© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection of Malicious Node Attacks in Mobile Ad-Hoc Networks using Link Quality Estimation Routing Protocol

A.Viji, J. Jaygeetha

Department of Electrical Communication Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India

ABSTRACT

Mobile Ad hoc Networks (MANETs) are used for providing Quality of Service (QoS) where nodes are having mobility and can travel in any random direction. There are several reactive protocols available in literatures which are suitable for MANETs based on single and multiple paths. Among these, AOMDV protocol is the most suitable for finding multiple paths to the destination. Multipath routing mechanisms have been preferred over single path routing to provide parallel safe paths and to maximize throughput. Applying traditional shortest path metric for multipath route selection leads to traffic concentration at some nodes resulting in congestion, thereby causing performance degradation. Reliable data transmission among mobile nodes in highly dynamic ad hoc networks was not ensured by AOMDV routing protocol due to the selection of the multiple node disjoint paths based on only minimal hop counts that lead to link failures and route breaks.

Keywords: Routing; Route discovery; Link quality; Ad hoc on-demand multipath distance vector routing (AOMDV).

I. INTRODUCTION

With emerging mobile applications, mobile ad hoc networks (MANETs) have concerned study from various groups due to its flexibility and usability in different applications. A MANET is a self-configuring temporary network of mobile nodes those are independent with each other and do not have any fixed infrastructure. MANETs do not control or regulate traffic in the network but utilize the routing capability of intermediate nodes. Here intermediate nodes are used as routers by source and destination nodes and a routing path must be established for actual communication. MANET success is mainly for routing protocols which are an active area for MANET research. Many routing protocols have been proposed for ad hoc networks in literature which detect a route based on given criteria for packet delivery from source to destination.

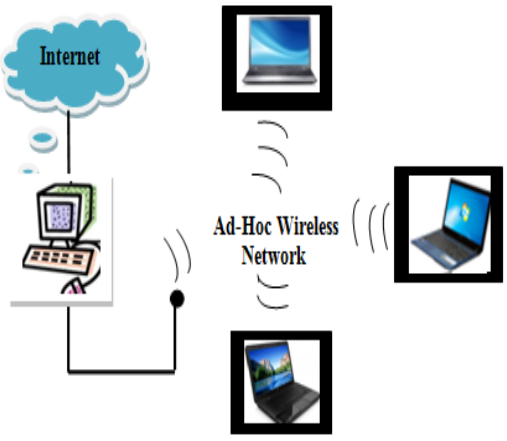

Figure 1. Mobile Ad-Hoc Networks

Ad hoc On-demand Multipath Distance Vector (AOMDV) protocol is an extension of AODV protocol. The routing table for destination includes a next hops and the number of hops to reach the destination. Here all the next- hop neighbors are assigned as the same sequence numbers. A node maintains every destination's advertised hop count that sends destination route advertisements. Every duplicate route advertisement that has been broadcasted and received by a node defines an

alternative destination path. Here the node does not discard duplicate RREQs instantaneously. Every RREQ has an additional field hop indicating its first hop. Also, a node maintains a first hop list for every RREQ to follow list of neighbors of source. To make certain link disjoints in RREP's first hop, destination replies to RREQs arriving through distinctive neighbors. Every RREP path may intersect at an intermediate node, but each goes on a various reverse path to source ensuring link disjointness.

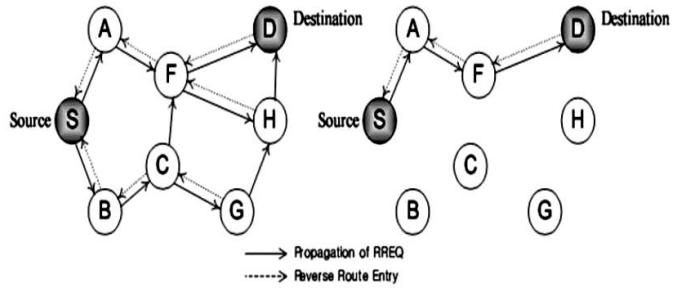

Figure 2. (a) RREQ Broadcast (b) RREP Forward path (Route Determination from Source to Destination)

II. METHODS AND MATERIAL

1. Packet Dropping In Wireless Ad Hoc Networks

In ad hoc networks, all packets lost should be does not viewed as malicious. Here we discuss some packet loss scenarios in wireless ad hoc networks.

