International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-3, February 2022

Black Hole Attacks on MANETs: Analysis and Prevention

Arudra Annepu, Priti Mishra

Abstract*: Wireless network technically, refers to the category of network in which communication is carried out without using wires. In modern era wireless network has great importance because the communication is taking place with the use of radio waves. Thus, the use of ad-hoc network starts yielding a great importance in variety of applications. The certain research work is carried out in this particular field. MANET is a constructed from various mobility in the form of mobile nodes and anytime without any need of fixed infrastructure. MANET can be made on fly due to lack of fixed infrastructure. MANET is numerous threats types of attacks due to dynamic changing topologies and wireless medium. Security of the MANET becomes one of the challenging tasks. Black hole attacks is the main type of attack that are possible in MANET. Black hole node not forward any data packets to the neighbour node instead it drops all the data packets. Black hole attacks are bit hard to detect due to lack of centralized access. This research work concentrates to enhance the security of MANET by identifying and blocking black hole assaults from occurring. A reactive routing system such as Ad-Hoc on Demand Distance Vector has previously been used to address security problems in the MANET (AODV). Various attack types were investigated, and the consequences of these assaults were detailed by describing how MANET performance was disrupted. Network Simulator 3 (NS3) is used for the simulation process.

***Keywords*: MANET, Black Hole, Routing Protocols, AODV, Network Simulator.**

I. INTRODUCTION

Decentralized and self-contained wireless networks are the hallmarks of Mobile Ad-Hoc Networks. In MANETs, mobile nodes are used unrestricted in their movement inside and outside of the network. In a network, nodes are systems or devices that are mobile and participate in the network. Alternatively, they may simultaneously function as a host and a router. Depending on their network connection, they may create any number of topologies. As a result of their self-configuration capability, these nodes may be quickly deployed without the requirement for infrastructure. The IETF's MANET working group (WG) develops IP routing protocols as part of the Internet Engineering Task Force. Routing protocols are a difficult and fascinating field of study. AODV, DSR, and other MANET routing technologies are available and others have been developed [1].

Nodes in MANETs interact with each other because of trust rather than because of a centralised management. As a result of this feature, MANETs are more susceptible to attack from inside the network. MANETs are made more vulnerable to assaults because of wireless connections. This makes it simpler for an attacker to penetrate the network and get access to on-going communication. Mobile devices that are in range of the wireless connection may hear what's going on and even join in on the fun.

MANETs need a secure means of transmission and communication, which is a difficult but critical problem given the rising number of mobile network attacks. Everybody's screaming about security these days. Engineers need to know about various kinds of attacks and how they affect MANETs in order to ensure safe communication and transmission. A MANET may be attacked via wormholes, black holes, sybils, floods, routing table overflows, DoS attacks, selfish nodes misbehaving, and impersonation attacks. Due to its lack of centralised network administration, authorisation facility, rapidly changing topology, and limited resources, a MANET is particularly vulnerable to denial-of-service assaults because of communication dependent on mutual trust between nodes.

For a long time, research on MANETs centred on various types of security risks and assaults DoS, DDoS, and Impersonation assaults are examples of such attacks. AODV reactive routing protocol is used to assess the BHA on MANET, and the consequences of this assault on MANET's performance are described. Studies on the effect of the BHA in MANET utilising reactive and proactive protocols and comparisons of the assault's susceptibility to both have received very little attention. This must change. Both kinds of protocols are under assault, and the attacks' effects on MANETs must be addressed.

This study examines the effects of a Black Hole assault on MANETs by comparing the response times of AODV and OLSR, which are both reactive systems.

II. RELATED WORK

In a mobile ad-hoc network, nodes/stations are linked through wireless connections and operate independently of one another. A node may act as a router, sending information to other nodes in the neighbourhood. As a result, infrastructure-less networks are another name for this kind of network. There is no centralised management for these networks.

Manuscript received on January 05, 2022.
Revised Manuscript received on January 12, 2022.
Manuscript published on February 28, 2022.

* Correspondence Author

Arudra Annepu*, Research Scholar, Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, R.T Nagar, Bangalore (Karnataka), India. Email: yarudra@gmail.com

Priti Mishra, Professor, Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, R.T Nagar, Bangalore (Karnataka), India. Email: mprits@rediffmail.com

MANETs are used in disaster recovery and relief operations when conventional wired networks have already been damaged, such as in the case of emergency services.
MANETs have a role in linking people in other It may be used for pleasure, education or commercial purposes. MANETs are becoming more popular nowadays as a result of these reasons. It's widely used owing to the simplicity of deployment and lack of cables it eliminates.
There is a lot of interest in MANETs because of their dynamic, infrastructure-less, and scalable nature. Despite MANET's widespread use, these networks remain very vulnerable to assault. Wireless connectivity further increase the vulnerability of the MANET to assaults, making it simpler for an attacker to enter the network and get access to the current conversation. In MANET, several attack types and their effects on the network have been examined. a grey hole attack is one in which the attacking node acts maliciously until the packets are lost, and then returns to its usual behaviour A flooding attack employing RREQ or data flooding is also used by attackers to take advantage of MANETs routing protocols, which are vulnerable to this kind of attack.

