Node Disjoint Multiple Paths Routing Technique for Secure, Reliable and Confidential Data Transmission against Black Hole Attacks in MANET

Rama Rao Tandu, P. V. Nageswara Rao

Abstract: The Ad-hoc On-Demand Multipath Distance Vector (AOMDV) is an extension of AODV protocol in the mobile ad-hoc network (MANET). It utilizes the features of DSDV, DSR, and AODV routing protocols for Secure, Reliable and confidential data transmission against the attacks in the MANET, but in black hole attack malicious nodes utilize the behavior of AODV and show its malicious behavior at the data transmission, it causes the loss of data packets. So to avoid this loss more researchers have been conducted several techniques for detection and put several efforts to prevent the Blackhole attacks. But still, it is not prevented completely, so this paper proposes a Node Disjoint Multiple paths routing algorithm technique on AOMDV against black hole attacks in MANET and shows its better performance in Network Simulator (NS2).

Keywords: -MANET, DSDV, DSR, AODV, and AOMDV routing protocols, Black hole attacks, Asymmetric Key Cryptography Technique.

I. INTRODUCTION

This paper fully describes the view of my Research on AOMDV in MANET to Provide Secure, Reliable and Confidential Data Transmission service against black Hole attack and MITM attack.

The MANET is one type of Wireless network. Generally, in all wireless networks, every component that connects to a wireless network is considered as a Station, it can fall into two categories, such as

a) Access points

b) Clients

The access points are also called as Base stations and its acts as a central point to some clients and clients are also called as End stations and its activity is an end station. At present, two types of mobile wireless networks are very used in the market such as [12]

a) The fixed Infrastructure wireless Networks. It does contain fixed infrastructure between nodes like a wired network.

b) The second one is wireless ad hoc networks. It does not have any fixed infrastructure, constraining a network in an ad-hoc manner with a group of self-organizing nodes. At present several types of ad-hoc networks are used [4], the MANET is one example of this network.

MANET:-

The MANET is a Dynamic, self-organized, co-operative, wireless and infrastructure-less mobile network. In this, the nodes (Smartphones, Laptops, etc.) are moveable and have friendly nature communication means that every node is responsible to involve in operations such as to discover the route and forwarding the data packet in a network [1][4], the dynamic topology means the network topology may keep changing randomly [6]. So the devices can be freely joined in-network and quit from the network at any time. So based on the above features the MANET is very useful in different aspects, for example, military, large scale disaster areas and earthquake areas [6].

In MANET, the mobile devices are end systems and also act as a Router for data forwarding. Besides, the nodes in a MANET think that no malicious nodes in MANET due to this behavior of MANET, is particularly suitable to various security attacks than wired networks [6]. So to prevent these attacks, we may require the study of basic MANET concepts. Such as

- Attacks in MANET
- Routing Tables in MANET
- Routing Protocols in MANET

Attacks in MANET:

Generally, in MANET the security is involved in the route establishment and data transmission. These both are suitable for different attacks [1][4][6]. In MANET all the routing attacks (i.e. Routing Data manipulation attack, Replay attack, Blackhole attack, Flooding attack, Denial of service attack …etc) are main categories into two types such as Passive attacks and Active attacks. The first attack does not disturb the network services, but listen to the important information in the flow and second type disturbs the network services means degrade performance of the network [6].
This paper mainly focused on none of the well-known active attacks that is called The Black Hole attack.

Routing tables in MANET:-
Generally, the MANET has different routing protocols and some of them contain routing tables at nodes and these tables are divided into two types such as Type 1: Static tables and Type 2: Dynamic tables.

a) In static routing tables, the content is entered or updated manually.
b) In dynamic routing tables, the content is entered or updated without manually, Means automatically.

Generally, the content in the routing tables are maintained by using the following methods:

iRoute method
iiNext-Hop method
iii Host-specific method
iv Network-specific method

For example, the below network shows the content in the table based on the above methods.

