*Turkish Journal of Computer and Mathematics Education* *Vol.13 No.03 (2022), 466-487*

*Research Article*

# Mitigate Black Hole Attack Using the Reply Generation Time In MANET

**Abderraouf Ahmed [a], Tami Abdelaziz [b] , Sofiane Boukli Hacene [c]**

[a] PhD Sutdent, University of Sidi-Bel-Abbes, Department of Electronics

[b] Associate Professor University of Sidi-Bel-Abbes, Department of Computer Science

[c] Professor University of Sidi-Bel-Abbes, Department of Computer Science

Evolutionary Engineering & Distributed Information Systems Laboratory

---

**Abstract:** MANET is designed as a self-configuring and organized network of mobile nodes that use wireless links to communicate without relying on a pre-configured infrastructure or a central base station. Nodes within MANET are free to move autonomously in any direction without any constraints, so MANET has a dynamic topology. Because of its salient characteristics, MANETs are suitable for applications such as military and disaster relief. However, the characteristics of dynamic network topology, lack of infrastructure, and lack of certificate authority make the security issue of MANETs more challenging. Routing protocols in MANETs are numerous, they ensure the routing of data between nodes however they neglect the security aspect. Although the AODV protocol is one of the protocols with certain performance and low overhead making it very suitable for the characteristics of MANETs, it contains certain breaches making it vulnerable to several attacks. A common attack is the black hole attack. This paper presents a mechanism using the time required to generate the RREP packet to detect and prevent malicious nodes from performing a black hole attack. This solution provides better results with less computation and less routing overhead.

**Keywords:** MANET, routing protocol, AODV, black hole attack

---

## 1. Introduction

Mobile ad hoc network is one of the wireless network types, where mobile nodes are a self-configuration use wireless links to connect each other without relying on any pre-configured infrastructure or centralized administration. Each node in the network is autonomous therefore it can freely join or leave the network at any point of time without getting permission. MANET is multi hop networks that means the nodes that located within the transmission range of each other can communicate directly and nodes that located beyond the transmission range have to use intermediate nodes to communicate between themselves, therefore each node besides its role as a host it also acts as a router **(Mirza et al.,2018)**.

Due to its unique characteristics, MANET is suitable to provide communications in several applications, particularly in cases where it is not possible to setup a network infrastructure or where there are unpredictable dynamic topologies. Such as military applications and the emergent disaster rescue.

The topology of MANETs keeps changing rapidly due to free mobility of nodes that join and leave the network at any time. Therefore the traditional routing protocols of the wired network are inapplicable in MANET, Thus it has designed special routing protocols for MANET. Routing protocols in a MANET can be classified into three categories: reactive routing protocols, proactive routing protocols, and hybrid routing protocol. AODV is the most widely used protocol for MANETs because of its low control message overhead.

Security is one of the main issues for MANET. It is more challenging due to the lack of a central access point to monitor node behavior which can join or leave the network without authorization. Therefore MANET is very easy to break through by a malicious node to perform any type of attack. A Black Hole attack is one of the most important security problems in MANET, when a malicious node received a RREQ packet, it immediately responds by sending fake RREP to a source node with false information as though it has a fresh enough path to the destination, when a source node receives that fake RREP will believe that the generating node has a fresh route to a destination node and starts to send data through a malicious node, but this node will drop every receiving data packet instead of forwarding it to a destination node.

In this paper, we have proposed an approach to detect and isolate a black hole attack. This approach is based on the first next hop node in the reverse route to calculate the response time when receiving a RREP packet from the originator node. If the response time less than the threshold value, this first next hop node in the reverse route will consider the originator node as a black hole node then initiate the isolate process.

The rest of this paper is organized as follows. The routing protocol in MANET is presented in the following section. In Section III the AODV routing protocol is described. Section IV discussed the black hole attack mechanism. Section V reviews a few previous works that were related to our work to detect and isolate black hole nodes. Section VI presents our proposed solution, which is followed by Section VII where the results obtained from the simulation are analyzed and discussed. Finally, in Section VIII, we conclude our research work and give some suggestions for future work.

## 2. Routing Protocols in MANET

Routing Protocol performs a major role in MANET.The main function of the routing protocol in MANETs is to discover and establish routes among different mobile nodes **(Mirza et al.,2018).** Due to the highly dynamic nature of mobile nodes in MANET, which leads to frequent and unpredictable changes in the network topology that makes it a more complex and difficult task to design an efficient routing protocol for MANET. Many different routing protocols for MANETs have been developed which can be classified into three categories they are: Proactive (Table-Driven Routing Protocols), Reactive (On-Demand Routing Protocols), and Hybrid Routing Protocols **(Aluvala et al., 2016)**.

### 2.1. Proactive Routing Protocols

Are also known as table-driven routing protocols. In this type, routes will always be available on request; therefore it attempts to evaluate any changes in the network topology to be reflected by propagating updates throughout the network in order to maintain accurate information in the routing information table of each node about every other node in the network. The three popular proactive routings are protocol DSDV, WRP, and OLSR.

### 2.2. Reactive Protocol

Are also named as the on-demand routing protocol. In reactive protocols, the nodes discover the route only when it is needed. A route is discovered by initiating a route discovery process to the destination. Unlike the proactive routing, the nodes update its routing table information about other nodes only during the route discovery process. The most known examples of proactive routing protocols are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR).

### 2.3. Hybrid Routing Protocol

The hybrid routing protocol is the combination of the advantages of both proactive and reactive routing protocols to overcome the drawbacks of them such as delay and overhead problems in the network. Some examples of hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA).

## 3. AODV Routing Protocol

AODV is on demand routing, which means it initiates its routing process only when there is a node that wants to transmit the data packets and it does not have a valid route to a destination in its routing table. AODV is capable of both unicast and multicast routing(Perkins et al., 2003), also it uses destination sequence numbers to judge the freshness of routes and guarantee loop freedom. It is designed to offer quick adaptation to dynamic link conditions and also to reduce processing and memory overhead. AODV employs three kinds of control packet to discover a route to the destination node in the network route request (RREQ), route reply (RREP) and route error (RERR) packet. The processes of the AODV routing protocol to establish a route can be divided into two main phases, route discovery and route maintenance.

### 3.1. Route Discovery

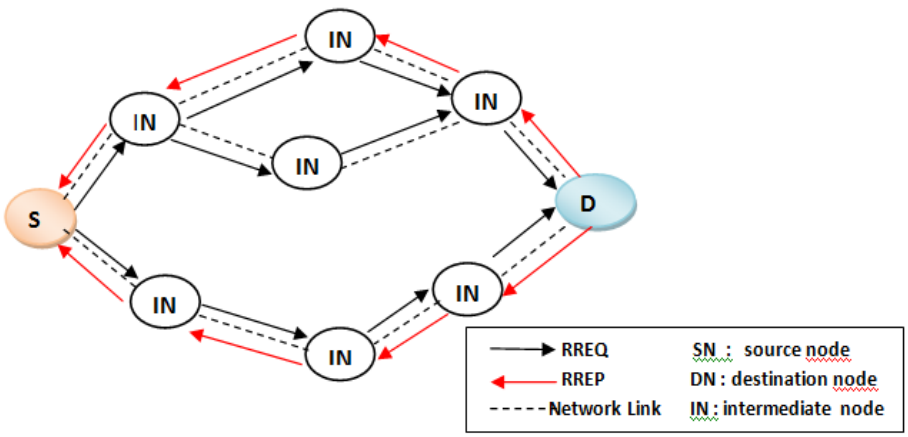
As shown in figure1, the route discovery process is started by broadcasting a RREQ over a network by a source node that does not have a valid route entry corresponding to a destination node in its routing table.

Every intermediate node receives a RREQ packet will rebroadcast and forwarded it to other intermediate nodes in the network until it reaches the destination node or an intermediate node that has a valid route to a destination node **(Perkins et al., 2003)**.

Each node when receiving the RREQ packet will create a reverse route back to the source node routing table as a new entry in its routing table or update it to correspond to the information involved in the RREQ packet if it is already an entry to a source node.

When a destination node or an intermediate node that has a valid route to a destination node receives RREQ packet (the intermediate node must have a destination sequence number greater than or equal to that included in RREQ packet ), it responds by unicast RREP packet back along the reverse route to a source node. Every node along the reverse route that receives a RREP, creates a valid route toward a destination node according to the included information in the RREP packet. At the end of this route discovery process, every node belongs to this discovered route must have a valid routing table entry to both the source node and destination node **(Arunmozhi & Venkataramani, 2012 )**.

**Figure.1.** Showing the route discovery phases



### 3.2. Route Maintenance

Due to nodes changing their places frequently may lead to a link broken during the active routes, therefore, nodes periodically send a HELLO packet to detect link breakages with neighbor nodes. In case a link break is detected for a next hop of an active route a RERR packet is sent to the nodes that belong to that active route, in order to notify that the route is not valid anymore **(Perkins et al., 2003)& (Arunmozhi &Venkataramani, 2012 )**.