In any network, instead than relying on the distance between nodes, they take use of the fact that they are close together geographically. Attackers use this defect to keep nodes awake until all of their energy has been consumed, at which point the node goes into permanent slumber. This is one of the most pressing concerns in MANET. Numerous more MANET attacks, such as the jellyfish assault, have been explored and revealed.
In [2] proposed a mechanism that will integrate the Data Routing Information table (DRI) with Ant Colony Optimization (ACO). The proposed mechanism send a promiscuous mode activation message to all neighbour nodes and checks the DRI table of all nodes and after that find all available path from source to destination using ACO table.
In [3] proposed a four step method For the identification of the network's "grey hole." The first step is Data Collection of neighbours in which the information of each node will be gathered by each node, its neighbour and enters in its DRI table, in next step which is ‘local anomaly detection’ source selects a Cooperative Node (CN) by checking the DRI table of that node. Source node forwards a RREQ packet to CN and asks it if it receives the packet or not, if not it will increase its maliciousness. Third step is Cooperative Anomaly Detection is done to avoid the mistake in the detection of malicious node. Last step is ‘Global Alarm Sending’ in which source broadcast the node as gray hole node.
In [4] proposed a technique based on IDAD. The IDAD monitored the activities of nodes and collect the audit data. IDAD compare the activity of each node containing audit data and other resources find the malicious node and isolate it from the system.
In [5] proposed the two combine method technique to prevent the Mobile Adhoc Network i.e. local collaboration of neighbouring nodes to monitor each other and cross validation method in which each node cross verify the next node and monitor overheads transmission. The technique improves the security of Mobile Adhoc Network to some extend but in some case this technique break.
In [6] proposed a technique that improve routing efficiency of Mobile Adhoc Network by selecting the most stable path so as to reduce the latency and overhead. The selection of path depends on mobility patterns of nodes in the network and these mobility pattern depends on the movement of nodes with respect to other nodes in the Mobile Adhoc Network.
In [7] proposed a new type of technique known as AODV-BR. The proposed technique is based on backing up the alternate routes to the destination. The technique uses different routes and a mesh structure. Ad hoc on-demand routing protocols may be combined with the system. The backed up alternate routes can be used when data packets are unable to be delivered using primary routes. The proposed technique will improve the efficiency of the network.
Black hole attacks exploit a rogue node's routing protocol to pretend to have the quickest route to the target the target node or the packet it seeks to decrypt. Although it claims the availability of new routes, this malicious node doesn't really verify its routing database[8]. To ensure that an attacker node will always be available when the route request is made, this attacker node will intercept and save the data packet it receives.
In [9], a path-based detection strategy is presented in which each node simply looks at the next hop in the current route path rather than watching every other node in the area. Extra control packets sent to identify a Black Hole assault are completely unnecessary.
One method provided in [10] proposes the technique of deactivating the reply message by the intermediary to counteract the BHA, one of several. To avoid the BH and construct a safe protocol, this approach does not need a reply from an intermediary node.
Unless RREP packets arrive from more than two nodes, the approach provided in [11,12] requires a source node to wait. As soon as the source node gets numerous RREPs, it checks to see whether there are any shared hops. If the source node discovers the shared hops, it will deem the routing safe [13]. There is a latency delay introduced by waiting for many RREPs to arrive before judging if the authentication of the node has been successful.

III. BLACK HOLE ATTACK AND CLASSIFICATION

MANETs are subject to a variety of security concerns, such as attacks aimed at disrupting the networks' regular operation. Previous chapter "Security concerns in MANET" classified these assaults based on the kind of attack they are [14]. Mobile Ad-Hoc networks node or the packet it seeks to intercept assaults known as BHA (MANET). There is information in this section on the Black Hole assault and other attacks on MANETs.

A. Black Hole Attack

BH attacks exploit a rogue node's routing protocol to pretend to have the quickest route to either the intended destination node or the targeted packet. Despite the fact that reviewing its routing database, this malicious node promotes the availability of new routes.

As a result, the attacker node will always be available to respond to the route request, allowing it to intercept and store the data packet it encounters[15,16].
As long as the network uses in the case of flooding, the malicious node's response is received before the genuine node's response, creating a malicious and forged route. Once the route has been established, the node has the option of dropping all packets or sending them to the new address.
The way a malicious node infiltrates data pathways might be any number of ways. Node "A" wishes to begin the route discovery process by sending packets to node "D." As shown in Fig. 1. So, if malicious node "C" receives RREQ packets, it will pretend to have an active route to the given destination.

