified fuzzy to find whether a route is selected.

A. Associativity Based Routing Protocol (ABR)

Associativity Based Routing (ABR), a bandwidth efficiently distributed routing protocol in Ad Hoc networks is a source-initiated On-Demand routing protocol. ABR uses point-to-point and broadcast routing. The destination node in ABR chooses a route basing on "Associativity", the selected route is used, and other routes discarded resulting in long-lived routes as the decision is made on "Associativity". ABR has three phases, which are route discovery, route re-construction (RRC) and route deletion [31].

The route discovery phase in ABR: Route discovery uses broadcast query BQ messages and await a reply [BQ_REPLY] messages. A BQ message has a unique identifier. A source node desiring a destination route broadcasts BQ messages to a network. An intermediate node on receipt of the query checks if the packet is processed: if yes, query packet is discarded, otherwise it checks if the node is the destination. If not, the intermediate nodes append the following information before broadcasting a BQ message:

- Its address
- The associativity ticks with its neighbors
- The route relaying load,
- The link propagation delay
- The hop counts information.

The next intermediate node then erases its upstream neighbour's associativity ticks retaining only those concerned with itself and its upstream neighbour [35].

The route re-construction phase in ABR: route reconstruction (RRC) may include operations like invalid route erasure, partial route discovery, valid route update and new route discovery. If the source movement causes a RRC, a new route discovery procedure is initiated, and source sends a route notification (RN) message to erase route entries concerning out-of-date routes. When a destination moves, its immediate upstream node erases routing entry associated with the destination. A localized query (LQ) is then sent by the immediate upstream node to check if the destination is reachable. The hop number of the node to a destination is included in LQ. When the destination receives an LQ, it selects the best partial route before replying [32].

Route reconstruction phase includes:

- Partial route discovery
- Invalid route deletion
- Valid route updates
- New route discovery

The route deletion phase in ABR: When a discovered route is not desired, a source node initiates a Route Delete (RD) broadcast enabling nodes on a route for updating their routing tables. Then the RD message is propagated by a full broadcast as against a directed broadcast, as the source node may be unaware of route node changes that occurred during route re-construction.

A route is selected based on the degree of association stability of mobile nodes in this routing protocol. A node generates beacons periodically to announce its existence. On receipt of a beacon message, a neighbour node updates its associativity table. For every beacon received the receiving node's associativity ticks with the beaconing node increases. A high value of associativity tick for a specific beaconing node means that the node is relatively static. Associativity tick is reset when a neighbouring node moves away from the neighbourhood of another node [33].

ABR's benefits:

- Stable routes have higher preference compared to shorter routes.
- The fewer path breaks, reducing flooding.
- A broken link is repaired locally so that source node does not new path-finding-process when broken link appears.

ABR's Limitations:

- Sometimes a chosen path may be longer than the shortest path, due to the preference for stable paths.
- Stability information is used only during route selection.
- Local query broadcasts result in high delays during route repair [34].

B. Fuzzy Based Trust Computation

Trust computations comprise 'experience', 'recommendation' and 'knowledge' components. A trust's 'experience' component for a node is directly measured by immediate neighbours and regularly updated in a trust table. The present trust table is propagated to other nodes as the trust's 'recommendation' part. At regular intervals, previously evaluated trust is included in total trust's current 'knowledge' component. The three components individually or combined are used in trust computing.

A packet routing and acknowledgement schemes based trust establishment strategy is for adhoc networks. The trust of a particular node x is calculated by node y as:

$$T = W(R_p) \times R_p + W(R_q) \times R_q + W(R_e) \times R_e + W(D) \times D$$

where W(.) is a weight assigned to a specific event, R_p, R_q, R_e *and* D are normalized route reply misbehaviour factors, route request misbehaviour factors, route error misbehaviour factors and data delivery misbehaviour factors respectively. Values of R_p, R_q, R_e *and* D are determined as follows:

$$R_p = \frac{R_{ps} - R_{pf}}{R_{ps} + R_{pf}}$$

$$R_q = \frac{R_{qs} - R_{qf}}{R_{qs} + R_{qf}}$$

$$R_e = \frac{R_{es} - R_{ef}}{R_{es} + R_{ef}}$$

$$D = \frac{D_s - D_f}{D_s + D_f}$$

where R_{ps}, R_{qs}, R_{es} *and* D_s are successful: route reply acknowledgement packets, route request acknowledgement packets, route error acknowledgement packets and data delivery acknowledgement packets, respectively. Similarly R_{pf}, R_{qf}, R_{ef} *and* D_f are the numbers of failed packets [36].

