DOI : https://doi.org/10.56452/772

ISSN: 0974-5823 Vol. 7 No. 1 January, 2022

International Journal of Mechanical Engineering

DETECTION OF ATTACKS AND IMPROVE THE SECURITY OF MANET BY USING MULTI OPTIONAL MODERATION METHOD (MOMM)

[1]Mrs.M.Kundalakesi, [2]Dr.M.Renuka Devi

[1]Research Scholar, Assistant professor, Department of Computer Applications,

Sri Krishna Arts And Science College, Coimbatore

[2]HOD &Associate Professor, Department of Computer Applications,

Sri Krishna Arts And Science College, Coimbatore

kundalakesim@skasc.ac.in,renukadevim@skasc.ac.in

ABSTRACT

MANET plays an important role as intermediate routers, but it is an infrastructure-less communication network which comes under autonomous devices. MANET routing protocols are divided into two types, they are proactive and reactive. Proactive routing protocols are classified as OLSR, and the Reactive routing protocols are classified as AODV [1] and DSR [2]. When compared to the proactive OLSR [3], the reactive AODV and DSR is considered as one of the much efficient and scalable due to their low routing outlay. AODV and DSR was developed under the presumption that entire nodes should trust every other node and also there must be no malicious spy between the nodes in the network. So, the existence of any node lay on the security challenges. The malicious node will cause serious disruption over a vast variety of attacks which involves both routing and data transferring attacks. These attacks are normally categorized into two, such as passive attacks and active attacks. The attackers in passive attacks will not disturb any functions of the network either it will attempt to produce new valuable detailed information. Alternately, active attacks will cause damages to the network in different ways that depend upon which type of the attack.

Keywords :AODV,DSR,OLSR, MANET, Protocols

I INTRODUCTION

The central infrastructure can control the wireless communication network because in the network, the communication between the nodes is also controlled by the central infrastructure otherwise it can be a framework-less communication network which is known as Ad hoc Networks. The mobile nodes are connected to each other using an application called Mobile Ad hoc Network (MANET) which comes under the Wireless Ad hoc Network (WANET). In MANET, the nodes of the network will not depend on the central node to carry out the data between them or to adapt the communication. Alternately, the work can be done jointly for carrying the data between the nodes which could not reach one another other directly. In simple words, while the sender and the receiver are not in the similar coverage, then the nodes would act as a link between sender and receiver. So, the mobility of nodes reaches to 00 topology due to dynamic changes. MANET routing protocols are planned to be adaptive for any changes in the dynamic topology [1].

MANET energy is considered as one of the major key connectivity components. This specifies that each and every node in the network has a fixed small volume of energy. Therefore, to avoid unnecessary utilization of energy, the work should be done with effective mechanisms and protocols. Since MANET nodes are connected to each other only with the help of wireless links. So, bandwidth plays an important role in network connectivity because wireless links are much better than wired links. The signals of the wireless links could be affected by noise, interference from other signal, or fading [2]. MANET is unsecured for various

types of attacks and offense risk. Since the nodes in the MANET are connected to each other with the help of wireless links which allows the unauthorized user to see or modify such data is known a seaves dropping threat. Since MANET does not have a centralized network which helps to control communication in-between the nodes, so the nodes depend on themselves for suppling the data to the destination node. Thus, the cruel attacker can change the connection link or discard the transmitted data. Denial of Service (DoS) attacks are considered as one of the dangerous threats to MANET, where a malicious attacker node absorb the battery of another node by asking them to transfer large number of data. The attacks on the MANET are classified into two types, (1) active attacks and (2) passive attacks. The attacker nodes in the active attack works only for affecting the performance of MANET, for quitting the transferred data, for changing the connector links, or for removing the battery in the nodes. The attacker nodes in the passive attack only listen to the connections between the nodes without interfering between the operation of communications.

II RELATED WORK

In [8], the newly introduced baiting method rely on its node id. The acquisition of a black hole node begins by broadcasting a seduction request to all nearby nodes. The bait request consists of the Source Sequence Number (SSN) and source id. So, when the source node receives the responses, it determines whether there is a response with a DSN higher than its SSN; this indicates that the response came from a black hole as no node in the network should have a higher DSN than the SSN of the source node. After identifying of a black hole node in a network, the source node transmits a black hole node to all nearby nodes to notify them. The limitations of this approach are to enable the smart black hole node to check that the RREQ received request for routing to the same RREQ source, and then not responding to that request. Also, the smart black-hole node will use a black hole alarm and start broadcasting false black-hole alarms to separate selected nodes from the network.