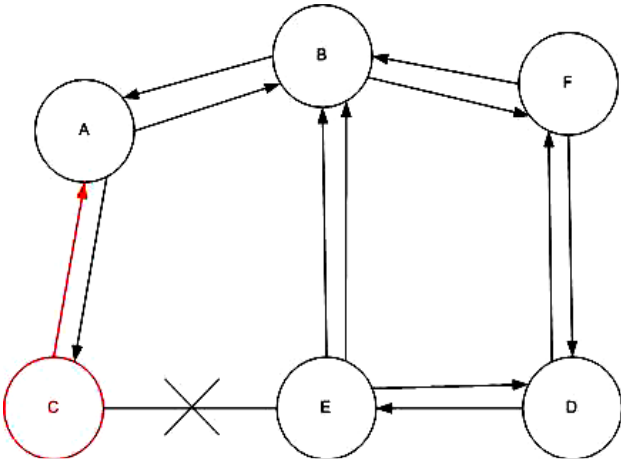

Figure. 1. Black-Hole Problem

The answer will be sent to node "A" first, before going to any other nodes. Active route discovery is accomplished when node "A" concludes that this is the active route. Upon receiving a response from node "C," node "A" will start seeding data packets to node "C." "C." will get them [17,18]. The whole data packet will be eaten or lost in this manner.
In AODV, there are two forms of black hole assault that may be stated to differentiate between them.

B. Internal BHA

There is a dangerous node within of this form, though of black hole attack that sits between the paths of the provided source and destination. TNodes on his malicious network will become active data route components. As soon as it has the opportunity [19,20]. At this point, it's capable of launching an assault as soon as the data transfer process gets underway. Because node is part of the data flow, this is an inside job. An internal assault is more difficult to detect, making it easier for the attacker to succeed.

C. External BHA

External assaults take place physically non-networked location have the potential deny transmissions over a network access, generate network blocking, or even cause the whole network to go down. They aren't, in fact. When an external attacker gains control of an inside hostile node, this is referred to as a "takeover." that node may be used to conduct attacks against other nodes in the MANET. The following are the primary characteristics of a black hole assault from the outside:

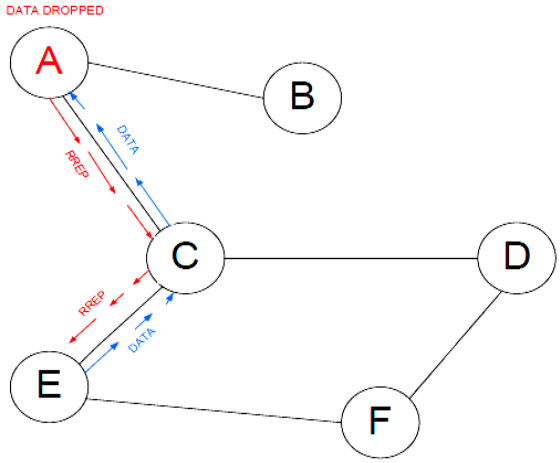

Figure.2. Black-hole attack specification

It is possible for a malicious node to discover the presently active route while also saving the destination address for future use. Sending an RREP to an unknown destination with the destination address field fudged is a bad practise. address is a rogue node's way of sending a route reply packet. Both the hop count and the sequence number have been reduced to their bare minimums. The rogue node sends an RREP packet to the next active route node in the network. Depending on if a route exists, the data may be forwarded straight to the source node. RREP packets received by the malicious node are sent over the inverted route to the next available node. The source node will be able to update the routing database on the destination node with the new information it receives in the route reply. The source node chooses a new path for choosing data since it is more direct. The rogue node will now delete anything it has access to along the way. The malicious node "A" conducts an AODV wormhole attacks in which it discovers a move in order between both the sender "E" as well as the recipient node "D."at the beginning of the assault. Node "C" sends the RREP packet to node "A," and the malicious node "A" uses it to relay the forged destination address to node "C" as soon as it gets it. It is transmitted to sender node "E" by node "C," and it is received by sender node "E." The sender will now utilise this route to deliver data to the malicious node, and data will arrive in this manner. These files will be deleted when they're no longer needed. Consequently, a black hole assault would not be possible. The sender and destination nodes will be unable to connect.

IV. BHA IN OLSR

In an OLSR wormhole attack, a rogue node selects itself as the master plan router (MPR). When an attacker node is present sends out a HELLO message, it always keeps its willingness field set to Will. In this situation, the neighbours of When an attacker node is present, that node will be designated as the MPR. As a consequence, the attacker node has access to sensitive information. access to the network, which it then uses to launch the DoS attack on other nodes.

