COMPARATIVE ANALYSIS OF AODV ROUTING PROTOCOL VS. NODES IN MANET

Ayasha Malik[1], Siddharth Gautam[2]
Student, Assistant Professor
Department of Computer Science & Engineering
Ambedkar Institute of Advanced Communication Technologies and Research, New Delhi, India

Abstract: Mobile Ad-hoc network system (MANET) is a self-ruling, self-organising, self-configured, peer-to-peer positioning of multitalented hubs/nodes analogous by faraway tie-ups. Each and every node/hub acts as termination subs-structure and switch too, to broadcast data packets. The mobility and flexibility of hubs/nodes are authorized to move and organise themselves dynamically to form a network/system. The topology of MANET is change time to time as per need. This feature causes the network unguarded to differing class of attacks. Thus, finding acceptable solutions for prevention of routing protocols is daring job for researcher. Routing protocols plays a remarkable job for magnifying Quality of Service (QoS) in MANET. Countless protocols are proposed by many researchers for this kind of network. Ad-hoc On Demand Distance Vector (AODV) routing protocol being one among them. Routing overhead is minimum in AODV as compared to other protocol, that's why it is always on top choice of user for providing efficient routing in MANET. In this paper, we analysed the performance of AODV based on some performance metrics, which are average end-to-end (E2E) delay, router drop, packet delivery ratio (PDR) etc. The simulation is done via NS2.

Keywords: Initial node, Goal node, Ad-hoc On Demand Distance Vector (AODV), DSN, RREQ, RREP/RRES, Mobile Ad-hoc Network (MANET), NS-2(Network Simulation Tool version 2), Routing Protocol.

INTRODUCTION

Wireless medium is playing a vital role to provide communication to real world by allowing user to take information and service electronically or digitally, spite their topographical site. Wireless connection/communication provide by two types: Infrastructure based (contains Access point) and Infrastructure less (without access point). MANET is infrastructure less network. [1] Wireless network are widely becoming popular and has enabled communication between mobile devices using standard network routing protocols. [2]

I. Mobile Ad-hoc network:-

Mobile Ad-hoc network does not require any licensed frequency band to act and it is free from any investment in infrastructure as it can able to form structure dynamically. These properties play a vital role to make them attractive for selected commercial applications. [3] The applications area of MANET is disaster consolation, hospitality, emergency actions, military purpose, vehicle networks, sensors, IoT, conferences, etc. But, the nodes of MANET have to suffer with resources such as storage, energy and power. Due to mobility, absence of centralized monitoring, limited power supply, scalability, protection less channels, it becomes difficult to provide security (including secure routing) in MANET. [4][5] Secure routing, service location issues and security; all the three are required to provide efficient employment of MANET. [6][7] Secure routing can be achieved by applying secure routing protocol i.e. AODV routing protocol.

II. Routing protocols:-

A routing protocol used to make a tie-up between to nodes and interchange data packets in MANET including proper and secure route organisation, concludes the final step to forward the data, decide or create rules for maintenance of route and healing from routing failure. [8] The main concept behind classification of routing protocol is determination of route i.e. when and how route is found, mainly it has three types; such as:-

II.A Proactive/Link-state Routing Protocols: - The link-state routing algorithm is used by the proactive routing protocol to found the path or make connection between nodes. In link-state algorithm, link information of adjacent node spread speedily over the network. This protocol amassed the path and preserves them too; the paths remain up to date with the help of control packet (RREQ, RREP and HELLO) from their adjacent nodes. The protocols which follow the whole scenario and lies under proactive/link-state routing protocols are DSDV, OLSR, TRRPF and WRP etc. [9] [11].

II.B Reactive/Distance-vector Routing Protocols: - In this protocol, the overhead is diminished. Distance-vector routing approach is used to make connection between nodes that's why it is called Distance-vector routing protocol, But only when the node requesting for doing so. The protocols which falls in reactive routing protocol are [10] DSR, AODV, TORA and LMR etc. [11]