![Network Specific](image)

**Figure 1. Network Specific**

| Table 1.1 Routing tables of the above device based on “Routing Method” |
|--------------------------|
| Destination | Route |
| Node B | R1, R2, Node B |
| a) Routing Table For Host A |
| Node B | R1, R2, Host B |
| b) Routing Table For R1 |
| Node B | R1, R2, Host D |
| c) Routing Table For R2 |

**Table 1.2 Routing tables of the above device based on “Next-hop Method”**

| Destination | Next Hop |
|-------------|----------|
| Node B | R1 |
| a) Routing Table For Host A |
| Node B | R2 |
| b) Routing Table For R1 |
| Node B | R1, Host D |
| c) Routing Table For R2 |

**Table 1.3 Routing Tables for Host A based on Host Specific and Network Specific method.**

| Destination | Next Hop |
|-------------|----------|
| Host B | R1 |
| a) Routing Table For Host A |
| Host C | R2 |
| b) Routing Table For Host B |
| Host D | R1 |

The above figure shows that the content of the tables is increasing or decreasing are depends on the above methods.

- Protocols in MANET:-
The MANET protocols are divided into four types depends on the following techniques.

| 1 | Depends on the Routing information update technique |
| 2 | Depends on the use of secure information |
| 3 | Depends on Routing topology |
| 4 | Depends on the Uses of specific resources |

This paper mainly concentrate on “Routing information update mechanism protocols”, because AOMDV protocol falls under this category and these can be again classified into three major categories [4] [8] [12].

1.1 Table driven Routing protocols
1.2 On-demand Routing protocols
1.3 Hybrid routing protocols.

**1.1 Table-Driven Protocols:-**
These protocols are called proactive protocols, at present many proactive protocols are available. But this paper only focused the mostly used proactive routing protocol i.e. [10] 1.1.1 DSDV (Destination Sequenced Distance Vector) routing protocol.

1.2 On-demand Protocols:-
These are called as reactive protocols, some of the protocols under this group do not use routing tables at nodes and some of them are used, where every node using “path-finding process” for finding the path. The most widely used reactive routing protocols are [10]
1.2.1 DSR (Dynamic Source Routing) Protocol.
1.2.2 AODV (Ad hoc On-demand Distance Vector) Protocol.
1.2.3 AOMDV (Ad hoc On-demand Multipath Distance Vector) Protocol.

**1.3 Hybrid Routing protocols:-**
These protocols are utilized some of the characteristics of Table driven & on-demand protocols to overcome the problems [8]. But this paper completely focused on proactive and reactive routing protocols.

**II. RELATED WORKS**
This paper working involves working of DSDV, DSR, AODV and AOMDV protocols. **DSDV**: It is one of the initially proposed protocols for ad hoc wireless networks and it is extended version of the protocol i.e. RIP. It is one of the Distance vector (DV) protocol,

**Routing Information Protocol:-**
This protocol is used to find out shortest path from the source node to all other nodes in the network by using the bellman-ford algorithm. Here each node maintains a table that holds the shortest distance to every node from that node.
This table contains three columns such as Destination, Cost (distance) and Nextnode; here we can think nodes as the famous places in an area and the lines as the roads connecting them then a table can shows minimum distance between famous places, for example, the below figure shows a network with five nodes and their corresponding tables.

![Figure 2. Routing Protocol Information.](image-url)

This protocol each node uses initialization, sharing and updating techniques to maintain the fresh topology facts in a routing table. Initially, each node routing table maintains only the distance between itself and its neighbors. The rest of the network node's distance is marked as infinity (unreachable) is shown in the below figure 3.

![Figure 3. Initialization of Tables at each node.](image-url)

In sharing technique, this protocol is sharing topology information periodically between neighbors for updating tables and this sharing is also done, if any changes are occurring in the network for updating tables. If any node gains a table from its neighbor then it generates its modified table by adding the costs between itself. In updating technique, each node comparing its modified table with its old table to generate its new table. The updating process at node A in the above network is shown below.

![Figure 4. Updating process at Node A using C’s table.](image-url)

Initially, node ‘A’ doesn’t know the path of E. But after comparison, it finds out the path of E via C in a new table. Similarly, updating is done at every node. But the problem with distance vector routing is Two-node and Three-node loop instability, for example, the below figure 5 shows the two-node instability problem.

![Figure 5. Two-node instability problem.](image-url)

These instability looping problems are solved by using the DSDV routing protocol.

**DSDV:**

In this protocol, every node also maintains the routing table and every routing table contain Destination, Next node, and Distance and Sequence number for maintaining the entire network topology information. Here the table updates and loop prevention is done based on the sequence number. The below figure 6. Shows the entire network with the Node 1 routing table.

