JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PERFORMANCE ANALYSIS OF ALGORITHM IN RATE TO DENSE NETWORK IN WIRELESS SENSOR NETWORKS

[1]Sumanpreet Kaur, [2] Dr. Mahendra Kumar

[1]Assistant Professor, [2] Associate Professor and Deputy Registrar (Academics)
[1]College of Engineering & Management, Neighborhood Campus Rampura Phul,
[1]Punjabi University, Patiala, India

ABSTRACT

Wireless Sensor Networks are the fastest growing networks due to their characteristics of self-configuration, self-administrationand dynamic topology. They are made up of a group of mobile nodes that are connected wirelessly in a self-configuring, self-healing network with no fixed infrastructure. In this paper, we used NS2 to stimulate and implement routing protocols and simulation outcomes for PDR (Packet Delivery Ratio),Delay and Throughput are being analysed and represented by all the graphs. Simulation is done to evaluate the packet delivery ratio, throughput and delay in which varied pause time and varied speed of nodes with variation in number of nodes for sparse, medium and dense network.The data analysis shows the results of ad-hoc networks for sparse and medium size and experiment continues for dense networks too.AODV is considered and selected as base protocol for implementation of new algorithm for securing network against intrusion.This exploration paper shows that AODV results in overall better performance after introducing malicious node as experiment results proves that theproposed algorithm helps in detecting and removing malicious nodes from rare, medium and dense wireless networks.

Keywords: Wireless Sensor Network, AODV, DSR, NS-2

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of a number of nodes. In this type of infrastructure-less network, nodes communicate without any centralized control or established infrastructure. One node act as a router. The routing is a challenging task in WSNs due to limited bandwidth and transmission range. Some nodes are fix and some moves quickly in this network and change their path quickly. Several small, inexpensive nodes and sensors are deployed in an open, unprotected environment for long periods of time to communicate and collection of sensitive data. The nodes in WSNs are supposed to self-organise into a network through wireless communication. The capability of self-configuration and wireless communication allows them to be deployed in an ad-hoc fashion in remote and hostile environments without any existing infrastructure. The figure 1 presents a WSNs, where a node is forwarding information to the base station via other nodes[1].

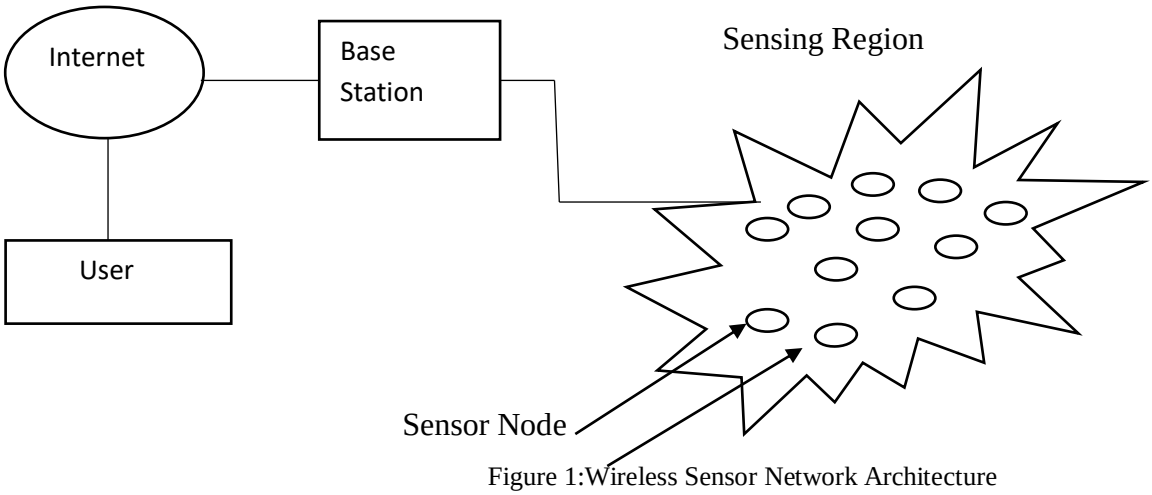


Figure 1:Wireless Sensor Network Architecture

What makes MANETS different from WSNs[2], we can say that on wireless networks, an ad-hoc network is instant network in which wireless devices are communicated directly with each other with self-configuration and short range. The mode of ad hoc allows all wireless devices within the communication range to operate together. Basically, MANET is designed for the establishment of a network anytime and anywhere, without specifications to infrastructure to support the mobility of the users in the network[3-4]. In such an environment, networks are subject to severe blocking. Therefore, the performance of an ad hoc system relies on the stability of the network architecture whereas a wireless sensor network (WSNs) is a network of several smallest nodes called sensors that is based on centralized communication with wireless signals. WSNs is special network that spread to sense the area of interest. The nodes in sensor network are limited with respect to energy supply, communication bandwidth and restricted computational capacity. It's expected that sensor nodes adjust and operate in changing environments and should be useable in large areas[5-6].The study is conducted in order to find an idea to build a new algorithm which may handle the intruder nodes efficiently. The purpose is to design an algorithm which may be able to find out the malicious node with surety and then discover a secure path for communication along with the removal of malicious node.

II. SIMULATION ENVIRONMENT

Simulator NS2 in WSN provides us with the idea of its output performance in real time situations [3]. The study is conducted in order to find an idea to build a new algorithm which may handle the intruder nodes efficiently. The purpose is to design an algorithm which may be able to search/find out the malicious node with surety and then discover a secure path for communication along with the removal of malicious node [7-10].This gives idea about new proposed algorithm SAODV in different types of wireless networks like sparse i.e., having low density of nodes in the network, medium size and dense i.e., having high density of nodes in the network [24-25]. The proposed algorithm is evaluated using three different calculation metrics namely delivery ratio of data packets (PDR), maximum output achieved i.e., throughput of the network and total communication delay i.e., end-to-end delay produced.The network will be established with the help of simulator NS-2. Therefore, first of all simulations of AODV and DSR executed under normal routing scenario in NS2 simulator and results are analysed by drawing graphs based on two separate parameters. The first parameter is variations in pause-time of simulation and the second parameter is changing speed of nodes in Manets. After that intruder nodes are deliberately inserted in the simulations of AODV and then their impact is studied and analysed with the help of drawing graphs. The intrusion of malicious nodes will be detected and metrics would be measured to check the efficiency of the network like PDF, Delay, Throughput, Load. The graphical notations will be used.In the present research work AODV is considered and selected as base protocol for implementation of new algorithm for securing networks against intrusion.The simulation details of all the three cases are illustrated in table 1.

Table 1: Simulation parameters for Sparse to Dense networks

Simulation Parameter	Sparse AdHoc Network	Medium Size AdHoc Network	Dense AdHoc Network
Nodes	10	20	50
Connections/ Channels	2-4	4-6	6-17
Model	Random Way Point	Random Way Point	Random Way Point
Simulation Time	700ms	700ms	700ms
Agents	CBR/TCP/UDP	CBR/TCP/UDP	CBR/TCP/UDP
Protocols	AODV	AODV	AODV
Packet Size	512	512	512
Area	700 × 700	700 × 700	1000 × 1000

AODV is used as base protocol for implementation of Proposed algorithm. The results of previous research are as mentioned in the table 2.

Table 2: Comparison of Proposed Algorithm with Previous study

Parameter	Network	Previous study [9]	AODV (normal)	AODV (with malicious)	AODV (proposed algo)
Delay(s)	Rare Network	.020	.01	.02	.010
	Medium Network	.025	.01	.03	.030
	Dense Network	.050	.03	.03	.030
Throughput (bps)	Rare Network	30000	31300	31750	31900
	Medium Network	30000	62130	52610	52090
	Dense Network	28000	15108	14729	14980
PDR (%)	Rare Network	100	98.9	98.2	98.7
	Medium Network	98	98.8	84.1	96.9
	Dense Network	97	94.1	92.2	93.9

III. METHODOLOGY

Many permutations and combinations were tried to tackle the issue. The initial phase was to use traditional methods like cryptography etc. It was tried but later on it was found that this method could notgive satisfactory results particularly for intruders. Also in most of the cases as overhead increases, calculations became tedious after a certain period of time. Then a new protocol was proposed based on existing AODV.Initial protocol use encryption and decryption for securing the data. It effectively encrypts the data and provides a good solution for securing the data from hackers. But the drawback of this scheme is that it is not able to detect and remove malicious nodes. Malicious nodes are not able to read the encrypted data but they can destroy the packets by providing fake route reply.