In [9, 10], they introduced a method based on the use of the Cooperative Bait Detection Method Scheme (CBDS). In the CBDS the black hole detection is classified into three categories such as Bait, Reverse Trace, and Reactive Defence. In the Bait phase source node will casually choose any one of the irneighbours and sends abait request with the help of its id. In the Reverse Trace section, a list of suspicious nodes is created from the RREP of RREQ bait, then the nearby nodes enter the loose behaviour mode to see if there is an attacker node along the way. For each and every black hole node found on the network, a black hole alarm is broadcasted to every near by node. In the Reactive Defence phase, the source code checks that the PDR is below the prescribed limit, and then launches the Bait phase again.

In [11], the newly introduced scheme relies on using a fake id to bait an area with a black hole node. The source node begins by reporting a bait request that contains an offline id. The black-hole node will respond to that RREQ bait because of its normal behaviour that responds to every RREQ in a network that claims to have a better approach. The advanced system is used in DSR, so they have modified the RREQ and RREP title to determine the black hole node within the specified path. The warning is reported to the nearby nodes when they foundthe black hole node. The source node keeps on tracking whether there is a drop below the certain limit; then again it beginsthebaiting. The restriction of this system is to increase the size of the control packets (RREQ and RREP) leading to overhead the increase in addition to black hole warnings which are used by a smart black hole to separate nodes in the network.

In [12], the developed model begins by flooding the fake network application. Any response from the node is considered a suspicious node; using the nearby nodes a black hole node will be found after examining that the suspicious node will transfer the packets to the destination node. This model contains localization system that provides location for the black-hole node as the model is upgraded for military use. The limit of this model is to consume the network with a fake request, which can lead to network congestion.

In [13], the newly developed system relies on a special type of node which is known as guard node. This assists in locating nodes with black holes in a network. The guard nodes in bad mode will examine the behaviour of all other nodes in the network. Guard notes consist of tables which records the nodes behaviours that are present in the network. Each and every node have trust value that is determined by its network behaviour, and they reduce it when the node sends RREP only without sending RREQ. If the nodes trust value falls below the limit, then it will be blocked or split. The guard notes display the alarm to all nearby nodes when they detect the black hole. The limitations of this application is that it requires a special type of nodes

(guard nodes) and a large number of guard nodes to cover the entire network; and this system will have huge overhead due to too many tables.

In [14], the developed model relies solely on the validation component which is set inside RREP. In this model it is believed that the attacker node is not having minimum authentication to be sent when sending RREP. When the source node gets the RREP it first examines the validity of the bit whether it is set to one, then uses that method again and if not then processes the RREP from the black hole node and throws it. The limit of this model is unreasonable speculation as the attacker node who wants to attack the network will apply the same protocol and they will analyze it before the attack. So, all the smart black-hole node will recognize this validity bit and sends RREP to each request along with the determined validity bit.

III TYPES OF ATTACKS IN MANET

In the wireless ad-hoc network, the security is one of the huge major challenges [9,10]. Learning all the possible features of an attack is always the first step in improving good security solutions. The security of the connection to MANET is necessary to secure transmission for all the required details. MANETattacks is mainly divided into different categories such as internal attacks, external attacks, active attacks, passive attacks. These classifications is most important because any time the attacker can damage the network as internal, external or active, passive.

External Attack: External attacks are carried out by nodes of third parties which are not the part of a particular network and it also attempts to stop the network by transmitting fraudulent information which leads to network malfunction.

Internal Attack: Internal attack comes from internal nodes which is the part of a network. The attacker would be a new node added to the network, that could gain the network access. Internal attack performs as a malicious node from a network that gains illegal access and pretends to be a real node. It is used for analyzing the traffic between the remaining nodes and could also participate in some other activities in the network. Compared to external attacks, internal attacks are very hard to predict.

Passive Attack: Here, the attacker only listens and often tracks the communicated information between the two nodes. After tracking there will be no changes done to the message. So, the attackers will easily find all the details regarding the complete network which is used for hijacking or injecting into a network attack. Compared to active attacks, passive attacks are very hard to detect.

