*Int. J. Open Problems Compt. Math., Vol. 13, No. 2, June 2020*
*ISSN 1998-6262; Copyright © ICSRS Publication, 2020*
*www.i-csrs.org*

# An Enhanced AODV Protocol Against Black Hole Attack Based on Classification Algorithm

**Hasan Al-Refai**

Department of Computer Science
Philadelphia University, Jordan
Email: halrefai@philadelphia.edu.jo

Received 15 January 2020; Accepted 21 March 2020

**(Communicated by Iqbal H. Jebril)**

## *Abstract*

***One of the most demanding topics is Covering areas that do not have ready infrastructures to support network connections; mobile ad hoc networks (MANET) were the solution to this problem. Protocols like Ad Hoc On-Demand Distance Vector(AODV)take action to manage the devices inside. As a result of such network characteristics, AODV protocol was vulnerable to a list of attacks like denial-of-service(DOS) attacks, which contains attacks like a black hole and wormhole attacks. In this paper, an enhanced algorithm for black hole attack detection and prevention are presented based on four features extracted from the AODV protocol. The ready data set is used to select the best features related to the black hole attack using symmetrical uncertainty (SU) feature selector based on the WEKA tool. The four features were evaluated by classification method called J48 to prove their capability of defining black hole nodes. Moreover, the presented algorithm implements straightforward test classification criteria over the regular AODV protocol to allow detection and sharing of the identities of the black nodes. The results of the experimental results were implemented using the Global Mobile Information System Simulator(GlomoSim) simulator over 50 nodes and compared to 3 other previously proposed algorithms. The new proposed algorithm proofed its capability in detecting and preventing black hole attacks with higher efficiency average on an END-TO-END time delay, lower overhead factor, and higher packet delivery ratio (PDR) than all other three algorithms.***

***Keywords:*** ***Ad Hoc On-Demand Distance Vector, symmetrical uncertainty, denial-of-service, black hole, and wormhole attacks.***

# 1. Introduction

The MANET is various infrastructure network support devices used in our daily life, such as phones, laptops, etc... This network is for setting up transmitting and receiving network that directly gives the wanted results without the need for an administration center. These devices are working together dynamically. The cellular devices are linked by wireless connection. The sending process is done in its radio range by using point to point with medium nodes cooperation. Each of which could be a sender or receiver. The drawback of this system is security; one of the security problems is the black hole attack. [1, 2, 3, 4, 5, 11, 13]. Figure 1 shows a set of cellular devices forming an ad hoc network.

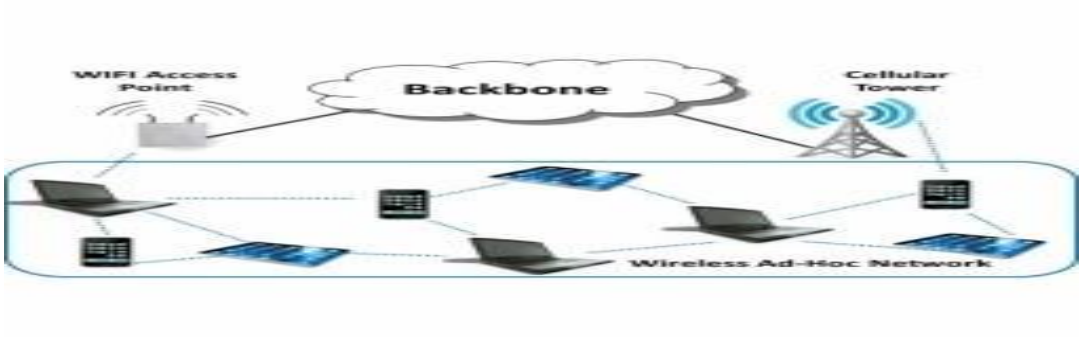


**Figure 1: A collection of mobile devices forming an ad- hoc network [34].**

To differentiate between the MANET and other networks, some specifications are described the MANET network. There is no central Access Point, and no infrastructure, in this case, makes the determination of the power impossible, so the performance and the matter of entering the nodes to the network. This characteristic is called self-organization and configuration. [11], [14], [15], [7]. Another thing is the topology of the mobility of nodes it works dynamically this means that the ad-hoc mobile devices often change their position without limits at different speeds and routs, the result of this the connection may get immediately broken, for that it's hard to define the position of the nodes. When this happens, there will be some transmitted data lost because the continuously new path will be re-built. Therefore, the ad-hoc network is not stable and might be changed at any time [14], [15], [12], [13], [27]. Wireless networks are continuously having a low bit rate and a high bit error when compared with the wired network. The wireless networks are sensitive to noise, signal to lose, and multiple access [14], [15], [6], [7], [8].

However, numerous challenges appear as a result of using MANET, including the security issue, decentralized protocols, the electricity issue, computational-efficiency, and robustness to mobility. The security difficulty is crucial and even more challenging in MANET because of its features, such as the mobility of the node, self-organizing functionality, and dynamic topology. One of the security issues is attack challenges, and MANETs are usually liable to various styles of attacks. There are different types of active attacks, such as Denial Of Service, Impersonation, Packet Modification, Flooding, Worm Hole, Selfish node, Gray Hole, Routing Table Run-off, and Black Hole. This paper will consider to observe and stop two varieties of active attacks that are black hole attack and gray hole attack. During a gray hole attack, the assailant drops the packet once it's received from a neighbor.

On the other hand, the black hole attack usually arises when the network is joined with a malicious node where the essential goal is of intercepting records packets that can be transmitted across the network and drop them. The main problem considered for the black hole attack is a malicious node that enters the network. It drops the whole data packet and prevents it from reaching the destination, which caused data loss, delay in the network, and sucking all the data traffic corrupt

the entire network. The data can be lost or intercepted in two ways: the first way the malicious nodes that use the AODV protocol for sending routing reply RREP to the source node directly at the receiving routing request RREQ. The second way, the malicious node intercepts the packets without using the AODV routing protocol that means not sending the RREP to the source node. In another way, once the data reach the node, the data will be directly dropped, and the destination node will be unreachable, which is called the gray hole attack [22], [35], [24],[16]. Usually, the black hole attack sends a fake route reply control message RREP to attract all requests and then drop the data packets. This paper offers significant contributions. For example, it allows choosing one of the functions selection models to discover more associated features from a collection of datasets, which is known as the Behavior-Driven Development (BDD) dataset for detecting the black hole attack. Secondly, we would then be able to propose a new approach that helps us eventually get the black hole attack detected and prevented.

Furthermore, each node consists of two tables, which might be a black table to decide a malicious node or a trust table for the normal node. The proposed approach relies on the features within the BDD dataset. The acquired overall performance results indicate that the chosen functions have succeeded in detecting and stopping black hole attacks and gray hole attacks. Wherein the proposed algorithm has resulted in a giant development over the unique AODV protocol with regards to the dropped packets ratio, the packet delivery ratio, end-to-end delay, and overhead.

Unfortunately, most of the previous works try to enhance the AODV protocol using many techniques like fuzzy and Classification Algorithm, etc... all of them tries to detect and prevent the black hole attackers. However, some of these works give a good result. However, still, there is no accuracy, a lot of redundant data, and overhead. These issues affect on the network capacity and efficiency of the whole system, the network capability will be affected by lagging, transmitting the data packets will be slower, the malicious nodes will drop the data and the destination node will be unreachable. So, the efficiency of the overall network is going to be less than the typical network. The creation of a new method and protocol is needed, since the related works that used different methods give some results, but still, there are some drawbacks. For that, this paper is going to enhance the AODV protocol by updating existing functions to achieve the following features:

- allow black hole attack detection
- to allow black hole attack prevention without losing paths between nods.
- preserve the network average transmission speed.
- preserve the MANET network average overhead.

