ISSN No:-2456-2165

Walk About Time Algorithm for Black Hole Attack Detection and Prevention in Manet with AODV Protocol

Andebet Dessiewu*
Department of Information Technology
Institute of Technology
Woldia University, Ethiopia

Tizazu Bayih
Department of Information Technology
Institute of Technology
Woldia University, Ethiopia

Semagn Shifere
Department of Computer science
Institute of Technology
Woldia University, Ethiopia

Abstract:- Mobile Ad-hoc Network (MANET) is an infrastructure less network in mobile nodes and these nodes are lightweight. In MANET nodes are vulnerable to attacks due to free movement of nodes, the dynamic nature of the network, insufficient resource, absence of authorized controlling body. In this research we develop an algorithm, walk about time algorithm, to detect and prevent one type of attack in MANET which is called black hole attack. This type of attack affects the network by dropping packets or taking packets to third parties. The malicious node acts as destination node and reply route when the source node discovers route path. Using this fake path the malicious node consumes all the packets sends for the destination nodes. The algorithm detects and prevents the black holes in MANET using Ad-hoc on Demand Distance Vector (AODV) protocol. In the algorithm, before broadcasting the Route Request (RREQ) the source node calculates walk about time to wait other Route Reply (RREP) if the one RREP reaches in the source node before the walk about time expires, this is detection scheme. Then based on the detection scheme the prevention scheme, using fake IP address the malicious node isolates from the network. The proposed algorithm is implemented using NS-3 simulation tool. This algorithm has the packet delivery ratio of 100 % for small area network and 98% for large scale network. The algorithm enhances packet delivery ratio, throughput, end-to-end delay.

Keywords:- *AODV, black hole, MANET, RREQ, RREP, walk about time.*

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a group of movable nodes that self-configure to make a temporary network without a fixed infrastructure or centralized management (S. S. Rajput and D. M. C. Trivedi, 2014). In other word MANET is collection of self-organized mobile nodes that dynamically establish infrastructure less temporary networks. A MANET have many advantages such as military service for connecting soldiers in the battlefield, robot networks, casual meeting, maritime communication, campus networks and so on (S. L. Dhende, 2018). In MANET, every node works as a client or server (router), find route, determine route and forward packets to the intended node in the network even though it is not in the transmission range of sender.

In MANETs nodes are lightweight, have small buffer, free to move and change topology dynamically. Due to this, routing is difficult as compared to wired network. So for these kind of network reactive routing protocols like DSR (Dynamic Source Routing) and AODV (Ad-hoc On-demand Distance Vector), are more suitable than proactive routing protocols. In a reactive routing protocols the route is determined if and when needed and the source initiates the route discovery. The reason they are known as reactive protocol is, they do not initiate route discovery process by themselves until they are requested, when source node request to find a route.

From thus reactive routing protocols, ad-hoc on-demand distance vector (AODV) routing protocol (Ragha, 2015) is more suitable for MANET. In these protocol the source discovers the route by broadcasting Route Request (RREQ) to its neighbors and the intermediate nodes forward the RREQ until it reaches the destination. The intermediate node constructs revers path for Route Replay (RREP). Finally, the destination node responses the RREP through the reverse path.

In AODV, the malicious node (black hole) which is an active type of attack, places itself between the communicating nodes and advertises a false shortest path from source to destination (S. Yadav, 2017). In black hole attack, each packet which is sent out from the source towards the target node is dropped by black hole node. So, a modified AODV routing protocol is needed to prevent and detect these malicious nodes. Therefor the basic aim of this paper is to develop a powerful algorithm, which is Walk about Time Algorithm, to detect and prevent black holes in AODV protocol.

II. RELATED WORK

In this section research works which are conducted by different researchers and related to this works are presented. There are a number of works which are conducted in the area of security in MANET especially in black hole attack.