When node i ask node j for a packet transmission of data or link information, node i finds it difficult to evaluate whether node j can provide the service at a specific time or whether service provided by node j is secure and trustworthy. Then, the situation is judged and monitored by node i from the history interaction records of node j.

Let C(t) represent the capability of a requested node (node j) on providing packets transfer services at time t, including the remnant utilization ratio of battery, CPU cycle, local memory and bandwidth at that point. Let H(t) represent at time t, history behaviours to offer services between past time intervals like packet-drop ratio. Let TL(t+1) refer to a node's trust level at time t+1. Assume the fuzzy member function of C(t) consists of three fuzzy sets: LOW(L), Medial(M) and High(H). The fuzzy membership function of H(t) and TL(t+1) comprises four different levels of fuzzy sets: LOW(L), Medial(M), High(H) and VeryHigh(VH).

According to the social control theory, the fuzzy inference rules establish a mapping from H×C to TL based on the analysis of a node's current condition and historic behaviour. When an overloaded node lacks CPU cycles, buffer space or available network bandwidth to forward packets, it will be untrustworthy in the next time interval due to low capability levels, even if its historic trust level is high. This is only the first rule, and an inference relationship is concluded with R_l:

$$R_l = H_t \times C_t \times TL_{t+1}$$

and for $\forall$ h ∈ H, c ∈ C, u ∈ TL,

$$\mathrm{R_l}(\mathrm{h,c,u}) = \mathrm{H}(h) \wedge C(c) \wedge TL(u)$$

For all n rules, we have a fuzzy inference relationship as

$$R(h,c,u) = \bigvee_{l=1}^{n} R_l(h,c,u)$$

For each pair of given input H* and C*, use the general total relationship R, where an output can be calculated:

$$TL^* = \left(H^* \times C^*\right) \circ R$$

Then, with the maximal membership degree approach, trust value, is calculated with defuzzy methods [37].

IV. Experiment Results

Experiments are conducted for varying mobility, speed of the nodes (10, 30, 50, 70 and 90 Kmph). The maliciousness in the network is varied 10%, 20% and 30%. ABR and the proposed Fuzzy ABR are simulated in these scenarios and its performance with regard to the number of hop count, end to end delay and packet delivery ratio is evaluated. Following table and figures depict the simulation results.

