Novelty Journals

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

Detection of Malicious Nodes Using Path Validation Message and Attacker Find Message in Mobile Ad-Hoc Network

[1]Ms. Bageshree U Chavan , [2]Prof. K. A. Adoni

[1,2] ME: E & TC dept., P.E.S'S Modern College of Engineering, Pune, India

Abstract: **Mobile Ad hoc Networks (MANET) are dynamic and self organized networks. Nodes in the network can operate independently. The nodes are wireless devices, can act as source, destination and routers. They cooperatively provide multi-hop communication. MANET routing devices are battery operated. The main task of MANET routing protocol is to transfer data between communicating parties successfully without any errors. Each node in the network must co-operate effectively and efficiently. MANETs are susceptible to various types of security attacks. Due to limited bandwidth, battery power, topology etc. nodes misbehave and degrade the system performance. A Modified Malicious free OLSR (OLSRMM) protocol mechanism is proposed using Path Validation Message (PVM) and Attacker Find Message (AFM). PVM verifies the validity of different paths along which the data packets can be transmitted. The security feature in OLSRMM is divided in two parts. The first part validates the communication path by sending periodic PVM messages. The second part is concern about finding malicious node in the invalid path using AFM messages. OLSRMM accurately detects malicious nodes in MANET based on End-to-End (E2E) communication between the source and the destination and avoids those malicious nodes for the communication. It ensures the selection of path with non-malicious nodes to forward the data traffic.**

Keywords: **MANET, OLSR, OLSRMM, PVM, AFM, E2E.**

I. INTRODUCTION

Many times building an infrastructure at some places is difficult or impractical e.g. disaster, earthquake, mines, military applications. Sometimes it is not economical e.g. two day conference, seminars on lawn, urgent business meetings. To overcome this difficulty MANET are used. It doesn't require any infrastructure during its setup. The communication of independent mobile nodes in MANET is through radio waves [1]. The mobile nodes present in radio range of each other can directly communicate, whereas other nodes take the help of intermediate nodes to route their packets. Nodes can appear, disappear and reappear as the time goes on. All the time the network connections should work between the nodes that are part of it. MANET is fully distributed and can work at any place without the help of any infrastructure in the particular range. This makes MANET highly robust.

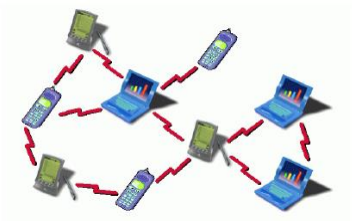

Fig.1. Mobile ad-hoc network

The communication in MANET comprises two phase's viz. the route discovery and data transmission [17]. To provide security to MANET at network layer, both phases of communication must be safeguarded [2]. One way is to secure the routing protocols by detecting malicious nodes in order to prevent the possible attacks [17]. The aim of the proposed mechanism is to detect malicious node in MANET and improve the performance of the network to avoid degradation.

The standard OLSR protocol is not secured one. To forward data packets during transmission in the network it selects shortest path, so some of the nodes may be used repetitively. The system performance of the network is been degraded due to the presence of malicious nodes in the network. To avoid this Multipath OLSR protocol (OLSRM) is used in which maximum number of nodes are participating in communication [2]. OLSRM protocol can detect malicious nodes but is not able to avoid the path containing malicious node during transmission. In this thesis, OLSRM protocol is modified to detect misbehavior nodes in the network named as "Malicious free Modified OLSR (OLSRMM)" protocol, and avoid those malicious nodes for the communication. It ensures the selection of path with non-malicious nodes to forward the data traffic.

II. OPTIMIZED LINK STATE ROUTING PROTOCOL

OLSR is the table driven, proactive routing protocol designed for mobile ad-hoc networks [2]. The routing information is exchanged periodically and when needed routes are immediately available. The OLSR protocol achieves optimization by determining for each node of the network a minimal subset of neighbors, called Multi Point Relays (MPR) [2]. They are able to reach all 2-hop neighbors of the node. In OLSR two types of routing messages are used a HELLO message and a Topology Control (TC) message [2].

1) HELLO message:

- It is periodically broadcasted by each node and has the sender's identity [2]:

a) List of neighbors from which control traffic has been heard.

b) List of neighbors with which bi-directionality has already confirmed.

c) List of MPR set of originator node.

- HELLO messages are forwarded by neighbor nodes. It is used for neighbor sensing, for selection of MPRs nodes.

2) TC messages:

- It is transmitted by MPR nodes periodically. They contain the list of the sender's MPR selector set [2].

In OLSR, only MPR nodes are suppose to forward TC messages. After receiving TC messages from all of the MPR nodes, all nodes are aware of the partial network topology and can build a path to every node in the network. TC message is used for route calculation.

The OLSR operation can be summarized as follows [2]:

1) Neighbor sensing: Is achieved by broadcasting HELLO messages to its 1-hop neighbors periodically.

2) MPR selection : There are two types of sets

a) MPR set – It is a set of selected neighbor nodes for each specific node from its 1-hop neighbors. After sending a routing message through nodes, only the nodes that are in its MPR set are responsible to forward this message.

b) MPR selector set - Each node also maintains information about the set of neighbors that selected it as MPR called as MPR selector set [2].

