International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

Innovative Technique to Detect and Prevent Malicious Nodes in AOMDV against Blackhole Attacks in MANET for Increase the Network Efficiency

[a] **Tandu Rama Rao**
[a] Research Scholar, Department of CSE, GITAM University (Deemed), Visakhapatnam, AP, India
ramarao_tandu@yahoo.co.in

[b] **Dr. P.V. Nageswara Rao**
[b] Professor, Department of CSE, GITAM University (Deemed), Visakhapatnam, AP, India
venkatanageswararao.padmanabhuni@gitam.edu

Abstract— The Ad hoc on-demand multipath distance vector (AOMDV) routing protocol is one type of reactive routing protocol used in MANET. It is designed on top of the AODV routing protocol, so it utilizes the features of the AODV protocol. The MANET is a wireless ad hoc network without any physical infrastructure; all nodes can be moved across the network, and connections are made between them as needed simply with the help of RREQ, RREP, and RERR packets. Because the network is dynamic, nodes can quickly join and depart anytime. So far, no security threats have been caused by this feature. The blackhole attack is one type of active and dangerous attack in MANET. In this attack, the attackers use the AOMDV flaw to demonstrate their bad intent, causing data loss and decreasing network performance. Many studies have been done on various detection and prevention methods to prevent blackhole attacks. But it still goes on. To improve network performance against black hole attacks, this study offers a dynamic threshold value with multiple paths technique approach on AOMDV; it will be demonstrated in Network Simulator 2.

Keywords- *MANET, AODV, AOMDV, Blackhole attacks*

1. INTRODUCTION

The mobile ad hoc network, often known as the MANET, is a sort of mobile wireless network that is dynamic, self-organizing, and without infrastructure. Due to the network's dynamic topology and the lack of any permanent infrastructure, devices have the ability to quickly join or leave the network at any moment. In this, the nodes are free to move about and answer questions in order to locate the most efficient route for the transmission of data in the network [12]. It is of great benefit, particularly in military and rescue operations, such as after an earthquake. The MANET's router and end system is controlled by the mobile nodes themselves. There are primarily two types of attacks, which are referred to as passive and active attacks, respectively. These categories are used to classify all assaults. Although passive assaults do not disrupt the network's resources, they do compromise users' anonymity and privacy. The other one, on the other hand, causes harm to the network's resources, which in turn lowers the network's success.

2. RELATED WORKS

2.1 AODV Routing protocol:

The AOMDV is an extension of the AODV [6][11][18]and the AODV is an add-on of the DSDV & DSR routing protocols. So before discussing working behaviour of AOMDV, we need to know working behaviour of above routing protocol. The DSDV is an extension of the wired network routing protocols because, in this protocol, every node keep the entire network topology details in a table, and the routing tables are periodically exchanged between nodes for updating the routing information. So it requires high bandwidth, high power consumption, and large memory. These are the drawbacks of DSDV.

The DSR is designed to restrict the drawbacks. Means the routing table is not maintained and periodic updates are not supported. But in this protocol, each node maintains the Route cache (memory) that stores existing paths, If that existing path is not useful then it discover the path on demand, once the path is ready then it will transfer the data packets with entire path. If the attacker hacks any one of the data packets then automatically he knows the entire path. So it causes different security attacks this is the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

main drawback in DSR, it is solved by the AODV protocol. In the similar way AODV protocol is also maintain the table with existing paths.

AOMDV:

Like AODV, AOMDV also keeps track of the routing tables for existing paths. When an AOMD source wants to transfer data, it first checks its routing database to see if any legitimate existing paths are being accessed or not. Use a path if it is accessible; otherwise, it will only broadcast RREQ packets to discover the route as needed. In this regard, the intermediate nodes receive RREQ packets, So these also check their tables for the corresponding route is available or not. RREQ format in AOMDV is shown in below.

Source Identifier (SrcID)	Destination Identifier (DestID)	Source Sequence Number (SrcSeqNum)	Destination Sequence Number (DestSeqNum)	Broadcast Identifier (BcastID)	Hop Count

Figure 1. RREQ format in AOMDV

If the path is obtainable, the Reply RREP packet is sent to the source; otherwise, the RREQ packet is rebroadcast [6][10][14][18].

DestID	SrcID	DestSeqNum	Discovered Path	Hop Count

Fig 2.RREP format in AOMDV

Based on the SrcID, the intermediate node eliminates duplicate route requests [6][18]. If the link is broken at any stage then the neighboring nodes of that link send RERR packet to the end nodes of that link because in this protocol the internal path repair is not possible [6][10][11][18].

DestID	SrcID	DestSeqNum	Hop Count

Fig 3.RERR format in AOMDV

In this regard, any intermediate node gets a RERR packet then immediately erases the path information associated with it from its routing table. [6].

The AOMDV protocol has the following characteristics.

