ISSN 2454-8596
www.vidhyayanaejournal.org
An International Multidisciplinary Research e-Journal

Experimental Study of AODV and its Vulnerability Assessments in Ad Hoc Network

Arzoo Khanderia

B. H. Gardi College of Engineering & Technology, Rajkot.

ISSN 2454-8596
www.vidhyayanaejournal.org
An International Multidisciplinary Research e-Journal

Experimental Study of AODV and its Vulnerability Assessments in Ad Hoc Network

Abstract:

MANET due to its open medium enable many application in wireless network.MANET is infrastructure less network in which node communicate directly without acesspoint.As it is in open medium, security comes to an picture. Many researches have been carried out in order to secure MANET. Though it seems gap between the researches, as increase in security decreases the overall performance of network. SAODV protocol is better in terms of security but due to its high packet size and computation time it causes lots of delay, throughput decreases, etc. Thus proposed method gives such a solution in which security can be increased with good network performance. Here, we have tried to decrease the network delay, increase in throughput, high packet delivery ratio to make it more stable.

Keywords: AODV, attacks, Vulnerabilities, Simulation

ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA An International Multidisciplinary Research e-Journal

Introduction

Wireless mobile network are more widely used in day to day with its open medium but main challenge comes is security. It can be said that security involves two major problems which are: 1) Secure Route discovery and 2) Secure data transmission in open medium. But main challenges in terms of MANET are their self-organized structure which can be consider as its strong point as well as weak point. Thus the feature invites much vulnerability in network. Now existing protocols are mainly divided into

1) Table driven: Example is DSDV, CGSR etc.
2) Demand driven: Examples are DSR and AODV etc.

But main problems with these two approaches are they do not have appropriate security mechanism. However, many proposals can be found to add security features to the existing protocol which are aimed either guaranteeing authenticity and integrity or monitoring the behavior of other nodes. But still they fail to manage between security and performance of network. The adhoc on demand distance vector (AODV) algorithm enables dynamic, self-starting, multi hop routing between participating mobile nodes wishing to establish and maintain an adhoc network. AODV is an example of reactive and stateless protocol that establishes routes only as desired by a source node using route request (RREQ) and route reply (RREP) messages. AODV protocol is also susceptible to security threats and any malicious intrusion may compromise its overall performance. Much advancement is done in AODV like SAODV, A-SAODV, I-SAODV etc. But each application is used or we can say that has its own advantages and disvantages. Analysis said that though security increases their performance is decrease considerably.

MOTIVATION

Today many research has been done in MANET, researchers had tried to resolve problems in order to have best performance of network, protocol. But still it seems many gaps in the research work. As we know AODV is protocol is having lack of security but gives better network performance but security is major concern. So its advance version is introduced called SAODV.TAODV, A-SAODV etc. But it causes many problems like packet size, stability of network, time delay, dropping ratio etc. So in proposed work, we tried to have better security along with better performance of network.

ISSN 2454-8596
www.vidhyayanaejournal.org
An International Multidisciplinary Research e-Journal

AD HOC ON DEMAND DISTANCE VECTOR ROUTING

AODV is reactive routing protocol in MANET. The reactive implies that a node exchange routing information only when it need to transfer some data and keep the routing information updated as long as the communication with the node exists. When nodes wants communicate and it does not have valid path then it carries out route discovery process in order to establish route to destination by sending RREQ message to its neighbor. Neighbor who receives the packet will increment the hope counter and forward message ahead.This is termed as flooding. Intermediate node may receive more than one RREQ but will accept the one which arrives first and discard other one. Finally RREQ reaches the destination, it replies back with RREP message using path towards the source node established by RREQ.

RREP message allows intermediate node to know about new route from one node to another. Along with two packets one more packet is used called RRER which is used to notify nodes about breakage of link in network and unreachable nodes. If any intermediate node has fresh route to destination it generate RREP and reply back to source and does not forward it.AODV uses sequence number in order to have freshness of route. Each node maintains it and increment it before forwarding RREQ or RREP to neighbors.

