International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Handling Intrusion Detection in MANET

Ritu Jaglan[1], Dr. Sawtantar Singh[2]
[1]S.U.S. Govt. College,Matak Majri, Karnal, Haryana, Research Scholar, IKGPTU, Kapurthala, Jalandhar
[2]Department of Computer Science, BMS Engineering College, Muktsar, IKG Punjab Technical University, Kapurtahala, Jalandhar

***Abstract*-- Versatile specially appointed systems have diverse properties as contrast with customary systems. These cause additional difficulties and troubles on security for specially appointed systems. In this paper, another plan to handle intrusion detection in MANET has been recommended and it has been assessed utilizing measurements. In view of the execution assessment, proposals have been made about the importance of the convention under different conditions . The proposed plan has been tested using Simulation on NS2 and has been incorporated on AODV.**

***Keyword*-- MANET, AODV, Intrusion, Security, IDS(Intrusion Detection System)**

I. Introduction

MANETs are the best solution for anytime anywhere connection establishment because they do not require any special intrastructre for connectivity and users are free to connect themselves as per their requirements. When such a free environment is available, security[3][4] is of prime concern as anybody can have malafide intensions to compromise data or cause damage to the network. Intrusion may be external or internal in the network. Security in wireless [3][4]network from intrusion is achieved either using prevention like encryption and authentication techniques or detection mechanism like IDS(Intrusion Detection System). The purpose of intrusion detection system is to alert the users about possible attacks on time so that they can be handled properly by the network. IDS detects the malacious node or intruder and avoid it and then remove the same from the network. It performs mainly three functions: [1][2]

1. Observe the network and Collect information/data
2. Process and Analyse data
3. Detect intruder and Alert the system

There are two types of protocols used in MANET categorised as proactive and reactive routing protocols. The present work has been carried out using AODV(Adhoc OnDemand Distance Vector) which is a reactive routing [15]protocol. It consists of two phases namely[13]

- Route Discovery Phase uses Route Request (RREQ) and Route Reply (RREP) packets to discover the route from source to distination
- Route Maintanenace Phase uses HELLO packet and route error (RERR) packet in order to maintain the route and inform about the error.

II. Proposed Plan

Detailed study of AODV routing protocol has been done. A New routing protocol has been proposed.New scheme detects the intruder nodes and removes them. In the proposed scheme there are three phases as Route Request, Route Reply and Data Transmission.

Route request is almost same as that of AODV. It starts with request to search shortest path. Two phases are used, first for intruder nodes and second for recovering nodes.

At the time of route request nodes are verified one by one for checking nodes status. If node status is “TRUE“ then this node enters in to the Non_Malicious phase and if node status is “FALSE“ then this node enters in to the Malicious Phase.

In Route Reply phase it checks the status of nodes whether they belongs to intruder or non intruder phase. All the possible routes will be searched by RREP from non intruder phase. Then available route will be selected by the RREP for broadcasting. It repeats procedure until it reaches to source node. Source node will select the path for data transmission based on the shortest path algorithm. Data Transmission starts from source to destination node.

It is expected that New Scheme will increase packet delivery ratio. Though the performance may be still poor as compared to (Ad-hoc On Demand Distance Vector) AODV. The reason to this is attributed to functioning of NEW because it detects and removes intruder nodes one by one.

In Route Reply phase it checks the status of nodes whether they belongs to intruder or non intruder phase. All the possible routes will be searched by RREP from non intruder phase. Then available route will be selected by the RREP for broadcasting. It repeats procedure until it reaches to source node. Source node will select the path for data transmission based on the shortest path algorithm. Data Transmission starts from source to destination node.

III. Simulation Environment

A comparative study have been carried out for 10, 20 and 50 nodes. The simulation has been performed using TCL scripts. The simulation results have been obtained with the help of three metrics as Packet delivery ratio, End to End Delay and Throughput. Results are represented in the form of Graphs. Using these Graphs performance comparisons have been made.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

To carry out the analysis intruder nodes have been introduced in the script. When these nodes used as routers for data transmission it results in hacker attack. This causes fall of packets. The proposed scheme takes care of these nodes and removes these nodes and generates a new path. This new path will be secured and will result in stable and secured routing.

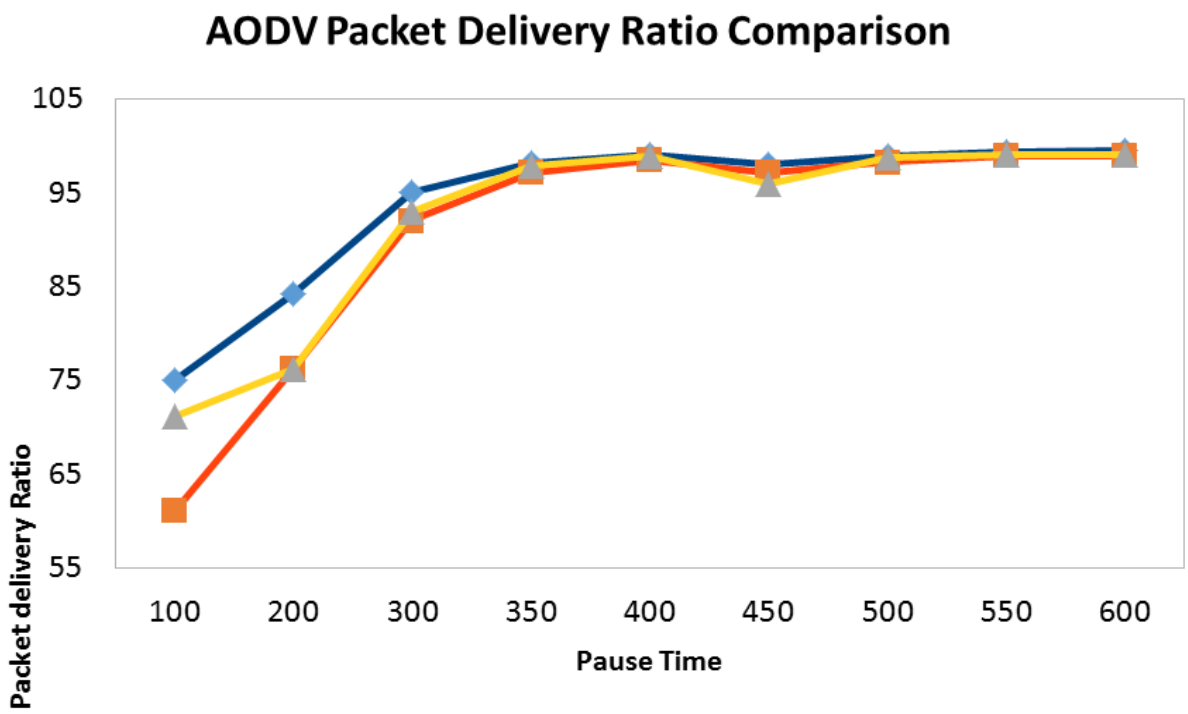
The simulations have been performed using Network Simulator (NS-2.34) [6]. The traffic sources are CBR (continuous bit–rate). The source-destination pairs are spread randomly over the network. Operating System used is Ubuntu Linux 14.0. The results have been derived by writing TCL scripts and generating corresponding Trace and NAM files. The mobility model used is random waypoint model.

The configuration area is 650 meter x 650 meter for 10 nodes and the packet size is 512 bytes. For 25 nodes the area becomes 850 meter x 850 meter. For 50 nodes the configuration area increases up to 1 Km x 1 Km.

Packets start their journey from a random location to a random destination. Same scenario has been used for performance evaluation of all three protocols.

