Mansoura Journal of Computers and Information Sciences

Software and Hardware Implementation of Local Intrusion Detection Strategy

Imad I. Saada
Faculty of computers and information systems , C.S dep.
Mansoura University, Egypt
sir_ias@hotmail.com

Rasha H. Sakr
Faculty of computers and information systems , C.S dep.
Mansoura University, Egypt
yssf_hamid@yahoo.com

Majdi Z. Rashad
Faculty of computers and information systems , C.S dep.
Mansoura University, Egypt
magdi_z2011@yahoo.com

ABSTRACT
A mobile ad hoc network (MANET) has many undesirable challenges, black hole (BH) is one of the most significant challenges in MANET. Many researchers have proposed researches which depend on different strategies to face this challenge. The problem is how much the ability of these strategies to detect and block BH in order to empty the network from the threats, and how much these solutions could be implemented practically to treat with threats. However, the required strategy should also maintain network performance at the same time. The idea of this research has been applied on AODV based MANET, the strategy deals with cooperative black hole by using a deceptive message with virtual address that is not in the addresses range [1]. The main interest in this paper beside proposing the new idea, is to convert this idea into strategy by providing the necessary details, in addition to implement the strategy by hardware and software models. These models have been built in order to illustrate how black hole works and how the strategy can detect and block the black hole practically in AODV based MANET. This paper presents the method in an integrated manner. In this method, the detection process starts from the previous node, not from the source node. However, this method can choose the shortest path and can deal with more than one black hole. These additions will preserve the performance of network, the hardware model has been provided with liquid crystal displays LCD put on each node. LCD is used to appear each step, and to make the system full-acknowledgment.

Keywords
MANET, Intrusion, Black Hole, MANET security.

1. INTRODUCTION
Black hole node (BH) is a kind of intrusion node that violently affects the network performance, because it drops all the packets received by itself. When the routing process starts, it tells the nodes that it has link to the source to receive the data packets. Finally, the data packet will not be delivered to the source.
An AODV routing protocol is on-demand routing protocol. Every node in MANET owns a routing table that contains the hop node information to next node for a route to the destination node. When a source node wants to route a packet to a destination node, it commonly uses the unique or specific route if a new route to the destination node is available in its routing table. If it's not, it try to begin a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors' nodes, the process of broadcasting is repeated by nodes until it reaches an intermediate node with a fresher route to the destination node [2][3].

