Design and Improve AODV Protocol for Congestion Control in MANET using Cryptography Technique

Ms. Binal Goswami
Hasmukh Goswami College of Engineering, Gujarat, India

Mr. Parth Wadhwa
Hasmukh Goswami College of Engineering, Gujarat, India

Mr. Ashvin Prajapati
Hasmukh Goswami College of Engineering, Gujarat, India

Abstract

The mobile adhoc networks are the decentralized type of community wherein cell nodes can talk with each other without the presence of primary controller. Due to non-presence of valuable controller routing, security and nice of service are the 3 major troubles of the community. The maximum green routing protocol is Ad Hoc On-demand Distance Vector AODV. It is most efficient to transmit records from supply to vacation spot by using the usage of AODV routing protocol. In this paintings, the development in the AODV protocol is executed for the congestion avoidance in the network. The proposed method is primarily based on the back propagation algorithm wherein blunders of every course is to be had from supply to destination is calculated. The first-rate course is selected which has minimal error or approach that which has least possibilities of congestion within the community. The proposed and existing algorithms are implemented in NS2 and it's been analyzed that proposed technique plays nicely in phrases of diverse parameters compared to present set of rules.

Keywords: AODV, Cryptography, Active attack detection, Throughput, packet Delivery Ratio

I. INTRODUCTION

Mobile ad-hoc network, conjointly called wireless circumstantial network or ad hoc wireless are network, could be a ceaselessly self-organizing, self-configuring and infrastructure less network of mobile connected wirelessly. It suggests that during this system; nodes liberal to move during a random pattern. Therefore, every node acts as a router likewise as a bunch. In MANET, routing could be a method for selecting path within the network. it's 2 operations as - for locating associate degree optimum routing path and to transfer information packet of supply to destination path. circumstantial On-demand Distance Vector (AODV) routing protocol is associate degree on-demand protocol i.e. it discovers routes on and pro re nata basis victimization route discovery method. As results of its options, Eduard Manets is a lot of appropriate for planet applications during which the topology changes quickly. Nodes in MANETs be a part of and leave the network dynamically exhibiting their freelance and self-deployable behavior. No mounted set of infrastructure and centralized administration is needed during this quite a network. Nodes are interconnected through wireless interfaces [7].

A. Objective

The objective of this research is to improve the throughput by analysis of the following parameters:

- Packet Delivery Ratio
- Throughput

B. AODV Protocol

AODV is a billboard hoc On Demand Distance Vector could be a routing protocol designed for unplanned mobile networks. AODV could be a reactive protocol, capable of each uncast and multicast routing [11]. AODV is associate on-demand routing protocol, within which the route search method is initiated between the supply and destination node as once required. During this protocol every node maintains routing data within the variety of a routing table having one entry per destination. AODV uses the destination sequence range to ensure the route freshness and loop freedom of the route. AODV defines 3 messages: Route Requests (RREQs), Route Errors (RERRs) and Route Replies (RREPs). so as to find and management the routing inside the network from supply to destination, these messages are used. [5].

The supply sends Route Request Message to its neighbours. If a neighbour has no data on the destination, it'll send message to any or all of its neighbours so on. Once request reaches a node that has data concerning the destination (either the destination itself or some node that contains a valid route to the destination), that node sends Route Reply Message to the Route Request Message instigator [15]. Within the intermediate nodes (the nodes that forward Route Request Message), data concerning supply and destination from Route Request Message is saved. Address of the neighbour that the Route Request Message came from is additionally saved. initiator, it is assigned a unique id. When a node receives Route Request Message, it will check this id and the address of the initiator and discard the message if it had already processed that request [14].

AODV could be a packet routing protocol designed to be used in mobile unplanned networks (MANET)Intended for networks that will contain thousands of nodes One of a category of demand-driven protocols AODV is nice in terms of information measure and energy conservation [16].

There are two phases: Route Discovery and Route Maintenance

C. *Route Discovery*

Two message types: RREQ and RREP Source broadcast RREQ messages. Node forwards the RREQ if it's not the destination. Maintain back-pointer to the creator. Destination generates RREP message. RREP sent back to supply mistreatment the reverse pointer founded by the intermediate nodes. [5].