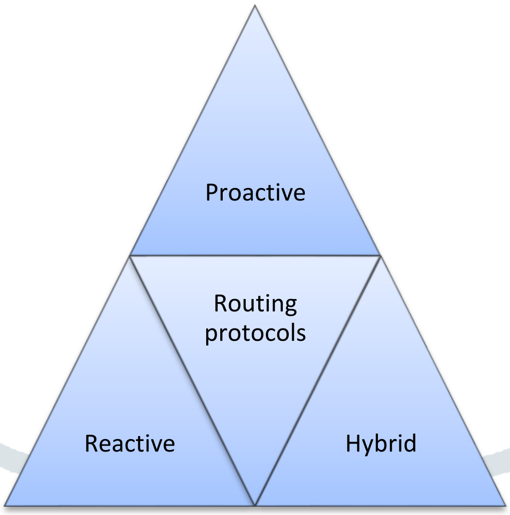


Fig-1 Types of Routing protocols

Table-1 Classification of routing protocols

Routing Protocol	**Classification**		**Example**
Routing Protocol	Position Based		ALARM, DREAM, LEKR, DRM
	Topology Based	Proactive	DSDV, OLSR, CGSR, WRP, TRRPF
		Reactive	AODV, TORA, LMR, DSR, LQSR
		Hybrid	ZRP, BGP, EIGRP

II.C Hybrid Routing Protocols: - This kind of protocols are said to be proactive routing protocol as well as reactive routing protocol. That is... Hybrid routing protocol is the addition of link-state and distance-vector routing protocols. These are some protocols that come under the Hybrid routing protocol ZRP, BGP, EIGRP etc. [11] Table 2 show the how these three protocols (discussed above) are different to each other. [11]

Table-2 Difference between all kinds of routing protocols

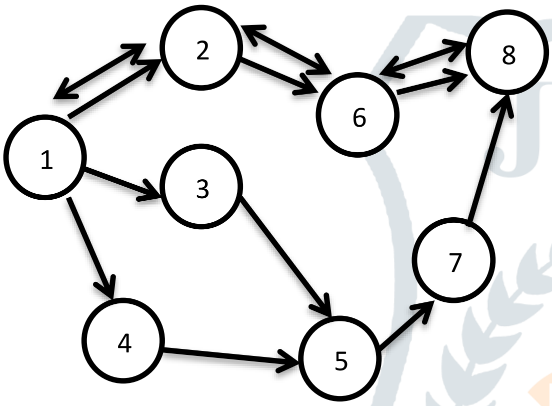
FEATURES	PROACTIVE	REACTIVE	HYBRID
Latency	Low due to routing table	High due to flooding	Inside low outside high
Scalability	Low	Not acceptable for sizable (big) networks	For sizable networks
Mobility	Periodic updates	Route maintenance	Combination of both
Need of power	High	Low	Medium
Need of storage	High	Low	Medium
Need of bandwidth	High	Low	Medium
Updation	Yes, when topology changes	Not needed	Yes
Routing intrusion	Always accessible	Available when needed	Fusion of both
Routing overhead	High	Low	Medium
Route acquisition	Table	On demand	Combination of both
Routing structure	Both	Mostly flat	Hierarchal
Control traffic	High	Low	Lower than other two
Benefit	Rapid establishment of route and routing information is updated rapidly	Obtain required route when needed, not exchange routing table periodically & loop free.	Limited search Cost, update routing information & scalable
Limitations	Convergence count is low, more amount of resource	Routes are not fresh, more end-to-end delay, packet	Needed extra resources for Big sized zones

	used, flooding of routing information in whole network	dropping is in high amount	
Routing scheme	Table-driven	On-demand	both

III. AODV: - AODV is an on-demand routing protocol. As the name indicate, it tie-up to find route when demand by someone/initial node. Sequence numbers is used by AODV to take guarantee of genuinity of path and to obtained fresh path. [12] AODV is qualified to provide single hop and multi hop routing. Established route/path is conserve until the communication finished by the nodes (initial node, intermedial nodes, goal node). Main blessings of AODV are provide loop free communication and scalable for large number of nodes. [2]

III.A. Route discovery

AODV broadcast RREQ to all its intermedial nodes, which hold addresses of initial node and goal node, their SN (SSN and DSN), broadcast ID and a counter. When source/initial nodes transmit a RREQ to its intermedial nodes it receive RREP/RRES either from its adjacent node or that adjacent node(s) retransmit RREQ to their adjacent node after making an addition in hop counter. If initial node inherits numerous RREQ from identical transmit ID, then that RREQ dropped to maintain a loop free tie-up [15]



Representation table

Node 1	*Source node*
Node 8	*Destination node*
Nodes 2,3,4,5,6,7	*Intermedial nodes*
⟶	*RREQ*
⟷	*RREP*