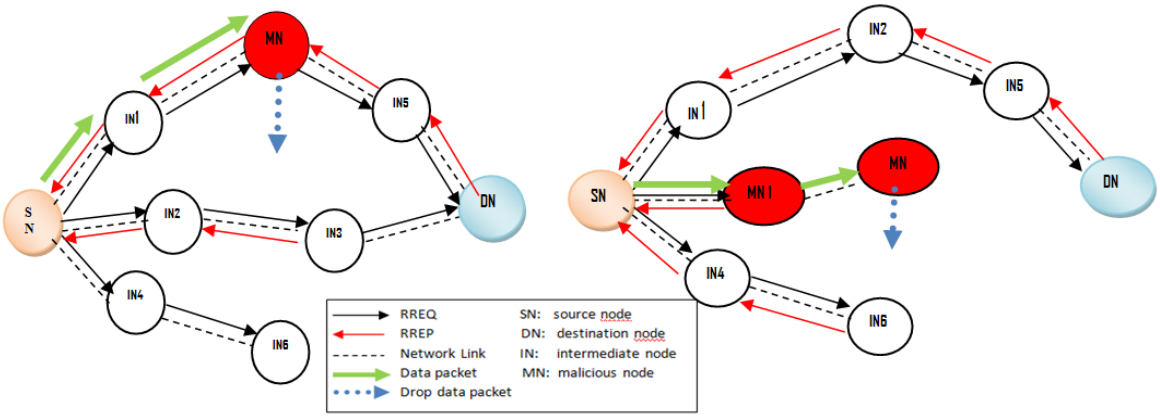
## 4. Black Hole Attack In MANET

A Black Hole Attack is a kind of active attack(Deng et al., 2002), where a malicious node absorbs all receiving data packets without forwarding them to the destination. A black hole exploits the vulnerabilities of the route discovery process of the AODV routing protocol to advertise itself as a node that has the shortest path to any request for the desired node. During the route discovery process, the source node which wants to find a path to a destination node broadcasts a RREQ packet over a network; any node that receives this request checks whether it has a fresh path to the destination node in its routing table. When a black hole node receives this request without checking its routing table it responds immediately by sending a fake RREP with the largest destination sequence number and smallest hop count in order to attract a source node to choose the path that passes across the black hole node as the shortest path to the destination node and ignore other RREP messages from other nodes, consequently, all the data packets will pass through Black hole node which will drop them instead of forwarding them to the destination node **(Sharma et al., 2012 )**.

### 4.1. Black Hole Attack Taxonomy

Based on the number of attacker nodes that perform and share in the attack, the black hole attacks are classified into two types(Khan et al., 2017): single and cooperative black hole attacks, where a single black hole attack Figure 2:A, the attack launched only by one attacker node. While in a cooperative black hole attack Figure 2:B, there are two or more black hole nodes that collaborate in order to degrade the network performance.

**Figure.2.** Showing the black hole attack classification




*A) Single black hole* *B) Cooperative black hole*

## 5. Related Works

**Imran, M., Khan, F. A., Abbas, H., & Iftikhar, M.(2014)** have proposed a system called (DPS) to detect and isolate a black hole attack in a network. This system is based on some nodes that continuously monitor the behavior of their neighbors to maintain an analysis DPS table, these tables contain information about node's status, this status change whenever a DPS node receives a RREQ or RREP from a corresponding node. If a suspicious node is confirmed as a malicious node the DPS node will broadcast a block message containing the ID of the black hole node. when normal nodes receive a block message from a DPS node add malicious node ID into their block lists. All packets received from the malicious nodes which belong to the block list will be dropped in order to isolate a black hole attack. This proposed solution shows there is none of routing overhead and delay in transmission. Furthermore, the improve performance metrics such as the throughput of the network by reducing the packet drop rate.

**Arathy, K. S., & Sminesh, C. N (2016)** proposed the D-MBH( Detection of Multiple Black hole Attack) algorithm in order to detect a single and cooperative black hole attack. it requires adding three elements. The first is an additional route request broadcasted without target address, the second is a threshold value represented as the average of Destination Sequence Number (ADSN) of all malicious RREPs received, whereas the third element is represented by creating two lists (BH list and CBH list ), the black hole list update only when a node receives RREP packet originated by node had received a fake RREQ packet included nonexistent target address. and the list of collaborative black hole node (CBH list) used when the proposed D-CBH (Detection of Collaborative black hole attack ) algorithm invoked, this algorithm starts when a node receives an RREP from a node that already identified in black hole list, in this case, the source node will check whether a Next Hop Node (NHN) of a node that sends RREP (RREPN) is in BH list. If yes, then the RREPN can be considered as a malicious node acting in collaboration with NHN. As a result, this proposed approach leads to reduction in routing overhead and computational overhead. However, it does not provide improvement in storage overhead.

**Al-Shurman, M., Yoo, S. M., & Park, S (2004)** have proposed two solutions to a black hole problem in the network. In the first solution, a source node seeks to find a safe route to the destination (using redundant paths bases ) through discovering more than one route. In this solution source nodes wait to receive a different RREP packet from more than two nodes, the source node selects a route that has some shared hope or nodes between routes as a safe route. This solution appears to perform best securely but may be suffering from a longer delay.

In the second solution, every node must record the sequence number of the last packet that it has received or sent in order to compare it with the next packet sequence number received from the same originator; therefore every node in the network must add two additional small sized tables. when a RREP sent by an intermediate node that has a route or by a destination node itself to a source node, must this RREP packet contain the last packet's sequence numbers that received from this source This solution provides a quick and reliable way to detect a suspicious reply without increasing overhead but the attacker node can overhear to the channel and update its tables according to listened information.

**Deshmukh, S. R., Chatur, P. N., & Bhople, N. B (2016)** proposed a solution for detect and eliminate both single and collaborative black hole attacks in the premature steps of route discovery through slight changing in RREP packet by adding a new field bit for validity value, which keeps the basic mechanism of AODV unchanged. The additional field bit will be set only by the node that has a legitimate route or destination node itself, but if RREP is generated by a black hole node the validity bit will have null value because a black hole attack is uninformed about mechanism. Each intermediate node receiving a route reply RREP packet will check if the validity bit in that RREP is set before forwarding it to the next hop; otherwise, it will drop that RREP without making entry in the route table. The detection and prevention black hole attack before starting the data transmission leads to reduce requirement processing and memory.

**Su, M. Y (2011)** have deployed IDS (intrusion detection system) nodes to detect and isolate black hole attacks. An IDS node monitors all nodes that are inside its transmission range by recording a number of broadcasted RREQs, and the number of forwarding RREQs. To judge if any node is a black hole the IDS node uses a suspicious value by computing the difference between RREQs and RREPs transmitted from the nodes that are within its transmission range. If a node's suspicious value reaches the predefined threshold value, it is considered as a black hole node and broadcasts a block message to give notice to all nodes on the network to isolate and block this malicious node.

**Shahabi, S., Ghazvini, M., & Bakhtiarian, M (2016)** in order to enhance the security of AODV routing protocol they proposed a new algorithm to detect malicious nodes called intrusion detection system new AODV algorithm (IDSNAODV). They have improved IDSAODV by introducing some rules that allow identifying the destructive nodes. This algorithm makes nodes pay more attention to the behavior of their neighbor nodes in the Network. To identify a destructive nodes and put them into the quarantine, the source node have follow the following rules.

The node which generates a RREP with the greatest sequence number and lowest number of hops in RREP may be a destructive node, or the node receives a considerable number of packets but only sends one packet may be a malicious node. As for the node which receives some packets but does not send them to its neighbors that node is considered a destructive node. Through the simulation result, turns out that the IDSNAODV provide a higher PDR and throughput than AODV and also the result showed a considerable decrease in the number of dropped packets and end-to-end delay.

**Tan, S., & Kim, K (2013)** to prevent a black hole attack in MANET they proposed a new mechanism called Secure Route Discovery for AODV-based MANET (SRD-AODV). This mechanism requires modifications in the standard AODV protocol by defining three thresholds. This mechanism urges the source nodes to use the defined thresholds to judge the multiple RREP messages received from intermediate nodes or destination nodes. The source node compared the defined threshold with the destination sequence number (D_Seq) in each RREP message, If the D_Seq in the RREP message is greater than the defined threshold (TH), the source node Considered this node which generates this RREP message to be a black hole node then discards this packet. Else, a route is created between the source node and the destination node.

As the result, the SRD-AODV mechanism showed that greatly increases in packet delivery ratio for three types of environments in the presence of black hole attacks in the network, but on another hand, the SRD-AODV mechanism adds new processes and calculations that maybe lead to an increase in delay and overhead.