When there are several malicious nodes between the sender and recipient nodes, the attack's impact is greatly diminished.

V. BLACK HOLE MODULE

In an ad hoc network using the AODV protocol, a Black Hole node is a node that absorbs network traffic and discards all of the packets that come through. Because of this, we included a malicious node to demonstrate the Black Hole attack.
This bad node shows Selfish behaviour, and it captures UDP packets while blocking TCP packets. Due to the receiving node's failure to provide TCP ACK, the sender node eventually realises that there is a link problem in the attack. The Black Hole may still deceive the transmitting node even if it transmits fresh TCP data packets.

VI. INTRUSION DETECTION & PREVENTION SYSTEM

As defined by the IDS community, an IDS is a set of technologies that can detect illegal or unacceptable network activity. Intrusion detection is not a stand-alone security solution, but rather a component of a larger protection system deployed around a system or device.
As a part of our simulation, we've included an IDS module that guards against Black Hole attacks when one happens to be in range. When IDS discovers that a specific path leads to a Black Hole, it immediately sends a message to the sending node instructing it to eliminate that path and look for an alternative route in accordance with IDS command.
Here, the IDS internal module just protects against malicious behaviour while also fostering reliable communication between the sender and the recipient of the message. After prevention, we discover the Black Hole node by trace analysis and ensure safe connection in the MANET environment.

VII. RESULTS AND DISCUSSION

NS-3 simulation results are the emphasis of this part, which includes an analysis of the data. Figures 3-14, show our simulated findings, which show how the network nodes change under Black Hole assault.
As a way to gauge how an intrusion-based black hole assault might behave, one used measures such as Latency, throughput, and network load are all measured for packets from beginning to finish.

A.Packet Delay from End to End

We ran two simulations to test the end-to-end latency of a packet. Routing procedures, protocols, and the number of nodes involved all have an impact on how an attack behaves. Figure.3. depicts the AODV and OLSR delays when there are 20 nodes.
In order to see the The effect of the black hole assault on the whole network is discussed below, the graph was compared to one using the usual operating protocol. When there isn't a rogue node in the network, the graph shows a longer delay.

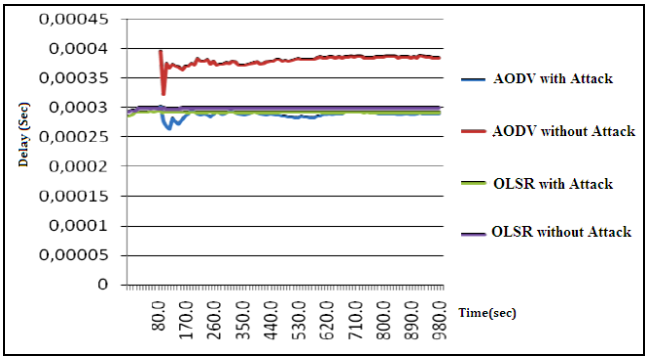

Figure. 3. Delay of OLSR and AODV (Case.1)

Similarly, if 40 nodes were inserted with the existence of a malicious node in the network, a simulation would be run. As can be seen in Figure.4. there is a noticeable delay when using 40 nodes. Similarly, when a rogue node was present, both protocols' delays were reduced significantly. AODV and OLSR were compared to see which protocol had been hit the most by the assault, and it turned out that when a smaller number of nodes (such as 20 nodes) is used, the average latency increases by roughly 5%.

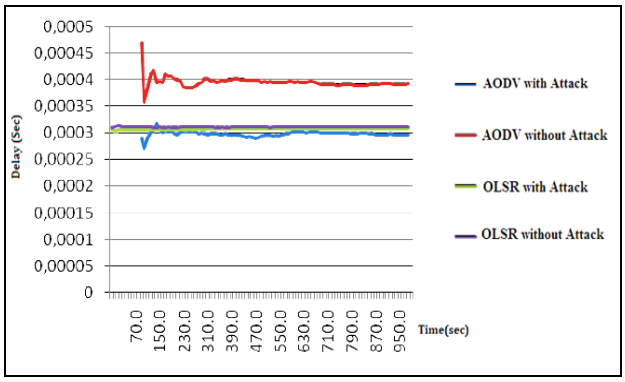

Figure. 4. Delay for OLSR and AODV (Case.2)

