Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777725

AD HOC ON- DEMAND DISTANCE VECTOR AND DYNAMIC SOURCE ROUTING PROTOCOL FOR ENHANCING THE QOS OF THE MANET UNDER WORM HOLE ATTACK MODEL

Versha Matre and Dr. Pradnya Ashish Vikhar
Department of Computer Science & Engineering
Dr. A.P.J. Abdul Kalam University, Indore (M.P.) - 452010, India
Corresponding Author Email : versha.matre@gmail.com

Abstract:
Mobile Ad hoc network (MANET) is a wireless network that has the capability to reconfigure itself without any centralized structure. This variety of network isn't in a situated number and configuration, but rather, it forms itself and allows for different nodes to adjoin in automatically. Since it has an adaptable and robust nature that makes it sensitive to attacks which could be fixed to the network really effortlessly. As an effect, the attacker would after serve as a sender or receiver for counterfeited packets. One of the most risky attacks of this network is wormhole attack. With wormhole attack, packets of data are transferred from one node to another dangerous node inside or outside the network. Thus, we hold in this work to study the aftereffect of a wormhole attack on two routing protocols, namely Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). The comparison will subsist held in terms of two main network interpretation standards throughput and end-to- end delay. Network Simulator- 2 (NS- 2) will be applied to operate the simulation tests in this work and compute the effects. This study gives a substitute contribution to the field of network attacks. It provides a substitute Worm Hole Attack Model (WHAM), which will exist applied to MANET routing applying NS- 2 WHAM has existed referred to the protocols mentioned above to test their resistance and strength under the attack.
Keywords: Mobile ad hoc network (MANET); Routing Protocols; AODV; DSR; Wormhole Attack.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is constructed to produce a network anywhere and wherever there's no fixed structure, in distribution to allow the mobility of the addict on the network. In different terms, MANET is a collection of mobile nodes that transmit and interact in an allowed proprieties with each different through wireless connections. In distribution to supply the mandatory network functionality. There's no centralized infrastructure, so the node itself does the routing. MANET can exist employed in fields similar as military service, sensor networks, disaster rescue operations, and conferences. Anyway of geographical position, this order of network provides the data as easy as services due to their self- reconfiguration constitution.

In MANET, there are three varieties of protocols which are, reactive, proactive, and hybrid routing protocols. This exploration aims to study two varieties of routing protocols, namely Ad

hoc On- Demand Distance Vector (AODV) and Dynamic Source Routing (DSR), under the concussion of wormhole attack. As far as we have, no researcher has gave such a study until anymore. This study gives a new beneficence to the field of network security. It provides a substitute Wormhole Attack Model (WHAM), which has subsisted referred in MANET routing applying network simulator- 2 (NS- 2). WHAM has existed referred to the protocols mentioned above to test their defiance and strength under the attack.

2. BACKGROUND AND RELATED WORK

2.1 Mobile Ad- Hoc Network

MANET is allowed to be applied in a special field, produced up of a cluster of nodes interconnected wirelessly. It's an infrastructure-less network which has a capability to configure itself without any natural intervention. Any node in the network is simultaneously a router as effortlessly as a host. Nodes can exist assigned easy as network topology differs anywise (1, 2). The evolution of communications and the addition of network fields has routed to an increment in MANET network operations similar as military fields, wildlife monitoring, medical uses, earthquakes and disaster fields operations (2, 3).

2.2 Ad Hoc On-Demand Distance Vector

This paperwork uses AODV routing protocol. AODV is a dynamic routing protocol. It has existed highly studied and evolved for multiple times, establishing its robustness and advantages. The critical advantages of the AODV protocol are that, comparative to different MANET routing protocols, the detention in message infrastructure with the destination is lower. Secondly, in discrepancy with different ad hoc routing protocols, AODV avoids congested routes. Third, the rapid ad hoc topological reconfigurations that can affect the different protocols of routing can exist handled (1, 4).