## 2. Ad-hoc On-Demand Distance Vector Protocol (AODV)

One of the most famous routing protocols designed for wireless and mobile ad hoc networks is An Ad Hoc On-Demand Distance Vector (AODV). This protocol creates routes from source to destination on demand and supports both unicast and multicast routing. AODV provides detailed information about the topology of the node by using control messages. The control messages in AODV dived into several forms Route Request (RREQ), Route Reply (RREP), Route Discovery part, and Route Error (RERR) part [17], [3], [18].

### 2.1. Route Discovery

Router Discovery Protocol (IRDP) is a protocol for computer hosts to discover the presence and location of routers on their local area network. IRDP eliminates the need to configure routing information manually. In the beginning. The IRDP protocol must check if the path is available to the node in its routing table, and if the protocol finds the familiar route to him to take it as a trusted node, then the packet will send to the destination node. On the other hand, if the protocol did not find the path, the source node can then introduce the invented method of the route and can notice

that route by broadcasting a route request packet (RREQ) to all or any of its neighbors. The RREQ control message will contain the IP addresses for the source and destination nodes, as well as, the most recent sequence number for each of the source node and the destination node, the broadcast ID number and the hop count, in that case, anyone from the neighboring nodes receives RREQ they must update their Routing Table for the source node depending on the content of the RREQ message.

Furthermore, make backward pointers for the source node to be followed by the route reply control message (RREP). There are three possibilities for the node, which is in charge of receiving the RREQ control message. Where this node can be the destination itself or can be an intermediate node with an active route within its Routing Table to the destination node, furthermore, this node can be an intermediate node that doesn't have an active route to the destination node in its Routing Table. In the first case, the destination node itself receives the RREQ control message, and then the destination node will unicast the RREP message back to the source node. Figure 2 explains this case.

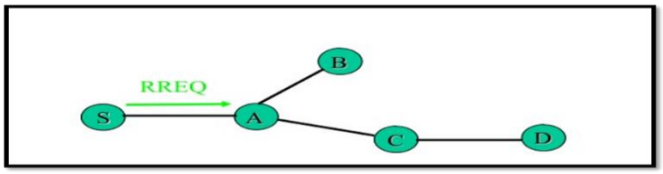


**Figure 2: RREQ received directly by the destination [16]**

In the second case, the intermediate node contains a path to the destination node that received the RREQ message. In this state, the intermediate node unicasts the RREP message back to the source node once it has the valid route, the route is going to be valid if the sequence variation of the destination node is correct; that is successively enclosed within the RREQ, is up to the sequence variety of the destination node that has been saved within the Routing Table. Otherwise, this intermediate node does not send RREP to the source node, but it rebroadcasts the RREQ to its neighbors [3], [5], [9], [10], [13], [17], [31]. Figure 3 illustrates this case.

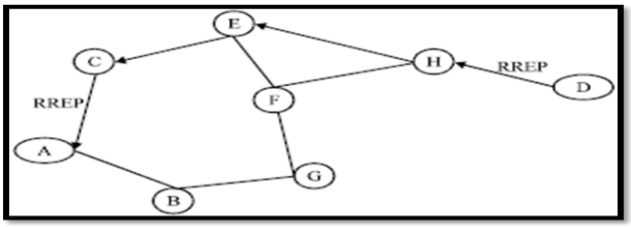


**Figure 3:RREQ received by an intermediate node having a valid route [35].**

In the final case, if the node that receives the RREQ control message is an intermediate node with no route, it will try to transmit an RREQ control message again. As the RREQ moves from the intermediate node to another, each node prepares its reverse path to its previous node and broadcasts the RREQ [10], [15], [3], [31]. Figure 4 shows the third situation (i.e., The RREQ is transmitted through one or more intermediate node(s), until being received by the destination).

The safety of the node's route may be ensured by comparison of the destination sequence number of its path to the destination sequence number of the received route. If the destination sequence number of its path seems to be more than or equal to the received path, it has a correct route [15], [17], [31], [19], [11]. Finally, RREQ is received by either an intermediate node with a valid route (here the scenario of the second case occurs) or to the destination itself (here the scenario of the first case takes place).

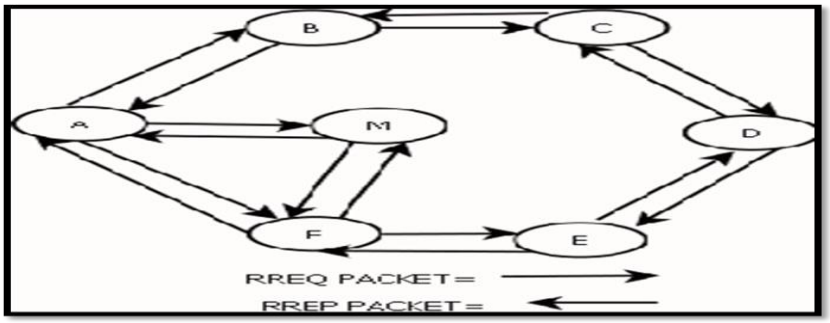


**Figure 4:RREQ transfers through an intermediate node(s) to the destination [36].**

### 2.2. Route Maintenance

Routes in MANETs are susceptible to breakage because of the mobility of the nodes. In AODV protocol, any link breakage along the established path between the supply node and also the destination node may be detected by the mechanism of route maintenance. With regards to this mechanism, if any intermediate node detects a link failure, it initiates a Route Error (RERR) message and sends it back to the supply node to announce to the source node that this path has become not valid to the destination node. When the source node receives the RRER message, it initiates a new route and discovers the process for the destination. In addition to that, when the RRER is sent back through the intermediate nodes to the source, the path that contains a legitimate link is going to be far away from the route caches of those nodes [4], [10], [17], [31], [19], [11].

## 3. Proposed Methodology (Enhanced AODV)

The nature of MANET networks since it constructed depending on the connected devices through their coverage ranges and no infrastructure needed to establish their connections or routs. Which means each node in the network act like receiver, and relay point. It makes the MANET network vulnerable to various types of attacks, just like a black hole attack, gray hole attack, and several other attacks. The Blackhole attack is considered one of the Denial of Service (DoS) attacks, which occurs by injecting malicious node inside the network to sink most of the traffic through its path and drop all the transmitted data through it, without allowing it to pass to the destination nodes [26],[27],[28],[29],[30]. Moreover, black hole attacks can be implemented through malicious nodes that can be easily injected into the network, leading to drop the network performance in a very massive way.

The behavior features of the black hole node need to be studded to present a new mechanism for detecting black hole attacks. List bellow summarizes the main behaviors of black hole attack [33],[29],[30],[20]:
1. behave as normal nodes in the first operation to receive the most RREQ packets transmitted by other nodes.

2. black hole nodes try to raise its transmission power to gain most of the RREQ packets from all the networks. Also, it mobilizes in a faster way than the normal nodes to corrupt all the networks.

3. RREP packets are sent directly as a response to any RREQ packet impersonating that the destination node is one hop count away from it.

4. Blackhole node does not generate data packets or even RREQ packets.

5. RREQ packets received by the black hole node does not rebroadcast to any other node to reduce the number of RREP and make sure that the black hole node is the best path to transmit data.

6. RREP message also will not be unicasted from the replying node to the source node through the black hole node.

Figure 5 shows the black hole node attack effect over the network.