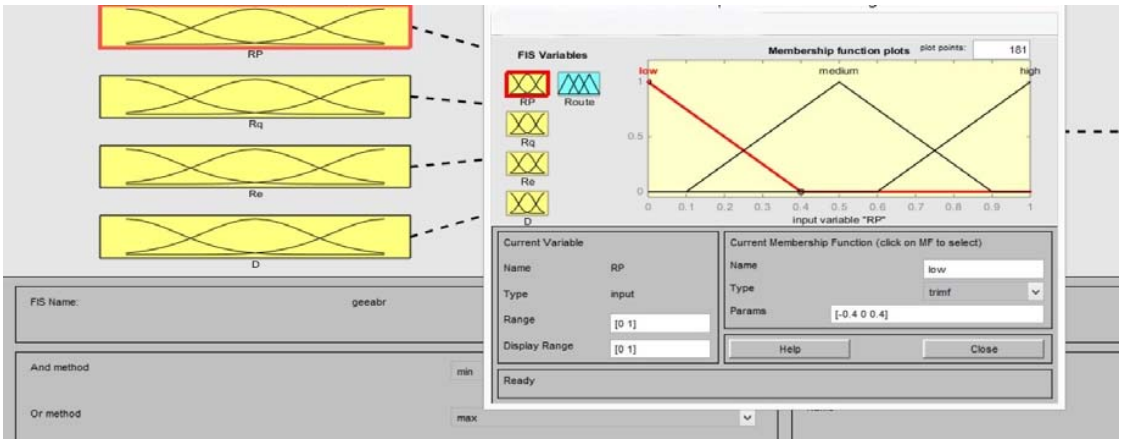

Fig. 1 The Proposed Fuzzy Membership Functions

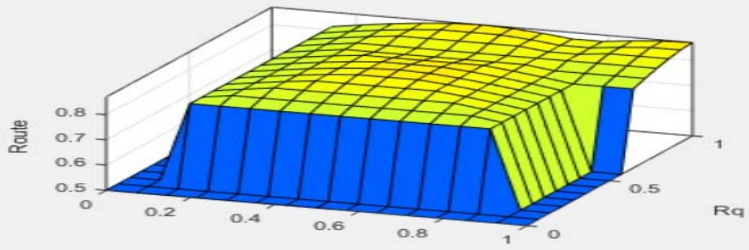

Fig. 2 Three Dimensional Representation of the Input with Respect to Output

TABLE I
NO OF HOPS TO DESTINATION FOR ABR

Node Mobility In Kmph	ABR	ABR - With 10% Maliciousness	ABR - With 20% Maliciousness	ABR - With 30% Maliciousness
10	2.8	3.1	3.3	3.5
30	3.1	3.4	3.6	3.8
50	3.7	4.1	4.3	4.4
70	4.1	4.4	4.7	4.7
90	4.3	4.6	4.9	4.9

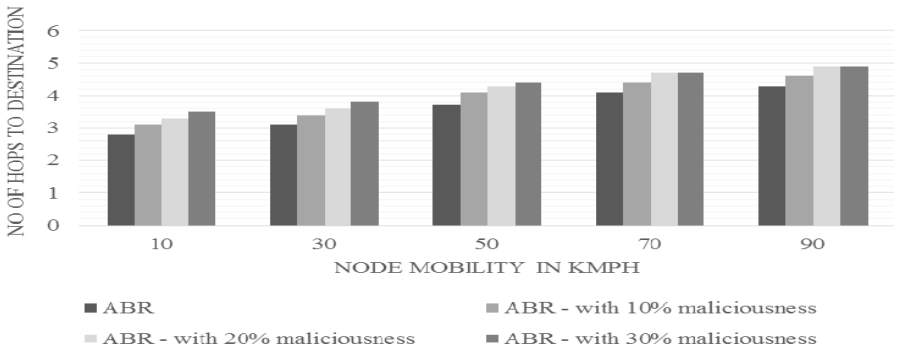

Fig. 3 No of hops to destination for ABR

It is perceived from Fig. 3 that the Number of hops to a destination for ABR increased with the increase in mobility speed and maliciousness. It is seen that the mobility has great impact on the Number of hops to destination, as the mobility increases from 30 to 90 kmph the Number of hops to destination increases by 10.1695% to 42.2535% when compared with 10 kmph speed in a non-maliciousness network.

It is perceived from Fig. 4 that the Number of hops to a destination for the proposed Fuzzy ABR increases with the increase in mobility speeds and maliciousness. As mobility increases from 30 to 90 kmph, the number of hops to destination increases by 10.1695 to 40% when compared with 10 kmph speed in a non-maliciousness network. The Number of hops to destination increases significantly more with the increase in maliciousness in the network. When compared to ABR, the proposed Fuzzy ABR on an average has similar number of hops to the destination when the network has no malicious nodes, whereas in a malicious network by 30% the proposed Fuzzy ABR achieves decreased Number of hops to destination by 2.8986 to 2.0619% than ABR.

It is perceived from Fig. 5 that the end to end delay for ABR decreased with the increase in mobility speed and maliciousness. It is seen that the mobility has great impact on the end to end delay, as the mobility increases from 30 to 90 kmph the end to end delay decreased by 16.7558% to 41.6025% when compared with 10 kmph speed in a non-maliciousness network.