![Figure 6. Route Establishment in DSDV.](image-url)

The initialization, sharing and updating tables are the same as RIP. Here main focus on Route establishment and maintenance in DSDV. If the nodes are moved from one place to another place then those links, either single (or) multiple links may be broken. If the link is broken then the adjacent nodes of a broken link update their routing table’s means which paths are passing through this broken link, those paths Distance values is set as infinity, the next node value is set as null and the sequence number value is set as greater than the previous one.
For example, in below figure node2 moves far away from node1 then that link will be damaged. So immediately the adjacent nodes 1 and 2 routing tables are updated, here node 1 updated table is shown in the below figure 7.

![Figure 7. Route maintenance in DSDV](image)

Here adjacent node1 knows about the damaged link, so it sets the paths via node2 as infinity and similarly node2 sets the paths via node 1 as infinity and after this updating, these tables are broadcast to its neighbors for significant changes in their routing tables and rebroadcast to their neighbors and this process is continued until the damaged link information is fertilizing throughout the network and when node5 getting a table change information from node2 then it informs their neighbors and wise versa up to all the nodes getting the new update message with higher sequence number. So this protocol needs large memory and high power consumption for multiple tables and it requires high bandwidth for maintaining the updated routing tables.

Advantages of DSDV:
1. To prevent loop infinity problems
2. Minimum delay at route setup

Disservices:
1. Requires large memory, high power, and high bandwidth
2. A heavy control overhead during high mobility

1.2. DSR:
The DSR is mainly designed to control the bandwidth means, this protocol didn't have any the routing tables and it does not need any periodic hello packet transmission, but this protocol contains the route cache (memory) at every node, it maintains the existing successful paths extracted from the data packets. These paths are used for future purpose means this information can be used during the route construction phase. In some cases, the stored valid paths can be enough for data transfer; the validity of a path is decided by a Sequence number. This protocol is found out the route before sending the data packet just like as wired network. This protocol is called “source routing protocol”. The basic approach is to establish a route only on demand by using the following control packets such as:
- Route request (RREQ) packet
- Route reply (RREP) packet
- Route error (RERR) packet

If the source wants to find out a route to the desired destination then first it checks the route cache, if the desired route is not available in its route cache then sender flooding RREQ packet in the network. If a route is available it checks the validity of a route. If it is valid using it otherwise delete that path from route cache and discover the path by flooding the RREQ packet in the network. Here each RREQ packet contains the following fields (Sequence number (Unique ID), List of connected nodes (initially empty), Source Address, and Destination Address) is shown in the below figure 8.

![Figure 8. RREQ packet format in DSR](image)

The source node generates a unique sequence number for each RREQ packet to avoid loops and duplicate RREQ packets. For example, when the source node wants to send data packets then first it checks its route cache for the desired destination path is available or not. If the path is available then use it, otherwise flooding the RREQ packet to the neighbors. Her neighbor also checks its route cache for the route, when after receiving the RREQ packet. If it has a route for the desired destination then it gives a reply to the source node by RREP packet. Otherwise, the RREQ packet is rebroadcast to its neighbors, this process is continuing until the RREQ packet is reached at the destination node. But, in this process, some of the nodes receive the same Route Request packet multiple times from multiple paths, so at that time the node considered the first received RREQ packet and the subsequent copy of the same RREQ is discarded based on the sequence number. If it is not a duplicate RREQ then simply forwarded. Here every RREQ packet carries the discovered route from source to destination. In this protocol, the destination node receives so many same RREQ packets. But destination considers only first RREQ packet and discards the subsequent copy of the same RREQ packets and sent the RREP packet back by using the same path to the source. Here the RREP packet carries an entire path from the source node to destination node. So in this regard every intermediate node, before forwarding the RREP packet back to the source first stores path information in its route cache. The RREP packet format is shown below figure 9.

![Figure 9. RREP packet format in DSR](image)
Here the source node is also stored that discovered path in its route cache and then use that path for data transmission. In this protocol, the data packet carries entire route information.

Advantages:-
1. Eliminate periodically flood table update Message (Hello packet)
2. Route cache is used to minimize the control overhead.

Dis services:-
1. It does not locally repair a damaged link.
2. More de-active paths are stored in a route Cache, it cases higher connection set-up delay than table-driven, even low mobility environment
3. Carry out the entire path in a data packet.
So, it causes so many routing attacks.

These problems are solved by using the AODV routing protocol.