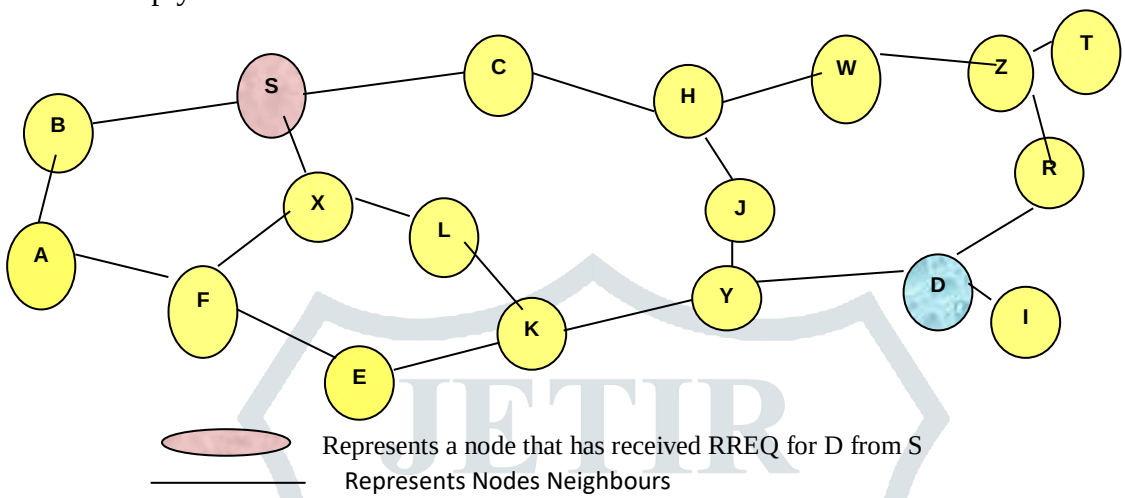
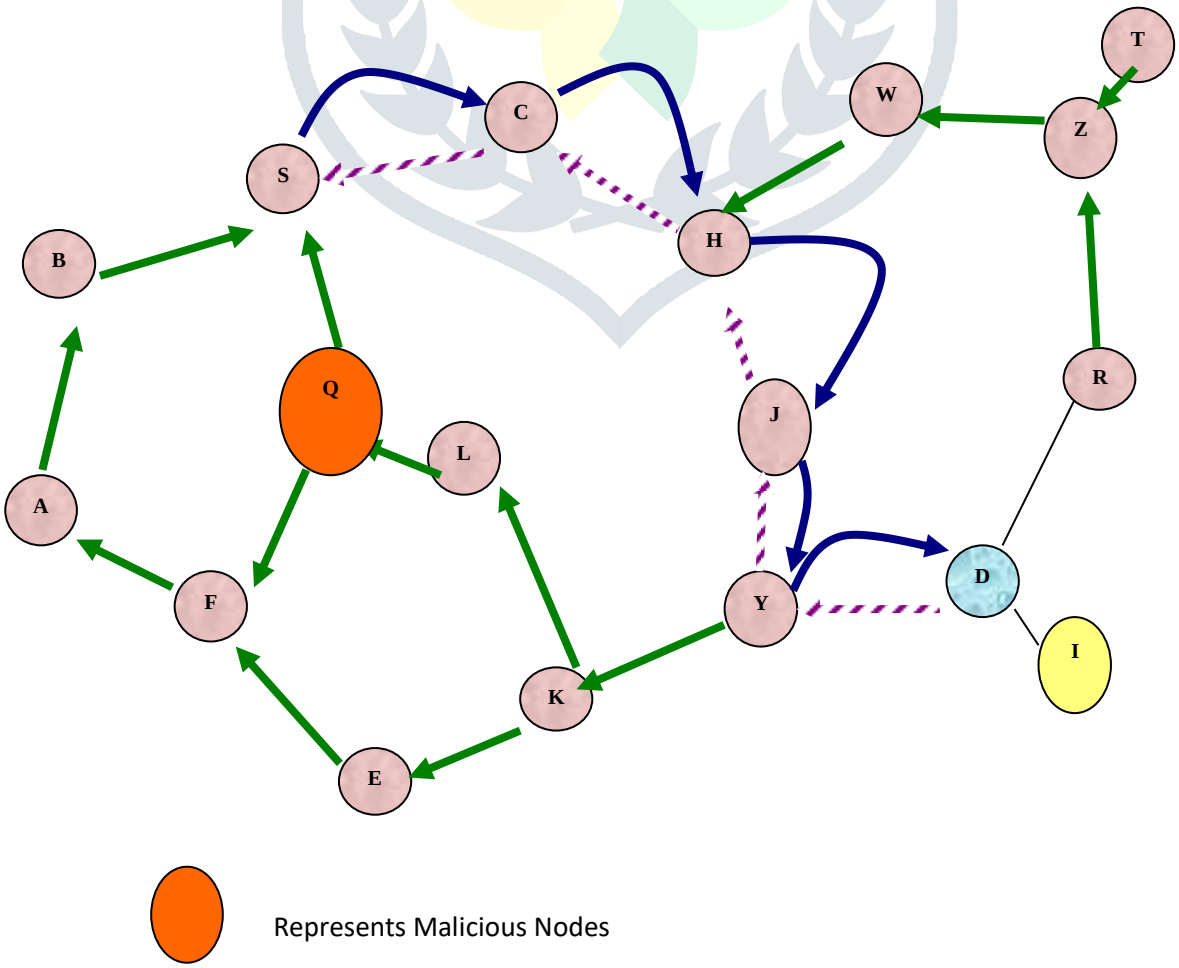


Figure 2:Route Requests in MAODV

If malicious nodes enter in the network they can provide fake route to the Source node and they can easily drop the packets. MaliciousAdhoc On-Demand Distance Vector Routing (MAODV) protocol shows the effect of malicious nodes on the performance of Ad-hoc On-Demand Distance Vector (AODV). In MAODV malicious



nodes are inserted at random locations in the existing AODV.

Figure 3: Malicious Node Enters in MAODV

These malicious nodes highly affect the performance of AODV. For detection and removal of malicious nodes second protocol Reverse on Demand Distance Vector (RAODV) has been proposed.

It successfully detects and removes malicious nodes. It also establishes a new path which is more stable and secure for MANET routing. AODV has been considered as the base protocol in the development of MAODV and RAODV.

3.1 Related Work in the field of Secure Routing

This section, proposes a methodology RAODV (Reverse Ad-Hoc On-Demand Distance Vector) for identifying malicious nodes with slightly modified SAODV (Proposed Algo) protocol. Every node has a sequence number.

- When a node wants to send data to any other node then RAODV set status of each node, participating in the routing process. It sets status of node as 'TRUE' whose sequence number is in between 'Source Node Sequence Number' and 'Destination Node Sequence Number'. Otherwise, it set status of this node as 'FALSE'.
- RAODV successfully detects and removes malicious nodes and generates a new path. This new path will be secured and will result in stable and secured routing. It starts with route request to search shortest path.
- Two arrays are used in this phase, first for malicious nodes and second for non-malicious 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 Array and if node status is 'FALSE' then this node enters in to the Malicious array.
- When transmission starts between Source and Destination, RAODV verifies status of each node in the path whether they belong to Malicious_Array or Non_Malicious_Array.
- If RAODV finds any node in the active route belongs to Malicious_Array then it generates a Route Error and stops.After detecting, RAODV marks this node as malicious node in the routing table and removes this node from the current route. When a RERR is generated, each intermediate node invalidates that particular route as shown in figure 4.
- After removing the malicious nodes RAODV tries to repair the route by releasing a local route request by an intermediate node. If the route is repaired then RAODV starts the transmission again between Source and Destination. If it is not able to repair the route then Source of the data receives the RERR, it invalidates the route and reinitiates route discovery. Then a new route is established by RAODV for data communication. After establishing this new route again, it verifies status of each node in the route.
- This process repeats until RAODV establishes a stable and secure route between Source and Destination.
- RAODV also takes care of the issue if malicious nodes enter in between the transmission. It checks status of every node if a current route is replaced by a new route.

