A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks

Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein
Jordan University of Science and Technology, Dept of Computer Science, Irbid, 22110, Jordan
{yaser, masadeh, mardini}@just.edu.jo, abdelraheem_1982@yahoo.com

Abstract: An ad hoc network is a collection of infrastructureless nodes, cooperating dynamically to form a temporary network which meets certain immediate needs. The lack of infrastructure implies that the nodes are connected peer-to-peer. Therefore, each node acts as a router beside its main role as a host. With the increased number of mobile devices, the applications of ad hoc network increased dramatically to capture different domains such as: academic communication, and mobile conferencing beside its traditional domains such as: military communication, and emergency communication.

Security issues become more challenging in ad hoc network due to its dynamic nature which allows any node to freely join as well as leave the network without having a physical address or getting permission. Ad hoc networks are vulnerable to different kinds of attacks such as: denial of services, impersonation, and eavesdropping.

This paper discusses one of the security problems in ad hoc networks called the black hole problem. It occurs when a malicious node referred as black hole joins the network. The black hole conducts its malicious behavior during the process of route discovery. For any received RREQ, the black hole claims having a route and propagates a faked RREP. The source node responds to these faked RREPs and sends its data through the received routes. Once the data is received by the black hole, it is dropped instead of being sent to the desired destination.

The proposed protocol is built on top of the original AODV. It extends the AODV to include the following functionalities: source node waits for a reliable route; each node has a table in which it adds the addresses of the reliable nodes; RREP is overloaded with an extra field to indicate the reliability of the replying node. The simulation of the proposed protocol shows significant improvement in the terms of: packet delivery ratio, number of dropped packets, and end-to-end delay. The overhead still needs more researches.

Keywords: Black Hole, Routing, Ad Hoc Networks, Behavioral Analysis, Mobility.

1. Introduction

An ad hoc network is a collection of infrastructureless nodes, cooperating dynamically to form a temporary network which meets certain immediate needs. The lack of infrastructure implies that the nodes are connected peer-to-peer; therefore, each node plays its role as a host beside its role as a router [1, 2].

The applications of ad hoc networks are growing significantly, and there are different domains where it is preferable to use ad hoc networks for communication, in order to reduce the time and cost of setting up an infrastructured network. The following are the main applications of ad hoc networks: military communication, mobile conferencing, and emergency and rescue missions [12, 13].

Ad hoc networks have the following features: power limitations, node mobility, topology changes, broadcast transmission medium, self organization and configuration of the nodes. These features have a direct impact on the following: link reliability, routing information, and network security [3, 4]. Ad hoc network communication systems consist of five layers. Each layer is implemented separately and provides a set of services to the next higher layer. The following are the layers of ad hoc networking systems: physical layer, data link layer, network layer, transport layer, and application layer [16, 17].

Routing is an essential operation in ad hoc networks. Any successful breakthrough for the routing has a direct impact on the performance of the whole network. This is the reason for which the routing is being targeted by different kinds of attacks.

Security is one of the main issues for networks. It becomes more challenging in ad hoc networks due to the lack of central access point to monitor node behavior and to manage node membership [4]. Any network security system aims at satisfying the following goals: privacy and confidently, authenticity, integrity, and access control. All security attacks on any system are a violation of one or more of these goals [5]. An ad hoc network is vulnerable to the following types of attacks: denial of service (DoS) which influences the availability of a certain node or even the services of the entire network, impersonation attacks which occurs when external nodes exploit the weak authentication of the network to join it as a normal node and begin to carry out its malicious behavior such as propagating fake routing information, eavesdropping to obtain some confidential information that should be kept confidential during the communication, and attacks against routing which include network partitioning, routing loops, and route hijacks [3].

This paper discusses the black hole problem which is classified as a denial of service problem [6]. The problem occurs when a malicious node joins the network with the intention of intercepting transmitted packets of data and dropping them instead of delivering them to the desired destination.

2. Statement of the Problem

The problem occurs when a malicious node referred as black hole joins the network and snoops on its neighboring nodes. The black hole receives the route requests from its neighboring nodes and sends fake route replies immediately claiming that it has a direct link to the destination node.
The incoming route reply from the malicious node could be received by the source before receiving other routes. In such case, the source node uses a route containing the malicious node and sends its data through it. As the malicious node receives data packets, it drops them instead of sending them to the destination, resulting in more message overhead and causing a failure in the routing protocol that covers a part of the network. The occurrence of the black hole problem and the operations of the malicious node depend on the routing protocol.

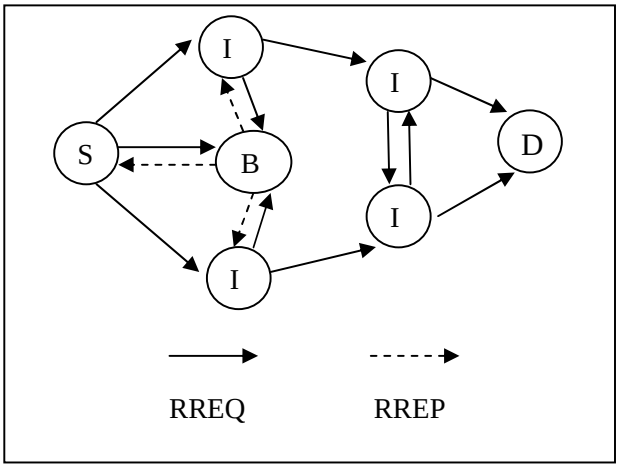

Figure 1: Black hole problem

Figure 1 shows a network consisting of seven nodes: the source (S), the destination (D), the black hole (BH), and four intermediate nodes (Ij). Firstly, S sends a RREQ asking for a route to D. The RREQ is received by all of its neighboring nodes (I1, BH, and I2). As shown in Figure 1, both I1 and I2 re-broadcast the RREQ. On the other hand BH does not re-broadcast the RREQ, where BH is a black hole. Instead it replies immediately claiming that it has a direct link to D. As usual, S responds to the RREP by sending the data to D through BH. Once the data is received by BH, it will be dropped directly. Moreover, BH will also send the same RREP to both I1 and I2 as soon as it receives the re-broadcasted RREQ from them. This implies that BH will be added to the route table of both I1 and I2 as the first hop to D.