Fig-2 Broadcasting RREQ

III.B. *Route Table Management*

We have to maintain/manage Routing in AODV, for this whenever a connection established; first, unwanted entries (that do not exist) from table has to be removed. It is done via DSN (Destination Sequence Number) [15]

III.C. AODV Route Maintenance

When network founds that a stored path is not workable anymore for communication then that path is deleted. And broadcast RREP/RRES to current active adjacent nodes and ask them to do the same. Only loop free path is maintained by AODV [15]

III.D. Routing Table Fields

- Goal IP address
- DSN
- Genuine DSN Flag
- State and routing flags
- Network Interface
- Hop Count (needed to reach destination)
- Adjacent Hop
- Forerunner record
- Lifespan (route expiration or deletion time)[13][14]

III.E. Control packet

- RREQ – Route request
- RREP – Route reply
- RERR – Route error
- HELLO – For link status monitoring[13][14]

SIMULATIONS AND RESULTS ANALYSIS

In this segment, we explore configuration of tool which used in this project, after that performance evaluation metrics, and last simulation results with analysis.

A. Experimental Configuration

We used NS-2.35 network simulator tool to examine the AODV routing protocol on the basis of nodes. This simulator is for discrete event invented at UC Berkeley. Over wired and wireless network; simulation of TCP, analysing of network, routing and multicast protocols etc is done by NS2 tool. These are the languages which is used to write code in NS2; C, C++, extension of TCL for OOPS, OTCL. [17] NS2 consist two simulation tools NS and NAM. Network simulator (NS) hold all frequently used IP protocols and network animator (NAM) for visualisation.

Table-3 Simulation setup

Parameter	**Value**
Channel type	Wireless channel
Radio propagation model	TwoRayGround
Network interface type	Wirelessphy
MAC type	MAC 802.11
Interface queue type	Queue/DropTail/PriQueue
Link layer type	LL
Antenna model	OmniAntenna
Max packet in ifq	50
Number of mobile nodes	7/17/27/47/57/77
Routing protocol	AODV
Simulation time	150.00s
X & Y dimensions	1800*840 sq.m
Simulation end	150.01s
Traffic type	TCP/UDP/CBR
Size	1024/512/1500
Rate	1.0Mb/2.0Mb/4.0Mb

B. Performance evolution Matrices

The following performance metrics are taken to examine AODV routing protocol vs. nodes i.e. we increase number of nodes (7, 17, 27, 47, 57, 77) while using above parameters (table-3) to analysis of AODV.

1. End-to-end delay: - Total time taken by data packets to hit receiver/destination from sender/source including delay (buffering time, transmission time, re-transmission time, waiting time, propagation time).

$$\text{Delay} = \text{End time} - \text{Start time}$$

2. Packet delivery ratio (PDR): - Total amount of data packets that received by goal/destination wealthy. It is the ratio between received packets to the generated packets.

$$\text{PDR} = (\text{Received packets}/\text{Generated packets})*100$$

3. Payload: - It is the amount of packets send by the protocol.

4. Router drop/Packet loss: - It explained as, the amount of packets that didn't receive by destination/goal wealthily. The main reason behind data drop is collision, hardware tempering, malicious behaviour and queue overflow etc.

5. Throughput: - Total amount of data transferred per unit time, i.e. transferred from node to node through a communication tie-up.