All nodes select and maintain their own MPR's. To select a node as MPR, for all two hop neighbor 'n' their must exist a MPR 'm' so that 'n' can be contacted via 'm' as shown in below fig.2

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

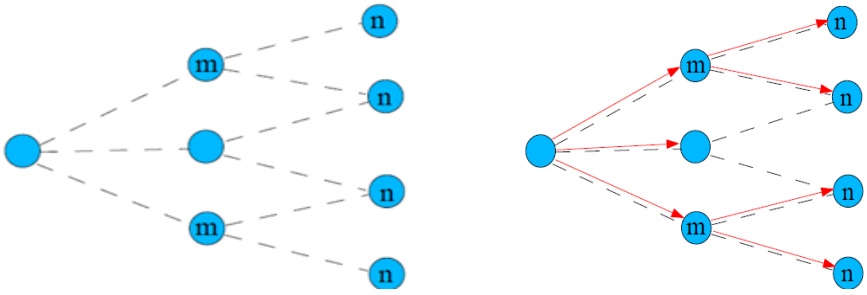

Fig. 2(a) **Fig. 2(b)**

Fig.2. Selection of MPR nodes

3) Topology Generation: Nodes which were selected as MPR must send TC messages in order to construct routing table. TC messages are flooded in the network and further they are forwarded by only MPRs.

Each node in OLSR protocol has two tasks:

i) Correctly generate the routing protocol control traffic

ii) Correctly relay the routing protocol control traffic on behalf of other nodes.

III. RELATED WORK

Routing in a MANET is done to find a short and optimized route from the source node to the destination node. Number of protocols has been developed for ad-hoc mobile network, but these routing protocols are not secured; they are vulnerable to several types of security attacks. Malicious nodes can degrade the network performance, so it is essential to detect these misbehaving nodes. The rigorous work is going on to provide security in MANET routing protocols, some of them are as follows.

Ahmed M.Abdalla et al. [2] presented an IDS mechanism, based on End-to-End connection for securing the OLSR protocol. This mechanism can detect types of misbehavior nodes through the path between the source and the destination, and then the blacklist of misbehavior nodes is created. This mechanism is able to detect any number of attackers and also in terms of network traffic the proposed solution keeps a reasonably low overhead.

Dr. Rajaram Marimuthu et al. [3] developed a security framework which involves: Detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention of data packets by using dispersion technique. A MRR (Multipath Reliable Routing) algorithm is developed which determines a set of node-disjoint reliable paths and proposed a frame work which reduces overhead, Delay and increases packet delivery ratio.

Anil Kumar Gupta, et al. [4] proposed and approach that improves the conventional AODV routing protocol in terms of packet loss, in presence of malicious nodes. If data is forwarded to affected nodes it leads to severe data loss, since they do not forward data packets. The proposed approach guarantees that data is never forwarded to such nodes. There is decrease in packet loss Trusted AODV decreased packet loss in presence of malicious nodes. Hence, the proposed approach helps in reducing data loss in presence of malicious nodes .

Hiba Sanadiki, et al. [5] identified spoofing and wormhole attacks as possible attacks against QoS-OLSR protocol. These attacks isolate some head nodes and have disconnected clusters which degrade the network performance [5]. To detect the two possible attacks, a novel detection approach is presented based on the cooperation among watchdogs where the reputation of nodes is considered [5]. The detection was then enhanced by adding the posterior belief function that increases the true detection and decreases the false detection rates.

Mohanapriya Marimuthu, et al. [6] analyzed the vulnerabilities of an OLSR protocol against an attack called as Denial-of-service (DOS) attack, also called as Node isolation attack. They have proposed a trust based technique known as EOLSR (Enhanced OLSR) protocol [6]. EOLSR verifies its HELLO packets and finds whether a node is transmitting correct topology information or not. Thus detecting DOS attack [6].

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

The original OLSR protocol is not secured one. In the present paper OLSR protocol is modified to detect misbehavior nodes in the network and avoid those malicious nodes for the communication. It ensures the selection of path with non-malicious nodes to forward the data traffic.

IV. PROPOSED MECHANISM FOR DETECTING MISBEHAVIOUR NODES

We extend the security of OLSR in two parts. The first part validates the communication path by sending periodic messages. The second part is concern about finding malicious node in the invalid path. The successfully detected malicious node is added to black-list and is excluded from the routing table.

Every time the node receives a new HELLO message. It updates 2-hop neighborhood list and find MPR nodes. Neighbors set are formed and choose one MPR among neighbors. Update 2 hop neighborhood list and form table. TC messages are exchanged in each MPR nodes, and find path to destination.

ALGORITHM:

The algorithm to obtain the 'M' paths from source to destination and constructs MPR selector set is,

1. Select the link with more energy in all the output links which start from all nodes 'n' at the beginning

2. Form a network of 'N' nodes and fix few nodes 'n' as attackers

3. Destination computes high energy path and reply to the source with top three highest energy paths.

4. Once reply received within the time from source, it send path validation message to destination and destination node must acknowledge back to the source with a Path Validation Message reply $(PVM)_r$ within time period source need to get reply, to verify the validity of path which transmits data packets, as shown in Fig. 3.