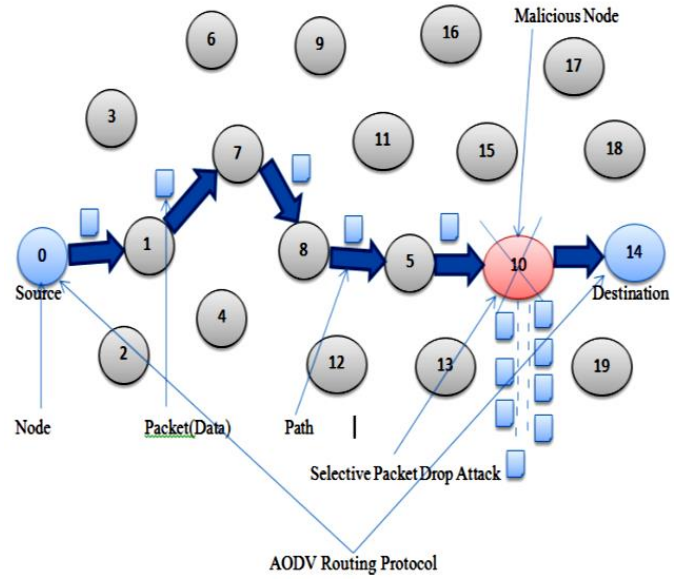

Figure 3. Packet Drop Attack

AOMDV Routing Protocol

AOMDV routing protocol is an enhanced version of a prominent and well-studied on-demand single path routing protocol known as AODV routing protocol. The main goal of AOMDV is to compute loop-free and link-disjoint multiple routes between any source and destination pair. It eliminates the occurrence of frequent link failures and route breaks due to node mobility, node failures, and congestion in traffic, packet collisions, and so on in highly dynamic ad hoc networks by adding some extra fields in routing tables and control packets of AODV.

In AOMDV routing protocol, the propagation of RREQs from a source to a destination via intermediate nodes are used to establish multiple reverse routes, the propagation of RREPs from a destination to a source via intermediate nodes are used to multiple forward routes and the flooding of HELLO packets between nodes are used mainly to obtain local link after route establishment.

2. Packet Drop Detection Using Various Protocols

A multipath routing protocol is a variant of single-path AODV routing protocol. This method established node disjoint paths with less delays based on interaction of factors from various layers.

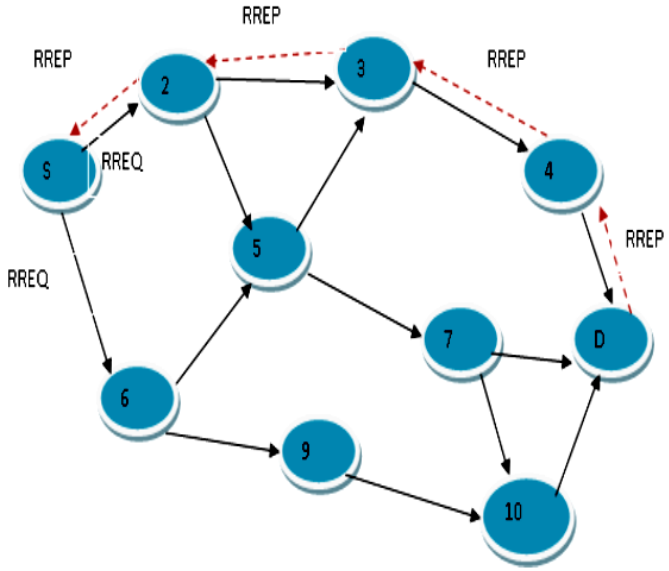

Figure 4. Route selection in AODV

The channel aware AOMDV (CA-AOMDV) used channel average non-fading duration as routing metric to select reliable links for path discovery. Here paths were reused and not discarded. Link availability estimation was used to choose most stable route from alternate paths and was implemented in AOMDV for route

selection. Results show that choosing the stable route leads to a high throughput in active network topologies.

