International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-3, March 2016

Time Base Control Model for Efficient Transmission in MANET

Harmanpreet Kaur, Puneet Kumar

***Abstract*— A mobile ad hoc network (MANET) is infrastructure less dynamic network consist of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Efficient data transmission is one of the major challenges in MANET. Data transmission is the most important concern for the basic functionality of network. The dynamic topology of MANETs allows nodes to join and leave network at any point. We proposed TBCM Approach for efficient data transmission.**

***Index Terms*— MANET, AODV, RREP, RREQ**

I. INTRODUCTION

MANET (mobile ad-hoc network) is basically a temporary wireless network made up of mobile nodes, in which infrastructure is not present. Mobile ad-hoc networks have dynamic topology and it is self-configurable network where the mobile nodes can move randomly. In MANET, Routing Protocols are used to establish communication within networks. These routing protocols help in finding different routes between nodes, in order to transfer data from source to sink. The main focus of routing protocol is on correct and efficient route establishment between nodes, so that messages can deliver within time. The networks are self organized and have limited bandwidth. In MANETs, the router connectivity may change frequently, leading to the multi-hop communication paradigm that can allow communication without the use of Base Station/Access Point, and provides alternative connections inside Hotspot cells [3].

MANET ARCHITECTURE

Harmanpreet Kaur, Student, M.Tech (CSE), PTU
Puneet Kumar, Assistant Professor, PTU.

The main routing protocols used for Manet are: Proactive (table driven), Reactive (on demand) & Hybrid (both reactive and proactive)

A. Proactive routing protocol:

In this protocol every node has the information of all other nodes in the network. All node information stores in the routing table that's why it is called table-driven. These protocols constantly maintain the updated topology of the network. Whenever there is any change in the network topology routing table are updated according to the change [1]. Many types of proactive protocols like OLSR, DSDV, and OSPF etc.

B. Reactive routing protocol:

Routes are found when there is a need (on demand). Hence, it reduces the routing overhead. It does not need to search for and maintain the routes on which there is no route request. The source node should wait until a route to the destination is discovered [2]. E.g AODV, DSR.

C. Hybrid routing protocol:

Hybrid protocols have the strength of both reactive and proactive protocols. In this protocol, network is divided into zones and different protocols use in different zone. One is used within the zone and other is used between the zones. In this protocols proactive mechanism use for route establishment and reactive protocol use for communication amongst the neighborhood node [1]. E.g ZRP.

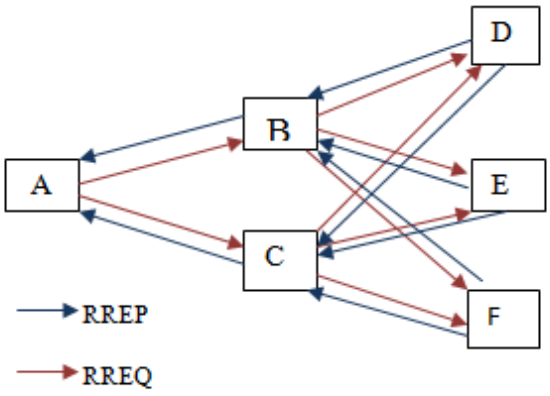
II. ADHOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV):

Ad hoc on demand distance vector (AODV) is a reactive protocol. So, it creates path from source to destination when it is required. AODV uses control messages to find the destination. These are:-

1. Route request message (RREQ)
2. Route reply message (RREP)
3. Route error message (RERR)
4. Hello message

In AODV, every node maintains a routing table containing next hop node information for a router to the destination node. . If node wants to send data packet to some destination, it first checks the route to that destination from source, if there is no route present between source and destination. Then, first by route discovery method route is established between source and destination for data delivery. Source node broadcast RREQ message to its neighbors, node which receive RREQ

may send RREP to source if it is destination node or it has route to destination with corresponding sequence number greater than or equal to that contained in the RREQ. 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. When source node receive RREP message from destination node route is established between source and destination, then HELLO message generate by source to destination through newly discovered route to check before the data transmission, then source send data through this route to destination. If due to any reason topology change or node die, then link failure occurs and RERR message send to source. After receiving the RERR, if the source node still desires the route, it can of AODV is that less memory space is required as information of only active routes are maintained in turn increasing the performance. While the disadvantage is that this protocol is not scalable and it is not efficient for large networks. The control messages consume lot of energy and causes bandwidth wastage. This also leads to delay in transferring the data packets from source to destination.



AODV RREQ/RREP PROCESS

III. RELATED WORK

Vaibhav Suhane, Mahesh Gaur and Sadhna K.Mishra et al. [1] proposed new protocol EAODV, which is an enhanced AODV and it is used to detect and prevent network from various attacks. The performance of the EAODV protocol is compared with the existing AODV routing protocol with variation in Pause time and Node speed.

Iftikhar Ahmad, Uzma Ashraf, Sadia Anum and Hira Tahir et al. [4] they developed an algorithm with an enhanced route discovery mechanism that avoids the pre-transmission delay. EAODV give priority to the source node of RT transmission. When RREQ packet sends to neighbor node, for RT transmission it accept route request on priority basis and starts the RT transmission.

Anumeha, Bhawna Mallick et al. [2] proposes an adaptive routing algorithm in MANET using modified AODV by calculating the loads on different routes using given parameters like aggregate interface queue length and nodes remaining energy. They try to enhance the AODV network performance, when frequent link failures in network due to mobility of the nodes.

Miral V. Vora, Prof. Jignesh H. Joshi et al. [10] states that source node does not send any data packet; until no enough energy (battery life time) of intermediate node and received RREP of its neighboring exceeds a particular threshold. They also suggested two approaches for making energy efficient algorithm. First, changes proposed in route request phase to make it energy efficient. Second, changes proposed in timer variation to make it energy efficient.

