THE ANNALS OF "DUNĂREA DE JOS" UNIVERSITY OF GALATI
FASCICLE III, 2017, VOL. 40, NO. 2, ISSN 2344-4738, ISSN-L 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS

AODV BASED BACKUP NODE MECHANISM WITH QOS ENABLE ROUTING IN MOBILE AD-HOC NETWORKS

Sanchi, Dr. Himanshu Monga*, Er. Sonika Soni

JCDM College of Engineering and Technology,
Sirsa, Haryana, INDIA
* *Corresponding author*

Abstract: To manage the intrinsic properties of MANETs, a backup path algorithm for quick reconnection during link failures, is proposed. Also, proposed model reduces current recovery time by improving reliability of network. Backup path is further added in the existing AODV routing protocol, in which after link breakage, re-routing analysis is automatically accomplished to sustain reconnection. In this way, reliability in routing is assured.Proposed work shows improvement over standard AODV protocol in terms of various network performance parameters like throughput and packet loss.

Keywords: MANET, on-demand routing protocol, Backup Routes, Throughput, Packet Loss, Quality of service (QOS).

1. INTRODUCTION

A Mobile ad hoc network (MANET - Sadjadpour et al, 2010 and, Lajos et. al, 2007) is a collection of mobile nodes (MNs)sharing a wireless channel without the need of any centralized controller (see figure1).

For QOS routing, it is not sufficient to only find a route from source to destination, the route has to even satisfy the QOS constraints such as bandwidth, end-to-end delay and energy. QOS routing protocols can be classified either as proactive or reactive. Proactive protocols continuously learn the topology of the network by exchanging topological information among the nodes.

The family of Distance-vector protocols is an example of a proactive scheme. Example: DSDV, OLSR. Reactive protocols, invoke a route determination procedure on demand only. Example: DSR, AODV. Routing protocols must incorporate the load balancing (Karaoglu & Hanzelman, 2013) to deal with congestion and ensure secure routing. The primary objectives of MANET routing protocols is to maximize throughput, minimize packet loss and to minimize recovery time.

Due to continuous node movement in Ad Hoc networks, radio links may get broken. This leads to increase in packet loss, reduction in throughput and degrade the efficiency of network.

To avoid these problems, efficient route repairing recovery techniques are provided (Kundu, 2014; Monga, 2016). The biggest challenge in routing is to provide reliable and short route in a network.

The routing (Monga, 2016; Mishra et al, 2009) involves two steps: first determining the optimal route and second transferring the information groups through an Ad Hoc networks. High mobility and

dynamic architecture of MANET make it vulnerable to security issues. This causes various types of attacks due to Lack of centralized management, Dynamic topology and link power supply.

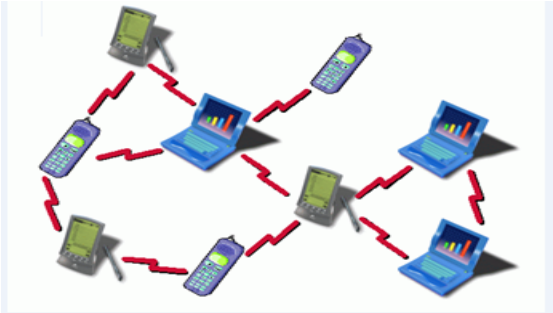

Fig.1. Mobile Ad Hoc Network

Trust (Manoj, 2012; Cho & al, 2011) has an important role for reliable and secured routing. Accurate trust values can be obtained by combining the Trust from direct observations and indirect observations.

2. AODV PROTOCOL

Ad-hoc on demand Distance Vector (AODV Singh & Jain, 2015) routing protocol is a reactive protocol that establishes the route only on demand and always search for the shortest path. The logic behind AODV is that the topology information is only transmitted by nodes on-demand. When a node wishes to transmit packets to destination to which it has no route, it will generate a route request (RREQ) message to other nodes. A route is found when the RREQ message reaches the destination node. Till effective route becomes available between two endpoint, AODV remains passive. AODV avoids the "Counting to infinity" problem by using sequence numbers for every route. It defines three types of control messages for route maintenance:

RREQ – A route request message is transmitted by a node requiring a route to a node.