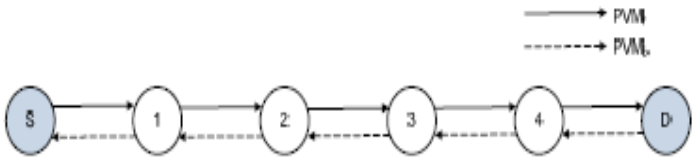

Fig.3. PVM process

5. If reply not received within time as shown in fig.4, start again PVM and increment the number of failed PVM. 'N' failed PVM's mean there is a problem in the path. If PVM fail count > 3 start Attacker find message (AFM)

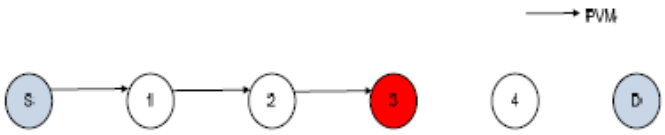

Fig.4.Attacker drop data packets

6. Then source send attack find message AFM and it need to get reply of each routing path node hop count and ID through source which can construct Next Node To Destination (NNTD) info in NNTD table. AFM is send to the destination through NNTD. Now start type 1 attack checking as shown in below Fig.5.

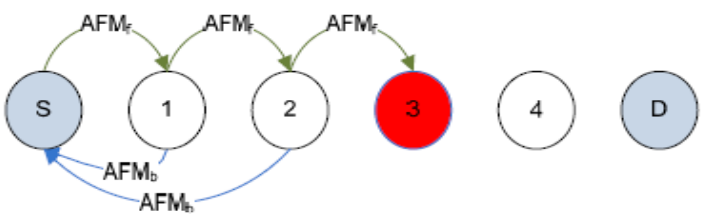

Fig.5. AFM process

7. NNTD has 2-hop neighborhood information.

8. Check all 2-hop neighborhood ID, energy level and then choose MPR node with high energy.

9. If MPR entry in attacker list, eliminate that node entry and broadcast all nodes about attackers. Last NNTD known by source is known to be type-1 attacker.

10. Start timer to get reply, source updates each node path and next neighbor ID.

11. Then Source starts PVM to each routing paths node and wait for reply within timer as type-2 checking.

12. If source does not get reply in given time period, mark that node as attacker and eliminate that path.

V. QUALITY OF SERVICE PARAMETERS

Quality of Service is the performance level of a service offered by the network to the user. When the real-time traffic is transmitted in the network, QoS becomes demanding. In addition, because of the limitation of network resources, especially in wireless networks, real time traffic need to be given higher priority to ensure that the real time traffic reaches the destination on time. The QoS parameters analyzed in this simulation are as follows

1) Average Throughput: Throughput is the number of bits received by the destination per second [1]. A high value of throughput in the network is desirable.

$$\text{Throughput} = \frac{\text{Number of bits received}}{(\text{stop time} - \text{start time})} \text{ bits/sec} \quad (1)$$

2) Packet Delivery Ratio (PDR): It is the ratio of the number of packets delivered to the number of packets sent by the source. It characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is preferred in the network.

$$\text{PDR (\%)} = \frac{\text{No.of data packets received by the destination node}}{\text{No.of data packets transmitted by the source node}} * 100 \quad (2)$$

3) Energy consumption: Energy Consumption is defined as the sum of units required to the key transmission throughout the duration of simulation. Thus the energy computed is involved in the selection of the optimal path which requires minimum energy to route the data from source to destination.

4) Residual Energy:

The residual energy is the remaining energy at every node which is the energy left after the packet transmission. The residual energy R.E can be calculated as follows

$$\text{R.E.} = \text{E}_\text{I} - \text{E}_\text{c}(\text{t}) \quad (3)$$

Where, E_I is the initial energy of a node and Ec(t) is energy consumed by a node after time t.

Total energy consumption ($T.E_c$) of all nodes is defined as the following equation

$$T.E_c = N * Initial\ Energy - R.E \quad (4)$$

Here 'N' is denoted as the number of nodes used in the network.

VI. SIMULATION RESULTS

The performance evaluation of the proposed technique is simulated in Network simulator NS-2.34 in Linux operating system with modified version of the UM-OLSR implementation version 0.8.8 of OLSR. The OLSR protocol implementation follows RFC 3626. The simulation scenarios had 50 wireless nodes over an area of 1000m*1000m for duration of 100seconds. With each simulation, number of nodes and interval to send data packets was varied and thus attacker nodes were successfully detected. The main objective was to successfully detect the attackers.

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

TABLE: I List of attackers detected in the path

Detector	Path	Attacker	Detecting time (sec)
1	1.43.35.15.24.5.46.26.	24	35.3168
1	1.35.36.9.48.8.14.26.	14	45.8157
1	1.13.34.26.	26	36.7098
1	1.44.41.33.28.24.26.	24,33	38.9511
1	1.35.15.24.5.46.26.	24	35.6253
1	1.35.36.9.24.5.46.26	24	36.0636

Table-I shows that source node 1 was able to detect the attackers successfully when present in the path at different time intervals.