## 6. Proposed Approach

In this approach, Every node that be located as the first next hop in the route inverse toward the source node when receives the RREP packet from the originator node must calculate the reply time for RREP packet and compare it with The average of the amount of time (threshold) required for a node to generate and traverse a packet between it.

According to a route discovery process, each intermediate node that receives the RREQ packet must follow the following processes.

First it checks whether it is the destination for this packet. If it is not the destination, it verifies in its routing table whether it has a valid route to the destination. If not, it creates the inverse route to the source node and rebroadcasts the RREQ packet to its neighbors. In case it has an entry corresponding to the destination in its routing table, it should compare its destination sequence number to the destination sequence number involved in the RREQ packet. If the destination sequence number present in the routing table is greater than or equal to the one contained in the RREQ, this node will generate a RREP packet and unicast it to the source node through the inverse route. All these processes of checking, updating, and comparison make the time reply of this node larger than a black hole node which immediately sends back an RREP packet to a source node, with the largest destination sequence number and smallest hop count . For that, we'll find always the time of reply of the black hole node is lesser than the time of reply of the normal intermediate nodes, in our propose we have used this idea to detect a black hole attack according to the amount of time required to generate an RREP packet so in this solution all nodes perform as monitoring to its neighbors, therefore the first next hop when received RREP packet should calculate the reply time for node that generates this RREP packet and compare it with the average value (threshold) if reply time value is lower than the threshold value then the monitoring node will consider this node as a black hole an alarm packet is broadcast over the network with indicating the IP address else it will send to a next hop node via a source node

Replay time = current _time ( received time ) - time_stamp ( sending time)

### 6.1. Algorithm

// IN :intermediate node

// FNHN : first next hop node

// RT : replay time

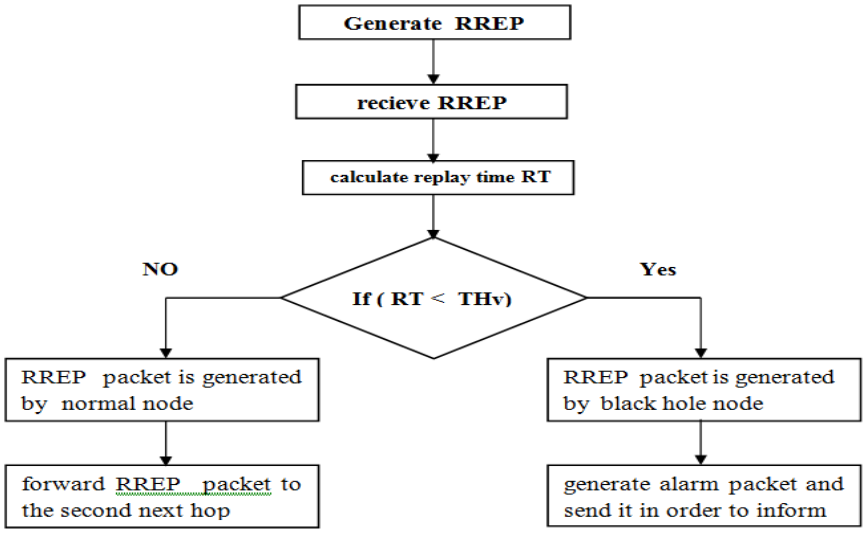
// THv : threshold value

```
1. IN generate RREP Packet
2. FNHN recieve RREP
                // calculate replay time
3. RT=  current _time - time_stamp
4. If ( RT <  THv)   then            /* RREP  packet is generated
   by  black hole node */
```

```
5.       Discard RREP packet
6.       generate alarm packet and send it in order to inform
7. Else  If ( RT > THv) then       /* RREP   packet is generated
   by  normal node */
8.           forward RREP  packet to the second next hop
```

### 6. 2. Organigram

**Figure.3.** Showing the flowchart of the proposed solution




### 7. Performance Evaluation and Result Discussions

To demonstrate the performance of our proposed solution, we implemented and performed our proposed mechanism using the popular network simulator (ns 2.35). The simulation consists of three scenarios AODV without black hole attack, AODV under black hole attacks, and AODV enhanced by our proposed solution.

#### 7.1. Simulation Parameters

We use a random pattern of node mobility, where each node can move randomly in an area of 1500m_300m. The simulation time is 900 seconds, the pause time varied as (0s, 30s, 60s, 120s, 200s, 300s, 600s, 900s), the communicating nodes number varied as (10, 20, 30, 40) on 50 nodes of the network with 4 packets/second. The most speed is 20 m/s, the packet size is 512 bytes. The attacking nodes number varied from 1 to 3. The main simulation parameters are shown in Table 1

**Table.1.** Showing the simulation parameter

| Parameter | Value |
|---|---|
| Simulation area (m × m) | 1500 × 300 |
| Number of nodes | 50 |
| Simulation time (s) | 900 |
| Mobility Model | Random way point |
| Maximum speed (m/s) | 20 |
| Pause time (s) | 0,30,60,120,200,300,600,900 |
| Number of communicating nodes | 10, 30, 30, 40 |
| Application layer | Constant Bit Rate (CBR) |

| | |
|---|---|
| Packet size | 512 bytes |
| Packet rate | 4 packet/second |
| Routing protocols | Normal AODV, AODV under black hole, AODV enhanced by our solution |
| Number of Black hole nodes | 1, 2,3 |

### 7.2. Performance Metrics

To measure how our proposed solution performs in terms of the following four metrics.

**7.2.1. Packet Delivery Ratio (PDR):** Which is the percentage of the total number of packets delivered to the destination node with respect to the total number of packets sent by the source node

**7.2.2. Average End to End Delay(AE2ED):** Represents the average end-to-end delay that the source node needs to transfer packets to the destination node.

**7.2.3. Drop Packets (DP):** Is the number of the packets that don't reach the destination and are dropped in the network during transmission.

**7.2.4. Routing Overhead: T**his metric represents the ratio of the total number of routing-related control packet transmissions (RREQ, RREP, RERR etc) to the total number of data transmissions

### 7.3. Simulation Results

#### 7.3.1. Packet Delivery Ratio

Figures 4, 5, 6, and 7 and tables 2, 3, 4 and 5 respectively present the PDR evolution for the normal AODV, AODV under black hole attack, and AODV enhanced by our solution for black hole attack with variation of the communicating nodes from 10 to 40 nodes, variation of the pause time from 0 to 900 seconds, and variation of the black hole nodes number from 1 to 3. In the first scenario where the communicating nodes number is 10 the result of PDR in normal AODV when there is no black hole node in the network was the highest from 96.12% to 98.91% and it down to 39.38% when pause time equal to 900. The Packet Delivery Ratio of the network reduces to a very low level in the presence of a black hole attack, this PDR value was changed according to the value of number of black hole attacks, whenever a number of black hole attacks increase, the PDR value decreased this is due to the fact that some packets are discarded by malicious node during the attack. While PDR increases to a highest level when implementing our solution to become similar to a normal AODV. The other scenarios (20,30 and 40 nodes connected) went the same way. Significantly, the normal AODV and AODV with solution have almost matching PDR values, which illustrates that our proposed solution has the ability to detect and prevent all black hole attacks.