1.2.2 AODV:-
It is an extension of the DSDV and DSR [12][13]. In this, every node contains a routing table and Timer just like DSDV. But, here the routing table does not maintain the entire topology information, just stores existing paths for future purpose and it’s also used to find out the next-hop information on each flow for data packet transmission. Here the existing paths are used during the route establishment phase and these are extracted from the RREP packet. The basic goal of this protocol is to establish a route only on demand. Here the source node first checks the table for any desired destination route is available or not. If any existing route is available then first use that route, if that existing desire destination path is not valid then immediately remove that path from the table and discovers the route by flooding the RREQ packet to the neighbors [13].

In this protocol, the RREQ packet carries SrcID, DestID, SrcSeqNum, and DestSeqNum, BcastID and Hop count etc are shown in the below figure 14.

**Figure 10. Format of the DSR data packet**

The route establishment in a network by using the RREQ packet shown in below figure 11.

**Figure 11. Route Establishment in DSR**

In the above figure, the source node using path is 1-3-6, because the RREP is received first in this way. If any device in the route moves away, then the link is broken, so at that time the route error message packet is generated by the adjacent nodes of the damaged link and sends to the end nodes for propagating this information [6]. In some cases, the malicious nodes also send an error message to decrease the achievement of the network [6]. The error packet format is shown below.

**Figure 12: RERR packet Format in DSR**

When the source node catches the RERR packet, then the stored corresponding path of this error packet is removed and reinitiates the route establishment procedure. This protocol allows piggybacking technique on the RREQ, the below diagram shows a broken link in the route

Advantages:-
1. Eliminate periodically flood table update Message (Hello packet)
2. Route cache is used to minimize the control overhead.

Dis services:-
1. It does not locally repair a damaged link.
2. More de-active paths are stored in a route Cache, it cases higher connection set-up delay than table-driven, even low mobility environment
3. Carry out the entire path in a data packet.
So, it causes so many routing attacks.

These problems are solved by using the AODV routing protocol.

1.2.2 AODV:-

It is an extension of the DSDV and DSR [12][13]. In this, every node contains a routing table and Timer just like DSDV. But, here the routing table does not maintain the entire topology information, just stores existing paths for future purpose and it’s also used to find out the next-hop information on each flow for data packet transmission. Here the existing paths are used during the route establishment phase and these are extracted from the RREP packet. The basic goal of this protocol is to establish a route only on demand. Here the source node first checks the table for any desired destination route is available or not. If any existing route is available then first use that route, if that existing desire destination path is not valid then immediately remove that path from the table and discovers the route by flooding the RREQ packet to the neighbors [13].

In this protocol, the RREQ packet carries SrcID, DestID, SrcSeqNum and DestSeqNum, BcastID and Hop count etc are shown in the below figure 14.

**Figure 14. RREQ packet format**
If any node receives an RREQ packet for route then checks its routing table for any valid route is available or not. If it has a valid route in the table, then it sends an RREP packet to the source node. Otherwise, it rebroadcasts an RREQ packet to its neighbors based on the routing table [5].
The validity of a route is arbitrated by comparing the DestSeqNum (Time Stamp) in a table with the DestSeqNum in the RREQ packet. If the DestSeqNum at the intermediate node is greater than the DestSeqNum in the RREQ packet, then the route is invalid in a table [7][9].

If any intermediate node receives RREQ packet multiple times, then the duplicate packets are discarding, the duplicates are identified by the BcastID-SrcID pair. This task is repeated at every intermediate node to delete the duplicate RREQ packets. Here every intermediate node takes the responsibility for entering and deleting information in a table, means that, when forwarding a route RREQ, the node enters the next-hop address, BcastID, and hop count in an RREQ packet and table, and in this protocol every node uses Timer in path establishment process means that every node set the time machine, when it forwards the route request and the node stores the previous node address and BcastID–SrcID of RREQ in a table and wait for the route replay. If the intermediate nodes receive route replay (RREP) before the timer expires then update their table with the latest route information and DestSeqNum. Otherwise, the intermediate node deletes information, which is stored in that table at route request forwarding time. In this protocol the destination node considered only first received RREQ packet and discard the subsequent received RREQ packets and send RREP packet back to the source node by using the same path, i.e., in which it receives first RREQ packet. Here RREP packet contains the entire disjoint route from source to destination [2]. Here every intermediate node stores entire path in its table extracted from RREP packet and in some cases the intermediate nodes have the desired valid route to the destination then these are also sent RREP packets to the source node. In this case, the source node receives multiple route replies. But the source node considered the first route replay for transferring the data and the source node before using that route, stores it in its table for future purpose. If the source node, no route reply is received before the timer expires, then the source node again rebroadcasts the new route request packet for constructing the path. The RREP packet format is shown below figure 15.