IV. Performance Evaluation

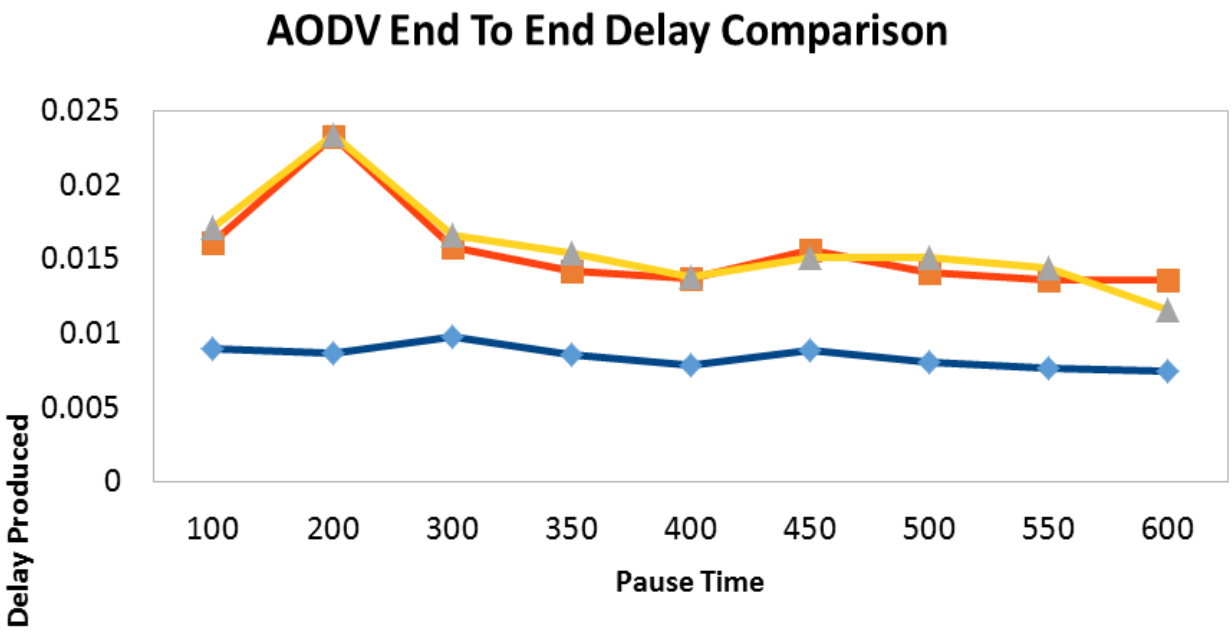
Various quantitative metrics used for evaluating the performance of routing protocols in ad-hoc networks are [5]: Packet Delivery Ratio, End to end delay and throughput. Transmission Control Protocol is the most commonly used protocol on the internet. Graphs are used to describe the results obtained from the execution of proposed plan. Each graph displays three scenarios of AODV routing protocol namely normal (in blue colour), after the intrusion when intruder enters the scene and creates havoc (in red colour) and then after the network is being repaired using the proposed new algorithm is shown in yellow colour. Graph 1 is Using PDR metric with varying pause time in smaller MANET



International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Graph 1 is description of 10 nodes scenario with pause time as a function in three different scenes. Pause time varies from 100 ms to 600 ms. Incase of 10 nodes intruder does not effect the network to large extent and thus situation is not so scritical ,still it has been shown using red notation.

And then proposed algorithm has been applied on the scenario. New scheme takes care of intruder, either byepasses it or removes it. Results shows that the new scheme has been able to modify the results in positive direction as displayed by yellow line.

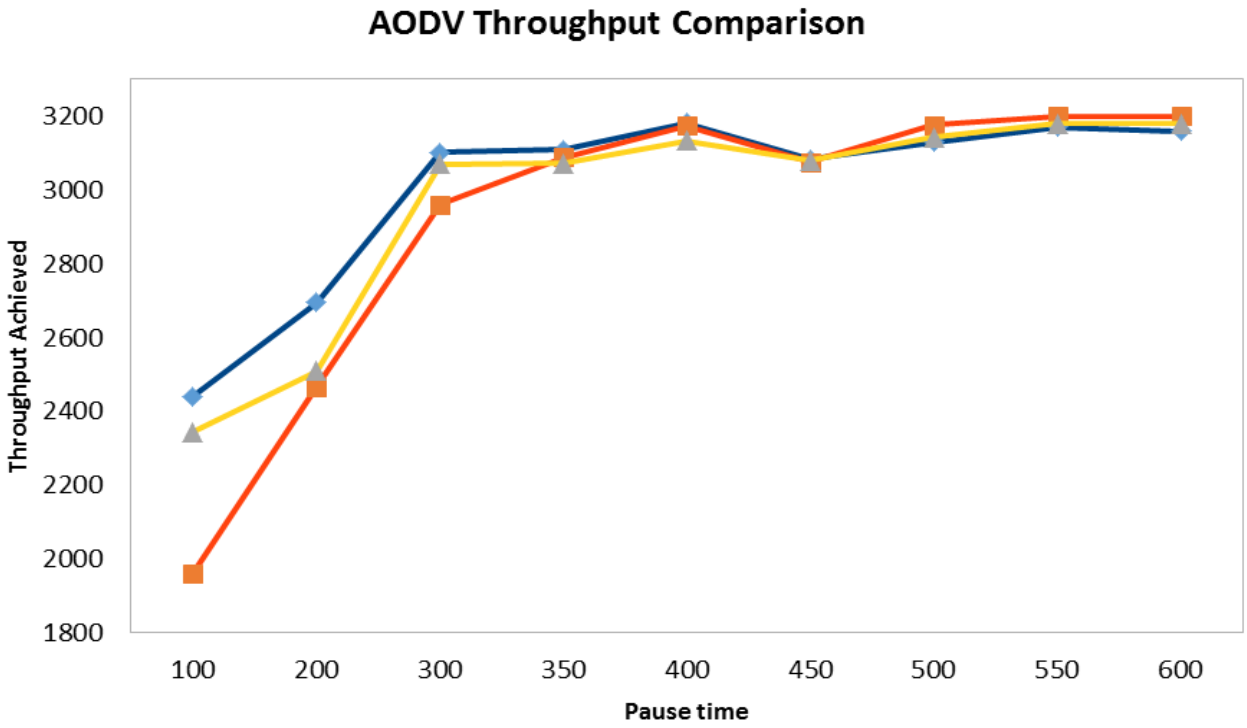


Graph 2 : protocol using delay metric for smaller MANET with varying pause time

Graph 2 is description of 10 nodes scenario with pause time as a function in three different scenes. Pause time varies from 100 ms to 600 ms. Normal scenario in blue line represent minimum delay in data transmission.

When intruder attacks the network delay prouced is increased to considerable extent shown in red line which is almost similar in case of proposed algorithm as displayed by yellow line and need to be improved upto normal.