RREP – A route reply message is unicasted back to the originator of a RREQ.

RERR – Nodes monitor the link status of next hopes in active routes. When a link break in an active route, a RERR message is delivered.

AODV keeps track of the following information for each route:

- Destination IP Address: IP address for the destination node.
- Destination Sequence Number: Sequence number for this destination.
- Hop Count: Number of hops to the destination.
- Next Hop: The neighbor, which has been designated to forward packets to destination.
- Lifetime: The time for which route is considered valid.

Backup Routing**:** In our proposed work, use of pre-computed backup path provides a solution to link failure and loss of connectivity. Pre-computed route give good performances in high-density conditions. Mobile nodes in the same range can exchange messages with their neighbors. Through these messages, the routing protocol will begin to construct the routing table between source and destination. The Backup mechanism computes a backup path after identifying the malicious nodes in primary path.

3. SYSTEM MODEL

In this system model, shortest path is provided in AODV protocol. In normal AODV, routing is achieved using nearby nodes and whole network is travelled to reach the destination node thereby following longer path. In our proposed work routing mechanism is based on destination phenomenon adopting the shortest path, even in the situation of link failure or loss of connectivity shortest path is followed. To achieve this, a backup node mechanism for quick reconnection is proposed. The procedure of computing the shortest path is shown in figure 2.

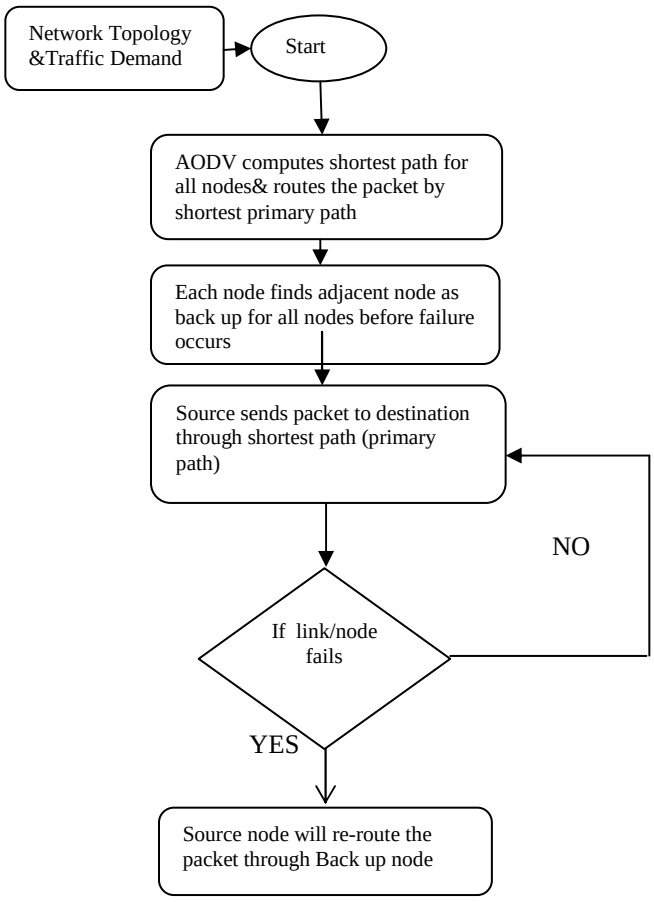

Fig.2. System Model of Proposed AODV

Routing in AODV protocol is using the following distance:

(1) $$Dist = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Where

x_2 = x-coordinate of destination node

x_1 = x-coordinate of source node

y_2 = y-coordinate of destination node

y_1 = y-coordinate of source node

3.1. Proposed Algorithm

The following assumptions are made in the implementation of proposed work:

Algorithm:

1. Node Initialization
   - Generate the number of nodes (N)
   - Assign node ID to the new node by MANET protocol
   - The new node's initial local table is established by direct transactions.
2. AODV computes the shortest distance for all nodes.
3. Provide a routing from source to destination from shortest path (primary).
4. Each Node finds an adjacent node as a backup before failure occurs.
5. If route to destination via adjacent node then
   - Update routing table

   Else
   - Choose a different adjacent node.