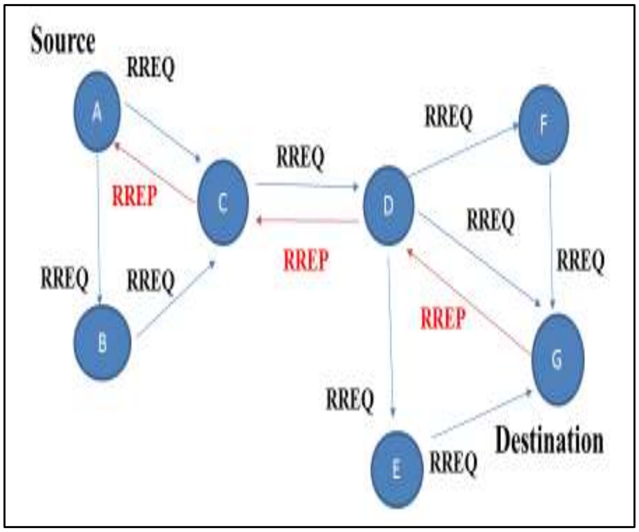


Fig. 2.1: RoutingDiscoveryinAODV

D. *Route Maintenance*

Route Maintenance – 2 message types: how-do-you-do and RERR Hello message is employed for link standing monitoring Ex: If a neighbor nod2.e doesn't receive any packets for over predefined interval time, link to it neighbor is broken. RERR Message is broadcasted when A node detects that a link with adjacent neighbor is broken If it receives a RERR from a neighbor for one or a lot of active routes. [5].

E. *Sequence Number*

AODV differs from different on-demand routing protocols in this is uses sequence numbers to work out associate degree up-to-date path to a destination. Each entry within the routing table is related to a sequence range [11]. The sequence range act as a route timestamp, making certain freshness of the route. Upon receiving a RREQ packet, associate degree intermediate node compares its sequence range with the sequence number within the RREQ packet. If the sequence range already registered is bigger than that within the packet, the prevailing route is additional up-to-date. Sequence number already registered is greater than that in the packet, the existing route is more up-to-date.

F. *Performance Parameters in MANET*

1) *Packet Delivery Ratio*

The fraction of the information packets delivered to destination nodes to those sent by supply nodes.

2) *Throughput*

Number of packets sends or receives in per unit of your time in network.

II. LITERATURE SURVEY

Gurveen Vaseer, Garima Ghai and Pushpinder Singh Patheja. “A Novel Intrusion Detection Algorithm: An AODV Routing Protocol” developed Mobile ad-hoc network (MANET) is a collection of movable nodes capable of self-routing, constraining energy and decentralized handling of nodes. It faces many challenges due to uncertainty of network topology i.e. security and congestion. In this paper we propose a novel algorithm for intrusion detection gainst attacks such as probing, Denial-of-service (DoS), vampire and User-To-Root (U2R) in a MANET environment. The attack detection has been carried out using a profile (behaviour) analysis and a confusion matrix (True positives, True negatives, False positives, False negatives). The performance of a standard Adhoc On-Demand Distance Vector (AODV) routing protocol has been reported for all 4 types of attack in a network simulator-2(ns-2) environment. To the best of authors' knowledge, this is the first paper reporting a novel intrusion detection algorithm using behaviour analysis for an AODV protocol in a MANET environment [1].

Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack "developed Routing in wireless network is fundamental task which helps node to send and receive packets. Due to lack of centralized authority security in mobile ad hoc networks is very difficult. Traditionally, routing protocols were designed for good performance only and security issues were not considered. So either new routing protocols should be designed which have security parameter also or security parameters must be included in the existing routing protocol. There are number of attacks on routing protocol, one of them is wormhole attack. We will evaluate the performance of AODV and DSR routing protocol under wormhole attack and compare the performance of these protocol without wormhole attack. Performance parameters are Average end to end delay, Throughput, and Packet delivery ratio(PDR). Neelam Janak Kumar Patel, Dr. Khushboo Tripathi "Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network" developed Mobile ad hoc network (MANET) is a special group of nodes; those are infrastructure less and wirelessly[2]. In MANET nodes are legitimate to leave and join the network at any point of the period. MANET is vulnerable to various types of security attacks like a wormhole, black hole, rushing attack etc., so security in MANET is the most significant concern to give secured communication and transmission between mobile nodes. Black hole attack is one of the most destructive attacks in network layer against routing in MANET. A black hole is a malicious node, an attacker provides a single-hop, high-quality path on behalf of all destination beginning all nodes around it to forward packets to it. A black hole node sends bogus routing information, advertised that it has an ideal route and springs other good nodes to route data packets through one. A malicious node drops all packets that it received instead of forwarding those packets. In this research paper, we implemented IDSAODV routing protocol for improving the securities in MANETs. It is the reactive type Ad hoc On-Demand Distance Vector (AODV) routing protocol to escape black hole attack. To identify and avoid the black hole attack using a proposed routing protocol (idsAODV). It deliberated a modification of the AODV protocol. Using Network Simulator NS-2.35 we get the experimental results that show an improvement in Throughput, Packet Delivery Ratio (PDR), and End to End delay using the proposed routing protocol that is idsAODV and results are comparing with Normal AODV routing protocol in the attendance of black hole attacks.

Satyam Kumar Sainy, Ravi Rai Chaudhary, Ajay Kumar" Performance Evaluation of Routing Protocols Based on Different Models in MANET" developed A mobile adhoc network is an independent system of mobile stations associated by wireless link to form a system. This system can be modeled in the form of an uninformed graph. Adhoc networks are peer to peer, multihope networks were data packets are transmitted to a source to destination through intermediate nodes (which serve as router). The performance of these three routing protocols is done on Glomosim Simulator and we 9 concluded LAR1 has better throughput in comparison to both AODV and DSR routing protocols in all three scenarios. Packet delivery Ratio behaves like throughput, LAR1 has better PDR in comparison to AODV and DSR [3]. Drop ratio is also similar to PDR, actually it is reverse of PDR so we can say that LAR1 has lower drop ratio in comparison to AODV and DSR. AODV and DSR have lower delay in comparison to LAR1. LAR1 routing protocol has higher delay, and it is also seen that as we increase the nodes, pause time and mobility delay is also increase. (CRAHNs) referred as Cognitive Improved Adhoc hoc On Demand Distance Vector (CIAODV) has been proposed with an aim to eliminate the overhead, resource consumption and taking advantage of conventional (AODV) protocol which considered as the most suitable protocol to dynamic and infrastructure less networks. The simulation results prove that the (CIAODV) protocol achieves better performance in the term of throughput, end to end delay and overhead as compared to (AODV) protocol [3].

Neelam Janak Kumar Patel, Dr. Khushboo Tripathi Modified AODV Protocol for Detection and Prevention of Black Hole Attack in Mobile Ad Hoc Network Developed Mobile ad hoc network (MANET) is a special group of nodes; those are infrastructure less and wirelessly. In MANET nodes are legitimate to leave and join the network at any point of the period. MANET is vulnerable to various types of security attacks like a wormhole, black hole, rushing attack etc., so security in MANET is the most significant concern to give secured communication and transmission between mobile nodes. Black hole attack is one of the most destructive attacks in network layer against routing in MANET. A black hole is a malicious node, an attacker provides a single-hop, high-quality path on behalf of all destination beginning all nodes around it to forward packets to it. A malicious node drops all packets that it received instead of forwarding those packets. In this research paper, we implemented IDSAODV routing protocol for improving the securities in MANETs. It is the reactive type Ad hoc On-Demand Distance Vector (AODV) routing protocol to escape black hole attack. To identify and avoid the black hole attack using a proposed routing protocol (idsAODV).

III. PROBLEM STATEMENT

Most of the existing algorithm do not focus on the security aspect while routing and moreover the congestion is the issue of the mobile adhoc network which reduce performance of the network.