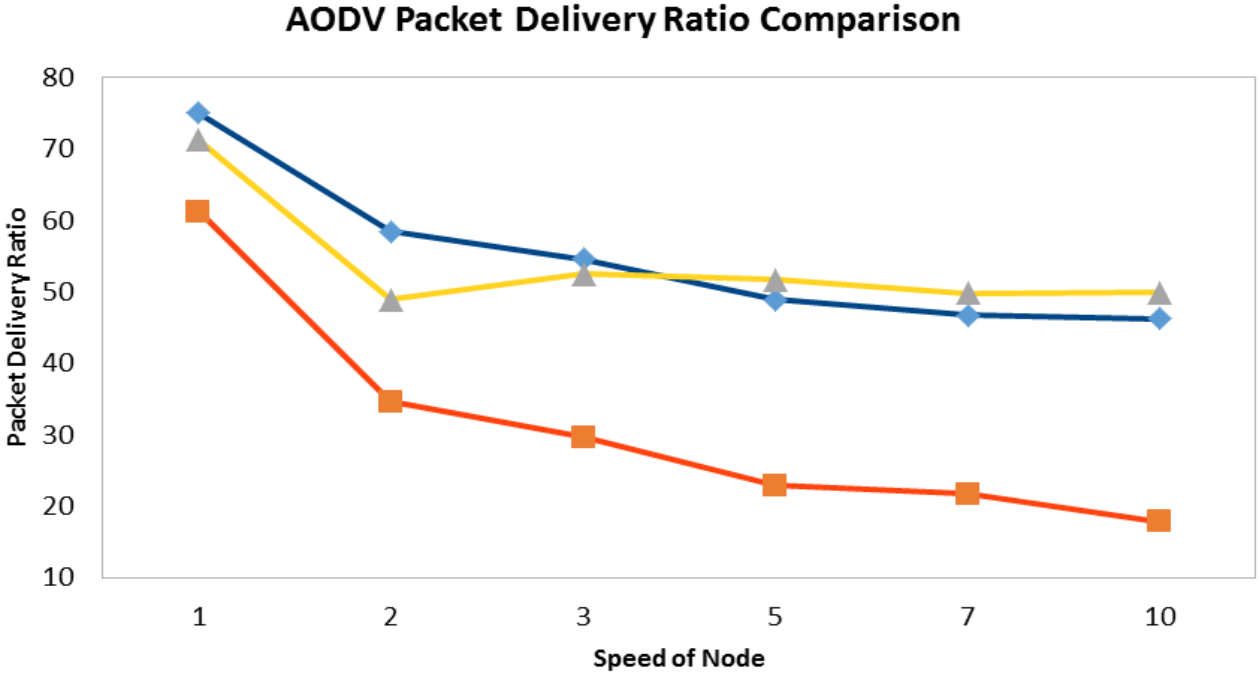
International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)



Graph 3: throughput metric in smaller MANET with vaying pause time

Graph 3 is description of 10 nodes scenario with pause time as a function in three different scenes. Pause time varies from 100 ms to 600 ms.

Throughput Achieved is reduced to 1900 from 2500 when intruder enters in the nework. The proposed scheme recovers the throghput to considerable amount.

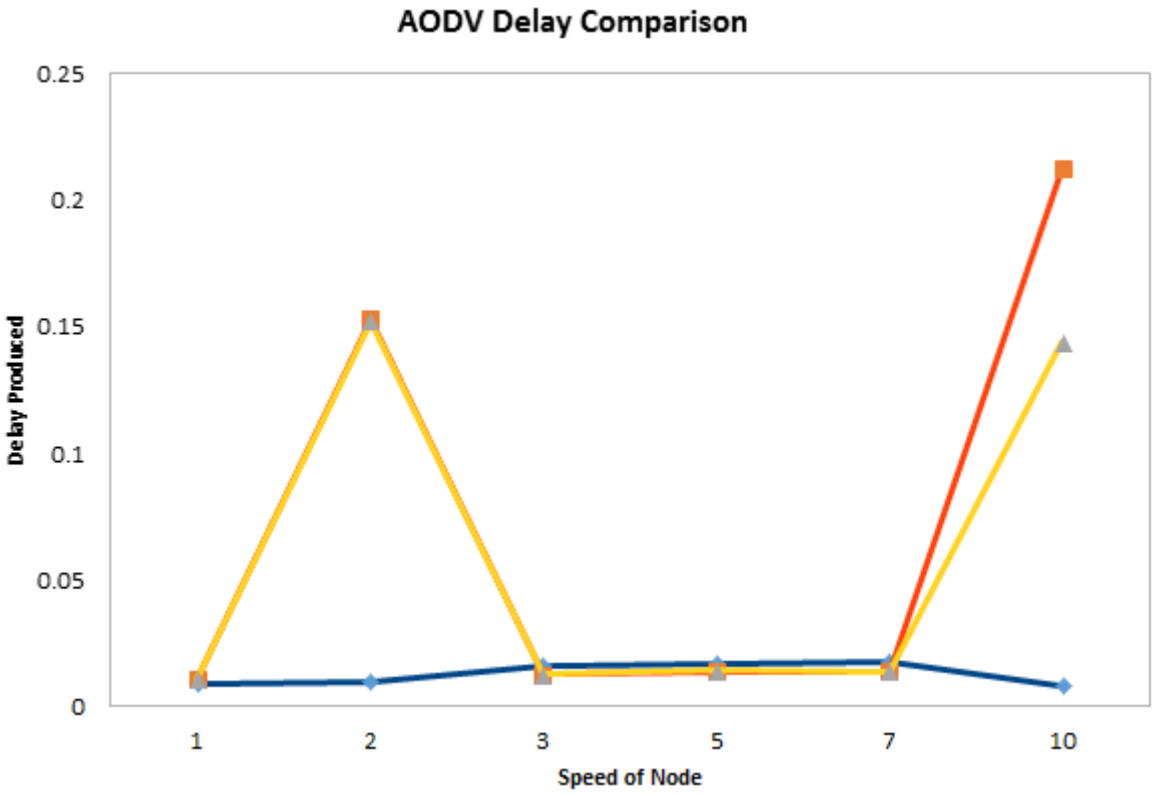


Graph 4 : PDR metric with varying speed of nodes in smaller MANET

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

The graph 4 is representation of PDR with speed as a function for 10 nodes in three scenes of AODV routing protocol. Speed has been varied from 1 m/s to 10 m/s. Normal scenario is blue line notation and red line notation denotes entry of an intruder.

Yellow line is depiction of recovery from intruder as proposped by new scheme. As desired the propsoed scheme is able to take care of Packet Delivery Ratio and is reaching the target at almost normal scene. As shown increase of 25% to 65 % is a great recovery particulary at higher speed of 10m/s.

