RESEARCH ARTICLE OPEN ACCESS

A Novel Fuzzy based Decision system for efficient Cross-Layer Based Multicast Routing in Manets

M. Chandramouli Reddy [1], P. Venkata Krishna [2]
Department of Computer Science and Engineering
Mewar University
Rajasthan - India

ABSTRACT
This paper present the Novel approach for a cross-layer based multicast routing in Manets. Initially by using MAODV (Multicast Ad hoc On-demand Distance Vector) routing protocol the multicast tree is constructed. Here the transmission of the data from source to destination is performed based on the fuzzy systems. The fuzzy systems established an optimal route by considering the parameters like bandwidth and path stability. For the creation of the routing table the proposed system uses different type of the message for efficient routing. Based on the available distance, battery power and link quality the path stability will be estimated.

Keywords **:-** Routing, Multi Cast, Manets, Fuzzy and Cross layer.

I. INTRODUCTION

The MANETS has wireless devices for communication with mobile router called as nodes. This node will move freely and can be located at any places such as cars, planes, trucks, ships, etc. but these systems will be operated in isolation with the gateways of the fixed network. In MANET, there are three different types namely Vehicular **Ad hoc Networks (VANETs)** are used for communication among vehicles and between vehicles and roadside equipment. **Internet-based Mobile Ad hoc Networks (iMANET)** connect mobile nodes and fixed Internet-gateway nodes. Normal ad-hoc routing algorithms have no direct application in such types of network. **Intelligent Vehicular Ad hoc Networks (InVANETs)** constitute a kind of artificial intelligence that enables intelligent behaviour in vehicles during vehicle-to-vehicle collisions, accidents during drunken driving etc.

The MANETs have the characteristics like Dynamically changing network topology: In mobile ad hoc network, all nodes move freely anywhere in the network. The links fail between nodes when high mobility present in the network causing route failure in the network (Corson & Macker 1999). Self-organization: They have central administration mechanisms. The nodes should be able to form a network themselves. Here each node also acts a router (Rachik Mustapha et al. 2012). Limited resource availability: In mobile ad hoc networks, the resources are limited. Nodes operating powers and bandwidth constraint are the critical resources. Hence, optimizing all operations may reduce energy consumption and bandwidth may be constrained (Goyal et al. 2011). Limited physical security: These networks are generally more prone to physical security threats than are fixed and hardwired networks (Macker et al. 1998). Multi-hopping: Communication between two end nodes for transmitting data is carried out through a number of intermediate nodes whose function is to relay information from one point to another by multi-hopping (Macker et al. 1998). Network Scalability: Due to the mobility of nodes, the scale of ad-hoc network keeps changing all the time (Goyal et al. 2011). Scalability is a major problem in mobile ad hoc networks (Taneja et al. 2007).

MANETs find uses in various applications, ranging from small to large, static networks, dynamic networks such as (Jeroen Hoebeke et al. 2004, Mohit Kumar & Rashmi Mishra 2012).

- Military communication and operations
- Search and rescue operations
- Disaster recovery
- Replacement of fixed infrastructure if causing environmental disasters

- Policing and fire fighting
- Supporting doctors and nurses in hospitals
- Virtual classrooms
- Ad hoc communications during meetings or lectures
- Consumer electronics is embedded with smart sensors and actuators, and more.

MANET environment has to overcome certain issues of limitation and inefficiency. These issues are as follows (Vikram Patalbansi et al.): The wireless link characteristics are time varying in nature. These links have transmission barriers like fading, path loss, blockage, and nterference. Different factors can affect the reliability of wireless transmission. Limited radio band results in reduced data rates compared to the other wireless networks. Hence, optimal usage of bandwidth is necessary by keeping low overhead as possible. MANET experiences higher packet loss due to several factors such as hidden terminals that result in collisions, wireless channel issues (i.e. high Bit Error Rate (BER)), interference, frequent breakage in paths caused by the mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links. The dynamic nature of network topology results in frequent path breaks. The random movement of nodes often leads to the partition of the network. This mostly affects the intermediate nodes.