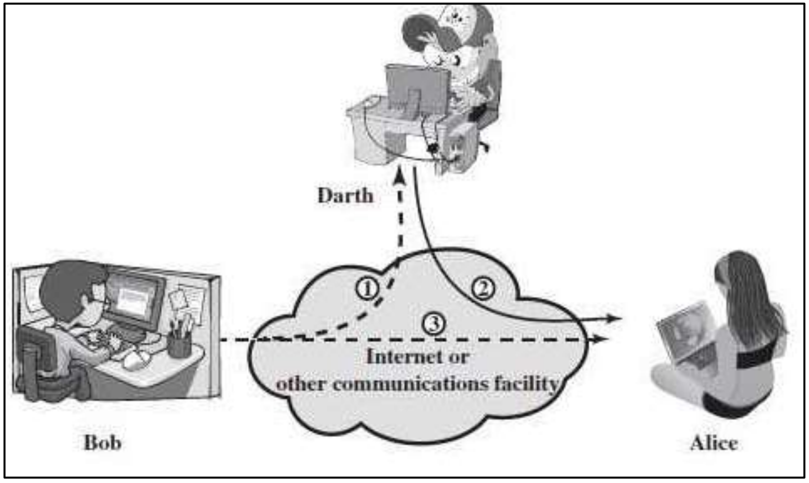
In this research the improvement in the AODV protocol is done for the congestion control and provide security against the active attack detection.

IV. WHAT IS CONGESTION CONTROL

A State occurring in network layer once the message traffic is thus significant that it slows down network latency. Effects of congestions delay will increase, performance decreases. If delay will increase, retransmission happens, creating scenario worse. When the quantity of packets will increase on the far side the limit and capability which will be handled by the network resources which ends degradation in network performance is termed congestion. Congestion is associate unwanted scenario wherever network faces the matter of additional traffic than its rated capability. Congestion is overcrowding or blockage thanks to overloading. The congestion happens in Eduard Manet thanks to restricted resources. thanks to the shared wireless channel and dynamic topology packet transmissions suffer from interference and weakening. Transmission errors conjointly cause burden on the network thanks to retransmissions of packets within the network. Congestion management technique is that the methodology by that the network information measure is distributed across multiple end to finish connections [8]. Congestion will be rate primarily based congestion management or buffer based congestion control.

A. *What is Active Attack Detection?*

Involve some modification of the information stream or the creation of a false stream. These attacks cannot be simply. Troublesome to forestall thanks to the big variety of potential physical, software, and network vulnerabilities. Goal is to discover attacks and to live through any disruption or delays caused by them.

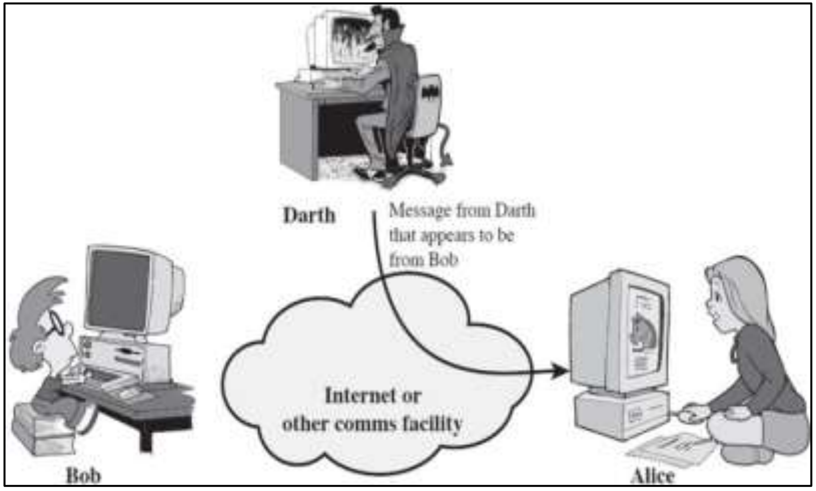


Active Attacks can be subdivided into four types:

1) Masquerade
2) Replay
3) Modification of messages
4) Denial of service

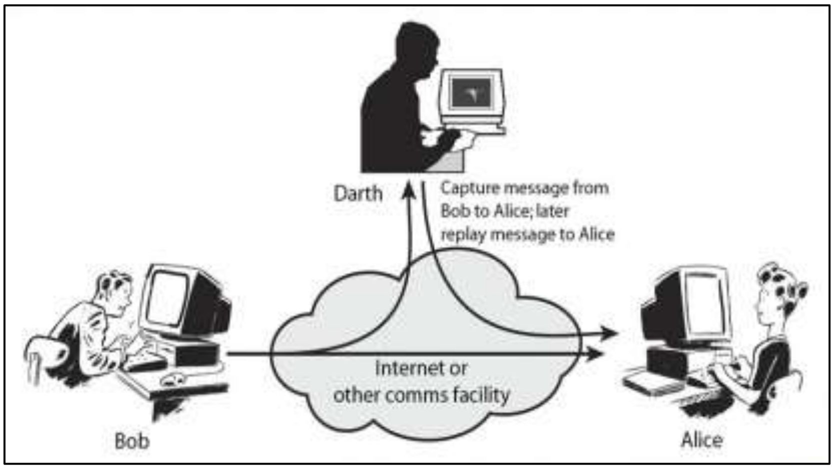
1) *Masquerade:*

Takes place once one entity pretends to be a unique entity sometimes includes one in all the opposite sorts of active attack.



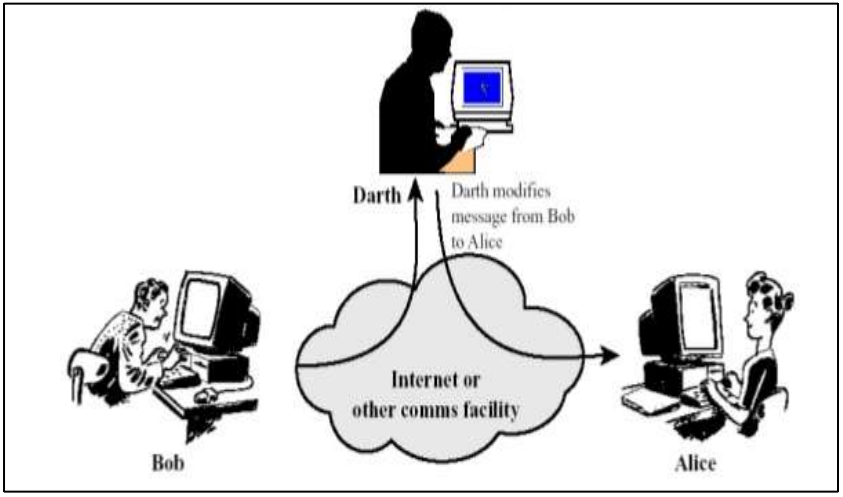
2) *Replay:*

Involves the passive capture of a knowledge unit associated its resulting retransmission to provide an unauthorized impact.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