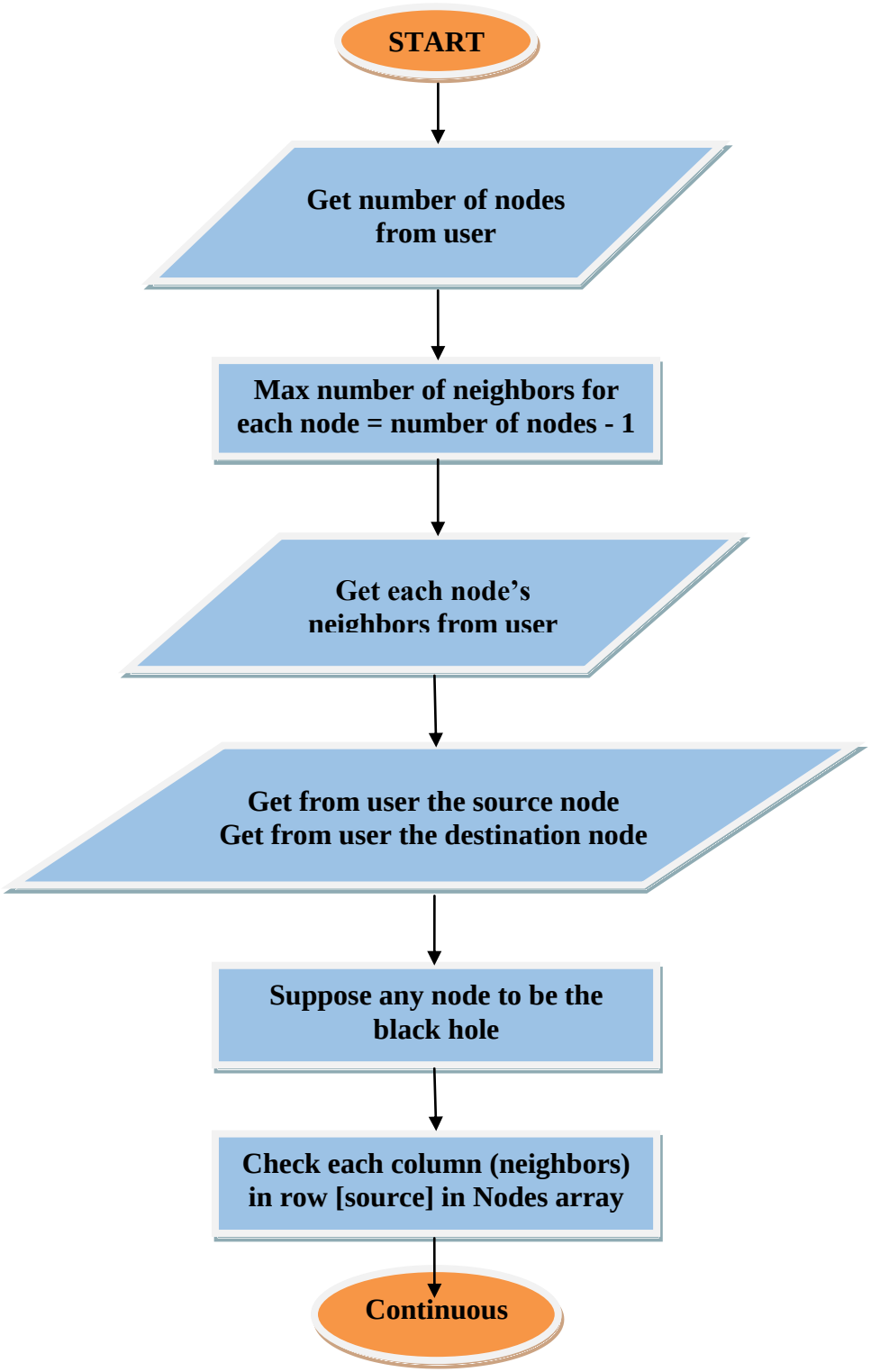
Many researches were discussed, the problem is that the ability of detecting and preventing BH is deferent from one solution to another, and some solutions adversely affected on network performance.
the proposed solution has tried to detect and to prevent BH, some additions have been performed such as Choosing the shortest path, dealing with multiple BH, detecting and blocking BH by the previous node, not by the source node, and implementing the system practically by software model and hardware model. These additions are necessary to create an integrated strategy.

2. OVERVIEW
Sanjay Ramaswamy, et al [4], proposed detection by DRI table which adds some modification to AODV routing protocol, it depends on using the Data Routing Information (DRI) table in addition to the cached and current routing tables. By this strategy each node of the network gets an additional (DRI) table.
Sergio Marti, et al [5], proposed the watchdog strategy for DSR based MANET; it detects single misbehaving nodes by getting a buffer which has sent packets recently. This means that the node's watchdog watches and observes the next node. If the next node does not deliver the packet, it is then treated as a misbehaving node.
Deng, H., et al [6], proposed a solution for AODV based MANET called SIDSR, this solution has created one more route to the intermediate node that replies to the RREQ message. This process is useful to decide whether the route from the intermediate node to the destination node is available or not. If it is available, the intermediate node can be trusted node. If the route is not available, the strategy will discard the reply message and the source broadcasts alarm notification to the network nodes.