Active Attack: Here, the attacker listens and tries to fix after the data switch on the network. It could interfere with the normal operation of networks. So, in active attack, intruders can able to change packets, inject packets, drop the packets or they can use different network features to run the attacks.

Wormhole Attack: In this attack, the attacker grabs and stores the packets in one place in the network and puts them in order to fix the target to the network, and then sends them back to the network from that point. The routing may be interrupted when a routing control message is moved. This tunnel between the two joint attacks is known as the wormhole.

Denial of Service attack: This attack sends a large number of unwanted packets or traffic at one time to the server and tries to slow down the server so that the resources might not be available for the user. Here, the attacker usually uses a radio signal jamming and a battery drain technique.

Impersonation: If the verification method is not performed correctly then the malicious node will act as a real node, and it also watch the network traffic. Sometimes it may also send unauthentic routing packets and obtains access to other hidden secret information.

Routing Attacks: A malicious node targeted routing resources because it the most important service to MANET. This routing attack has two bites. The first attack is on the routing protocol and the second attack is on the transmission of the packets or delivery method. The first is intended to block the spread of routing information to the node. The second is intended to disrupt the delivery of the packets against the previously defined method.

Black hole Attack: Here, the attacker publishes a zero metric for all the destinations that bring all the nodes around it to make the packets move towards it. [9] Malicious node sends false path information that claims to

have the best route and also make the remaining good nodes to route data packets over this malicious one. A malicious node lay off all the packets but usually receives instead of forwarding such packets. Attacker listens the requests in a flood-based protocol.

Replay Attack: The replay attacker will repeatedly transmit the valid data continuously to inject a pre-captured network traffic. These attacks often target the originality of the routes even though it is used for breaking the badly designed security solutions.

Jamming: While jamming, the attacker first monitors the wireless medium to predict the frequency where the destination node will receive the signal from the sender. Then it deliver the signal to that specified frequency so that the correct receiver will be blocked.

Man- in- the- middle attack: A network attacker lays down between the sender and the recipient and sniffs every detailed information for being sent in-between the two nodes. In other cases, the attacker would pretend the sender to contact the recipient or pretend the recipient to respond to the sender.

Gray-hole attack: This attack is also called as routing misbehaviour attack that results in dropping the messages. This attack contains two stages. In first stage, the node broadcast itself as it has a valid route to the destination node whereas in the second stage, the nodes blocks the captured packets with some specific probability.

IV PROPOSED METHOD

Multi Optional Moderation Method(MOMM) approach performs the detection of various attacks in mobile ad hoc networks and mitigates them to develop the quality of service in mobile ad hoc networks. The proposed has various phases namely, traffic-register task, traffic change overtask, time variant snapshot task, sinkhole attack detection, routing attack detection and DoS attack detection. In Traffic-Register Task, a record about a particular traffic is generated. In traffic changeover pattern, the traffic Route sequence is generated with a set of node names to represent the transition path. In time variant snapshot task, the topology snapshot of the network is created. In Sinkhole Detection presence of presence of sinkhole in the network is identified. The figure 1 will explain the tasks involved in the proposed approach.

i. Traffic-Register Task
ii. Traffic Changeover Task
iii. time abnormal snapshot Task
iv. sinkhole attack detection
v. routing attack detection
vi. DoS attack detection