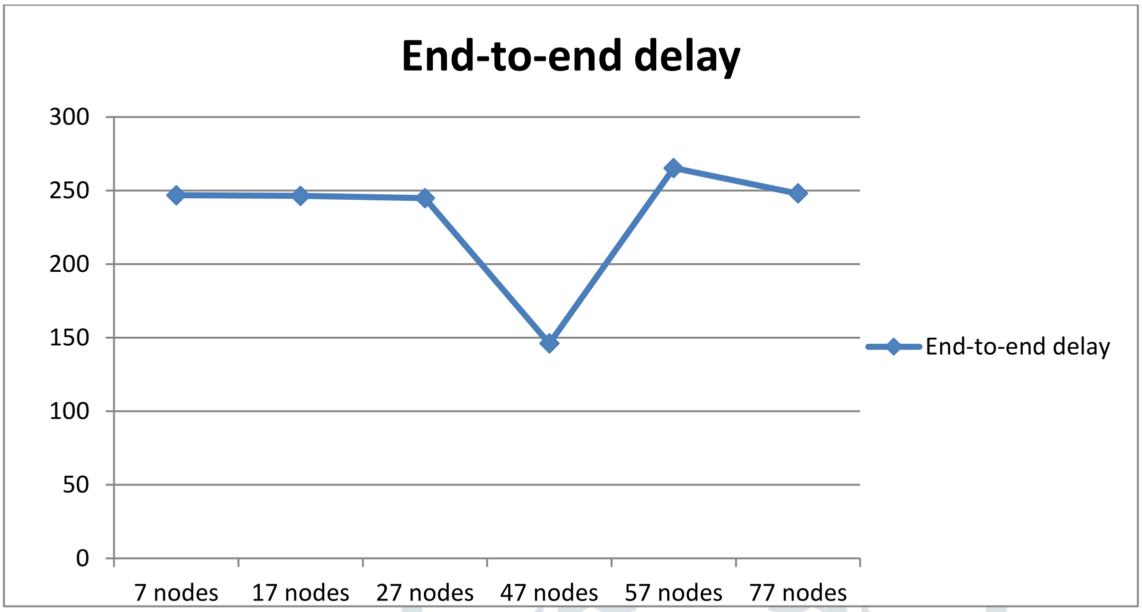
$$\text{Throughput} = (\text{Received data } *8)/\text{data dissemination interval}$$

6. Control packet: - It is the packet which contains the control information.

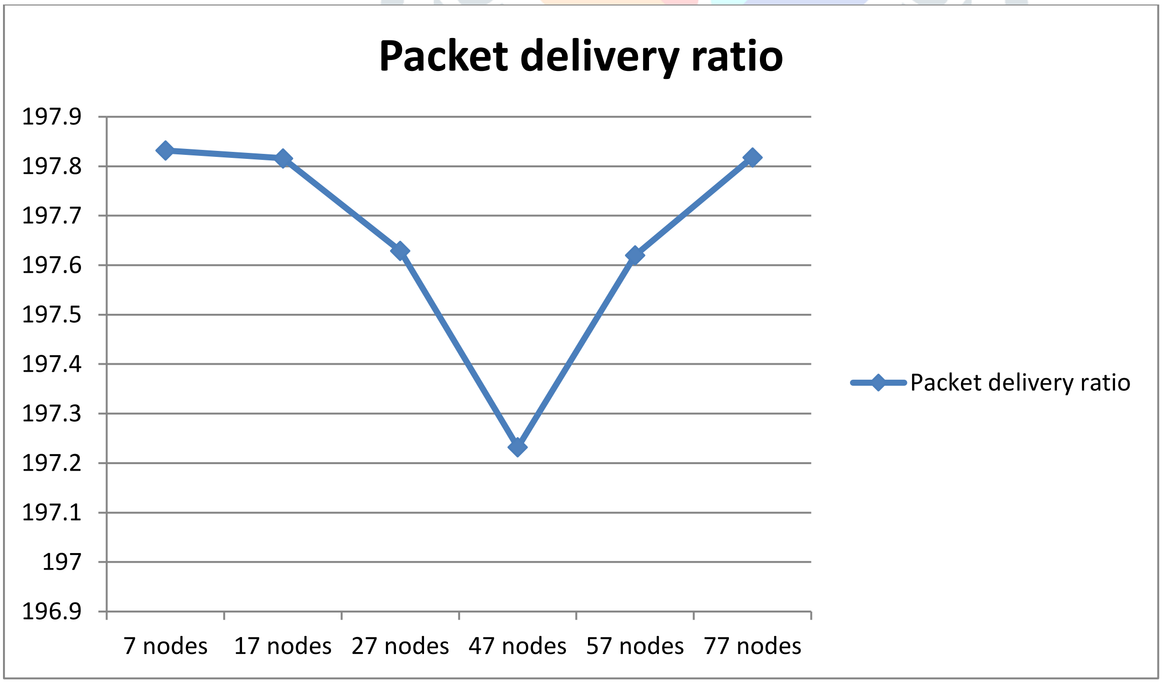
7. Generated&Received packets: - It is the total amount of generated and received data packets during whole simulation.