In the route discovery hoop of the AODV routing protocol in MANET, the source broadcasts RREQ to the neighbors, as show in Figure 1. Observing RREQ, we have that it contains the IP addresses of the beneficiary, the broadcast ID, and the consequence composition of the destination. Every middle node receives the RREQ packet does two individual procedures instead, it checks whether the RREQ packet has previously existed transferred by the identical address as originator of the RREQ, predicated on this according it also either discards or accepts the RREQ packet. Flooding attacks can exist scaped by delivering this step of verification. Second, the middle node tests the destination consequence number held in its routing table if the RREQ packet is approved. It unicasts the RREP packet to the root node if it's higher than or composed to the one contained in the RREQpacket.However, the RREQ packet can hold its navigation until it reaches the destination node itself, releasing the RREP packet to the root node, If no middle node has a suitably substitute (fresh destination sequence composition) path to the destination node.

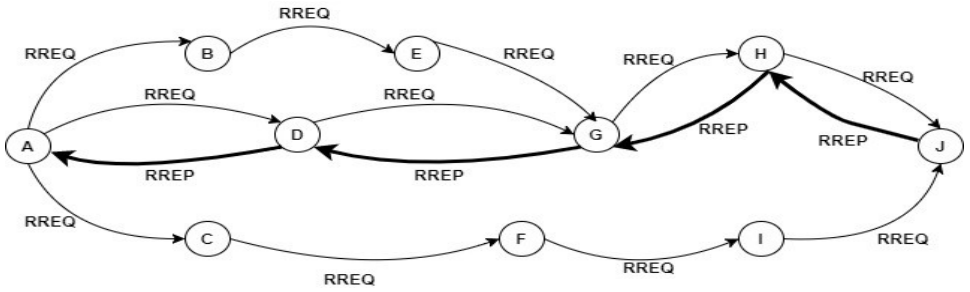


Figure 1: AODV

2.3 Dynamic Source Routing

DSR is a routing protocol that comes within the classification of reactive routing protocols. It can discover or trace the route from the source to the destination simply when required. An operation called the Rout Discovery Method is employed by DSR to discover the path from the root node to the destination node (6).

The path detection and path maintenance steps affect three varieties of communications

1. RREQ packet it's circulate from root node to destination node that contains packet ID, destination address, and own address.

2. RREP packet when the destination receives from the root node a RREQ packet. It generates a substitute packet of RREP and forwards it to the root.

3. RERR packet during the packet delivery, the RERR correspond to know if the route of the node has modified, also the node won't exist suitable to transfer the packet, so it'll transfer the RERR packet to the root of the packet (7)

The DSR Protocol transmits the route to its neighbors but doesn't overflow it. It exactly tracks the route by measuring the incremental length between the root node and the destination node or computing the composition of nodes extant. (8) As displayed Figure 2 for illustration, we've a network containing 7 nodes, the root node is the node number (N1), and the destination node is the node number (N7)

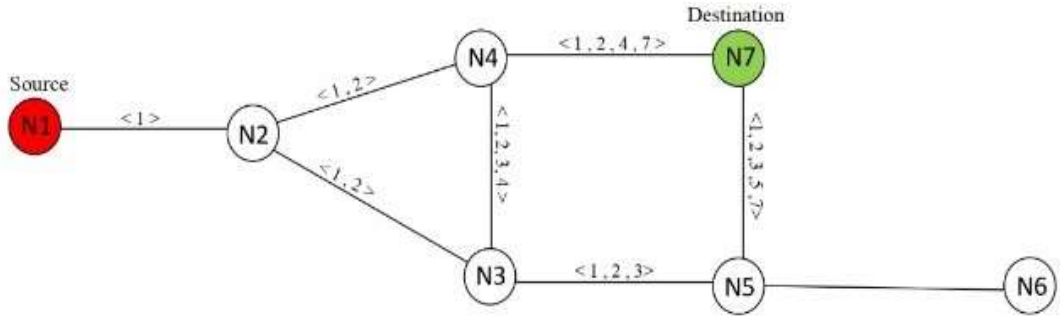


Figure 2: the Route Discovery and Route Maintenance

Step 1 You'll subsist starting from the node number N1 and circulate the data about it to its neighbors. In this case the path info is< 1> because it has a link (one-to-one) between node

number N1 and number N2.

Step 2 Broadcast preceding path data to neighbors of node N2 to nodes number N3 and N4. And the substitute path will remain identical<2> in all the cases.