1 Link disjoint multiple paths
2 Node disjoint multiple paths

The middle nodes in link disjoint multiple paths permit duplicate RREQ packets for creating other routes from that node, broadcast the first RREQ packet and discard the remaining RREQ packets after putting their hop counts in a routing table. Up until it reaches the destination, this process is repeated at each intermediate node. It does not take the common route but uses the same node on several separate paths.. It is shown below figure 4.

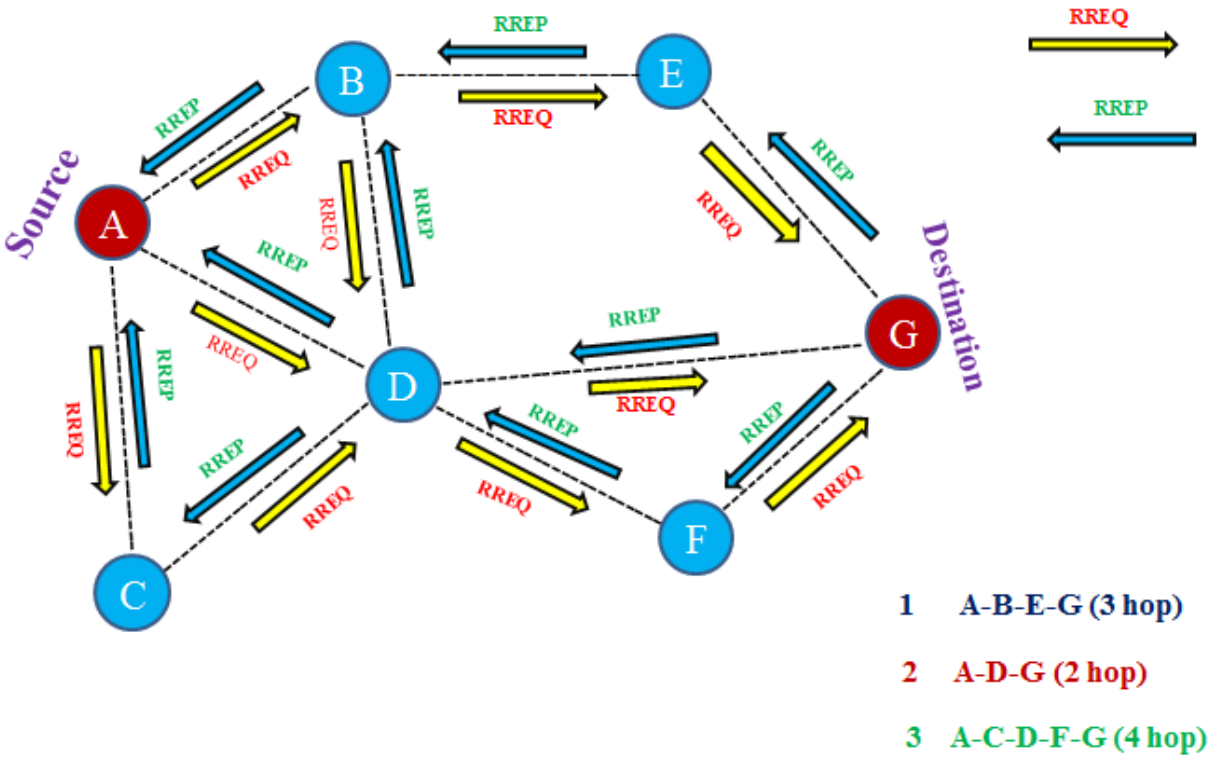

Fig 4.Link disjoint multiple paths

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

In the second characteristic, the middle nodes accept only the first received RREQ packet and forward it to only its one neighboring, which one has the shortest path. and reject the later duplicate RREQ's based on the sequence number. It is shown in below Fig 5.