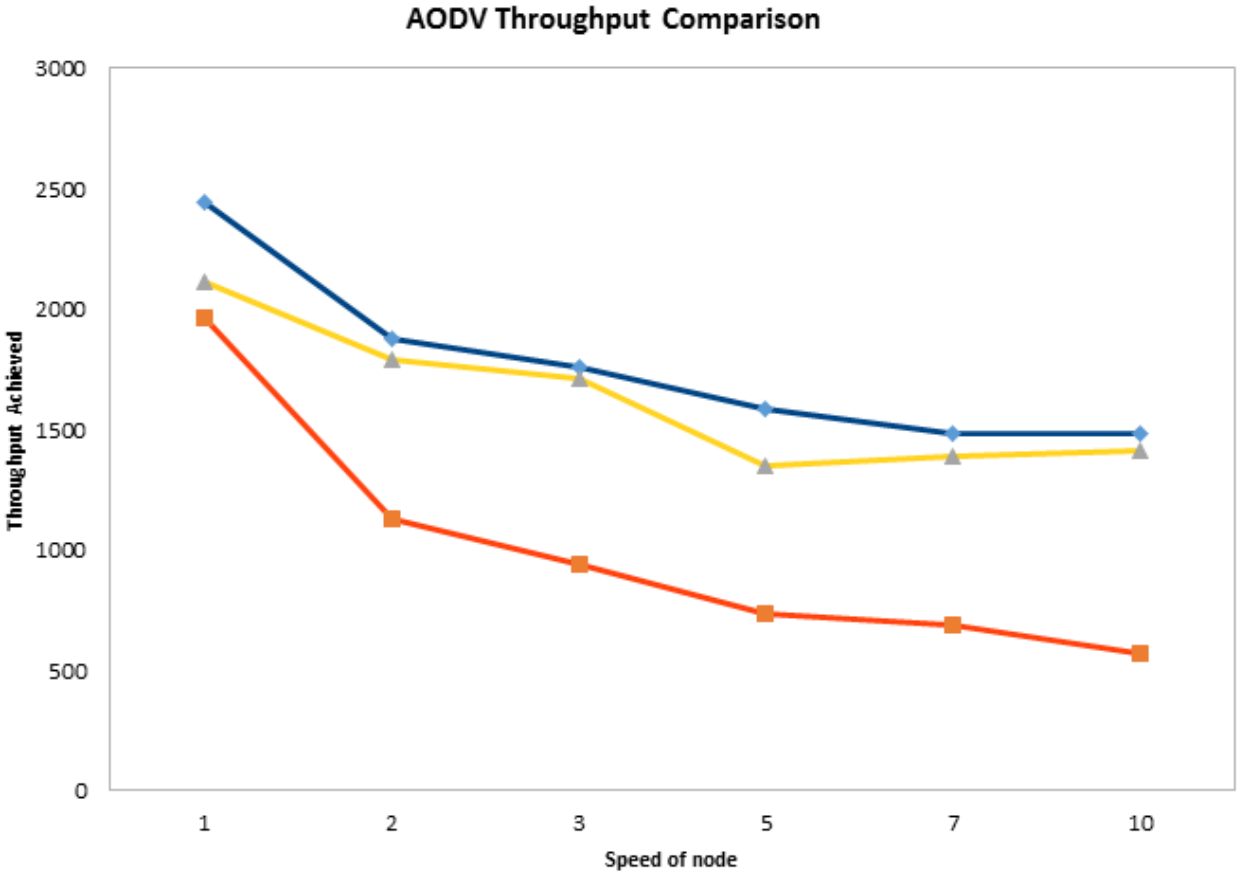


Graph 5 : varying speed in smaller MANET using delay metric

The graph 5 is representation of end to end delay with vaying speed of nodes from 1 m/s to 10 m/s for 10 nodes in three scenes of AODV routing protocol.Normal scenario is blue line notation and red line notation denotes entry of an intruder.

Yellow line is depiction of recovery from intruder as proposped by new scheme. As shown in graph the proposed algorithm minimized the delay to almost half particulary at higher speed of 10m/s.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

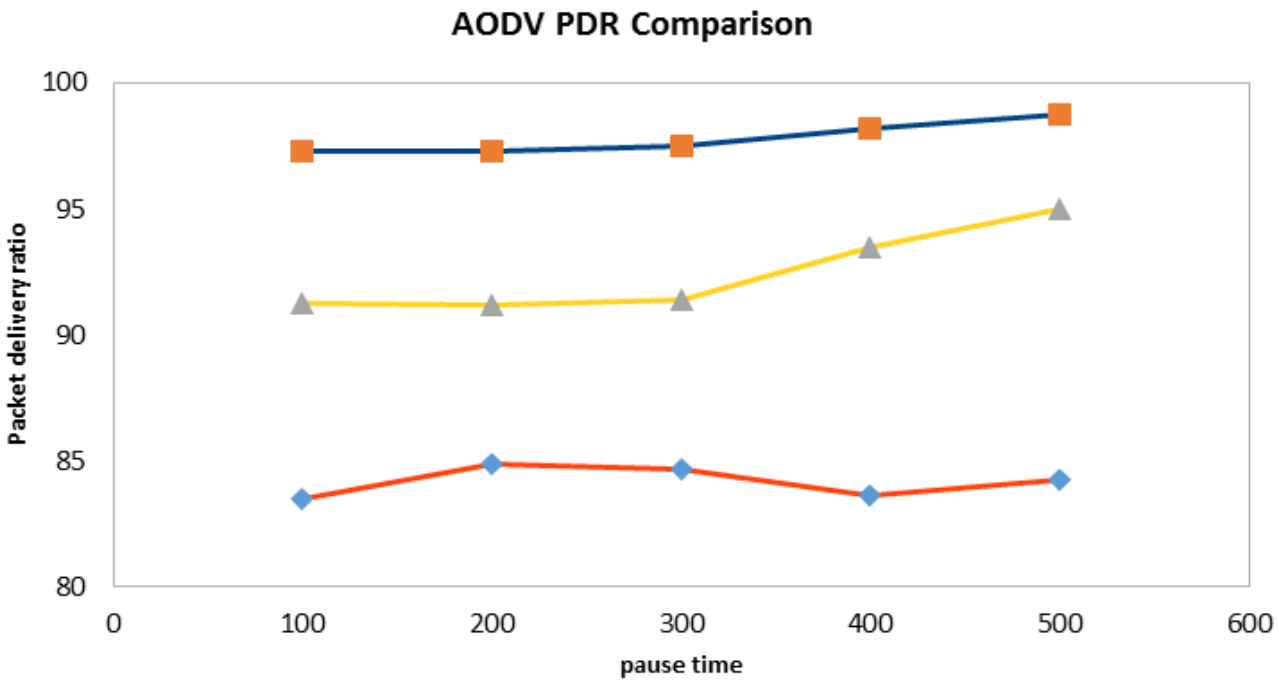


Graph 6 : Varying speed of node in smaller MANET using Throughput metric

The graph 6 is representation of throughput achieved in the network when speed of nodes varies from 1 m/s to 10 m/s using AODV routing protocol.

The graph explains that as the speed of nodes increases the throughput of the network decreases and further the intruder decreased the normal throughput of 2000(blue line) to 900(red line) at the speed 10 m/s which is almost recoverd to 1900 as shown by yellow line. This is the great sucess of proposed algorithm.

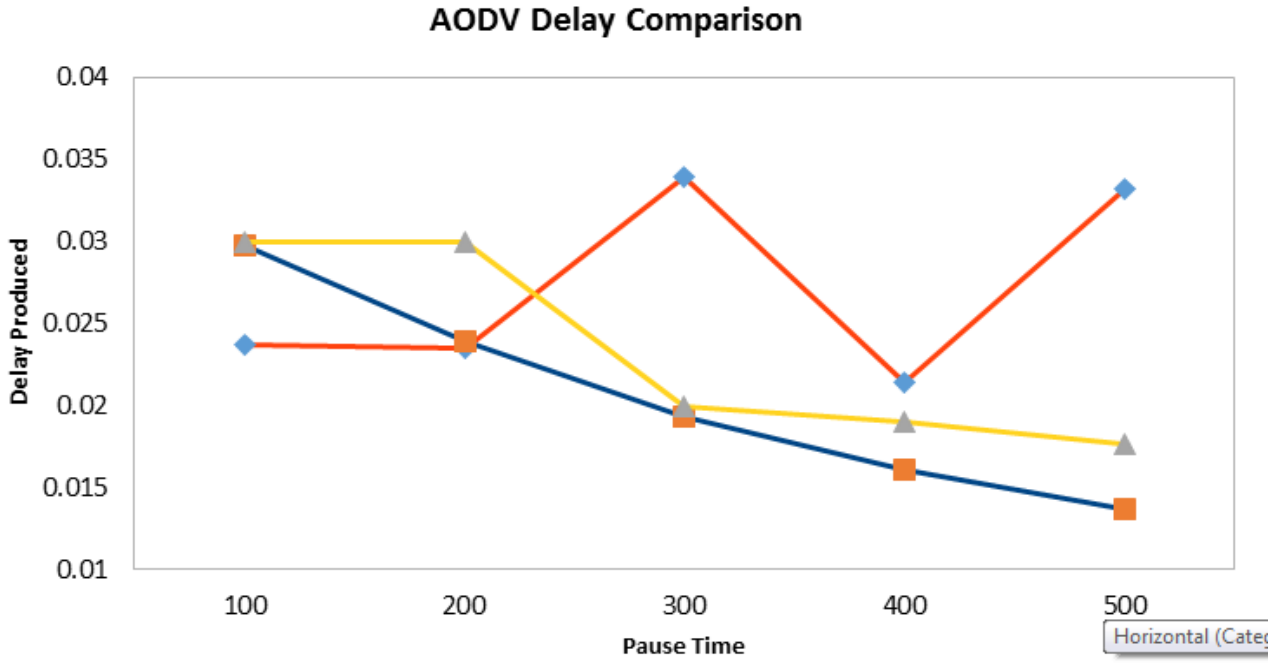
International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)



Graph 7 : PDR metric in Medium Sized MANET with varying pause time

Graph 7 clearly explains that a considerable decrease from 97%(blue line) to 83%(red line) in packet delivery ratio happens when intruder comes in the network which was not the case for smaller MANETs and it further increases in larger networks as shown ahead in graphs for larger MANETs.