3. Link Quality Estimation Routing Protocol

Link quality estimation routing (LQER) protocol find the optimal route for AOMDV based on link quality and neighbouring node queuing delay. The proposed system uses Link Quality Estimation based Routing (LQER) protocol. In existing system, when source node has data to send, it will select a neighbour node as the next hop node which has the shortest distance from destination node than the other neighbors. It can build a route which has the minimum hops dynamically; it is suitable for dynamic networks. But it doesn't consider the reliability of communication. So, to overcome this problem LQER protocol is used.

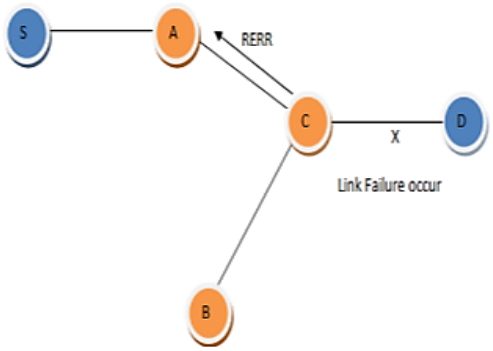

Figure 5. Link failure Problem

If intermediate nodes or the destination move then following conditions possible:

1. The next hop links break resulting in link failures.
2. Routing tables are updated when link failure occurs.
3. All active neighbors are informed by Route Error message.

Here link between C and D breaks. Now node C invalidate route D in the route table .Node C creates Route Error message and lists all destinations that are now unreachable and sends to upstream neighbor this messages.