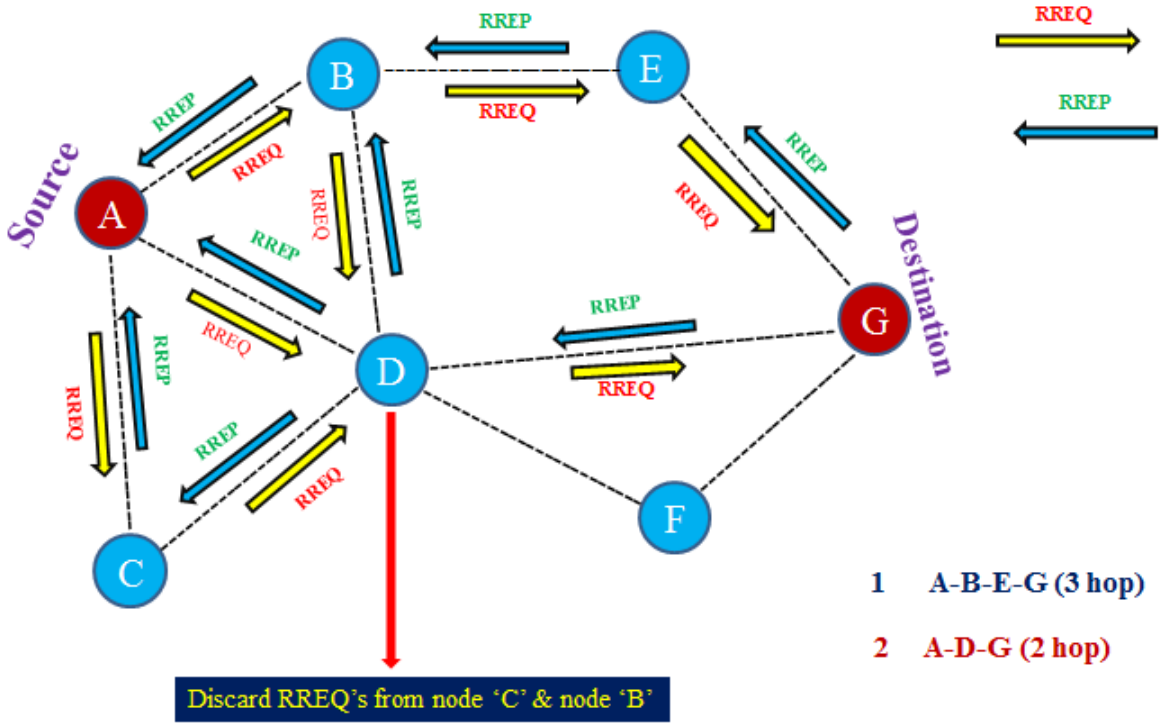

Fig 5.Node disjoint multiple paths

3. PROBLEM DEFINATION

The goal of the research is to identify and stop Blackhole attacks on MANET's AOMDV routing protocol in order to increase network efficiency and provide secure, Reliable, and confidential data transmission. The black hole attack is one type of active attack in MANET. It is launched by bad nodes. The malicious nodes in MANET also get RREQ packets during route discovery because these act as authorized nodes. so, they will send RREP packets to the source node with fictitious information about the shortest path even though it has no path to the destination [6][8][18], and then the source node will choose the shortest path RREP from a group of RREPs in accordance with the AOMDV protocol to transmit data. But a malicious node drops all data packets as it receives them, resulting in data loss. This is known as a "Blackhole attack."

Blackhole attack Types:- There are two black hole attacks in MANET [15][18].

1. Ordinary Blackhole attack: This attack is also familiar as a single Blackhole attack because it involves only single malicious node

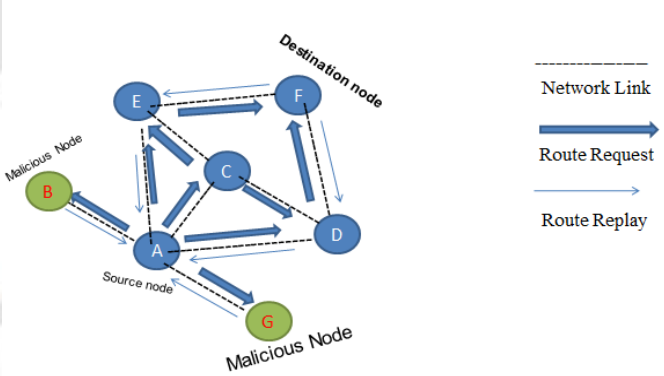

Fig 6. Ordinary Blackhole attack in AODV

In the above figure, the malicious node G instantly drops the data packets, so it causes loss of data.

2. Collaborative Blackhole attacks:- This attack involves more than one malicious node.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

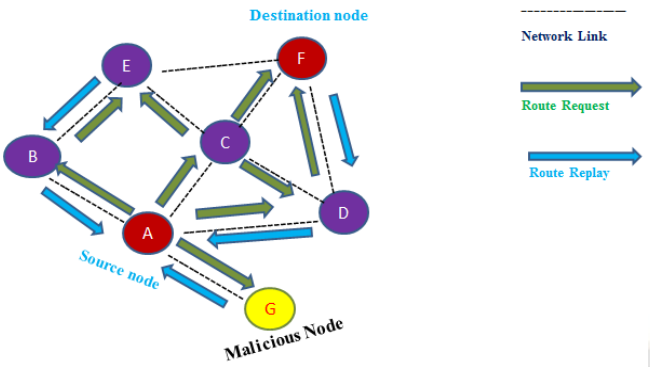

Fig 7.Collaborative Blackhole attack in AODV

Figure 7 shows how malicious nodes 'G' and 'B' are causing data loss and obstructing with communication between each other by immediately dropping data packets. Because of this, We employ a Dynamic threshold value and a number of different pathways routing strategy to solve the issue of Blackhole attacks on AOMDV in MANET. Many researchers are using numerous methods, such as [1][2][3].....[18], to detect and avoid Blackhole attacks in MANET. However, they cannot decline all activity.

