Received: April 12, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Attack Analysis and Designing of Quality of Service Framework for Optimized Link State Routing Protocol in MANET

Himani Bali [1]* **Naveen Hemrajani [1]**

[1]*Jaipur Engineering College & Research Centre University, Rajasthan, India*
* Corresponding author's Email: himanibali0530@gmail.com

Abstract: Mobile Ad-hoc Network (MANET) routing is considered a challenging task because of the unpredictable changes in the network topology due to the absence of any centralized control. This routing has led to the development of several different routing protocols for MANET. In MANET, routing plays an important role in providing connectivity for mobile nodes that are not within the same radio range. Existing routing protocols in MANET assume a trusted and reliable environment. Here we have utilized soft computing technique for the selection of nodes in order to provide accurate means of transmission of data. Initially the nodes are clustered using Hybrid K means algorithm. Once the clustering is done path is formed based on optimized link state routing protocol. The routing is done by optimizing the nodes with the aid of Hybrid Genetic algorithm (GA). The implementation is done in NS2/NS3 platform and the results obtained are compared with various existing methods in order to prove the efficiency of our proposed technique. . The data transmission in proposed method (OLSR) occurs with maximum data gathering capacity and cluster head selection and shortest path selection in reaching the sink node. But in the existing method there is no cluster head selection and hence the information is gathered from all the nodes (AODV and DSDV). The results show that our secure QoS versions of the OLSR routing protocol more efficient than existing works.

Keywords: Mobile ad-hoc network, Soft computing, Routing protocol, K-means clustering, Optimal link state routing protocol, Genetic algorithm.

1. Introduction

Mobile Ad Hoc network (MANET) is a multihop mobile wireless network, which does not have any preexisting network infrastructure or centralized administration. Due to its convenience of mobile communication, MANET is explored for numerous applications, such as network extension, ubiquitous computing, urban sensing and vehicular networking [1]. Due to its convenience of mobile communication, MANET is explored for numerous applications, such as network extension, ubiquitous computing, urban sensing and vehicular networking. In multi-hop wireless ad-hoc networks, designing energy-efficient routing protocols is critical since nodes have very limited energy, computing power and communication capabilities [2]. The nodes in MANET communicate with each other through single or multi-hop. The nodes play the role of a router and compel the nodes to cooperate for the correct operation of the network. The resources are consumed rapidly due to the network activities of nodes [3, 4].

Understanding node mobility is one of the keys to determine the potential capacity of an ad hoc network [5]. Network resources such as bandwidth and power have to be dealt with in fundamentally different ways compared to wireline or centralized cellular networks [6]. A mobility model is one of the most important components in the simulation of MANETs. This component describes the movement pattern of mobile nodes, impacting on protocol performance, topology and network connectivity, data replication, and security [7]. OLSR (Optimized Link State Routing Protocol), as a widely used and well tested protocol, is one of the main two Internet standards for wireless networks. However, MANET is involved in some other issues, such as instability [8]. Optimized Link State Routing (OLSR) is a proactive optimized link state routing protocol. The optimization results in reduced control and traffic message flooding into the network with the help of MPRs nodes, the selected division of one-hop neighbors [9].

1.1 Organization of thesis

In this work, we propose a new technique for attack analysis and designing of quality of service framework justifying optimized link state routing protocol in MANET. Initially the nodes are clustered using Hybrid K-means algorithm. Once the clustering is done path is formed based on optimized link state routing protocol. The routing is done by optimizing the nodes with the aid of Hybrid Genetic algorithm (GA).

Reminder of the paper is organized as follows. In Section 1 introduction work is discussed. In section 2 the related work is discussed. Section 3 presents problem identification of the existing studies. In section 4 presents the proposed attack analysis and designing the quality of services. The performance evaluation results and the experimental environment are presented in Section 5. Section 6 concludes the paper and presents future works.

2. Related work

Numerous researches have been done in the field of MANET for improving the mobility metrics. Some of the recent researches done in the field of MANET are given below,

Opportunistic data forwarding has drawn much attention in the research community of multi-hop wireless networking, with most research conducted for stationary wireless networks. One of the reasons why opportunistic data forwarding has not been widely utilized in mobile ad hoc networks (MANETs) was the lack of an efficient, light-weight proactive routing scheme with strong source routing capability. Wang *et al.* [10] have proposed a light-weight Proactive Source Routing protocol, PSR. PSR could maintain more network topology information than distance vector routing to facilitate source routing.