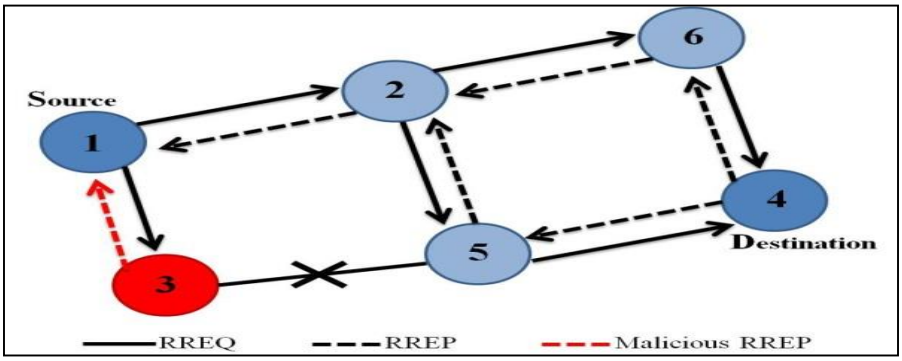


**Figure 5: the black hole problem [37].**

For the proposed methodology, two phases were implemented:

- the features selection phase
- the modified AODV phase.

## 3.1. Feature Selection Phase

Through the first phase, the Symmetrical uncertainty (SU) feature selection model is used to find the most related features to the whole black attack from (BDD) data set proposed by [28]. However, some features may be significant to identify the black hole attack, and others may not. In the first phase, the features selected from the BDD data set using SU were tested through a classification method called J48 to verify that the features are capable of detecting blackhole attacks in a very accurate way. As proposed in [28], the features of the MANET network nodes can be classified into 29 features, as shown in figure 6 below.

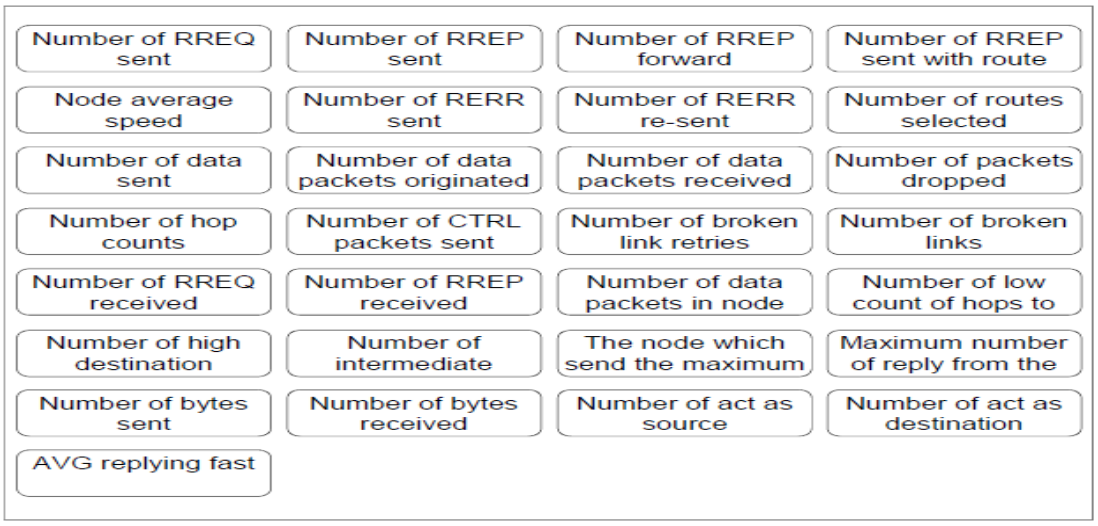


**Figure 6: The Collected Features for each node.**

To identify the best features from the 29-feature set shown in the previous figure, a comparison between the used feature selection IG method used in the proposed paper [13],[28], and SU feature selector, which is used in this paper were applied. The comparison also was implemented with

the feature selection method called Relief-F to cover most of the feature selection types and get the best features related to the black hole attack.

### 3.1.1 Symmetric Uncertainty (SU)

One of the best feature known selection methods is Symmetric Uncertainty (SU). For that, it is utilized for measuring feature selection systems based on mutual information. It is used as a correlation measure between the features and the class.

$$SU= (H(X)+H(Y)-H(X\backslash Y))/ (H(X)+H(Y)) \qquad (1)$$

where H(X) and H(Y) are the entropies based on the probability associated with each feature and class value respectively, and H(X, Y), the joint probabilities of all combinations of values of X and Y [4],[5],[9],[13].

### 3.1.2. Information Gain (IG)

For measuring ranking features, Information Gain **(IG)** is used. Given that entropy is a standard of deficiency in a training set S, this can characterize a measure reflecting any additional information about Y provided by X that represents the amount by which the entropy of Y decreases. This measure is known as IG. It is given by

$$IG = H(Y) - H(Y \backslash X ) = H(X ) - H(X \backslash Y) \qquad (2)$$

where IG is a symmetrical measure, the information gained about Y after observing X is equal to the information gained about X after observing Y. A weakness of the IG criterion is that it is biased in favor of features with more values, even when they are not more informative [4],[5],[9],[13].

### 3.1.3. Relief-F

The basic idea of Relief-F is to draw instances at random, compute their nearest neighbors, and adjust a feature weighting vector to give more weight to features that distinguish the instance from neighbors of different classes. Specifically, it tries to find a reasonable estimate of the following probability to assign as the weight for each feature F.

$$WF = P(\text{different value of F/different class}) - P(\text{different value of F/same class}) \qquad (3)$$

This approach has shown good performance in various domains [6],[9],[13].

### 3.1.4. Futures Selection Stages

The processes stages in the first phase were illustrated in figure 7 bellow as:

1- feature selection using SU, IG, and Relief-F
2- J48 classification method implementations (training and testing for the three used selection methods)
3- testing the accuracy of the three feature selectors to choose the best features through the J48 classification method.

This paper depends on the ready BDD data set created by [28], so the data set to establish the features selection phase were ready. Because of that, the presented work starts by implementing the SU, and Relief-F feature selection methods directly based on the WEKA AI learning machine tool, which is open-source software for Knowledge Analysis and data mining, contains ready implementations for most classifiers such as decision trees, Naïve Bayes (NB), Sequential

Minimal Optimization (SMO), Lazy (IBK), and others. It also contains feature selectors like IG, SU, and others. For the IG feature selection, we depend on the results mentioned on paper [28] as they already used the IG as their selection method.

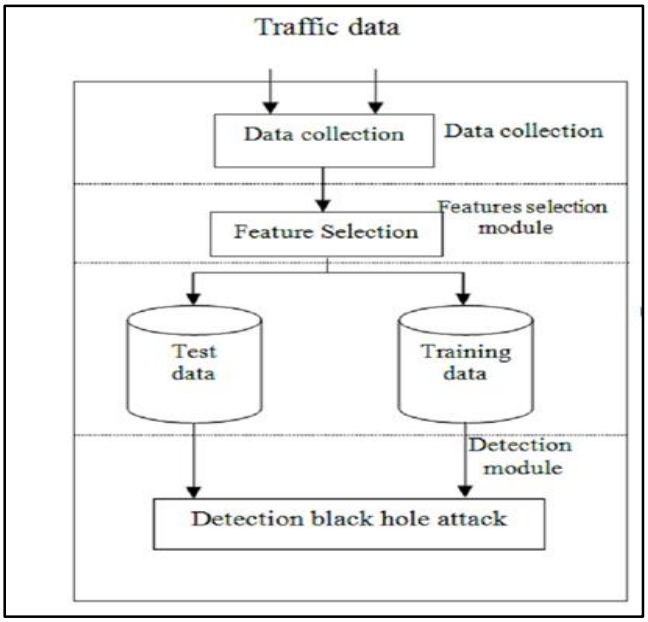


**Figure 7: feature selection phase stages.**

It is essential to say that applying the feature selection phase reduces the overall time of the final black hole detection and prevention algorithm execution over the AODV protocol and decreases the complexity of the proposed algorithm. This can be explained by the fact that having a minimum number of features related to the black hole attack and ignoring the full features to be checked leads to reduce the algorithm complexity and speed up the detection phase. For each of the selection methods, the existing features inside the BDD dataset were analyzed based on the WEKA tool implementation, and then features were filtered based on the weights average calculated using equations (1,2, and 3) in the previous section. The features, which is higher than the average, was chosen to be the most relevant features for the black hole attack. The feature analysis results for the most significant characteristics related to each selection method are shown in table 1 below.