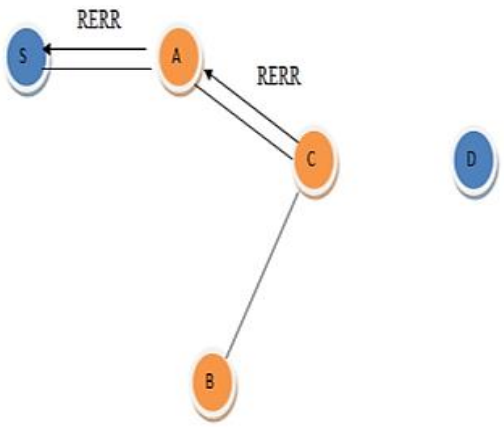

Figure 6. Route Error to upstream nodes

A. Link Quality Prediction Algorithms

FLOW DIAGRAM

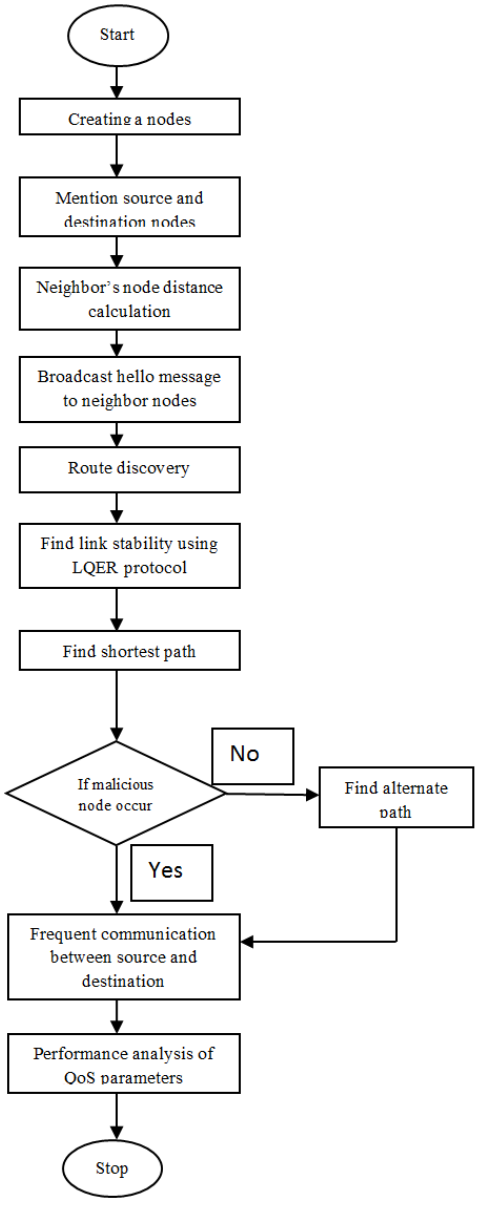

Figure 7. Flow Diagram

If the output of an LQP algorithm is a subset of an infinite set of states, we classify this prediction as stochastic since the output is in that case usually a probability. For example, an algorithm that estimates the probability of successfully receiving future transmitted packets is stochastic. Another possible classification criterion is the application of LQP. Successful applications are found in the area of routing, group communication, multicast communication and clustering.

The proposed metric has several desirable properties:

- LQER is based on packet reception ratios that are strongly correlated to the throughput.
- LQER considers the asymmetry of links by incorporating the packet loss in both directions.
- LQER penalizes routes with higher hop counts that have naturally a lower throughput.

B. Link Quality Value

The estimation of link quality is based on signal power of transmission packets.If the link is high value the signal power of the sending packet is not reduced at the receiving side. Otherwise it is reduced.

LQER protocol is preferred for selecting the efficient path in a MANET. Link stability of the path is mainly concentrated. Link break is mostly avoided. Packet drop is very less compared with existing method.In this project, two-ray ground model is adopted. This model [25] considers both the direct path and a ground reflection path. The model gives more accurate prediction at a long distance than the free space model.

The received power is predicted by:

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \qquad (4.8)$$

Where *Pt* is the transmitted signal power; *Gt* and *Gr* are the antenna gains of the transmitter and the receiver respectively; *L* is the system loss; *d* is the distance between transmitter and receiver; *ht* and *hr* are the heights of transmit and receive antennas respectively.
Here the transmit range of each node is equivalent. So, the link quality $LQ=P_r$.

III. RESULTS AND DISCUSSION

A. Simulation Parameters

The parameters which are considered for simulation are,

- Packet Drop
- Energy Consumption
- Residual Energy

B. Design of Simulation Parameters

Table 1. Design Parameters

PARAMETERS	VALUES
N(No of nodes)	50 nodes
MAC Type	802.11
Routing Protocol	LQER
Transmission Protocol	UDP
Antenna	Omni-Directional Antenna
Total Packets Sent	500
Initial Energy	100 J

C. Node Deployment

The nodes are deployed in random way. The node deployment strategy is accomplished based on the applications. In this application the 50 nodes are deployed in random manner.

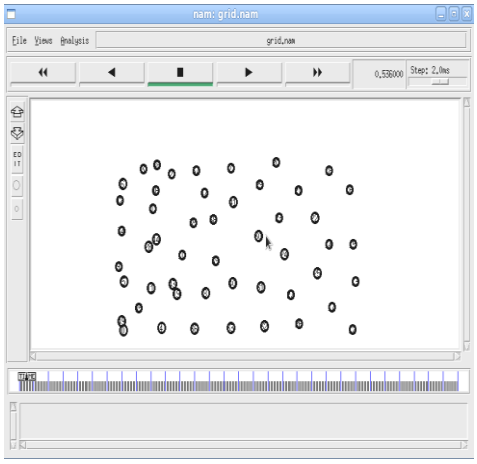

Figure 8. Node Deployment

Nodal deployment considered here is in random way. Using NS 2.34 simulator fifty nodes are created for data packets transmission.

D. Selection of Source And Destination Nodes

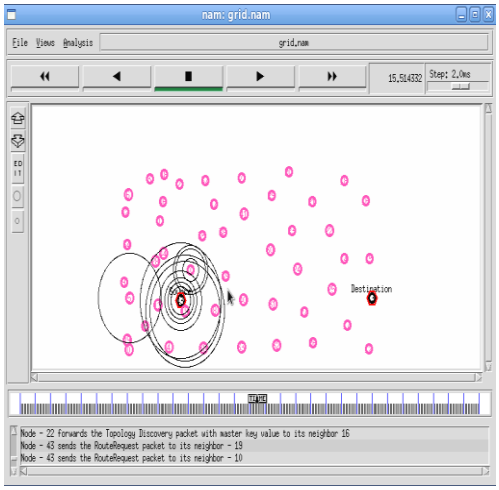

Figure 9. Selection of source and destination nodes

After the node deployment, the source and destination nodes are selected among the fifty nodes. Then all the nodes discover their transmission range continuously.