ISSN No:-2456-2165

Choudhary et al. (Tharani, 2015) in 2015 proposed a timer detection mechanism for black hole. In this approach initially each node in the network assigns a maximum trust value to all its neighboring nodes. This algorithm is good for dropping attack. The limitation of this work is, in this method the node N sets timer to the actual data not for RREQ. When the trust value assigns the malicious node will act as normal and receive the trust value from the neighbor nodes. Then as node N sets timer to the actual data, this timer will used to resend the data if the data will not reach to the destination. This will create extra burden to the network. And also if the data is sensitive like military data, the attacker will use it or give to the third party.

Balachandra et al. (Shetty, 2016) proposes a secure AODV watch dog mechanism. According to the paper watchdog mechanism is an intrusion detection technique used to keep all the packets passes through the network to the destination by spotting the offending or selfish nodes and dodging them. The basic hypothesis of watchdog mechanism is overhearing, when the node gives packet to its neighbor it sniffs that weather it passes or not. In this paper, (Shetty, 2016) they use intermediate nodes as watchdogs to evaluate traffic for malicious nodes. These mechanism consumes more computation time and buffer space of the nodes.

On the other work I-Watchdog technique is proposed by Nidhi Lal, to trace malicious nodes (Lal, 2014). Here the source node sees the next node in the path about the packet by hearing to the next node's transmissions. Watchdog says the next node as a malicious node to the source node if it finds that the that next node is not forwarding the packet in a given threshold time. The benefit of the Watchdog protocol is that, they make use of only local information and are proficient to spot the malicious node. But watchdog technique has disadvantage (Lal, 2014) it decreases the network performance in terms of throughput, it does not support mobility with high number of nodes, and it doesn't detect the actual reason of the packet loss. To overcome the disadvantage of watchdog technique I-Watchdog (Improved watchdog) timer technique was developed.

III. WORKING OF AODV AND BLACK HOLE ATTACK

➢ *AODV Routing Protocol*

Ad-hoc on-demand distance vector (AODV) routing protocol (Ragha, 2015) is more suitable for MANET. It is a source initiated on-demand routing protocol. AODV constructs a route from source to destination by broadcasting route request (RREQ) message to all its neighbor nodes (H. Khattak, 2013). The intermediate nodes between sources to destination forward this message until it reach to the destination. The intermediate node also constructs a reverse path for the replay message. When destination node receives RREQ message, it sends back route reply (RREP) message to the source by using unicast method on the path constructed by reverse operation. In this way, route is established from source to destination. If any link breakage occurs between two nodes in this route, a route error (RERR) message is sent to the source informing about lost link. In such a case, source rebroadcasts the RREQ to the destination. In this way AODV discovers the shortest optimal path form source node to destination and sends the packets over this route (Tharani, 2015)

➢ *Black hole attack in AODV, MANET*

Basically, there are two kinds of attacks in ad-hoc networks, especially in MANETs (V. K. Saurabh, 2017), one is Passive attack and other is an Active attack. In first type of attack, the attacker silently listens to the network without modifying the data packets. On the other side in active attack (Noorani, 2018), attacker can alter or drop the crude data. The active attacks like Sink hole Byzantine attack, Black hole attack, Wormhole attack have great effect on the transmission of the network. Black hole attack is an active type of attack that occurs in the Reactive protocols like AODV (H. Khattak, 2013). A black-hole node locates itself between the source and the destination and attracts the packets by maliciously claiming that it has the shortest and fresh route to traverse the destination, and then drops the packets (V. K. Saurabh, 2017).