**Table 1: Selected Features using SU, IG, and Relif-f**

| Feature selection method | IG | SU | Relief-F |
|---|---|---|---|
| Selected features | 1-Total number of RREQ sent Feature<br>2-Total number of RREP that forward:<br>3-Total number of the high destination sequence number<br>4-Total number of low count of hops to the destination<br>5-Total number of activities as a source<br>6- number of activities as the destination | 1- Total number of Packets Dropped.<br>2- Route Error<br>3- Rout Reply<br>4- sequence number | 1- Total number of Packets Dropped.<br>2- Route Error<br>3- Rout Reply<br>4- Total number of RREP that forward<br>5- Total number of RREQ sent Feature |

To prove the efficiency of the SU selection method, the J48 classification method was carried out over the BDD data set for the three selected features sets from each of the three selection methods (SU, IG, and Relief-F). To evaluate each of the features list significance in detecting the black nodes. By calculating the list of metrics shown in section 3.1.4.1 below using the classification result values from each feature set.

### 3.1.4.1. Metrics used in Evaluating SU Feature Selection Method Over other Features Selection Methods Based on J45 Classifier:

- Precision (Retrieved Results accuracy) [20], [23], [25], Let TP be the number of black nods classified correctly as black, FP is the number of black nodes classified as regular nods, and FN is the number of regular nods classified as black nodes. Then precision is defined as:

$$\text{Precision} = \frac{TP}{TP+FN} \quad . \qquad (4)$$

- Accuracy: the accuracy metric gives notation for the percentage between correctly classified samples over the whole samples set. and can be calculated as:

$$\text{accuracy} = \frac{TN+TP}{TP+FP+TN+FN} \quad . \qquad (5)$$

- Recall: this metric is the ratio between the numbers of Correctly classified black nodes to the total number of black nodes in the data set [20], [23], [25].

$$\text{Recall} = \frac{TP}{TP+FP} \quad . \qquad (6)$$

It is worth mentioning that the BDD data set consists of 1289 Node reading classified into two main classes black and trust, with 100 nodes in the black class, and 1189 nodes in the trusted class.

### 3.1.4.2. Decision Tree J48 Classifier:

J48 classifier is one of the commonly used classifiers implemented inside the WEKA machine learning tool. In theory, J48 is the primary implementation decision tree named C4.5. J48 consists of two phases the learning phase and the classifying or evaluating phase. In the first phase, the J48 classifier generates a binary tree depending on the attribute values for the supplied training set. In the evaluating phase, the J48 classifier uses the generated binary tree, for each record in the testing set to classify these records [9, 21, 23].

### 3.1.4.3. SU Feature Selection Performance Evaluation:

In this stage, the BDD data set was split into two parts one for the learning phase of the J48 and the other for the testing phase. After that, for each features set extracted from the SU, IG, and Relief-F, the J48 were feed with the features, and the two phases (learning and evaluating) were applied. The results were recorded in the confusion matrix table 2 below.

**Table 2: Confusion Matrix table for the IG, SU, Relief-F over J48 classifier**

| Feature selection method | IG | SU | | | Relief-F | |
|---|---|---|---|---|---|---|
| classes | Normal | black | Normal | black | normal | black |
| Normal (TP, TN) | 1188 | 1 | 1188 | 1 | 1189 | 0 |
| Black (FN,FP) | 0 | 100 | 0 | 100 | 17 | 83 |

Table 3 below illustrates the metrics calculation results and performance comparison based on the confusion matrix.

**Table 3: performance testing results between SU, IG, Relief-F**

| Testing metric | Feature selection method | | |
|---|---|---|---|
| | IG | SU | Relief-F |
| Accuracy | 99.9224% | 99.9224% | 98.6811% |
| Precision | 0.999 | 0.999 | 0.987 |
| Recall | 0.999 | 0.999 | 0.987 |

It is important to mention that we do not compare the classifier performance; instead, we compare the selected feature significance to black hole detection. Even with IG and SU, results are the same, but the selected futures number is reduced between them. Leading to make SU less selected features perform faster over the proposed algorithm in the modified AODV phase. Moreover, the shared messages over the modified protocol will be smaller in size, affecting the all over network overhead to be reduced, which is the target for this research.

## 3.2. Modified AODV Phase:

In this phase, the paper presents an enhanced AODV protocol with new features that allow it to detect and preventing DOS attacks of the types of black hole and wormhole attacks. The enhancement was held by adding a test over the selected features from the first phase inside each node in the MANET network. Moreover, the enhancement was applied in a way that reduces the transmitted messages between different nodes in the network to the minimum, leading to reduce the complexity of the modified algorithm to achieve best protocol performance in terms of ( fast End to end delay, low overhead, and maintain high packet delivery ratio (PDR)). Also, the packet delivery ratio will be a factor of device transmission speed on the MANET network and the traffic average load factor but still affected by the malicious node performing attacks over the network. Therefore, the faster detection algorithm means faster in ignoring the attack effect to achieve higher PRD values. That is why the more reduced features to be tested, and the fewer complexity algorithms with fast performance are the target of this study. Based on the four features extracted from the feature selection phase, modified AODV protocol was implemented as explained below:

### 3.2.1 Handling RREQ

As with original AODV, when the source node (S) should be contacted to a specific destination (D) in the network by using the DPAA-AODV protocol, first it will check if there is an available path to the destination in its Routing Table. In case the route is found, this route is used by the source node to send the data packets through it to the destination node. However, the route discovery process will be initiated by flooding the network with an RREQ message if the path is not found.

As we mentioned previously, the black nodes don't broadcast RREQ messages in the network where the black hole node doesn't generate an information packet, so it doesn't broadcast RREQ to find the route for a specific destination. Furthermore, the black node will not re-broadcast the incoming RREQ messages where it transmits the RREP message immediately for any received RREQ packet. Each node in the network that uses the DPAA-AODV protocol is provided by an extra structure called Black Table in whose function is to contain the nodes that are regarded as a malicious node. Each node will check if there is any black node in its black table or not if there is any black node, the node will ignore this black node and exit the function. Additionally, an RREP packet will be sent to the source node to transmit data and update a routing table if the node is a destination node. Otherwise, the RREP packet will be sent by this node and update the routing table for each node if the node is an intermediate node and has a new route to the destination. In addition to that, if the intermediate node has a route to the destination node, but not fresh, then

there will be a relay in the RREQ packet by an intermediate node, and the routing table will be updated. Finally, there will be a relay in the RREQ packet by an intermediate node, and its route table will be updated if the intermediate node doesn't have any route to the destination node.

### 3.2.2 Handle DATA

According to the fact that the Data packets are dropped due to different reasons such as collisions, time expiration, or by black hole node(s), so the data packet can be dropped due to broken links between the source node and destination node. With regards to the dataset features the "Total number of dropped packets, "the total number of RREP and the total number of RERR is an important characteristic that differentiates between the normal node and black hole node. Firstly, we do some experiments under some seed to calculate a threshold for the number of dropped packets, RREP, and RERR for all networks. Thus, this threshold value is considered in the proposed protocol. Where if a node isn't destination node (intermediate node), then check if the values of the number of packet drop >= threshold of the total number of packets dropped to all networks if the values of REPP >= threshold of the total number of REPP and if the values of RERR >= threshold of the total number of RERR to all networks, then assigned this node as a black node and insert it into the black table. However, retransmit the messages to the next hop to a destination address if a node is an intermediate node and the values of the number of packet drop, REPP, and RERR <threshold of the total number of packets dropped, REPP and RERR respectively. Otherwise, the route is broken or unreachable, and the data will drop, so in this case, the RERR will send to stop sending data.