3. Related Work

Different ideas and studies discuss the black hole problem and its effects on the routing process. One of them proposes to solve the problem by preventing the intermediate nodes from replying to the received route requests. Such idea forces the intermediate nodes to broadcast the route request. In this solution, only the destination node holds the responsibility of sending the route reply. Such idea limits the cooperative behavior of the nodes, where it prevents the exchange of route information between the nodes, and hence increases the overhead of route discovery.
V Sankaranarayanan and Latha Tamilselvan [6] discuss the problem of black hole and its effects on the AODV routing protocol, and propose a solution that detects the route and ensures its reliability before sending the data packets through it. The proposed solution modifies the AODV protocol to handle the problem as follows: when the source node receives a route reply it does not send data through it immediately, instead it waits until receiving other routes from other neighboring nodes and checks the safe route to send data through. The source node runs a timer to collect the route replies from the neighboring nodes. The source node maintains the collected route replies in a table. After the timer reaches the timeout value, the source node chooses the most reliable route from the table of collected routes.
Routes containing more repeated common nodes are considered more reliable by the source, if there are no repeated common nodes in the routes; the source node considers the route as reliable if the replying node provides information about its next hop in the route [6]. Figure 1 shows the proposed solution in [6].
Marti, Giuli, Lai and Baker proposed a solution based on two techniques: watchdog, and path rater. In the first technique, each node monitors the behavior of its neighboring nodes and runs a counter to record the number of errors committed by them. Any node that exceeds the allowed number of errors is removed from the network. The second technique supports the first technique by computing trust values for each node in the network according to its behavior. This value is increased or decreased proportional to the behavior of the node. The trust values of the nodes are exchanged over the network. The more trusted nodes in the route the more priority of using it to send data through [8]. Both, watchdog and path rater approaches, encourage node misbehavior such as selfishness and misbehaving nodes to transmit packets without punishing them [9].
Wei Li, and Agrawal [10] present a study to solve the black hole problem as follows: the source node sends a route request as usual, it receives route replies from neighboring nodes, and delays transmitting data until checking the reliability of the received routes (route is considered reliable if the source node has routed data through the replying node successfully).
To check the reliability of the replying node, the source sends a further route request (FRQ) to the next hop of the replying node. FRQ is sent through a route which does not contain the replying node. The next hop of the replying node responds by a further route reply (FRR) and provides information about the replying node and about the destination node. If the received information in the FRR indicates that there is a route from the next hop of the replying node to the replying node, and there is a route from the next hop node to the destination, then the replying node

is reliable. The received route is added to the reliable routes, and the source node announces the replying node as reliable by broadcasting a message to its neighbors [10].

Latha Tamilselvan and Dr. V Sankaranarayanan [9] present a study which considers the cooperative behavior of two black hole nodes working as a team. The study borrows the concept of path rater from [8] which computes the trust values of each participating node. Each node has a fidelity table in which it records the fidelity values of the participating nodes. The fidelity value of a given node is incremented or decremented proportional to its behavior in the network.

The protocol works as follows: the source node sends a RREQ and waits for a predefined period of time to collect the RREPs. Once the routes are collected, the source checks the fidelity values of both the replying node and its next hop in each received route. The source node chooses the route with the highest fidelity values and sends its data through. If there is more than one route with the same fidelity values, the source chooses the one with least number of hops.

Once the destination node receives the data it sends an acknowledgement to the source informing it that it has successfully received the data. The source increments the fidelity values of the replying node and its next hop if the acknowledgment is received, and decrement them if the acknowledgement is not received. The updates of the fidelity values are exchanged over the network. When the fidelity value of the replying node drops to zero, both of the node and its next hop are considered as a cooperative team of black hole nodes and eliminated from the network.

Zahi Ya'quob [24] discusses the problem, and proposes a solution which depends on the ability of each node to listen to its neighbors. The proposed protocol woks as follows: the source nodes sends a route request and waits for a period of time to collect the route replies. Once the route replies are received, the source node chooses the route with the least number of hops and sends its data through. The source node listens to ensure if the first hop sends the data to its next hop. Not only the source node listens, also each node in the route listens to ensure that its next hop transmitted the data, until the data reaches the destination. During the transmission, a timer is set in each node after sending the data to the next hop. Each node must transmit the data before the timer of its previous hop reaches the timeout value; otherwise the node is announced as a black hole by its previous hop whose timer has already expired.

Another type of black holes is discussed by Payal N. Raj and Prashant B. Swadas [29]. In this type, the black hole propagates a RREP with a high sequence number for the destination. As the source receives this RREP it either adds the received route to its route table if it is not already exist or updates the current route if it is already exist.

The proposed solution in [29] modifies the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbors.

The threshold represents the usual increment of the sequence number of the replying node. It is the computed average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

Table 1 provides a summary of the above-mentioned protocols from the performance point of view. The table provides the comparison of each study separately, due to the differences in the environment and the parameters of the simulation between the presented studies. In table 1, both PDR and NDP correspond to packet delivery ratio and number of dropped packets respectively. Note that number of dropped packets (NDP) is considered only in the study [24].

Note that some of the intervals mentioned in the table are increasing, where other intervals are decreasing. Basically, this depends on the simulation parameters and the figures provided in the corresponding study. The sentence “not provided” appears in two cells in the table which indicates that theses values are not provided in the study.