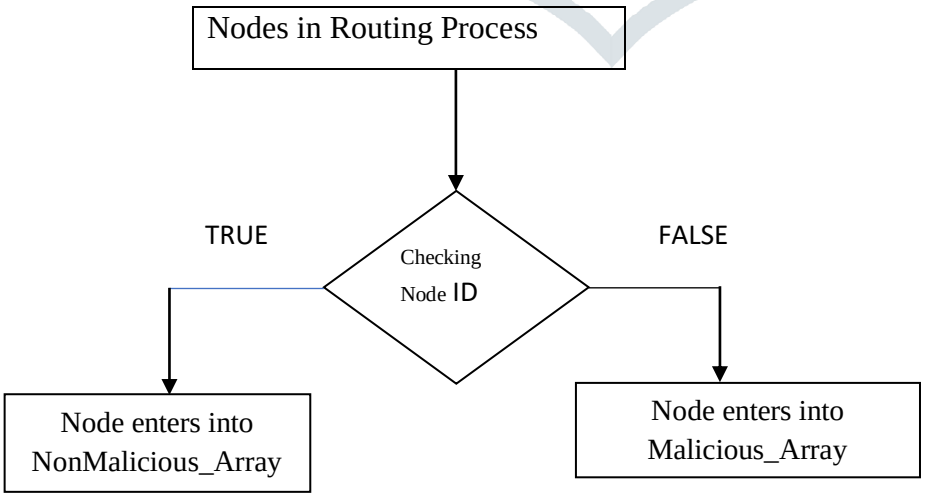


Figure 4: Setting Nodes Status

In MAODV it is not possible to detect malicious nodes but RAODV can detect the malicious nodes. RAODV verifies status of every node in the active route one by one. It checks the status of nodes whether they belong to

malicious or non malicious Array as shown in Figure 5. If there is any node in the route which does not belong to NonMalicious_Array then it generates an ERROR message.

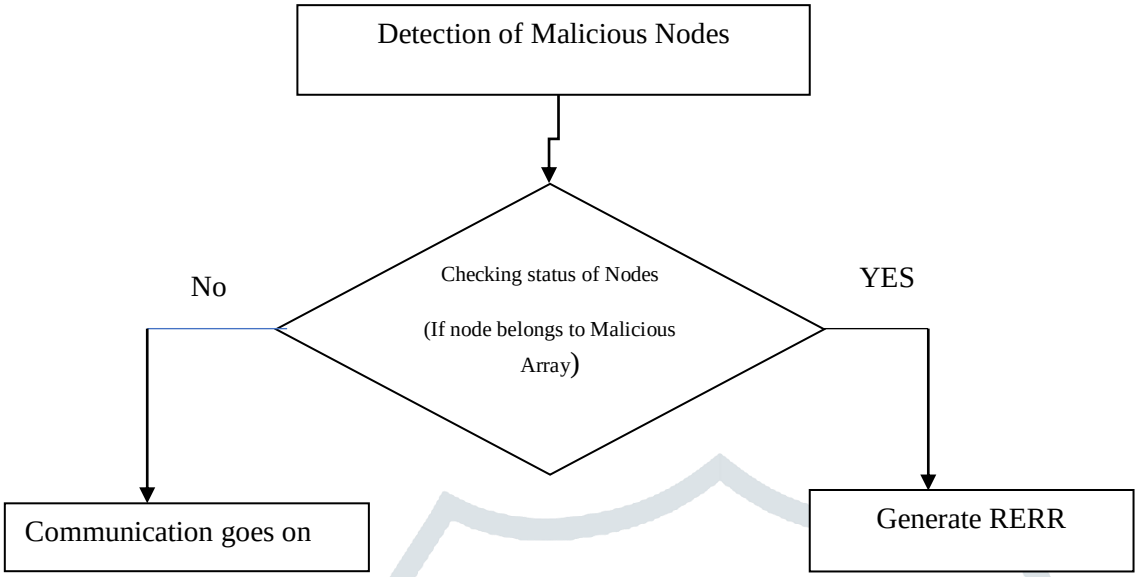


Figure 5: Detecting Malicious Nodes

3.1.1 Error Message Generation

After Detection of malicious nodes RAODV releases an ERROR message. The Route Error Message (RERR) allows RAODV to adjust routes when nodes move around. Whenever a node receives RERR it looks at the Routing Table and removes all the routes that contain the malicious nodes. It identifies that Q is a malicious node and it deactivates the path via Node Q as shown in Figure 6. It also mark Q as a malicious node in the routing table. After that it removes Node Q from the route.