### 3.2.3. Handling RREP by Source Node

According to the DPAA-AODV protocol, the data packet will not be sent directly by the source node for the first RREP that includes a valid route. Still, it will perform several processes to send the data through the path or wait for another path. These procedures are:

1- If the node that sends a REPP exists in the black table, the REPP packet from this node will be ignored and exit the function.
2- Check if the node's address that sent an RREP is equivalent to the source address, and the REPP is a first one received, then the node will send all data and update its route table.

### 3.2.4. Handling RREP by Intermediate Node

If the black hole node doesn't transmit the receiving RREQ packet, then it also doesn't unicast the receiving RREP packet to the source node where the RREP packet is delivered back to the source node following the same path that was employed by the RREQ packet for this RREP message. According to the Handel REPP by an intermediate node, there are numbers of the process to send the data through the path or wait for another path. These procedures are:
1- If an RREPP packet is at first one of it that reached this intermediate node, then this RREP will be relayed by the intermediate node, set a timer, and update its route table.
2- If the REPP packet that arrived at the intermediate node contains a better route to the destination node, the RREP packet will be relayed by the intermediate node, set timers, and update the routing table.

## 4. Results and Discussion

In this section, metrics used in evaluating the proposed algorithm are discussed, evaluation of the performance of the proposed approach are illustrated. Provide the results and discussions of the performed tests and experiments. Also, talk about the simulator environment and simulation cases adopted.

## 4.1 Metrics Used in performance evaluation

To evaluate the proposed algorithm performance, three other proposed algorithms were adopted to compare with them, the standard AODV, the BDD-AODV algorithm [28], which presented by the paper proposed the BDD dataset. And neural network detection method proposed in [26]. The comparison between the four methods was implemented based on three testing metrics as listed below:

### 4.1.1 Packet Delivery Ratio (PRD)

This metric represents the ratio between the total number of received packets by the node to the total number of packets sent to the same node. equation 4.1 bellow shows the way of calculating the PDR metric value.

$$\boldsymbol{PDR = \frac{Total\ Number\ of\ Data\ Packets\ Received}{Total\ Number\ of\ Data\ Packets\ sent}} \ldots 4.1$$

### 4.1.2. Overhead

This metric represents the ratio between the overall generated control packets such as RREQ and RREP...Etc. to the overall sent data packets of the network. Equation 4.2 shows the calculation way of the overhead metric value.

$$\boldsymbol{Overhead = \frac{Total\ Number\ of\ Control\ Packet\ sent}{Total\ Number\ of\ Data\ Packets\ recevied}} \quad \textbf{...4.2}$$

### 4.1.3 Average End-to-End delay

End–To–End delay metric can be clarified as the duration time needed to transmit the data from source to destination. This metric is significant in this research since the delay in delivering data may occur due to messages caused by enhanced AODV protocols, the route discovery process, propagation, queuing, and transfer time.

## 4.2 GloMoSim Simulator

Global Mobile Information System Simulator (GloMoSim) is a network protocol simulation software for wireless and satellite network simulation environments for large and wireline communication networks. GloMoSim was developed over the parallel discrete event simulation technology provided by Parsec, which is a parallel programming language that uses C programming language. GlomoSim simulator contains ready implementation for MANET networks like Proactive routing protocol, Hybrid routing protocol, and Reactive routing protocol, which contains AODV standard protocol. With an obvious and easy way to understand and update structure and classes.

It also contains all network layers reports over any running scenario, which makes it easy to analyze the reports rapidly. Moreover, the parallel technology used inside GlomoSimmakes it capable of simulating huge networks speedily and efficiently. Therefore, the GlomoSIM simulator was chosen in this paper, for experimental test purpose. Table 4 shows the applied protocol in each layer of the GloMoSim simulator for this study.

***Table 4****:The protocol layers of GloMoSim*

| The layer | The protocol |
|---|---|
| Application | CBR |
| Transport | UDP |
| Network Routing | AODV |
| Mac | IEEE 802.11 |
| Physical (radio propagation) | Two-Ray Ground Reflection |

### 4.3 Simulation environment

It is a matter of the fact that to be able to examine the proposed algorithm, the experiments in this simulation comprise of 15, 20, 25, 30, 35, and 50 nodes. Uniform node placement is the strategy that is used to spread the node in the network. According to this strategy, the network area can be split up into several cells, which in turn are comparable to the number of nodes. However, each node is designated to one of these cells at random. The devices move in the network with a velocity of (0 – 20 m/s) over the square area, whichever dimension is 1000m*1000m. The simulation lasts for 1200 seconds for each and every run, where the results of the simulation are affected by the simulation time. Moreover, the bandwidth will be 2 MB/s, while the radio range will be 250 meters for all network nodes. Through all the experiments, the random-waypoint model is utilized to define the nodes' movement within the network area. Once using this, a unique direction within the area of the network during its trip will be selected by each node. After that, it moves towards the chosen direction with the velocity that is within the range (0 to 20 m/s), approximating the pedestrian speed. Once the nodes complete their trip and arrive in the desired direction, they stop and stay in their location for a period of time, and this is called the Pause time. After that, they start another vacation to move towards this new direction. The simulation parameter for more than one scenario is being explained in Table 5.

**Table 5:**Simulation Parameters

| **Parameter Value** | **Value** |
|---|---|
| Simulation duration | 1200 seconds |
| Simulation area | 1000 * 1000 |
| Number of nodes | 15, 20, 25, 30, 35 and 50 |
| Number of a black node | 1, 2, 3 |
| Mobility Model | Random waypoint |
| Minimum velocity of the nodes | 0 , 0.5 meter/second |
| Maximum velocity of the nodes | 20 , 2 meter/second |
| Pause time | 0, 10, 20 |
| Radio range | 250m |
| Bandwidth | 2 Mb/s |

Constant Bit Rate (CBR) application can be employed in the simulation as a data resources model. Moreover, the data packets' size has been put 512 bytes, which in turn generates many packets through the UDP connection. The experiment in this research is repeated 6times with different random seeds for each time, and the average of the six experiments is calculated for eventually getting more accurate results.

### 4.4 Result and Analysis

For the system evaluation, a sequence of tests has been executed Over the GlomoSim simulator using the different simulation scenarios, as mentioned in the previous section, to extract the test's metrics explained in section 4.1, which are overhead, PDR, and the end to end delay. 50 nodes were adopted in the simulation cases, and all the metrics values were calculated for the proposed Modified-AODV and the other three referenced algorithms. Figure 8 shows the overhead graph for the proposed algorithm and the other three algorithms (standard AODV, BDD-AODV, and ANN-AODV). The network contains zero black nodes to test the natural performance of the proposed protocol compared with standard AODV and other modified versions.