AODV is just used to transfer data which does not contain security mechanism. Thus much advancement is done in AODV to protect it from different attacks.

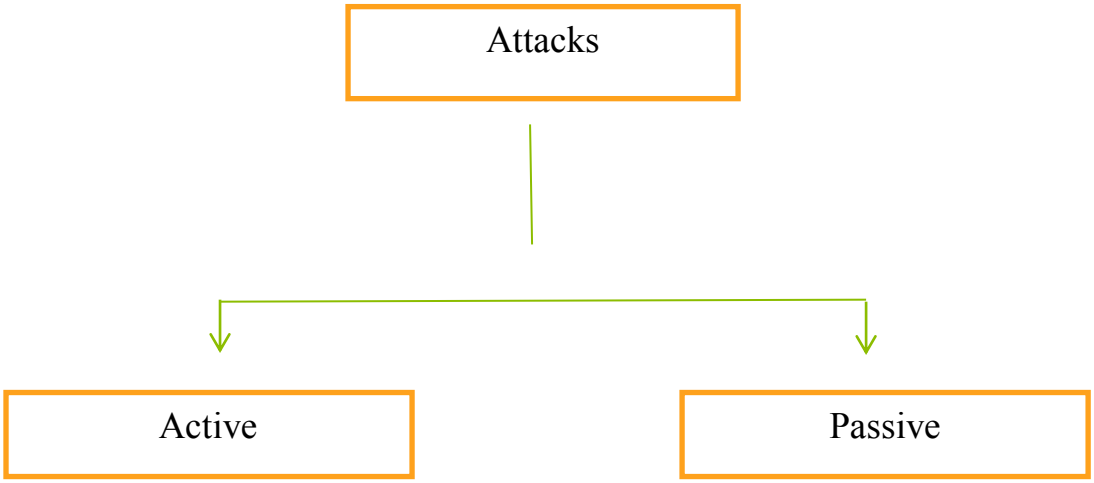
General definition of security

Generally security is said to have network which is out of any kind of danger or threat or we can say that prevention and protection of network against assault, damage, fraud, theft, authorization etc. Security can be implemented through many techniques watchdog, digital signature, hash functions, etc.

Security attacks

Security attacks can be classified on basis of source or we can say that on basis of control they require on network, data, identity etc. it can be classified as active and passive attacks. They are follows [8]:

ISSN 2454-8596
www.vidhyayanaejournal.org
An International Multidisciplinary Research e-Journal



1) **Active attack:** An attacker introduces the false information in network in order to confuse and degrade the performance of network.

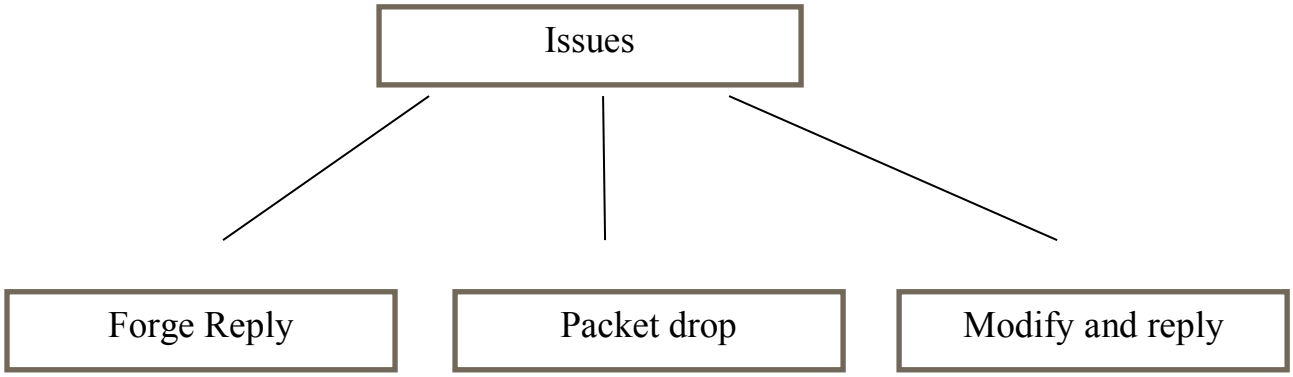
2) **Passive attack:** In this, attacker drops the packet or hides the information from network. In network the attacker does not pass packet to next but instead drop it silently. And as a result packet delivery ration deceases a lot it can even be less than 3%.