4. PROPOSED SOLUTION

With our suggested novel strategy, we combine two approaches. Using a dynamic threshold value during the route discovery process, the first technique is able to identify and avoid blackhole nodes in MANET, while the second, which employs a multiple-path routing algorithm, ensures that data is transmitted securely, reliably, and in complete privacy. During the root-finding phase of a MANET, the source node employs the dynamic threshold value approach to detect and block malicious nodes (blackhole nodes). Once the pathways have been determined, the source node employs the multiple path routing technique. Blackhole attacks in a MANET may be countered with two different methods, the first of which focuses only on identifying and eliminating malicious nodes, and the second of which concentrates solely on improving the delivery rate, throughput, and elapsed time of each individual packet. Now we will see the working principle of both techniques.

4.1 Detect and Prevent BHN with DTH value

If the source node wants to send data, it will check its routing table first to find out any valid paths is available or not. If available use those paths otherwise discover the paths by broadcasting the RREQ packets. In this regard, some of the intermediate nodes have received multiple RREQ's with different id's then these nodes are also checked in's routing table to find out valid path is available or not. If available send RREP back to the origin node otherwise rebroadcast only the first received RREQ packet and discard subsequently received RREQ packets after entering the next-hop address in a routing table. This procedure is continued until to reach the destination. In this regard, the receiver node receives multiple RREQ's and transfers multiple RREP packets by using the same paths. In this regard, the intermediate nodes receive multiple RREP's. So every intermediate node uses the Dynamic Threshold value-based Technique, It involves two mechanisms such as

4.1.1 Filter Mechanism

In this Mechanism, every intermediate node detects and prevents the Blackhole nodes based on the Dynamic threshold value (DTH). It is calculated by using the multiple DestSeqNumbers from multiple RREP's.when the intermediate node receives the maximum number of ('N') RREP packets then immediately find out the dynamic threshold value (DTH) by using the following formula

$$DTH = \frac{\sum \text{DestSeqNo's of received RREP packets}}{\text{Count (Maximum number of RREP's)}}$$

Fig 8.DTH formula

After finding out the DTH value, the ode compares the DTH value with DestSequNum of the RREP packet.

RREP DestSeqNo -->DTH

Fig 9.formula for detecting Blackhole node

If the RREP packet DestSequNum is big than the DTH value then that RREP packet cre

ator node will be considered as a Blackhole node as announce a higher destination sequence number. So reject RREP packets from that node.

4.1.2 Forwarding Mechanism

After completion of the filtering mechanism, the intermediate node creates duplicate valid RREP packets based on the previous next hop's entry in a table and forward after storing the RREP information in a table. This process is continued until it reaches the origin node. So In this regard, the origin node gets multiple RREP's. The below fig shows the DTH technique.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
Article Received: 02 July 2022 Revised: 09 August 2022 Accepted: 18 August 2022 Publication: 30 September 2022

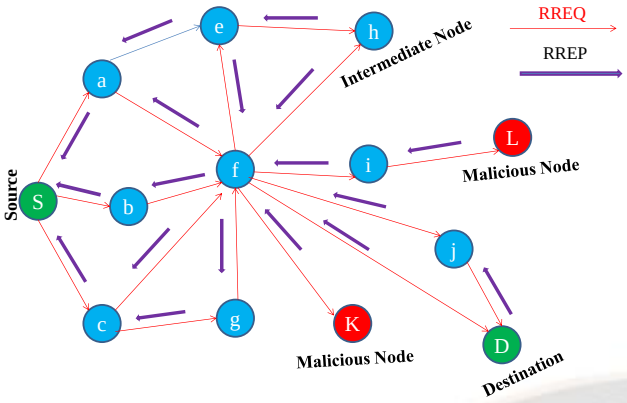

Fig 10.DTH Technique in MANET

The above example figure shows the DTH technique with filtering and Forwarding mechanisms. For example, node 'S' broadcasts the RREQ to find out the route to node 'D'. In this regard, the node 'f' receives 4 RREQ's on the same DestSeqNo. Whenever it will receive the first RREQ under the same DestSeqNo then immediately checks its routing table for any valid route is accessible or not. If available it will send RREP back to the origin node otherwise forward RREQ to the next hop's and discard other RREQ's after entering its previous node address in a table. This process is the same at every intermediate node until it reaches the destination. As per the above network, the destination node receives two RREQ's, so it will send two RREP's back. But the intermediate node 'f' receives multiple RREP's from various nodes and they are stored in a routing table until to find out the dynamic threshold value (DTH).