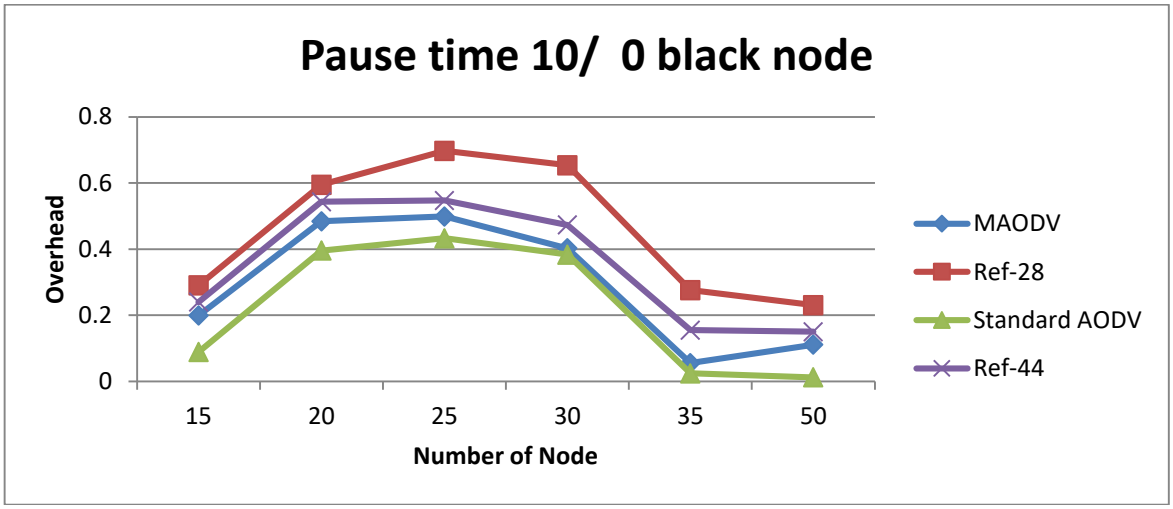


**Figure 8:Overhead, Zero Black holes, Pause 10**

As shown in figure 10 the new proposed algorithm outperforms the other presented protocols in references [28] and [44], in terms of the overhead. Also, the other messages used in the proposed protocol does not generate high extra overhead traffic compared with the standard AODV protocol, which maintains the protocol efficiency. As shown in Figure 9, the additional overhead due to the proposed protocol over the standard AODV was reduced 41.71% in comparison to by 36.55% and 37.32% for the other two algorithms in [28] and [26].

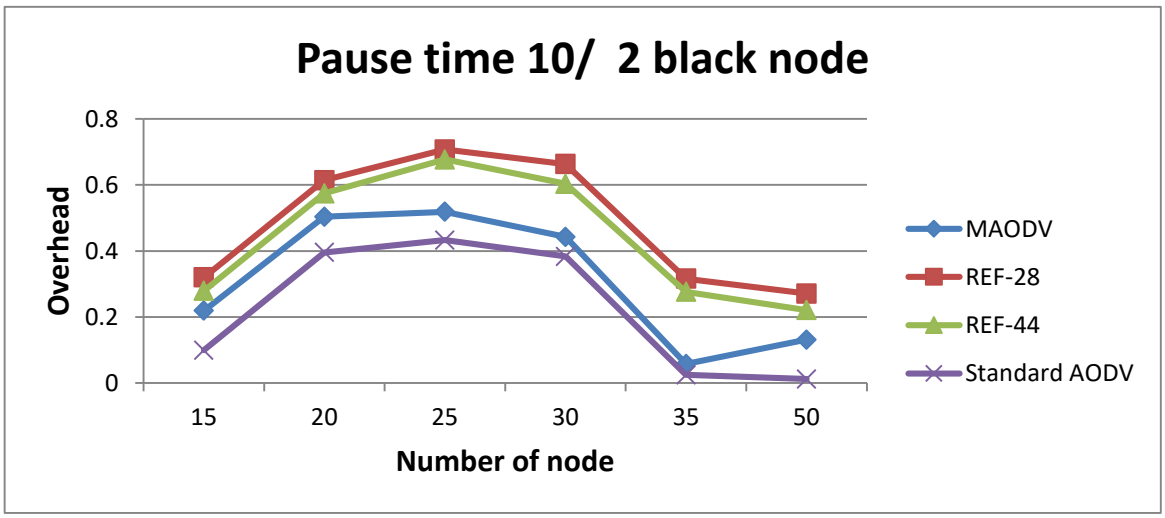


**Figure 9:Overhead, Two Black holes, Pause 10**

Figure 11, also for the four protocols, when the node increases from 15 to 25 nodes, the overhead increases. The explanation for this is the increasing number of nodes in the network that results in subsequently an increase in the number of control packets (e.g. RREQ and RREP), which in turn are transmitted through the network. Therefore, the overhead increases as the number of nodes increases in the network. However, Figure 9 shows that the overhead of running the BDD-AODV is more than the overhead by running the other two protocols. However, the performance of the overhead of the proposed algorithm is better than the other two protocols compared to the original AODV protocol, but higher than the original AODV protocol. The reason for that goes back to the fact of how the black hole attack largely influences the original AODV protocol and that no function can detect these attacks. Thereby, the route discovery process in this protocol is deficient in comparison with the new modified protocol, do not forget to mention the extra messages needed to be sent in the newly proposed protocol to handle black hole attacks. On

another level, the running overhead of the BDD-AODV and ANN-AODV protocols is more than the overhead of running the proposed AODV, and this is because there are more conditions in BDD-AODV protocol, which in turn need to send more control packets (RREQ, RREP, RERR, etc...). The neural network parameters and results add extra message overhead on ANN-AODV. While the conditions in the proposed protocol are much less and faster to execute.
For a network attacked by two black holes, in figure 10, the Original AODV shows the highest end-to-end delay, while the proposed algorithm displays the best end-to-end delay results.

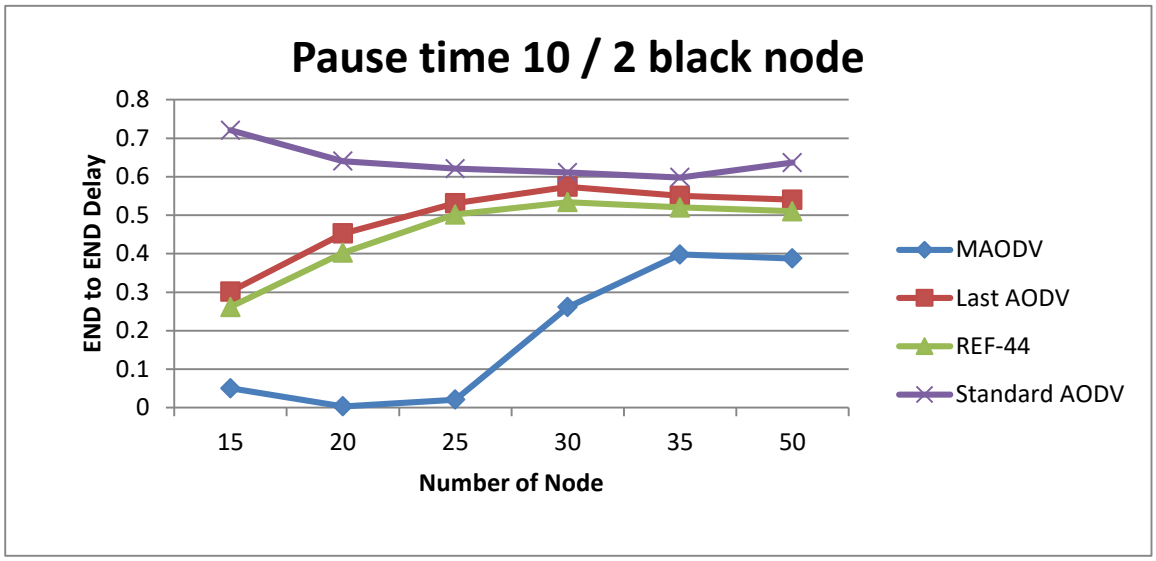


**Figure 10:Delay, Two Black holes, Pause 10**

The standard AODV protocol increases the delay to very high values, which means that the network is almost hanged up, and operationally faulted. While the proposed algorithm shows a low end to end delay time. This is through the fact that the algorithm is capable of detecting the blackhole attacks in early stages and eliminating their effects directly, which appear in the standard AODV because the black nodes operating inside, the more packets dropped and not reaching their real destinations. Also, the more nodes involved in the network means the more route request probabilities and more messages, leading to more end to end delay, as shown in nodes from 25 to 50 for the four protocols.