The yellow line displays the large recovery in packet delivery ratio upto 94% which is closer to normal profile and success of proposed algorithm.

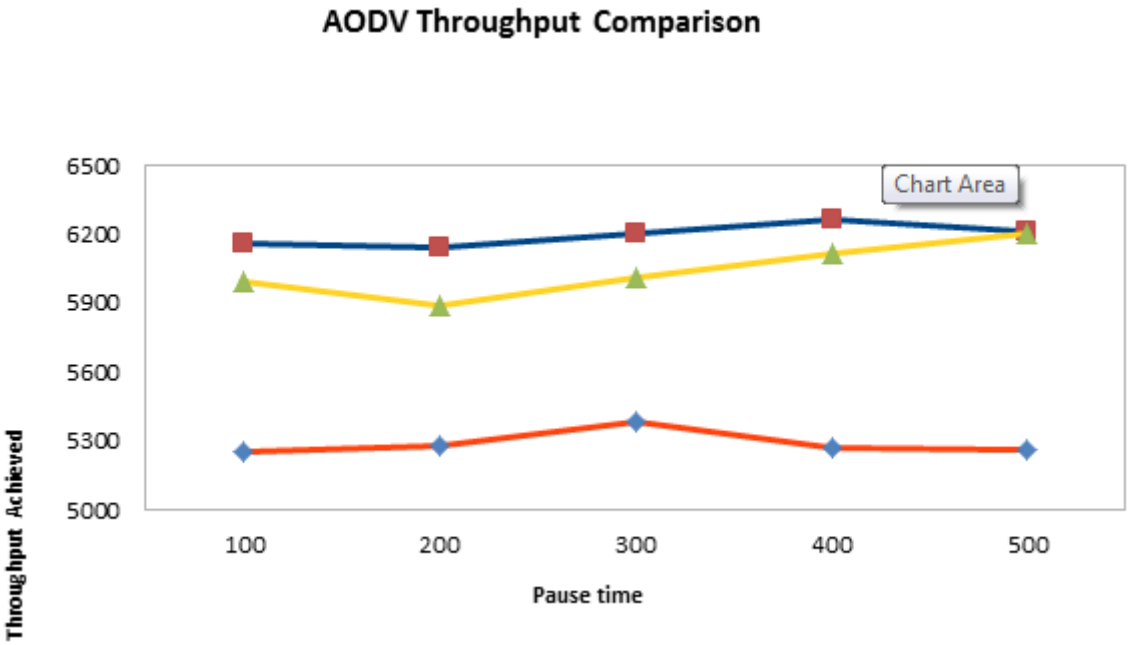


Graph 8 : Delay metric in medium sized MANET with varying pause time

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Graph 8 is representation of delay introduced in the network when packets travels from souce to destination. The pause time varies from 100 to 500. The graph shows that with increasing pause time the delay produced reduces in normal AODV protocol as displayed in blue line but the same in increasing on the introduction of intruder displayed by red line in the MANETs.

It worsen the situation. When the proposed algorithm is applied to repair the network and removing the intruder the delay decreases very fast and comes closer to normal profile of the network. Clearly the algorithm is performing well in medium sized networks as compared to smaller MANETs where delay is still required to be minimized.

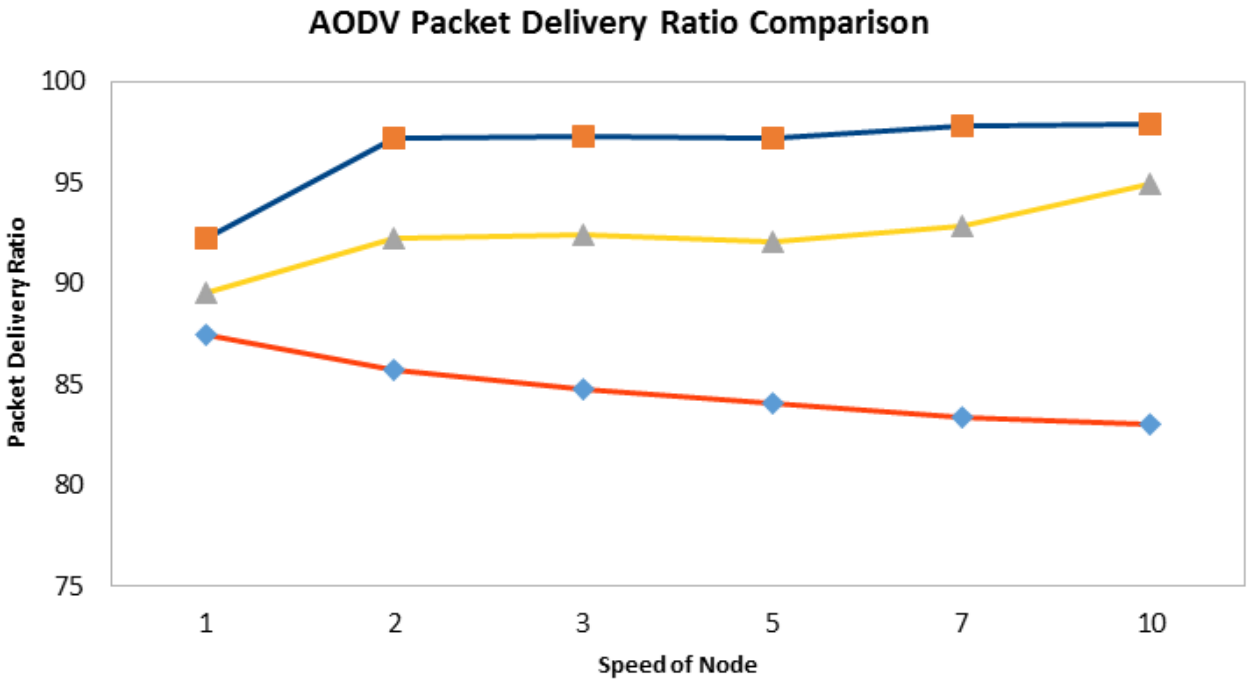


Graph 9 : Throughput metric in medium sized MANET with varying pause time

The results of graph 9 shows a large decrease in throghput by the malicious node (red line) and a considerable recovery by the proposed algorithm (Yellow line) in comparison to normal scenario (blue line).