A Mobile Ad-Hoc Network (MANET) was a self-configured or an infrastructure less set of mobile nodes that could change their geographic positions randomly such that these networks have dynamic configurations and random mobility with restrained resources. It often works by flooding the information. Its behavior was broadcasting so there was a chance to interrupt network by intruder. The number of attack could be performed in Mobile Ad Hoc Network. Renu Sharma and Praveen Sharma [11] have examined several mechanisms to determine and prevent wormhole attack and compare them.

Son *et al.* [12] have introduced a routing model which has the ability to detect the mobile ad-hoc network (MANET) mobility states and self-adapt routing metrics accordingly. The proposed model takes advantages of both ETX and MF metrics thus enhancing the overall routing performance for MANET in different mobility states. Packet delivery ratio increases 10% in both static and mobile conditions whereas the number of drop packets reduces half compared with the original optimized link state routing protocol.

In OLSR, link state information was generated only by nodes elected as MPRs. Thus, optimization was achieved by minimizing the number of control messages flooded in the network. However, security, trust, and robustness were still a sizable challenge for OLSR. Hajare and Tijare [13] have first highlighted potential attacks, vulnerabilities, and key countermeasure points of OLSR in terms of security. Based on this analysis, they proposed a robust OLSR protocol for ad hoc network. They also demonstrated that the proposed protocol could defend against various sophisticated attacks.

A hybrid broadcast scheme for mobile wireless networks was proposed by Reina *et al.* [14]. The main objective was to combine different flooding schemes in order to solve the broadcast storm issue encountered by the simple flooding scheme. For this purpose, the density of nodes was taken into account using a density metric called expansion metric. In addition, in order to reduce the broken links due to mobility of nodes and increasing dissimilarity among the intermediate nodes, a forwarding zone criterion was included in the proposed schemes. The proposed approaches have been implemented and compared with pure probabilistic flooding, and simple flooding schemes.

MANET plays an important role in emergency communications where network needs to be constructed temporarily and quickly. Since the nodes move randomly, routing protocols must be highly effective and reliable to guarantee successful packet delivery. Based on the data delivery structure, most of the existing multicast routing protocols could be classified into two folders: tree-based and mesh-based. The tree based multicast routing protocol; MAODV (Multicast Ad hoc On-demand Vector) shows an excellent performance in lightweight ad hoc networks. Xu *et al.*[15] have analyzed the impact of network load on MAODV protocol, and proposed an optimized protocol MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves robustness of the MAODV protocol by combining advantages of the tree structure and the mesh structure. It not only could update shorter tree branches but also constructed a multicast tree with backup branches.

3. Problem identification

Mobile networks receive increasing research interest recently; mobile ad hoc networks (MANET) and vehicular ad hoc networks (VANET) are two prominent examples. In many real world networks, an interesting application is to broadcast the information from some source node to the whole network. For wireless ad hoc and sensor networks, a node triggered by the event of interest may want to inform the whole network about the situation as quickly as possible.

- Effect on information spreading is still not efficient.
- The transmission is subjected to wide range of attacks.
- The information spreading speeds up or slows down effectiveness.
- Quantify the potential improvement or degradation due to mobility.
- However, existing group mobility metrics cannot assess quantitatively whether a mobility model can provide the necessary degree of group mobility. In our proposed Multi-hop networks have limitations, possibly resulting in misleading results.
- The MANET are very sensitive to attacks and can lead to loss of information while transmission. In this work, we propose a new technique for attack analysis and designing of quality of service framework justifying optimized link state routing protocol in MANET.