Vulnerability in AODV

AODV protocol is designed in such a way that it lacks security in network. It does not give features like confidentiality, integrality, non-repudiation, and as a result it invites malicious node to attack the network in order to have control of network or disrupt the network. Along with other attacks in AODV can be as below with block diagram[1].

AODV also enable attacks like black hole, gray hole, DOS attack. Along with this various other issues like incrementing sequence number, decreasing hop count are also there which shows the fresh route of network and as a result malicious node have all network traffic and finally have control over network and may drop the packet just like selfish attack, black hole attacks etc.

ISSN 2454-8596
www.vidhyayanaejournal.org
An International Multidisciplinary Research e-Journal



1) Forge reply include sending fake the RREQ or RREP packet.

2) Packet drop includes various attacks like black hole attack, gray hole attack, selfish attack in which attract traffic of packet and finally when it enter the network it starts dropping packet instead of forwarding.

3) Modify and reply include that malicious node modify the RREQ and RREP packet in which it increment sequence number or decrement hop count as a result this is categorized in modification attack.

4) Along with this there can other issues with AODV are:

- Attacker can impersonate a source node's IP by forgeing RREQ or RREP with IP address as IP address of source node's IP.
- Modification of routing may lead to inconsistency in network
- Routing table may contain false information about the network topology.

Security requirement of AODV includes [7]:

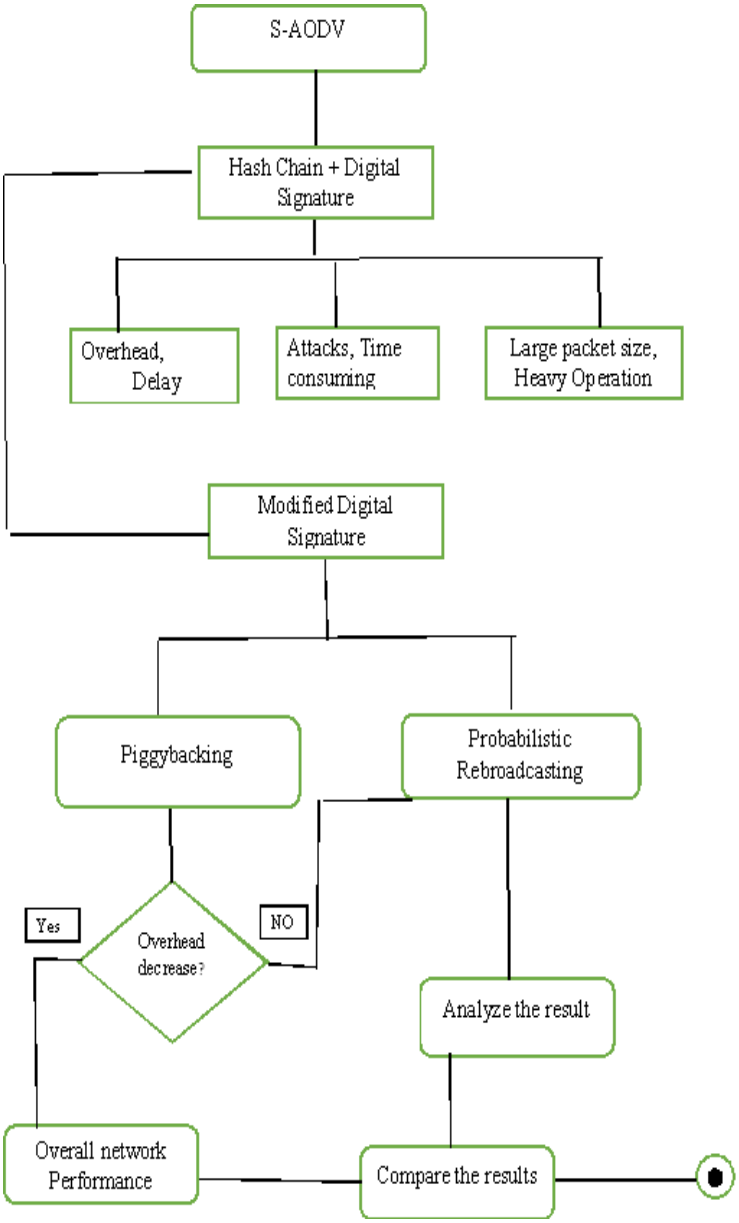
1) Source authentication: Source or Node is one which claims to be.
2) Neighbor authentication: confirmation regarding the identity of sender who claims to be.
3) Message integrity: Message content must be unaltered.
4) Message confidentially: Message content must be authenticated to sender and receiver.
5) Access control: must have access rights.