The new scheme has good results in medium sized MANETs

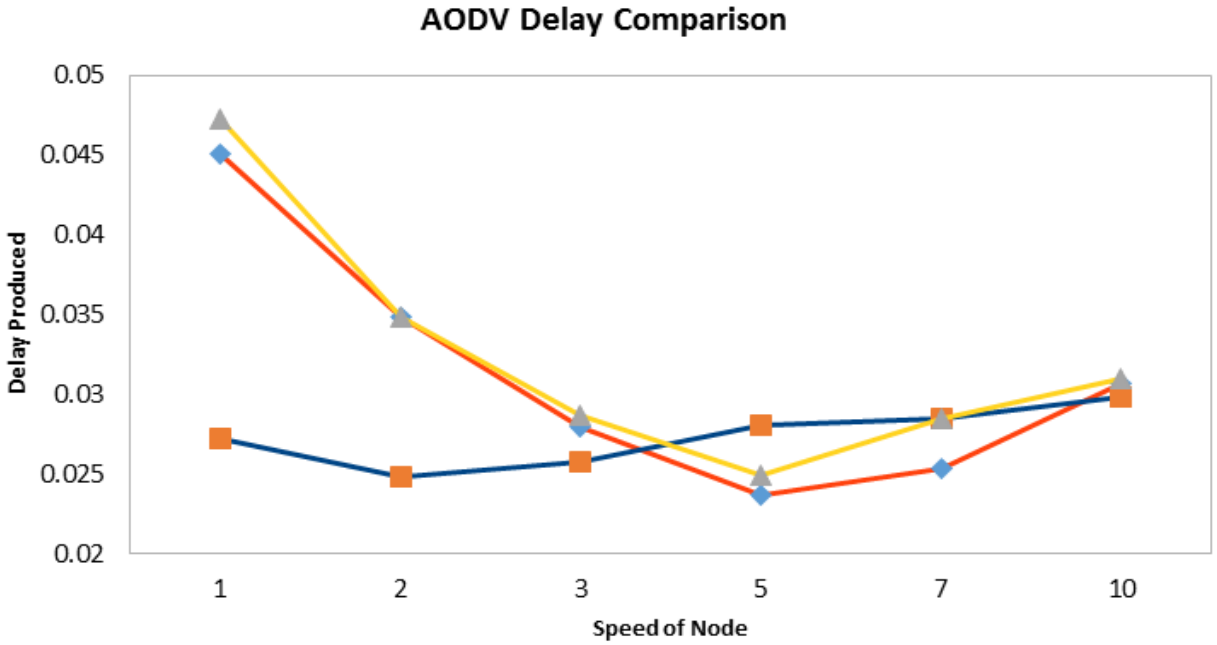
International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)



Graph 10 : PDR metric in Medium sized MANET with varying speeds of nodes

Graph 10 shows that in normal profile displayed using blue line tha packet delivery ratio increases as the speed of node increases but when intruder comes into play normal scenario reverses means packet delivery ratio decreases as the speed of node increases displayed by red line.

The proposed algoritm displayed by the yellow line recovers the normal scenario shows the sucess of algorithm.

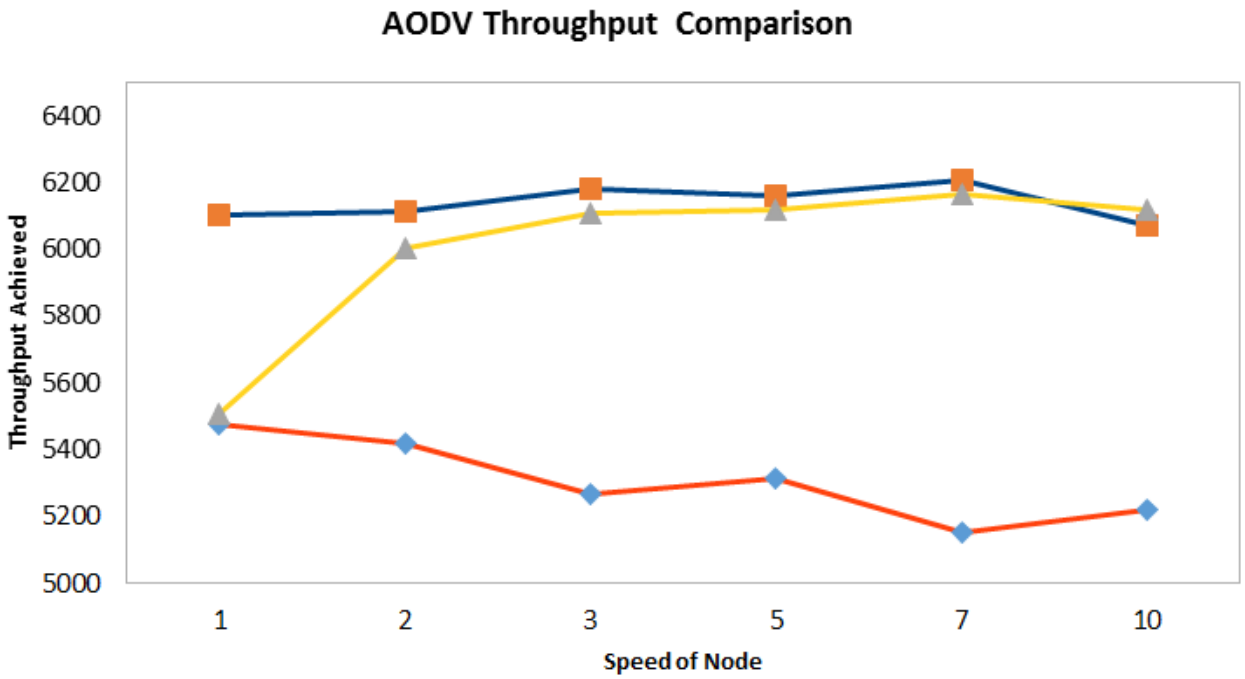


Graph 11 : Delay metric in Medium sized MANET with varying speeds of nodes

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Graph 11 is representation of delay produced in three different scenario of AODV protocol in case of medium sized MANETs. The varying speed of nodes from 1 m/s to 10 m/s is used as the parameter of evaluation. The blue line displays the normal scenario clearly indicates that delay produced is more than smaller MANETs.

But when a malicious node enters the network the situation gets worsen displayed using red line which needs to improved. The proposed algorithm displayed by yellow line is not showing much promising results in this case.

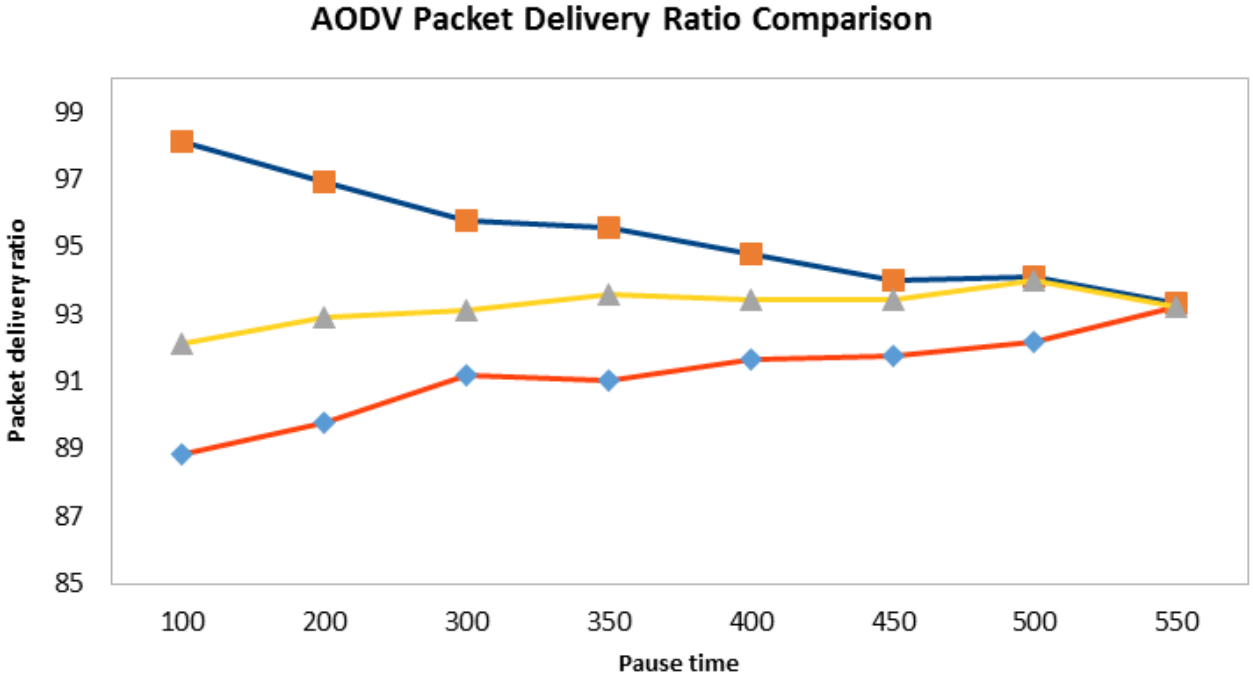


Graph 12 : Throghput metric in Medium sized MANET with varying speeds of nodes

Graph 12 shows a large decrease in throghput from 6100 packets to 5300 packets by the malicious node (red line) and a considerable recovery aaproximately 6100 by the proposed algorithm (Yellow line) in comparison to normal scenario (blue line).