   If it provide a disjoint path to destination then
   - Update routing table

   Else
   - Choose a different adjacent node.

   End

   End
6. While source sends traffic to destination via shortest path
   - If node/link failure occurs in primary path then
     - Store the location of failures.
     - Provide the rerouting through backup node.
     - Select a set of path having minimum path length.
     - Choose available best path for Communication.

     End

   End

4. SIMULATION, RESULTS AND ANALYSIS

Our proposed work is simulated on MATLAB. The simulation parameters used in this work are given in Table 1:

Table 1. Simulation Parameters

Parameter	Value
Simulation Tool	MATLAB
Min no. of nodes	10
Max no. of nodes	50
Routing protocol	AODV
Traffic type	TCP
Packet size	100

Routing in AODV is described in following graphs:

1. Placement of nodes: Figure 3 shows that the number of nodes is variable. We have considered 50 nodes. Nodes can be increased or decrease as per requirement.

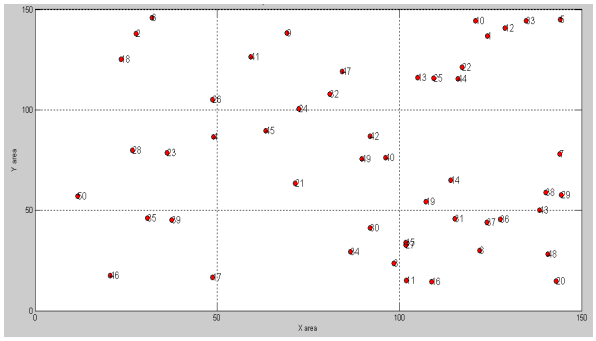

Fig.3. Sample placement of nodes

2. Proposed Routing in AODV: Figure [4] shows that Routing takes place using shortest path which is destination based. If node/link failure occurs in primary path then it provide the rerouting through backup node and Select a set of path having minimum path length which Choose available best path for Communication.

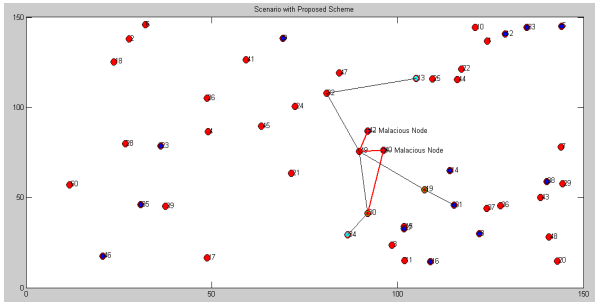

Fig.4. Proposed Routing in AODV

4.1. 4.1 Simulation results:

For this work the comparison of performance matrices i.e. throughput and Packet loss is shown in the Table 2:

Table 2 - Parameter values for each case

Parameter	Normal AODV	Trust and load AODV	Proposed AODV
Throughput	10 nodes=1	10 nodes=1.4	10 nodes=1.8
	20nodes=1.09	20 nodes=1.4	20 nodes=1.9
	30 nodes=1.09	30 nodes=1.42	30 nodes=1.94
	40 nodes=1.48	40 nodes=1.43	40 nodes=1.96
Packet loss	10 nodes=22	10 nodes=17	10 nodes=10
	20 nodes=22	20 nodes=17	20 nodes=5
	30 nodes=40	30 nodes=35	30 nodes=4
	40 nodes=40	40 nodes=35	40 nodes=3