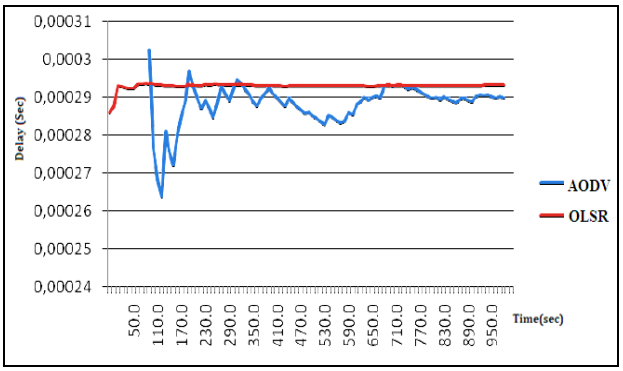

Figure.5. Delay [20 nodes] AODV vs. OLSR while being attacked

Figure.5 shows that the OLSR has a little longer delay compared to the AODV. If there are fewer nodes, this is also true. However, as the number of nodes grows, the AODV latency grows as well. This may be seen in a node graph made up of 40 different integers. Figure.6. shows that for a network of 40 nodes, AODV has a significant delay when compared to OLSR.

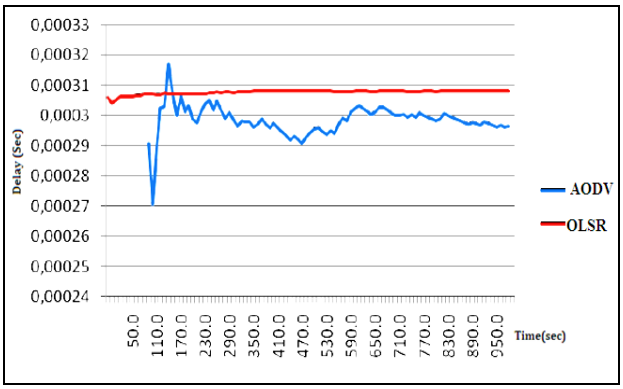

Figure.6. AODV vs. OLSR with attack [40 nodes]

Due to its table-driven design, OLSR's delay performance improves as the number of nodes increases. Routing information is kept up to date from one node to the next throughout the network.

B. Throughput

If there is no assault (no malicious node present), OLSR's throughput will be greater than OLSR's throughput while under attack (see Fig.7. for 20 nodes). As a result, there is much less routing forwarding and traffic flowing through the system. Rather of sending the data, the rogue node just discards it, slowing down overall throughput. The same is true for AODV, which has a better throughput when not under attack since the malicious node discards packets. When comparing the two protocols side by side, OLSR has a better throughput than AODV.

A similar result can be seen in Fig.8. for 40 nodes, where Because of the increasing number of nodes, throughput is great, but there is a trade-off. both attack and no-attack throughput trends are consistent with those for 20 nodes.

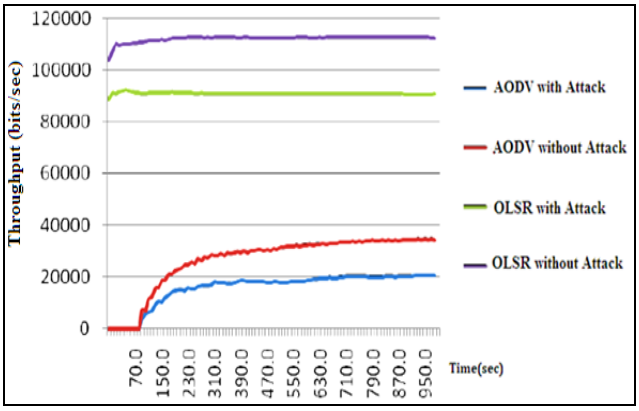

Figure.7. OLSR and AODV Throughput [20 Nodes]

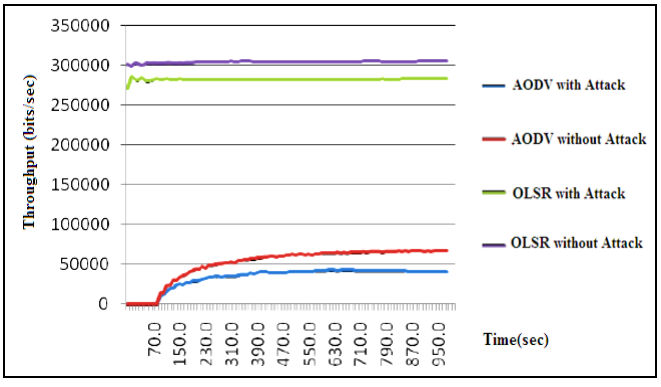

Figure.8. OLSR and AODV Throughput [40 Nodes]

As seen in Figures 9 and 10, there is a rogue node present in the network. and 10. In a regular operating protocol, the throughput of OLSR and AODV is quite high when no attacks are introduced. In the event of an attack, both protocols have significantly reduced throughput.