The new scheme has good results in medium sized MANETs and proves to be much promising.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

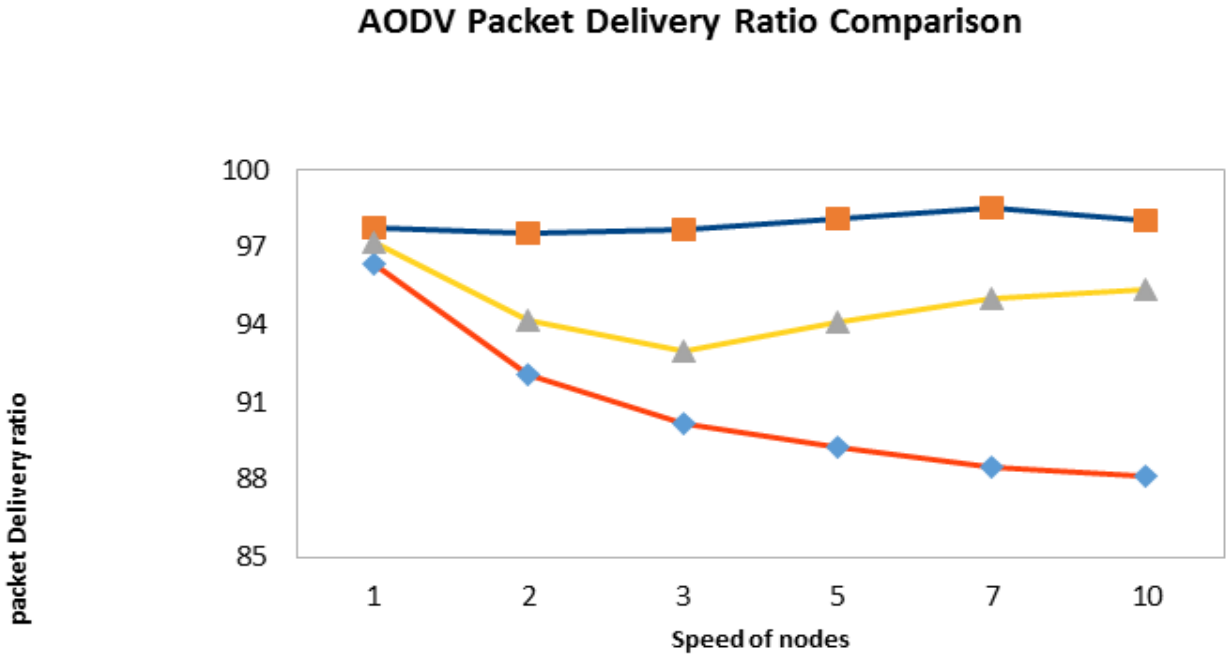


Graph 13 : PDR metric with varying Pause time in Larger MANET

Graph 13 is shows the execution of AODV protocol in MANET of 50 nodes for varying pause time from 100 ms to 550 ms. Graph clearly depicts the huge reduction in packet delivery ratio caused by malacious node (intruder) as blue line is at comparatively much higher level/value than red line. The increased traffic may be the reason for intruder to effect the performance of neighbouring nodes.

In case of 10 nodes this situation is not so critical since the traffic is very less. After applying the proposed algorithm to repair the false or malacious node considerable improvement in packet delivery ratio has been achieved shown in graph by yellow notation.This shows the proposed algorithm is working well to improve the performance of AODV protocol as the network becomes more denser.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

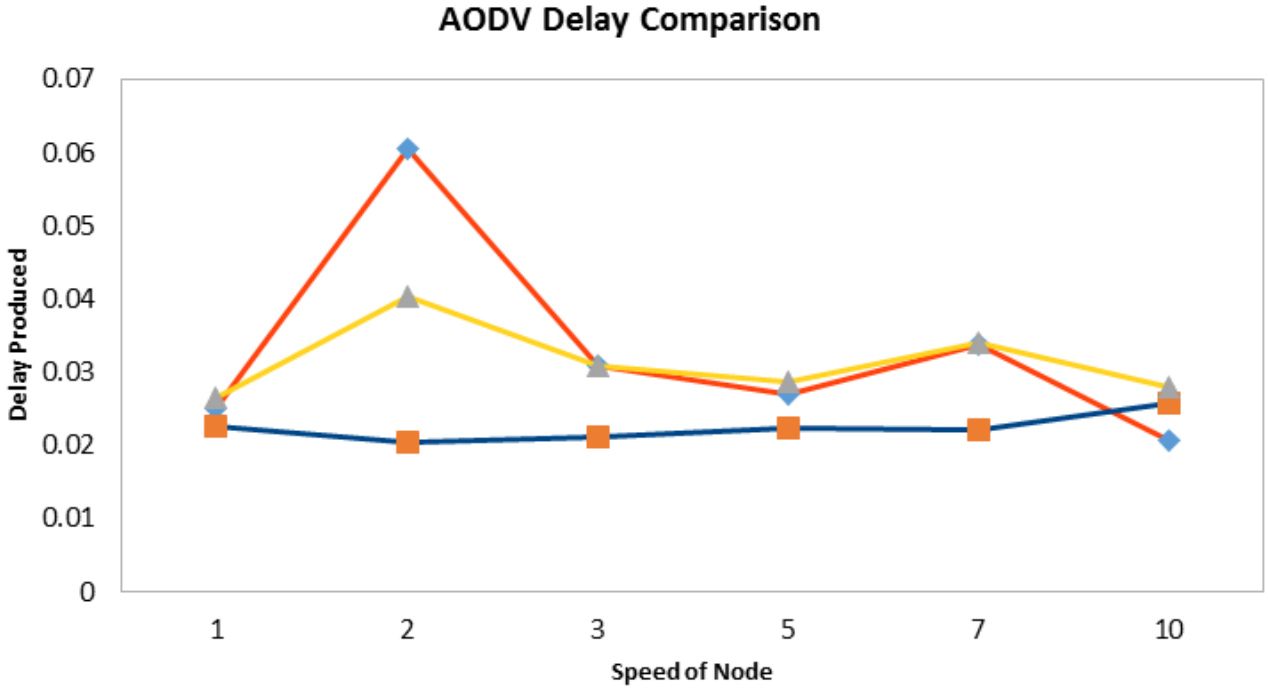


Graph 14 : PDR metric in larger MANET with varying speeds of nodes

The graph 14 is representation of PDR with speed as a function for 50 nodes in three scenes of AODV routing protocol. Speed has been varied from 1 m/s to 10 m/s. Normal scenario is blue line notation and red line notation denotes entry of an intruder. Yellow line is depiction of recovery from intruder as proposed by new scheme.