TABLE II
NO OF HOPS TO DESTINATION FOR FUZZY ABR

Node Mobility In Kmph	Fuzzy ABR	Fuzzy-ABR - With 10% Maliciousness	Fuzzy-ABR - With 20% Maliciousness	Fuzzy-ABR - With 30% Maliciousness
10	2.8	3.1	3.3	3.4
30	3.1	3.3	3.3	3.8
50	3.6	3.8	3.9	4.3
70	4.2	4.2	4.6	4.6
90	4.2	4.5	4.6	4.8

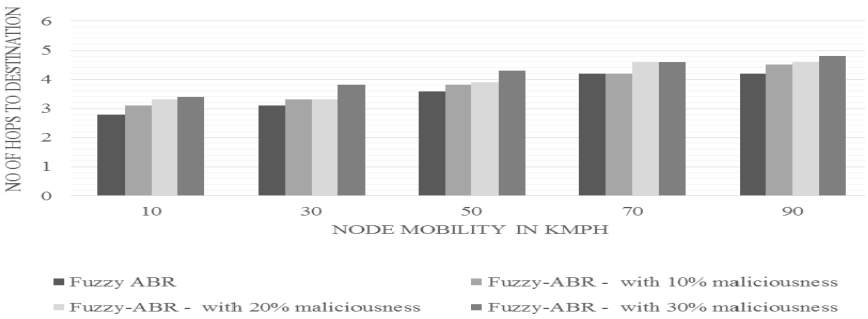

Fig. 4 No of hops to destination for Fuzzy ABR

TABLE III
END TO END DELAY FOR ABR

Node Mobility In Kmph	ABR	ABR - With 10% Maliciousness	ABR - With 20% Maliciousness	ABR - With 30% Maliciousness
10	0.0514	0.0566	0.0624	0.0688
30	0.0608	0.067	0.0738	0.0813
50	0.0684	0.0754	0.0831	0.0916
70	0.0726	0.08	0.0882	0.0972
90	0.0784	0.0864	0.0952	0.1049

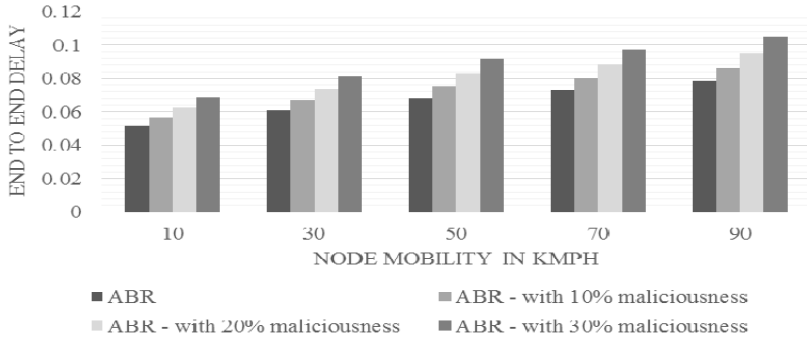

Fig. 5 End to End Delay for ABR

TABLE IV
END TO END DELAY FOR FUZZY ABR

Node Mobility In Kmph	Fuzzy ABR	Fuzzy-ABR - With 10% Maliciousness	Fuzzy-ABR - With 20% Maliciousness	Fuzzy-ABR - With 30% Maliciousness
10	0.0516	0.0558	0.062	0.0675
30	0.0602	0.0668	0.0736	0.0791
50	0.0688	0.075	0.0808	0.0888
70	0.0733	0.0781	0.0873	0.0941
90	0.0789	0.0851	0.0944	0.1027