Similarly, when both protocols are compared to see how vulnerable they are to a black hole attack, it was shown that OLSR has a substantially greater throughput than AODV. Because OLSR is a proactive routing protocol, it first checks to see whether a routing route is available before directing traffic to it. We've found that having more sources has a smaller impact on throughput than having fewer sources. Due to the increased number of sources, there is also an increase in congestion. Overall, OLSR helps reduce latency by ensuring consistent routing patterns inside the network. A network's throughput is measured in bits of data transmitted from a source to an intended recipient in an allotted time period divided by the number of packets. Higher throughput is achieved by reducing the delay. Route reply is to blame for AODV's poor overall throughput. As soon Data is given to the malicious node as soon as the attacker node provides their route reply, the malicious node is given the opportunity to act quickly.. discards it. Because of this, the network's throughput is significantly reduced.

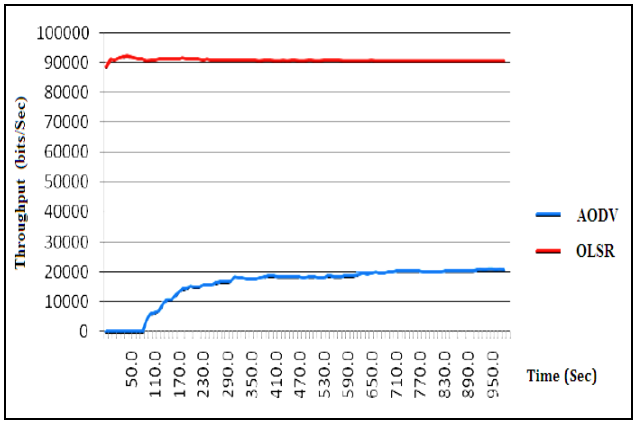

Figure.9. Throughput with assault [20 nodes]

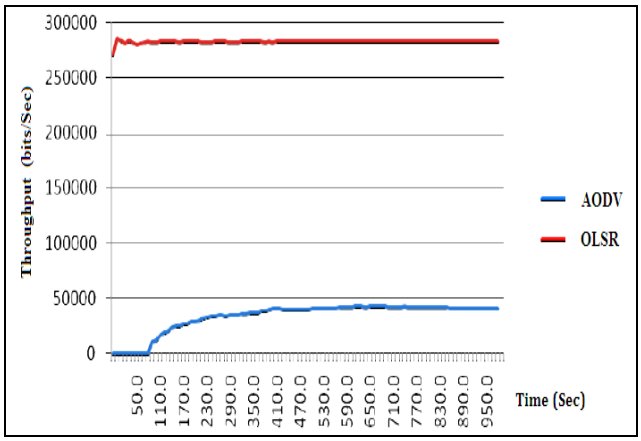

Figure.10. AODV vs. OLSR Throughput with attack [40 nodes]

For the first time, the freight on the OLSR and AODV networks was measured across 20 nodes. There were 20 nodes, and both situations were tested: there isn't a single malicious node in the network, and when there is one bad node in the network (typically functional protocol). Figures 11 and 12 show the network burden respectively, for OLSR both also with a rogue node, as well as AODV.

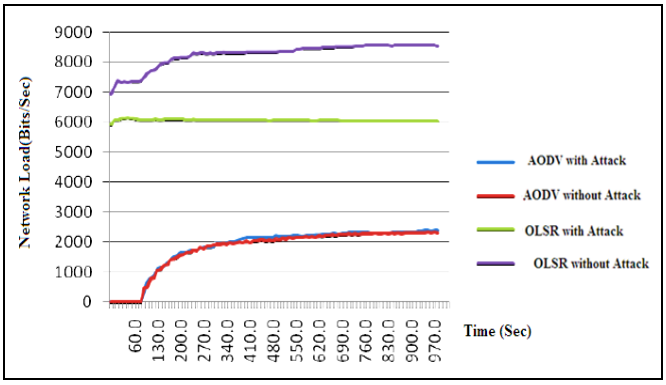

Figure.11. OLSR and AODV Network Load [20 Nodes]

According to Figure.11., when there is an assault on the network, OLSR and AODV have lower network loads. There's less network traffic since the rogue node doesn't transmit any data out into the network; instead, it just drops all of the packets it gets. OLSR's network burden is roughly three times greater in the absence of an attack, indicating that it is correctly routing its packets to their final destination, as seen in the following figure. Because of this packet rejection reduces network demand while the system is under assault. In the same graph, AODV follows the similar trend.

There is a little difference between OLSR with and without attack when there are 40 nodes. Due to the large number of nodes, routing traffic has increased. Even with 20 and 40 nodes, AODV doesn't show any changes When comparing the two protocols, it was found that OLSR has a higher network burden when there is a malicious node present (Fig. 13 and 14) than AODV. Because the routing protocols can adapt to its changes between node restart and node stopping, the OLSR network has high network load whether it includes 20 or 40 nodes. For example, at high speeds, the routing procedures need more time to change before traffic can be sent to the new routes. AODV reacts more rapidly than It gets increasingly difficult to compute the OLSR with increasing number of nodes in the network. resulting in a significant difference in network burden. With each stop and restart, the node adds to the network burden, which increases as the node becomes more stable.