3. BLACK HOLE WORKING
The flowing flowchart in figure 1 represents how black hole node is working in MANET. The black hole deals with any request and it tells that it has a path to the destination, and when the source receives the reply message it will send the packet to the black hole. The packet will not be received by the destination because black hole node will drop it. The flow chart also show that the honest node will not reply if it has not

a path to the destination depending on checking its routing table, but the honest node will broadcast this message to neighbors.
The shortest path is created when the reply message retrains to the source, this path will be used to send the data message. The shortest path is determined depending on the lowest number of hops in the path, so the source will choose the fresher reply message.

If the black hole node exists in the network and in shortest path, the packet will not be reached to its destination. This will inversely affect on the performance of network.



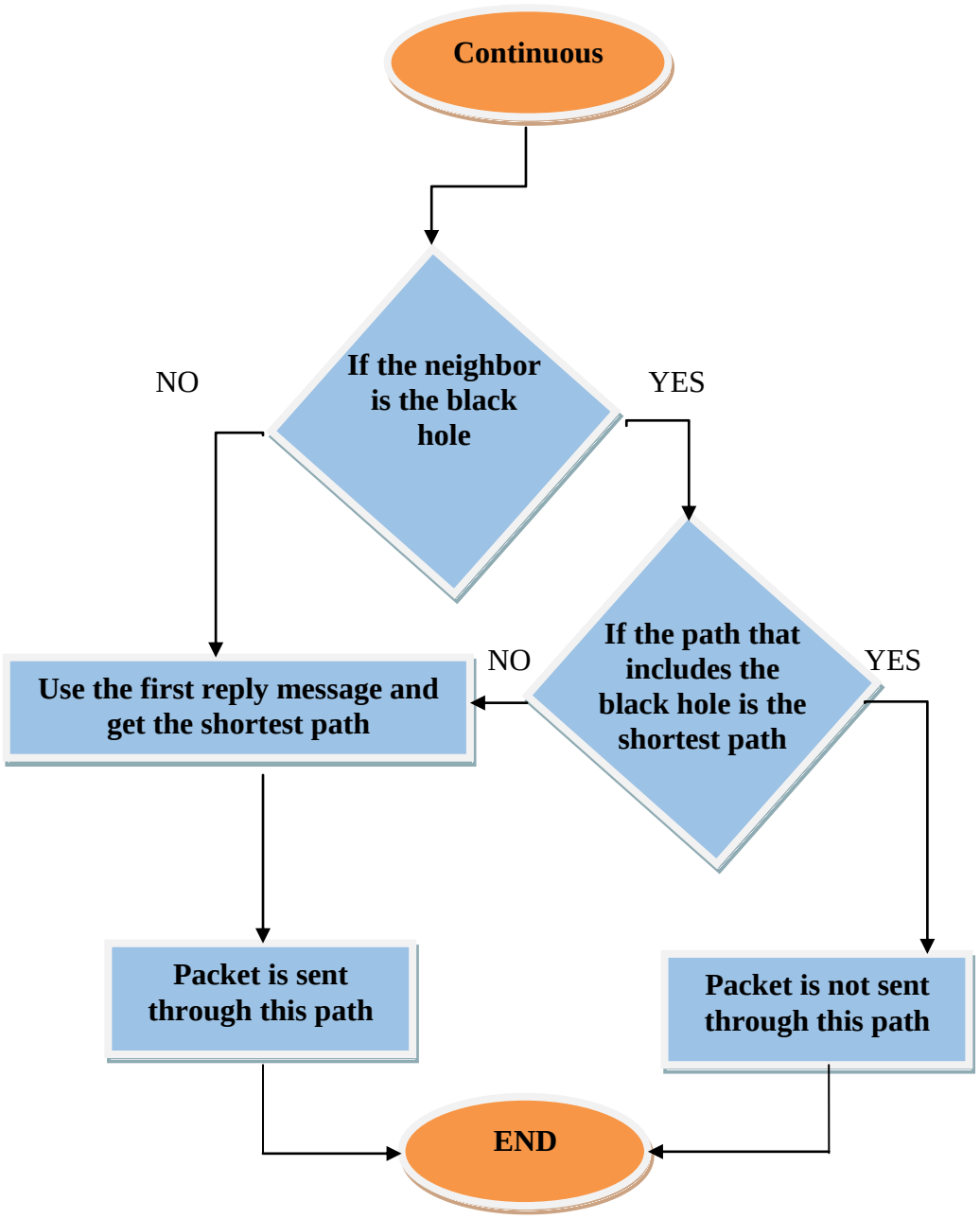


Fig ١: BH working flowchart

4. LOCAL INTRUSION DETECTION

Local intrusion detection has been proposed in order to detect and block the cooperative black hole in AODV based MANET. The black hole used to respond to any route request, the adopted strategy has used the route request message with virtual address. By using this way the black hole node will be misleading.

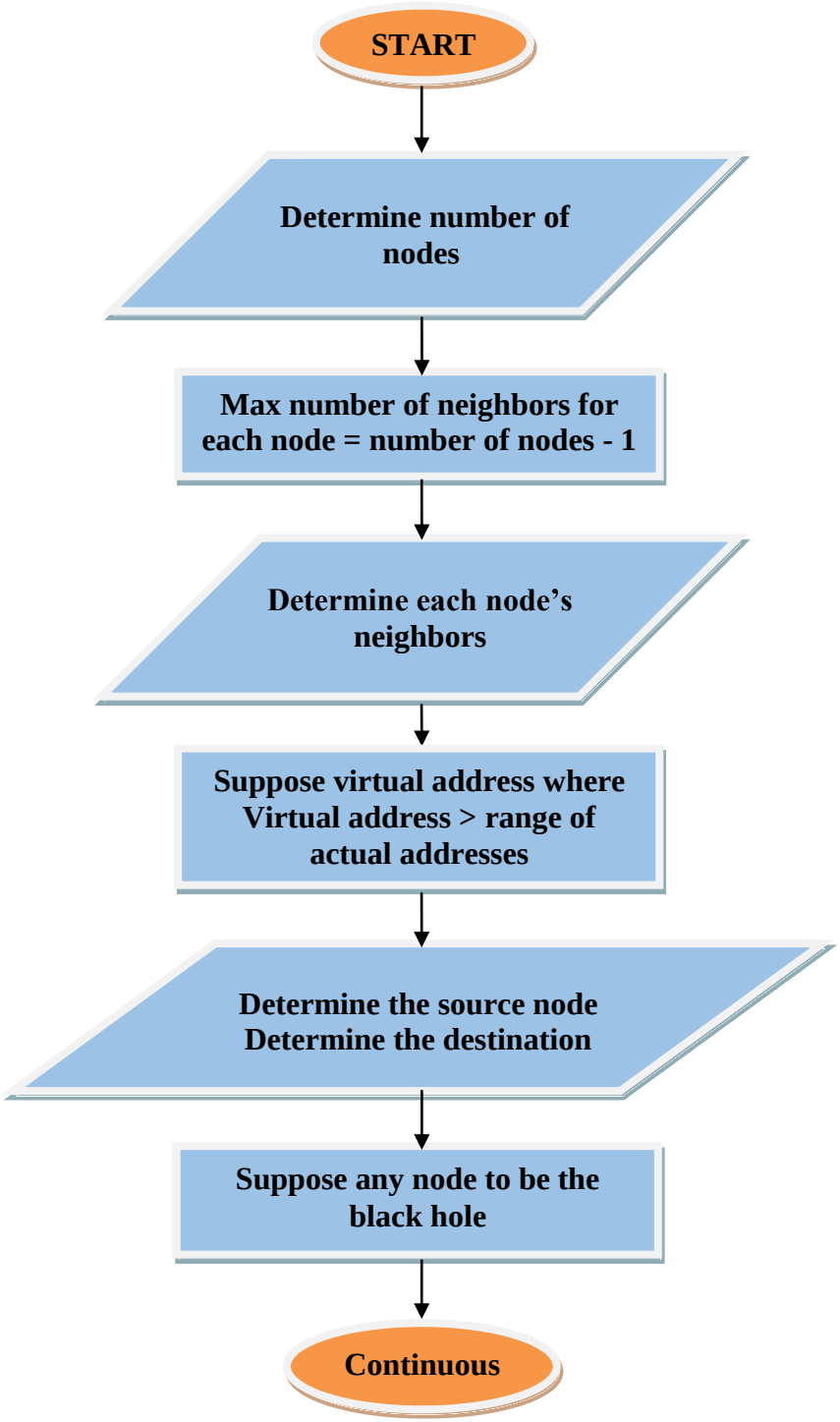
All options which are available in the local intrusion detection are illustrated by software and hardware implementation such as the blocking process which starts from the previous node and not from the source node in order to minimize the number of steps of the blocking process. However, this solution can choose the shortest path, and deal with more than one black hole. The system is provided with liquid crystal displays LCD to be full acknowledgment**.**