**Figure 4.** Packet delivery ratio for 10 communicating nodes

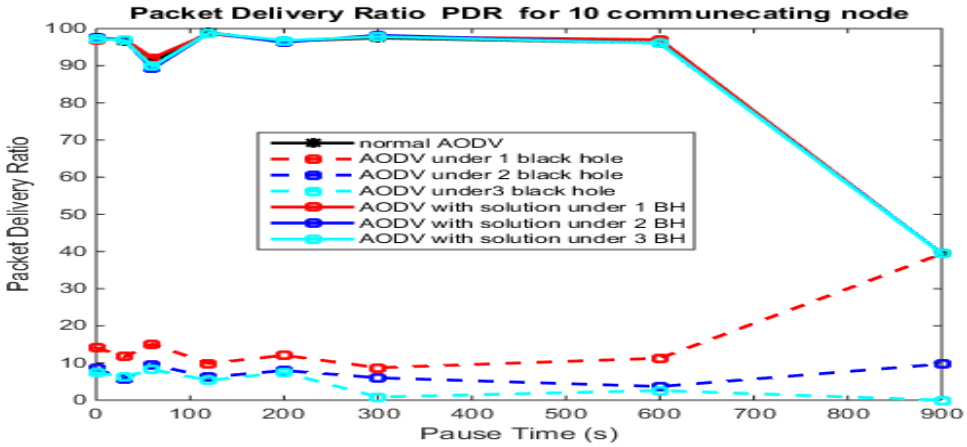



**Figure.5.** Packet delivery ratio for 20 communicating nodes

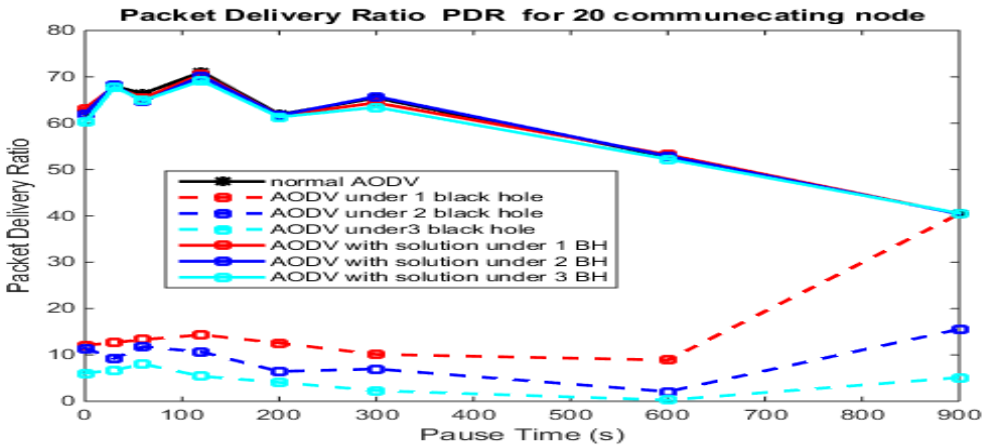



**Figure.6.** Packet delivery ratio for 30 communicating nodes

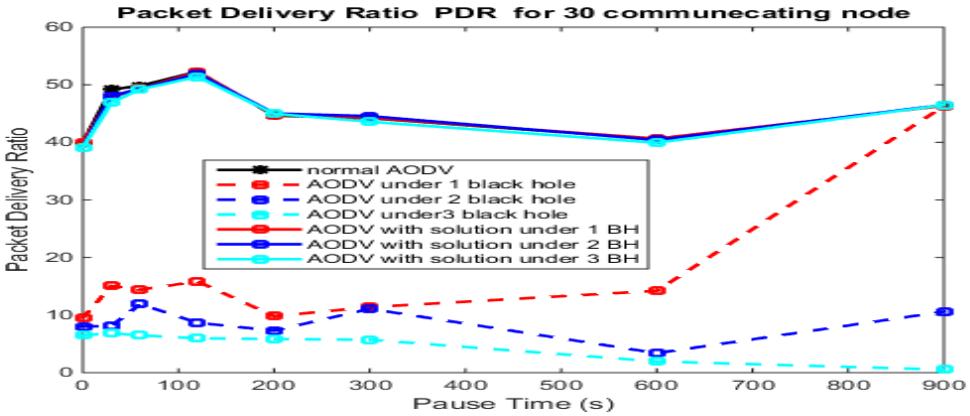


**Figure.7.** Packet delivery ratio for 40 communicating node

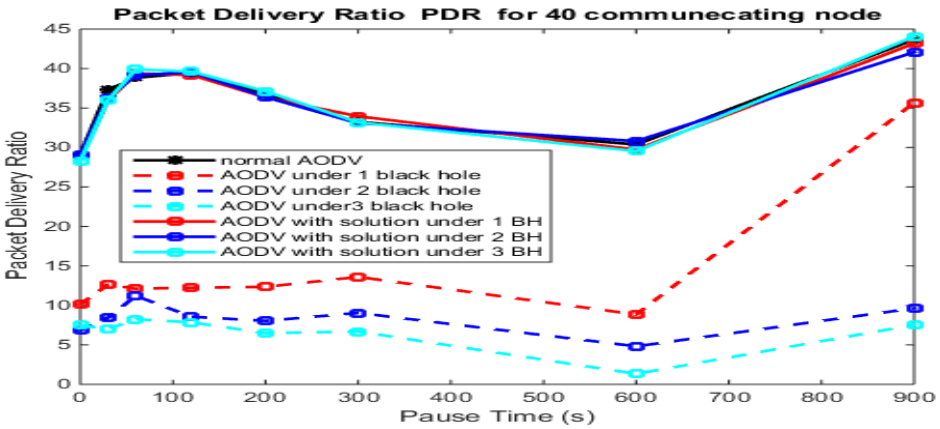



**Table.2.** Packet delivery ratio PDR for 10 communicating nodes

| **Packet Delivery Ratio PDR for 10 communicating node ( % )** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 97.44 | 14.13 | 8.5 | 7.41 | 97.05 | 97.55 | 97.34 |
| 30 | 96.74 | 11.69 | 5.55 | 6.34 | 97.06 | 96.95 | 96.81 |
| 60 | 91.10 | 15.07 | 9.55 | 8.20 | 92.10 | 89.29 | 89.82 |
| 120 | 98.91 | 9.87 | 6.19 | 5.35 | 98.62 | 98.82 | 98.82 |
| 200 | 96.61 | 12.08 | 7.99 | 7.43 | 96.58 | 96.33 | 96.79 |
| 300 | 97.49 | 8.74 | 6.01 | 0.85 | 97.81 | 98.20 | 97.82 |
| 600 | 96.12 | 11.28 | 3.67 | 2.60 | 97.00 | 96.05 | 96.08 |
| 900 | 39.38 | 39.37 | 9.73 | 0.00 | 39.38 | 39.51 | 39.39 |

**Table. 3.** Packet delivery ratio PDR for 20 communicating nodes

| **Packet Delivery Ratio PDR for 20 communicating node ( % )** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 62.61 | 12.04 | 11.42 | 6.03 | 63.16 | 62.03 | 60.18 |
| 30 | 67.98 | 12.67 | 9.25 | 6.72 | 67.80 | 68.15 | 67.84 |
| 60 | 66.41 | 13.31 | 11.76 | 8.02 | 65.45 | 64.70 | 64.92 |
| 120 | 71.05 | 14.34 | 10.65 | 5.39 | 70.51 | 70.14 | 69.18 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 200 | 61.91 | 12.56 | 6.43 | 4.08 | 61.71 | 61.72 | 61.33 |
| 300 | 65.44 | 10.12 | 6.97 | 2.29 | 64.40 | 65.77 | 63.44 |
| 600 | 52.76 | 8.89 | 2.08 | 0.26 | 53.21 | 52.91 | 52.23 |
| 900 | 40.51 | 40.43 | 15.54 | 5.11 | 40.43 | 40.40 | 40.57 |

**Table.4.** Packet delivery ratio PDR for 30 communicating nodes

| **Packet Delivery Ratio PDR for 30 communicating node ( % )** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 39.87 | 9.55 | 8.02 | 6.51 | 39.94 | 39.15 | 39.10 |
| 30 | 49.17 | 15.05 | 8.10 | 6.83 | 47.88 | 48.08 | 46.95 |
| 60 | 49.82 | 14.40 | 11.91 | 6.49 | 49.33 | 49.31 | 49.22 |
| 120 | 52.28 | 15.85 | 8.66 | 5.97 | 52.23 | 51.91 | 51.40 |
| 200 | 44.65 | 9.81 | 7.30 | 5.84 | 44.77 | 45.02 | 44.97 |
| 300 | 44.21 | 11.38 | 11.09 | 5.72 | 44.27 | 44.56 | 43.59 |
| 600 | 40.56 | 14.22 | 3.39 | 1.95 | 40.65 | 40.41 | 39.93 |
| 900 | 46.39 | 46.29 | 10.60 | 0.53 | 46.35 | 46.51 | 46.49 |

**Table.5.** Packet delivery ratio PDR for 40 Communicating Nodes

| **Packet Delivery Ratio PDR for 40 communicating node ( % )** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 29.06 | 10.14 | 6.83 | 7.48 | 28.29 | 29.10 | 28.26 |
| 30 | 37.29 | 12.62 | 8.46 | 7.01 | 35.95 | 36.29 | 36.03 |
| 60 | 38.84 | 12.12 | 11.21 | 8.25 | 39.39 | 39.15 | 39.90 |
| 120 | 39.45 | 12.24 | 8.57 | 7.85 | 39.18 | 39.55 | 39.63 |
| 200 | 36.73 | 12.35 | 8.04 | 6.49 | 36.35 | 36.38 | 37.12 |
| 300 | 33.24 | 13.61 | 9.05 | 6.69 | 33.95 | 33.08 | 33.18 |
| 600 | 30.38 | 8.85 | 4.82 | 1.33 | 29.73 | 30.81 | 29.53 |
| 900 | 43.68 | 35.68 | 9.64 | 7.54 | 43.18 | 42.08 | 44.07 |

### 7.3.2. Average End To End Delay

Figures 8,9,10 and 11 represent the simulation result recorded in the tables 6, 7, 8 and 9 respectively of the average end to end delay for normal AODV, AODV under black hole, and AODV enhanced by our solution, these figure show that end-to-end delay increases when the number of node communicate increase. The average end to end delay of AODV under black hole gets even lower compared to both standard AODV and AODV with solution because the malicious node responds immediately and pretends to have a valid route to the destination without checking in its routing table for this reason its route discovery process takes a shorter reply time, unlike normal intermediate nodes which must follow some process as checking and updating its routing tables before a reply. Also, we can see that the graphs of average end-to-end delay for the standard AODV and AODV enhanced by our solution are identical and very parallel, due to their values being very close, which proves the validity of our approach.