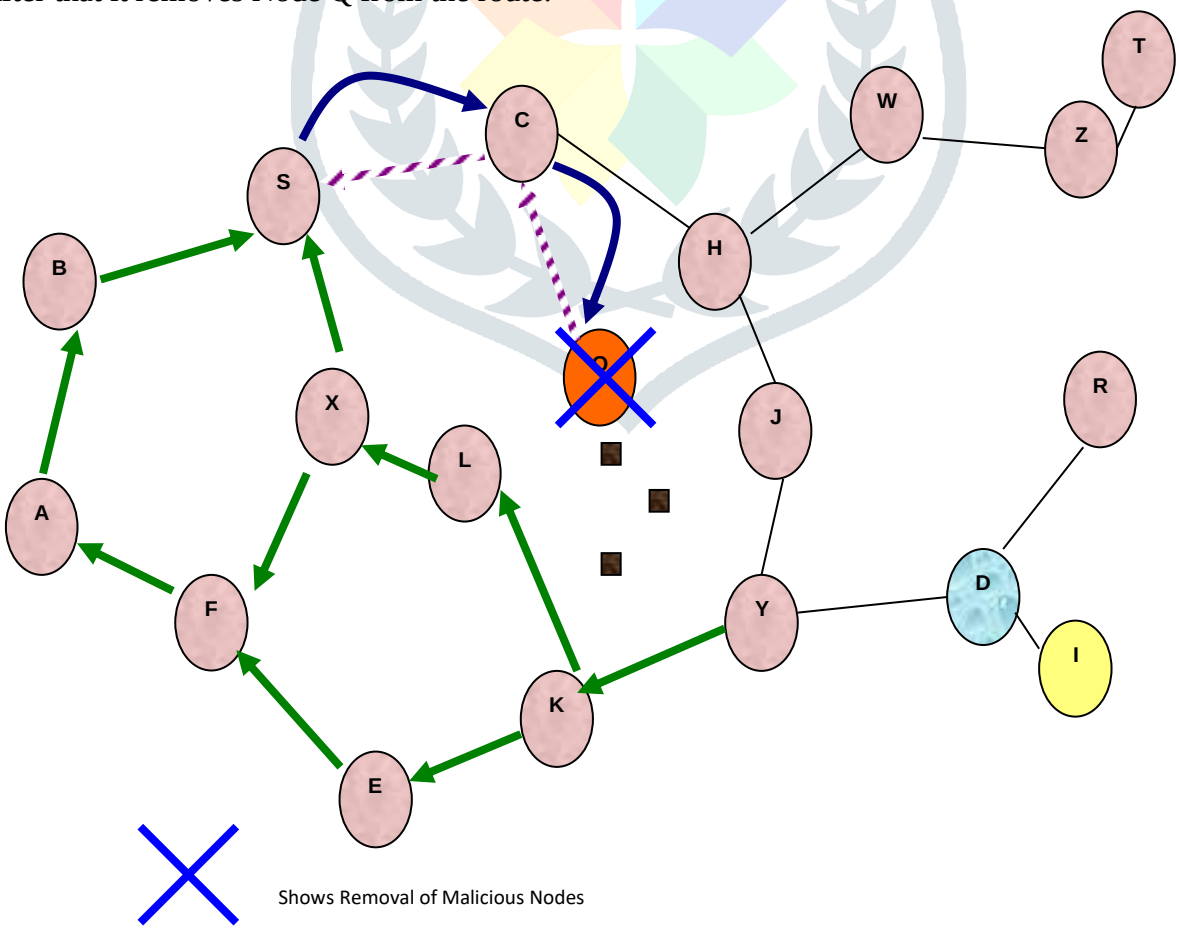


Figure 6: Removal of Malicious Node

IV. EXPERIMENTAL RESULTS

Simulation is done to evaluate the packet delivery ratio, throughput and delay in which varied pause time 100ms, 200ms, 300ms, 400ms and 500 ms and varied speed of nodes as 1m/s, 6 m/s and 100 m/swith variation in number of nodes 10, 20 and 50 i.e., for sparse, medium and dense network. The simulation outcomes for PDR(Packet Delivery Ratio), Delay and throughput are shown in Figures 2 to 13. Throughput (TP) is a measure of the data rate i.e. bits per second (bps) generated by the application.

TP =PacketSize/(PacketArrival- PacketStart) (i)

The latency (or delay) would be time taken by the packets to transverse from the source to the destination.

Average delay= (Packet Arrival- Packet Start)/n Average Jitter (ii)

Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source.

Packet Delivery Ratio =∑Number of packets received (iii)

∑Numberofpackets sent

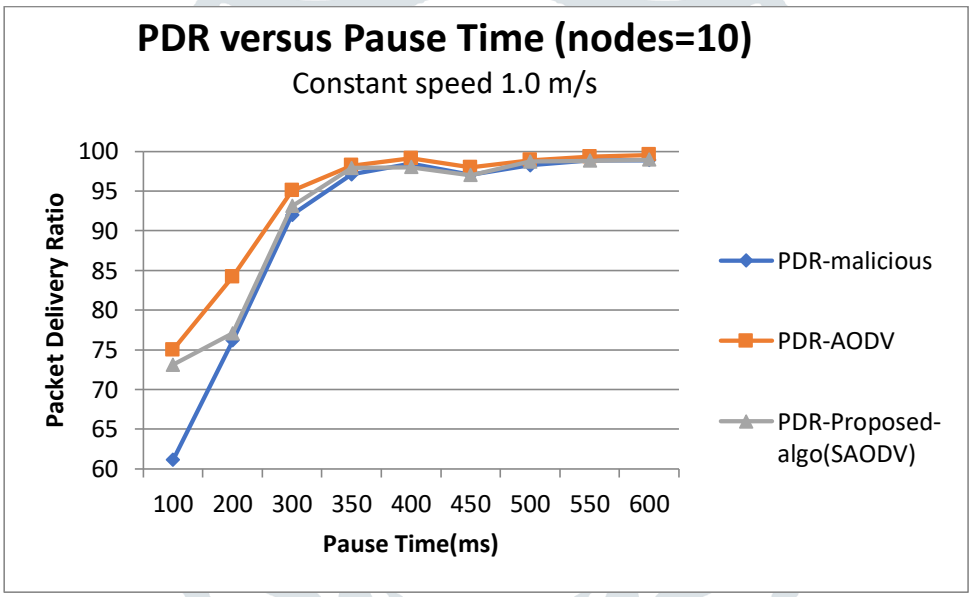


Figure 7: Average variation in Wireless Sensor Network with proposed Algorithm

It has been calculated based on three protocol distribution as, **Normal AODV** (without any modifications), then Malicious nodes are entered into the scenario and AODV becomes **Malicious AODV**, in this case unwanted node act as malicious or intruder and can cause loss of data, and third and final case is **Modified AODV** with proposed scheme.

The Fig. 7 shows Packet delivery ratio as a metric with pause time as function. It may be noted that when pause time is 100 ms it shows maximum movement of nodes and when pause time is 600 ms it actually denotes minimum movement.

It has been observed in figure that Packet delivery is best for Normal AODV when there are no malicious or unwanted intrusions and route is more or less stable. Almost 100 percent is achievable when pause time is reaching standard mark of 600 ms.

Then ADOV malicious case has been observed, as is obvious PDR declines sharply and there is loss of packets. This status is alarming, here comes into proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm and results are in line. It shows improvement in packet delivery. This is the desired result.

Result: Fig. 7 shows the desired result, so it can be stated that the proposed algorithm is working as per expected behaviour.

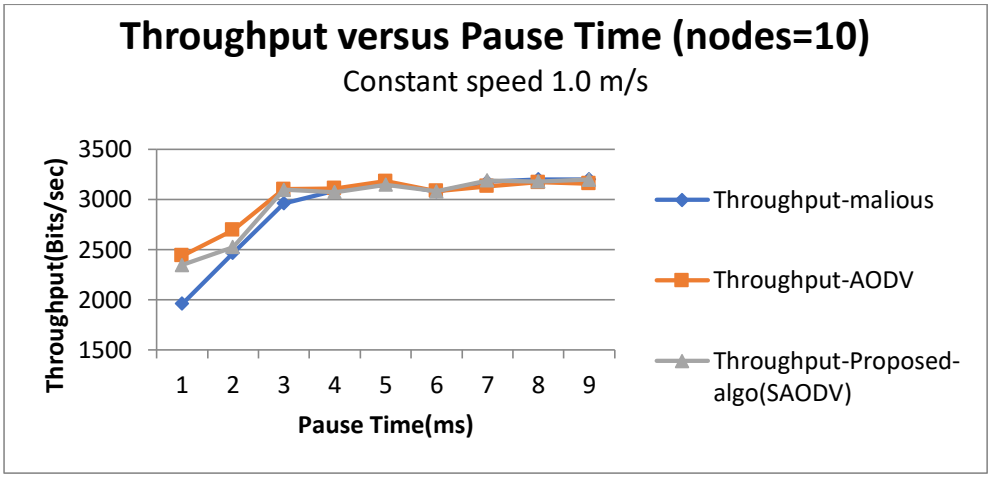


Figure 8: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 8 shows throughput as a metric with pause time as a function. It may be noted that in normal AODV when pause time is 100 ms throughput is 2400 packets which increases to 2700 packets at 200ms then 3100 packets to 300ms and finally reaches nearly 3200 packets when pause-time is 600ms during normal AODV. Then ADOV malicious case has been observed, as is obvious packet delivery declines sharply and there is loss of packets. This status is alarming, here comes into proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm and results are in line. Towards the end of simulation, it has been observed that in graph the Packet delivery is best for Normal AODV when there are no malicious or unwanted intrusions and route is more or less stable. Almost 100 percent is achievable when pause time is reaching standard mark of 600 ms. Throughput nearly becomes uniform in normal AODV as well as in proposed algorithm because network nearly acts as fixed network.

Result: Fig. 8 displays that the proposed algorithm is working as per expected behaviour as higher throughput is obtained in proposed algo.