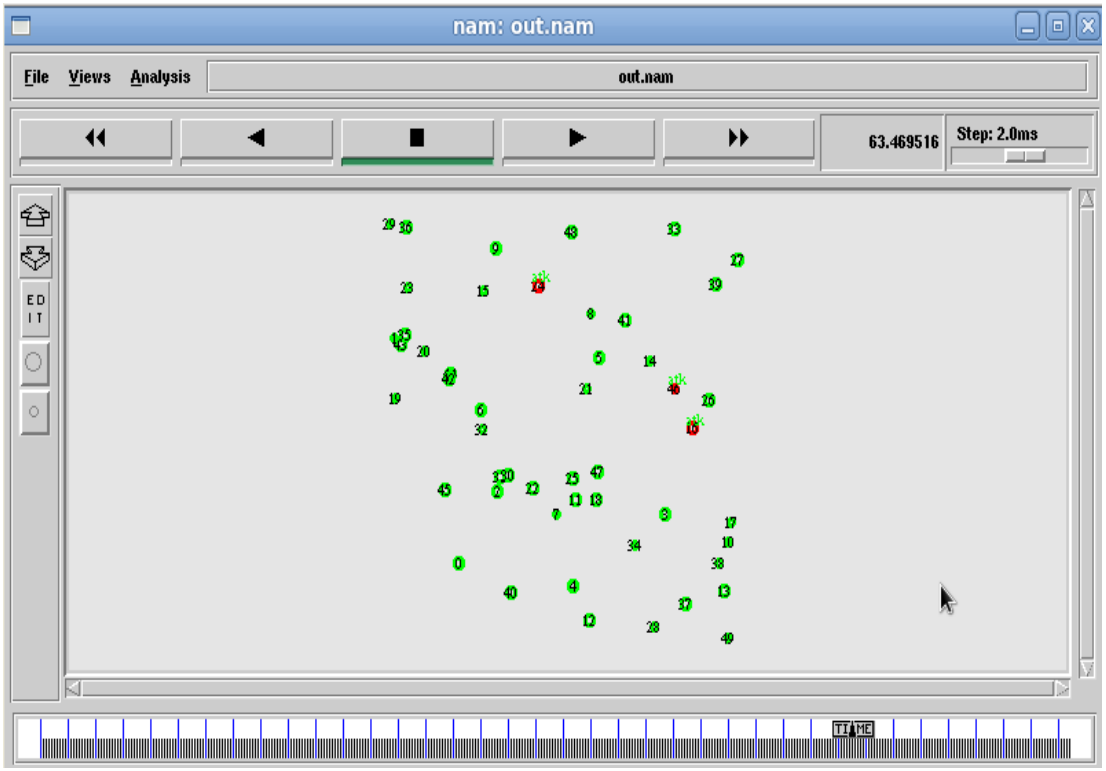

Fig.6. .nam file plot indicating detected attacker nodes

Here three protocols are compared by varying interval at which data is been forwarded and thus different performance parameters are observed. The standard OLSR protocol, base paper implemented [2] named as OLSRM and the proposed method named as OLSRMM are compared further.

TABLE II: Simulation parameters

Simulator	**NS-2**	
Simulation area	**1000*1000 m^2**	
Simulation time	**100sec**	
Transmission range	**250 m**	
Interval*10^{-6} (sec)	**0.12, 0.13, 0.14, 0.15**	
Traffic type	**CBR/UDP**	
Packet size	**1024 bytes**	
No. of nodes	**50**	
Energy	**100 Joules**	

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

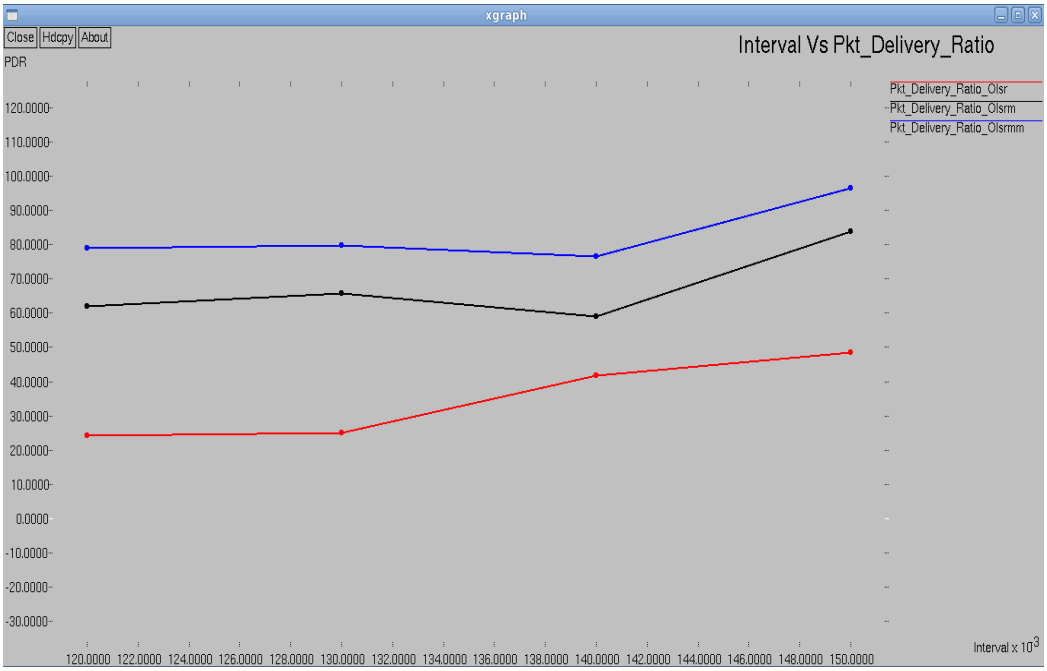

Fig.7. Packet delivery ratio Vs Interval

Fig.7 shows the packet delivery ratio of our proposed algorithm with respect to the data send at different intervals. The figure above shows that as the data is forwarded at different intervals, the packet delivery ratio of the proposed OLSRMM varies from 79% to 96% whereas the packet delivery ratio of OLSRM varies from 62% to 83% for different intervals and OLSR from 24% to 48%. The performance of OLSRMM is better than that of other protocols since its PDR is much higher than that of OLSRM and OLSR protocols.