Table 1: Comparison between the performances of the black hole protocols

	Protocol of [6]	**AODV with BH**
PDR	98% – 85%	5% – 25%
Delay	6 ms – 8 ms	Around 1 ms
Overhead	0.05 – 0.3	0.05 – 0.3
	Protocol of [9]	**AODV with BH**
PDR	Around 60%	About 1%
Delay	0.4 ms – 1 ms	0.4 ms – 0.7 ms
Overhead	15% – 65%	5% – 30%
	Protocol of [24]	**AODV with BH**
PDR	55% – 65%	45% – 25%
NDP	50 – 55	90 – 125
Throughput	80000 – 90000 b/s	70000 – 55000 b/s
Overhead	5 – 10	5 – 35

	Protocol of [29]	**AODV without BH**	**AODV with BH**
PDR	95% – 99%	95% – 99%	Around 10%
Delay	0.4 ms – 4.8 ms	0.4 ms – 4.8 ms	Not provided
Overhead	0.20 – 0.28	Not provided	0.20 – 0.28

4. Proposed Protocol

The default case in any routing protocol is to send the data packets through the first received route. Such behavior reduces the burden of the following: setting a timer, waiting for further routes, and buffering more data packets. In the typical cases, the protocol works properly and performs the task with the desired results, but when the network is attacked by a black hole node, the performance of the protocol decreases dramatically. To propose a solution to the problem, the behavior of the black hole node needs to be addressed more specifically.

4.1. Behavioral Analysis of the Black Hole Node

The black hole node is a strange malicious node joins the network with the intention of dropping the transmitted data packets instead of delivering them to the desired destination. The following are the main behavioral characteristics of the black hole node:

It snoops on its neighbors to discover which node is preparing to send a RREQ. For any received RREQ, the black hole node propagates a RREP claiming that it has a direct link to the destination.

It constantly attempts to locate itself within the transmission range of any source node in order to reply as quickly as possible. This requires a continual movement of the black hole in the network. Moreover, its movement speed may be higher than the normal nodes.

Referring to the second characteristic, the black hole never contributes in the operation of route discovery (i.e. never broadcasts the received RREQs). Moreover, for any route including a black hole, the black hole always appears as the last hop before the destination.

Referring to the third characteristic, the number of the routes that the black hole contributes in them is greater than the number of routes that the normal node contributes in them.

4.2. The Proposed Protocol

The proposed protocol modifies the behavior of the original AODV to include the following techniques:
Every node is provided with a data structure referred as trust table. This table is responsible for holding the addresses of the reliable nodes.
The RREP is extended with an extra field called trust field. This field indicates the reliability of the replying node (i.e. the propagating node of the RREP).
The source node sends its data only if the RREP is propagated by a reliable node. Otherwise it waits for further RREP.
The details of the protocol are given in the following sub-sections.

4.2.1. Route Discovery

When a source node (S) needs to communicate with a destination node (D), the source node initiates the process of route discovery by flooding the network with a RREQ.

Propagating RREQ by S

If S has data packet to send and there is no route to D then it does the following:

Prepare the RREQ
Broadcast it

4.2.2. The Trust Table

Before the communication takes place the trust table is initialized to null for all the participating nodes. In order for a node to be added to the trust table of another node, it needs firstly to pass the behavioral analysis filter. This filter considers the following aspects:

- Continual change of neighborhood. The black hole moves continually resulting in a continual change in the state of the neighborhood with the other nodes. Normal node can detect such behavior by observing changes in its neighborhood table.
- Number of active connections that a node is part of. Normal node can detect this by checking its route table.
- The link activity duration. The duration of the link activity between a given node and the black hole is long compared to the normal average duration of the link activity.
- Each node in the network keeps a file of history registers information about its neighbors regarding the mentioned above aspects. This file is saved in the cache and acts as a reference which supports the filter with the needed information about a given node (i.e. the broadcasting node of the RREQ). Once the network is flooded with a RREQ, each node receives the RREQ checks whether the broadcasting node passes the filter or not. Once the broadcasting node passes the filter, it is added to the trust table. The process is repeated until the RREQ is received by the replying node. Figure 2 shows the behavioral analysis filter.

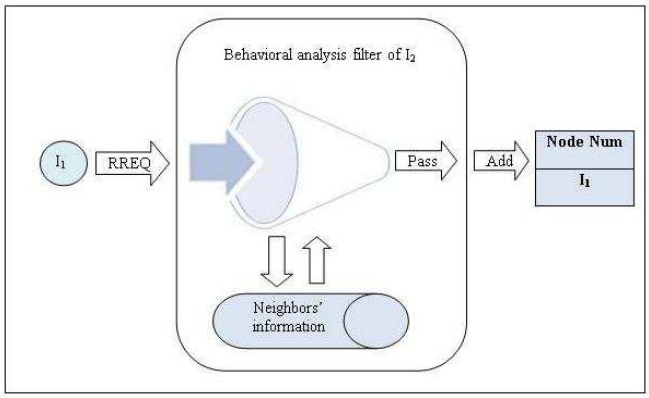

Figure 2: The behavioral analysis filter

The following box shows the algorithm of handling RREQ by the intermediate nodes.

Handling the RREQ by I

When I receives a RREQ, it does the following:

If (broadcasting_node pass the filter)
Add broadcasting_node to its trust table

If I has a route to D then
It propagates a RREP

Else
It re-broadcasts the RREQ

Figure 3 shows the process of adding a new input to the trust table during the trip of the RREQ from the source to the destination.

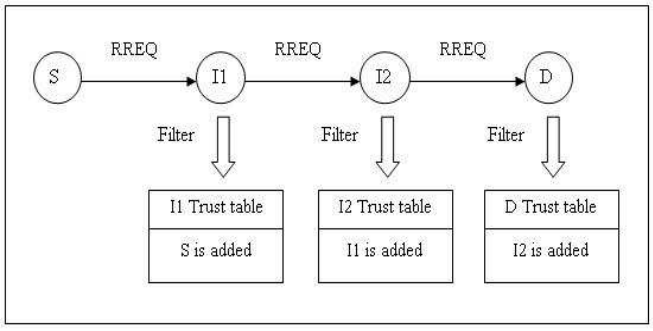

Figure 3: Adding a new input to the trust table

4.2.3. Handling RREQ by the Replying Node

The replying node is one of the following three possibilities: the destination itself, an intermediate node has a real route to the destination, or a black hole claims having a route. Once the replying node receives the RREQ, it prepares the RREP. The RREP is overloaded with an extra field to indicate the reliability of the received route.
The replying node extends the original RREP of the AODV with a field of integer value to express the reliability of the replying node. This field is initialized to zero by the replying node, and may change its value in the first hop of the reverse path. Note that the replying node only initializes the field. The reliability of the route is not given by the replying node. Evaluating the reliability of the route takes place in the first hop of the reverse path, because it is the most expected node to have information about the replying node. The algorithm of handling the RREQ and preparing the RREP is given in the following box.
The algorithm is given in case the replying node is the destination itself. The scenario of the other two cases is similar to that of the destination.