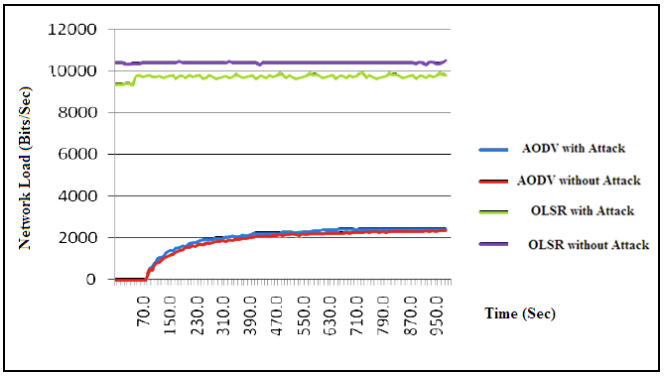

Figure.12. OLSR and AODV Network Load [40 nodes]

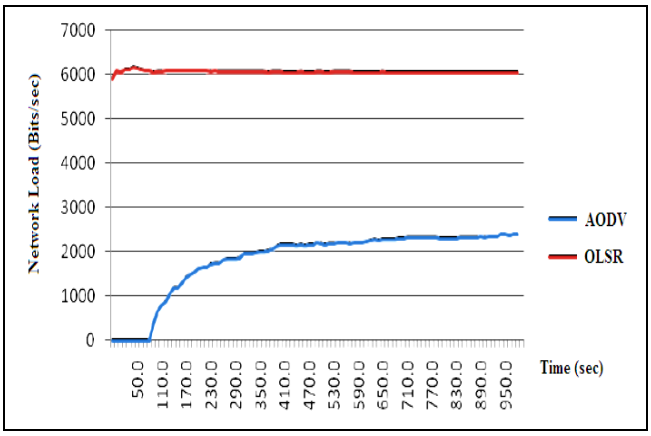

Figure. 13. AODV vs. OLSR Network load with attack [20 nodes]

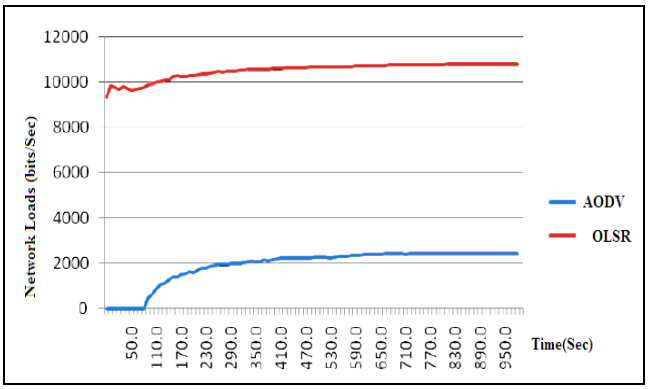

Figure.14. AODV vs. OLSR Network load [40 nodes] with attack

VIII. CONCLUSION

Traditional network infrastructure cannot be used to build Mobile Ad-Hoc Networks since they are mobile. In light of MANET's enormous potential, there are still several obstacles to be addressed. One of the most critical aspects of MANET implementation is security. We examined the Black Hole assault in four distinct situations, looking at latency, throughput, and network load from end to end as performance factors. A protocol's redundancy and efficiency in terms of security are critical in a network. Two protocols, OLSR and AODV, were examined for vulnerabilities. The effects are more severe as there are more nodes and route requests. In the case of OLSR, severances are delayed at a rate of 2 to 5 percent, whereas at an AODV rate of between 5% to 10%. When AODV and OLSR are compared, AODV has a higher throughput. two times higher with AODV. The rogue node's impact on AODV is smaller when it comes to network burden, on the other hand, than it is on OLSR. AODV was shown to be substantially MANETs as a whole are more susceptible to the Black Hole assault than OLSR, making them a greater target. We discovered that the AODV protocol is more vulnerable to an attack by a Black Hole than the OLSR protocol, according to the findings of our analysis.