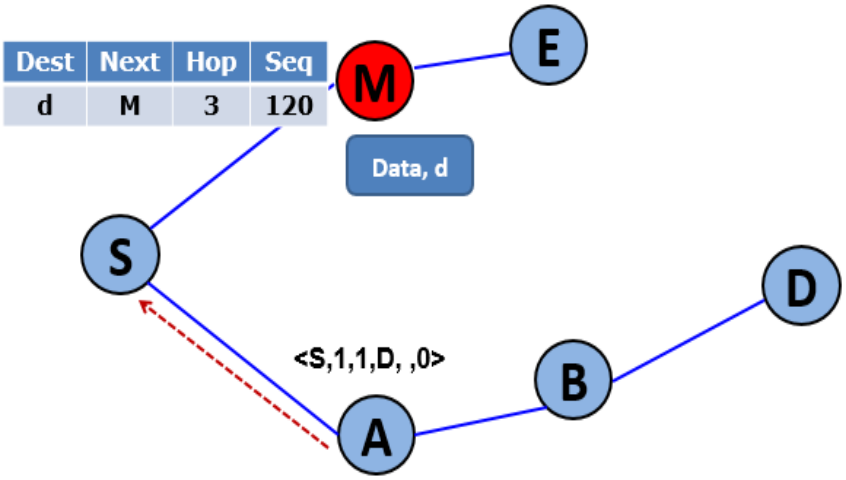


Fig 1:- Black hole attack in MANET

ISSN No:-2456-2165

As we have seen from figure 1 that the malicious node locate themselves near to the source node. When the source node S broadcast RREQ packet, then the malicious node M capture the packet and prepare false RREP packet and advertise there is a short path to the destination D through it. On that time the source node S sends the actual data to D through M, then the malicious node M drop the packet or forward the packet to unauthorized third party. This is the way how black hole attack attacks the MANET. If the number of like malicious node is more than one we call it cooperative black hole attack (Ragha, 2015).

IV. PROPOSED METHOD

The objective of this paper is to limit the effects of black hole attack on the performance of AODV. The basic idea behind the proposed technique is based on Black hole detection and prevention system.

In walk about time the source node calculates walk about time before broadcasting RREQ packet. And then it counts rrepAwt from zero and broadcasts the RREQ packet. When it receive the RREP packet it compares the rrepAwt and walk about time. If the rrepAwt is less than walk about time it will wait another RREP. In this case if other RREP reach on the source node S, the source node detects the first RREP is from malicious node and the final RREP is from destination D. In this case the source node will detect and prevent malicious nodes.

There are basic principles here. The following are principles.

- By its nature black hole nodes are near to the source nodes (by different parameters) and then it will replay the false RREP to the source node (M. Sathish, 2016), (S. Banerjee, 2014).
- This false RREP will reaches to node S before walk about time expires. In this case the source node dose not forward the exact data until timer expires.
- The RREQ must reach to the exact destination in different path before walk about time expires, then the destination node replays exact RREP.
- This RREP reaches to the source node S before timer expires. In this time two RREP reach on node S, therefore node S understand that the first RREP is from malicious nodes. Because if there is no malicious node D always replays only one RREP packet.
- Node S will notify to its neighbor that is the path to the malicious, there is a malicious node on this route path.
- If node S receives more than two RREPs it prepares fake packet and fake IP address to isolate the black hole nodes.
- Finally node S will forward the message to the destination D by the exact path.

There are parameters used to calculate walk about time. The following are parameters used to calculate it.

- Node Traversal Time: conservative estimate of the average one hope traversal time for packets and should include queuing delays, interrupt processing times and transfer times. It is denoted by “NodeTraversalTime”
  NodeTraversalTime = 40 milliseconds …….. {1}.
- Network Diameter: measures the maximum possible number of hopes between two nodes in the network. It is denoted by “NetDiameter” and measured by integer value.
  NetDiameter = 35 ……. {2}.
- Network Traversal Time: estimate of the average network traversal time. It is denoted by “NetTraversalTime” and measured by second.
  NetTraversalTime = 2 * {1} * {2} = 2 * NodeTraversalTime * NetDiameter ….{3}.
- Path Discovery Time: estimate of maximum time needed to find route in network. It is denoted by “PathDiscoveryTime” measured by second.
  PathDiscoveryTime = 2 * {3} = 2 * NetTraversalTime …… {4}.

Based on the above listed parameters, {1}, {2}, {3} and {4}, the source node calculates the Walk about Time. So, Walk about Time is the estimate of maximum time needed to wait RREP packet. It is denoted by “WalkAboutTime”.