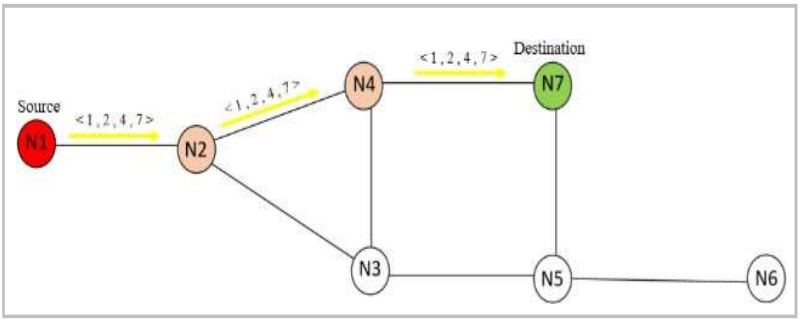
Step 3 In node number N3 the foregoing path
<1, 2> is circulate to following neighboring nodes. Substitute path till node N5 will exist<1, 2, and 3> and identical procedure can exist done for different nodes.

Step 4 Broadcast the substitutive routes<1, 2, 3, 5>,
<1, 2, 4> to nodes N6 and N7, individually.

Step 5 all the preceding path are iterated until the root node reaches the destination node via all ways. Three achievable ways are generated

- Route 1<1, 2, 3, 4, 7>
- Route 2<1, 2, 3, 6, 7>
- Route 3<1, 2, 4, 7>

DSR take the shortest path which is path 3 as displayed in Figure 3.



•

Figure 3: RREP packet sent from destination node N7

3. WORMHOLE ATTACK

This attack is the demolition of a single route in MANET and is one of the most frequent security challenges in this variety of network. It's similarly esteemed a variety of tunnel attack where a special malicious node receives a special package and also transfers it to different locations in the network and also returns it to the network, Wormhole attacks effect a revelatory declension in network assignment and interpretation and menace exclusive network security. Which is displayed in the figure below, Figure 4.

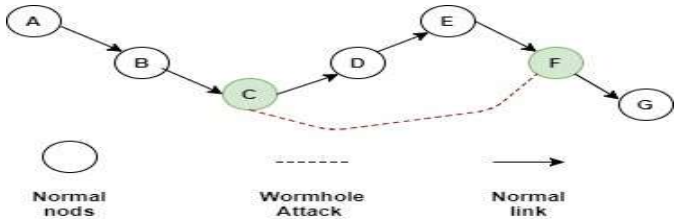


Figure 4 Wormhole Attack

The conception of the attack will exist transparent through the succeeding illustration. firstly, we will accept that we've two networks one named A and the different is B, we hold that one of these two networks will start as a malicious node, and each of these nodes is linked through a connected link between them, so node X in A and node Y in B are two neighbours if they produce a confidential direct association between each different, know Figure 5. This kind of attack is viewed one of the most sophisticated varieties of attacks in MANET, if the attackers are interconnected to the unexceptional link and not to the wormhole in this case the attacker has an adaptable atmosphere so that he can conduct the incorrect instruction.

• The wormhole link is applied to as the tunnel that's crystallized between the attackers.
• The tunnel is either a wire association or links in which the frequencies is really high (21).

The working principles of the wormhole attack are viewed in Figure 5 under, and the identical line is applied for transferring and taking packets during transmission between X andY.

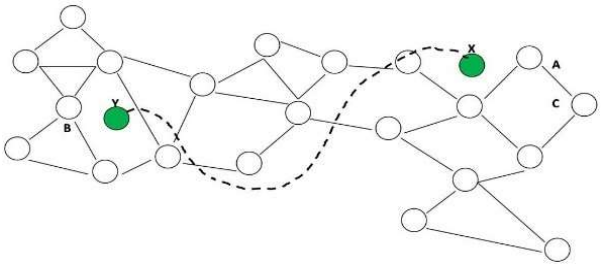


Figure 5 Wormhole Attack

4. AODV AND DSR VULNERABILITY TO WORMHOLE ATTACK

In a wormhole Attack, the attacker finds a strong strategic position in the network applying the shortest way between nodes. Attacker advertises the route that establish to allow the rest of nodes knows about the shortest way to circulate the data. Once the nodes created an immediate link from each distinct, the attacker will admit the packets from one specific position in the network and encapsulate these packets employing the tunnel to enter by another position in the equal network, and also the packet will exist promoted from that position. This is the route to attack routing protocols of networks. This variety of attack is actually risky, truly when the network provides confidentiality and protection.