### Figure 15: RREP packet Format in AODV

In some cases, the link is broken at any intermediate node due to some problems or mobility then it is not repaired locally, at that time the adjacent nodes of that broken link is generated RERR packet with hop count field value is set as infinity (∞) and send it to its end nodes. It is shown below figure 16.

### Figure 16:- RERR Packet format in AODV

When the intermediate nodes and end nodes receive an error message packet, then immediately delete the route corresponding to the error message from the table and the source node re-establishing the route with new BcastID and previous destination sequence number (DestSeqNum) by rebroadcasting the RREQ Packet and this protocol always wise the neighborhood nodes through periodical hello message.

In AODV the data packet carries only data, but in DSR the data packet carries data with path information (complete path). Here AODV uses a DestSeqNumber to determine the freshness of the path (i.e., recent path), if the DestSeqNum of the currently received packet is greater than the DestSeqNum stored in the table that node then path information is fresh. So the node updates its table [5]. The below figure 17 shows route establishment in AODV.

### Figure 17. Route Establishment in AODV

1.2.3 AOMDV:-

The AOMDV is invariant of the AODV routing protocol, In this, every node maintains multiple paths during data transmission [1]. In this protocol any node contains multiple routes to the same destination then it shares its neighbors regarding route which one has a maximum hop count from multiple routes.

The main difference of AODV and AOMDV is, In AODV the destination node considers only one RREQ packet, which one arrived first and the subsequent RREQ packets under the same sequence number are discarded. But in AOMDV the destination node considers all RREQ packets and sends multiple RREP packets back to the source node by using the same paths, which means which paths are carried through RREQ packets. It uses a hop-by-hop routing approach to carry out transmission.

This protocol having the following properties such as:

1. Maintaining link disjoint multiple paths
2. Maintaining Node disjoint multiple paths
In link disjoint property, the intermediate nodes accept the duplicate RREQ packets for establishing the alternative routes from that node, but the multiple paths which are not having any common path. In this regard, every intermediate node checks the route information and Sequence number in RREQ packet to avoid the common path. It is shown in below figure 18.

Figure 18. Link disjoints multiple paths property.

In node disjoint multiple paths property, the intermediate nodes accept only first received RREQ packet and discard the subsequent duplicate RREQ packets based on the sequence number on the RREQ packet just like AODV. It maintains only a few multiple disjoint paths are shown in Figure 19.

Figure 19. Node disjoints Multiple Path.

From the above two cases, the source node selects only one path, which one having the less hop count from multiple disjoint paths for data transmission. But every intermediate node maintains the routing table for stores the existing paths and these are used at route failure. If all the routes are failing then new route discovery is needed, the route discovery process is just like AODV. The main aim of AOMDV is increases reliability and reduces conjunction.

III. PROBLEM DEFINITION
My Research Problem is To Transfer Secure, Reliable and Highly Confidential Data Transmission against Blackhole attack on AOMDV Routing protocol in MANET.

1. Description of Blackhole Attack:-
The Blackhole Attack is one type of active attack is occurred in a network by the malicious nodes because these nodes can freely join in MANET and act as Authorized nodes and utilize the loophole of the AOMDV routing protocol until to receive the data packet from the source node. For example, in MANET based on the AOMDV routing protocol, any source node wants to send data to the destination then it discovers the path by flooding the RREQ packet to its neighbors in the network. Here each neighbor receiving this RREQ packet then checks its routing table for the desired destination route, if the route is available, then the intermediate node gives replies to the source node by sending RREP packet. Otherwise, the RREQ packet is rebroadcast to its neighbors. This process is continued until to reach the desired destination. But unfortunately, in our network, some unauthorized nodes act as authorized nodes and these are called malicious nodes. These malicious nodes also receive RREQ packet from the source node and then malicious node declares it has a very shortest path (lowest hop count) to the desired destination by sending RREP packet to the source node, even though it didn’t have any path to the desired destination means it does not forward RREQ packet to its neighbors. Here based on the behavior of AOMDV protocol the source node will give the priority to the shortest path RREP packet from multiple RREP packets. In this regard the source node sends data packets to the malicious node is treated as an authorized node, herethis malicious node drops all data packets when it receives, so it causes data loss is called a Blackhole attack [3][4].