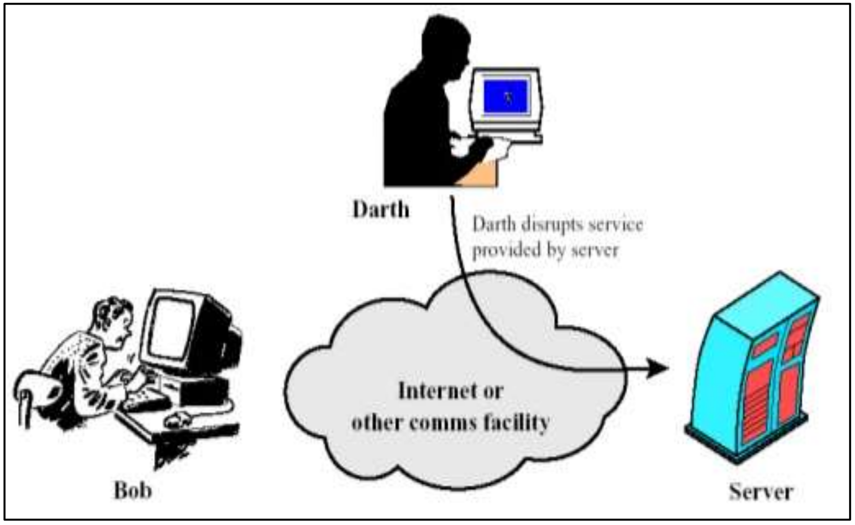
3) *Modification of Messages:*

Some portion of a legitimate message is altered, or messages are delayed or reordered to provide AN unauthorized result.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

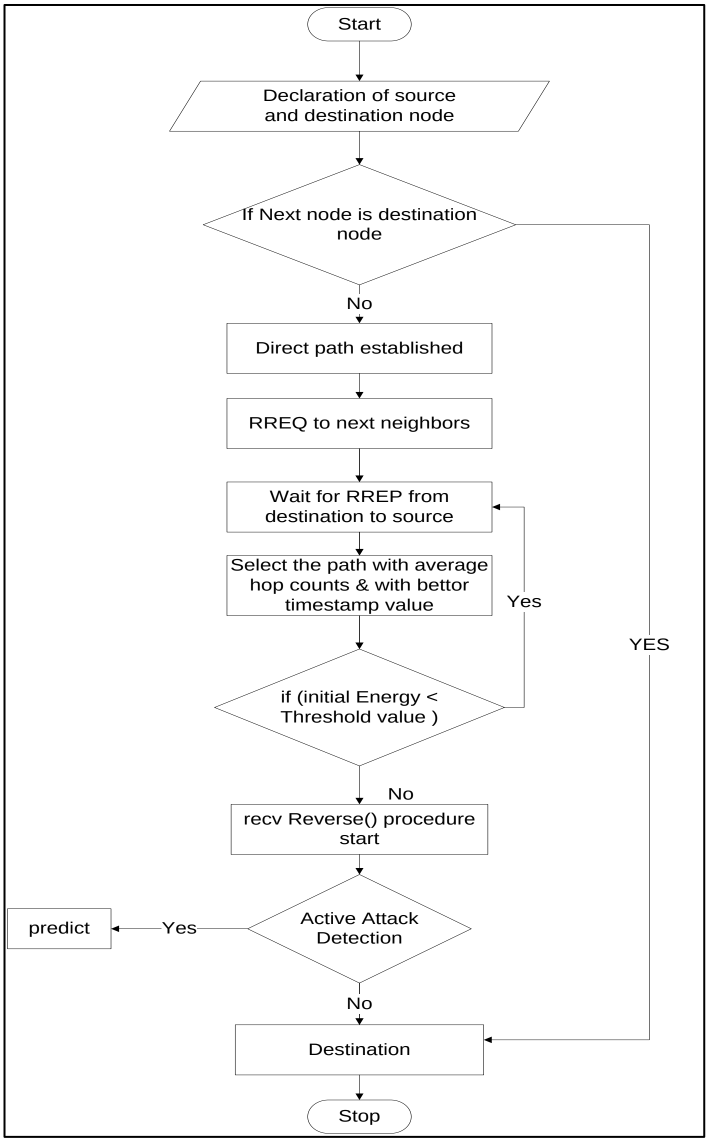
4) *Denial of Service:*

Prevents or inhibits the conventional use or management of communications facilities


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

V. PROPOSED METHOD

A. Flow Chart of the Proposed Algorithm


Start
Declaration of source and destination node
If Next node is destination node
No
Direct path established
RREQ to next neighbors
Wait for RREP from destination to source
Select the path with average hop counts & with bettor timestamp value
Yes
YES
if (initial Energy < Threshold value)
No
recv Reverse() procedure start
Active Attack Detection
Yes
predict
No
Destination
Stop

The AODV protocol first Declaration the multipath route to the Source to destination and sends the DES encrypted and next node to the direct destination path established. The flowchart of the declaration is shown in Fig. After RREQ to the next node neighbors. Wait the RREP from destination to source select the path with average hop counts and with better timestamp value if generated energy less threshold value and yes, wait for RREP from destination to source, no the reverse the procedures start and active attack detection if yes attack is predicting otherwise direct go to destination.