II. RELATED WORK

Loukas Lazos & Radha Poovendran (2007) have addressed the problem of group access in secure multicast communications for wireless ad hoc networks. In order to conserve energy, they have integrated the network topology, the power proximity between network nodes and the path loss characteristics of the medium in the key distribution tree design. They have also developed new algorithms for homogeneous and heterogeneous environments. They have shown that, when the medium is homogeneous, the node location can be used to design energy-efficient balanced key trees and when it is heterogeneous, they have developed algorithms that consider power proximity in the design of balanced key trees. Their cross layer approach has considered transmission power (energy) as a key parameter. Transmission power measurement is taken at the PHY layer. Their secure multicasting mechanism has not considered the mobility of nodes.

Vishwanath et al. (2010) have used artificial neural networks for a reliable secure multicast routing in mobile ad hoc networks. The method considers the selection of input Variables for the ANN, determines the optimum number of neurons for the hidden Layer selection of Multicasting using supporting nodes routing function. The proposed ANN model uses the feed forward network using back propagation algorithms. Their routing approach has not used any detailed methods for the security multicast mechanism. Furthermore, they have not described clearly about QoS metrics.

Chang & Kuo (2009) have proposed a two-step secure authentication for multicast MANETs. First, the Markov chain analysis was adopted for the analysis of each one-hop neighbor‟s TV based on its previous trust performance. The analyzed TV was then exchanged among all group members. The proposed trust model was recognized as an ergodic CTMC model. The node with the highest TV was then selected as a CA to manage the group‟s trust table. The node with the second highest TV was chosen for achieving high security and reliability of a multicast group as the BCA that takes over the CA when the CA fails abnormally. The message overhead and the worst-case time complexity of the trust determination model were analyzed. In addition, the procedures of the secure authentication for group management and several attacks were examined, which showed that the proposed approach has achieved secure reliable authentication in multicast MANETs.

Numerical results have indicated the exacted nature of the closeness of the analytical results to the simulation results of light, medium, and high TVs under different NDSs. Furthermore, the speed of the convergence of the analysis TV has shown the independence of the analyzed TV of the initial values and the trust classes, which is a noble feature for analytical models. Finally, by simulation, the number of times a node has acted as the NCA and the NBCA, and the NREJ of a node, have been examined. The results have contended that a node with a high TV yields high NCA and low NREJ, and vice versa.

Narsimha et al. (2008) have proposed the Ad hoc QoS Multicasting (AQM) protocol, which improves multicasting efficiency through QoS management. Their AQM protocol tracks the availability QoS within a node's neighborhood based on previous reservations and reveals it at the initiation of the session. This information is updated

during the joining process of the nodes and it is used to select routes that can satisfy the QoS requirements of the session. Thus, the efficiency of the multicast session is improved significantly by their AQM. They have also proposed a cross-layer framework to support admission control using the available bandwidth information. Their bandwidth estimation method estimates the available bandwidth without the need for any extra control overhead. Bandwidth availability was considered as a QoS metric by them. Multicast routing in MANET is sensitive to more attacks and vulnerabilities. However, their mechanism does not demand any steps for security. Further, calls having bandwidth below the threshold value will be rejected in line with their call admission control strategy.

III. PROPOSED METHOD

The proposed technique involves selection of optimal routes using the fuzzy logic system. The Fuzzy Logic System (FLS): Optimal Path Selection is chosen mainly due to the following two reasons:

c) No clear boundary exists in between the normal and abnormal events.

d) Fuzzy rules should level the normality and abnormality separation.

The proposed mechanism is described in the following section sequentially.

A. Multicast Tree Construction

Multicast Ad hoc On-demand Distance Vector (MAODV) routing protocol uses four different message types for the creation of the multicast routing table.

1. Route request (RREQ)
2. Route reply (RREP)
3. Multicast activation (MACT)
4. Group hello (GRPH)

The MAODV algorithm is described in algorithm 1.

Algorithm 1

1. When a node wants to join a multicast group, it initially selects itself as the group leader.
2. This group leader node periodically broadcasts „Group hello" message in the network so as to handle the sequence number, disseminate group information and to repair partitioned multicast tree.
3. When a node wants to discover a route towards a destination, it broadcasts an RREP and starts a timer which has a minimum duration equal to double the one hop time.
4. When a node is a member of the multicast tree and has a sequence number greater than the RREQ message, and receives an RREQ, it checks the Join flag. If the Join flag is set, it replies to the request in the form of RREP. If the Join flag is not set, but if the route is unexpired, then it can send RREP.
5. When the node does not get the reply before the timer expires, it rebroadcasts the RREQ by doubling the timer value, increasing the hop count by one and reducing TTL by 1.
6. When the node does not receive any reply from any of the nodes, it selects itself as the group leader.
7. When the group leader gets RREP from several nodes, it selects the next best hop node and informs it by sending an MACT message.
8. Once a node receives an MACT message, it updates its multicast routing table.

