Implementation and Performance Evaluation of QoS Routing based on Energy Conservation with Malicious Node Detection and Isolation in MANET

Dhanalakshmi N and Alli P

Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, India.
Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai, India.

ABSTRACT
The mobile ad hoc networks (MANETs) are a collection of mobile nodes that can act as routers to forward the packets without using any additional infrastructure. Data routing in such networks is a challenging task owing to the limited energy, node mobility and security issues. The link failures and node failures in ad hoc networks are a major problem due to the node mobility or node power which may cause the path break for routing. The routing resiliency can be enhanced by using multiple disjoint routes. Imbalance network load increases the intersection of nodes violates the QoS parameters. The main objective of this research work is, to design the multi-path routing protocol to balance the network load, decrease the intersection of nodes or connections among the parallel routes using Modified Dijkstra's algorithm. In this connection, link failure in one path should not affect other routes. The enhancement of the quality of service (QoS) with the consideration of energy and table updating (ECAO) which leads to decrease the delay, overhead, and increase throughput and the network lifetime and the reliable communication is provided by using the (NISD).

KEYWORDS: AOLS, DSR, ECAO MANET, NISD,NS-2.

INTRODUCTION

As MANETs are said to be a multi hop network which contains collection of nodes that can communicate directly within the communication range, Whereas the other nodes can make use intermediate node for data transmission and also has frequent variations in the topology due to nodal mobility. Routing protocols to be enhanced in order to establish communication path between nodes without incur additional overheads or computational delay on the power-constrained devices [1]. Due to its self-configured nature, it is well suited for emergency situations like medical situations, natural disasters, military conflicts, etc. [4] [5]. Many previous studies have used Random Waypoint as reference model [6] [7]. However, in future MANETs are likely to be used in various applications with diverse topography and node configuration. Lot of routing protocols have already been proposed. The most important design issue for any type of network is to provide a guaranteed Quality of Service. QoS measures in terms of throughput, delay and packet distribution guarantee [3]. The traffic may contains style of knowledge like voice, data, image, video, etc. may have totally different QoS
needs. QoS-aware routing admit multiple parameters that improves the quality. To provide a QoS routing is a difficult task due to its constraints and network nature. Additional significantly, node quality causes frequent failure and reactivation of links, effecting a reaction to the changes in topology from the network routing, so increasing network control traffic and flood the already engorged links. Hence, of these aspects necessitate a cheap QoS-aware routing [2].

This paper has organized as follows: MANET routing protocols and Proposed Methods are described in section II and III, then Simulation Environment and performance metrics are described in section IV. In section V shows simulation result and analysis of observation. Finally conclusion is given in section VI.

II. Manet Routing Protocol:
Routing may be a mechanism that is employed to decide on best path from available paths for communication between sources to destination. Numerous routing protocols have been designed for ad-hoc networks. MANET routing protocols is classified as:

2.1. Proactive Routing Protocols:
These routing protocols are referred to as table driven routing protocols as a result of each node has got to maintain routing table to each alternative node within the network and interchange these information to search out ways for communication. There are numerous proactive routing protocols are existsuch as Destination Sequence Distance Vector Routing (DSDV), Optimized link state routing (OLSR), etc.

2.2. Reactive Routing Protocols:
These routing protocols are mentioned as On Demand routing protocols as a results of it finds a route from source to destination whenever a node needs to send information to various node within the network. On Demand routing has two phases like route discovery and route maintenance. There are many sorts of reactive routing protocols like DSR, AODV and TORA.[6][8]

2.3. Hybrid Routing Protocols:
Hybrid routing protocols combination of each reactive and proactive routing protocols. This sort of routing protocol was projected to reduce the control overhead of proactive routing protocols and the latency caused by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA[8] (Temporarily Ordered Routing Algorithm). In this proposed work, proactive routing protocol is changed to hybrid nature which is named as optimized Link State Routing (AOLSR) and to enhance path stability which is achieved by using the proposed model Energy Conservation Advanced OLSR (ECAO) and Node Id Based Secure Detection NISD model.

III. Proposed Methodology:
An advanced OLSR (AOLSR) protocol is proposed based on a modified Dijkstra's algorithm which permits routing in multiple paths of dense and sparse network topologies. The determination of paths is based on an on-demand methodology to obviate the density estimation of multiple paths for every feasible destination. The lifetime of the nodes and links determine the path selection.

During the MPR selection process, a malicious node disrupts the flooding of topology control information by misbehaving the information. A novel Node ID Based Secure Detection (NISD) Method is proposed to isolate and block the misbehaving nodes from the communication among nodes. Initially, all the nodes are generated and distribute the key to each other. The MPR set is selected based on the Node ID and the random number generated based on the key generation concept.

The beacon message is distributed periodically to know about the neighboring nodes. It helps to identify the misbehaving nodes by validating the keys. If any misbehaving nodes are identified, then re-authentication process takes place to select the authenticated MPR set for data forwarding. The MRP selection procedure is continued until the set contains only the authenticated nodes.