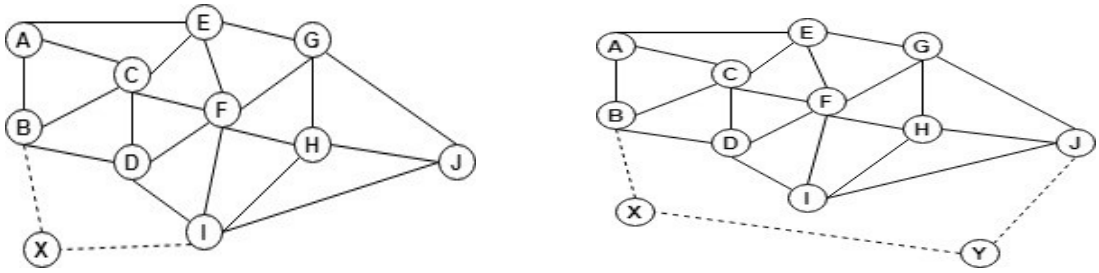


Figure 6: Wormhole Attack in AODV and DSR

AODV and DSR are really sensitive to wormhole attack. The attacker may transmit RREQ packets direct to the destination node by exploiting wormhole through thenetwork.However, they will promote it and discard all different RREQ packets from the standard node, if the neighbours of the destination node admitted the request. For routes that hold other than one hop, the attacker can easy produce a packet transferred bypass through the wormhole link and appear rapidly which is displayed in Figure 6(a). The attacker can similarly transmit the packet bit by bit to reduce the delay time, which is displayed in Figure 6(b) (21).

5. SIMULATION ENVIRONMENT AND SETTINGS

In Figure 7, theadvanced wormhole attack model (WHAM) infrastructure is referred on the two taken routing protocols namely, AODV and DSR. When IP protocol requests a path, the routing protocol starts to discover routes in this case, WHAM starts wormhole attack on MANET.

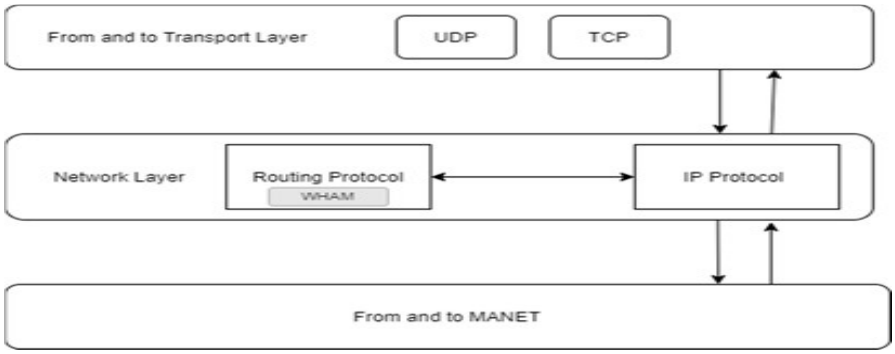


Figure 7: WHAM Architecture

OTcl is an extension to Tcl/ Tk for object- orientated programming. NS- 2 uses OTcL for the simulation programmer to make up the network objects in the recollection. NS- 2 uses the ultimate style, where the framework file is an OTcl file called “OTcl simulation Script”. As shown in Figure 8, below, this script contains an interpretation Parameters, which contain composition of Attackers and Radio Range. For Network simulation the composition will exist on the two routing protocols which are AODV and DSR. In NS- 2 simulation result kept in Trace file, which gives Network Animator (NAM) is an animation tool predicated on Tcl/ TK for displaying traces of network emulation and traces of authentic packets. AWK Scripts for NS- 2 to recover data from Trace Files. Also, the interpretation metrics that are viewed in our work are Throughput and End- to- end delay. Ultimately, the output is showed as graphs exploiting Microsoft Excel 2013.