E. Neighbor Node Distance Determination

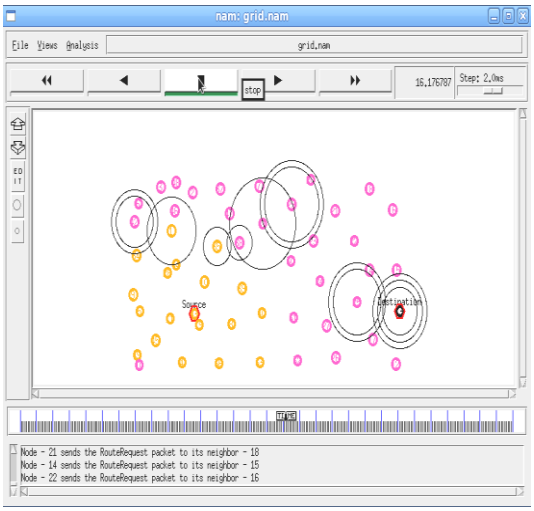

Figure 10. Neighbor node distance determination

After the selection of source and destination nodes, the source node sent the hello packets (RREQ) to their neighbour nodes through the number of intermediate nodes. Each node sent the RREP packets to the source node after receive the RREQ packets. Here the colour change (pink to yellow) of the node mentioned the nodes which are sent the RREP packets to the source node.

F. Malicious Node Detection

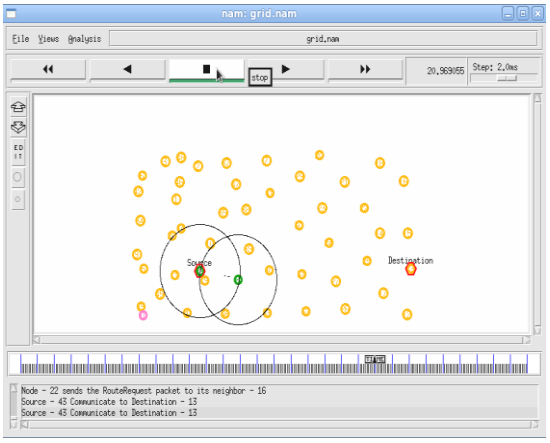

Figure 11. Malicious node detection

By using the LQER protocol the source node find the link quality value of the all the available paths for data packets transmission. Then select the path which has both the high link stability value and the shortest hop count value. If malicious node occurs in that path, the source node detects that node immediately and ignores that path. So here the packet drop is avoided.

G. Comparison Graph

Packet Drop

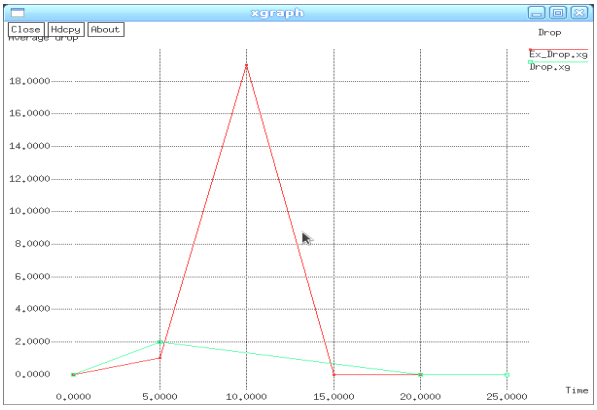

Figure 12. Packet Drop

From the above graph the packet drop of a proposed method is very small amount than existing method. The graph clearly shows that the packet drop of a existing method is very high in the period of 5 to 15 milliseconds.

Packet drop can be happened in two ways. Nodes are purposely discarding the packets with no reasons and the packets can be dropped because of insufficient resources.