4. Proposed methodology

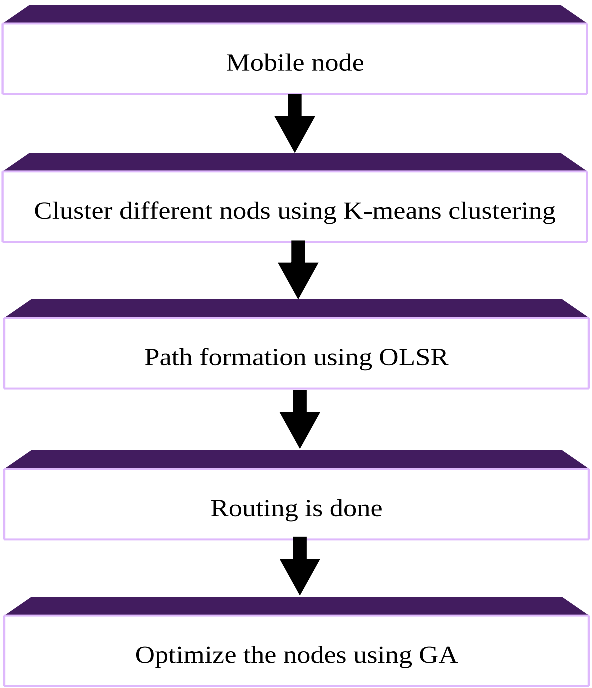

Mobile node
Cluster different nods using K-means clustering
Path formation using OLSR
Routing is done
Optimize the nodes using GA

Figure. 1 Proposed attack analysis based on OLSR MANET

In highly mobile networks, mobility based clustering schemes exploit the group mobility of nodes to form stable communication structure by grouping nodes with similar mobility pattern together. However, existing group mobility metrics cannot assess quantitatively whether a mobility model can provide the necessary degree of group mobility. Multi-hop networks have limitations, possibly resulting in misleading results. The MANET are very sensitive to attacks and can lead to loss of information while transmission. In this work, we propose a new technique for attack analysis and designing of quality of service framework justifying optimized link state routing protocol in Manet. Here we have utilized soft computing technique for the selection of nodes in order to provide accurate means of transmission of data. Initially the nodes are clustered using Hybrid K means algorithm. Once the clustering is done path is formed based on optimized link state routing protocol. The routing is done by optimizing the nodes with the aid of Hybrid Genetic algorithm (GA). The implementation is done in NS2/NS3 platform and the results obtained are compared with various existing methods in order to prove the efficiency of our proposed technique.

4.1. Mobile ad-hoc network (MANET)

Ad hoc networks form spontaneously without a need of an infrastructure or centralized controller. The type of peer-to-peer system infers that each node, or user, in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. These types of networks are also popularly known to as “mesh networks” because the topology of network communications resembles a mesh [2]. Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), unidirectional (broadcast), probably steerable, or some combination. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

In MANET, nodes are not sure of connectivity when they move. They face considerable delay. The routing protocol use store and forward technique. A protocol is suggested about opportunistic routing with media access control in delay tolerant network. The MAC protocol utilizes characteristic of broadcasting in wireless medium and the nodes working together participate by swapping RST/CTS/DATA/ACK. The routing protocol uses store and forward technique for taking end to end reliability. The used protocol states that each node must know its velocity and position and that its movement is regular, so the ad-hoc networks use the nodes of GPS devices. The mobility-aware protocol shows the best performance than other protocols of delay tolerant (epidemic routing, geographic routing, and stray-and-wait routing) resulting small packet delay and total packet transmission.

In MANET technology various protocols are developed by programmers. MANET uses the concept of (SMP) shortest mobile path in a mobile graph for checking routing protocol. There is a comparison that the protocol uses the mean ratio of cost of route with the optimal path for same network. The protocol change resulting due to change over time. The MEAN REALVS IDEAL COSTMERIT spectrum is the representation of protocol effectiveness and it is a scalable framework instead of checking several protocols directly; compare the optimal solution of protocol as focus the comparison in same system; check in its environment one time for each protocol. The MERIT framework is good with wider generality and potential applicability as compared with routing protocol.

The characteristics ofthese networks are summarized as follows: Communication via wireless means.

- Nodes can perform the roles of both hosts and routers.
- Bandwidth-constrained, variable capacity links.
- Dynamic network topology.
- Frequent routing updates

In this MANET based attack analysis research contains some attacks initially by clustering these attacks by finding different nodes with the aid of k-means clustering technique.

Attacks

Dynamic nature, decentralized approach and infrastructure less makes MANET vulnerable to attacks. There are various attacks that can occur in the Mobile Adhoc networks. Some of them are discussed in this paper like various networks; there are two kinds of attacks in MANET; passive and active. Passive attacks do not change the data transmitted over network, instead it attempts to explore the sensitive information from the traffic that is routed in the network. A node that attack passively may act selfish to catch the transmitted information. Passive attackers are difficult to detect as they do not disturb the normality of network. Encryption is normally used to fight against passive attacks. Active attacks create hurdles in message flow between nodes Attackers inject the erroneous information to the network. These attacks can occur at network, transport, application or any other protocol layer. Active attacks are more severe and are of two types internal and external. External attacks are executed by unauthorized source. Internal attacks are performed by selfish nodes. These attacks because unauthorized access to network that allow the enemy to make certain alteration in network. Active attacks are categorized into four groups:

Active Attacks: In these attacks attacker tries to gain access to the system’s data and then drop, alter and fabricate the data in order to affect the system. Such type of attacks can be easily detected as they are modifying and dropping the packets. Active attack can be external as well as internal.

