International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Enhancement of Tolerant Mechanism for AODV Routing Protocol by Using Probabilistic Approach

Ratnesh Kumar[1], Raj Kumar Paul[2]

[1]Computer Science and Engineering, Vedica Institute of Technology, Bhopal, Madhya Pradesh, India

[2]Assistant Professor, Computer Science and Engineering, Vedica Institute of Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

Mobile Ad-Hoc Network is a wireless network without infrastructure. It is self-configuring network of nodes connected via wireless without any form of centralized administration. This kind of networks is currently one of the most important research subjects, due to the huge variety of applications (emergency, military, etc...). Efficient routing protocols will make MANETs reliable. Multiple path routing protocols are shown to be performance-effective alternatives over single-path routing for ad hoc networks and it represents a promising routing method for wireless mobile ad hoc networks. Multi-path routing achieves load balancing and is more resilient to route failures. aim of this thesis is to improve the route error tolerant mechanism of Adhoc On demand Distance Vector Routing Protocol (AODV) for the dynamic MANET system. In traditional AODV, if the route error occurs at the middle of transmission means the source node reconstruct the route to start the transmission from the beginning. So more delay is occurred in the network. In the proposed mechanism, every node contains two version's of routing table , the route error RERR is not sent to the source node. It is send to the Previous node, and then previous node check own old version of routing table and if there are any path available for that destination then it uses that path for transmission.

Keywords : AODV, MANET, Route Failure, Malicious Node.

I. INTRODUCTION

A mobile ad hoc networks (MANET) is a collection of mo- bile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET,each node acts not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range[1]. Each device in a MANET is free to move independently in any direction, and will there- fore change its links to other devices frequently. MANETs are much more vulnerable and are susceptible to various kinds of security attacks [2]

These nodes have routing capabilities which allow them to create multihop paths connecting node which are not within radio range. The routing protocols can be roughly divided into three categories: proactive (table driven routing protocols), reactive (on- demand routing protocols), and hybrid. The primary goal of such an ad hoc network routing protocol is to provide correct and efficient route establishment between pair of nodes so that messages may be delivered in time. In proactive, each node maintains a routing table, containing routing information on reaching every other node in the network. In reactive, when a node whishes to send packet to a particular destination, it initiates the

route discovery process, in order to find the destination[3].

Ad-Hoc On demand Distance Vector Routing protocol (AODV) is widely used for the route discovery in the MANET. The AODV routing protocol comes under the category of reactive routing protocol , which means that it discover the route after receiving the Route Request (RREQ) from the source node[4]. AODV does not allow keeping extra routing which is not in use [5].

There are three AODV messages i.e. Route Request (RREQs), Route Replies (RREPs), and Route Errors (RERRs) [6].

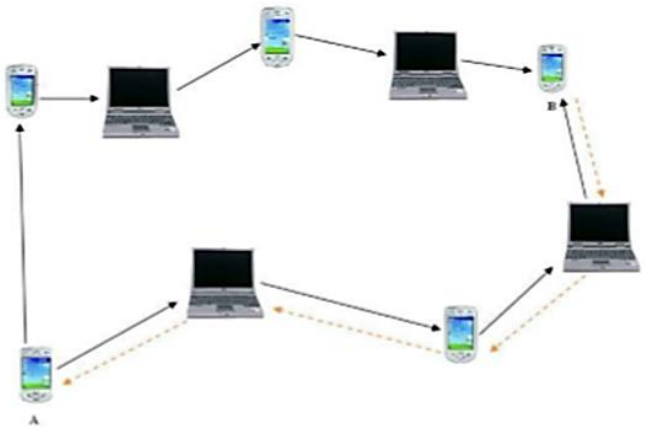

Figure 1. RREQ and RREP messages in MANET using AODV [7]

When the source node wants to create a new route to the destination, the requesting node broadcast an RREQ message in the network [8]. In the figure 1.2 the RREQ message is broadcasted from source node A to the destination node B. The RREQ message is shown by the black line from source node A to many directions. The source node A broadcasts the RREQ message in the neighbor nodes [9]. When the neighbor nodes receive the RREQ message it creates a reverse route to the source node A. This neighbor node is the next hop to the source node A. The hop count of the RREQ is incremented by one. The neighbor node will check if it has an active route to the destination or not. If it has a route so it will forward a RREP to the source node A. If it does not have an active route to the destination it will broadcast the RREQ message in the network again with an incremented hop count value. The figure 1.2 shows the procedure for finding the destination node B [9]. The RREQ message is flooded in the network in searching for finding the destination node B. The intermediate nodes can reply to the RREQ message only if they have the destination sequence number (DSN) equal to or greater than the number contained in the packet header of RREQ [10].