WalkAboutTime = 2 + {4} = 2 + PathDiscoveryTime.

Pseudo code of the Walk about Time algorithm

The walk about time algorithm is an algorithm modified in AODV. It performs the process in the following way.

In the source node S,
Source node S calculate walk about time before broadcasting RREQ.
Then broadcast RREQ and count rrepAwt.
When node S receive RREP it compares rrepAwt and Walk about Time.
If rrepAwt is less than WalkAboutTime{
Node S waits another RREP.
}
Else {
Node S send message to the destination node D.}
Else If node S receive other RREP, {
Then the first RREP is from malicious node.
Source node detects black hole node.
Source node try to prevent the black hole.
}
Else If node S receives more than two RREPs{

Then node S prepares fake IP and fake packet.
Multicasts to the nodes which replays.
Isolate the black hole nodes.
}
Else {The node is normal node.}

- *Walk about Time algorithm in AODV Protocol*

In old AODV protocol the source node S initiates the route discovery RREQ and broadcasts to all its neighbors. On this time the source node only sets its TTL (Time to Live) to send other RREQ (RRREQ) if RREP is not reached to the source node S. On receiving RREQ the intermediate node looks up on the destination address of the packet to check if that is for it. If the address is not its then it broadcasts the RREQ and construct reverse path. Else it responds with route reply (RREP) to the source node S. However when a link failure occurs, a route error (RERR) message is sent to notify others about the same. On receiving a RREQ, a black hole node exploits this feature by immediately sending back a malicious RREP, having destination sequence number (DSN) set to the maximum possible value and hop count set to the minimum value and hence claims to have the freshest and shortest route to destination. Since a malicious node does not even check in its routing table, it is the first node that responds to a RREQ in most cases. Finally when the RREP reaches on node S then, node S sends the actual message through the discovered route.

In our developed algorithm when the source node initiates the route discovery RREQ it calculates the walk about time (WalkAboutTime) for the RREP. Then it broadcasts the RREQ and starts to count route reply wait time (rrepAwtTime). And the other activity is similar with the old AODV. When the route reply RREP packet is reached to the source node, then the source node compares the route reply wait time and walk about time. If the route reply wait time is less than the walk about time, then it waits other RREP. Else it sends the actual message to destination node. If the other RREP is reached to the source node S, node S checks the source address of the all RREP packets. The source address of the RREP packets will be the same or different. When the source address of the RREP packets is the same the source node sends the actual message through the last discovered route. Otherwise the source address of the RREP packets become different and the destination sequence number will also different. In this case the source node assumes there is malicious node in the network and tries to detect the black hole. As we have seen in the definition of black hole, black holes locate themselves near to the source node. Therefore node S detects the first RREP is from malicious node and detects that node as black hole node. Node S also tries to prevent that malicious node by using fake IPv4 address. The source node also will receive more than two RREPs. For this kind of condition the source node prepares fake IP address and multicasts fake packet to all the replayed nodes.

V. SIMULATION RESULT

The experiment simulations, all are carried out by keeping the number of sources constant and varying the number of black holes nodes and changing the number of nodes in the network. The number of nodes in the network topology is varying from 10 to 100 by keeping the increment 10. When varying the number of nodes, the nodes mobility is kept random between 0 to 20 m/s. And the number of malicious node is varying from.

In order to show the effectiveness and efficiency of the developed algorithm, we compare our developed algorithm and the old AODV. Why because, even if there are different researches conducted in this area, there is no acceptable and effective mechanism to detect and prevent black holes in MANET (S. L. Dhende, 2018). We compared our algorithm within old AODV in terms of packet delivery ratio, end to end delay and throughput. Table 1 is the parameters for the simulation.