Proposed Mathematical Model

SAODV(Secure AODV) adds more features of integrity, confidentiality, non-repudiation etc. which uses digital signature and hash function in order to secure network but research says that there seems a gap between this. Though it causes network degradation like more delay, less throughput due to large packet size, take more computation time, SAODV has higher over load due to asymmetric cryptography, as it needs considerable processing time to verify signatures and hashes at each node. Along with this, it is good in terms of fewer path but must obey trust requirement of sender but simultaneously it may follow long path if does not fulfill requirement.

Here is new proposed solution in order to have better security and enhancing the network performance.

ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA
An International Multidisciplinary Research e-Journal



Simulation of AODV

ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA An International Multidisciplinary Research e-Journal

Here shows the implementation phase of AODV routing protocol. The simulation parameter used in experiment is as follow:

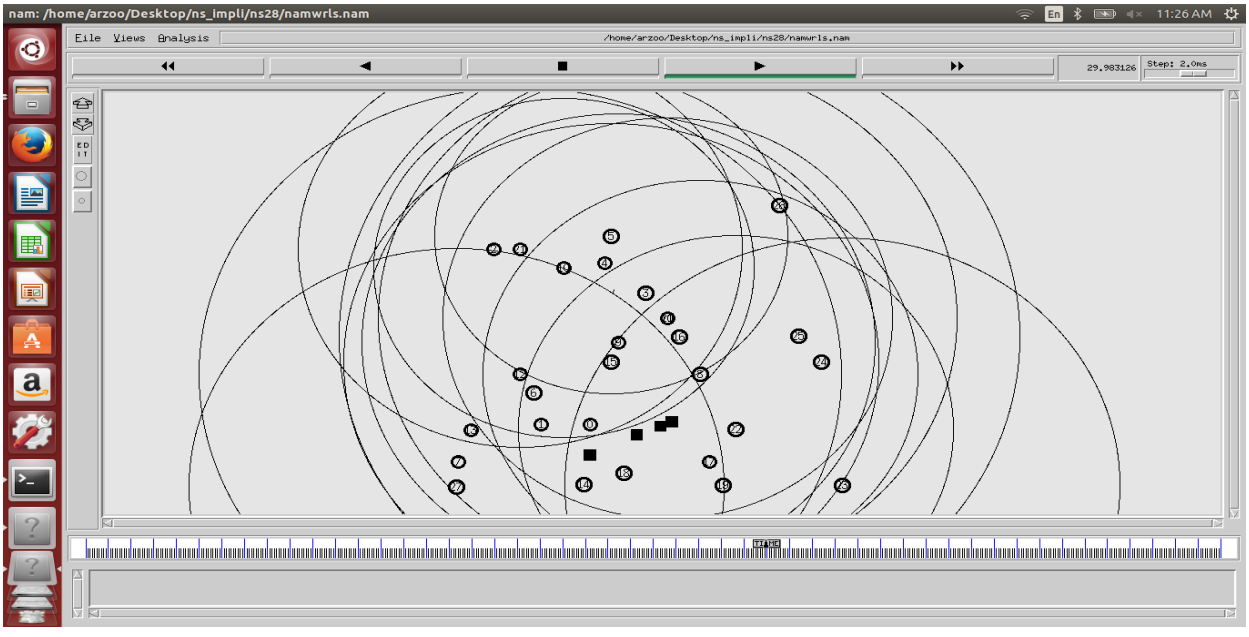
Parameter	**Value**
Operating system	Ubuntu
Simulator	NS-2(2.35)
Number of nodes	Varies from 5 to 100
Simulation area	1000*1000 m
Packet size	512 bytes
Protocol	AODV