Handling RREQ by D

When D receives a RREQ, it does the following:

If (broadcasting_node pass the filter)
Adds the sending node to its trust table

Prepares RREP, and initializes its trust field to 0

Sends the prepared RREP through the reverse path

4.2.4. Handling RREP by the Remaining Nodes

Once the RREP is received by the first hop of the reverse path, the identity of the replying node is determined, and the value of the trust field is modified accordingly. Basically, the first hop of the reverse path is the most critical node in it. It is the only node which is qualified to determine the identity of the replying node and change the value of the trust field accordingly.
By receiving the RREP by the first hop in the reverse path, the value of the trust may be modified as follows:
If the replying node is the destination itself, the trust value is changed from 0 to 2.
If the replying node is not the destination, but still exists in the trust table, then the trust value is changed from 0 to 1.
If the replying node is neither the destination nor exists in the trust table, then the trust value is not changed.
Figures 4 shows how the RREP is handled by the first hop of the reverse path, in case of receiving a RREP from the destination itself.

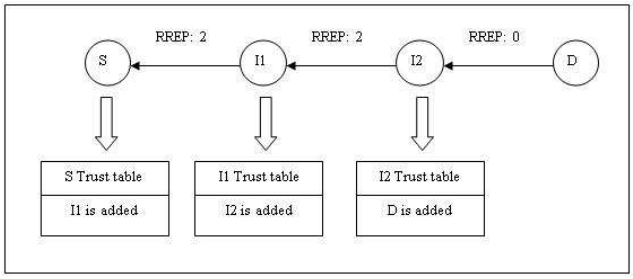

Figure 4: First case of the algorithm

Figure 5 shows how the RREP is handled by the first hop of the reverse path, in case of receiving a RREP from a reliable intermediate node (exist in the trust table).

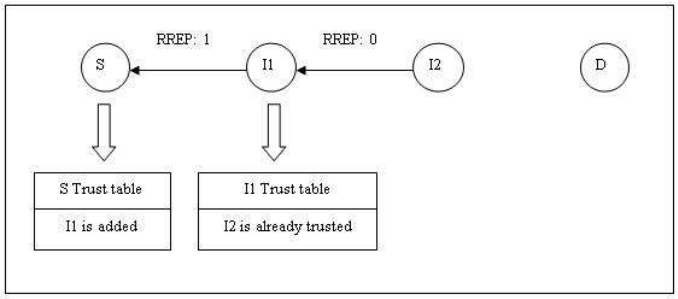

Figure 5: Second case of the algorithm

Figure 6 shows how the RREP is handled by the first hop of the reverse path, in case of receiving a RREP from a node which is not exist in the trust table (could be black hole).

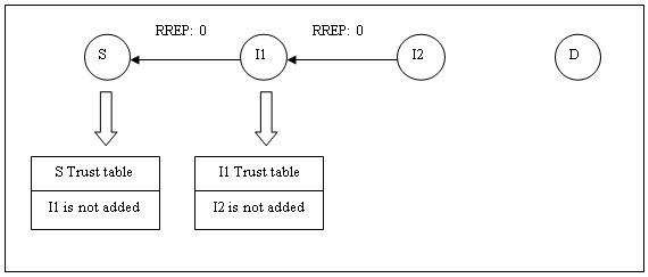

Figure 6: Third case of the algorithm

As the RREP moves in the reverse path, each node checks the trust field. If the trust field is 1, or 2, then the current node adds its last hop to its trust table for further use. The following box shows the algorithm of handling RREP by the first hop of the reverse path.

Handling RREP by the first hop in the reverse path

When I receives a RREP, it does one of the following depending on the replying node

Case 1: the replying node is an intermediate node, and not exists in trust table
RREP is sent through the reverse path without modifying the trust field

Case 2: the replying node is an intermediate and exists in the trust table
Modify trust field from 0 to 1, then send the RREP

Case3: the replying node is D
Modify trust value from 0 to 2, then send the RREP

For the rest of the nodes in the reverse path, the algorithm of handling the RREP is given in the following box.

Handling RREP by the rest of the nodes in the reverse path

When I receives RREP, it just forward it to the next hop

4.2.5. Handling RREP by the Source Node

Depending on the value of the trust field in the RREP, the source node chooses either to send the data through the route or to wait for another route. For the trust value equals to 1 or 2, the source node sends the data. Otherwise the source node waits for another route. The algorithm of handling the RREP by the source is given in the following box.

Handling RREP by S

When S receives the RREP, it checks the trust value and does the following:

If (trust value = 1 or 2)
S sends the data packet

Else
S waits for further trusted route

5. Simulation and results

GloMoSim is one of the well known simulators. It was developed at the parallel computing laboratories at California University. The design of the simulator is based on the discrete parallel event environment simulator (PARSEC) which is written in C language. The present study uses version 2.03 of GloMoSim.

5.1. Simulation Environment

The simulation is held for ad hoc networks of 15, 20, 25, 30, and 35 nodes. The nodes move with a velocity of (0 – 20 m/s) in a square area whose dimension is 1000m*1000m. The simulation lasts for 100 seconds for each experiment.
The radio range is set to 250 m for all the nodes and the bandwidth is set to 2 Mb/s. The adopted strategy to distribute the nodes on the network is uniform node placement, where the network area is divided into a number of cells equals to the number of nodes, and each node is assigned randomly to one of the cells.
The motion of the nodes within the network area is described using random-waypoint model. In this model, the node chooses a random direction within the network area, and then it starts its trip of movement toward that direction with a velocity varies regularly within the range of (0 – 20 m/s). CBR is used as a model of data resources and the size of data packets is set to 512 byte. GloMoSim uses an agent called *seed* whose function is to guarantee a random distribution and motion of the nodes within and on the network area during the simulation period.
Table 2 shows the simulation parameters for the different scenarios.