Energy Consumption

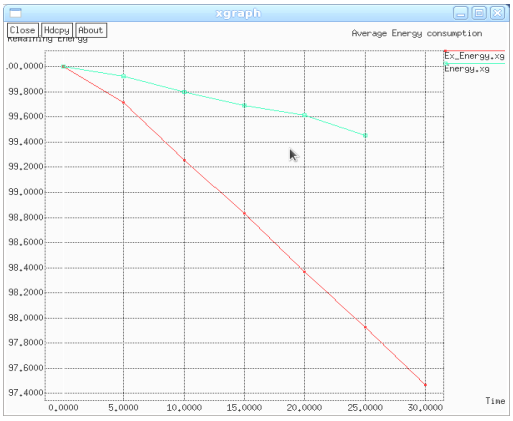

Figure 12. Energy Consumption

Figure 12 shows the energy consumption by the nodes in data transmission. The energy consumption during transmission includes sensing the link quality and the actual data transfer. Energy consumption will be more in communication process only. The graph delivers that energy consumption of proposed system is less compared to the existing one.

The following table consists of comparison between the proposed work and the one which already prevails.

Table 2. Parameters analysis

Parameters	Time(Ms)	Existing	Proposed
Packet Drop	10	19	**1**
	14	6	**1**
Energy Consumption(J)	10	0.75	**0.12**
	20	1.60	**0.40**

From the above comparison it is analyzed that the packet drop of the proposed method was very less amount compared to the existing method. And the energy consumed by the nodes for the data transmission in the proposed method was also very low compared to the prevailing system. When the packet drop is minimized, the packet delivery Ratio is increases. So the system performance is improved in the proposed method than existing method.

IV. CONCLUSION

Mobile ad-hoc network have been wast area of research work from past few years because it's widely used application in battlefield and business purpose. Due to openness, dynamic topology network is vulnerable from attacker. In this paper we have discussed MANET protocol, its characteristics and attack which trigger on it. We have discussed various techniques to isolate and prevent packet drop attack which degrade the system performance by decreasing latency, throughput and increasing end-to-end delay. There are acknowledgments and Link estimation based schema which prevent this attack in AOMDV protocol. In our feature work we proposed new algorithm based on monitor node technique to which improves network efficiency.

V. REFERENCES

[1] Abusalah L., Khokhar A., 2008: "A survey of secure mobile ad hoc routing protocols," Commun Surveys Tuts 10(4), pp 78–93.

[2] Bandaranayake A.U., Agrawal D.P., 2012: "Indoor link quality comparison of IEEE 802.11 a channels in a multi-radio mesh network testbed," J Inf Process Syst 8(1), pp 1–20

[3] Chung K.S., Lee J.E., 2012: "Design and Development of m-Learning Service Based on 3G Cellular Phones," JIPS 8(3), pp 521.

[4] Gawande A., 2013: "Performance analysis of DSR protocol under sinkhole attack in MANETs," International Journal, 1.

[5] Kapoor R.K., Rizvi M.A., 2011: "Exploring Multi Path routing Protocols in Mobile Ad hoc Networks," JCMS, pp. 693–779.

[6] Li X., Mitton N., 2012: "Achieving load awareness in position-based wireless ad hoc routing," Journal of Convergence.

[7] Luo H., Shyu M.L., 2011: "Quality of service provision in mobile multimedia survey," HCIS, pp 1–15.

[8] Mallapur S.V., Patil S.R., 2013: "Stable backbone based multipath routing protocol for mobile ad-hoc networks," ICCPCT, IEEE, pp. 1105–1110.

[9] Marina M.K., Das S.R., 2001: "On-demand multipath distance vector routing in ad hoc networks," International Conference,IEEE, pp. 14-23.

[10] Peng-cheng G.U., 2011: "Research of AODV Routing Protocol for Ad Hoc Networks," Science Technology and Engineering, pp 18-023.

[11] Sumathi R., Srinivas M.G.,2012: "A survey of QoS based routing protocols for wireless sensor networks," J Inf Process Syst 8(4), pp 589–602.

[12] Taneja S.,Kush A., 2010: "Experimental Analysis of DSR, AODV using Speed and Pause time," IJIMT, pp 453–458.