Passive Attacks: In these attacks, attacker only seeks information, but doesn’t affect the system by using this information. The attacker listens to the channel, record patterns, analyze them. These types of attacks are difficult to detect as they are not changing data, and are not affecting the system. Encryption algorithms should be used in order to prevent these attacks.

Modification Attacks: These attacks disturb the overall communication among nodes by altering the data packets. Compromised nodes publicize itself in such manner that it provides shortest and smallest path to final receiver. By doing so, malicious nodes then catch routing information and use it for more attacks. Sinkhole attack is an instance of modification attack.

Dropping Attacks: In MANET all nodes are supposed to forward packets towards the destination node. In this Attack, selfish nodes do not forward packets to any node; instead discard them to disturb the operation of network. End-to-end communication among nodes is avoided by selfish nodes, if the dropping hop is at crucial edge. Several routing protocols use no such tools that detect either datagram have been sent to destination or not.

Timing Attacks: In timing attacks, attacker publicizes itself in such a way that it is closer to the final destination node, having optimal path, to attract other nodes. Hello flood and rushing attacks use this technique.

Fabrication Attacks: In this attack, without getting any analogous message the malicious user forward fake information to its neighboring nodes. In response to related legal route request message, the attackers can also send false packets. The attributes of MANETs make them exposed to further attacks. In accordance with particular layer there are several types of attacks which differ in their nature. Attacks at different layers are defined below. Initially the input contains a no of nodes we will cluster different kinds of nodes using k-means clustering technique it will be explained in below section.

4.2. K-means clustering algorithm

A standout amongst the most broadly utilized grouping calculations is K-Means grouping. This minimizes the mean squared Euclidean separation from every information point to its closest focus. Here we have a decent control upon the quantity of groups delivered. So, while diminishing the test suit contingent on the quantity of administrations we can settle the estimation of k. The K-Means Clustering method has risen as one of the most straightforward unconfirmed learning strategies which are very much outfitted with the abilities of discovering compelling answers for the well known grouping difficulties generally, the importance of the grouping methodologies is making progress as they are broadly utilized in various applications. The basic procedure utilizes a simple and easy technique to order indicated documents into a particular number of groups. The mind blowing capability of the first means method owes a great deal to the underlying centroids, which tellingly affect the quantity of cycles required for executing the first k-implies procedure. Nonetheless, computational difficulty of the first k-implies calculation is observed to be profoundly over the top, especially in admiration of monstrous gigantic records. The present examination is put resources into propelling an enhanced procedure for finding the top positioning group record. Here we will use this k-means clustering technique is used to cluster a different kind of nodes.

The quantity of groups K is esteemed to be changeless in the k-implies grouping system. Let K models ($\omega_1 \dots\dots \omega_k$) be actuated into one of the n input administrations *($i_1 \dots\dots i_n$)*. Henceforth

$$\omega_j = i_1, j \in \{1, \dots, k\}, i \in \{1, \dots, n\} \qquad (1)$$

The reasonable determination of k constantly relies on upon the issue and space and chronically a client endeavors various estimations of k. It is assumed that there are n benefits, each of measurements d.

Step1: Randomly pick k focuses as centroids of k groups.

Step2: For every point dole out the point to the closest group.

- Recomputed the group centroids.
- Repeat Step2 (until there is no adjustment in groups between back to back emphases). With this thought of what k-Means do now we are going to talk about specific actualities regarding group conduct.
- Grouping is to gathering information things having high likeness and to isolate from disparate information things.
- The nature of a group is characterized as high intra group likeness and low bury group comparability. Having grouped our information, we now require some component to pick experiments from every group. In the following segment we utilized a calculation called Pickup group that does the determination work. Steps for our proposed k-means clustering is given below,

Input: *The no of Input nodes*

Output: *A set of different nodes*

Identifying unique nodes from the given input

1. Selection of weight for the nodes

2. Specifying the value of k (number of clusters)

3. Randomly select K nodes and place one K selected nodes in each cluster based on its weight

4. Compute centroid for each K-Clusters

5. Compute weight of each nodes r for each K-Clusters

6. Again using weight Wi for each nodes, Find the distance between the centroid and weight Wi

7. Now place the nodes in the cluster based on similarity between nodes and the centroid of clusters.

In our proposed k-means clustering technique will cluster different kinds of nodes from the input now the route will be find with the aid of Optimal Link State Routing Protocol.