Table 2: Simulation parameters

Parameter	Value
Simulation duration	100 seconds
Number of nodes	15, 20, 25, 30, 35
Pause time	0, 10
Simulation area	1000 * 1000
Minimum velocity of the nodes	0
Maximum velocity of the nodes	20
Radio range	250m
Bandwidth	2 Mb/s

The simulation evaluates the performance of the original and the modified versions of AODV with the presence of one black hole and with the presence of two black holes.

Table 4.3: Simulated scenarios

Scenario number	Description
1	Original AODV with one black hole node
2	Modified AODV with one black hole node
3	Original AODV with two black hole nodes
4	Modified AODV with two black hole nodes

5.2. Metrics of Performance Evaluation

The present study uses four performance metrics to evaluate and compare the modified AODV to the original one. These metrics are: packet delivery ratio, number of dropped

packets, end - to - end delay, and overhead. The following is a short description of each metric.

Packet Delivery Ratio: is the total number of the packets received by the destinations to the total number of packets originated by the sources. It describes the effectiveness the protocol enjoys in forwarding the data packets from their sources to their destinations.

Number of Dropped Packets: is the number of packets dropped for different reasons, like for example: time expiration or collisions. This metric is necessary for the present study because it can discover and compare the number of the dropped packets by the black hole node in both of the modified AODV and the original one.

End – To – End Delay: is the consumed time between originating the data packet by the source node and receiving it by the destination node. The average of the delay is computed for all the transmissions to measure the efficiency of the protocol in transmitting data subject to the unit of time.

Overhead is the ratio between the total number of the originated control packets and the total number of the received data packets.

5.3. Result and Analysis

This section shows the results of simulating both the original and the modified versions of AODV with the presence of the black hole problem. There were four scenarios simulated in order to consider the different parameters whose impact directly touches the problem of the study. Theses parameters are: number of black hole nodes and the whole number of nodes in the network.

5.3.1. Packet Delivery Ratio

In all figures throughout the document, the red solid line with the square markers represents the original protocol and the green solid line with the triangular markers represents the modified protocol. Both of the two black lines above and below each of the red and the green lines represent the margin of errors for the experiments of the corresponding line. The margin of errors is computed at confidence 95%.

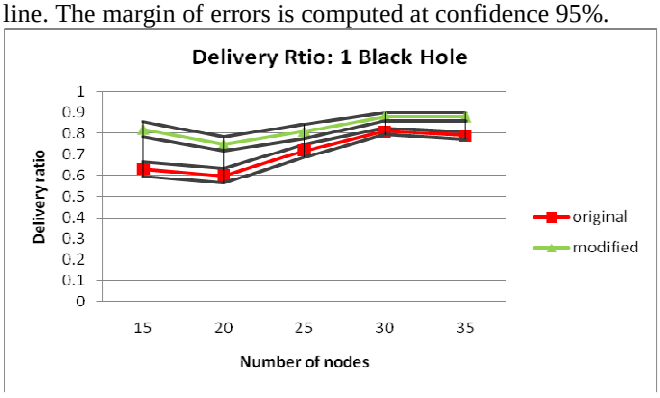

Figure 7: Delivery ratio, 1 Black hole

Figure 7 shows the improvement the modified protocol achieved compared to the original AODV in term of packet delivery ratio for a network attacked by one black hole. Figure 8 shows the same for a network attacked by two black holes. The improvement ratio is computed using the following formula:

$$DeliveryImprovment = \frac{(ModifiedDelivery - OriginalDelivery)}{ModifiedDelivery}$$

The modified protocol improves the delivery ratio by 15% compared to the original AODV for a network attacked by one black hole. The effects of the black hole diverge with respect to the number of nodes in the network as shown by Figure 7. It can be seen in Figure 7 that the delivery ratio decreases as the number of nodes increases from 15 to 20. Within this interval, as the number of nodes increases the black hole has the chance to contribute in more connections and to drop more packets. This is the reason behind the decreasing ratio of delivery for both the original and the modified versions of AODV.

As shown by Figure 7 the delivery ratio increases as the number of nodes increases from 20 to 30 for both the original and the modified versions of AODV. Within this interval the black hole has the chance to contribute in more connections, but the source node has a greater chance to receive routes propagated by other reliable nodes. This is the reason behind the increasing ratio of delivery. By increasing the number of nodes from 30 to 35, the source node becomes sorrounded by more neighbors. In such case the chance of having more nodes with a direct link to the destination increases, and the chance of having more neighbors replying quickly increases. The black hole competes with the other nodes in a fair manner. Therefore the delivery ratio decreases slightly and approaches to a stable state within this interval as shown by Figure 7.

For a network attacked by two black holes, the modified protocol improves the packet delivery ratio by 13% compared to the original AODV. Figure 8 shows the improvement.

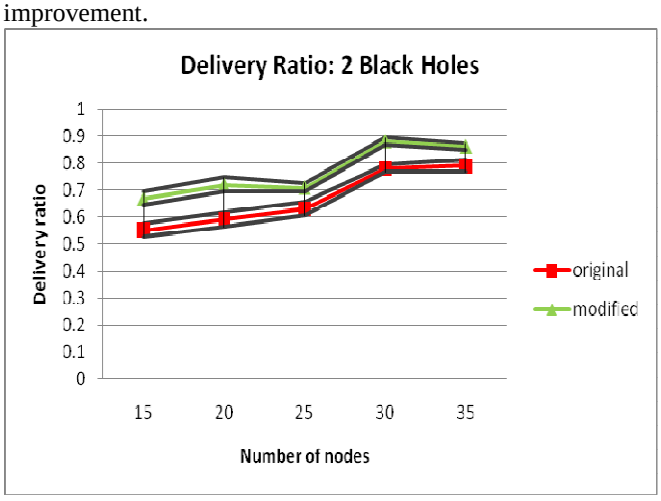

Figure 8: Delivery ratio, 2 Black holes

Figure 8 shows that the delivery ratio increases as the number of nodes increases from 15 to 30. This is normal, because the number of black hole nodes is fixed to 2 and the whole number of nodes increases. By increasing the number of nodes from 30 to 35, the source node becomes sorrounded by more neighbors. In such case, again, the chance of having more nodes with a direct link to the destination increases, and the chance of having more neighbors replying quickly increases. The black hole competes with the other nodes in a fair manner. Therefore the delivery ratio decreases slightly and approaches to a stable state within this interval as shown by Figure 8.