- Types of Blackhole attacks:-
In MANET Blackhole attacks are two types such as [5][8].
1. Ordinary Black hole attack
2. Collaborative Black hole attack

1. Ordinary Blackhole Attack:-
This attack is also known as a single black hole attack. In this attack, only one malicious node act as an Authorized node and claims itself is being the shortest path to the destination node. The below example is the best example of an ordinary Blackhole attack [5].

In the above figure 20, the Source node A, the Destination node F, and a malicious node are G. If node A wants to discover a route to the desired destination then it flooding the RREQ packet to the neighbors and wait for the reply. But here the malicious node G is act as an authorized node. So it receives an RREQ packet and gives a reply by RREP packet to the source node A even though it didn’t have any route to the destination node F and inform it has a very shortest path to the desired destination.
Here thenode A believes this information and sends their data packets to the node G. But when node G receiving the data packet then immediately it shows its malicious behavior means to drop the data packets, it causes data loss. This type of attack is called an ordinary Blackhole attack.

2 Collaborative Blackhole attack:
In this attack, more than one malicious nodes act as authorized nodes and co-ordinates with each other for declare itself is being the shortest path to the destination [5]. For example, in some cases, the route request is also asking the next-hop information from the neighbors for route confirmation. But in this case, malicious nodes are given information about another malicious node and communicated with each other and provide fake information. So this fake information causes data loss. This attack is called the collaborative Blackhole attack. The below figure is the best example for an attack. In this node B and node G are malicious nodes working in collaboration; actually, they didn’t have the route to the destination even though they are sending fake replays to the source node.

![Figure 21. Collaborative Black Hole Attack in AODV](image)

**IV. BACKGROUND WORK**

The so many existing techniques are introduced by many researchers to prevent the blackhole attacks in MANET such as mentioned below [3]. But still, they are not prevented completely, such as

1. Cryptography based technique
2. Overhearing based technique
3. Sequence number threshold-based technique
4. Acknowledgment-based technique
5. Clustering-based technique
6. Cross-layer collaboration based technique
7. Cross-checking based technique
8. Trust-based technique
9. IDS based technique
10. Some other techniques

**V. PROPOSED SOLUTION**

In MANET, The AOMDV is used to find out the path only based on the demand by using RREQ, RREP and RERR control packets. Here based on the nature of AODV protocol. In AOMDV, the source node considers only the first RREP packet, which one having the shortest path from multiple RREP packets for choosing the path because AOMDV protocol is advanced of AODV. In this regard, the unauthorized nodesthesia sends the RREP packet to the sender which declares the lowest hop count to the destination even though it did not have any route to the desired destination. So it causes the Black Hole attacks. But in our research, the source node considers ‘N’ number of RREP packets from multiple RREP packets, which of these contain the shortest paths. Here each RREP contains disjoint path information from source to the destination it is shown in the below flowchart 22.

![Figure 22. Route Discovery in AOMDV](image)

The main aim of ‘N’ number of Node disjoint multiple paths technique is Secure, Reliable and Confidential datagram transmission between source and destination against Black Hole attacks in MANET [1]. In this new scheme, the source node receives ‘N’ RREP packets, so it has ‘N’ node disjoint multiple paths. These ‘N’ paths are split into ‘X’ groups and each group contain ‘N/X’ node disjoint multiple paths and Similarly the sender split the entire message (M) into ‘y’ parts (m1, m2, m3….my) based on groups(y=X) and creates msg_id’s, msg_split_id’s and msg_split_id’s_sum_id for identification purpose. Here msg_id’s represent the MesSeqNumber, and msg_split_id’s represents the GroupId’s i.e groupid1, groupid2….groupidN and these are carried with data packets at transmission time [1]. Here each part of the message is separately encrypted by using asymmetric key cryptography technique and after each encrypted part is assigned to the specific group then flood it into the ‘N/X’ node disjoint multiple paths in a group.