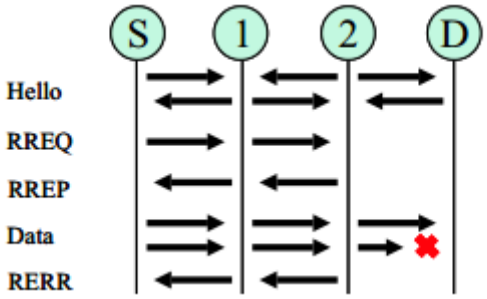

Figure 2. AODV Protocol Messaging

Neighboring nodes periodically exchange hello message, Absence of hello message is used as an indication of link failure.

II. RELATED WORK

In [11] the improved AODV routing protocol is proposed. By reducing the control message overhead the performance of the AODV is enhanced. The new routing methodology called as AD-AODV is described in, the hop count and the mobility of the node in the route is also take into consideration while selecting the best path to reach the destination. AD-AODV is mainly built to provide the best route in the highly dynamic environment. It does not consider the received signal strength and the authentication while routing the data. The traditional enhancement

in the AODV routing protocol for MANET is failure to consider the route error tolerant mechanism. In this paper, the route error tolerant mechanism is improved to increase the performance of the Mobile Ad hoc Network. The throughput of the network gets increased by handling the route error efficiently. In the proposed method, the node which previously forwards the data packet handles route failure. So, it reduces the source overhead in the transmission.

In the proposed mechanism[4], the route error is not sent to the source node. In traditional AODV, the link failure is handled by source node by rerouting the data packets. In [4] It is send to the node which is prior to itself in the route. So, forwarder node also can handle the route failure and the proposed scheme considers the presence of malicious node while constructing the route. So, the proposed scheme improves the performance of traditional AODV in terms of throughput and packet loss.

Metric based enhancement to AODV is proposed in [12] to reduce the route failure. For that they consider the stability of the route while choosing the best path to reach the destination. EM-AODV routing protocol maintains multiple routes to the destination to share the traffic load. This protocol gives better performance when compared with AODV. But it fails to take the signal quality and the trustableness in to account.

III. PROPOSED WORK

In Ad-hoc network root selection is very important factor. for some critical application, like fire detection where data should we deliver with minimum time delay. So time delay is important factor as compare to memory requirement.

In my approach every node contains two version's of routing table, current updated routing table and previously updated routing table. If link between two intermediate nodes get failed on the basis of latest version of routing table then before sending route (RERR) message to previously forwarder node, a node check own old version of routing table and if there are any path available for that destination then it assume that path for transmission. And node deletes the entry for that destination from latest version of routing table.

Whenever any RREQ message is received for any destination then first of all node check own recent version of routing, if path is available for that destination then it will send back RRPLY message to source and if there is not available any path for that destination then node check own old version of routing table and if there is any path available for that destination then it will also send RRPLY message to source node and if neither in recent version nor in old version , root is available then node will send RREQ message to all its neighbours.