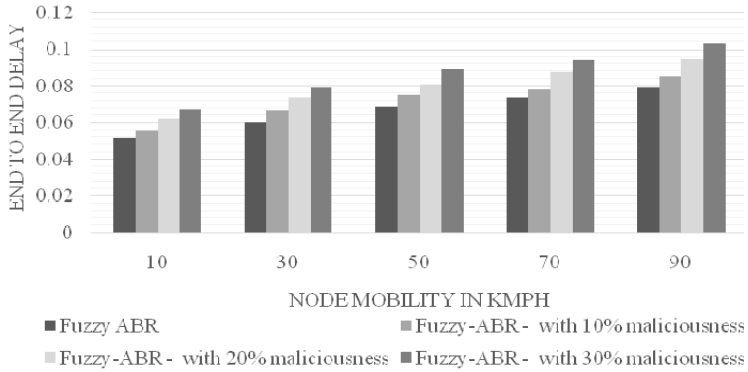

Fig. 6 End to End Delay for Fuzzy ABR

It has been perceived from Fig. 6 that the end to end delay for the proposed Fuzzy-ABR decreased with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph, the end to end delay decreased by 15.3846% to 41.8391% when compared with 10 kmph speed in a non-maliciousness network. When compared to ABR, the proposed Fuzzy-ABR has more end to end delay in the range of 0.3883% to 0.9917% when the network has no malicious nodes, whereas in a malicious network of 30% the proposed Fuzzy-ABR decreased delay of 1.9076% to 3.241% than ABR.

TABLE V
PACKET RATIO DELIVERY FOR ABR

Node Mobility In Kmph	ABR	ABR - With 10% Maliciousness	ABR - With 20% Maliciousness	ABR - With 30% Maliciousness
10	0.90278	0.8279	0.7593	0.6964
30	0.8948	0.8206	0.7526	0.6902
50	0.8642	0.7926	0.7269	0.6666
70	0.8321	0.7631	0.6998	0.6418
90	0.8144	0.7469	0.685	0.6282

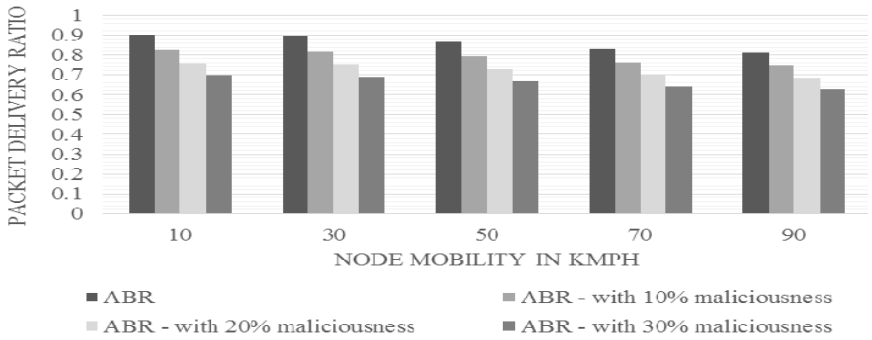

Fig. 7 Packet Ratio Delivery for ABR

It is observed from Fig. 7 that the packet delivery ratio for ABR increased with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph the packet delivery ratio increased by 0.8879% to 10.2936% when compared with 10 kmph speed in a non-maliciousness network.

TABLE VI
PACKET DELIVERY RATIO FOR FUZZY ABR

Node Mobility In Kmph	Fuzzy ABR	Fuzzy-ABR - With 10% Maliciousness	Fuzzy-ABR - With 20% Maliciousness	Fuzzy-ABR - With 30% Maliciousness
10	0.935	0.8561	0.7903	0.7284
30	0.9498	0.8321	0.7835	0.7142
50	0.9093	0.8305	0.7444	0.6682
70	0.8519	0.8151	0.7182	0.6722
90	0.8621	0.7948	0.7389	0.6643

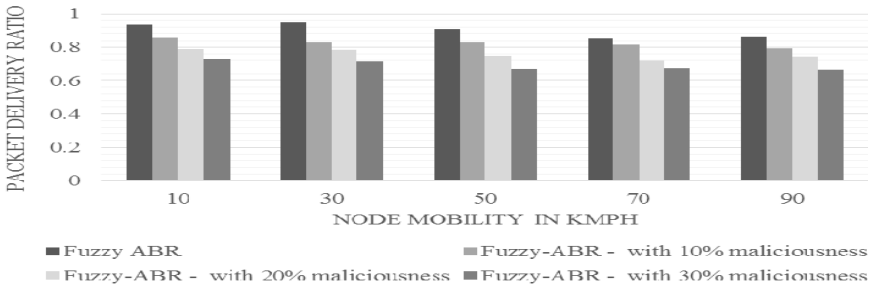

Fig. 8 Packet Delivery Ratio for Fuzzy ABR

It is perceived from Fig. 8 that the packet delivery ratio for proposed Fuzzy ABR increased with the increase in mobility speed and maliciousness. As the mobility increases from 30 to 90 kmph, the packet delivery ratio increased by 1.5705% to 8.1131% when compared with 10 kmph speed in a non-maliciousness network. The packet delivery ratio increased significantly more in the increase in maliciousness in the network. When compared to ABR, the proposed Fuzzy ABR

has better packet delivery ratio in the range of 2.3515% to 5.9634% when the network has no malicious nodes, whereas in a malicious network of 30% the proposed Fuzzy ABR achieved higher packet delivery ratio of 0.2397% to 5.5861% than ABR.