Here focus is only on throughput and packet deliver ratio and to increase them for better scalability.

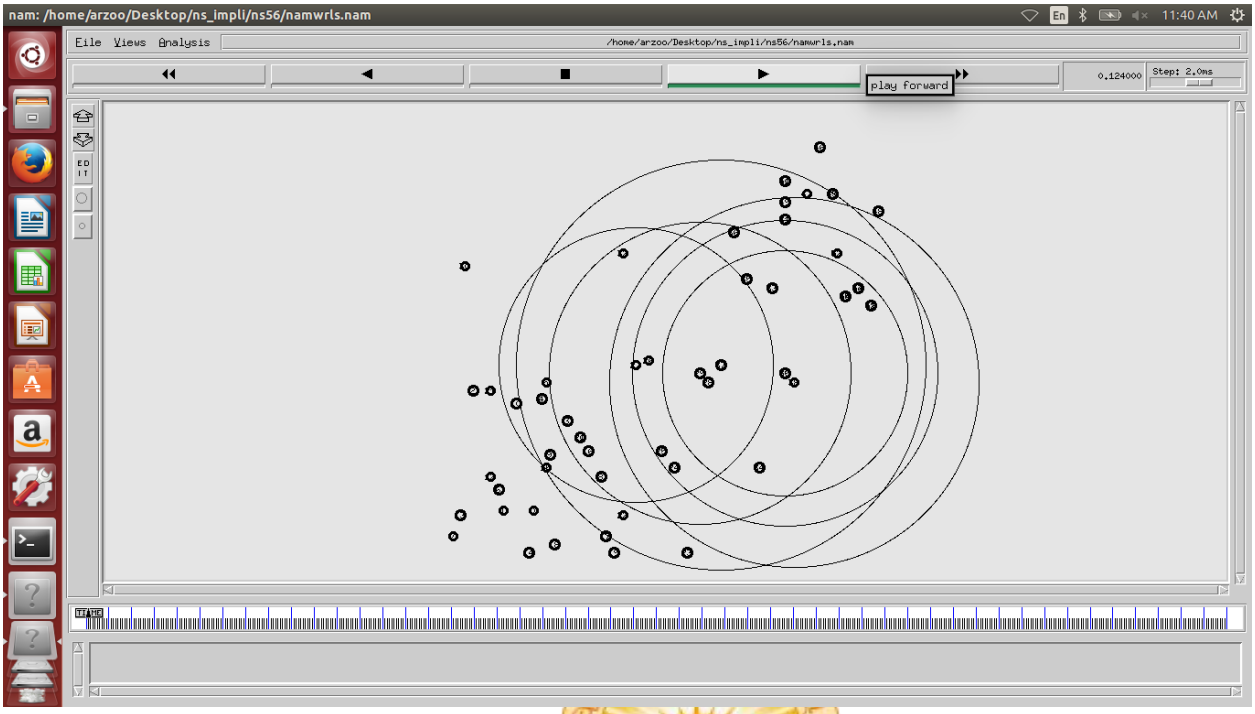
Throughput: The amount of data transferred over the period of time expressed in kilobits per second [9, 3].

Packet Deliver Ratio:The ratio of total number of data packets successfully received by all the destinations to the total number of data packets generated by all the sources [9, 3].