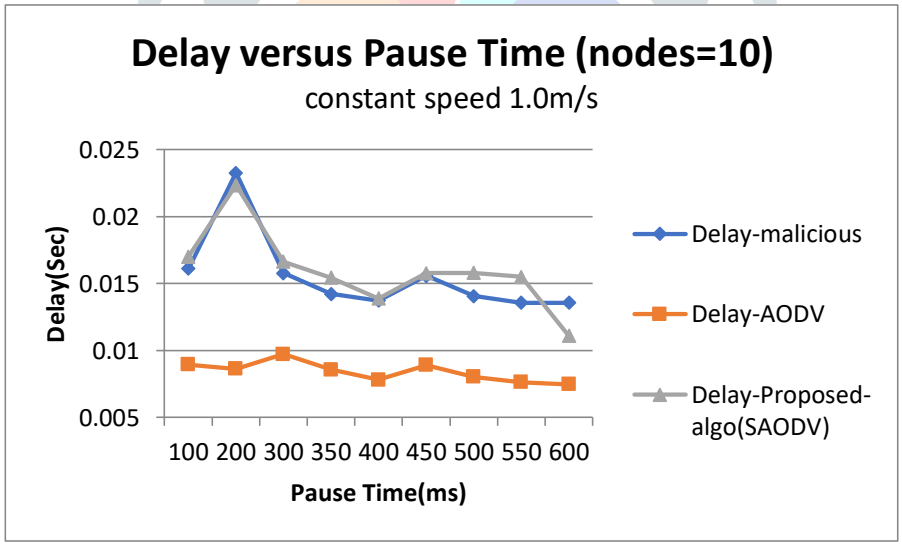


Figure 9: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 9 shows the variation in end-to-end delay metric with respect to pause-time as a function. During this scenario End-To-End delay, AODV has very low value lying between .008ms - .007ms, when pause-time varies from 100ms to 600ms which is considered almost negligible for mobile adhoc network scenario. Whereas, the proposed modified AODV shows more delays that is, 0.017-0.011ms when pause time varies between 100ms-600ms than normal scheme, more calculations are required to eliminate the malicious entry of node and this may cause a bit extra delay.

Result: Fig. 9 shows higher delay is produced in proposed scheme as compared to AODV. This can be acceptable easily as it comes with more packet delivery which is more important.

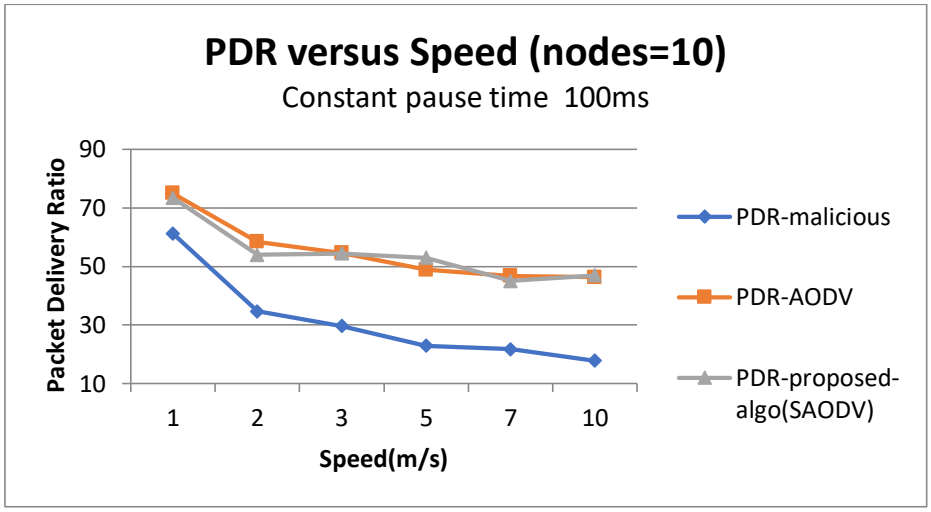


Figure 10: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig.10 shows Packet delivery ratio as a metric with speed as a function. During normal AODV routing execution, it is seen that PDR decreases with increasing speed of nodes. Figure shows that PDR is decreasing from 75% to 58% to 54% to 48% then to 46% when speed of node is increasing from 1m/s to 10m/s. Then Malicious nodes are entered into the scenario where PDR declines from 61% -17% when speed increases from 1m/s-10m/s. It has been observed in figure that Packet delivery is best for Normal AODV when there are no malicious or unwanted intrusions and route is more or less stable. Then ADOV malicious case has been observed, as is obvious PDR declines sharply and there is loss of packets. Then comes the proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm and results are in line. It shows improvement in packet delivery. The abrupt and sudden decrease of PDR in AODV may be due to the frequent route requests of route discovery process of AODV initiated with increasing speed of nodes.

Result: Fig. 10 clearly shows that the proposed algorithm and normal AODV almost gives equal results but packet drop is less in proposed algo as compared to normal AODV.

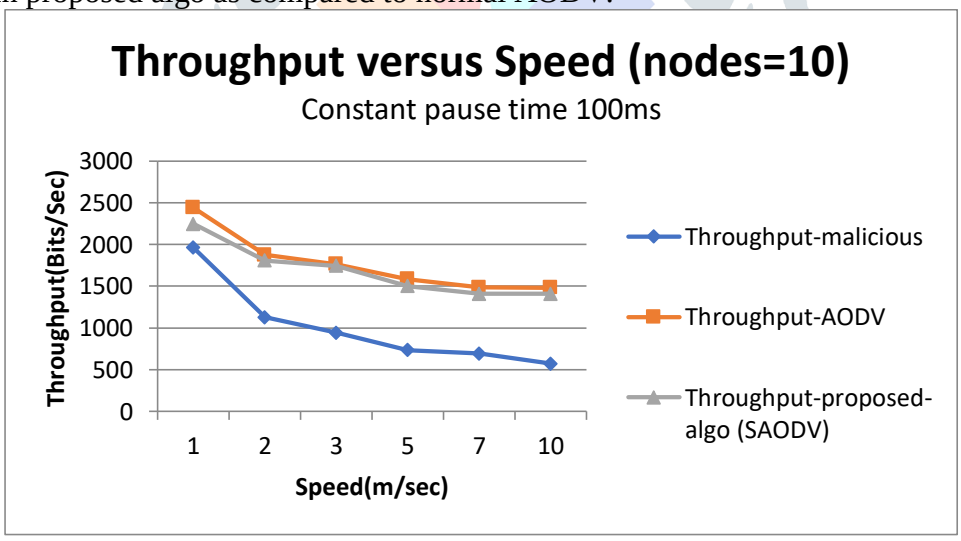


Figure 11: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 11 shows how throughput as a metric is affected with speed of node as a function. During normal AODV routing it is seen that when speed of node is 1m/s throughput is 2400 packets which decreases to 1800 packets at speed of node 2m/s then 1700 packets to 3m/s 1500 packets when speed of node is 5m/s and finally reaches nearly 1400 packets when speed of node is 7m/s and 10m/s. Then ADOV malicious case has been observed, as is obvious packet delivery declines sharply and there is loss of packets. This status is alarming, here comes into proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm. Towards the end of simulation, it has been observed that in figure the Packet delivery is best for Normal AODV when there are no malicious or unwanted intrusions and route is more or less stable. At the end of simulations result, throughput nearly becomes uniform. Figure clearly shows that throughput achieved in normal AODV is high as compared to proposed algo with increasing speed of nodes.

Result:It can be stated that throughput achieved in AODV is high as compared to proposed algorithm with increasing speed of nodes.

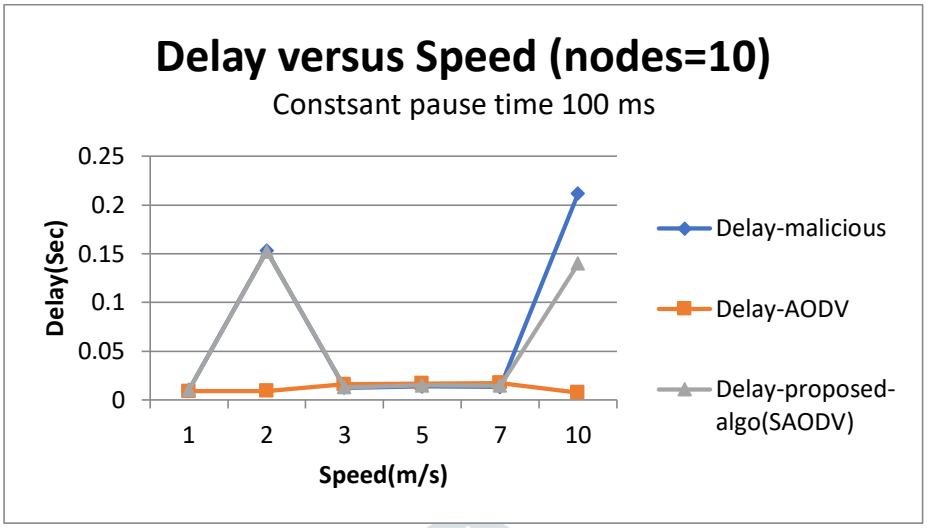


Figure 12: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 12 show the variations in End-To-End Delay metric with respect to speed of node as a function. During this scenario, AODV delay has very low value than desirable for wireless adhoc networks and same is lying in between .008ms to .007ms for varying speed of nodes from 1m/s to 10m/s which is almost negligible. But the delay value is increasing in AODV with respect to increase in speed of nodes. Whereas, the proposed modified AODV shows more delays than normal scheme. So, more calculations are required to eliminate the malicious entry of node and this may cause a bit extra delay. This can be acceptable easily as it comes with more packet delivery which is more important.