Carrying the simulation results experimentations. The experimentations were transported out by varying one side, the composition of attackers (2, 4, 6 and 8), placing the attackers near the target, which helps to conclude the impact of wormhole attack. The CBR message begins with a traffic load of 2 packets/ s from1.0 s to the termination of the simulation. The packet size is 1000 bytes and the attacker starts the simulation at 30s until the termination. The mobility model and radio propagation model employed are, arbitrary waypoint and two- ray ground

reflection models, independently

5.1 Simulation WHAM system components

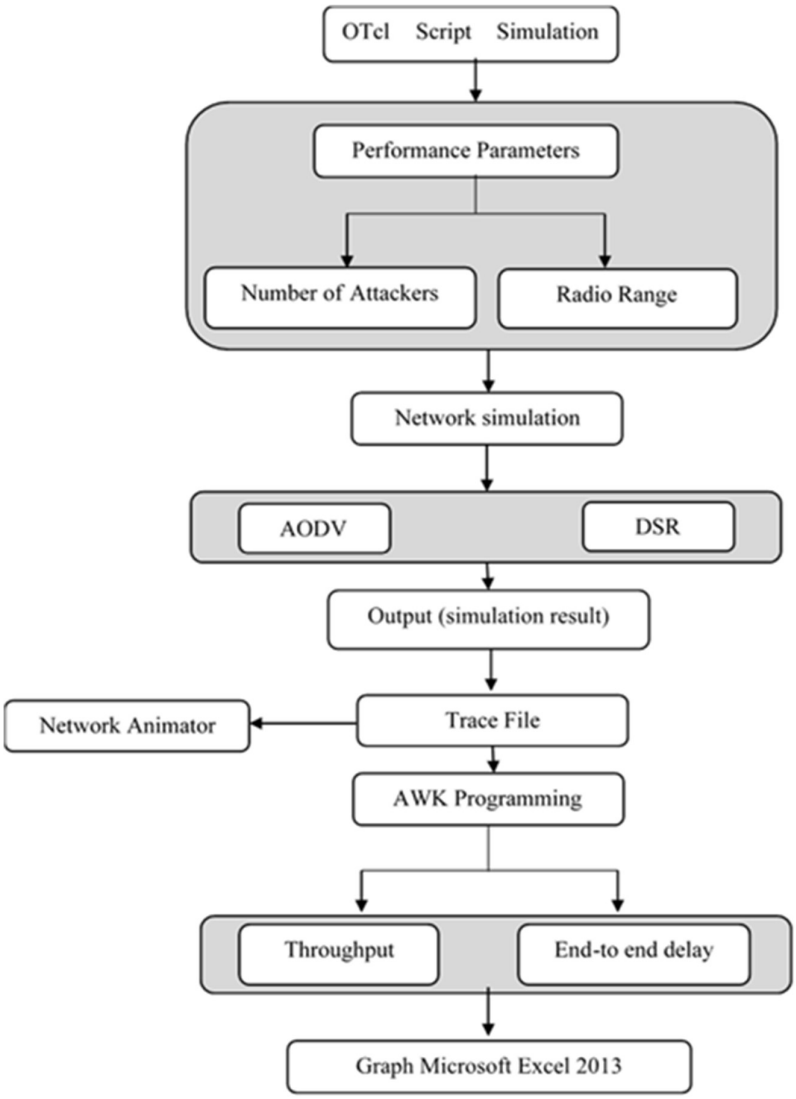


Figure 8: Simulation System Components

5.2 Performance metric

In this work, each consequential valuation is composed from the standard of 5 runs for the experimentation in NS- 2. For each routing protocol two- performance metrics has existed observed which are end- to- end delay and throughput. The Table 2 below illustrates the node adjuncts that we applied in our experimentation.

In this work, each consequential valuation is composed from the standard of 5 runs for the experiment in NS- 2. For each routing protocol two- performance metrics has existed observed which are end- to- end delay and throughput.

End- to- end delay the moment that a data packet takes to transfer the destination. This involves any implicit delays incurred during route detection latency by buffering. The standard of standing for the destination is recorded in each experimentation. The delay of E2E is calculated as follows

Throughput it's the complete composition of delivered packets for the comprehensive time of the simulation. It represents the standard of the throughput valuations for destinations in each experimental outcome

Parameter	Value
Network area	1000m × 1000m
Number of nodes	20
Nodes speed	0 – 7 m/s
Bandwidth	11 mbps
Traffic Packet size	512 bytes
Packet rate	2 packets per second
Traffic type	CBR

6. RESULTS AND DISCUSSION

The outcome of computing the intermediate Throughput for AODV and DSR when we modify the composition of worm attack nodes, we've observed that the AODV hold higher intermediate throughput valuations when analogized with the DSR protocol. While, the DSR has lower intermediate throughput valuations. Figure 11 under display the comparison between AODV and DSR. AODV protocol has the line with red shade and DSR has the line with blue shade.