Below shows the Implementation scenario of AODV protocol

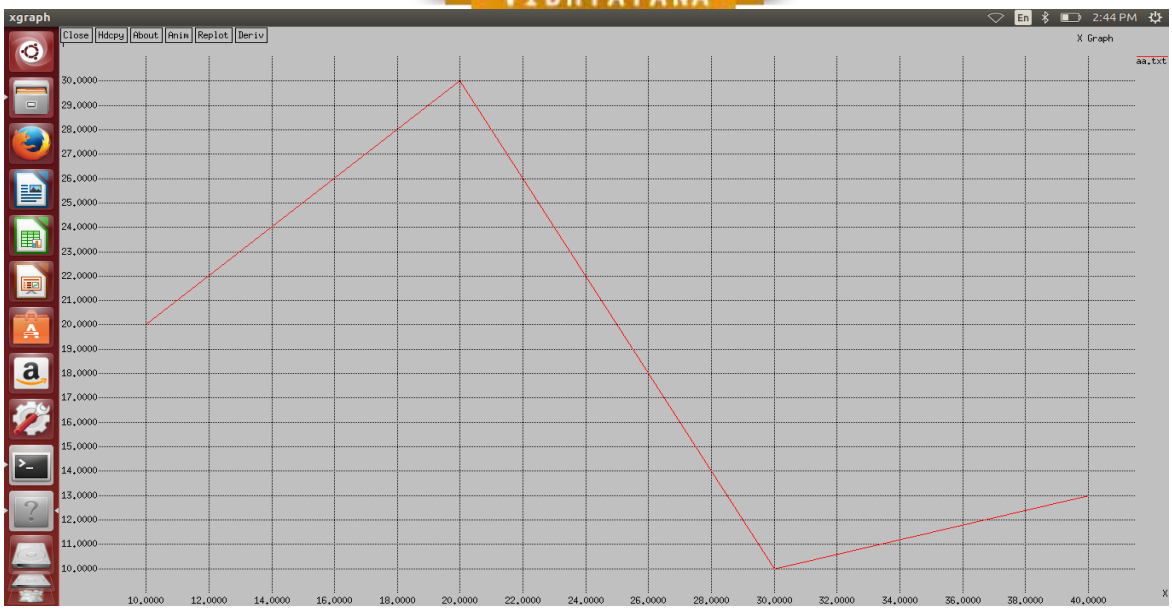


ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA
An International Multidisciplinary Research e-Journal



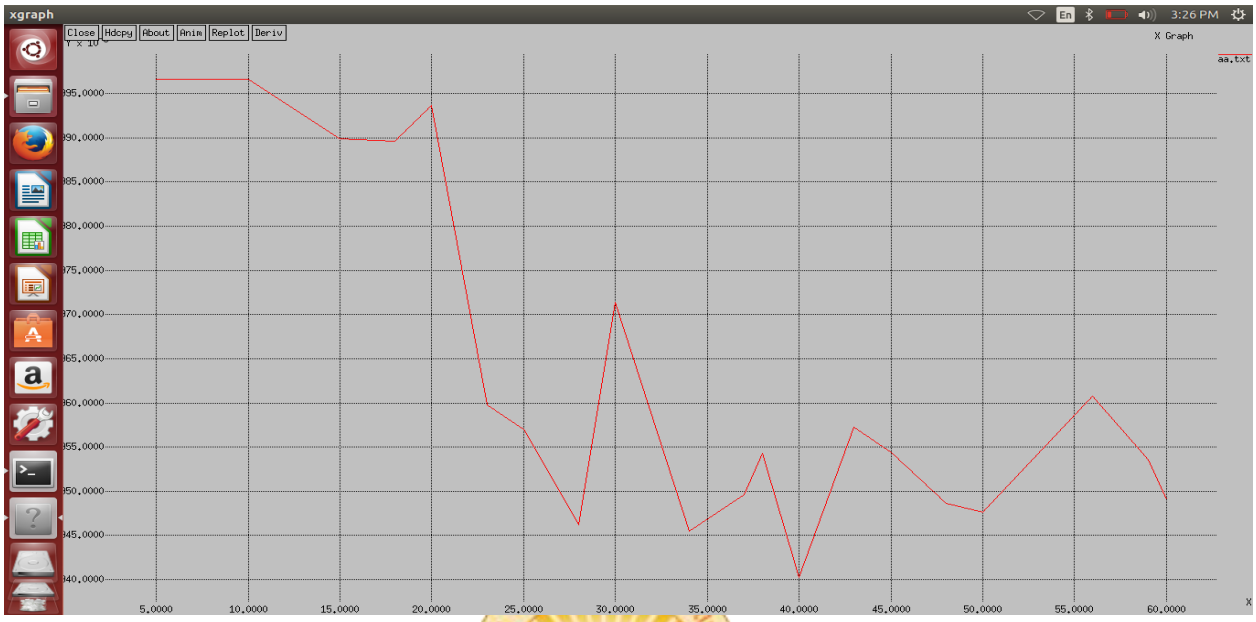
Scalability in nodes impacts on performance which can be shows as below:

1) Throughput when there are 40 nodes.



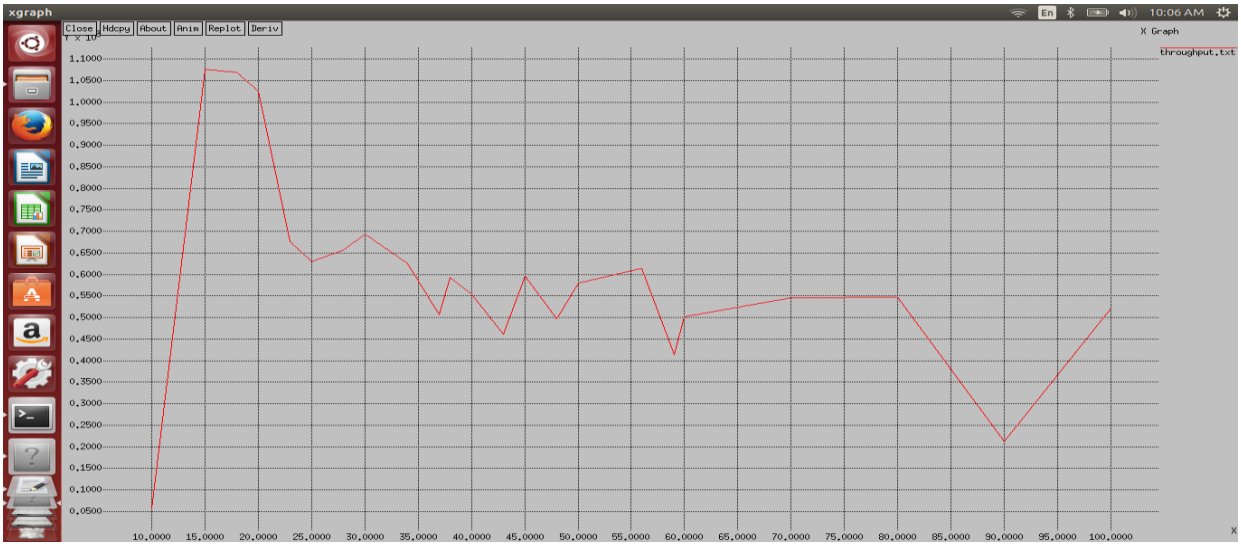
ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA An International Multidisciplinary Research e-Journal

2) Throughput when number of nodes changes from 40 to 60.



Thus from above it can be concluded that as number of nodes (scalability) increases there is impact on performance as well.