No	Parameter	Value with Black hole	Value without black hole
1	Number of nodes	1,2,3,…, 7	10, 20, 30, 40, 50,…, 100.
2	Node speed		20 m/s
3	Bit rate	250 Kbps	2048 Kbps
4	Transmission power		10dBm
5	Movement model	Random	Random
6	MAC type	IEEE802.11_b	IEEE802.11_b
7	IP address type	IPv4	IPv4
8	Simulation area		400 * 600
9	Measuring parameters	TX, RX, Delivery ratio and Throughput	Total packets lost, Throughput, Packet delivery ratio
10	Traffic	CBR	CBR
11	Mobility model	RWMM	RWMM
11	Simulator	NS-3	NS-3

Table 1:- Parameters for the simulation

➢ *Effect of Number of Nodes (Network Size)*

The effect of number of nodes with-out changing other parameters in our algorithm and old AODV on the evaluation metrics (PDR, End to End Delay and Throughput) is presented below.

- ***Packet Delivery Ratio:*** the ratio of the total packets received by the destination node D without error to the total packets sent by source node S is called packet delivery ratio (PDR).

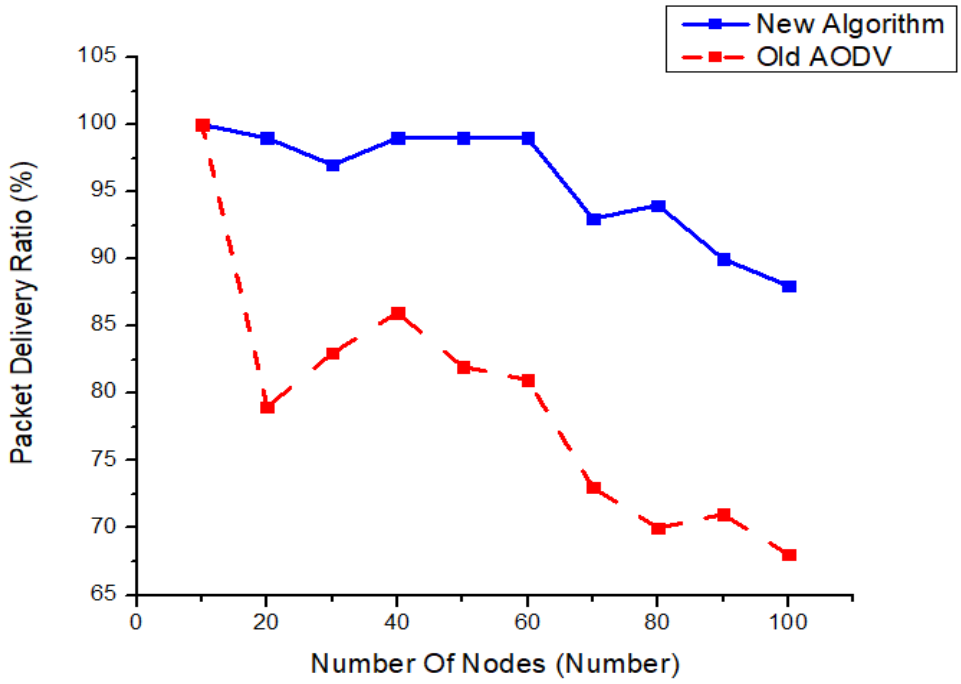


Fig 2:- Average Packet Delivery Ratio graph with increase in number of nodes

- ***End to End Delay:*** this is the time taken in which the packet takes to reach in the exact destination.