C. Results (Including snaps)

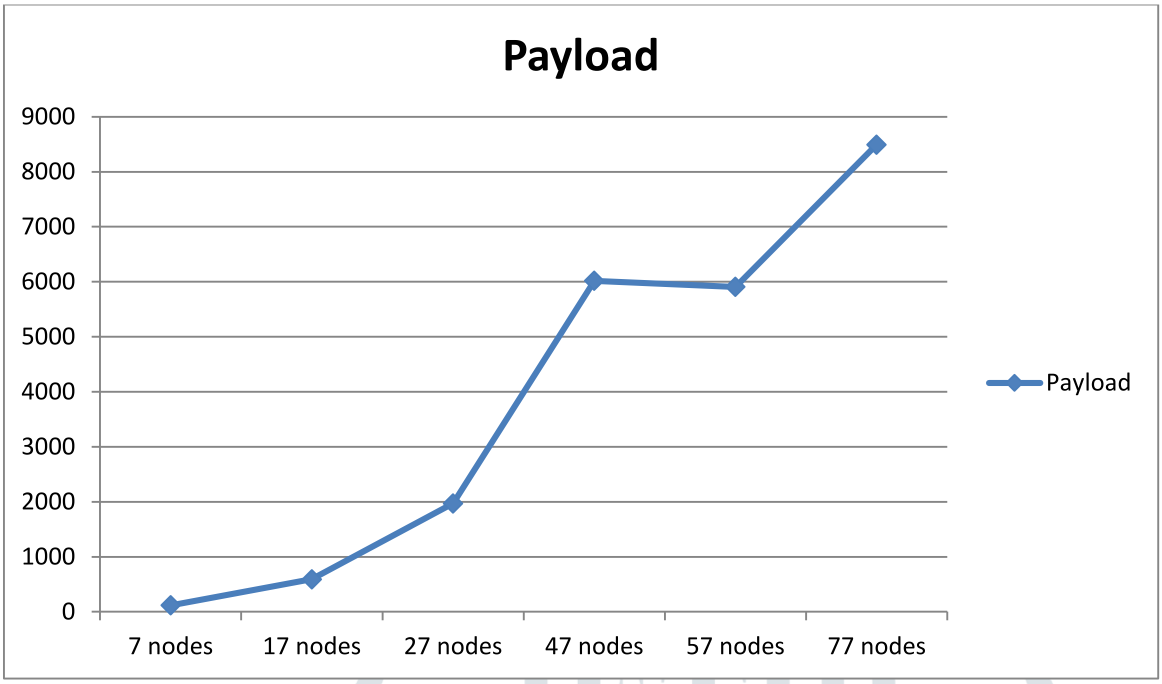
1. End-to-end delay: - to achieve better performance E2E delay should be low. In our project, when we increase number of nodes then end-to-end delay reduces but not constantly, as we can see when numbers of nodes are 57 then graph line increases and then again start to decrease. So we can conclude when we widen the number of nodes in network then end-to-end delay decreases and performances increases.



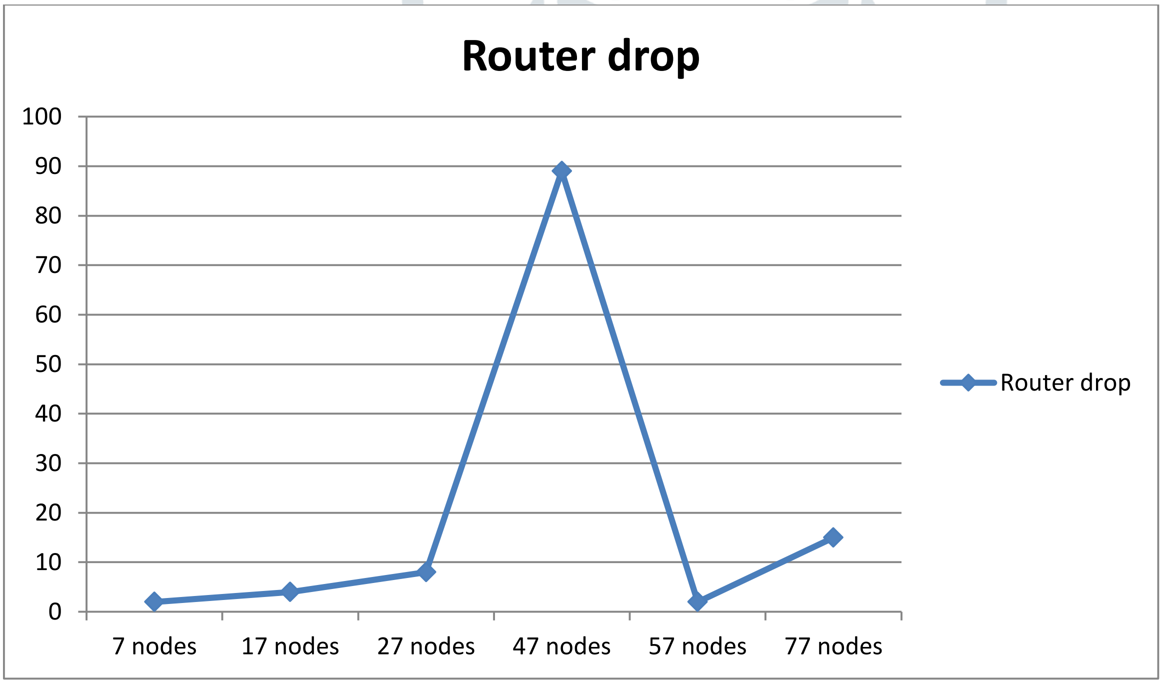
2. Packet delivery ratio: - It should be high. In our project as we can see, when the number of nodes increases then PDR's graph line decreases but again start to increase. So we can conclude that, when we increase the number of nodes then PDR become low but when we use a huge amount of nodes in small area then PDR rate increases.