Retrieval Number: 100.1/ijeat.C33410211322
DOI: 10.35940/ijeat.C3341.0211322
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. F. Taranum, A. Sarvat, N. Ali and S. Siddiqui, "Detection and Prevention of Blackhole node," *2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, 2020, pp. 1-7, doi: 10.1109/IEMENTech51367.2020.9270072.
2. D. Nitnaware and A. Thakur, "Black hole attack detection and prevention strategy in DYMO for MANET," *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2016, pp. 279-284, doi: 10.1109/SPIN.2016.7566704.
3. A. Kumari and S. Krishnan, "Analysis of Malicious Behavior of Blackhole and Rushing Attack in MANET," *2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, 2019, pp. 1-6, doi: 10.1109/ICNTE44896.2019.8946052.
4. Gajendra Singh Chandel and Rajul Chowksi, "Effect of Rushing Attack in AODV and its Prevention Technique", *International Journal of Computer Applications*, vol. 83, no. 16, pp. 0975-8887, December 2018.
5. L. Mejaele and E. Oketch Ochola, "Effect of varying node mobility in the analysis of black hole attack on MANET reactive routing protocols", *2016 Information Security for South Africa (ISSA)*, pp. 62-68, 2019.
6. Rakesh Kumar Singh, Rajesh Joshi and Mayank Singhal, "Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)", *International Journal of Computer Applications*, vol. 68, no. 4, pp. 0975-8887, April 2019.
7. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", *Proceeding of IFIP Sixth Joint Working Conference on Communication and Multimedia Security*, pp. 107-121, 2017.
8. Tarandeep Kaur and Amarvir Singh, "Performance Evaluation of MANET with Blackhole Attack Using Routing Protocols", *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 4, pp. 1324-1328, 2018.
9. Harmandeep Singh and Manpreeet Singh, "Effect of Blackhole Attack on AODV OLSR and ZRP Protocol in MANETs", *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 2, no. 3, May 2018.
10. Jeenat Sultana and Tasnuva Ahmed, "Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 6, pp. 4412-4422, December 2018.
11. Ashok Koujalagi, "Considerable detection of blackhole attack and analyzing its performance on AODV routing protocol in MANET (Mobile Ad Hoc Network)", *American Journal of Computer Science and Information Technology*, vol. 6, no. 2, pp. 25, 2018.
12. Sushil. Kumar, Deepak Singh Rana and Sushil Chandra Dimri, "Analysis and Implementation of AODV Routing Protocol against Blackhole Attack in MANET", *International Journal of Computer Applications*, vol. 124, no. 1, 2015.
13. Akhilesh Singh and Muzammil Hasan, "An Improved Mechanism to Prevent Blackhole Attack in MANET", *Progress in Advanced Computing and Intelligent Engineering*, vol. 563, pp. 511-520, 2018.
14. Guoquam Li, Zheng Yan and Yulong Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network", *IEEE Conference on Communications and Network Security (CNS)*, pp. 1-6, 2018.
15. Mohammed Imran, Farrukh Aslam Khan, Haider Abbas, Mohsin Iftikhar et al., "Detection and Prevention of Blackhole Attacks in Mobile Ad hoc Networks", *ADHOC-NOW Workshops 2014*, pp. 111-122, 2015.
16. K. Sangeetha, "Secure Data Transmission in MANETS Using Elliptic Curve Cryptography", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, no. 1, March 2019.
17. A. S. Bhandare and S. B. Patil, "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis - A Case Study," *2015 International Conference on Computing Communication Control and Automation*, 2015, pp. 301-305, doi: 10.1109/ICCUBEA.2015.63.
18. L. Tamilselvan and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET", *Wireless Broadband and Ultra Wideband Communications 2007. Aus Wireless 2017. The 2nd International Conference on*, vol. 21, pp. 27-30, Aug. 2017.
19. Zhao Min and Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", *Information Engineering and Electronic Commerce 2019. IEEC '19. International Symposium on*, pp. 26-30, 16–17 May 2019.
20. K. Lakshmi, S. Manju Priya, A. Jeevarathinam, K. Rama and K. Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", *International Journal of Engineering and Technology*, vol. 2, no. 6, pp. 444-449, 2018.

AUTHORS PROFILE

Arudra Annepu, is currently working as Assistant Professor in Computer Science & Engineering Department at the Rajiv Gandhi Institute of Technology (RGIT), Bangalore, affiliated to VTU. She is having more than 14 years of Teaching Experience. She received her Bachelor's of Technology from JNTU and M.Tech from Andhra University. She is currently a Research Scholar from RGIT Research Center. Her areas of interest are Network Security and Machine Learning. She has guided projects for B.E and M.Tech degree Students in the domain of Networking and IOT.

Dr. Priti Mishra, earned a bachelor's degree in information science and engineering from SRSIT College of Engineering in Bangalore, which is affiliated with VTU. MVJ College of Engineering, affiliated to VTU, Bangalore, and Maharaj Vinayak Global University, Jaipur, respectively, with a PG in Computer Science & Engineering and a Ph.D in Computer Science, with a focus on network security. She's been a teacher for the past 16 years. In several technological organisations, she served in various roles such as Associate Professor and Professor. She is currently employed in Rajiv Gandhi Institute of Technology, Bangalore, as a Professor in the Department of Computer Science and Engineering.