5.3.2. Number of Dropped Packets

Figure 9 shows how the modified protocol decreases the number of dropped packets compared to the original one for a network attacked by one black hole. Figure 10 shows the same for a network attacked by two black holes. Both figures consider only the packets dropped by the black hole node(s) in order to shed light on the problem of the study. The formula of the improvement is:

$$\text{DroppedImprovement} = \frac{(\text{OriginalDrop} - \text{ModifiedDrop})}{\text{OriginalDrop}}$$

The modified protocol reduces the number of dropped packets by 55% compared to the original one for a network attacked by one black hole. As shown by Figure 9 the number of dropped packets increases as the number of nodes increases from 15 to 20. Within this interval, as the number of nodes increases the black hole has the chance to contribute in more connections and to drop more packets. This is the reason behind the increasing number of dropped packets. The results of Figure 9 agree with those results of Figure 7. This is expected because the more dropped packets the less delivery ratio.

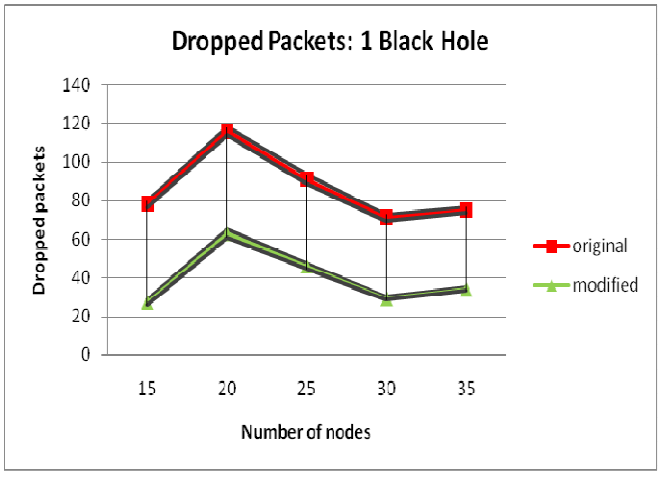

Figure 9: Dropped packets, 1 Black hole

For a network attacked by two black holes, the modified prtocol improves the number of dropped packets by 51% compared to the original one. As shown by Figure 10, for the modified protocol, the number of dropped packets increases as the number of nodes increases from 15 to 25. Within this interval, the black hole can contribute in more connections and find more victims. This is the reason behind the increasing number of dropped packets within this interval.

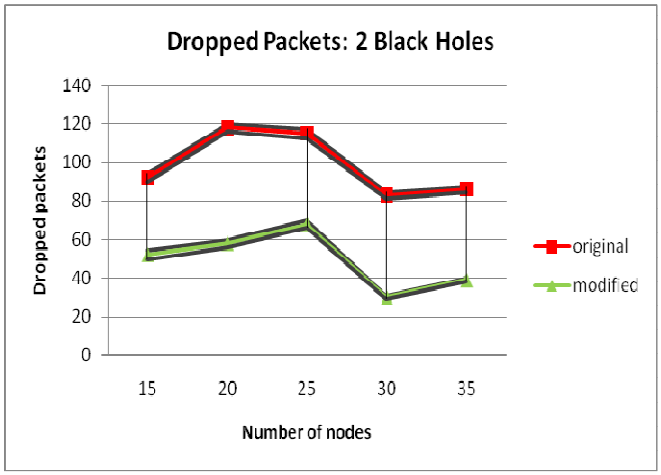

Figure 10: Dropped packets, 2 Black holes

By increasing the number of nodes from 25 to 30, the number of dropped packets decreases. In this case the source node becomes sorrounded by more neighbors and has the chance to receive more alternative routes to the desired destination. This is the reason behind the decreasing number of dropped packets within this interval. There is an observable agreement between the dropped packets and delivery ratio for a network attacked by 2 black holes. The more dropped packets in figuer 4 the less delivery ratio in Figure 8.

5.3.3. End-to-end Delay

For a network attacked by one black hole the protocol reduces the average end - to - end delay dramatically. Figure 11 shows the difference between the original and the modified protocols. The modified protocol improves the delay by 36% compared to the original protocol. The improvement the modified protocol achieved is computed using the formula:

$$DelayImprovement = \frac{(original\ delay - modified\ delay)}{original\ delay}$$

For the original AODV, the delay increases as the number of nodes increases from 15 to 20 as shown by Figure 11. This is justified by the increasing number of dropped packets within this interval as shown by Figure 9. By incresing the number of nodes from 20 to 25 the delay also increases, but

with a lower rate than that of the previous interval. This is can be justified by the decreasing number of dropped packets within this interval as shown by Figure 9. The delay decreases as the number of nodes increases from 25 to 30, and then it stabilizes as the number of nodes increases from 30 to 35. There is an observable agreement between the delay and the number of dropped packets within theses 2 intervals.

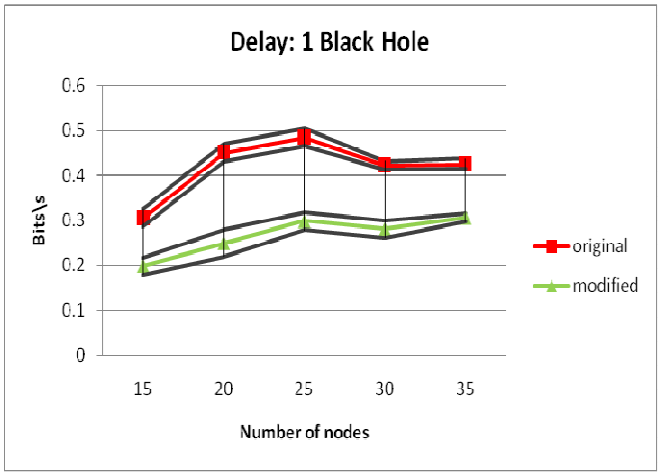

Figure 11: Delay, 1 Black hole

For the modified AODV, the delay increases as the number of nodes increases from 15 to 25. Within the interval 15 to 20, the delay increases with proportion to the increasing number of dropped packets as shown in Figure 9. The hihger the number of the packets dropped the more the load on resources. Basically this is the reason behind incresing the delay within this interval. Within the interval 20 to 25, the delay increases with proportion to the increasing delivery ratio as shown by Figure 7. As the delivery ratio increases the resources provides its services to a larger number of packets, resulting in an increasing delay.