**Figure.8.** Showing the average end to end delay for 10 communicating nodes

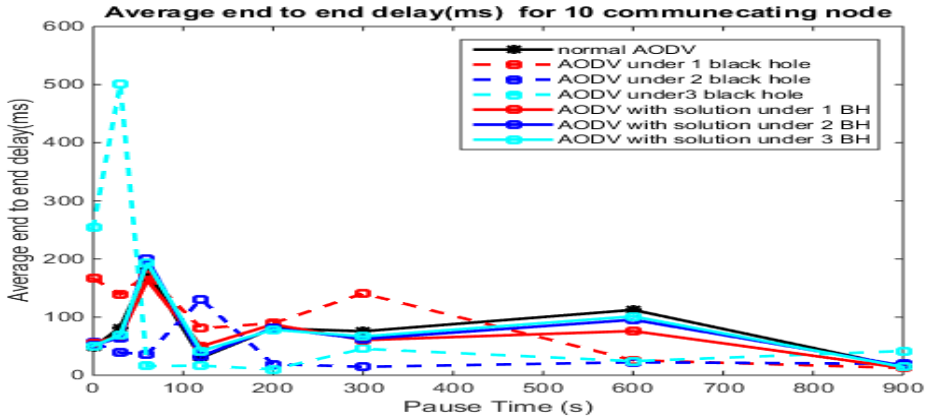



**Figure.9.** Showing the average end to end delay for 20 communicating nodes

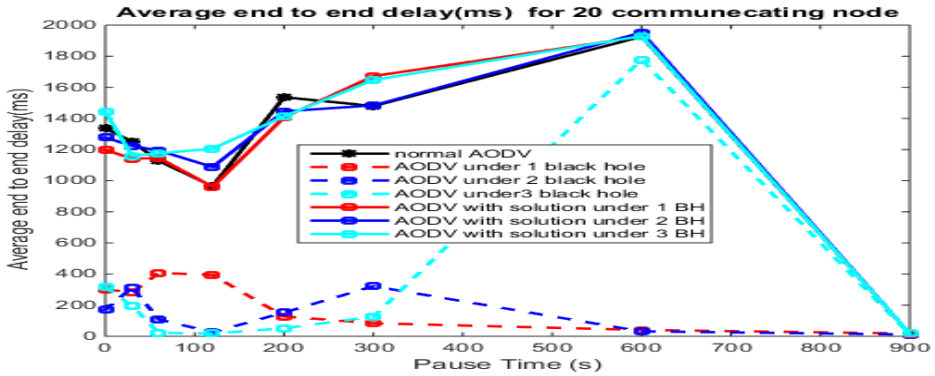



**Figure.10**. Showing the average end to end delay for 30 communicating nodes

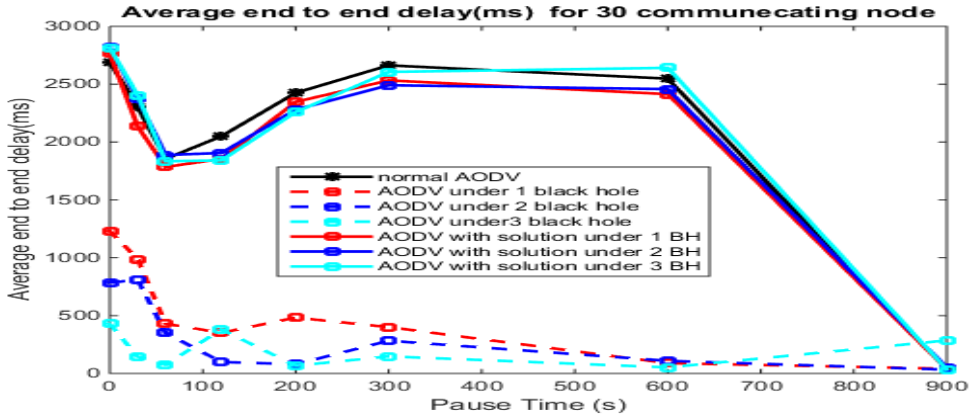


**Figure.11.** Showing the average end to end delay for 40 communicating nodes

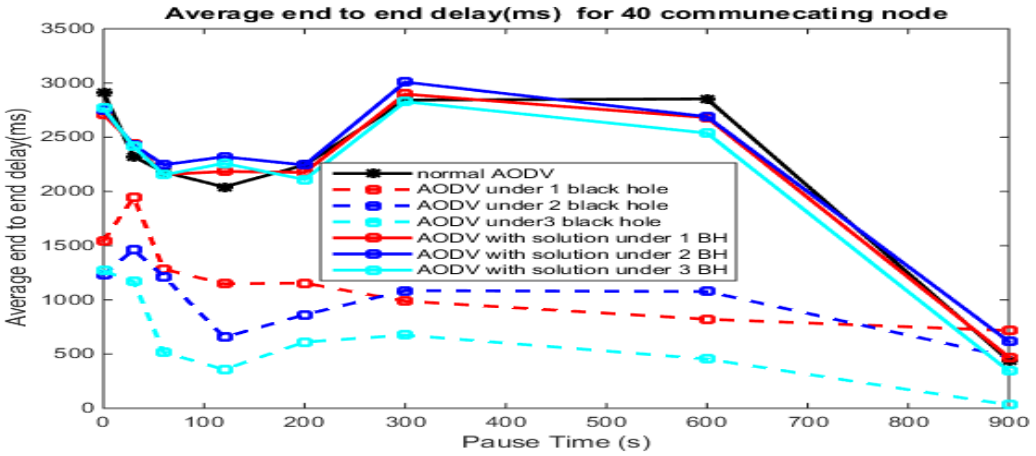



**Table.6.** Average end to end delay (AE2END) for 10 communicating nodes

| **Average end to end delay(ms)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 47.72 | 166.49 | 56.15 | 253.88 | 55.85 | 51.99 | 50.24 |
| 30 | 81.80 | 139.16 | 38.99 | 500.55 | 67.25 | 64.39 | 69.14 |
| 60 | 180.04 | 172.61 | 36.12 | 15.81 | 163.99 | 199.43 | 193.45 |
| 120 | 30.42 | 80.62 | 130.77 | 16.42 | 49.71 | 32.66 | 41.97 |
| 200 | 80.70 | 89.58 | 19.17 | 10.24 | 87.58 | 81.10 | 78.24 |
| 300 | 75.62 | 140.63 | 14.46 | 45.49 | 60.45 | 62.31 | 66.75 |
| 600 | 112.43 | 25.87 | 22.29 | 24.22 | 76.04 | 95.42 | 101.23 |
| 900 | 14.18 | 12.45 | 19.63 | 41.71 | 12.35 | 16.54 | 14.11 |

**Table.7.** Average end to end delay (AE2END) for 20 communicating nodes

| **Average end to end delay(ms)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 1336.63 | 301.45 | 170.25 | 318.87 | 1198.66 | 1277.83 | 1443.05 |
| 30 | 1252.02 | 281.53 | 313.03 | 195.24 | 1141.31 | 1223.99 | 1160.23 |
| 60 | 1126.69 | 407.31 | 108.09 | 21.77 | 1145.77 | 1193.67 | 1175.40 |
| 120 | 964.87 | 393.93 | 25.59 | 17.96 | 961.23 | 1088.12 | 1205.53 |
| 200 | 1536.48 | 127.67 | 152.50 | 51.35 | 1407.16 | 1445.68 | 1413.47 |
| 300 | 1479.85 | 83.70 | 321.53 | 125.86 | 1672.37 | 1484.09 | 1647.68 |
| 600 | 1925.95 | 40.49 | 31.55 | 1777.94 | 1926.98 | 1952.20 | 1929.33 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 900 | 17.03 | 18.02 | 11.52 | 12.20 | 16.94 | 18.12 | 18.17 |