Figure 13 shows the packet's delivery ratio results, which are obtained by running the proposed algorithm, BDD-AODV, ANN-AODV, and the standard AODV protocols in the ad-hoc network that is attacked by three black hole nodes when pause time equals 10.
According to Figure 11, the effect of black hole attack can be clarified based on the packet delivery ratio as:

- effect of the black hole node is proportional to the position of the node inside the network, as the black nodes exist on the edges of the network intercept only a little amount of the whole network request packets. Therefore, it does not affect the network majorly. On the other hand,

the black nodes that exist in the middle of the network may cause a massive drop in the network traffic, as shown in figure 11 for the standard AODV protocol.

- the proposed algorithm shows the highest PDR over the other three protocols, meaning that it has a fast capability of detecting and ignoring the black hole attack. Also, the ANN-AODV network was capable of delivering relatively

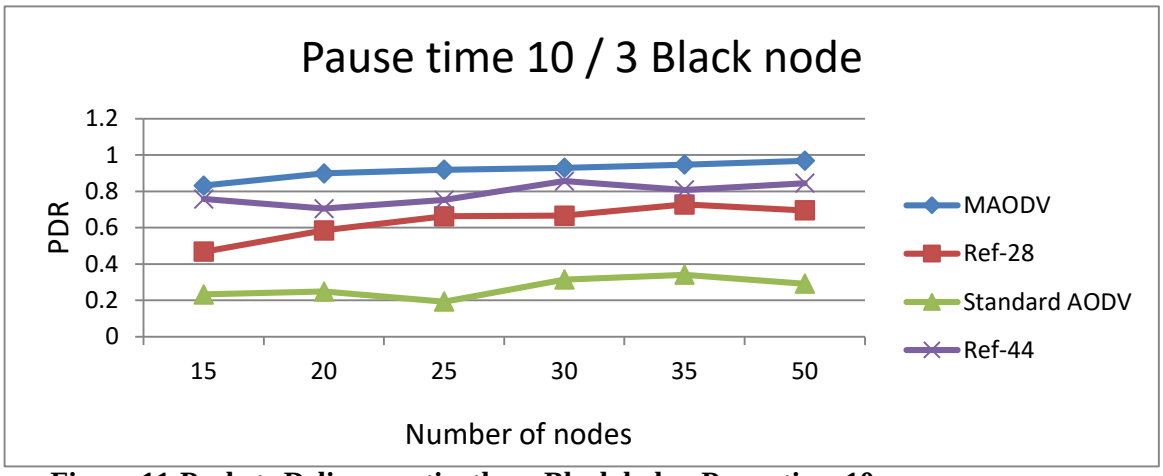


**Figure 11:Packets Delivery ratio, three Black holes, Pause time 10.**

good PDR, but still miss some black nodes in classification and has higher latency in detecting the black attacks. Moreover, BDD_AODV has lower PDR than ANN-AODV regarding the fact it does not regenerate a new path after ignoring detecting black nodes, meaning which causes to lost most of the traffic in that ignored route. Therefore, the proposed algorithm was the best between the three protocols.

The same results can be shown in figure 12, using six black nodes and zero pause time, as the proposed algorithm had the best PDR values, compared to BDD_AODV and ANN-AODV.

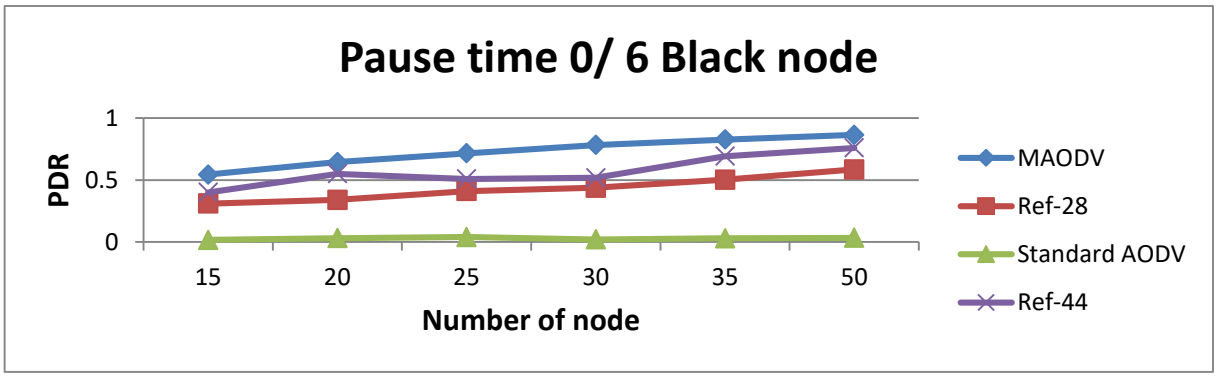


**Figure 2:Packets Delivery ratio, six Black holes, Pause time 0.**

While the effect of six black nodes paralyzed the network on the standard AODV as the curve shown in the same figure, also, the figure shows that the proposed algorithm PDR increases while the number of nodes increases. This is due to the fact that increasing the number of nodes raises the number of routes available to deliver data from source to destination, therefore, reducing the unreachable destination problem due to detected and ignored black nodes, which may cause loss

of connections between nodes especially when there are no other valid paths between nods than going through the black node.

### 5.1 Conclusion

Sharing data through networks between different devices had become one of the most demanding requirements now a day; because of that, network establishment and protocols that manage the devices inside it are a critical topic. Moreover, on areas that do not have ready infrastructures to support network connections, there was a need to develop networks between devices within their coverage ranges depending on devices themself only, without having to have any infrastructure. MANET networks were the solution for this problem where protocols like AODV act to manage the devices inside. As a result of such network characteristics, AODV protocol was vulnerable to a list of attacks like DOS attacks, which contains attacks like a black hole and wormhole attacks. In this research, a new algorithm for black hole attack detection and prevention was presented based on four features extracted from the AODV protocol. The four features were evaluated by classification method called J48 to prove their capability of defining black hole nodes. Moreover, the presented algorithm implements straightforward test classification criteria over the regular AODV protocol to allow detection and sharing of the identities of the black nodes. The results of the experimental results were implemented using GlomoSim simulator over 50 nodes, and compared to 3 other previously proposed algorithms (Standard AODV, BDD-AODV, and ANN-AODV), where the new proposed algorithm proofed its capability in detecting and preventing black hole attacks with higher efficiency average on the END-TO-END time delay of 67.19% faster over the standard AODV protocol, 55% faster than the BDD-AODV, and 49% faster than the ANN-AODV. Also, in terms of overhead factor, the proposed algorithm showed better performance than other compared algorithms with a lower average of 30.92% compared to BDD-AODV and 48.7% less value compared ANN-AODV algorithm.

## 5.2 Suggestions for Future Work

For future work, a new upgrade for the Enhanced AODV protocol will be implemented to allow the algorithm to change the thresholds for the selected features dynamically during operation. Also, add new testing criteria for detecting collaborative black hole attacks by building new BDD for collaborative nodes and their list of related features.
Moreover, study other types of attacks like wormhole attacks and suggest a new algorithm for detecting such attacks.