V. Conclusion

MANETs must provide required QoS for delivery of real-time communications like audio and video which has varied technical challenges and new definitions. Trust is based on neighbourhood trust and recommendation based trust. Experiments in varied scenarios using ABR and the new method were conducted. Results showed the new approach's improved performance regarding the packet delivery ratio. The new Fuzzy ABR had a packet delivery ratio ranging between 2.3515% and 5.9634% when the network had no malicious nodes. In a 30%, malicious network, the new 3 Fuzzy ABR ensured a higher packet delivery ratio, which ranged between 0.2397% and 5.5861% compared to ABR.

References

[1] Bang, A. O., & Ramteke, L. P. (2013). MANET: History, Challenges And Applications. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(9), 249-251.

[2] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: Vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.

[3] Kumar, M., & Mishra, R. (2012). An Overview of MANET: History, Challenges and Applications. Indian Journal of Computer Science and Engineering (IJCSE), 3(1), 121-125.

[4] Bakshi, A., Sharma, A. K., & Mishra, A. Significance of Mobile AD-HOC Networks (MANETS).

[5] Virendra, M., Jadliwala, M., Chandrasekaran, M., & Upadhyaya, S. (2005, April). Quantifying trust in mobile ad-hoc networks. In Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS).

[6] Rajaram, A., & Palaniswami, D. S. (2009). A trust based cross layer security protocol for mobile ad hoc networks. arXiv preprint arXiv:0911.0503.

[7] Subramanian, S., & Ramachandran, B. (2012). Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks. arXiv preprint arXiv:1202.1664.

[8] Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 13(4), 562-583.

[9] Wang, C., Yang, X., & Gao, Y. (2005). A routing protocol based on trust for MANETs. In Grid and Cooperative Computing-GCC 2005 (pp. 959-964). Springer Berlin Heidelberg.

[10] Luo, J., Liu, X., Zhang, Y., Ye, D., & Xu, Z. (2008, October). Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks. InLCN (pp. 305-311).

[11] Duraimurugan, A., Karthi, S., & Kirupagaran, D. A Trust Based Secure Source Routing using Fuzzy Logic Rules Prediction in Mobile Ad Hoc Networks.

[12] Singh, Y., & Siwach, M. V. (2012). Quality of Service in MANET. Int. J. Innov. Eng. Technol.

[13] Upadhayaya, S., & Gandhi, C. (2009). Quality of service routing in mobile ad hoc networks Using location and energy parameters. Int. Journal of Wireless & Mobile Networks (IJWMN), 1(2).

[14] Jawhar, I., & Wu, J. (2005). Quality of service routing in mobile ad hoc networks. In Resource Management in Wireless Networking (pp. 365-400). Springer US.

[15] Zhu, C., & Corson, M. S. (2002). QoS routing for mobile ad hoc networks. InINFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 2, pp. 958-967). IEEE.

[16] Mamatha, T. (2012). Network security for MANETS. In International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2.

[17] Fujiwara, S., Ohta, T., & Kakuda, Y. (2012, June). An inter-domain routing for heterogeneous mobile ad hoc networks using packet conversion and address sharing. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on (pp. 349-355). IEEE.

[18] Othman, N. E., & Weber, S. (2011, October). Towards Tag-based cooperation for mobile ad hoc networks. In Reliable Distributed Systems Workshops (SRDSW), 2011 30th IEEE Symposium on (pp. 20-25). IEEE.

[19] Li-Qing, C., & Rong-lin, H. (2010, July). Group key agreement scheme for mobile ad hoc networks based on threshold secret sharing. In Electronic Commerce and Security (ISECS), 2010 Third International Symposium on (pp. 176-180). IEEE.