**Table.8.** Average end to end delay (AE2END) for 30 communicating nodes

| **Average end to end delay(ms)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 2690.68 | 1231.41 | 785.42 | 428.93 | 2764.48 | 2821.26 | 2814.66 |
| 30 | 2303.84 | 987.90 | 808.03 | 144.95 | 2134.58 | 2378.22 | 2404.95 |
| 60 | 1854.20 | 430.22 | 350.29 | 74.84 | 1784.61 | 1888.08 | 1833.95 |
| 120 | 2050.31 | 351.33 | 98.95 | 380.49 | 1854.13 | 1905.78 | 1841.78 |
| 200 | 2425.29 | 482.57 | 79.80 | 66.57 | 2347.49 | 2280.09 | 2258.98 |
| 300 | 2663.09 | 400.30 | 282.72 | 147.44 | 2533.04 | 2491.20 | 2606.21 |
| 600 | 2548.04 | 88.77 | 108.87 | 52.14 | 2413.98 | 2457.53 | 2641.56 |
| 900 | 35.38 | 40.95 | 32.94 | 285.28 | 37.42 | 52.34 | 34.58 |

**Table.9.** Average end to end delay (AE2END) for 40 communicating nodes

| **Average end to end delay(ms)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 2909.28 | 1543.76 | 1232.29 | 1267.51 | 2713.90 | 2753.56 | 2766.65 |
| 30 | 2321.32 | 1943.21 | 1461.44 | 1168.67 | 2435.88 | 2427.38 | 2413.95 |
| 60 | 2178.65 | 1282.95 | 1216.27 | 515.99 | 2155.72 | 2245.91 | 2153.19 |
| 120 | 2041.54 | 1148.52 | 654.46 | 358.02 | 2184.05 | 2319.88 | 2259.18 |
| 200 | 2243.48 | 1154.70 | 863.03 | 610.86 | 2176.16 | 2243.70 | 2109.73 |
| 300 | 2842.91 | 988.25 | 1085.16 | 675.23 | 2897.33 | 3008.18 | 2827.47 |
| 600 | 2853.27 | 821.27 | 1076.79 | 454.06 | 2680.61 | 2689.33 | 2537.90 |
| 900 | 442.19 | 716.71 | 472.63 | 31.75 | 471.60 | 615.89 | 343.01 |

### 7.3.3 Drop Packets (DP)

Figures 12,13,14 and 15 which are drawn from simulation data recorded in tables 10, 11, 12 and 13 respectively, which illustrate the dropped packet data for AODV, AODV under a black hole, and AODV with our solution As shown in Figure the result of a dropped packet when the AODV is under a black-hole node in the network was very high because the black hole node always aims to absorb all packets between any two nodes that try to communicate in the network. Thus, the dropped packets value varies according to the number of black hole attacks, whenever a number of black hole attacks increase the dropped packets value will increase. On the other hand in a normal AODV, the dropped packets value decreased to a lower level that is very close to AODV enhanced by our solution Which leads to indicate that our proposed suitable to prevent losing a packet in a more reliable fashion.

**Figure.12.** Showing the total packets dropped for 10 communicating nodes

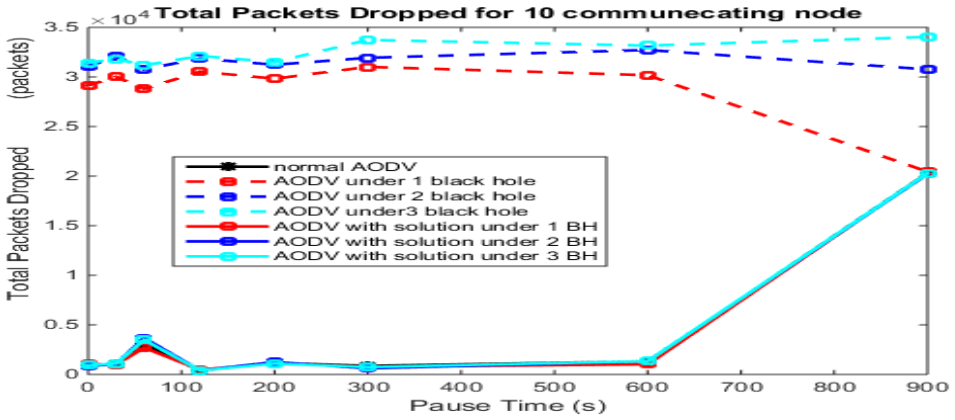



**Figure.13.** Showing the total packets dropped for 20 communicating nodes

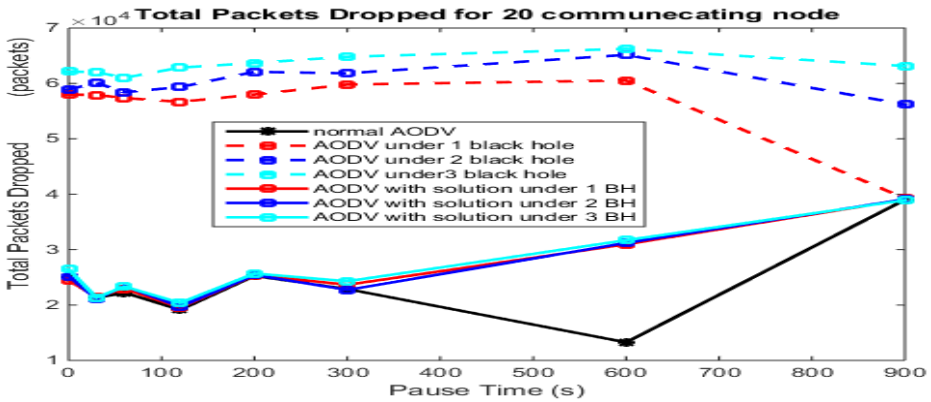



**Figure.14.** Showing the total packets dropped for 30 communicating nodes

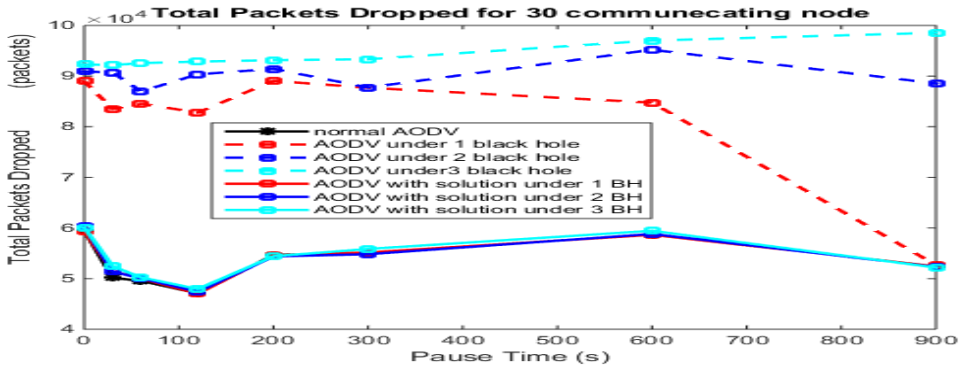



**Figure.15.** Showing the total packets dropped for 40 communicating nodes

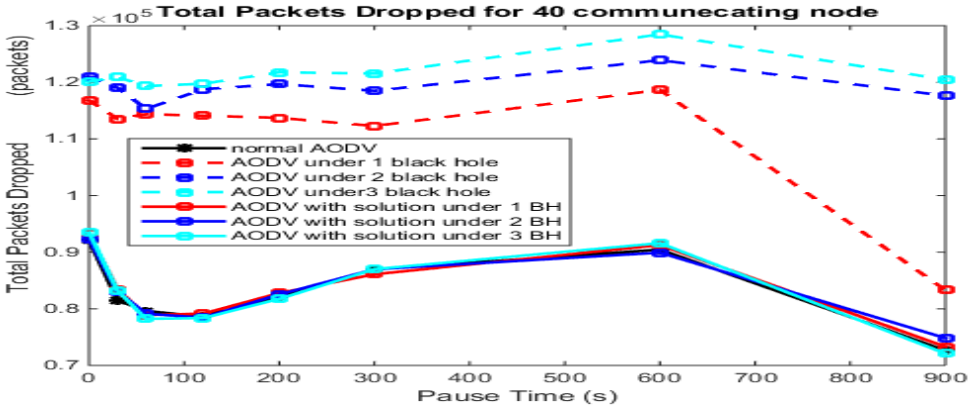


**Table.10.** Total packets dropped ( TPD ) for 10 communicating nodes

| **Total Packets Dropped ( packets)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 891 | 29155 | 31035 | 31421 | 1025 | 839 | 919 |
| 30 | 1119 | 30007 | 32103 | 31834 | 1011 | 1051 | 1095 |
| 60 | 3036 | 28804 | 30768 | 31168 | 2698 | 3660 | 3477 |
| 120 | 380 | 30533 | 31859 | 32123 | 474 | 402 | 406 |
| 200 | 1162 | 29828 | 31233 | 31497 | 1164 | 1250 | 1092 |
| 300 | 859 | 31017 | 31932 | 33735 | 750 | 613 | 744 |
| 600 | 1320 | 30175 | 32720 | 33164 | 1024 | 1342 | 1332 |
| 900 | 20299 | 20446 | 30762 | 34040 | 20303 | 20222 | 20274 |