Result: Fig. 12 clearly shows that with the increasing speed of nodes, proposed algorithm has larger delay values because of frequent route requests but it can be acceptable easily as it comes with more packet delivery which is more important.
The fig. 7 to fig. 12 shows proposed AODV is better routing protocol with respect to pause-time as parameter and normal AODV is better routing protocol if speed of nodes is changing.

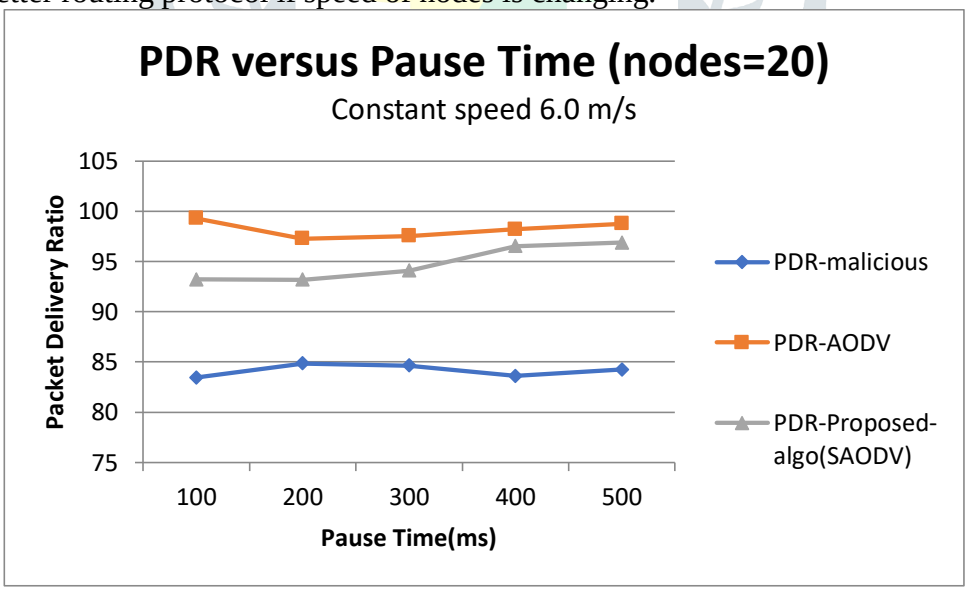


Figure 13: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 13 shows Packet delivery ratio as a metric with pause time as a function. It may be noted that during proposed algorithm when pause-time is 100ms and 200ms PDR is 93% which increases to 94% at 300ms and 400ms then to 96% at pause-time is 500ms.When Pause-time is 400-600ms, the PDR reaches to nearly 96% because the network nearly becomes fixed as the simulation runs upto pause time 500ms. It has been observed in figure that Packet delivery is best for Normal AODV when there are no malicious or unwanted intrusions and route is more or less stable. Then ADOV malicious case has been observed, as is obvious PDR declines sharply and there is loss of packets. Here comes into proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm and results are in line. It shows improvement in packet delivery.

Result: Fig.13 shows that for medium size network, normal AODV routing scenario and in proposed algorithm, packet delivery ratio is almost similar as proposed algo shows little improvement in packet delivery.

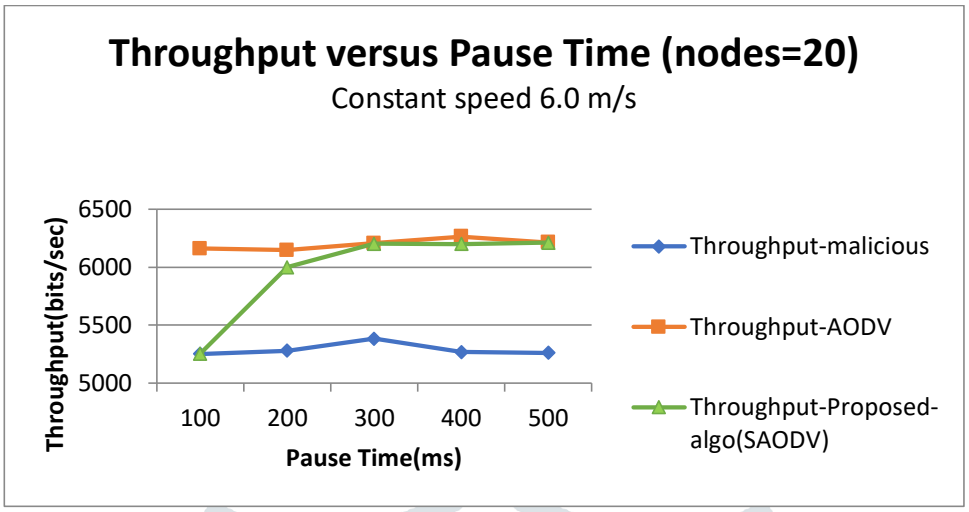


Figure 14: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 14 shows throughput as a metric with pause time as a function. It may be noted that when pause-time is 100ms and 200ms throughput is 6100 packets which increases to 6200 packets at pause-time 300ms-500ms during normal AODV routing. Then ADOV malicious case has been observed, as is obvious packet delivery declines and there is loss of packets. It is seen that when pause-time is 100ms and 200ms throughput is 5200 packets which increases to 6200 packets at pause-time 300ms-500ms during proposed algorithm. Third line shows modified scheme of AODV with implementation of algorithm and results are in line.

Result: Both normal AODV and proposed algo behaves equally good for medium size adhoc networks. However, Throughput of proposed AODV is greater than normal AODV routing.

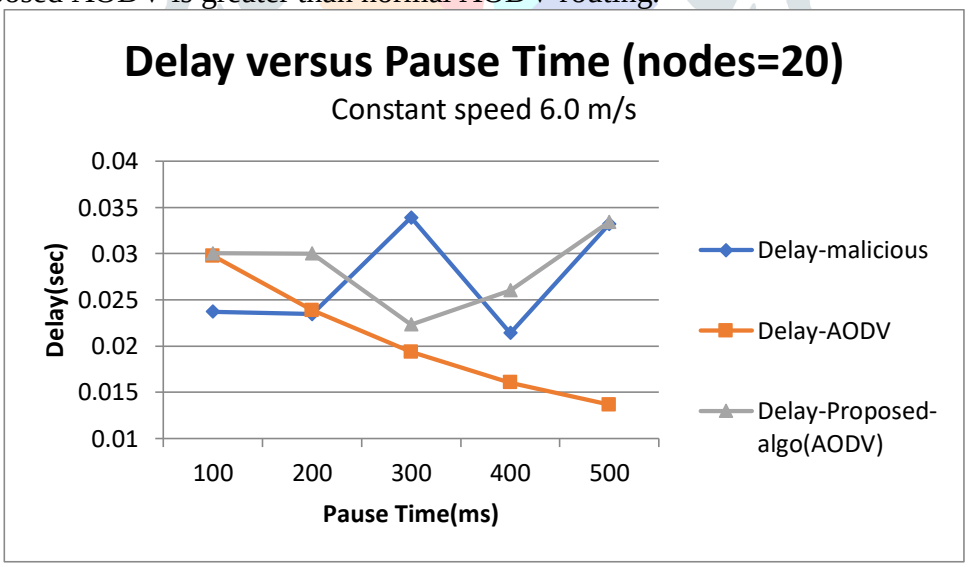


Figure 15: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 15 shows the variation of end-to-end delay metric with respect topause-time as one parameter. During normal AODV routing scenario end-to-end delay is considerable. However, delay reduces with respect to increase in pause-time having values lying in between .02ms - .013ms, when pause-time varies from 100ms to 500ms. The delay has value .03ms at 100ms, .023ms at 300ms and .03ms at 500ms pause-time during proposed algorithm. The proposed modified AODV shows more delays than normal scheme, more calculations are required to eliminate the malicious entry of node and this may cause a bit extra delay. This can be acceptable easily as it comes with more packet delivery which is more important.