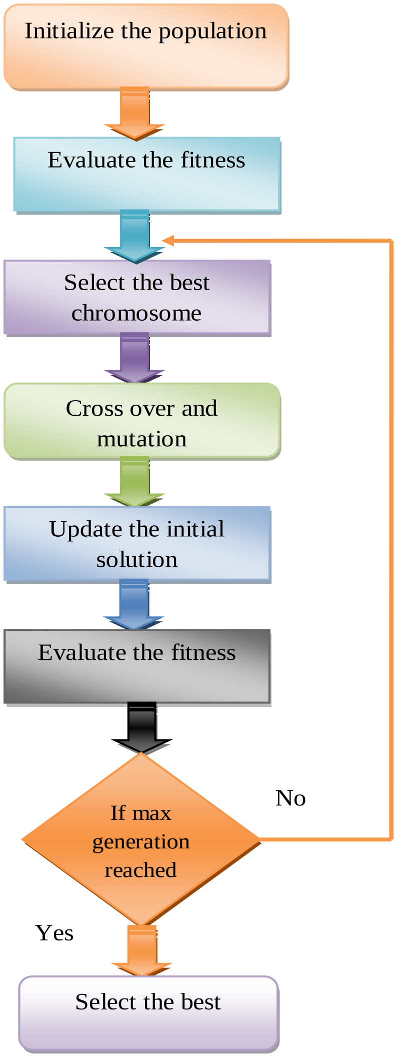
4.3. Optimized link state routing (OLSR)

Here we introduce a optimal link space routing is used to find a route with the aid of this Optimized Link State Protocol (OLSR) is a proactive routing protocol, so the routes are always immediately available when needed. OLSR is an optimization version of a pure link state protocol. So, the topological changes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network protocol uses flooding of broadcast in some regions in this chapter. Another reduce is to provide a shortest path. The reducing the time interval for the control messages transmission can bring reactivity to the topological changes. Here, route information always stored in table. Therefore, route is always available when needed. Thus, being proactive delay is less as no waiting will be there for route discovery. Link state packets are being forwarded for topology information which is called Multi point relay (MPR). Here, each node selects its MPR from neighbor nodes.

Periodic exchange of link state packets will be done in order to gather information about the nodes and their topology. OLSR uses two kinds of the control messages. Hello and Topology control (TC). Hello message are used for finding the information about the link status and the host's neighbor. With the Hello massage the multipoint relay (MPR) selector set is constructed which describes which neighbor has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. the Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages. These optimal link states routing protocol is used to find the optimal route for sending nodes.

Merits

- OLSR is distributed protocol so no central administration to handle the routing process.
- The link is reliable since the update messages are sent periodically.
- OLSR works well with for large and high density networks as optimization is done by using MPRs.
- Routes are always available so no route discovery delays for finding a route.


Initialize the population
Evaluate the fitness
Select the best chromosome
Cross over and mutation
Update the initial solution
Evaluate the fitness
If max generation reached
No
Yes
Select the best

❖

❖ Figure. 2 Flow chart for Genetic Algorithm

4.4. Genetic algorithm (GA)

Genetic Algorithm is adaptive global search algorithm based on the evolutionary data of genetics. In order to work out the optimization problems Genetic Algorithm is an arbitrary search algorithm applied. Iterations are symbolized as generation and the population is symbolized as chromosomes in genetic algorithm.

Now the input of genetic algorithm is the consequence of test case generation. The specified process of genetic algorithm is made cleared beneath, in our proposed research we will utilize this genetic algorithm for optimization process with the aid of theses algorithm we will select a node.

Step 1: Initial Phase

In genetic algorithm, at first produce the population of chromosomes S_i $(i=1, 2, 3 \ldots N)$ randomly. N represents the population size.