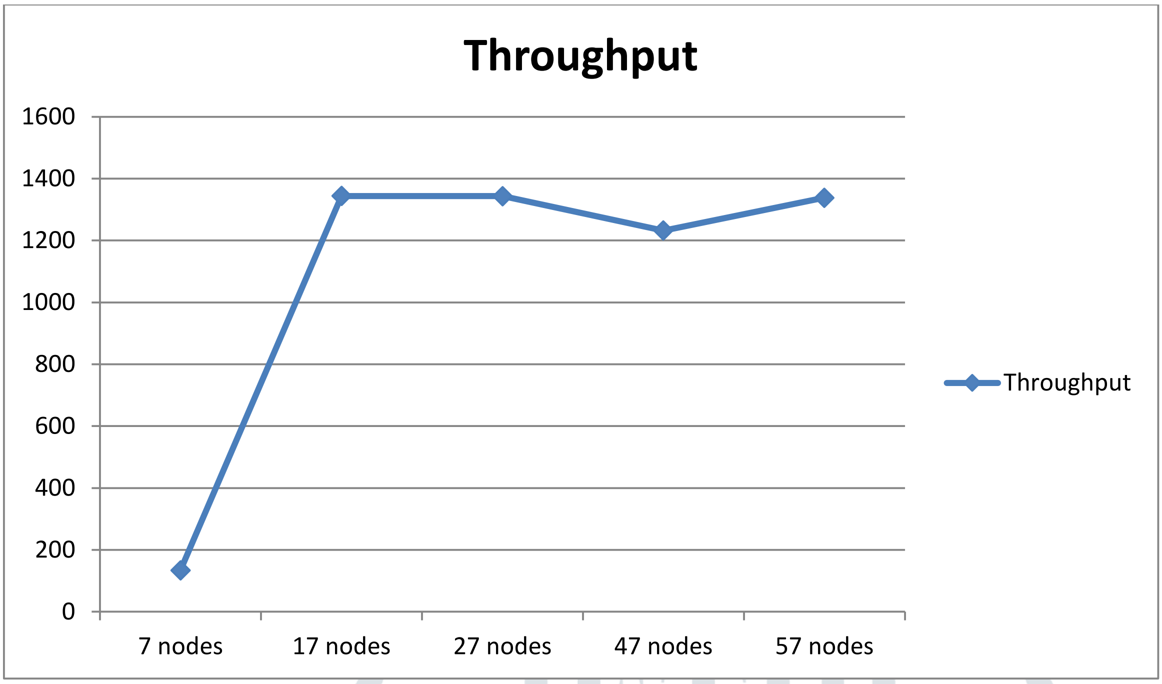
3. Payload: - It should be high excluding fake packets. In our project payload is increases when number of nodes increases. So we can conclude, when number of nodes increases then payload of network also increases.(mostly)