For a network attacked by two black holes, the difference in delay between the original and modified protocols is great. Figure 12 shows the improvement the modified protocol achieved compared to the original AODV. The modified protocol reduces the average of delay by 46% compared to the original AODV. The delay of the modified protocol increases as the number of nodes increases from 15 to 30. This could be justified by the increasing delivery ratio as shown by Figure 8. Needless to say that there is a trade off between the delivery ratio and the delay.

For the original AODV, the delay increases as the number of nodes increases until it reaches to its maximum value when the number of nodes equals to 35. For the original protocol, the delay increases with proportion to the delivery ratio as shown in figures 6 and 2.

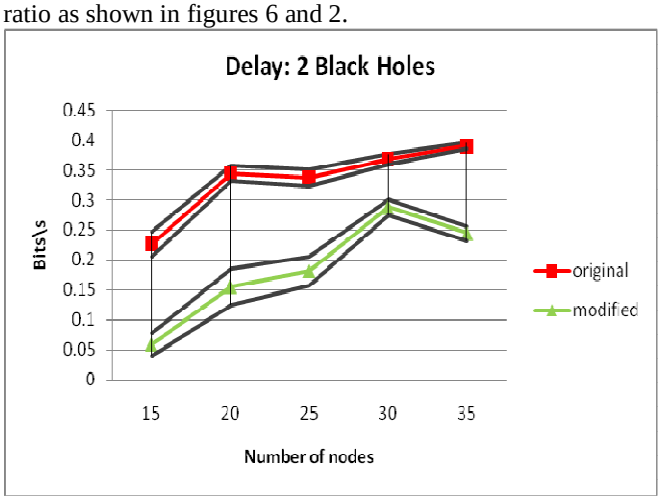

Figure 12: Delay, 2 Black holes

5.3.4. Overhead

The modified protocol outperforms the original AODV with respect to the additional overhead. Figures 13 and 14 show the improvement the modified protocol achieves for networks attacked by one black hole and two black holes respectively.

In Figure 13, the modified protocol improves the additional overhead by 20% compared to the original AODV. The improvement of the overhead is computed using the following formula:

$$Overhead\ Improvement = \frac{(Original\ overhead - Moified\ overhead)}{Original\ overhead}$$

As shown by Figure 13, for the original AODV, the overhead increases as the number of nodes increases from 15 to 20. This can be interpreted by the increasing number of dropped packets within this interval as shown by Figure 9. Dropping more packets by the black hole results in retransmitting them by the source node, and hence more overhead is suffered by the network. As the number of nodes increases from 20 to 35, the overhead fluctuates with proportion to the number of dropped packets shown in Figure 9.

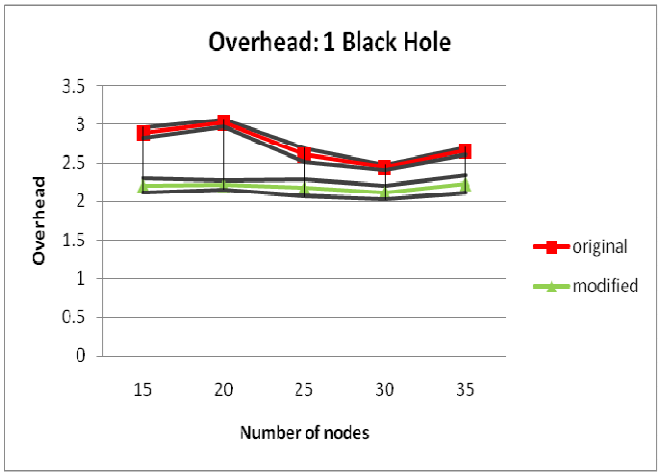

Figure 13: Overhead, 1 Black hole

Figure 14 shows that the modified protocol reduces the additional overhead compared to the original AODV. The modified protocol reduces the overhead by 14% compared to the original AODV. The ratio is computed using the above-mentioned formula.

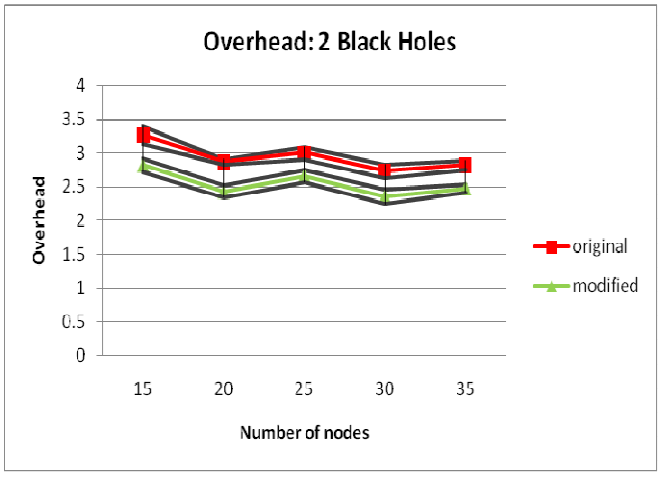

Figure 14: Overhead, 2 Black holes

6. Conclusion and Future Work

The proposed protocol modifies the behavior of the original AODV to check the reliability of the received routes before sending the data packets. The modification with which the researcher came up can be summarized as given below.