Madhvi Saxena, Neha Jain et al. [8] proposed an algorithm to improve the network lifetime in Manet. MAODV a new approach is developed by modifying the standard of AODV routing protocol. By using this algorithm the source node will select energy efficient path and this helps in reducing the broadcasting of packet so, energy of the network gets consumed and it provides energy efficient network.

Reena Singh, Shilpa Gupta et al. [6] proposes an EE- AODV routing protocol. This algorithm has enhanced the RREQ and RREP handling process to save the energy in mobile devices. EE-AODV considers some level of energy as the minimum energy which should be available in the node to be used as an intermediary node (or hop). When the energy of a node reaches to or below that level, the node should not be considered as an intermediary node, until and unless no alternative path is available.

Shruti Bhalodiya, Krunal Vaghela et al. [11] explained the effect of flooding attack in AODV based network. The network parameters like Throughput, Packet Delivery Fraction (PDF) and End to End Delay are compared with normal network (without flooding attack) and a network with one or more flooder nodes. The performance of network parameters is compared in all the three scenarios. They proposed a scheme which is finds single or number of malicious nodes in the network and drops fake packets.

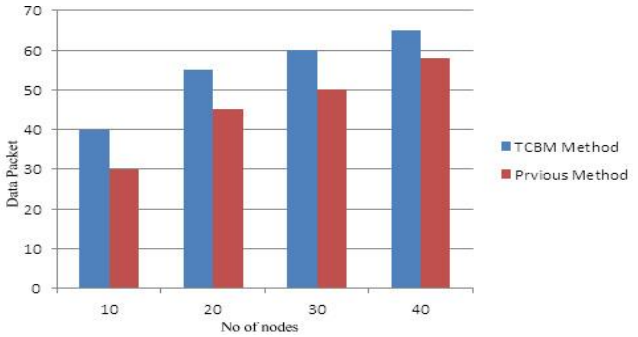
IV. PROPOSED SOLUTION

In the Proposed technique, to detect the malicious node in network and Intelligent nodes are used for prevention and detection of black hole attack in the network In AODV the route request is send to neighbor nodes by the source node. If destination node is one of them then ok otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node id) in node information column and hop count column which contains the number of visiting nodes used in path. Using INRD path updated by these nodes will be used for prevention and detection. Proposed algorithm:-

Step 1: Generate Manet scenario using NS2
Step 2**:** Start with some initial elements like ‘no of nodes’, ‘neighbor node ’
Step 3: Initialize with n no. of nodes.
Step 4: Implement TBCM technique.
Step 5: initially Start TBCM algorithm for finding route form source node to destination node and TBCM will save previous and next node on id
Step 6: In TBCM the route is discovered than ok unless on time base on ever node it will find new path on proactive basis
Step7: Then finally With TBCM Algorithm the delay free transmission will be formed

Step 8: This process continuation until the efficient path is formed in network.

V. RESULT AND ANALYSIS



The result show proposed TCBM data transmission has better result than previous method

VI. CONCLUSION

This paper mainly focused on the efficient route in network. How can we Provide efficient data transmission Due to their dynamic nature, it will require higher data stability. A future scope is to apply various techniques for better results.

REFERENCES

[1] Vaibhav Suhane, Mahesh Gaur, Sadhna K.Mishra, "Detection and Prevention of Network from Network Attacks using EAODV", IJARCSEE, vol-4, pp.80-91, 2015.

[2] Anumeha, Prof. (Dr.) Bhawna Mallick, "Introducing efficient & improved .AODV routing protocol for Manet", IJSTM, vol-no.4, pp.36-44, 2015.

[3] Krupa A Talwar, Benakappa S M, Dr. Yuvaraju B N, "A Survey: Routing Protocols in MANETs", IJIRCCE, Vol.2 Issue.7, 2014.

[4] Iftikhar Ahmad, Uzma Ashraf, Sadia Anum, Hira Tahir, "enhanced AODV route discovery and route establishment for QOS provision for real time transmission in Manet", IJCNC, Vol.6, No.2, 2014.

[5] Arthur Ndlovu, "Improved Energy Efficient AODV Routing using K-means Algorithm for Cluster Head Selection", IJCSME, vol-4, pp.177-187, 2015.

[6] Reena Singh, Shilpa Gupta, "EE-AODV: Energy Efficient AODV routing protocol by Optimizing route selection process", IJRCCT, Vol.3, Issue.1, 2014.

[7] IS.Venktasubramnian, IIR.Mohankumar, IIIC.Hemalatha, "Improved AODV Routing Protocol for Manet to Enhance the Network Performance", IJARCST, Vol.2, Issue.4, 2014.

[8] Madhvi Saxena, Neha Jain, "Network Lifetime Improvement Using Energy Efficient Multipath ad hoc on demand distance vector routing", IJET, vol-4, pp.69-73, 2015.

[9] Jaspreet Singh, Kartik Sharma 2015, "Energy Efficient AODV Routing Protocol for Mobile Ad-hoc Networks", IJARCCE, vol-4, pp.121-124.

[10] Miral V. Vora, Prof. Jignesh H. Joshi, "A Novel Approach on Energy Efficient AODV Algorithm for MANETs", IJIRCCE, vol-3, pp.1071-1077, 2015.

[11] Shruti Bhalodiya, Krunal Vaghela, "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol", IJCA, vol.125-no.4, pp.10-15, 2015.

[12] Ashraf Abu-Ein, Jihad Nader, "An enhanced AODV routing protocol for MANETs", IJCSI, Vol.11, Issue.1, No.1, 2014