Table 1.Store the DestSeqNo's in a Routing Table

DestID	RREPgenID	DestSeqNo	Maxlimit for find out DTH	Dynamic Threshold Value
D	e	30	6	36.66
D	h	20		36.66
D	i	50		36.66
D	j	30		36.66
D	D	50		36.66
D	K	40		36.66

The DTH value is finding out whenever the RREP's count reaches to Max limit (n).

$$DTH = \frac{30+20+50+30+50+40}{6}$$

DTH = 36.33

Once the DTH value is found then inspect DTH and each RREP DestSeqNo. If the DestSeqNo of any RREP packet is bigger than the DTH, then that RREP packet creator node is considered as a black hole node and reject RREP's from that node and remaining RREP's are forwarded to the next hop's considered on the previous entry in a table. This process is continuing until the RREP's reach the source node[18]. This technique is only focused on detecting and preventing malicious nodes, the data transmission depends on the second technique. The working behavior is shown in below flowchart

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

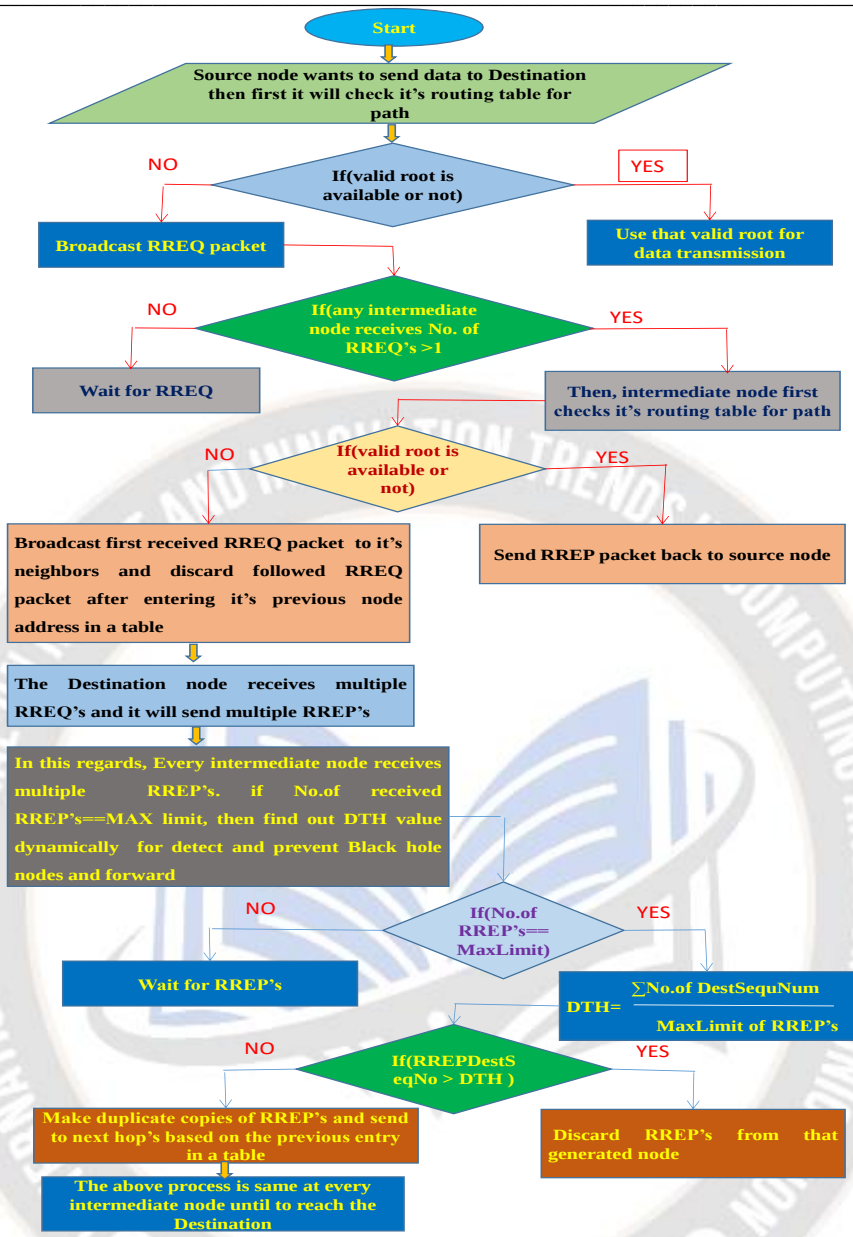

Fig 11.flow chart of Dynamic threshold value based Technique

Multiple paths Routing Technique:

Once the sender receives multiple paths then it will apply the second method, this method includes some procedure means that before transmitting the data, the sender select 'N' selected less hop count paths from multiple paths and split these paths into "P' groups, for example

Total received paths=200

Selected paths (N) =120

No.of groups (P)=6

No.of paths in each group (N/P) =120/6=20

Similarly, the origin node will split the entire data into 'Q' parts. Here split parts are equivalent to groups i.e (P==Q) and 'Q' message parts are encrypted individually with SHA (Secure Hybrid Algorithm) algorithm, This algorithm contains two levels of security, In first level, each message part is encrypted with symmetric key and in second level the generated encrypted message is again encrypted with public key of destination node then final encrypted message is generated and then it is assigned to each group. It is shown in below figure, Here