B. Proposed Algorithm:

Set Sender = S;
Set receiver = R;
Set protocol = AODV:

1) Step 1: Start
2) Step 2: Declaration of Source and destination node.
3) Step 3: if next node is destination node yes to direct destination path.
4) Step 4: No, to the direct path established.
5) Step 5: Else RREQ to next neighbors
6) Step 6: wait for RREP from destination to source
7) Step 7: Select the path with average hop counts & with better timestamp value
8) Step 8: if (initial Energy < Threshold value)

9) Step 9: yes, wait for RREP from destination to source
10) Step 10: No recv Reverse () procedure start
11) Step 11: Active attack detection
12) Step 12: If Yes, Attack is predict
13) Step 13: otherwise direct go to Destination
14) Step 14: Stop

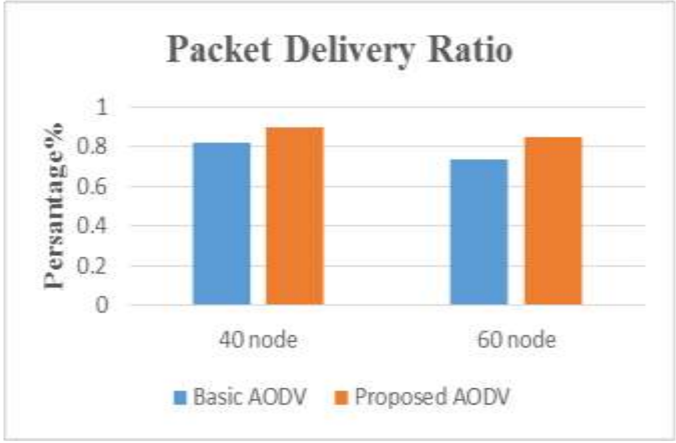
VI. SIMULATION PARAMETERS

Parameters	*Value*
Simulator	*NS-2(Version2.34)*
Channel type	*Wireless*
MAC Type	*Mac/802.11*
Mobility model	*Random way point mobility model*
Number of mobile node	*40,60 Nodes*
Traffic Type	*CBR*
Routing Protocols	*AODV*
Simulation Time	*300ms*
Simulation area	*1000*500m*
Packet Size	*512byets*

VII. RESULT

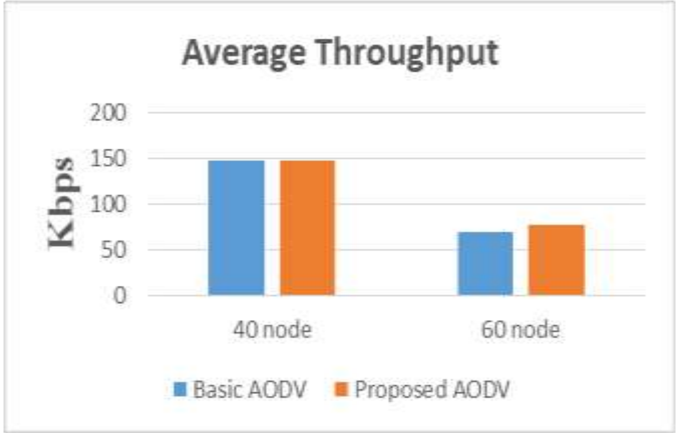
A. *Packet Delivery Ratio*

The fraction of the information packets delivered to destination nodes to those sent by supply nodes.
indicates the comparison of Packet delivery ratio of Basic AODV and Improved AODV is increase for 40 nodes and 60 nodes.



B. *Average Throughput*

Number of packets sends or receives in per unit of your time in network.
indicates the average throughput of Basic AODV and Improved AODV is increase for 40 nodes and 60 nodes.