**Table.11.** Total packets dropped ( TPD ) for 20 communicating nodes

| **Total Packets Dropped ( packets)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 24888 | 57981 | 58912 | 62160 | 24505 | 25217 | 26447 |
| 30 | 21289 | 57919 | 60094 | 62027 | 21409 | 21109 | 21354 |
| 60 | 22233 | 57366 | 58406 | 61016 | 22933 | 23444 | 23332 |
| 120 | 19141 | 56675 | 59348 | 62857 | 19549 | 19710 | 20394 |
| 200 | 25264 | 57995 | 62090 | 63689 | 25389 | 25424 | 25692 |
| 300 | 22876 | 59803 | 61830 | 64817 | 23656 | 22725 | 24291 |
| 600 | 13264 | 60539 | 65166 | 66245 | 30966 | 31212 | 31705 |
| 900 | 38988 | 39267 | 56204 | 63136 | 39035 | 39089 | 38926 |

**Table.12.** Total packets dropped ( TPD ) for 30 communicating nodes

| **Total Packets Dropped ( packets)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 59562 | 88990 | 90928 | 92322 | 59408 | 60303 | 60098 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 30 | 50152 | 83500 | 90710 | 92156 | 51466 | 51380 | 52436 |
| 60 | 49560 | 84528 | 86972 | 92564 | 49996 | 50058 | 50241 |
| 120 | 47095 | 82794 | 90344 | 92859 | 47032 | 47417 | 47946 |
| 200 | 54670 | 89060 | 91424 | 93147 | 54563 | 54380 | 54418 |
| 300 | 55121 | 87690 | 87741 | 93334 | 55168 | 54821 | 55859 |
| 600 | 58708 | 84753 | 95205 | 97020 | 58651 | 58824 | 59444 |
| 900 | 52409 | 52679 | 88548 | 98550 | 52411 | 52292 | 52186 |

**Table.13.** Total packets dropped ( TPD ) for 40 communicating nodes

| **Total Packets Dropped ( packets)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 92187 | 116819 | 121041 | 120135 | 93359 | 92346 | 93484 |
| 30 | 81526 | 113555 | 119024 | 120912 | 83344 | 83027 | 83196 |
| 60 | 79613 | 114378 | 115310 | 119339 | 78900 | 79120 | 78229 |
| 120 | 78647 | 114099 | 118780 | 119749 | 79148 | 78454 | 78364 |
| 200 | 82122 | 113724 | 119693 | 121778 | 82773 | 82538 | 81750 |
| 300 | 86953 | 112286 | 118499 | 121539 | 86095 | 86981 | 87010 |
| 600 | 90464 | 118666 | 123904 | 128471 | 91257 | 89920 | 91606 |
| 900 | 72631 | 83304 | 117642 | 120464 | 73309 | 74828 | 72112 |

### 7.3.4 Routing Overhead

From the figures 16,17,18 and 19 which represent from the result recorded from the tables 14,15,16, and 17 it is clear that the overhead is increased when the number of nodes communicate is increased, because the control packet has to be generated to discover the route between a source node and a destination node, therefore as long as the number of nodes increases, the overhead level increase. Also, we can see that normal AODV has a low overhead due to its reactive nature, on the other hand with the presence of black hole nodes, the overhead rises according to the number of black hole nodes in the network which means it becomes worse as the number of black hole nodes increase. When we applied the enhanced AODV by our solution we got a similar overhead level to the normal AODV, which denotes that our proposed mechanism has succeeded in terms of detection and doing well in terms of Routing Overhead because it didn't add any extra control packet.