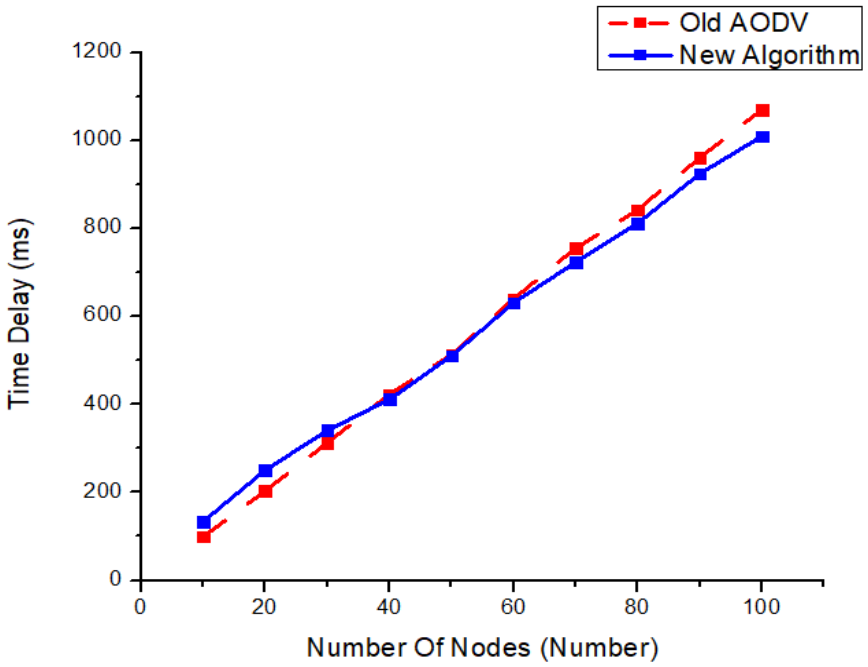


Fig 3:- End to End Delay in ms with the increasing of number of node.

- ***Throughput:*** the rate at which the information is sent in the network.

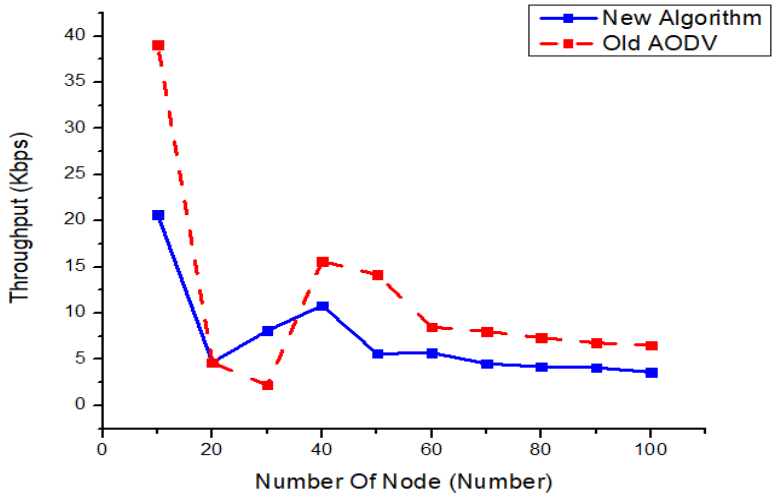
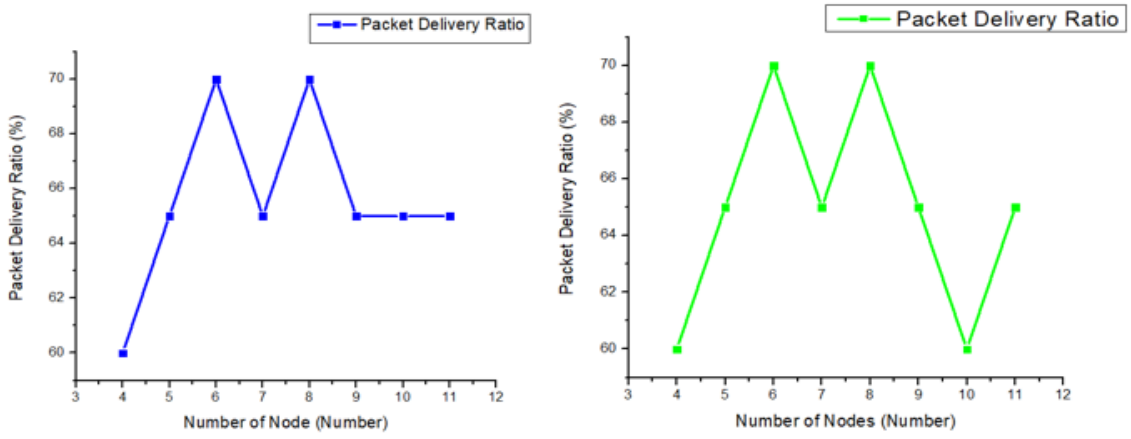