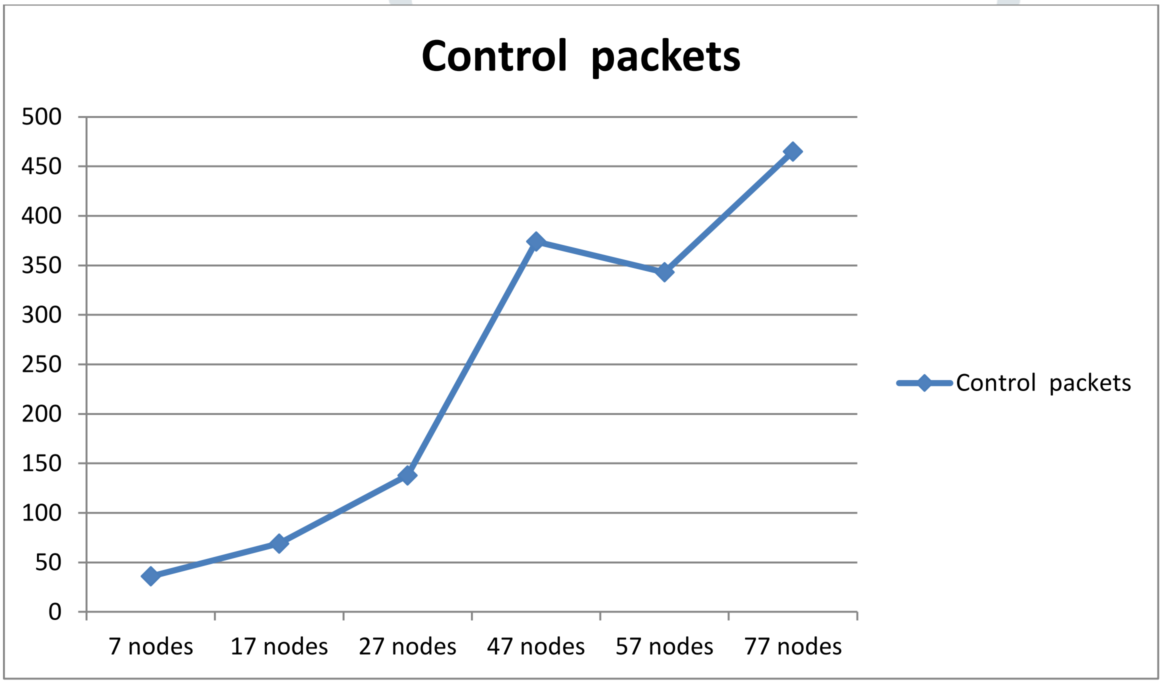
4. Router drop/Packet loss: - It should be low. In our project when we increases nodes then router drop also be increases so we can conclude that when number of nodes widen/increases in network then router drop/packet loss also grow.(but sometime it can be decreases as mobile nature of nodes)



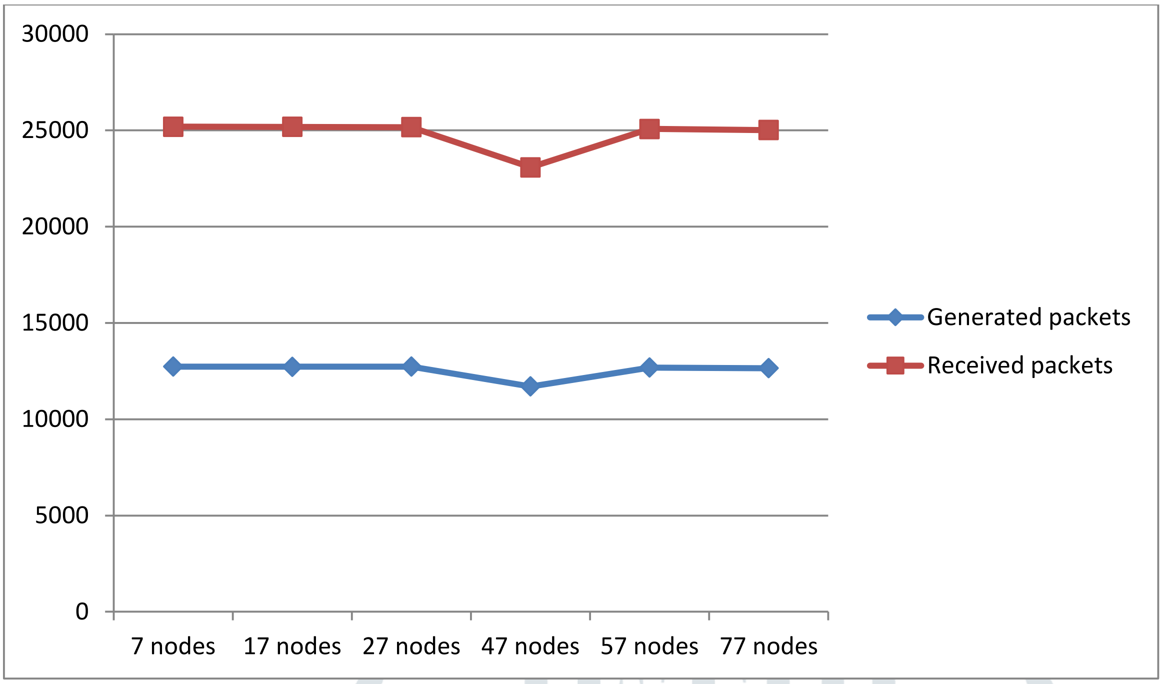
5. Throughput: - It should be high. In our project it is shown that when number of nodes widen then the throughput is also increases. (But sometimes it can also decrease).