As desired the proposed scheme is able overcome the loss introduced by the intruder or malacious node and recover the PDR which is very close to normal profile of the network. The graph displays that as the speed of node increases the normal PDR reaching upto 98% and intruder reduces it to 88% which is recovered by the proposed scheme upto 96% is a significant gain.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

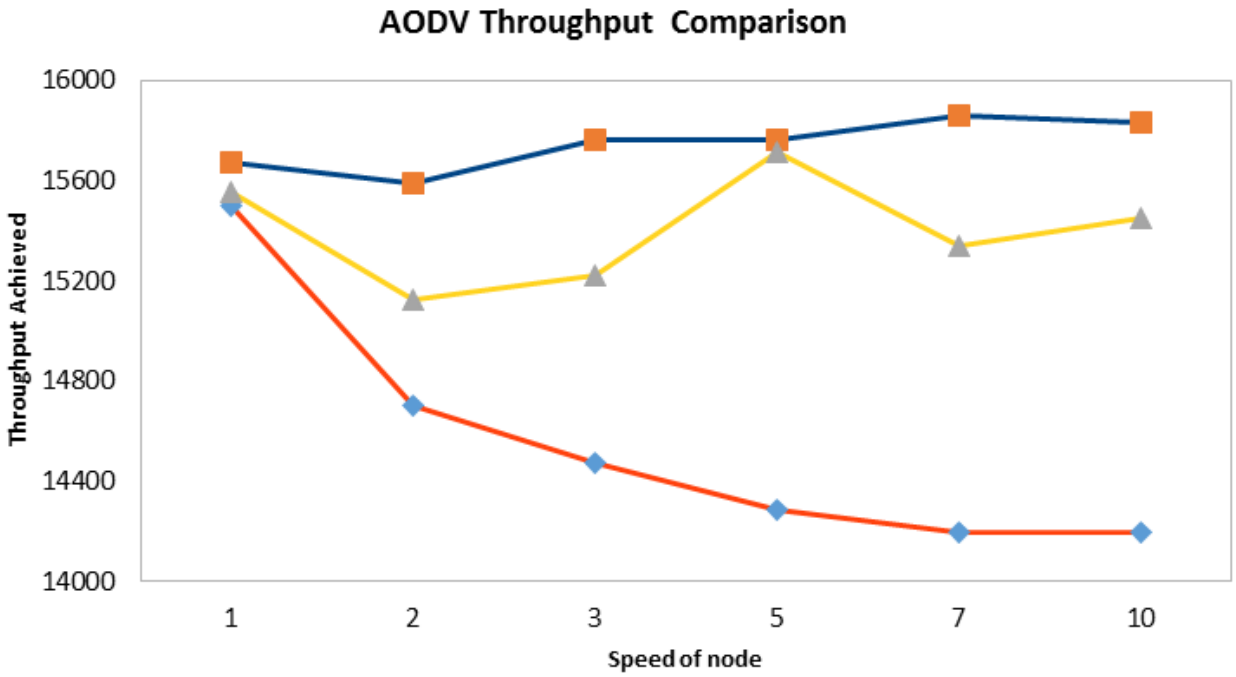


Graph 15 : PDR metric in larger MANET with varying speeds of nodes

The graph 15 is representation of end to end delay introduced in data communication having larger MANET with varying speeds from 1 m/s to 10 m/s and AODV as routing protocol. Normal scenario is blue line notation and red line notation denotes entry of an intruder. Yellow line is depiction of recovery from intruder as proposped by new scheme.

As desired the propsoed scheme is able overcome the loss introduced by the intruder or malacious node and minimized the delay which is very close to normal profile of the network. The graph displays that at speed normally more than 2% delay introduced in the network which is increased upto 6% by the intruder and after recovering the intrusion using proposed algorithm the delay is minimized upto 3% which seems to be good performance of proposed algorithm.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)



Graph 18 : Performance of AODV using Throughput metric in larger MANET with varying speeds of nodes

The graph 18 is representation of throughput in larger MANET with nodes varying their speeds from 1 m/s to 10 m/s using AODV routing protocol. Normal scenario in blue line displays the maximum throghput is nearest to 16000 packets and the same is reduced to 14000 packets by the intruder as shown by red line . The proposped new scheme recovers it to 15500 packets displayed in yellow line.This shows that with the increase in nodes's speed performance of proposed algorithm increases.

V. Conclusion

The paper is a detailed study of intrusion's effect and its recovery by the proposed new algorithm on the MANETs taking AODV as base protocol. It also considers the effect of malicious nodes for smaller , medium as well as larger MANETs having 10, 20 and 50 nodes respectively. A new algorithm is designed to recover and repair from the effect of intrusion. The recovery is perfomed in second phase of the AODV and a new route is discovered either by bypassing or removing the intruder node. Three metrics namely packet delivery ratio, end to end delay and throughput used to verify the proposed scheme. Two parameters Pause time and speed of nodes used to evaluate the performance of proposed algorithm and the results are displayed using 18 graphs. The results explains that proposed new algorithm for handling intrusion gives excellent results for PDR and Throghput in smaller network but delay is still need to be improved.

In case of medium sized network intrusion has been more damaging and new algorithm recovers the damage to considerable extent and gives better results as compared to smaller networks. For Larger network graphs display much recoverd PDR and Throghput and delay is also minimized to large extent. Therefore, the new algorithm work well as the size of network becomes larger and larger. The whole work has been conducted using NS2 and using various scenarios with Random wayPoint Model.

In future the performance of new algorithm will be compared for other protocols like DSR and TORA. The effect of fading will also be considerd and more emphasis will be on use of stable routes.

REFERENCES

[1] Novarun Deb, Manali Chakraborty, Nabendu Chaki, “The evolution of IDS Solutions in Wireless Adhoc Networks to Wireless Mesh Network”,IJNSA vol 3, no. 6, November 2011.

[2] Ganesh J Solanke, Chandra P.R., “Literature Survey on IDS in MANET”, IJSET, vol. 4,issue 1, January 2015, ISSSN 2278-7798

[3] A. Kush, Seema “Evaluation of Routing Schemes for MANET” in A. Mantri et al. (Eds.): HPAGC 2011, CCIS 169, pp. 575–580, 2011. © Springer-Verlag Berlin Heidelberg 2011.

[4] A.Kush,Divya,Vishal ,” Energy efficient Routing for MANET” , Intl conf on applied and communication tech, Elsevier Pub, pp 189-194., 2014.

[5] R. Chaki, N. Chaki; "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.

[6] Aikaterini Mitrokotsa, Nikos Komninos, Christos Douligeris, "Intrusion Detection with Neural Networks and Watermarking Techniques for MANET," International Conference on Pervasive Services, pp. 118-127, IEEE Int'l Conference on Pervasive Services, 2007.

[7] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, Prabir Bhattacharya, Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 99, no. 1, 2008.

[8] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, 2002.

[9] H. Yang, J. Shu, X. Meng, S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE J. on Sel. Areas in Communications, vol. 24, pp. 261-273, 2006.

[10] P. Sil, R. Chaki, N. Chaki; "HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks", Proc. of 7th IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2008.

[11] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[12] Ayyaswamy Kathirvel, Enhanced Triple Umpiring System for Security and Performance Improvement in Wireless MANETS, International Journal of Communication Networks and Information Security (IJCNIS), Vol 2, No 2 (2010).

[13] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Adhoc Networks",International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[14] Apurva Kulkarni,Prashant Rewagad,Mayur Agrawal, "Literature Survey on IDS of MANET", International Journal of scientific research and management (IJSRM) , volume3,issue9,Pages3549-3552, 2015, www.ijsrm.in ISSN (e): 2321-3418.

[15] S. Taneja, D. A. Kush and A. Makkar (2011), "End to End Analysis of Prominent on Demand Routing protocols" ,International Journal of Computer Science and technology,vol. II, no. 1, pp. 42-46.