[20] Thorat, S. A., & Kulkarni, P. J. (2014, July). Design issues in trust based routing for MANET. In Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on (pp. 1-7). IEEE.

[21] Chze, P. L. R., Yan, W. K. W., & Leong, K. S. (2012, August). A User-Controllable Multi-Layer Secure Algorithm for MANET. In Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International (pp. 1080-1084). IEEE.

[22] Nakahara, S., Ohta, T., & Kakuda, Y. (2013, December). Experimental Evaluation of MANET Based on Autonomous Clustering and P2P Overlay Network. In Computing and Networking (CANDAR), 2013 First International Symposium on (pp. 480-483). IEEE.

[23] Joshi, S., Sheikh, R., & Mishra, D. K. (2010, September). Schematize Trust Overlays and Management for Privacy Preservation in MANET. In Computational Intelligence, Modelling and Simulation (CIMSiM), 2010 Second International Conference on (pp. 106-110). IEEE.

[24] Liao, J., Zhang, H., Jiang, L., & Liu, Y. (2011, April). A clustering algorithm based on subjective trust in MANET. In Electric Information and Control Engineering (ICEICE), 2011 International Conference on (pp. 3817-3820). IEEE.

[25] Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. Communications Surveys & Tutorials, IEEE, 13(4), 562-583.

[26] Jabbehdari, S., Shamaei, M., & Darehshoorzadeh, A. (2010, October). IQoS-ODMRP: A novel routing protocol considering QoS parameter in MANET. InIndustrial Electronics & Applications (ISIEA), 2010 IEEE Symposium on (pp. 126-130). IEEE.

[27] Lal, C., Laxmi, V., & Gaur, M. S. (2013, August). QoS-aware routing for transmission of H. 264/SVC encoded video traffic over MANETs. In Communications (APCC), 2013 19th Asia-Pacific Conference on (pp. 104-109). IEEE.

[28] Peng, H., Bai, Y., & Liu, X. (2012, March). End-to-End QoS Guaranteed Approach Using Multi-object Genetic Algorithm in Cognitive MANETs. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on (pp. 938-943). IEEE.

[29] Santhi, G., Nachiappan, A., Ibrahime, M. Z., Raghunadhane, R., & Favas, M. K. (2011, June). Q-learning based adaptive QoS routing protocol for MANETs. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on (pp. 1233-1238). IEEE.

[30] Kulla, E., Spaho, E., Xhafa, F., Barolli, L., & Takizawa, M. (2012, November). Using data replication for improving QoS in MANETS. In Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (pp. 529-533). IEEE Computer Society.

[31] Shaar, S. A., Masoud, F. A., Murad, A., Shalabi, R. A., & Kanaan, G. (2006). Analysis of enhanced associativity based routing protocol. Journal of Computer Science, 2(12), 853.

[32] Liu, C., & Kaiser, J. (2003). A survey of mobile ad hoc network routing protocols. Universität Ulm, Fakultät für Informatik..

[33] Sharma, S. K., Kumar, R., Gangwar, A., & Pakhre, K. Routing Protocols and Security Issues in MANET: A Survey.

[34] Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2), 46-55.

[35] Raja, J., & Santosh, S. (2013). Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET. IJECS, 2(3).

[36] Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: a survey. Communications Surveys & Tutorials, IEEE, 14(2), 279-298.

[37] Dai, H., Jia, Z., & Qin, Z. (2009). Trust evaluation and dynamic routing decision based on fuzzy theory for manets. Journal of Software, 4(10), 1091-1101.

Mrs. K. Geetha holds a M.E degree in Computer Science and Engineering from K. S. Rangasamy College of technology, affiliated to Anna University of Technology Coimbatore, Tamil Nadu, India in 2010. Now she is pursuing Ph.D at Anna University of Technology, Coimbatore. She is currently working as an Assistant Professor in the Department of Information Technology, Excel Engineering College. She has 8 years of teaching experience. She has published 6 international journals and presented three papers in the national and international Conferences. She is an active member of ISTE. Her Research interests include Mobile computing, Ad hoc Networks and Network Security.