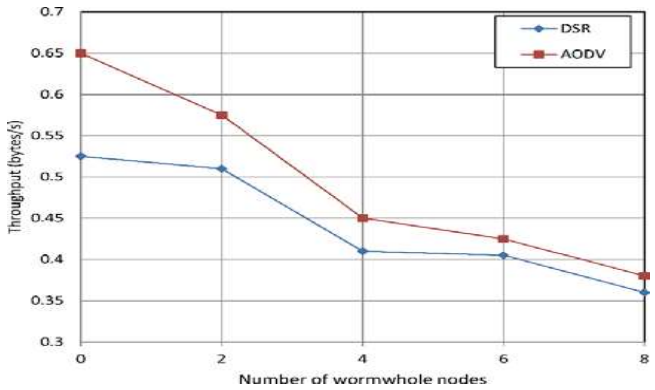


Figure 11: Average Throughput VS Number of Wormhole Nodes

The effect of computing the End- to- End Delay for AODV and DSR when we modify the composition of worm attack nodes, we've viewed that the AODV hold lower end- to- end delay valuations when analogized with the DSR protocol. Similarly, the DSR has high delay. The figure 12 under display the comparison between AODV & DSR. The AODV protocol has the line with red tone and DSR has the line with blue tone.

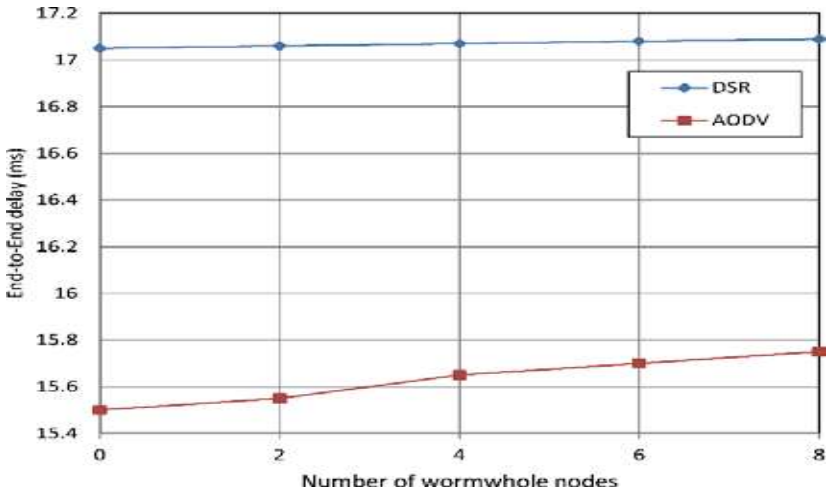


Figure 12: End- To- End Delay vs Number of Wormhole Nodes

The results of experimentations display that AODV is better than DSR. AODV has high interpretation than DSR, which has high outcome of throughput and lower end- to- end delay from DSR. DSR shows that it collapses to wormhole attacks. The outcomes produce that the extending the radio range on all protocols expand the throughput and expand the end- to- end delay valuations. The experimental outcomes in figure 13, demonstrate that when the evolved radio range the high throughput. When the radio range expand it allow the network to expand the throughput. The following figure 13 produce the throughput when exploiting other radio rang. In which the colored red belongs to AODV and blue belong to DSR.