VIII. CONCLUSION

We conclude that the improvement in AODV protocol by congestion control and also provide security against attack, which provide the better performance of the network using different number of nodes.

REFERENCES

[1] "Gurveen Vaseer, Garima Ghai and Pushpinder Singh Patheja.", "Intrusion Detection Algorithm: An AODV Routing Protocol", 978-1-5386-1356-6/17 $31.00 © 2017 IEEE.

[2] "Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja", "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack",978-1-4673-6101-9/13/$31.00 ©2013 IEEE.

[3] "Satyam Kumar Sainy, Ravi Rai Chaudhary, Ajay Kumar", "Performance Evaluation of Routing Protocols Based on Different Models in MANET", 978-1-5090-0774-5/16/$31.00 © 2016 IEEE.

[4] "LI Shibao, JIA Wei", "AODV Route Protocol Research Based on Improved ERS Algorithm", 978-1-4244-5849-3/10/$26.00 ©2010 IEEE.

[5] "Priya Mankotia1 and Er. Amandeep Kaur2"," Design and Improve AODV Protocol for Congestion Avoidance in MANET Using Neural Network", Volume 6, Issue 5, September- October 2017 ISSN 2278-6856.

[6] "Neelam Janak Kumar Patel, and Dr. Khushboo Tripathi" "Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network", All Rights Reserved © 2018 IJERCSE ,Vol 5, Issue 3, March 2018.

[7] "Anishi Gupta", "Black Hole Attack Mitigation Method based on Route Discovery Mechanism in AODV Protocol", 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.

[8] "Mr. Hardik N. Talsania and Prof. Zishan Noorani", "Techniques to Handle Black HoleAttack for AODV in MANET", IJIRST –International Journal for Innovative Research in Science & Technology| Volume 4 | Issue 10 | March 2018.

[9] "Rajaram Jatothu, Dr. RP Singh", "Efficient routing and High security transmission using AODV and Distributed protocol key generation with Dual RSA", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 23 (2017).

[10] "Vivek Soi and Dr. B.S. Dhaliwal", "Performance comparison of DSR and AODV Routing Protocol in Mobile Ad hoc Networks", ISSN 0973-1873 Volume 13, Number 7 (2017), pp. 1605-1616 © Research India Publications.

[11] "Radha Rani Gupta, Mahindra Ku. Mishra and Manish Srivastava", "Power Saving Routing Protocol for Ad hoc Networks based on AODV", International Journal of Computer Applications Volume 85 – No 19, January 2014.

[12] "Rasha Eltayeb, Adel Gaafar", "Cognitive Improved AODV Routing Protocol for Cognitive Radio Adhoc Network", (IJISSET) ISSN 2455-4863 (Online) Volume: 3 Issue: 10 | October 2017.

[13] "Abdelhafid Abouaissa1, Riri Fitri Sari2 and Pascal Lorenz1", "Security and performance enhancement of AODV routing protocol", Copyright © 2014 John Wiley & Sons, Ltd. Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2837.

[14] "Madhup Shrivastava, Monika Sahu, M.A. Rizvi and Khaleel Ahmad", "An improve AODV routing protocol for MANET", International Journal of Advanced Research in Computer Science, Volume 9, No. 2, March-April 2018.

[15] "Tanya Koohpayeh Araghi, Mazdak Zamani, Azizah BT Abdul Mnaf", "Performance Analysis in Reactive Routing Protocols in Wireless Mobile Ad Hoc Networks Using DSR, AODV and AOMDV", 978-0-7695-5133-3/13 $26.00 © 2013 IEEE.

[16] "Uma Rathore Bhatt, Abhishek Dangarh, Akanksha Kashyap, Aishwarya Vyas", "Performance analysis of AODV & DSR Routing protocols for MANET", 978-1-4799-3070-8/14 $31.00 © 2014 IEEE.

[17] "Mohamed S. El-azhari, Othman A. Al-amoudi, Mike Woodward and Irfan Awan", "Performance Analysis in AODV Based Protocols for MANETs", 978-0-7695-3639-2/09 $25.00 © 2009 IEEE.