Then the multiple paths are identified from MPR set using two cost functions in the modified Dijkstra algorithm. Two cost functions are introduced to construct link-disjoint or node-disjoint routes. The cost function contains the evaluation of link state and energy parameters. If the nodes obtained by Dijkstra’s algorithm lie within the range of the limit, then the path is estimated. The routing is based on the energy of nodes and links (implied from the lifetime) and the mobility of the nodes. If all nodes in the networks have a relatively high speed, neighbors of every node may change quickly and the topology also changed frequently which causes the failure of a valid route that can lead the destinations unreachable, which will further affect normal communication in the network.

To predict the high mobility of the node, distance to be calculated between two coordinate positions of the same node at different time interval. If the distance is less than the threshold limit, then the energy cost of the node is calculated based on the prediction of the energy consumption level of the node, using ECAO mode.
because which shows the node movement speed is low. Otherwise velocity to be calculated based on the direction of the movement. The energy cost represents energy consumption of the network in order to prolong all connections between source and destination nodes. The energy cost includes transmission power $P_t$ at time $T$, receiving power $P_r$, and power consuming of ideal node $P_i$ and sleeping node $P_s$ at time $t$.

Finally, energy consumption is computed from the difference between the total energy and energy cost. The multiple paths are identified from MPR set in which nodes are along the path to maximum residual energy. Now, the optimal path is selected after the multipath analysis, based on the Modified Dijkstra’s algorithm. Once again re-authentication process to be carried out to avoid malicious nodes along the path during transmission.

During the transmission, topology changes can be made which is managed by path recovery and loop recovery process. First, a node checks whether the next hop in the source path is one of its neighbors. If so, the packet is transmitted normally; otherwise, it is decided that the ‘next hop’ node is not available. Next, the node will recalculate the path and transmit the packet in the new route.

After the process of path recovery, a new route will be estimated from the present node to the destination. This method will utilize the new route when there are no loops in the network; otherwise, the repetitive process of MDA and ECAO governs the path estimation and link establishment respectively. After this repetitive process, the NIDS process assures the communication by the authentication process.

IV Simulation Environment And Performance Metrics:

This section principally centered on the implementation of the planned Advanced Optimized Link State Routing (AOLSR)[12], Energy Conservation Mechanism with the proactive MANET routing scheme(ECAO)[14], and a completely unique novel Node ID primarily Based Secure Detection (NISD)[13]technique in MANET. The tool used for the simulation is Network Simulator version-2 (NS-2)[10][11]. In this, the performance of the planned methods AOLSR, ECAO and NISD are compared with ancient routing protocols like DSR and OLSR.

In this analysis work, a hundred nodes are thought about with random distribution technique within the simulation space for knowledge transmission. The topology with the distribution of nodes is shown in Figure 1.

![Simulation Environment And Performance Metrics](image)

**Fig. 1:**

The following metrics are accustomed to estimate the performance of the proposed methods, which includes,

- Number of Transmission Control (TC) messages
- Packet Delivery Ratio (PDR)
- End-to-end Delay (E2E Delay)

V. Performance Evaluation:

Table 1 shows the performance analysis of the existing DSR, OLSR[9] and the proposed AOLSR[12], ECAO[14] and NISD[13] methods with respect to node speed. The speed of node taken for evaluation is 10 to 50 m/s. The metrics used for analyzing the performance is Average Delay, End-to-end Delay (E2E), PDR.
Table 1: Performance analysis of the existing and proposed with respect to node Speed

<table>
<thead>
<tr>
<th>Performance with respect to node speed</th>
<th>Node speed (m/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10 20 30 40 50</td>
</tr>
<tr>
<td>End-to-End delay (sec)</td>
<td></td>
</tr>
<tr>
<td>DSR</td>
<td>0.05 0.07 0.15 0.15 0.18</td>
</tr>
<tr>
<td>OLSR</td>
<td>0.06 0.09 0.15 0.152 0.16</td>
</tr>
<tr>
<td>AOLSR</td>
<td>0.07 0.1 0.14 0.15 0.16</td>
</tr>
<tr>
<td>ECAO</td>
<td>0.5 0.85 1.39 1.15 1.17</td>
</tr>
<tr>
<td>NISD</td>
<td>0.7 1.5 2.02 2.57 2.98</td>
</tr>
<tr>
<td>PDR (%)</td>
<td></td>
</tr>
<tr>
<td>DSR</td>
<td>92 83 78 68 60</td>
</tr>
<tr>
<td>OLSR</td>
<td>95 88 87 85 83</td>
</tr>
<tr>
<td>AOLSR</td>
<td>96 92.5 88 87.5 86</td>
</tr>
<tr>
<td>ECAO</td>
<td>95.2 93 91.8 90.9 89.4</td>
</tr>
<tr>
<td>NISD</td>
<td>98.5 97.5 95.9 95 93</td>
</tr>
</tbody>
</table>

Table 2 shows the performance analysis of the existing DSR, OLSR and the proposed AOLSR, ECAO and NISD methods with respect to Number of malicious nodes. The number of malicious nodes used for evaluating the performance of the proposed methods are 5 to 25 nodes and the metrics used with respect to No. of Malicious nodes are Number of TC messages, and PDR.