6. Control packet: - When the number of nodes increases/expand then control packets also increases (most of the time).



7. Generated&Received packets: - When number of nodes grows then the amount of generated&received packets also grows.



CONCLUSION

In this paper, we have started with wireless network then discussed Ad-hoc network including its blessings, application and limitations. After that, we explain routing protocols, its classifications and differentiate them on the basis of some parameters. Then we elaborated AODV protocol including route discovery process, route table management, route maintenance, routing table fields and control packets. At last simulation of AODV protocol vs. nodes (7, 17, 27, 47, 57, 77) is done and results concluded on the basis of some performance matrices (End-to-end delay, payload, router drop, throughput, packet delivery ratio (PDR), control packets and generated&received packets) using NS2 simulator tool.

REFERENCES

[1] Amandeep and Gurmeet kaur “Performance analysis of aodv routing protocol in manets” Amandeep et al. / International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.08 August 2012.

[2] K. Tamizarasu and M. Rajaram “Analysis of AODV Routing Protocol for Minimized Routing Delay in Ad Hoc Networks” K. Tamizarasu et al. / International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 3 Mar 2011.

[3] Ayasha Malik and Vishal Gupta “Security Attacks on Ad-Hoc Networks: A survey”, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.8, No.4, 2018.

[4] HoudaMoudni, Mohamed Er-rouidi, HichamMouncif and Benachir El Hadadi “Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks” 2nd International Conference on Electrical and Information Technologies ICEIT’2016, 978-1-4673-8469-8/16/$31.00 ©2016 IEEE

[5] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security (pp. 103-135). Springer US.

[6] E.Guttman and C.Perkins et al, “Service Location Protocol version 2”, “Internet Engineering Task Force, RFC2608”, June 1999.

[7] P.Papadimitratos and Z. Haas, “Secure Routing for Mobile Adhoc Networks”, in proceedings of CNDS 2002.

[8] Tajinder Kaur and A. K. Verma, “Simulation and Analysis of AODV routing protocol in VANETs” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[9] BR, A.K., Reddy, L.C. and Hiremath, P.S. Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols. IJCSNS International Journal of Computer Science and Network Security, 8, 337-343, 2008.

[10] H.Ehsan, Z. Uzmi, “Performance comparison of adhoc wireless network routing protocols”, Proceedings of IEEE International Multi-topic Conference (INMIC) 2004.

[11] Sachin Lalar and Arun Kumar Yadav, “Comparative Study of Routing Protocols in MANET” Oriental Journal of Computer Science & Technology, Vol. 10. No. (1): Pgs. 174-179

[12] Madhu and Sarika “ Performance Analysis of AODV Routing Protocol in Mobile Ad hoc Network” , International Journal of Science, Engineering and Technology Research (IJSETR),Volume 4, Issue 6, June 2015.

[13] Rashmi, Ameeta Seehra “Detection and Prevention of Black-Hole Attack in MANETS”, International Journal of Computer Science Trends and Technology (IJCST), 2014.

[14] PPT “Ad hoc On-demand Distance Vector (AODV) Routing Protocol” ECE 695 Spring 2006.

[15] Tajinder Kaur and A. K. Verma "Simulation and Analysis of AODV routing protocol in VANETs" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16] www.computerscijournal.org

[17] NAM Network Animator. http://www.isi.edu/nsnam/nam/