Thus, an effective multicast tree is developed using the MAODV algorithm.

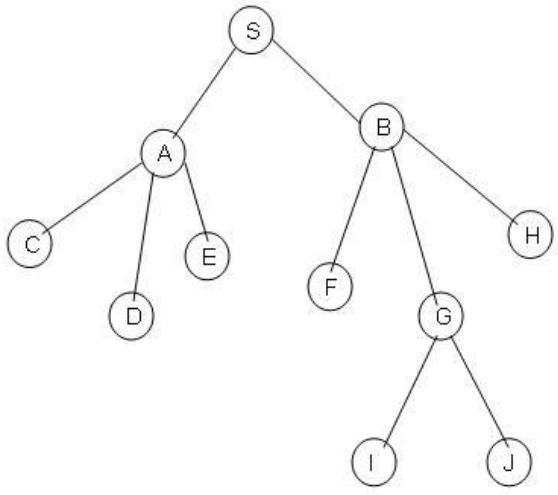


Fig 1: Multicast Tree Structure

A multicast tree structure is described in Figure 6.1. Node S is the group leader; nodes A, B and G are the intermediate nodes. A is the parent of node C, D, and E. Node B is the parent of nodes F, G and H. Node G is the parent of nodes I and J. Nodes C, D, E, F, I, J and H are the leaf nodes.

B. Algorithm for Optimal Path Selection

The steps involved the optimal path selections are as follows

Algorithm 2

1. When S wants to transmit a data packet to D, it verifies its route cache for path availability. If the path exists, then go to step 10; else, go to Step 2.
2. S broadcasts RREQ packet towards the D through the intermediate nodes (Ni)
3. Upon receipt of the RREQ, Ni updates the route cache about the source, destination, previous hop node, battery power, link quality and available bandwidth. Ni then either re-broadcasts the RREQ to its neighbors or sends the route reply (RREP) When the node is D. This process is repeated till RREQ reaches D.
4. When D receives RREQ, the RREP packet is unicast for every received RREQ in the reverse path towards the source.
5. Every Ni that receives RREP updates its cache for the next-hop of the RREP and then unicasts this RREP in the reverse-path using the earlier-stored previous-hop node information.
6. Step 6 is repeated till RREP reaches S.
7. S then computes path stability and bandwidth (Estimated in section 6.2.1 and 6.2.2) on the basis of collected information from RREP.
8. The values computed by S in step 8 are considered as inputs for the fuzzy logic system (Explained in section 6.4.1). Based on the result, S selects an optimal path that has high link stability and bandwidth value. This optimal path is used for data transmission between the source and the destination.
9. The path available in the route cache is considered for data transmission.

C. **Fuzzy Logic System (FLS)**

Fuzzy Logic System (FLS) involves the selection of an optimal path for data transmission. This is performed by considering the two inputs viz., path stability and bandwidth. These inputs are fuzzified to obtain the appropriate optimal path.

IV. RESULTS AND DISCUSSIONS

The performance of Cross-layer based Multicast Routing Protocol (CBMRP) technique is evaluated through NS2 [8] simulation. A random network deployed in an area of 1000 X 1000sqm is considered. The sink is assumed to be situated 100 meters away from the above-specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is CBR with UDP source and sink. The number of sources is fixed as 4 around a phenomenon.

4.1 Performance Metrics

The performance of CBMRP technique is compared with the PDTMRP [88]. The performance is evaluated mainly, on the basis of the following metrics.

- Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully to the total number of packets transmitted.