Step 2: Fitness Evaluation

Assess the fitness function of each chromosome and the highest fitness value is chosen as the best one.

$$F = S(V), R(V), L\&LC \quad (2)$$

Where, F- Fitness
$S(V)$ – Sum of if value
$R(V)$ – Ratio Value
$L \& LC$ – Line & Loop Coverage

Step 3: Cross over to the best solution

One or more parent chromosomes are selected and carry out the single point cross over

Step 4: Mutation

In mutation process chromosome values are differed according to the possibility after that produced novel chromosome.

Step 5: Updation

The present chromosome is substituted with the novel chromosome in this step

Step 6: Discover the fitness function

If the fitness value of novel chromosome is greater than the present chromosome. Choose the novel chromosome is the best chromosome. The optimal result will be contrasted to all the function after getting result from the adaptive genetic algorithm. Eliminate from the application if any function not in the optimal result the consequent function. Hence that adaptive genetic algorithm attains decrease of faults rate based on the optimal test case. In our proposed results of k-means clustering technique we obtain requires clustered results for our proposed method. The false reduction is obtained with the aid of optimization algorithm. Here we using a Gray wolf optimization results based on the fitness value that we assigned for combinatorial testing. Our method, the result of GSO is reducing the fault only not reducing the test cases hence by using the GA we obtain required test cases for our proposed method. After getting result from the adaptive genetic algorithm, the optimal result will be compare to all the function. If any function not in the optimal result the corresponding function remove from the application. So that adaptive genetic algorithm achieves reduction of faults rate based on the optimal test case.

5. Result and discussion

This section gives a detailed view of the results that are obtained using our proposed Optimal Link State Routing Protocol. We have proposed the cluster formation clustering is done path is formed based on optimized link state routing protocol. The routing is done by optimizing the nodes with the aid of Genetic Algorithm. The proposed method is implemented in NS2. The experimental result and the performance of the proposed method are clearly explained in the following section.

5.1. Evaluation metrics

By using the evaluation metrics end to end delay, Packet delivery Fraction and throughput, overhead the performance of the recommended system is evaluated.

Throughput

It is the measure of how fast a node can actually sent the data through a network. So7 throughput is the average rate of successful message delivery over a communication channel.

Packet delivery fraction (PDF)

The packet delivery ratio in this simulation is defined as the ratio between the number of packets sent by constant bit rate sources and the number of packets received by the CBR sink at destination.

$$PDF = \frac{CBR \overset{PD}{\longrightarrow} CBR}{CBR \overset{PS}{\longleftarrow} CBR} \quad (3)$$

Where, PDF – Packet Delivery Fraction
PD – Packet Delivery
PS – Packet Send

End-to-End Delay of data packets (AED)

The end-to-end delay is defined as time between the point in time the source wants to send a packet and the moment the packet reaches its destination. It includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

$$AED = \sum \frac{T(DRP) - T(DSP)}{N(SP)} \quad (4)$$

Where, AED - Average End to End Delay
DRP – Destination Received Packet
DSP – Destination Source Packet
$N(SP)$ – Number of Source Packet

5.2. Comparison analysis of recommended technique

This section provides the clear view on the comparison of the proposed method with the existing method with respect to delay, packet delivery fraction and throughput value. In our proposed method the mobile nodes collect the information from the cluster MANET are very sensitive to attacks and can lead to loss of information while transmission. The data transmission in proposed method (OLSR) occurs with maximum data gathering capacity and cluster head selection and shortest path selection in reaching the sink node. But in the existing method there is no cluster head selection and hence the information is gathered from all the nodes (AODV and DSDV). This is explained in the form of table and graph; it is shown in below,

Here we have compare our proposed research with the existing reference [16]. The graphical representation of the delay comparison results for proposed and existing method is plotted in beneath, For 40 nodes the delay obtained using OLSR is 807% and the delay obtained using AODV is 956%and delay obtained using DSDV is 2461%. For 50 nodes the delay obtained using OLSR is 526% and the delay obtained using AODV is 865% and delay obtained using DSDV is 2625%. For 60 nodes the delay obtained for OLSR is 395% and the delay obtained using ADOV is 882%and delay obtained using DSDV is 1282%. For 70 nodes the delay obtained for OLSR is 294% and the delay obtained using ADOV is 585% and delay obtained using DEDV is 1148%. For 80 nodes the delay obtained for OLSR is 342% and the delay obtained using ADOV is 599% and delay obtained for DEDV is 2107%. When we compare these proposed and existing results we prove that our proposed OLSR has given better results.