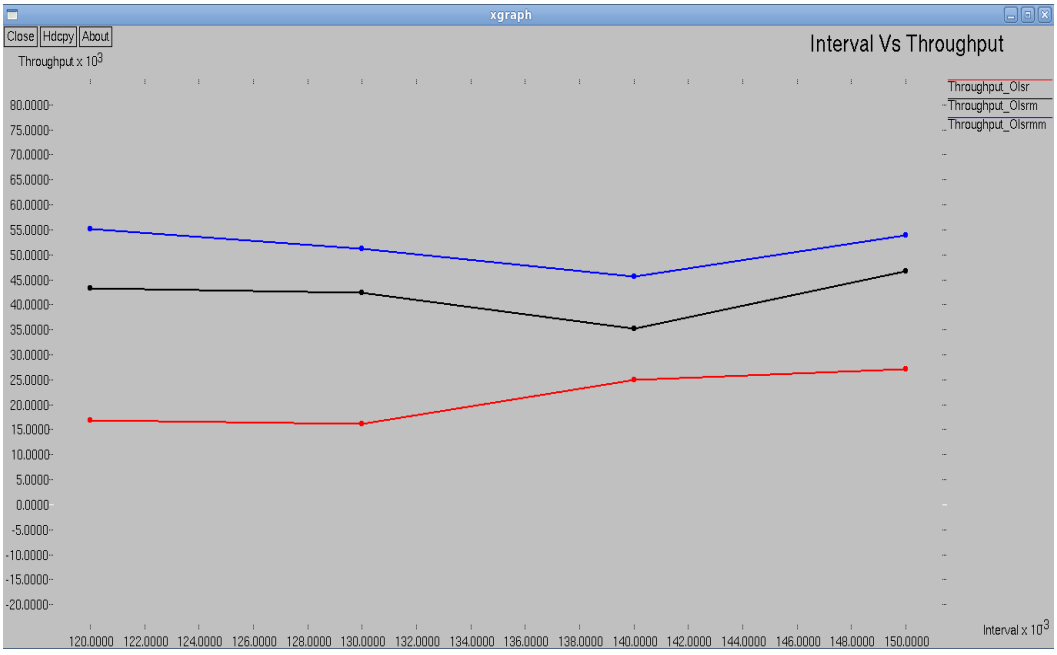

Fig.8. Throughput Vs Interval

Fig.8 shows the throughput of our proposed algorithm with respect to the data send at different intervals. The throughput of OLSR varies from 16kbps to 27kbps, for OLSRM it varies from 43 to 46 Kbps and for OLSRMM it varies from 55 Kbps to 53 Kbps. From the above results one can conclude that as the data is forwarded at different intervals, the throughput of the proposed OLSRMM is much better than that of other protocols.

International Journal of Novel Research in Electronics and Communication
Vol. 3, Issue 2, pp: (81-92), Month: September 2016 - February 2017, Available at: www.noveltyjournals.com

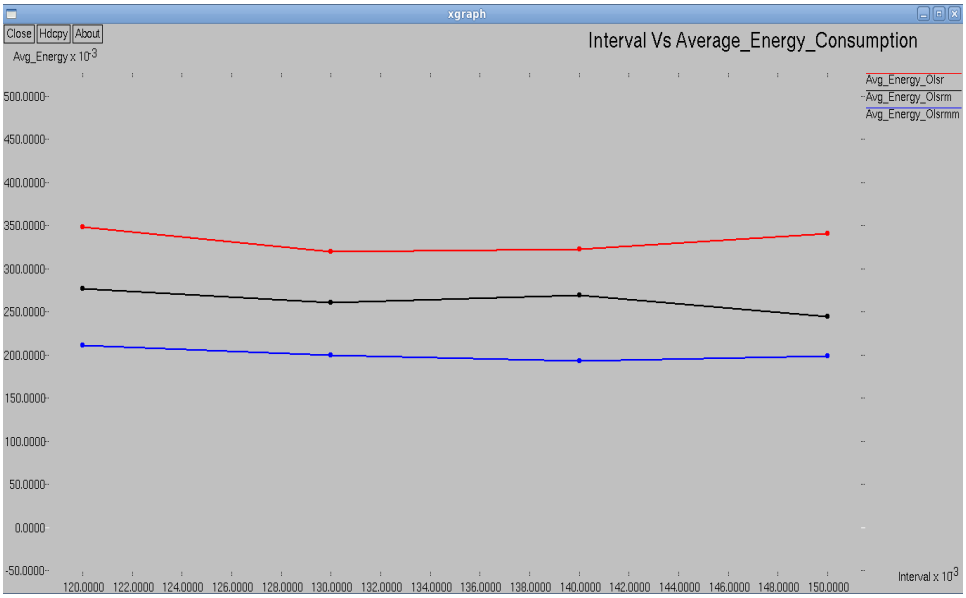

Fig.9. Average Energy consumption Vs Interval

In MANET energy consumption is an important issue as most mobile hosts operate on limited battery resource. Fig.9 shows the average energy consumed by our proposed algorithm with respect to the data send at different intervals. The energy consumption for OLSR varies from 0.348 to 0.340 Joules, for OLSRM it varies from 0.276 to 0.2448 Joules and for OLSRMM it varies from 0.211 to 0.198 Joules. The above fig. shows that OLSRMM consumes less energy than other two protocols.