Fig 4:- Throughput in Kbps with the increasing of number of nodes

Figure 2, 3 and 4 Shows that with the increment in mobile nodes have slight effect in all PDR, End to End Delay and throughput. It increases the End to and Delay and subsequently it decreases the PDR and Throughput.

➢ *The effect of number of malicious nodes in the developed algorithm*

The effect of number of nodes is analyzed in our developed algorithm the following way. But this does not indicate the final findings of the developed result. Because in this part we want to show the ability of the algorithm to detect and prevent cooperative black holes.



A) With one black hole B) With two black hole

Fig 5:- Effect of number of malicious node in PDR

Fig 5 shows that there is no more change in throughput and PDR in the increasing of malicious nodes.

VI. CONCLUSION

The complete work concludes that walk about time algorithm helps to find an effective route between source and destination in the presence of malicious nodes in MANET on the top of AODV protocol. We can conclude from the simulation result that, as the number of malicious nodes increases the network performance decreases. Because it increases the chances that the attacker will become part of the discovered routes. In walk about time algorithm the number of malicious nodes has no great effect in network performance.

The walk about time algorithm has the packet delivery ratio of 100 % for small area network and 98% for large scale network. It has relatively small delay and 63.79% throughput as compared to old AODV. This can be interpreted as the walk about time algorithm is scalable and powerful to detect and black holes in MANET. In the future

- After replaying the RREP the destination node becomes off. We will develop a mechanism to prolong the existence of destination nodes after sending the reply to receive the actual message.
- Basically mobile nodes have low battery. So we will investigate our investigation to develop low energy consumption algorithms.
- Mostly mobile nodes are heterogynous. So it is difficult to use the same routing protocol for different functions, for example for voice data and for video data. We will develop the routing protocol used for different functions.

REFERENCES

[1]. H. Khattak, N. F. (2013). Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash. *IEEE*, 645-648.
[2]. Lal, N. (2014). An Effective Approach for Mobile ad hoc Network Via I-Watchdog Protocol. *IJAIIM*, 36-43.
[3]. M. Sathish, H. K. (2016). Detection of Single and Collaborative Black Hole Attack in MANET. *IEEE*, 2040-2044.
[4]. Noorani, H. N. (2018). A Survey on Techniques to Handle Black Hole Attack for AODV in MANET. *IJIRST*, 33-37.
[5]. Ragha, Y. G. (2015). Security Agents for Detecting and Avoiding Cooperative Blackhole Attacks in MANET. *IEEE*, 306-311.
[6]. S. Banerjee, M. S. (2014). AODV Based Black-Hole Attack Mitigation in MANET. *Springer*, 345-352.
[7]. S. L. Dhende, D. S. (2018). A Survey on Black Hole Attack in Mobile Ad Hoc Networks. *IEEE*, 1-7.
[8]. S. S. Rajput and D. M. C. Trivedi. (2014). Securing Zone Routing Protocol in MANET using Authentication Technique. *IEEE*, 872–877.
[9]. S. Yadav, M. C. (2017). Securing AODV Routing Protocol against Black hole Attack in MANET using Outlier Detection Scheme. *IEEE*, 4-7.
[10]. Shetty, B. a. (2016). Interception of Black- Hole Attacks in Mobile AD-HOC Networks. *IEEE*, 1-5.
[11]. Tharani, N. C. (2015). Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism. *SPACES*, 1-4.
[12]. V. K. Saurabh, P. R. (2017). Cluster-based Technique for Detection and Prevention of Black-Hole Attack in MANETS. *IEEE*, 489-494.