Table 1. Delay comparison of proposed and existing method

Node	OLSR (Proposed Method)	AODV (Existing Method)	DSDV (Existing Method)
40	807	956	2461
50	526	865	2625
60	395	882	1281
70	294	585	1148
80	342	599	2107

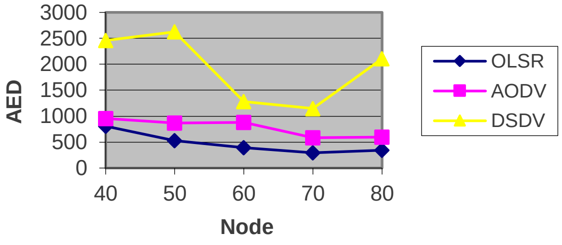


Figure. 3 Graph for delay comparison

Table 2. Packet delivery fraction comparison for proposed and existing method

Nodes	OLSR	AODV	DSDV
40	75	72	47
50	76	47	44
60	84	46	53
70	94	69	60
80	81	68	55

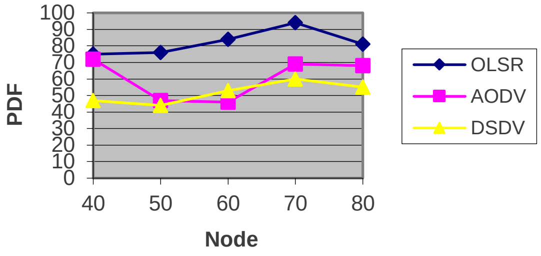


Figure. 4 Graph for packet delivery fraction comparison for proposed and existing method

The graphical representation of the packet delivery fraction comparison results for proposed and existing method is plotted in above, 50 nodes the

For nodes 40 obtained packet delivery fraction using OLSR is 75% and the delivery obtained for using AODV is 72% and the delivery fraction obtained for DSDV is 47%. For nodes 50 obtained packet delivery fraction using OLSR is 76% and the delivery obtained for AODV is 47% and delivery obtained for DSDV is 44%. For 60 the packet delivery fraction obtained for OLSR is 84% and delivery obtained for using AODV is 46% and delivery obtained for DSDV is 53%. For nodes 70

Table 3. Throughput comparison for proposed and existing method

Nodes	OLSR	AODV	DSDV
40	4041	3989	1547
50	6207	4399	1449
60	8250	4312	2970
70	11091	6498	3318
80	9525	6349	1808

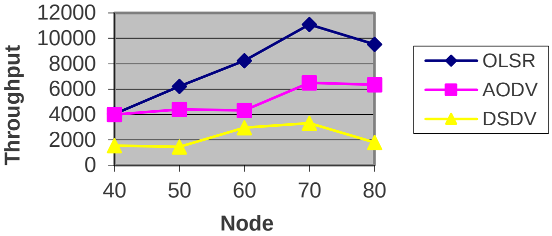


Figure. 5 Graph for throughput comparison for proposed and existing method

packet delivery fraction obtained for OLSR is 94% and delivery obtained for using ADOV is 69% and delivery obtained for DSDV is 60%. For nodes 70 packet delivery fraction obtained for 70 is 81% and the delivery obtained for ADOV is 68% and the delivery obtained for DSDV is 55%. When we compare our proposed and existing researches we prove that our proposed OLSR will obtained better results.

The graphical representation of the Throughput comparison results for proposed and existing method is plotted in above. For 40 nodes the throughput is 4.41% using OLSR while using AODV and DSDV the throughput is 3983% and 1547%. 6207% of throughput is needed for the proposed method for 50 nodes while 4399% and 1449%of throughput is needed for the existing method. The throughput value is 8250% using proposed method for 60 nodes while the throughput value is 4312% and 2970% using the existing method. For 70 nodes the value of throughput is 11091% using OLSR while using AODV and DSDV the value of throughput is 6498% and 3318%. The value of throughput is 9525% using the proposed method for 80 nodes while using the existing method the value of throughput is 6349% and 1808%. Hence, from the above analysis it is clear that the proposed method performs better than the existing method in terms of Average End to End Delay, Packet Delivery Fraction, and Throughput. Generally the Objective of this paper is to Study two common Proactive protocols (DSDV & OLSR) for secure QoS incorporation, selecting a protocol with promising performance for SECURE QOS, proposing and implementing BW aware route discovery for the selected protocol and study the performance achieved. We will discuss in detail our idea of adding Secure Qos into the OLSR protocol. Our algorithm allows OLSR to find the maximum bandwidth path with optimal number of MPR