DOI : https://doi.org/10.56452/772

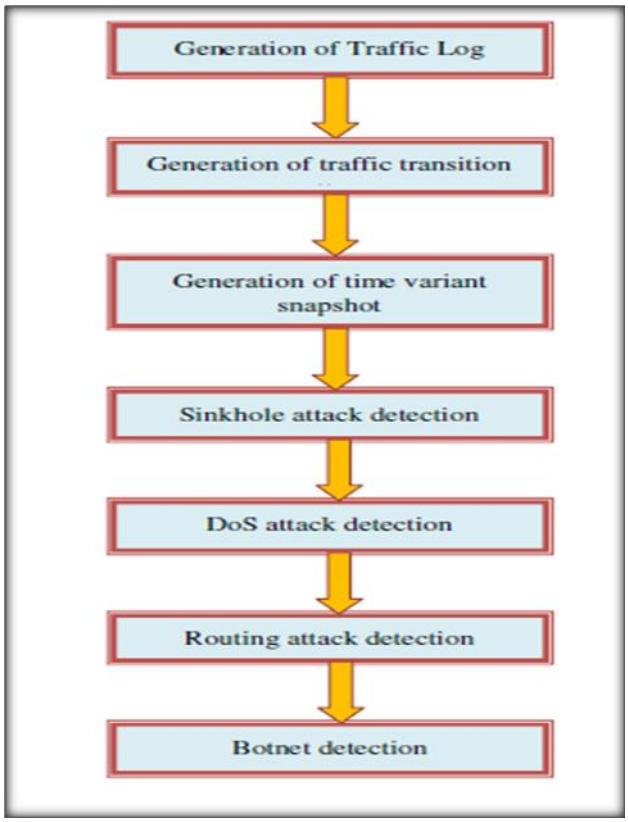

Figure 1. Process flow of Proposed Method

i. Traffic-Register Task

The proposed approach makes the assumption that node sends the packet to the destination via some of its neighbors and adds the address of its own at the transition field of the packet. The attack detection system computes the set of nodes present in the transition path logs to the database by extracting transition field. The traffic register store the details of packets such as Source Address(SA), time received and Destination Address (DA).

ii. Traffic Changeover Task

The traffic changeover task is computed using the log produced by the node. The node maintains numbers of traffic pattern and at each time frame a new instance of traffic pattern will be feed into the traffic log table.So that the log file contains the information about packets which are received at few previous time frames. For each time window, the method generates the log by splitting them from the log trace.Using the log trace, the time orient traffic pattern will be generated.

iii. Time Abnormal Snapshot Task

The proposed method collects time snapshot at regular intervals to know the topology information. From the topology information, it generates the snapshot and updates the route table and node table. The route table contains information about a set of nodes and routes to reach other nodes whereas the node table has information about the neighbors of the node. At a later stage, the node generates the snapshot at a regular time interval to detect the presence of sinkhole. Using the traffic pattern which is computed earlier, it finds out set of nodes which it feels guilty about working condition.

iv. Sinkhole Attack prediction

The available routes for these nodes are obtained using route table Rt. Based on the identified routes and route from transition path, the length of the route present in the pattern is identified.

If the route is longer then there is a sinkhole in the path. To avoid sink hole from packet transmission, a control message will be sent to all the nodes.

v. DoS Prediction

DOI : https://doi.org/10.56452/772

The DoS attack detection is performed using the traffic pattern has been generated. Whenever a packet has been received, the node generates the traffic pattern and computes the traffic condition at the current time window.

vi. Routing Attack prediction

The routing attack detection is performed using the time variant snapshot algorithm. This method identifies the set of all routes available in the network to reach the node. This method computes the distance and traffic rate of each and every route.

```
Multi Optional Moderation Method (MOMM)

Step1:For each log from TrLog
TrLogi = read log from TrLog.

Compute traffic transition path

Tpi = {Source Address,Destination Address Transition Path}.

Tpi =Tp + (Tpi + Ti)

Step2:for each node ni from n
for each traffic pattern tpi from tp
transition path trp =_x(tpi,tp(traversal path))
if trp ' ni then
else
add to gs = _n + ni
end

Step 3:if Tpi' ASi then
Ap= compute available path from Route Table Rt an
snapshot S.
validate the distance of route used and routes from Ap.
if found guilty then
create alert message
AM={seq.No,SourceAddr, Destination Addr,
Sinkhole Addr}
send AM through different path

Step 4:Compute traffic pattern at current time window.
        Tpi ? Tl

if size(Tpi)> Traffic Threshold
        Drop the packet

Step 5: Compute distance
        Dist = _ Hops ? Ri
Compute traffic rate
        Tr = _ Tl.Ri==Ri
if Pv.Route==Ri&&Pv.
Route.Distance>Dist&&Pv.Route.Tr>Tr
drop Packet.
```

DOI : https://doi.org/10.56452/772

V PERFORMANCE METRICS

The performance of proposed method is evaluated by using simulator. The following parameters are used to estimate the performance of proposed method such as Packet Deliver, End to End Deliver and Throughput ratio.

a. Packet Deliver

The packet delivery ratio can be obtained from the total number of data packets arrived at destinations divided by the total data packets sent from sources.