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

Total message=M

Total message is splitted into 'Q' parts

Q= {m1,m2,m3.....mQ}

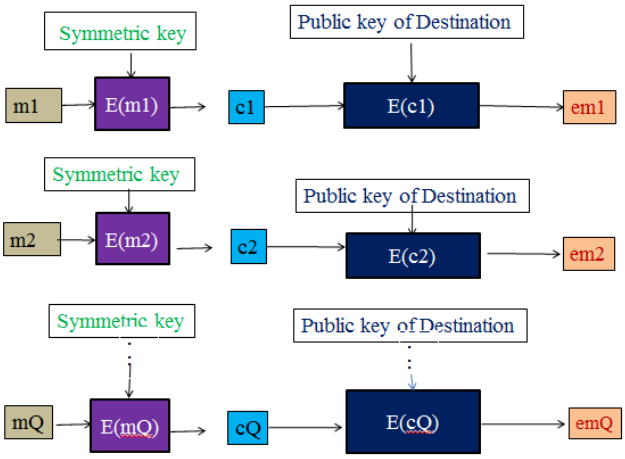

Fig 12.Encryption Algorithm

The encrypted messages are assigned to groups and create equivalent (N/P) duplicate copies of each encrypted message and flood into the group. It is shown below figure.

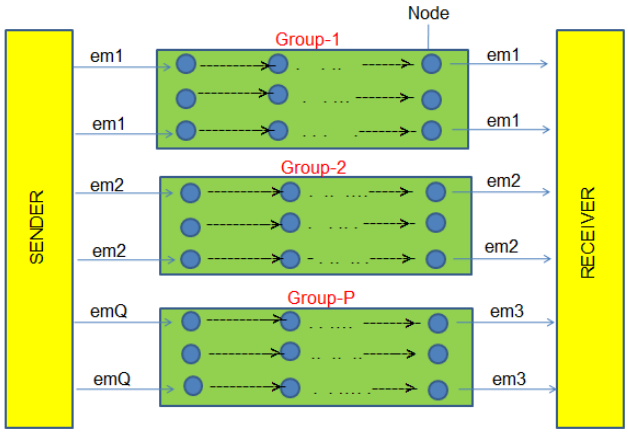

Fig 13.Multiple paths routing technique

In this technique, the same secure data is transmitted (N/P) paths in each group. So here (N/P)-1 paths in each group are affected with blackhole attack then the remaining one path is enough for transmitting that data part[18].

In this technique, the receiver will consider only the first received encrypted part of the message from each group and discard the subsequent same messages and arrange these encrypted message parts in order by using msg_split_id and apply decryption technique to these parts and then combine these parts for getting original data. It is shown below figure.

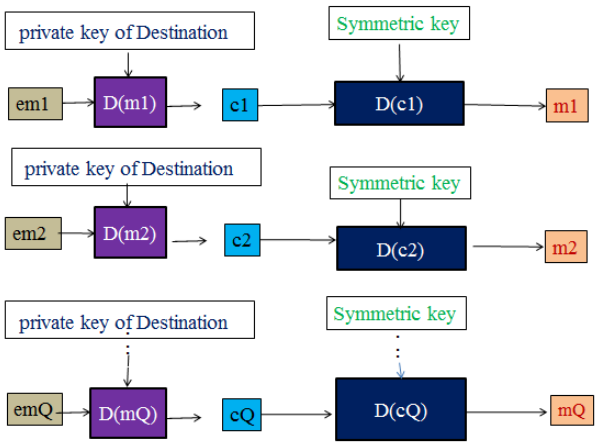

Fig 14.Decryption algorithm

M=m1+m2+.....m6

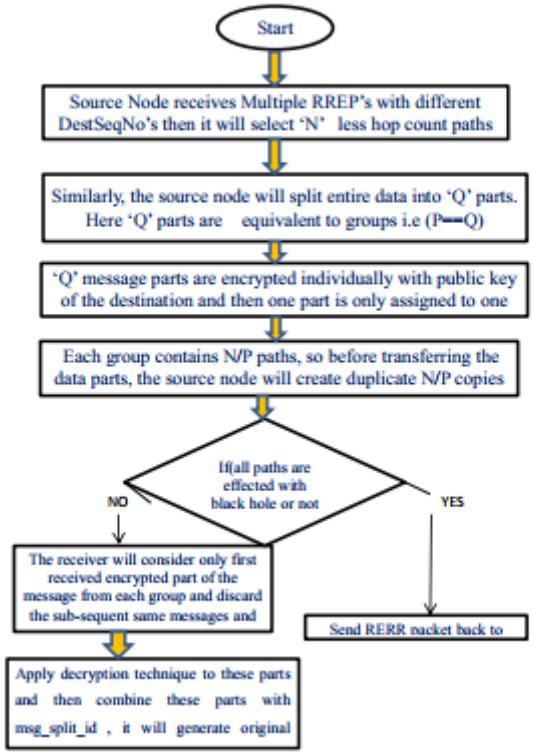

Fig 15.flow chart of multiple paths routing technique

5. SIMULATION RESULTS

Table 2 shows the available parameters for the simulation below.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