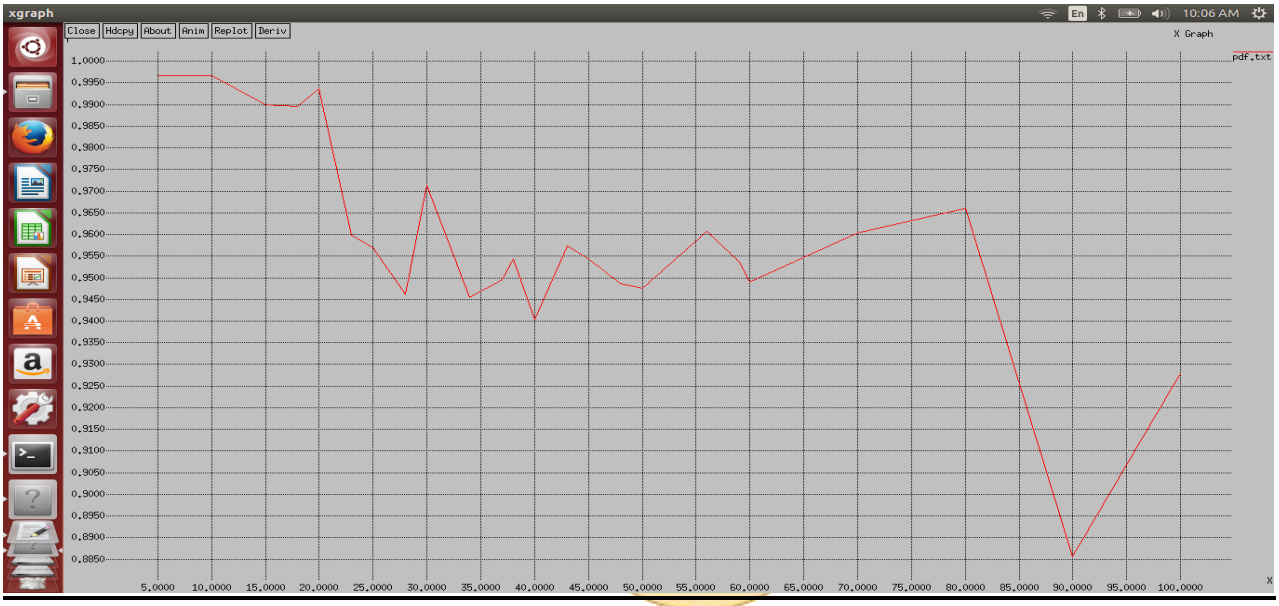
Throughput vs. Nodes



ISSN 2454-8596
www.vidhyayanaejournal.org
VIDHYAYANA An International Multidisciplinary Research e-Journal

As seen from the graph the value of throughput is decreasing as we move from lower nodes to higher nodes i.e. from node number 10 to node 100. X axis shows number of nodes and y axis shows values of throughput as number of nodes increases.

Packet delivery ratio vs. Nodes



Similarly as shown in figure we can figure it out that same as throughput packet delivery ration drastically decreases as number of nodes increases.

Conclusion

From the above study, it can be concluded that AODV seems to show less performance when number of nodes increases. Along with it security feature is also not present in order to avoid attacks. Hence enhancement is needed in security and performance aspects as well. Thus SAODV is implemented but due to larger packet size and computation time it also suffers from performance issue though security can be better than AODV. So advance features must be added in future to increase both security and performance.

References

[1] Anurag Gupta, Kamlesh Rana "Assessment of Various Attacks on Aodv in Malicious Environment" 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015

[2] Mahamed Abdelshalfy and Peter King "Analysis of Security Attacks on AODV Routing" IEEE 2013

[3] Ashok Kanthe and et al.," Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks" 2012

[4] F. Mann and et al., "Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network Routing Attacks and Performance Comparisons" 2011Wireless Advance

[5] M.F. juwad and et al." OPNET Performance Comparisons between SAODV&AODV"2007

[6]Sandhya Khurana and et al, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol" Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies 2006

[7]Asar Amir Pirzada and et al.," Secure Routing with the AODV Protocol" 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.

[8]Weichao wang and et al., "On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol" IEEE 2003

[9] M.F juwad and et al.,"Experimental Performance Comparisons between SAODV & AODV" Second Asia International Conference on Modeling& Simulation, IEEE 2008

[10] Asish bhagwari and et al., "Performance of AODV Routing Protocol with increasing the MANET Node and it's effects on QoS of Mobile Ad hoc Networks" 2012 International Conference on Communication Systems and Network Technologies, IEEE 2012.