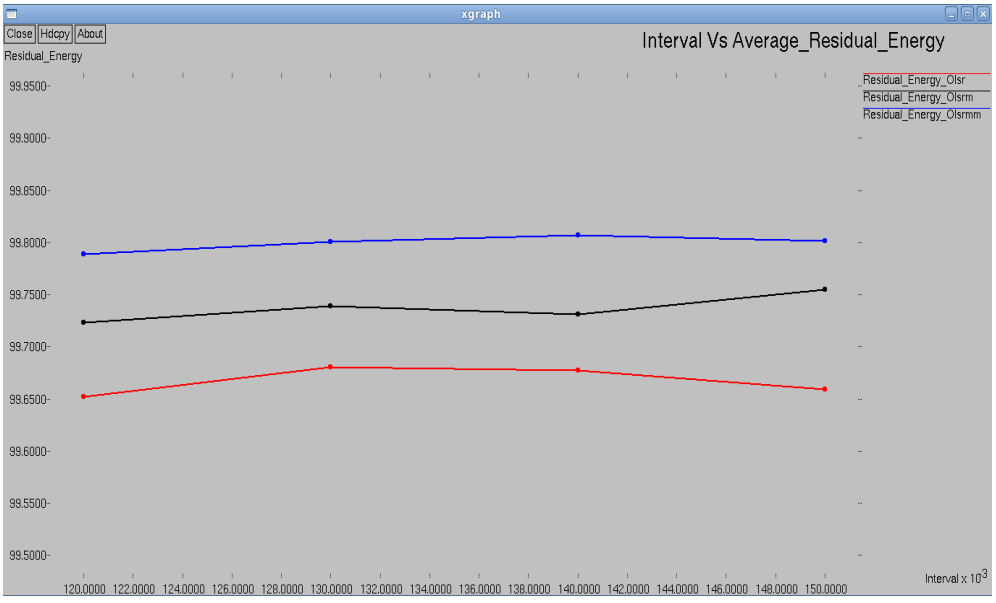

Fig.10. Average Residual energy Vs Interval

Fig.10 shows the average residual energy by our proposed algorithm with respect to the data send at different intervals. The residual energy for OLSR varies from 99.651 – 99.658 Joules, for OLSRM it varies from 99.723 – 99.755 Joules and for OLSRMM it varies from 99.788 to 99.801 Joules. The above fig. shows that OLSRMM has high residual energy than other two protocols.

The comparison and performance evaluation for all three routing protocols viz. OLSR, OLSRM, OLSRMM is now performed by varying Number of nodes in the network, keeping simulation time constant with 100sec and simulation area of 1000*1000m^2.

Table III: Simulation parameters

Simulator	**NS-2**	
Simulation area	**1000*1000 m^2**	
Simulation time	**100sec**	
Transmission range	**250 m**	
Traffic type	**CBR/UDP**	
Packet size	**1024 bytes**	
No. of nodes	**30, 40, 50**	
Energy	**100 Joules**	

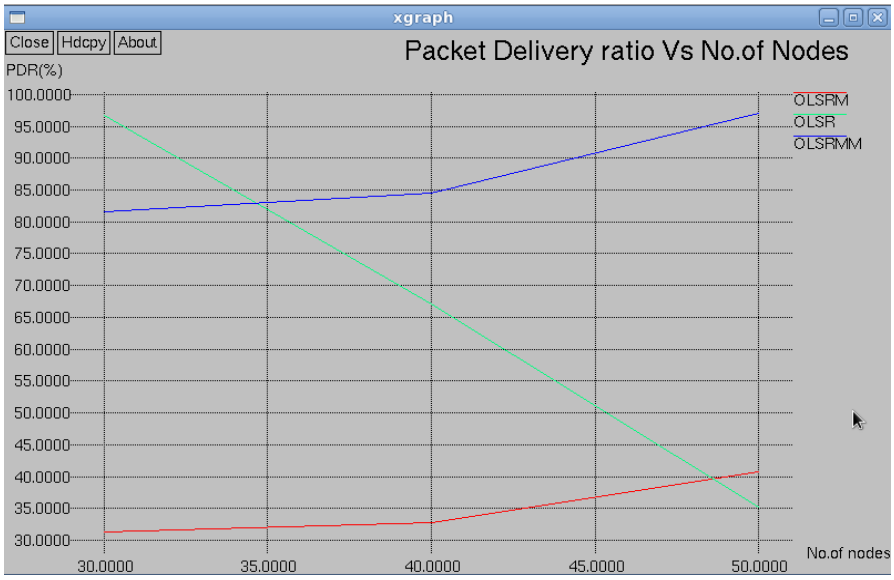

Fig.11. Packet delivery ratio Vs No. of nodes

From the above results obtained as shown in fig.11 by varying number of nodes, the PDR for OLSR varies from 96.677% to 35.215%. The PDR for OLSRM varies from 31.343% to 40.796% and for OLSRMM it varies from 81.592% to 97.041%. From the fig. it is observed that the packet delivery ratio of OLSRMM is much greater than OLSRM and OLSR. Since the malicious nodes get detected in OLSRMM protocol and also the path carrying malicious node get avoided during passing data packets.