Table 2.Simulation Parameters

Simulation parameters	values
Network Simulator	NS-2.35
Simulation time	100 s
Area of Network	1186 x 584 m
kind of interface	wireless
Model of mobility	random waypoint
N.of nodes	20, 25, 30, 35
kind of flow	CBR
protocol	UDP
data packet size	512 bytes
parameter MAX rrep	6
Total black hole nodes	0, 1, 2 ……..10

PDR:

In this technique the packet delivery ratio is very high to compare with AFFAODV and AOMDV, because it uses detection and prevention technique for Blackhole attacks and uses multiple paths technique for data transmission.

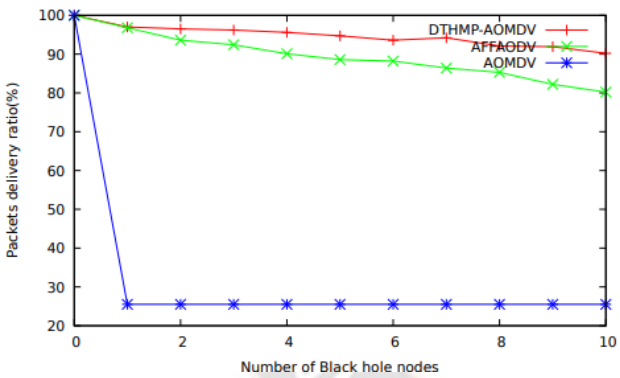

Fig 16.Packet delivery Ratio

Throughput:

In this technique the Throughput is very high to compare with AFFAODV and AOMDV, because sender uses multiple paths technique for data transmission.

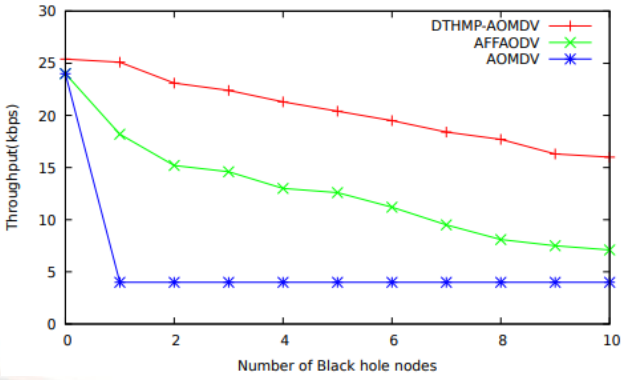

Fig 17.Throughput

Packet Loss:

In this technique the packet loss is very low to compare with AFFAODV and AOMDV, because it uses multiple paths technique for data transmission. Where as in AFFAODV and AOMDV sender uses only one path, so if any attack is occurred in this path, lose maximum number of packets.

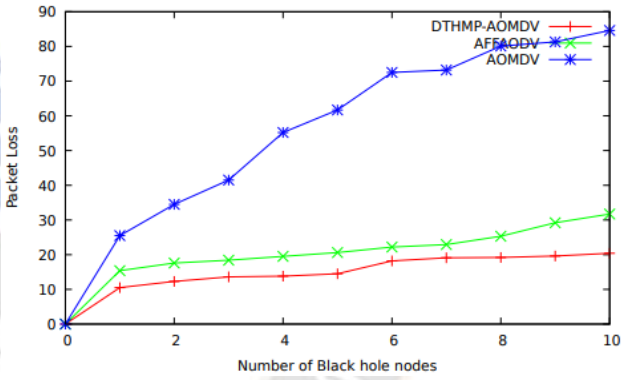

Fig 18.Packet loss

End-to-End Delay:

In this technique the End-to-End delay is very low to compare with AFFAODV and AOMDV, because it uses multiple paths technique for data transmission.

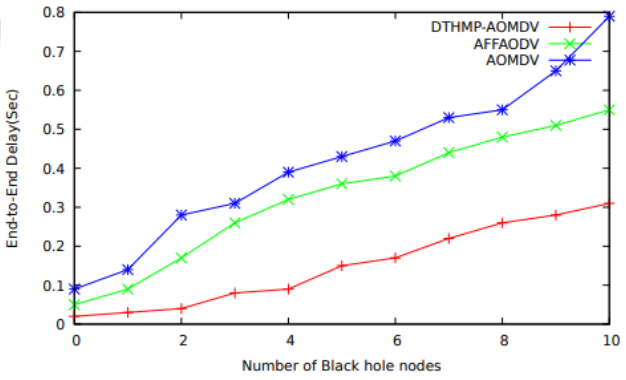

Fig 19.End-to-End Delay

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v10i9.5708
***Article Received**: 02 July 2022 **Revised**: 09 August 2022 **Accepted**: 18 August 2022 **Publication**: 30 September 2022*

6. CONCLUSION

In this paper, the DTHMP approach combines the Hybrid technique on Dynamic Threshold value-based Technique and Multiple paths Routing Technique to improve the performance of AOMDV in MANET against Blackhole attacks. The simulation results are shown in NS2. Numerous studies have been undertaken on a wide range of detection and preventative measures with the goal of preventing blackhole attacks. However, it is still going on. To improve network performance against black hole attacks.