IV. RESULTS

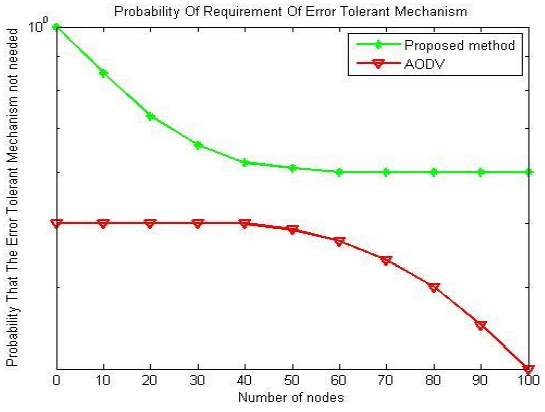

Figure 3. Probability of Requirement of Error Tolerant Mechanism

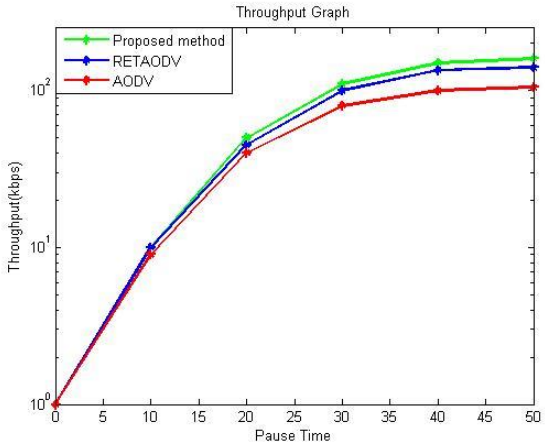

Figure 4. Throughput(kbps) vs Pause Time

V. CONCLUSION

In this paper we have proposed a approach in which every node contain 2 versions of routing table, so it maintaining 2 version so more memory will be required, but it will give better performance with minimum delay, because time is more important as compare to memory. If there are any root available in old version of routing table then new route discovery process is not required.

VI. REFERENCES

[1]. Mohanapriya Marimuthu and Iglano Krishnamurthi, "Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks", JOURNAL OF COMMUNICATIONSAND NETWORKS, VOL. 15, NO. 1, FEBRUARY 2013

[2]. B.Kannhavong, H.Nakayama, andA.Jamalipour, "Asurveyofrouting at- tacks in mobile ad hoc networks," IEEEtrans. Wireless Commun., vol. 14, no. 5, pp. 85-91, Oct. 2007.

[3]. M. Rezaee1, M. Yaghmaee2, "Cluster based Routing Protocol for Mobile Ad Hoc Networks", Department of Computer Engineering, Ferdowsi University of Mashhad, Iran

[4]. S.Shanthini Devi, Dr.K.Thirunadana Sikamani, "Improved Route Error Tolerant Mechanism For Aodv Routing Protocol In Manet", International Conference on Current Trends in Engineering and Technology, ICCTET'13.

[5]. C. Perkins, E. Royer, Ad-hoc On-demand DistanceVector Routing, 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, United States, pp 90-100, Feb. 1999.

[6]. Khazaei, M. and R. Berangi,"A multi-path routing protocol with fault tolerance in mobile ad hoc networks", Proceedings of the 14th International CSI Computer Conference, Oct. 20-21, IEEE Xplore Press, Tehran, pp 77-82, 2009.

[7]. Jyoti Gupta," Fault Tolerant Wireless Mesh Network: An Approach", International Journal of Computer Applications, Volume- 23, issue- 3, pp 43-46, June 2011.

[8]. Rajkumar, K. Duraiswamy," A Fault Tolerant Congestion Aware Routing Protocol for Mobile Adhoc Networks", Journal of Computer Science volume- 8, issue- 5, pp 673-680, 2012.

[9]. Zamree Che-Aron, Wajdi Al-Khateeb and Farhat Anwar, "The Enhanced Fault-Tolerance Mechanism of AODV Routing Protocol for Wireless Sensor Network", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

[10]. Gurpreet Singh Shahi, Manmohan Sharma, "Fault Tolerance Mechanism for Time on Demand Distance Vector Protocol with Clustering in MANETs", 2012 IJAIR, ISSN: 2278-7844

[11]. L. B. Ruiz, I. G.. Siqueira, L. B. e-Oliveira, H. C. Wong et al., "Fault Management in Event-driven Wireless Sensor Networks", 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems (MSWiM), Venice, Italy, 2004.

[12]. M. Demirbas, "Scalable Design of Fault-Tolerance for Wireless Sensor Networks", Doctoral Dissertation. Ohio State University, USA, 2004.