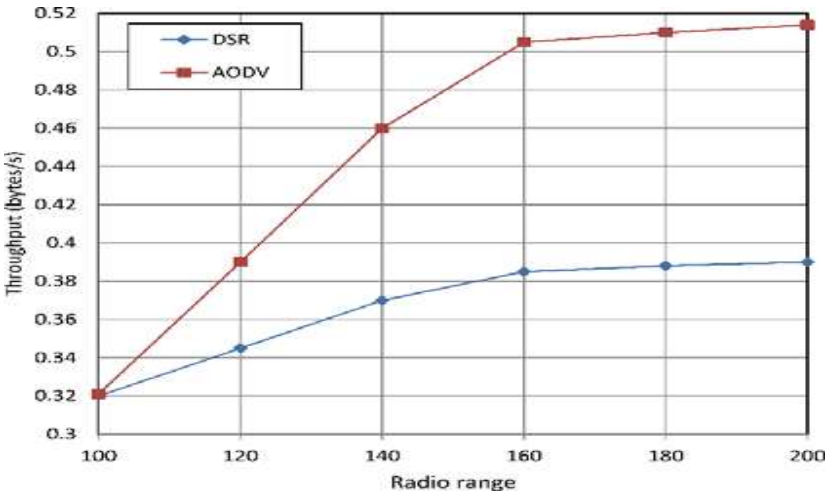


Figure 13: Average Throughput vs Different Radio Range

For the end-to-end delay we introduce that the AODV hold shortest end-to-end delay when analogized with the DSR, and DSR hold high end- to- end delay when the range increases. The succeeding figure 14 display the outcome of end- to- end delay when the radio range modified and AODV protocol with the red tone and the DSR with blue tone.

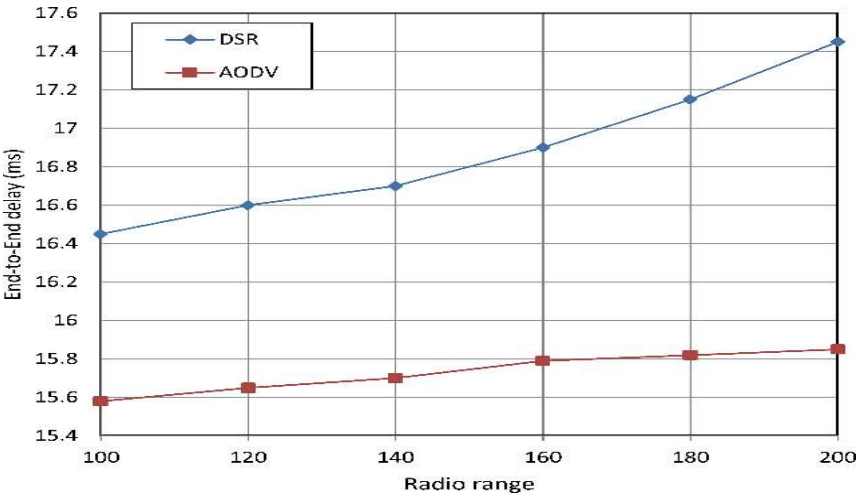


Figure 14: End- To- End Delay vs Different Radio Range

7. CONCLUSIONS AND FUTURE WORK

This work examined two routing protocols in MANET and presented a worm hole attack model(WHAM) that creates wormhole nodes in CBR traffic, which existed applied in AODV and DSR routing protocols applying NS2. Two network interpretation criteria were exploited to analogize the two protocols under attack throughput and end-to-end delay. The outcomes and their analysis hold subsisted presented. As displayed in the previous graphs, AODV executed more in terms of throughput and end- to- end delay and shew the most resistant behaviour analogized to DSR.

In this study, we suitednot valuate the interpretation of our model applying jitter, routing overhead and packet lose rate network performance criteria. In the future, we will estimate the performance of these protocols using these performance criteria and we're appearing for going true implementation.

REFERENCES

1. A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET: CRC press, NW, USA,2016.
2. S. Mishra, P. Varshney, S. Choudhary, and R. Purohit, "Performance Evolution of Conventional and Swarm based Routing MethodsinMobileAd-HocNetworks,"in2019 2ndInternationalConferenceonPowerEnergy, Environment and Intelligent Control (PEEIC), 2019, pp.528-531.