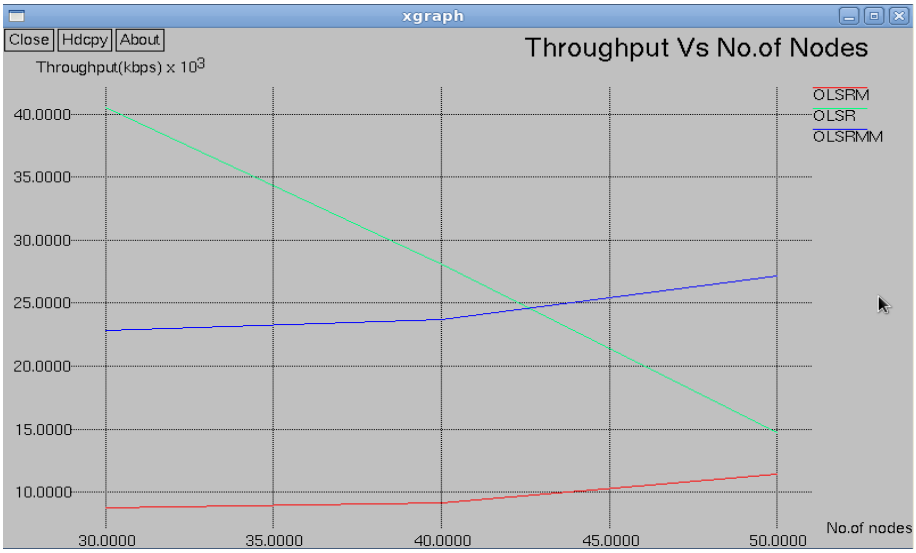

Fig.12. Throughput Vs No. of nodes

From the above result as shown in Fig.12 by varying number of nodes, the Throughput for OLSR varies from 40.507kbps to 14.755kbps. The throughput for OLSRM varies from 8.769kbps to 11.414kbps and for OLSRMM it varies from 22.828kbps to 27.144kbps. It can be observed that as number of nodes increases the throughput of OLSR decreases tremendously and also the throughput of OLSRM is less as compared to OLSRMM. The performance of OLSRMM protocol is much higher than that of OLSR and OLSRM protocols.

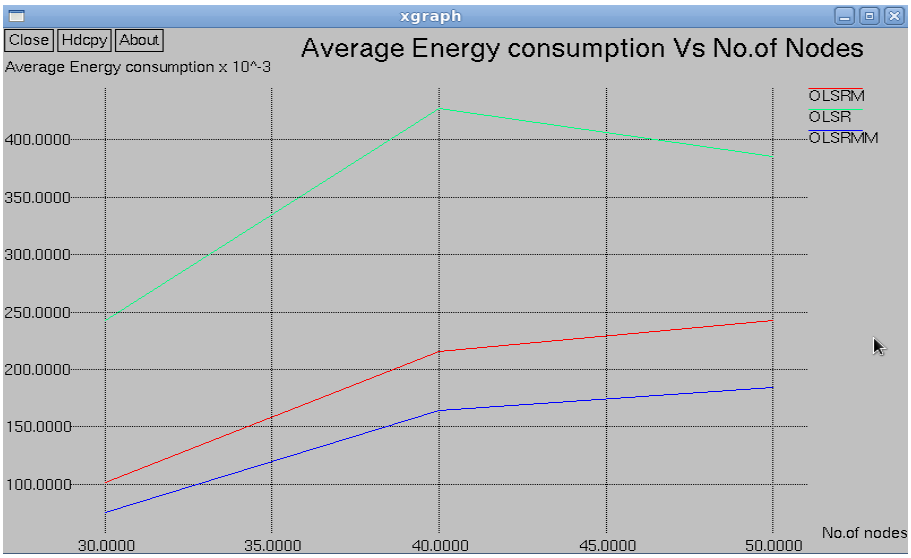

Fig.13. Average Energy consumption Vs No. of nodes

In MANET energy consumption is an important issue as most mobile hosts operate on limited battery resource. Fig.13 shows the average energy consumed by our proposed algorithm with respect to the data send by varying number of nodes. The energy consumption for OLSR varies from 0.2422 to 0.3850 Joules, for OLSRM it varies from 0.1012 to 0.2427 Joules and for OLSRMM it varies from 0.0756 to 0.1841 Joules. The above fig. shows that OLSRMM consumes less energy than other two protocols.