Result: Fig. 15 shows higher delay produced in proposed algo routing as compared to normal AODV routing.

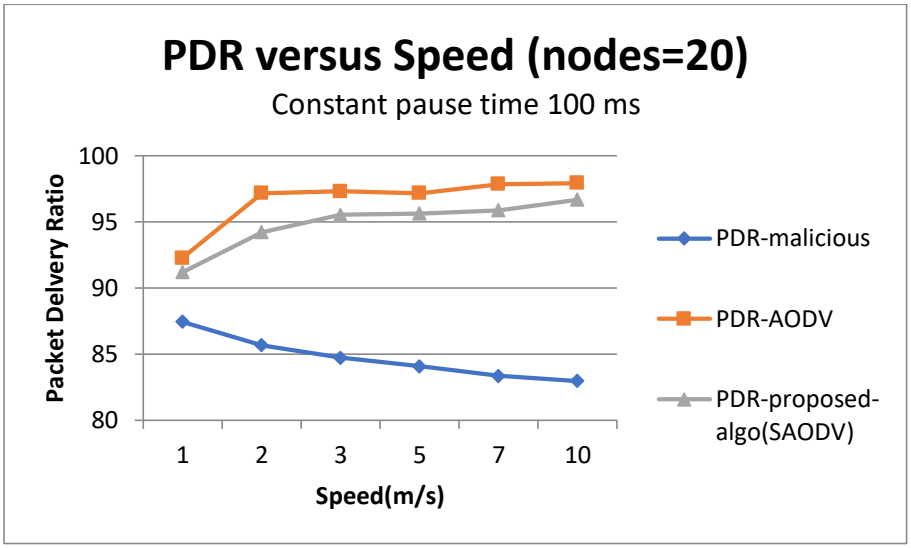


Figure 16: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 16 shows how PDR as a parameter is affected with node's speed as a function. During normal AODV routing execution it is seen that PDR increases as the speed of node increases. Itshows that PDR is increasing from 92% to 98% as the speed of node is increasing from 1m/s to 10m/s respectively. During malicious routing execution, it has been seen that PDR decreases with increasing speed of nodes. Then comes into proposed algorithm and third line shows modified scheme of AODV with implementation of algorithm. It shows improvement in packet delivery.

Result: Fig. 16 clearly shows that in normal routing scenario AODV achieved very high packet delivery ratio as compared to proposed algo with the increasing speed of nodes.

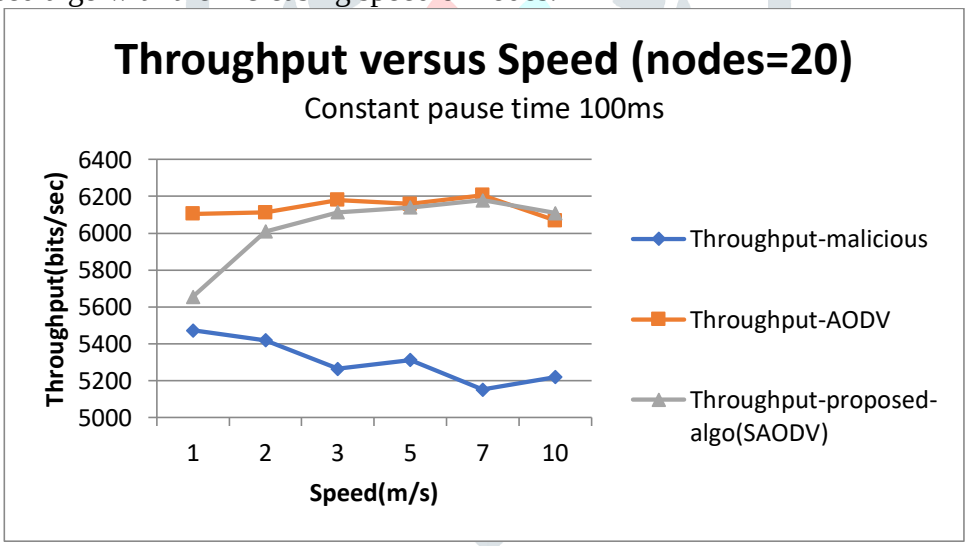


Figure 17: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 17 shows how throughput is affected with speed of node as the other parameter. During normal AODV routing it is seen that when speed of node is 1m/s and 2m/s throughput is 6100 packets which increases to 6180 packets at speed of node 3m/s then 6150 packets when speed of node is 5m/s, 6200 packets when speed of node is 7m/s and finally reaches nearly 6000 packets when speed of node is 10m/s. Clearly there is a uniform throughput achieved in the range of 6000-6200 packets under normal AODV execution. During malicious routing it is seen that when speed of node is 1m/s throughput is 5400 packets which reaches to 5200 packets at speed of node 3m/s then 5300 packets when speed of node is 5m/s and finally reaches nearly 5200 packets when speed of node is 10m/s. Clearly there is a uniform throughput achieved in the range of 5400-5200 packets under malicious execution, as PDR declines and there is loss of packets. Then, here comes into proposed algorithm where high throughput is achieved with the changing speed.

Result: It can be stated that the proposed algorithm is working as per expected behaviour.

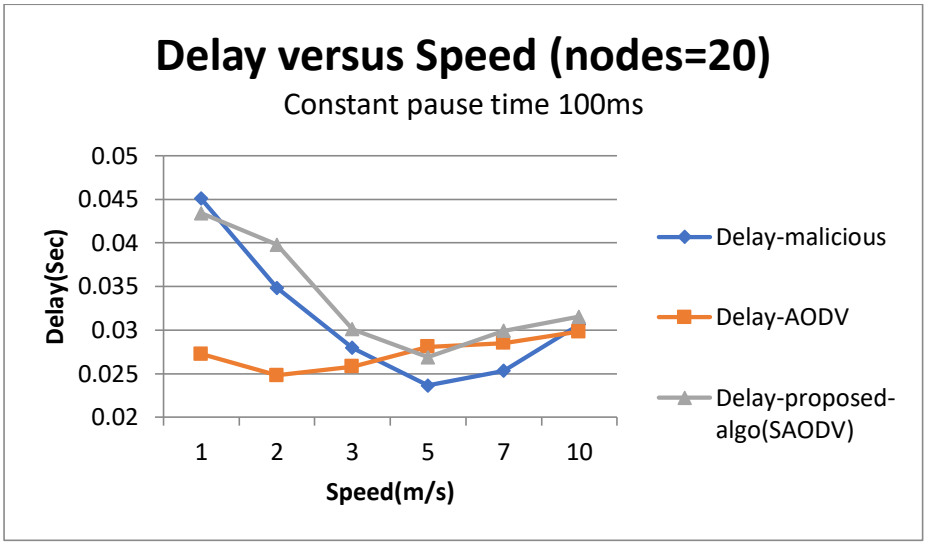


Figure 18: Average variation in Wireless Sensor Network with proposed Algorithm

The Fig. 18 shows the variations in Delay metric with node's speed as a parameter. During normal AODV execution scenario end-to-end delay is having considerable value lying in between .027ms or .03ms which first decreases with increase in speed of nodes and then starts increasing with further increase in speed of node. Clearly, end-to-end delay produced is not uniform in normal AODV routing scenario with speed of node as parameter. The varying values of delay produced are .027ms, .024ms, .025ms, .028ms, .029ms and .029ms approx. when speed of nodes is increasing from 1m/s to 10m/s. During proposed algorithm, the value of end-to-end delay lies in between .043ms - .031ms and decreases with increase in speed of nodes. Hence, delay increases uniformly with increase in speed of node. The proposed modified AODV shows more delays than normal scheme, as more calculations are required to eliminate malicious entry of node and this may cause more delay. It can be accepted easily as it comes with more packet delivery which is more important.