Graphical comparison of throughput (bps) and packet loss is shown in figures 5 and 6 below:

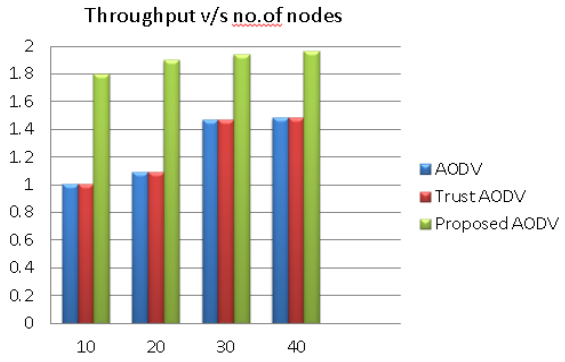

Fig.5. Graph of Throughput

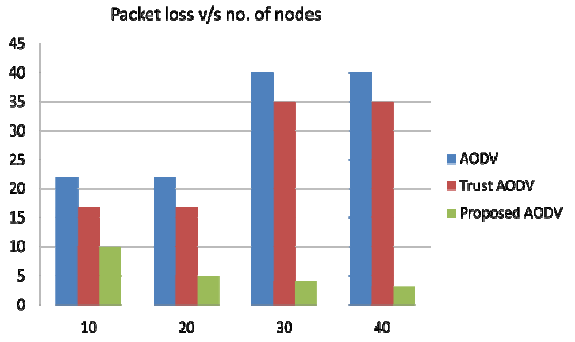

Fig.6. Graph of Packet Loss

For the proposed work, a graph shows exceptional improvement.

5. CONCLUSION

In this paper, protocol AODV is proposed. It could provide backup node mechanism for quick reconnection. When a link failure occurs due to faulty nodes, it sets up another route to destination by indicating faulty nodes as a malicious node. Additionally, the proposed scheme selects the shortest path containing the largest number of backup paths to provide efficient recovery from route failure and maintain an adequate routing length. Moreover, we have compared the proposed AODV with normal AODV in terms of Throughput and Packet loss.

6. REFERENCES

Sadjadpour, H., et al. "A Unified Analysis of Routing Protocols in MANETs", IEEE Transactions on communications, vol. 58, no. 3, march 2010.

Lajos Hanzo & Rahim Tafazolli, "A Survey Of Qos Routing Solutions For Manet", IEEE Communications Surveys & Tutorials, , volume 9, pp. 911-922, 2007

Bora Karaoglu, Wendi Heinzelman, "Cooperative Load Balancing and Dynamic Channel Allocation for Cluster-based Mobile AdHoc Networks", IEEE Transactions onMobile Computing. 2013.

M.K. Kundu., et al.:" An efficient route repairing technique of AODV protocol in MANET", Springer International Publishing, 2014,Volume 2.

Dr. Himanshu Monga, Sandeep Kumar Arora, "Performance Evaluation of MANET on the basis of Knowledge Base Algorithm" Optik - International Journal for Light and Electron Optics, Volume 127, Issue 18, September 2016, Pages 7283–7291.

Mishra, D., et al.: "Behavior Analysis of Malicious Node in the Different Routing Algorithms in MANET. 2009 International Conference on Advances in Computing, IEEE.

V. Manoj, et al.: "Trust Based Certificate Authorityfor Detection of Malicious Nodes in MANET".Springer-Verlag Berlin Heidelberg 2012

J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Communications Surveys and Tutorials,vol. 13, no. 4, pp. 562–583, 2011.

Vijaya Singh, Ms. Megha Jain, "Analysis of Trust Dynamics in Cyclic Mobile Ad Hoc Network", 1st International Conference on Futuristic trend in Computational Analysis and Knowledge Management. ©2015 IEEE