- Packet Delivery Ratio=$\frac{\sum \text{Total packets received by all destination node)}}{\Sigma(\text{ Total packets send by all source node)}}$-→(1)

b. End-to-end delay

Average End-to-end delay is the time taken by a packet to route through the network from a source to its destination. The average end-to-end delay can be obtained computing the mean of end-to-end delay of all successfully delivered messages. Therefore, end–to-end delay partially depends on the packet delivery ratio.

$$D = \frac{1}{n}\sum_{i=1}^{n} (\text{Tri - Tsi})* 1000 \text{ [ms]}----\rightarrow 2$$

Where

D = Average E2E Delay

i = packet identifier

Tri = Reception time

Tsi = Send time

n = Number of packets successfully delivered

c. Throughput Ratio

It is the average of the total throughput. It is also measured in packets per unit TIL. TIL is Time Interval Length. Mathematically it can be shown as equation (v).

$$\textit{Average Throughput} = \frac{(\text{recvdSize}}{(\text{stopTime-startTime})})*(8/1000)\rightarrow(3)$$

Where

recvdSize = Store received packet's size

stopTime = Simulation stop time

startTime = Simulation start time

VI RESULT AND DISCUSSION

The Packet Delivery Ratio (PDR) is used to evaluate the quality ofthe network. In this scenario, the number of nodes varied from 25 to 150.Figure 2 shows the effect of network density and packet delivery ratio. The packet delivery ratio of AODVwith attack is reduced by 5% with increasing the number of nodes from 25 to150. In the case of MOMM with attack, the drop in packet delivery ratio isonly 1.5%.

DOI : https://doi.org/10.56452/772

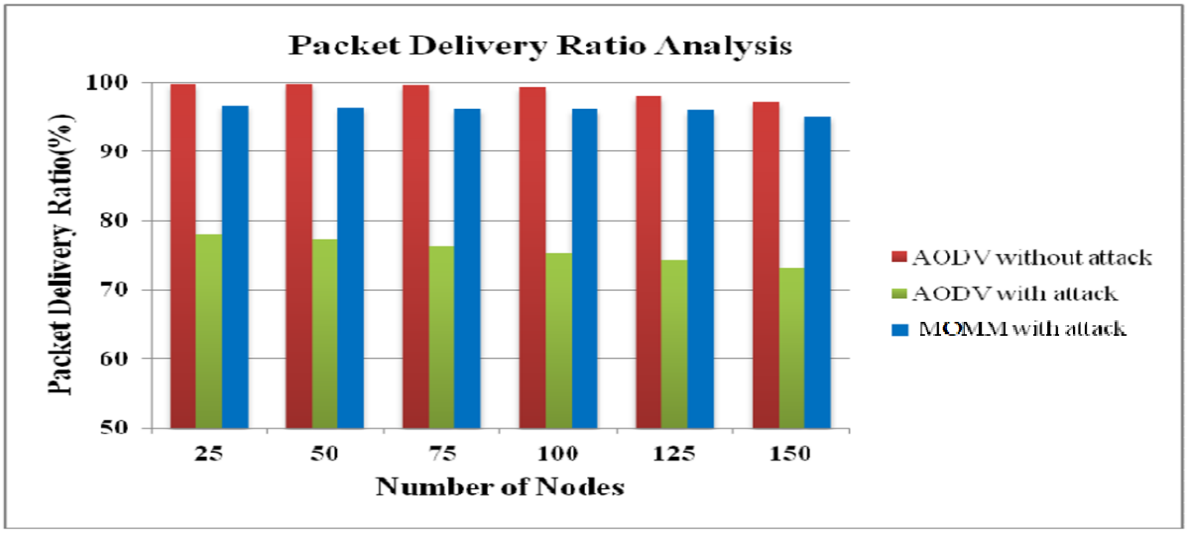

Figure 2. Comparison of Packet Delivery Ratio

The figure 3 indicates throughput of all schemes decreasesmarginally when the number of nodes increases. The proposed approachachieved a throughput of 1700kbps which is an improvement over the700kbps in an attacked situation.