## References:

1. Khanna, N. "Mitigation of Collaborative Blackhole Attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol".International Journal of Future Generation Communication and Networking, volume 9, page(s), 157-166, 2016.
2. Mitrokotsa, A., and Christos Dimitrakakis. "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection." Elsevier, volume 11, page(s): 226-237, 2012.
3. Manwani, P., &Dubey, D. (2016). "Hybrid Protocol for Security Peril Black Hole Attack in MANET," International Journal of Computer Engineering In Research Trends, volume 3, page(s):92-97, 2016.
4. Bawa, K., &Rana, S. B. "Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization".International Journal of Current Engineering and Technology, volume 5, page(s), 2015.
5. Firas Al Balas, Omar Almomani, Reema M. Abu Jazoh, Yaser M. Khamayseh, Adeeb Saaidah. "An Enhanced End to End Route Discovery in AODV using Multi-Objectives Genetic Algorithm", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019
6. Sherif, A., MahaElsabrouty, and Amin Shoukry. "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)".IEEE, page(s): 346-352, 2013.

7. Balan, E. V., Priyan, M. K., Gokulnath, C. & Devi, G. U. "Fuzzy based intrusion detection systems in MANET". Elsevier, volume50, page(s) 109-114, 2015.
8. 8.Baishali Goswami, A NOVEL INTRUSION DETECTION SYSTEM FOR DETECTING BLACK-HOLE NODES IN MANETS, International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (GRAPH-HOC) Vol.8, No.2, June 2016.
9. Thu Zar Phyu , Nyein Nyein Oo . Performance Comparison of Feature Selection Methods. MATEC Web of Conferences "mateconf", published by EDP Sciences, 2016.
10. Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack InBodv Based Manet." In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009
11. Marcus Okunlola Johnson Computer Science & Informatics University of East London (UEL)London, UK,A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks,International Journal of Computer Applications(8887 - 0975) Volume 174 - No.4, September 2017.
12. 12.A. Mitra, R. Ghosh, A. Chakraborty, D. Srivastva, "An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network" in IJARCSSE, 2013. G. Wahane, A. Kanthe, techniques for detection of cooperative Black hole Attack in MANET" in IOSR-JCE, 2014.
13. Firas Albalas, Munner Bani Yaseen, Asma'a Nassar. "Detecting black hole attacks in MANET using relieff classification algorithm", Proceedings of the 5th International Conference on Engineering and MIS - ICEMIS '19, 2019
14. Assistant Professor Department of ECE SJCET, Palai, ANN to Detect Network under Black Hole Attack, International Journal of Computer Applications (0975 – 8887) International Conference on Emerging Trends in Technology and Applied Sciences (ICETTAS 2015).
15. 14.Ramanpreet Kaur et al, BLACKHOLE DETECTION IN MANETS USING ARTIFICIAL NEURAL NETWORKS, International Journal For Technological Research In Engineering, Volume 1, Issue 9, May-2014.
16. Manwani, P., &Dubey, D. (2016). "Hybrid Protocol for Security Peril Black Hole Attack in MANET", International Journal of Computer Engineering In Research Trends, volume 3, page(s):92-97, 2016.
17. Jawandhiya, "Intelligent Secure Routing Model For MANET". Proceedings ofComputer Science and Information Technology (ICCSIT), IEEE, volume 3, page(s): 452 -456, 2010.
18. JaydipSen, SripadKoilakonda, ArijitUkil, "A Mechanism for Detection ofCooperative Black Hole Attack in Mobile Ad Hoc Networks", Proceedings ofIntelligent Systems, Modelling and Simulation (ISMS) , IEEE, page(s): 338 - 343, 2011.
19. Lee, S.-J., Elizabeth M. Belding-Royer, and Charles E. Perkins. "Scalability study of the ad hoc on-demand distance vector routing protocol." International Journal of Network Management, volume 13, page(s): 97–114, 2003.
20. Tamilselvan, L., &Sankaranarayanan, V. "Prevention of co-operative black hole attack in MANET". Journal of Networks, volume 3, page (s) 13-20, 2008.
21. Sumanth, K., Gutta, S., Umar, S., Kumar, K. K., &Hussain, M. A. (2016). "A PROPOSAL FOR MITIGATION OF GRAY HOLE ATTACK IN WIRELESS MESH AD-HOC NETWORKS USING S-DSDV". Journal of Theoretical and Applied Information Technology, volume84, page(s):79-87, 2016.
22. Garg, N., and R. P. Mahapatra."MANET Security issues." IJCSNS International Journal of Computer Science and Network Security, volume 9, page(s): 241-246, 2009.
23. Bharti, A. "PREVENTION OF FLOODING ATTACK IN MANET USING OPNET". International Journal of Collaborative Research in Engineering Sciences, volume 1, page(s): 1-6, 2014.
24. Shakshuki, E. M., Nan Kang, and Tarek R. Sheltami."EAACK—a secure intrusion-detection system for MANETs." Industrial Electronics, IEEE Transactions, volume16, page(s): 1089-1098, 2013.
25. Singh, H. P., and Sanjeev Sharma. "Guard against cooperative black hole attack in Mobile Ad-Hoc Network." International Journal of Engineering Science and Technology, volume 3, page(s): 5629-5634, 2011.
26. Sherif, A., MahaElsabrouty, and Amin Shoukry. "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)".IEEE, page(s): 346-352, 2013
27. Ganapathy S, Kulothungan K, Muthurajkumar S, Vijayalakshmi M, Yogesh P, Kannan A. "Intelligent Feature Selection and Classification Techniques for Intrusion Detection in Networks: A Survey". EURASIP Journal on Wireless Communications and Networking, volume 1, Page(s):1-16, 2013.

28. Kauser, SkHeena, and P. Anil Kumar. "MANET: Services, Parameters, Applications, Attacks &Challenges."International Journal of Scientific Research in Science, Engineering and Technology, volumw2, page(s):4-9, 2016.
29. Ms.ChetanaKhetmal, P. S. K., Mr.NileshBhosale. "MANET: Black Hole Node Detection in AODV". International Journal of Computational Engineering Research, volume 3, page(s): 79-85, 2013.
30. Bhatti, K., and SonamDhawan. "An Improved Performance of MANET using AODV Protocol for Black Hole Detection." IJRCCT International Journal of Research in Computer and Communication Technology, volume3, page(s): 627-632, 2014.
31. Balan, E. V., Priyan, M. K., Gokulnath, C. & Devi, G. U. "Fuzzy based intrusion detection systems in MANET". Elsevier, volume50, page(s) 109-114, 2015.
32. Patel, M., Sharma, S., &Sharan, D. "Detection and Prevention of Flooding Attack Using SVM". In Communication Systems and Network Technologies (CSNT), page(s): 533-537, 2013.
33. Khanna, N. "Mitigation of Collaborative Blackhole Attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol".International Journal of Future Generation Communication and Networking, volume 9, page(s), 157-166, 2016.
34. Mohamad Tahir, H., Hasan, W., Md Said, A., Zakaria, N. H., Katuk, N., Kabir, N. F., ... &Yahya, N. I. " Hybrid machine learning technique for intrusion detection system". 5th International Conference on Computing and Informatics (ICOCI), page(s): 464-472, 2015.
35. PatilT. R, Sherekar M. S. "Performance Analysis of Naive Bayes and J48 Classification Algorithm for Data Classification". International Journal of Computer Science and Applications, volume 6, page(s): 256-261, 2013.
36. Chandolikar N. S., Nandavadekar V. D. "Comparative Analysis of Two Algorithms for Intrusion Attack Classification Using KDD Cup Datase"t. International Journal of Computer Science and Engineering (IJCSE), volume 73, page(s): 81-88, 2012.
37. Mukherjee, S., & Sharma, N. "Intrusion detection using naive Bayes classifier with feature reduction". Elsevier, volume 4, page(s):119-128, 2012.