Table 2: Performance analysis of the existing and proposed with respect to No. of Malicious nodes

<table>
<thead>
<tr>
<th>Performance with respect to number of malicious nodes</th>
<th>No. of malicious nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5 10 15 20 25</td>
</tr>
<tr>
<td>Number of TC Messages</td>
<td></td>
</tr>
<tr>
<td>DSR</td>
<td>2600 2800 2500 2600 2800</td>
</tr>
<tr>
<td>OLSR</td>
<td>2500 2450 2400 2450 2400</td>
</tr>
<tr>
<td>AOLSR</td>
<td>2450 2420 2390 2350 2370</td>
</tr>
<tr>
<td>ECAO</td>
<td>1270 1400 1350 1400 1450</td>
</tr>
<tr>
<td>NISD</td>
<td>1250 1300 1310 1325 1325</td>
</tr>
<tr>
<td>Packet Delivery Ratio (%)</td>
<td></td>
</tr>
<tr>
<td>DSR</td>
<td>41.5 41.3 38.5 39.5 39.8</td>
</tr>
<tr>
<td>OLSR</td>
<td>71.5 69.5 62.3 59 58.5</td>
</tr>
<tr>
<td>AOLSR</td>
<td>84 85 87 88 89</td>
</tr>
<tr>
<td>ECAO</td>
<td>94 89.8 87.2 85.1 80</td>
</tr>
<tr>
<td>NISD</td>
<td>94.5 95.1 95.3 96.1 97.2</td>
</tr>
</tbody>
</table>

5.1 End-To-End Delay (E2E):

The E2E delay is the metric used for analyzing the performance of the proposed methods.

Figure 3 shows the comparative analysis for DSR, OLSR, and the proposed AOLSR, ECAO, and NISD methods. Here, the x-axis denotes the node speed in (m/s) and y-axis denotes end-to-end delay in (ms). It justifies that the E2E Delay of the proposed AOLSR, ECAO and NISD is less, when compared to that of the existing DSR, and OLSR methods.
5.2. Packet Delivery Ratio (PDR) With Node Speed:

The PDR is the second metric for evaluating the performance of the proposed AOLSR, ECAO and the NISD methods. Figure 4 shows the comparative analysis for existing DSR, OLSR, and the proposed AOLSR, ECAO, and NISD methods. Here, x-axis represents node speed in (m/s) and y-axis denotes PDR in (%). It is clear that the proposed methods AOLSR, ECAO and NISD achieved high PDR.

![Fig. 3: Node Speed Vs PDR](image)

5.3. Number of Tc Messages:

The next metric used for evaluating the proposed ECAO and NISD methods are Number of Transmission Control (TC) Messages. Figure 5 shows the comparative analysis for the existing DSR, OLSR and the proposed ECAO and NISD methods. Here, x-axis is the Number of malicious nodes and the y-axis represents the Number of TC messages. It justifies that the proposed ECAO and NISD methods has less number of TC messages, when compared to that of the existing DSR and OLSR methods.

![Fig. 4: No. of malicious nodes Vs No. of TC messages](image)

5.4. PDR With Malicious Nodes:

The metric considered for evaluation of the existing DSR, OLSR and the proposed ECAO and NISD methods are PDR with malicious nodes. Figure 6 shows the comparative analysis of the PDR for the existing and the proposed methods. Here, x-axis denotes the no. of malicious nodes and the y-axis denotes the PDR(%). It justifies that the proposed ECAO and NISD methods has high Packet Delivery Ratio.
Conclusion:
The comparison results shows that the proposed AOLS R, ECAO and NISD methods has less number of TC messages, E2E delay and high PDR. The throughput achieved by the proposed NISD method is 5130 kbps and PDR of NISD method is 98.5%, when compared to that of the existing methods. In this work, the quality of service (QoS) is enhanced by using ECAO which leads to decrease the delay, overhead, and increase throughput and the network lifetime and the assured reliable communication is provided by using the NISD.

REFERENCES
9. Implementation of Multipath and Multiple Description Coding in OLSR Jiazi Yi, Eddy Cizeron, Salima Hamma, Benoît Parrein and Pascal Lesage* Université de Nantes, Nantes Atlantique Universités IRCCyN, CNRS UMR 6597, Polytech’Nantes, rue Christian Pauc - BP50609
10. The ns Manual, formerly ns Notes and Documentation.

Fig. 5: No. of Malicious nodes Vs PDR