REFERENCES

[1]. Parmjeet Chouhan and Dr. Sunil Kumar, "Enhanced Ad-Hoc On-Demand Distance Vector (AODV) Routing Protocol against Blackhole Attacks in MANET". ISSN (online): 2321-774X Volume 8, Issue 1, (IJSTM)-2021

[2]. Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development: Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 09–12. https://doi.org/10.17762/ijfrcsce.v8i2.2068

[3]. Yoshiaki Inoue and Tomotaka Kimura, " Age-Effective Information Updating Over Intermittently Connected MANETs: A Review". IEEE 2021.

[4]. Abdelaziz Tami, Sofiane Boukli Hacene, and Moussa Ali Cherif, "Detection and Prevention of Blackhole Attack in the AOMDV Routing Protocol", DOI: 10.24138/jcomss-2021

[5]. Sasmita Padhy1 , Smrutiranjan Swain2, "Novel node monitoring Fellowship Model against Black Hole Attacks in MANET", ISSN (Online): 2320-9364 ,(IJRES)Volume 8 Issue 4 ǁ 2020 ǁ PP. 06-10.

[6]. POOJA RANI1 , KAVITA, "Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network", IEEE Access- 2020.

[7]. Rama Rao Tandu, P. V. Nageswara Rao, "Node Disjoint Multiple Paths Routing Technique for Secure, Reliable and Confidential Data Transmission against Black Hole Attacks in MANET", Scopus, DOI:10.35940/ijitee 2020

[8]. A. M. El-Semary, H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map", IEEE Access-2019.

[9]. Niranjan Panda, Binod Kumar Pattanayak, "Analysis of Blackhole Attack in AODV and DSR", ISSN: 2088-8708, DOI: 10.11591/ijece-2018

[10]. Guoquan Li, Zheng Yan, Yulong Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network", IEEE 2018

[11]. Elbasher Elmahdi, Seong-Moo Yoo, Kumar sharshembiev, "Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks", IEEE 2018.

[12]. M. J. Traum, J. Fiorentine. (2021). Rapid Evaluation On-Line Assessment of Student Learning Gains for Just-In-Time Course Modification. Journal of Online Engineering Education, 12(1), 06–13. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/45

[13]. Sandeep Lalasaheb Dhende, Dr.S.D.Shirbahadurkar, Dr.S.S.Musale, Shridhar K Galande, "A Survey on Black Hole Attack in Mobile Ad Hoc Networks". IEEE 2018.

[14]. Manyi Qian, Xin Huang, Dan Tao, "Performance Evaluation of Proactive and Reactive Routing Protocols in Mobile Ad-Hoc Networks", IEEE 2018.

[15]. Swapnil P.Bhagat, Puja Padiya, Nilesh Marathe, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET", DOI 10.1007/s11276-017, Cross Mark-2017

[16]. Swapnil P.Bhagat, Puja Padiya, Nilesh Marathe, "A Generic Request/Reply Based Algorithm for Detection Of Blackhole Attack In MANET", IEEE 2017.

[17]. Mohammed Baquer M.Kamel, Ibrahim Alameri, Ameer N.Onaizah, "STAODV: A Secure and Trust-based Approach to Mitigate Blackhole Attack on AODV based MANET", IEEE 2017.

[18]. Shashi Gurung, Siddhartha Chauhan "A Review of Black-Hole Attack Mitigation Techniques and its Drawbacks in Mobile Ad-hoc Networks", IEEE 2017.

[19]. Osama, I., Rihan, M., Elhefnawy, M., Eldolil, S., & Abd El-Azem Malhat, H. (2022). A review on Precoding Techniques For mm-Wave Massive MIMO Wireless Systems. International Journal of Communication Networks and Information Security (IJCNIS), 14(1).

[20]. Dhouib, S. (2022). An Intelligent Assignment Problem Using Novel Heuristic: The Dhouib-Matrix-AP1 (DM-AP1): Novel Method for Assignment Problem. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 135–141. https://doi.org/10.18201/ijisae.2022.277

[21]. Dansika Khan, Mah zaib Jamil," Study of detecting and overcoming black hole attacks in MANET: A Review". IEEE 2017.

[22]. Rama Rao Tandu, P. V. Nageswara Rao, "AFFAODV: Accept, Filter and Forwarding Multiple RREPs Technique on AODV to Prevent Blackhole Attacks in MANET". Scopus, Vol. 29, No. 5, (2020), pp. 4660 - 4669 / ISSN: 2005-4238 IJAST 2020.