Each node has a table prepared to hold the addresses of the reliable nodes. During the process of route discovery, for each node receives a RREQ, it checks the behavior of the broadcasting node. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node. RREP is overloaded with an extra field to indicate the reliability of the replying node. The value of the trust field is initialized to zero by the replying node and might be modified by its previous hop during the trip of the RREP. The value of the trust field could be modified either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exist in the trust table. Once the RREP is received by the source node, it decides whether to send the data or to wait for further route. In case the trust field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route. The protocol reduces the bad affects of the black hole problem and outperforms the original AODV in terms of packet delivery ratio, number of dropped packets, end-to-end delay, and overhead. For example, the results show that, when the node is attacked by two black hole nodes and the pause time is set to zero, the protocol outperforms the original AODV by 13%, 51%, 46%, and 14% regarding the mentioned above metrics respectively. The main priority of the protocol is to send the data through reliable route. The protocol need to be supported by a technique to eliminate the black hole node from the network.

The conditions of passing the behavioral analysis filter are not satisfied enough to judge the reliability of the node. Moreover, the protocol does not consider the behavior of two black hole nodes working together as a team. The next step is to support the protocol with a certain mechanism to handle the problem for more than one black hole working as a team. The overhead stands as a barrier in the face of realizing the protocol. More researches need to be devoted to reduce it.

References

[1] Johnson, B. Maltz, A. and Josh, B. (2001). “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks,” in Perkins, Charles E. *(ed.) Ad Hoc Networking*, Chapter 5, Addison-Wesely, pp. 139-172.

[2] Perkins, Charles E. and Royer, Elizabeth M. (1999). “Ad-hoc On-Demand Distance Vector Routing”. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (IEEE WMCSA '99), New Orleans, Louisiana, February 1999: 90-100.

[3] Li, Wenjia. and Joshi, Anupam. “Security in mobile ad hoc network *(survey)*”. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimor County.

[4] Ghaffari, Ali. (2006). “Vulnerability and Security of Mobile Ad hoc Networks”, Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24.

[5] Kargl, F. ,Schlott, S., Klenk, A., Geiss, A. and Weber, M. (2002). “Securing Ad hoc Routing Protocols”, Proceedings of the 1st ACM Workshop on Wireless Security. Atlanta, GA, USA. Pages 1-10.

[6] Tamilselvan, Latha and Sankaranarayanan, V. (2007). "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (Aus Wireless 2007) India, 2007 IEEE.

[7] Hu, Y., Perrig, A. and Johnson, D. (2002). "A secure On-demand Routing Protocol for Ad Hoc Networks", in Proceedings of ACM MOBIC' 02. Atlanta, USA September 23–26.

[8] Marti, S., Giuli, T. J., Lai, K. and Bake, M. (2000). Mitigating Routing Misbehavior. In *Mobile Ad hoc networks. 6th MobiCom*, BA Massachuestts.

[9] Tamilselvan, Latha and Sankaranarayanan, V. (2008). "Prevention of cooperative black hole attack in MANET", in *Journal of Networks*, Vol. 3, NO. 5, MAY 2008.

[10] Deng, Hongmei , Li, Wei and Agrawal, Dharma P (2002). "Routing Security in Wireless Ad HocNetwork", in IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[11] Gatzianas, Marios and Georgiadis, Leonidas (2008). "A Distributed Algorithm for Maximum Lifetime Routing in Sensor Networks with Mobile Sinks", IEEE Transactions on Wireless Communications 7(3): 984-944.

[12] Sobeih A. (2002). "Reliable Multicasting in Wireless Mobile Multi-Hop Ad Hoc Network Ms". Master thesis. Cairo: Cairo University.

[13] Zimmehrman T. (1996). "Personal Area Networks: Near-field Intrabody Communication". In IBM Systems Journal 35(3&4), 1996. 609-617.

[14] Singh, Amandeep , Singh, Charanjit, and Kaur, Rajbir (2007). "Security Issues in Wireless ad hoc Network". Proceeding of COIT, RIMT-IET, Manadi Gobindgarth.

[15] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002). "Wireless Sensor Networks: A survey". In Computer Networks Journal 38(4), 2002. 393-422.

[16] Stalling, William (2001). High Speed Networks and Internets, second edition, New Jersey: prentice hall.

[17] Stalling, William (2001). Wireless Communication and Networks, first edition, New Jersey: prentice hall.

[18] Lidong Zhou, Zygmunt J. Haas (1999). "Securing Ad Hoc Networks". In IEEE network, special issue on network security, November.

[19] Perkins C. (2000). "Ad Hoc Networking an Introduction". In Addison-Wesley Professional, November 28; 13-19.

[20] Royer E., and Toh C. (1999). "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks". In IEEE Pers. Commun. Apr; 6(4): 46-55.

[21] Perkins C. and Bhagwat P. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector routing (DSDV) for Mobile Computers". Proceedings of the conference on Communications architectures, protocols and applications. London, United Kingdom, October; 24(4): 234-244.

[22] Murthy S., Garcia-Luna-Aceves J. (1996). "An Efficient Routing Protocol for Wireless Networks". ACM Mobile Networks and Applications, October 1996; 1(2): 183-197.

[23] Perkins C. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers". Proc. ACM SIGCOMM; 234-344.

[24] Yaqoub, Zahi (2008). "Black hole Avoidance in Ad Hoc Networks". Master thesis, Jordan, Al-albayt University.

[25] Mishra, Amitabh and Nadkarni, Ketan M. (2003). "Security in Wireless Ad Hoc Networks". In The Handbook of Ad Hoc Wireless Networks (*ed*.) (Chapter 30), CRC Press LLC.

[26] Abdalla, A. M. (2005). "Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)". Doctoral dissertation. Cairo, the American University in Cairo.

[27] Wedian, S. (2009). "Neighborhood-based Route Discovery Protocols for Mobile Ad hoc Networks". Master thesis, Jordan, Jordan University of Science and Technology.

[28] Zeng, X., Bagrodia, R. and Gerla, M. (1998). "GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks". Proceeding of the 12th workshop on Parallel and distributed simulation, Banff, Alberta, Canada; 1998: 154-161.

[29] Payal, N. Raj, B. and Prashant, Swadas. (2009). "DPRAODV: A Dyanamic Learning System Against Blackhole Attack in AODV Based Manet", in IJCSI International Journal of Computer Science Issues, Vol. 2.