6. Conclusion

In MANET, routing attack is particularly a major concern. In this paper, we have presented a routing attack, called OLSR-based mobile ad hoc network. In our proposed research we have compare our work with existing method to prove our proposed research will give better results. The data transmission in proposed method (OLSR) occurs with maximum data gathering capacity and cluster head selection and shortest path selection in reaching the sink node. But in the existing method there is no cluster head selection and hence the information is gathered from all the nodes (AODV and DSDV). Currently, we are seriously working on this issue. Our future work will also be focused on investigating other sophisticated attacks which have not been well studied as well as studying the possible countermeasure against such attacks

Reference

[1] S. V. Yeruru and T. R. Rangaswamy, “An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad Hoc Network”, *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 4, pp. 81-90, 2017.

[2] S. V. Yeruru and T. R. Rangaswamy, “An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad Hoc Network”, *International Journal of Intelligence Engineering and Syatems*, Vol.10, No.4, pp. 81-90, 2017.

[3] V. Yerur, P. Natarajan and T. R. Rangaswamy, “Proactive Hybrid Intrusion Prevention System for Mobile Adhoc Networks”, *International Journal of Intelligent Engineering and Systems*, Vol.10, No.6, pp. 273-283, 2017.

[4] S. R. Inamdar, S. B. Basavaiah and R. M. Yadahalli, “Co-Operative Directional Routing Protocol for MANET”, *International Journal of Intelligent Engineering and Systems*, Vol. 11, No.2, pp. 93-101, 2018.

[5] S. Xu, K. L. Blackmore, and H. M. Jones, “An Analysis Framework for Mobility Metrics in Mobile Ad Hoc Networks”, *Journal on Wireless Communications and Networking,* Vol.2007, 2007.

[6] C. Curescu and S. Nadjm-Tehrani, “A Bidding Algorithm for Optimized Utility-Based Resource Allocation in Ad Hoc Networks”, *IEEE Transactions on Mobile Computing,* Vol.7, No.12, 2008.

[7] E. R. Cavalcanti and M. A. Spohn, “Improved Spatial and Temporal Mobility Metrics for Mobile Ad Hoc Networks”, In: *Proc. of the Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies,* pp.189-195, 2010.

[8] Z. Yihui, Q. Xirong, W. Wendong, G. Xiangyang and M. jian, “N3S-OLSR: Node-Status Self-Sensing Optimized Link-State Routing Protocols for MANET”, In: *Proc. of 2010 International Conference on Communications and Mobile Computing,* 2010.

[9] K. T. Selvi and S. Kuppuswami, “Enhancing Security in Optimized Link State Routing Protocol for MANET using Threshold Cryptography Technique”, In: *Proc. of International Conference on Recent Trends in Information Technology,* 2014.

[10] Z. Wang, Y. Chen, and C. Li, “PSR: a Light-Weight Proactive Source Routing Protocol For Mobile Ad Hoc Networks”, *IEEE Transactions on Vehicular Technology,* Vol.63, No.2, 2014.

[11] R. Sharma and P. Sharma, “Detection and Prevention of Wormhole Attack in MANETs: A Review”, *International Journal of Science, Engineering and Technology Research,* Vol.5, No.5, 2016.

[12] H. L. Minh, G. Sexton, and N. Aslam, “Self-adaptive proactive routing scheme for mobile ad-hoc networks”, *IET Networks,* Vol.4, No.2, pp.128–136, 2015

[13] P. A. Hajare and P. A. Tijare, “Secure Optimized Link State Routing Protocol for Ad-Hoc Networks”, *International Journal of Computer Science and Information Technologies,* Vol.3, No.1, pp.3053-3058, 2012.

[14] D. G. Reina, S. L. Toral, P. Jonhson, and F. Barrero, “Hybrid Flooding Scheme for Mobile Ad Hoc Networks”, *IEEE Communications Letters,* Vol.17, No.3, 2013.

[15] X. Li, T. Liu, Y. Liu, and Y. Tang, “Optimized Multicast Routing Algorithm Based on Tree Structure in MANETs”, *China Communications,* Vol.11, No.2, 2014.

[16] A. K. Jain, “Performance Based Secure Optimized Routing Protocol for Mobile Ad-Hoc Network”, *International Journal of Global Research in Computer Science*, Vol.3, No.4, 2012.