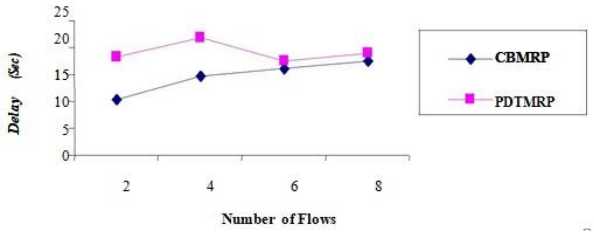
No. of Nodes	50,75,100,125,150
Area Size	1000 X 1000 sqm
Mac	802.11
Routing protocol	FBRRT
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Rate	100kb
Transmission Range	150m
Speed of events	5 m/s
Pause time	5,10,15,20 and 25 sec.
Flows	2,4,6 and 8

- Drop: It is the number of packets dropped during the transmission.
- Delay: It refers to the average end to end delay of packets.
- Overhead: It is the ratio of the number of packets rejected to the number of packets sent.

4.1 Results

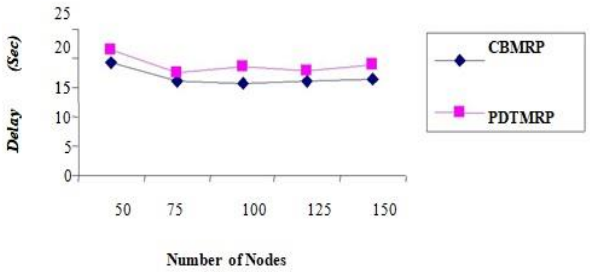
A. Based on Flows

In the initial experiment, the flows are varied as 2, 4, 6 and 8.



B. Based on Nodes

In the second experiment, the number of nodes is varied as 50, 75,100,125 and 150.



The inference when comparing the performance of the two protocols is that CBMRP outperforms PDTMRP by 43% in terms of delay, 31% in terms of delivery ratio, 74% in terms of packet drop and 42% in terms of overhead.

REFERENCES

[1] Abdrabou, A & Zhuang, W 2009, „Statistical QoS Routing for IEEE 802.11 Multihop Ad Hoc Networks", IEEE ansactions on Wireless Communications, vol. 8, no.3.

[2] Aditya Karnik, Ravi Mazumdar & Catherine Rosenberg 2006, „Rate Control and Dynamic Dimensioning of Multihop Wireless Networks", Information Sciences and Systems, 40th Annual Conference IEEE, pp.1-5.

[3] Alima Beebi, PK, Sulava Singha & Ranjit Mane, „A Study on Cross Layer MAC design for performance optimization of routing protocols in MANETs", International Journal of Advanced Computer Science and Applications IJACSA.

[4] Alqobaty, A, Shaheen, S & Ibrahim, S 2012, „A new cross layer based routing technique for mobile ad hoc networks using forwarding node selection," Computer Engineering & Systems ICCES, 2012 Seventh International Conference on, Cairo, pp. 9-15

[5] Ashraf, M 2009, „Rate Adaptive Channel MAC for Opportunistic Communication in Ad hoc Wireless Networks", IEEE/ACM Transactions on Networking.

[6] Asokan, R, Natarajan, AM & Venkatesh, C 2008, „Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service QoS Metrics in Mobile Ad Hoc Networks", IJCSS: International Journal of Computer Science and Security, vol. 2, no. 3, pp. 48-56.

[7] Badarneh, Osamah, S & Michel Kadoch 2009„„Multicast routing protocols in mobile ad hoc networks: a comparative survey and taxonomy", EURASIP Journal on Wireless Communications and Networking, vol.2009, p.26.

[8] Bani Yassein, M, Manaseer, S & Al-Turani, A 2009„„A Performance Comparison of Different Backoff Algorithms under Different Rebroadcast Probabilities for MANET"s", 25th UK Performance Engineering Workshop.

[9] Basu Dev Shivahare, Charu Wahi & Shalini Shivhare 2012, „Comparison of Proactive and Reactive Routing Protocols In Mobile Adhoc Network using Routing Protocol Property", International Journal of Emerging Technology and Advanced Engineering, vol. 2, issue 3, pp. 356-359.

[10] Benfattoum, Y, Martin, S & Agha, KA 2013„„QoS for Real-time Reliable Multicasting in Wireless Multi-hop Networks using a Generation-Based Network Coding. Computer Networks.

[11] Cameron Lesiuk, B 1998, „Routing in Ad Hoc Networks of Mobile Hosts", http://ghost.lesiuk.org/AdHoc/adhoc/#I5, pp. 01-20.

[12] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.

[13] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.

.