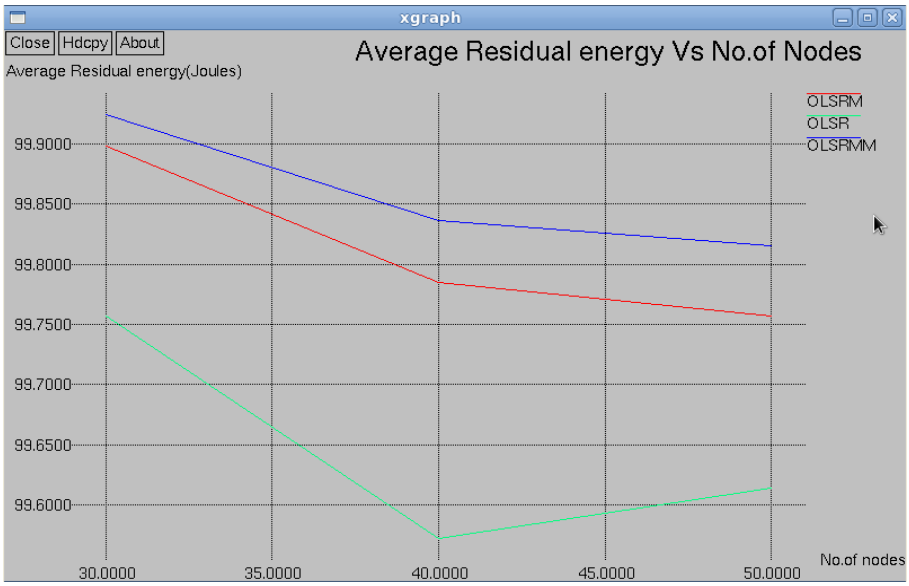

Fig.14. Average Residual energy Vs No. of nodes

Fig.14 shows the average residual energy by our proposed algorithm with respect to the data send for varying number of nodes. The residual energy for OLSR varies from 99.757 to 99.6413 Joules, for OLSRM it varies from 99.898 to 99.757 Joules and for OLSRMM it varies from 99.924 to 99.815 Joules. OLSRMM has high residual energy than other two protocols.

VII. CONCLUSION

The standard OLSR protocol is not secured. It selects shortest path to forward data packets from source to destination, so some of the nodes may be used repetitively. In MANET there are several types of attacks like black hole, wormhole, etc which degrade the system performance. To avoid this Multipath OLSR protocol (OLSRM) is used in which maximum number of nodes are participating in communication. OLSRM protocol can detect malicious nodes but is not able to avoid the path containing malicious node during transmission. In this paper, OLSRM protocol is modified to detect misbehavior nodes in the network named as "Malicious free Modified OLSR (OLSRMM)" protocol.

Standard OLSR protocol is compared with the proposed idea with the help of different performance parameters by varying number of nodes and interval at which data is been forwarded. The Packet delivery ratio and throughput of OLSRMM is much high than standard OLSR protocol and the energy consumed by the proposed protocol is much less. By using less battery, OLSRMM gives much better performance than standard OLSR and OLSRM protocol.

The Proposed OLSRMM protocol gives the solution of malicious nodes problem in OLSR protocol and after detection avoids data to be transmitted through the path containing malicious nodes, thus avoid transmission of data through invalid path. OLSRMM ensures the selection of path with non-malicious nodes to forward the data traffic. The future scope can be focused on simulating OLSRMM for different performance parameters, by varying simulation time, network area etc. The same proposed mechanism can be used for modifying different protocols for MANET.

REFERENCES

[1] Abu Hena Al Muktadir et al. " Energy consumption study of OLSR and DMYO MANET routing protocols in urban areas", National Conference on Communication and Information Security, NCCIS 2007 Daffodil International University, Dhaka, Bangladesh, 24 November 2007

[2] Ahmed M. Abdalla et al. "An IDS for Detecting Misbehavior Nodes in Optimized Link State Routing Protocol" 2010 2nd International Conference on Computer Technology and Development (ICCTD 2010)

[3] Dr. Rajaram Marimuthu et.al. "A Multipath Reliable Routing for Detection and Isolation of Malicious Nodes in MANET" Proceedings of the 2008 International Conference on Computing, Communication and Networking (ICCCN2008) 978-1-4244-3595-1/08/$25.00 ©2008 IEEE

[4] Anil Kumar Gupta et al. "Detecting and Dealing with Malicious Nodes Problem in MANET" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013

[5] Hiba Sanadikia, Hadi Otrokb, Azzam Mourada, and Jean-Marc Robertc "Detecting Attacks in QoS-OLSR Protocol" 978-1-4673-2480-9/13/$31.00 ©2013 IEEE

[6] Mohanapriya Marimuthu and Ilango Krishnamurti " Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks " Journal of Communications and networks, Vol. 15, No. 1, February 2013 IEEE

[7] E. Edwin Lawrence et al. "A Comparative Study of Routing Protocols for Mobile Ad-Hoc Networks" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.11, November- 2014

[8] "The network simulator –ns-2,"http://www.isi.edu/nsnam/ns/index.html

[9] Mrs. Kirti Aniruddha Adoni et al. "Trust Aware Routing Framework for OLSR protocol to enhance performance of Mobile Ad-hoc Networks" International Conference on Pervasive Computing (ICPC) -1-4799-6272-3/15/$31.00 (c)2015 IEEE

[10] Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das "A Survey of Black Hole Attack Detection in Manet" 978-1-4799-2900-9/14/$31.00 ©2014 IEEE

[11] Nidhi Choudhary et.al. "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORK" IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.4, August 2014

[12] Amith Khandakar "Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol" 2012 4th International Conference on Computer Engineering and Technology (ICCET 2012)

[13] D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont, "Implementing a fully distributed certificate autorithy in an OLSR MANET," in Proc. IEEE WCNC, 2004.

[14] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an IDS to safeguard OLSR integrity in MANETs," in Proc. IWCMC, 2006.

[15] A. J. P. Vilela and J. Barros, "A cooperative security scheme for optimized link state routing in mobile ad-hoc networks," in Proc. IST MWCS, 2006.

[16] A. Adnane, R. de Sousa, C. Bidan, and L. Mé, "Analysis of the implicit trust within the OLSR protocol," in Proc. IFIP, 2007

[17] Zougagh, Hicham, Ahmed Toumanari, Rachid Latif, and Noureddine.Idboufker -."Mitigating Black Hole attack in MANET by Extending Network Knowledge", International Journal of Advanced Computer Science and Applications, 2013.