**Figure.16.** Showing the routing overhead for 10 communicating nodes

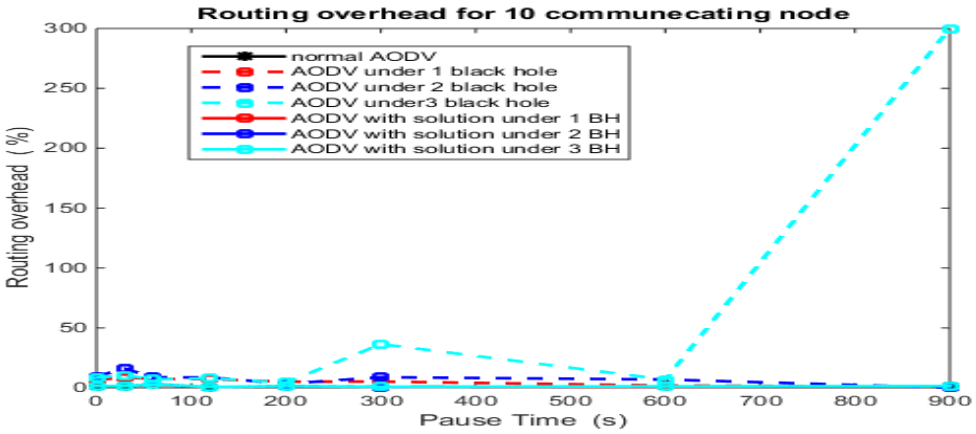



**Figure.17.** Showing the routing overhead for 20 communicating nodes

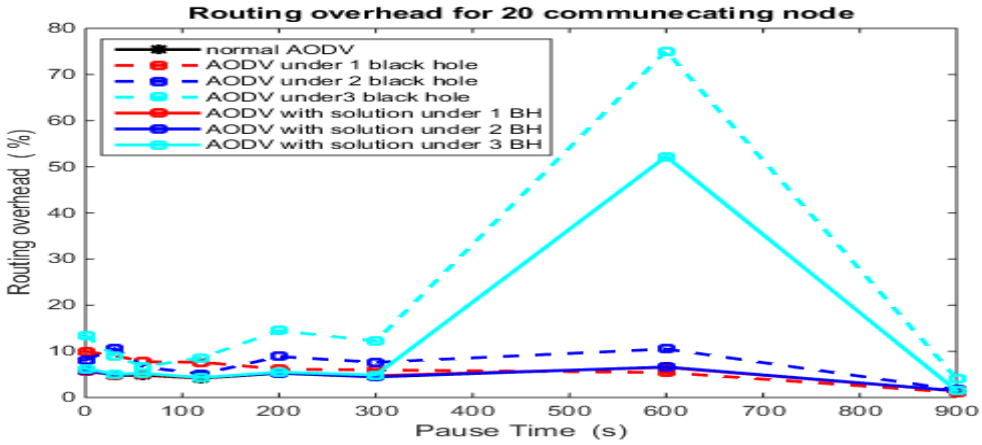



**Figure.18.** Showing the routing overhead for 30 communicating nodes

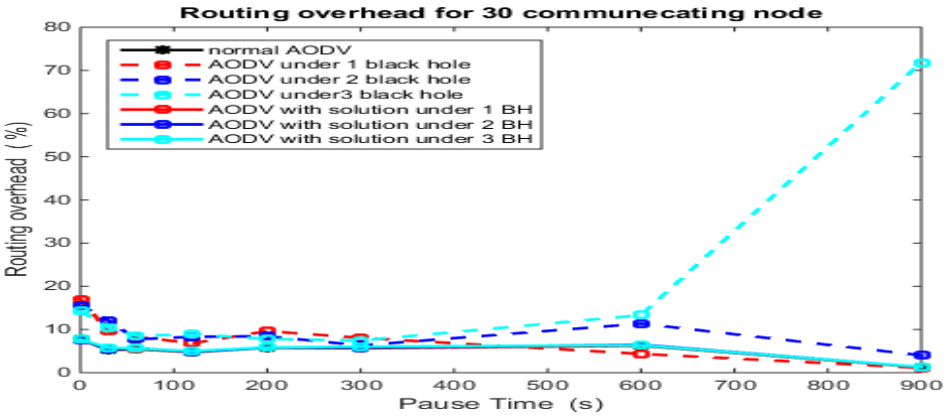


**Figure.19.** Showing the routing overhead for 40 communicating nodes

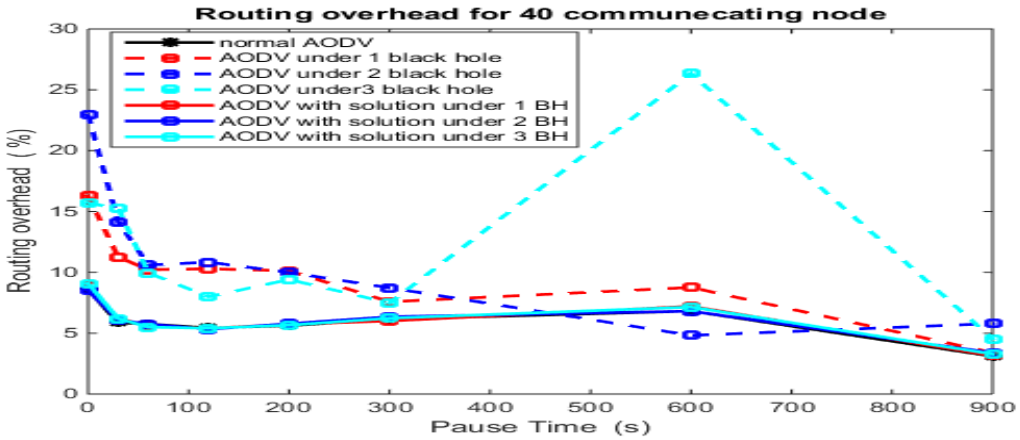



**Table.14.** Routing overhead for 10 communicating nodes

| **Routing Overhead (%)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 1.46 | 6.54 | 9.58 | 8.42 | 1.49 | 1.43 | 1.48 |
| 30 | 1.44 | 8.65 | 15.93 | 10.44 | 1.41 | 1.46 | 1.52 |
| 60 | 2.96 | 7.5 | 8.77 | 7.10 | 2.67 | 3.13 | 2.93 |
| 120 | 0.58 | 7.23 | 8.66 | 7.93 | 0.63 | 0.61 | 0.69 |
| 200 | 1.41 | 5.07 | 3.38 | 4.42 | 1.47 | 1.53 | 1.43 |
| 300 | 0.94 | 5.23 | 8.85 | 36.44 | 0.86 | 0.86 | 0.88 |
| 600 | 1.19 | 1.87 | 6.92 | 6.89 | 1.01 | 1.24 | 1.27 |
| 900 | 1.37 | 0.98 | 0.09 | 300.00 | 1.38 | 1.42 | 1.45 |

**Table.15.** Routing overhead for 20 communicating nodes

| **Routing Overhead (%)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 5.82 | 9.97 | 8.14 | 13.43 | 5.75 | 5.88 | 6.27 |
| 30 | 4.78 | 9.08 | 10.56 | 9.05 | 4.89 | 4.92 | 5.07 |
| 60 | 4.83 | 7.74 | 6.62 | 6.68 | 5.06 | 5.21 | 5.23 |
| 120 | 4.16 | 7.64 | 5.08 | 8.62 | 4.22 | 4.31 | 4.32 |
| 200 | 5.26 | 6.13 | 8.87 | 14.48 | 5.38 | 5.34 | 5.50 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 300 | 4.45 | 5.97 | 7.62 | 12.21 | 4.72 | 4.50 | 4.88 |
| 600 | 6.62 | 5.41 | 10.51 | 75.09 | 6.52 | 6.61 | 52.23 |
| 900 | 1.39 | 1.10 | 1.67 | 4.11 | 1.42 | 1.46 | 1.47 |

**Table.16.** Routing overhead for 30 communicating nodes

| **Routing Overhead (%)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 7.71 | 16.99 | 15.62 | 14.24 | 7.49 | 7.69 | 7.70 |
| 30 | 5.26 | 9.57 | 12.06 | 10.44 | 5.52 | 5.50 | 5.75 |
| 60 | 5.45 | 8.27 | 7.73 | 8.55 | 5.59 | 5.70 | 5.61 |
| 120 | 4.76 | 6.84 | 8.31 | 8.91 | 4.80 | 4.83 | 4.99 |
| 200 | 5.79 | 9.62 | 8.44 | 7.81 | 5.88 | 5.84 | 5.86 |
| 300 | 5.65 | 8.06 | 6.31 | 7.45 | 5.69 | 5.83 | 6.01 |
| 600 | 6.26 | 4.35 | 11.35 | 13.32 | 6.33 | 6.48 | 6.38 |
| 900 | 1.25 | 1.10 | 4.01 | 71.83 | 1.29 | 1.32 | 1.33 |

**Table.17.** Routing overhead for 40 communicating nodes

| **Routing Overhead (%)** | | | | | | | |
|---|---|---|---|---|---|---|---|
| pause time (s) | AODV normal | AODV under black hole | | | AODV with solution | | |
| | | 1 BH | 2BH | 3BH | 1 BH | 2BH | 3BH |
| 0 | 8.59 | 16.27 | 22.93 | 15.70 | 8.92 | 8.56 | 9.08 |
| 30 | 5.87 | 11.26 | 14.14 | 15.25 | 6.20 | 6.07 | 6.20 |
| 60 | 5.75 | 10.22 | 10.60 | 9.96 | 5.63 | 5.75 | 5.50 |
| 120 | 5.43 | 10.29 | 10.84 | 7.99 | 5.40 | 5.33 | 5.41 |
| 200 | 5.62 | 10.13 | 9.99 | 9.41 | 5.74 | 5.78 | 5.66 |
| 300 | 6.15 | 7.58 | 8.73 | 7.48 | 6.01 | 6.35 | 6.23 |
| 600 | 6.82 | 8.76 | 4.82 | 26.34 | 7.21 | 6.81 | 7.15 |
| 900 | 3.11 | 3.40 | 5.79 | 4.54 | 3.16 | 3.39 | 3.29 |

## 8. Conclusion

AODV is the most popular and efficient protocol for MANET due to its natural features as low overhead. But, it is not designed to provide security to MANET, therefore mobile ad-hoc networks suffer from several types of attacks, the Black hole attack is one of the conceivable attacks that aims to disrupt the routing performance in MANETs by dropping all packet forwarded between source and destination node. For that reason we proposed a new solution to detect and isolate this attack. Our proposed solution is based on the fact that the black hole nodes when receiving RREQ packet immediately reply with the fake packet as possible as quickly without checking or updating its routing table, therefore the time required to generate a RREP packet for a black hole node will be the least. The next-hop node in the reverse route calculates the reply time for the originator node and compares it with the threshold value, if the reply time is less than threshold value, it will consider the node as a black hole node then initiate the isolate process. In this research, we analyzed the effect of the black hole in a MANET. We implemented an AODV protocol that behaves as a Black Hole in NS-2.35 with various black hole attack numbers, in order to detect and prevent this attack type in MANET we also implemented AOVD enhanced by the proposed solution against a black hole attack. To evaluate the performance of the proposed solution we performed three scenarios using NS-2.35, Firstly protocols were simulated in a network that is there no attack (normal AODV without a black hole), secondly the protocols were simulated in a network where black hole attack has been launched(AODV under Black Hole ) and thirdly Enhanced AODV protocol by the proposed solution against a black hole attack. The performance metrics that were used to perform the evaluation are packet delivery rate, end to end delay, total packet dropped and routing overhead.

The results showed that the network performance gets destructed in the presence of the black hole attack but when implemented AODV that is enhanced by the proposed solution it gives better results which are very close to normal AODV without black hole attack.

So our proposal improves the security of AODV routing protocols and enables it to eliminate both a single and multiple black hole attack completely without affecting the network performance with reduced cost because our proposed solution requires just a slight modification.

As future work, we intend to study the performance of the proposed solution on a collaborative attack, implement the solution for other routing protocols and provide a solution to prevent these types of attacks.

## References

Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97).

Aluvala, S., Sekhar, K. R., & Vodnala, D. (2016). An empirical study of routing attacks in mobile ad-hoc networks. *Procedia Computer Science*, *92*, 554-561.

Arathy, K. S., & Sminesh, C. N. (2016). A novel approach for detection of single and collaborative black hole attacks in MANET. *Procedia Technology*, *25*, 264-271.

Arunmozhi, S. A., & Venkataramani, Y. (2012). Black hole attack detection and performance improvement in mobile ad-hoc network. *Information Security Journal: A Global Perspective*, *21*(3), 150-158.

Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications magazine*, *40*(10), 70-75.

Deshmukh, S. R., Chatur, P. N., & Bhople, N. B. (2016, May). AODV-based secure routing against blackhole attack in MANET. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1960-1964). IEEE.

Imran, M., Khan, F. A., Abbas, H., & Iftikhar, M. (2014, June). Detection and Prevention of black hole attacks in mobile ad hoc networks. In *International Conference on Ad-Hoc Networks and Wireless* (pp. 111-122). Springer, Berlin, Heidelberg.

Khan, D., & Jamil, M. (2017, November). Study of detecting and overcoming black hole attacks in MANET: A review. In *2017 International Symposium on Wireless Systems and Networks (ISWSN)* (pp. 1-4). IEEE.

Mirza, S., & Bakshi, S. Z. (2018). Introduction to MANET. *International research journal of engineering and technology*, *5*(1), 17-20.

Perkins, C., Belding-Royer, E., & Das, S. (2003). RFC3561: Ad hoc on-demand distance vector (AODV) routing.

Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2016). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks*, *22*(5), 1505-1511.

Sharma, N., & Sharma, A. (2012, January). The black-hole node attack in MANET. In *2012 second international conference on Advanced Computing & Communication Technologies* (pp. 546-550). IEEE.

Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, *34*(1), 107-117.

Tan, S., & Kim, K. (2013, November). Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing* (pp. 1159-1164). IEEE.