3. Umakant Dinkar Butkar, et.al "Accident Detection and Alert System (Current Location) Using Global Positioning System" JOURNAL OF ALGEBRAIC STATISTICSVol. 13 No. 3 (2022) e-ISSN: 1309-3452
4. R. Singh, "An Overview of MANET: Characteristics, Applications Attacks and Security Parameters as well as Security Mechanism,"InternationalResearchJournalof Engineering and Technology (IRJET), vol. 5, pp. 1155-1159,2018.
5. K. Rajani, P. Aishwarya, and S. Meenakshi, "A review on multicasting routing protocols for mobile ad-hoc wireless networks," in 2016 International Conference on Communication and Signal Processing (ICCSP), 2016, pp. 1045-1052.
6. R. Sadakale, A. Bhosale, and N. Ramesh, "Performance Analysis of Traffic Types in AODVRoutingProtocolforVANETs,"in2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp.1-5.
7. Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Advanced robotic manipulator renewable energy and smart applications. Computer Integrated Manufacturing Systems, 29(2), 19–31. Retrieved from http://cims-journal.com/index.php/CN/article/view/782
8. N. Jain, A. Rahman, and A. K. Dubey, "Code AwareDynamicSourceRoutingforDistributed Sensor Network," in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp.272-276.
9. I.-R. R. P.1546, "Method for point-to-area predictions for terrestrial services in the frequency range 30 MHz to 3 000 MHz," International Telecommunication Union Radiocommunication Sector (ITU-R)P.1546-4, 2009.
10. Butkar Uamakant, "A Formation of Cloud Data Sharing With Integrity and User Revocation", International Journal Of Engineering And Computer Science, Vol 6, Issue 5, 2017
11. S. Ali and P. Nand, "Comparative performance analysis of AODV and DSR routing protocols under wormhole attack in mobile ad hoc network on different node's speeds," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp.641-644.
12. H.Moudni,M.Er-rouidi,H.Mouncif,andB.El Hadadi, "Performance analysis of AODV routingprotocolinMANETundertheinfluence of routing attacks," in 2016 International Conference on Electrical and Information Technologies (ICEIT), 2016, pp.536-542.
13. S. Garg, "Performance analysis of AODV and TORA under DDoS attack in MANETs," IJSR International journal of science and research, vol. 3, pp. 297-304,2014.
14. G. Gupta and A. Mishra, "Simulation Based Study of Cooperative Black Hole Attack Resolution using Cross-Checking Algorithm," International Journal on AdHoc Networking Systems (IJANS), vol. 5, pp.17-28.
15. S. Ruj and R. Sachdeva, "Analysis of Selfish Node Attack in AODV Routing Protocol using GLOMOSIM," International Journal of EngineeringDevelopmentandResearch,vol.5, pp. 784-789,2017.
16. Y. Bai, Y. Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," in 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, 2017, pp.1-5.
17. Umakant Butkar, "An execution of intrusion detection system by using generic

algorithm",IJIFR, Vol 1, Issue 10, 2014
18. R. Singh and T. P. Sharma, "Present Status of Distributed Denial of service (DDoS) attacks in internet world," International Journal of Mathematical, Engineering and Management Sciences, vol. 4, pp. 1008-1017,2019. P. Oberoi, S. Mittal, and R. K. Gujral, "ADRCN: A framework to detect and mitigate malicious insider attacks incloud-based environment on IaaS," International Journal of Mathematical, Engineering and Management Sciences, vol. 4, pp. 654-670, 2019.
19. A. A. Ajibesin, M. M. Kah, A. T. Ishaq, andC. Ajibesin, "Performance Analysis of Topology and Destination Based Routing Protocols in Mobile Ad-Hoc Network Using NS2," in 2019 IEEE 13th International Conference on Application of Information and CommunicationTechnologies(AICT),2019,pp. 1-6.
20. Umakant Butkar, "A Fuzzy Filtering Rule Based Median Filter For Artifacts Reduction of Compressed Images",IJIFR, Vol 1, Issue 11, 2014
21. A. Sahoo, A. Shreya, C. S. Dash, I. Priyadarshini, S. Sobhanayak, S. S. Panda, et al., "Performance Evaluation of AODV, DSDV and DSR Routing Protocol For Wireless Adhoc Network," in 2018 International Conference on Advances in Computing, Communication ControlandNetworking(ICACCCN),2018,pp. 348-351.
22. S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," Journal of Network and Computer Applications, vol. 36, pp. 582-592,2013.
23. E. Hyytiä and J. Virtamo, "Random waypoint model in n-dimensional space," Operations Research Letters, vol. 33, pp. 567-571,2005.
24. Umakant Butkar, " Review On- Efficient Data Transfer for Mobile devices By Using Ad-Hoc Network", International Journal of Engineering and Computer Science, vol 5, Issue 3, 2016
25. A. M. Kanthe, D. Simunic, and R. Prasad, "Effects of propagation models on AODV in mobile ad-hoc networks," Wireless personal communications, vol. 79, pp. 389-403,2014.