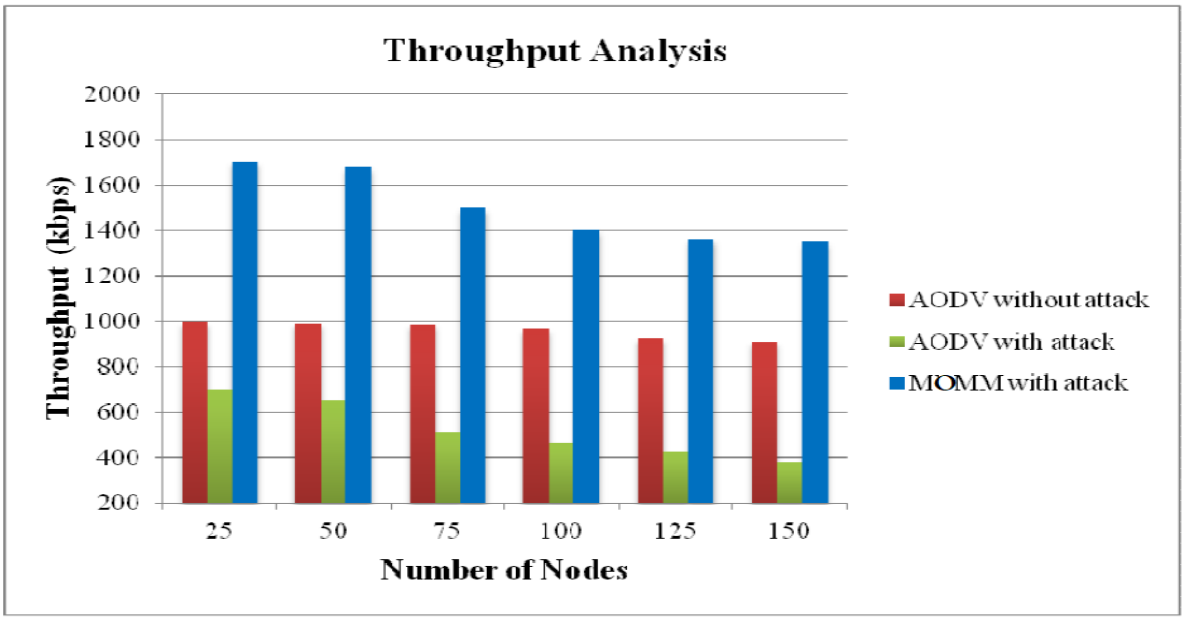

Figure 3 Comparison of Throughput Ratio

The figure 4 indicates that end-to-end delay ofAODV with attack is very high compared with MOMM. The end-to-enddelay of MOMM with attack is reduced by 0.8 seconds compared withAODV under attack.