In this new approach, the same part of the encrypted message is flooding to every node in a specific group. If any intermediate node in any disjoint path in the group shows malicious behavior (dropping data packet), then the other disjoint paths in that group are forwarded that part of the encrypted message.
In this regard the receiver will receive the so many same encrypted data packets, those are identified by msg_split_id’s. But the receiver will take only one encrypted data packet from each group and discard the remaining redundant data packets, which one contains the same msg_split_id. So that we ensure that the receiver will successfully receive all message encrypted parts with msg_id’s, msg_split_id’s and msg_split_id’s_sum_id without any loss of data. Here the full original message can be recovered by applying the decryption with asymmetric cryptography technique to each encrypted parts of the message, and then combine these parts by using msg_split_ids. For example, In my approach, the encrypted data packets are dropped in [N/X-1] paths in a group due to black hole attacks, even though the remaining one path in a group can transfer the same encrypted data packet to the desired destination, so the receiver can receive all the encrypted data packets. So based on this new approach we can send Secure, Reliable and Confidential data to the destination.

Notations:-
The notations of the new approach is shown below

M= Original Message
y= the sender split the entire message (M) Into ‘y’ parts (m1, m2, m3, m4.......my)
M=m1+m2+.......my
N= selected shortest node disjoint Paths from multiple replies
X= Number of groups
N/X= set of node disjoint Paths in each group
E (m)= Encrypted part of the message or Encrypted data packet
D (E(m))= Decrypted part of the encrypted Message

M= Original Message
y=3 (Message is split into 3 parts) M=m1+m2+m3
N=9 (select 9 shortest node disjoint paths from Total node disjoint paths)
X=3 (prepare 3 Groups)
9/3=3 (each group contain 3 node disjoint paths)
The sender encrypts each part of the message (m1, m2, and m3) with the public key of the Destination and generates the encrypted messages (em1, em2 and em3) is shown below.

Figure 24. Asymmetric Encryption

After encrypted, the encrypted data packets are assigned to each group and flood it’s into N/X groups, it is observed in below fig.

Figure 25. Encrypted data transmitted through ‘X’ groups.

When the destination node receiving these all encrypted packets then apply the decryption individually with its private key and generate the original message parts (m1, m2, and m3) is shown in below fig

Figure 26. Asymmetric Decryption
Node Disjoint Multiple Paths Routing Technique for Secure, Reliable and Confidential Data Transmission against Black Hole Attacks in MANET

\[ m_1 = D(e^{m_1}) \]
\[ m_2 = D(e^{m_2}) \]
\[ m_3 = D(e^{m_3}) \]

VI. SIMULATION RESULTS

By using NS2, the AOMDV node disjoint multiple paths approach is applied to my proposed system with unauthorized nodes. Here use 100 nodes in simulation and some of them are black hole nodes. The simulation dimensions are (552 x 552) m. The data packets are created with CBR 512 Bytes. Here mobile nodes are move without having any constraints.

To evaluate the performance with AOMDV and our new technique and observe the results in packet delivery ratio, throughput, packet loss and end to end delay.

| Table 2. Simulation Parameters |
|--------------------------------|
| Parameter                   | value                        |
| Total Number of nodes       | 100                          |
| Simulator                   | NS2(2.35)                    |
| Number of Malicious nodes   | 0 to 3                       |
| Queue length                | 40 packets                   |
| Communication area          | 250 m                        |
| Routing protocol            | AOMDV                        |
| MAC                         | IEEE 802.11.                 |
| Simulation time             | 140 seconds                  |
| Traffic rate                | 1 kbps                       |
| Interface type              | Wireless                     |
| Mobility                    | Random waypoint              |
| Propagation type            | TwoRayGround                 |
| Data Packet size            | 512 bytes                    |
| Simulation area             | 550 m x 550 m                |
| Queue Type                  | Drop Tail/priority queue     |
| Transport Agent             | UDP                          |
| Traffic Type                | CBR                          |
| Antenna Type                | Omni antenna                 |

Packet Delivery ratio (%):-

The PDR is very high in my proposed system because in existing AOMDV select only one path from multiple paths and utilized for data transmission. If one attacker is lunched in that selected path then it is more impact the data transmission, because here all the data is transmitted via this path. But no more impact is occurred, even though multiple attackers are lunched in that path because the first attacker is already dropped the data packets. But, in our proposed system, the AOMDV select ‘N’ number of active paths from the total number of multiple paths. Here any data packet is received by an attacker by using any one of the paths in a group, then the remaining paths in a group are used to transfer the data packets. If an \((x - 1)\) path in a group is attacked, then the remaining one path in a group is enough for transferring the data packets. The below fig shown a good performance of the proposed technique.

Throughput:-

In existing AOMDV the throughput is very weak because it uses only one path. If any active attacker occurs in a selected path then the throughput is zero and one advantage in the existing system that is the numbers of malicious nodes are increased, even though there is no extra impact is occur on data packets. But in our proposed system, the malicious nodes are increased means that attack on all paths in a group then only it impacts on throughput otherwise the throughput is high.