Result: Normal AODV performs better and has less delay value. The proposed algoshows more delays as more calculations are required to eliminate malicious entry of node and this may cause more delay.

Fig.13 to fig. 18 explains AODV is better routing protocol for both the parameters pause-time and speed of nodes in medium size adhoc networks.

V. CONCLUSION AND FUTURE SCOPE

Considering the analysis represented by all the graphs displayed above, AODV results in overall better performance after introducing malicious node and also proposed algo gives better results as per our requirement. Therefore, in the present research work AODV is considered and selected as base protocol for implementation of new algorithm for securing networks against intrusion. The above data analysis showsthe results of ad-hoc networks for sparse and medium size and experiment continues for dense networks too by considering 50 nodes. The three simulation scenarios from sparse adhoc networks to dense adhoc networks are able to represent all possible formations of MANETs that may occur in real time or actual applications of moving devices connected using adhoc networks.

5.1 FUTURE SCOPE

Network architecture is dynamically created by the cooperation of mobile and self-organizing nodes in a Mobile Ad-Hoc Network (MANET). Because of its limitations and environmental sensitivity, the wireless links are particularly susceptible to failure and the network architecture is subject to frequent shifts. In this manuscript the comparison between three protocol distributions as a) normal AODV (without any modifications), b) with intrusion of malicious nodes into the scenario thus AODV becomes malicious AODV, in this case unwanted node act as malicious or intruder) causing loss of data, and third case is modified AODV with proposed scheme. The proposed algorithm behaves equivalent to original AODV with addition to intrusion handling functionality. The performance of this protocol has been evaluated with respect to AODV using three performance metrics viz. packet delivery ratio, end-to-end delay and network throughput. AODV is vulnerable to various kinds of attacks as it is based on the assumption that all nodes must cooperate and without their cooperation no route can be established. In addition, when the malicious nodes enter into the network, various metrics show deterioration for AODV. The purpose of this research is to develop a new secure algorithm which can handle intrusion without any packet loss. More efforts can be made to increase the number of mobile of nodes and to introduce more malicious

nodes to check unwanted intrusions in the network scenario so that its impact on the network performance may be determined and improved. The research scholars can search new ways and implement new algorithms to decrease the overheads of pause time and processing time to bypass the malicious activities and improve security additional parameters like biometric credentials, passwords, IP addresses can be used apart from other important factors.

REFERENCES

[1] Akkaya, K., & Younis, M. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, *3*(3), 325–349. https://doi.org/10.1016/j.adhoc.2003.09.010

[2] Hadi, T. H., (2017). MANET and WSN: WHAT MAKES THEM DIFFERENT? *IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC)*, *7*(6), 23-28.

[3] Bala, R., and Singh, Y.(2015)."Secure Routing in Wireless Sensor Network", *International Journal of Computer Science and Mobile Computing*, 4(5), 966-973.

[4] Kumar R, Kumar R "Review Paper on Wireless Sensor Network" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181,4(32),2016.

[5] Wang, J., Gao, Y., Liu, W., Sangaiah, A. K., & Kim, H. J. (2019). Energy Efficient Routing Algorithm with Mobile Sink Support for Wireless Sensor Networks. *Sensors*, *19*(7), 1494. https://doi.org/10.3390/s19071494

[6] Yadav, A. K., & Kush, A. (2018). TCP-and UDP-based performance evaluation of AODV and DSR routing protocol on varying speed and pause time in mobile ad hoc networks. In *Next-Generation Networks* (pp. 323-332). Springer, Singapore.

[7] Zhang, F., & Yang, G. (2020). A Stable Backup Routing Protocol for Wireless Ad Hoc Networks. *Sensors*, *20*(23), 6743. https://doi.org/10.3390/s20236743

[8] Yu, J. Kaiser, "A Survey of Mobile Ad Hoc network Routing Protocols", International Journal of Information Technology and Knowledge Management, Vol. 6, 2007.

[9] Vikas Goyal, Shaveta Rani, Paramjit Singh, "Performance Comparison of Routing Protocols for Remote Login in MANETs" International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 7, 413-421,2013.

[10] Chen, L., Thombre, S., Jarvinen, K., Lohan, E. S., Alen-Savikko, A., Leppakoski, H., Bhuiyan, M. Z. H., Bu-Pasha, S., Ferrara, G. N., Honkala, S., Lindqvist, J., Ruotsalainen, L., Korpisaari, P., &Kuusniemi, H. (2017). Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. *IEEE Access*, *5*, 8956–8977. https://doi.org/10.1109/access.2017.2695525

[11] G. Subhrananda, J. Subhankar, D. B. Chandan, K. Samarajit, P. K. Dibyendu (2017). Performance Analysis of three routing protocols in MANET using the NS-2 and ANOVA test with varying speed of nodes, EBOOK (PDF) ISBN978-953-51-4841-8, DOI: 10.5772/66521.

[12] Suchita Baxla, Rajesh Nema (2013). A Review Paper on Performance Analysis of AODV, OLSR, DSR and GRP Routing Protocols of Ad Hoc Networks. International Journal of Science and Research (IJSR), 2(5).

[13] H. Al-Bahadili, (2012). Simulation in Computer Network Design and Modeling: Use and Analysis: IGI Global, 2012.

[14] S. Mohapatra, P.Kanungob , "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator" International Conference on Communication Technology and System Design 2011,www.sciencedirect.com, Procedia Engineering 30 (2012) 69 – 76.

[15] Tuteja A, Gujral A, Thalia A, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", IEEE Comp. Society, 2010, pp. 330-333.

[16] A. Akshai, G. Savitha, C. Nirbhay "Performance analysis of AODV, DSDV AND DSR IN MANETS" International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, Issue 6, February 2014, 167-177.

[17] Hao, B., Chang, D., Zhang, Z., & Ji, H., 2019. Performance Analysis of Routing for Wireless Sensor Network. In *3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019)* (pp. 328-334). Atlantis Press.

[18] Dwivedi, R., K., Sharma, P., and Kumar, R. (2018). Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network. *IEEE*, 978-1-5386-1719-9/18/$31.00, 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence),727-732.

[19] Feradus, J., and Salihi, R., (2015). Routing: Internet Routing Protocols and Algorithms. http://dx.doi.org/10.13140/RG.2.1.4341.1680, Asian University for Women.

[20] Govindasamy, J., &Punniakody, S. (2018). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. *Journal of Electrical Systems and Information Technology*, *5*(3), 735–744. https://doi.org/10.1016/j.jesit.2017.02.002

[21] Kaur, H., & Singh, J. (2017). Analysis of Hybrid Routing Protocols ZRP, HCR and ANTHOCNET: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, *7*(6), 642–647. https://doi.org/10.23956/ijarcsse/v7i6/0289

[22] Singh, R., Kathuria, K., & Sagar, A. K. (2018). Secure Routing Protocols for Wireless Sensor Networks. *In prec.* 4th International Conference on Computing Communication and Automation (ICCCA). https://doi.org/10.1109/ccaa.2018.8777557

[23] Sureshkumar, A., Ellappan, V., &Manivel, K. (2017). A comparison analysis of DSDV and AODV routing protocols in mobile AD HOC networks. *In prec*, Conference on Emerging Devices and Smart Systems (ICEDSS), 234-237.

[24] Singh, N., Kumar, M., Verma, A. (2017). Automatic Gain-Controlled HOA with Residual Pumping. Journal of Optical Communication, 41(3), 215-221.

[25] Singh, N., Kumar, M., verma, A. (2019). Analysis of Four Wave Mixing In Ultra Dense WDM-Hybrid Optical Amplifier Systems. Journal of Optical Communication. 43(3), 303-309.