DOI : https://doi.org/10.56452/772

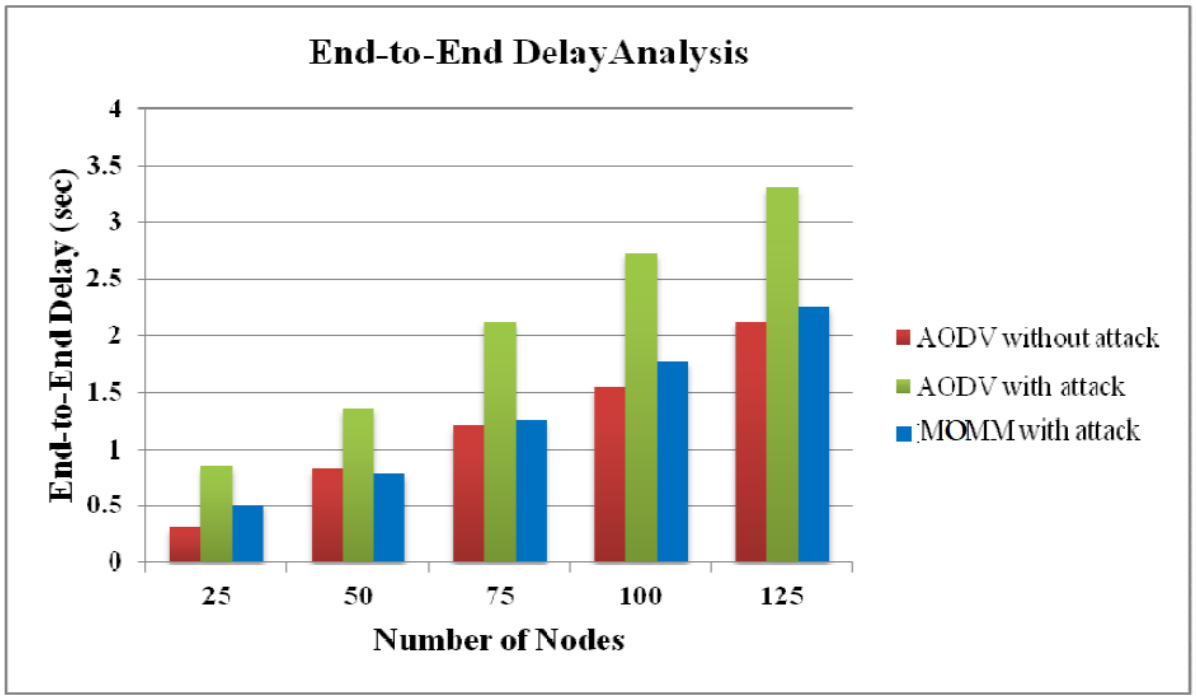

Figure 4 Comparison of End to End Delay

VII CONCLUSION

In this model,traffic pattern of the network and time variant snapshot is used to detect andmitigate various attacks. The efficiency of the model is analyzed with AODVwith attack, AODV without attack and MVMM with attack using differentperformance metrics. MVMM increases the packet delivery ratio to 96.5%and throughput by 1000kbps comparing with AODV with attack. Further, itsignificantly decreases the control overhead by 17000 packets, collision rateby 6.64% and end-to-end delay by 0.51 seconds. The simulation results showthat the performance of the MVMM model is improved compared withAODV under attack.

REFERENCES

[1] S. Mirza and S. Z. Bakshi, “Introduction to MANET,” International Research Journal of Engineering and Technology, vol. 5, no. 1, pp. 17–20, 2018.

[2] V. Goyal and G. Arora, “Review paper on security issues in mobile adhoc networks,” International Research Journal of Advanced Engineering and Science, vol. 2, no. 1, pp. 203–207, 2017.

[3] M. M. Alani, “MANET security: A survey,” in Proceedings of the 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 559–564, Penang, Malaysia, November 2014.

[4] A. Joshi, “A review paper on black hole attack in MANET,” International Journal of Advance Research in Computer Science and Management Studies, vol. 4, no. 5, pp. 16–21, 2016.

[5] A. K. S. Ali and U. V. Kulkarni, “Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in QoS of manet,” in Proceedings of the 7th IEEE International Advanced Computing Conference, IACC 2017, pp. 345–348, Hyderabad, India, January 2017.

[6] L. Prashar and R. K. Kapur, “Performance analysis of routing protocols under different types of attacks in MANETs,” in Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016, pp. 405– 408, Noida, India, September 2016.

[7] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks,” in Proceedings of the 2nd International Conference on Electrical and Information Technologies, ICEIT 2016, pp. 536–542, Tangiers, Morocco, May 2016.

[8] N. Kalia and H. Sharma, “Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol,” International Journal on Computer Science and Engineering, vol. 8, no. 5, pp. 160–174, 2016.

[9] P. L. Chelani and S. T. Bagde, “Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme,” in Proceedings of the 2016 International Conference on Communication and Electronics Systems, ICCES 2016, Coimbatore, India, October 2016.

[10] M. Sathya and M. Priyadharshini, “Detection and removal of black hole attack in mobile ad-hoc networks using cooperative bait detection method scheme,” International Journal of Scientifc& Engineering Research, vol. 7, no. 3, pp. 81–85, 2016.

[11] P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, “Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs,” in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011, pp. 755–760, Seoul, Republic of Korea, February 2011.

[12] B. Singh, D. Srikanth, and C. R. S. Kumar, “Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective,” in Proceedings of the 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016, pp. 810– 814, Coimbatore, India, March 2016.

[13] A. R. Rajeswari, K. Kulothungan, and A. Kannan, “GNBAODV: guard node based –aodv to mitigate black hole attack in MANET,” International Journal of Scientifc Research in Science, Engineering and Technology, vol. 2, no. 6, pp. 671–677, 2016.

[14] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, “AODVBased secure routing against blackhole attack in MANET,” in Proceedings of the 1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, pp. 1960–1964, Bangalore, India, May 2016.

[15] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, “SAODV: Black hole and gray hole attack detection protocol in MANETs,” in Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2391–2394, Chennai, India, March 2017.