Packet Loss:-

In AOMDV, if the attackers are increased, even though it’s not affected on the packet loss because it utilizes only a single path from multiple paths. So the first attacker will create an effect on packet loss and the remaining attackers will not create any effect because all data packets are already dropped by the first attacker. But in our proposed system the packet loss is very less because here we use multiple nodes disjoint paths and these are splitting into groups and each group and all the paths in each group transfer the same data packets. So to ensure that the packet loss is very less.
End to End delay:-

It is a sum of time taken for a data packet transmission from source to destination. It includes all the delays in the network [10]. In our proposed technique the end-to-end delay is high because, here encrypted and splitting data packets are transferred.

![Figure 29. Data packets loss](image)

**Figure 29. Data packets loss**

VII. CONCLUSION

This paper intended to propose a technique against Black Hole Attacks in MANET which made secure, reliable and confidential data transmission by splitting the entire message into multiple parts based on the number of groups under asymmetric encryption crypto system. Hypothetical results shows that our proposed technique performs with better than the presented techniques. It concludes that good packet delivery is important in emergency applications in MANETs. Our proposed technique is to provide security, reliability, and confidential data packet delivery at the destination.

**FUTURE WORK**

The Research is continuing to decreasing the end-to-end delay in MANETs. With the help of modified AOMDV with a new approach and the result is executed by using NS3 Network Simulator.

**REFERENCES**

1. ElbashserElmhadi, Seong-Moo Yoo, Kumar sharshembiev, “Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks”, IEEE 2018
2. SwapnilBhagat, Puja Padiya, NileshMarathe, “A Generic Request/Reply Based Algorithm for Detection OfBlackhole Attack In MANET”, IEEE 2017
3. ShashiGurung, Siddhartha Chauhan, “A Review of Black-Hole Attack Mitigation Techniques and its rawbacks in Mobile Ad-hoc Networks”, IEEE 2017
4. Mohammed BaquerM.Kamel, Ibrahim Alameri, AmerenOnaizah, “STAOVD: A Secure and Trust Based Approach to Mitigate Blackhole Attack on AODV based MANET”, IEEE 2017
5. HoudaMoudni, Mohamed Er-rouindi, HichamMouncif, Benachir El Hadadi,” Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack”, IEEE 2016
6. HoudaMoudni, Mohamed Er-rouindi, HichamMouncif, Benachir El Hadadi, “Secure Routing Protocols for Mobile Ad Hoc Networks”, IEEE 20016
7. SinaSiahabi,MahdiehGhazvini, Mehdi Bakhtiarian, “A modified Algorithm to improve security and Performance of AODV protocol against Black hole attack”, IEEE 2015
8. Fan-Hsun Tseng, Li-Der Chou, Han-chien Chao, “A survey of black hole attacks in wireless mobile ad hoc Networks”, IEEE 2011
9. Taku Noguchi, Mayuko Hayakawa, “Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks”, IEEE 2018
10. Guoquan Li, Zheng Yan, Yulong Fu, “A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network”, IEEE 2018
11. ManyiQian, Xin Huang, Dan Tao, “Performance Evaluation of Proactive and Reactive Routing Protocols in Mobile Ad-Hoc Networks”, IEEE 2018
12. Ms.Shaveta, Mr.PawanLuthra, Er.Gagandeep, “Implementation of Blackhole Attack under AODV Routing Protocol”, IEEE 2017
13. LokeshBaghel, Prakash Mishra, MakrandSamvatsar, UpendraSingh,“Detection of Black hole attack in Mobile Ad hoc Network using AadaptiveApproach”,IEEE 2017.

**AUTHOR PROFILE**

**Rama RaoTandu,** received D.C.M.E from SBTE in 2001 and B.Tech (CSIT), M.Tech (IT) from JNT University Hyderabad in 2005 and 2010 and had 10 years of teaching experience. Currently he is Ph.D.Scholar in Computer Science & Engineering at GITAM University, Visakhapatnam.

**P.V. Nageswara Rao,** received M.Tech (CST) from Andhra University and Ph.D. from AcharyaNagarjuna University and had 25 years of teaching and research experience. Presently working as Professor, Department of CSE, GITAM University, Visakhapatnam. His research interests include Soft Computing, Bioinformatics and Computer Networks.