5. DETECTING and BLOCKING a BLACK HOLE

The flowchart in figure 2 illustrates the process of detecting and blocking the black hole. If the network has black hole then surely there will be a reply message in all cases (in case of virtual address), so we will send a request message with virtual address. This address is not exists in the network, the node must not reply this message if it is an honest node, but if any node replies the request message then, it can be concluded that this node is misbehavior node (black hole node).

When the previous node receives a reply message from the black hole, it will detect it and broadcast an update message to its neighbors in order to update the routing tables, finally the

routing tables will be clean from black hole, this will increase the performance of the network.
The process of detecting and blocking the black hole node starts locally from the previous node, not from the source node, this option will quicken the detecting and blocking process with minimum number of hops.



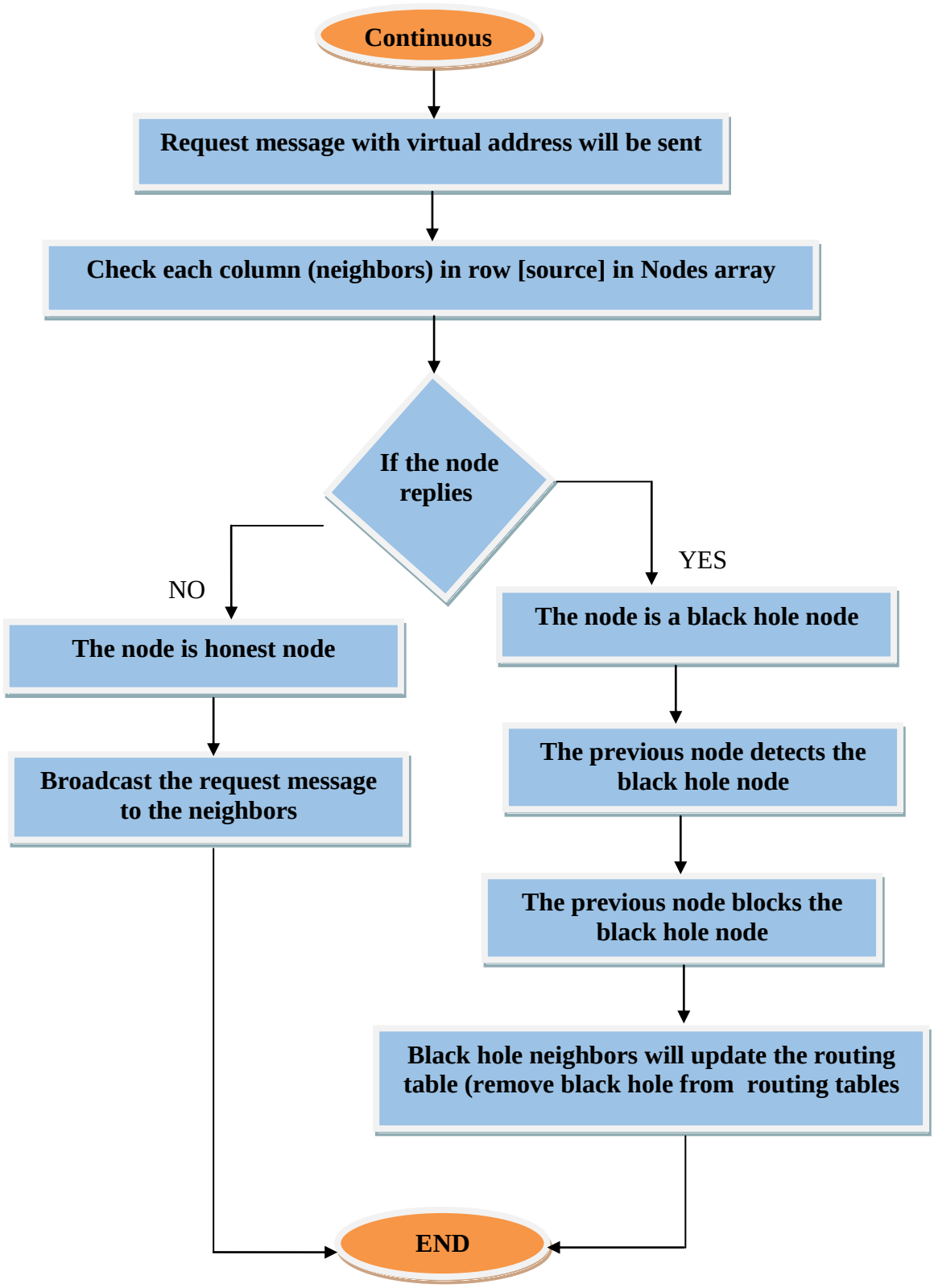


Fig 2 : Flowchart of detecting and blocking BH

6. DISSCUSSION and RESULTS

6.1 Software Models

6.1.1 Black Hole Working Model

To illustrate the working process of black hole node, and how the black hole node can drop the packet, we present this software model.

The model supposes that there are five nodes. One of these nodes is a black hole node. If the black hole is available in the shortest path, the message then will be dropped as shown in figures 3,4.

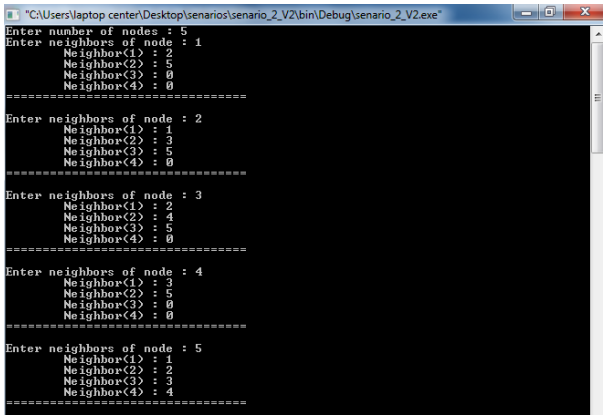


Fig 3: Configuring nodes and routing tables of MANET

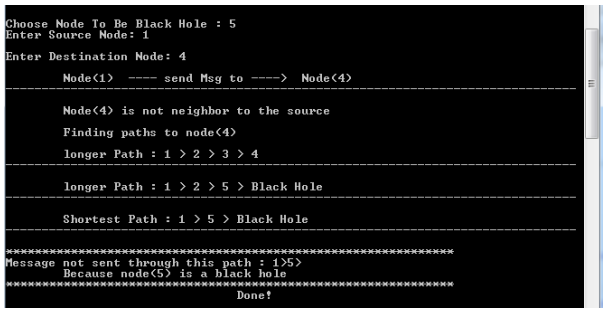


Fig 4: Dropping the message by BH

There are three paths:

Path 1: 1 → 2 → 3 → 4
Path 2: 1 → 2 → 5 → BH
Path 3: 1 → 5 → BH

The shortest path is path 3. This path will be chosen to send data packet, but the shortest path contains a black hole, so the message will be dropped.

6.1.2 Model of Detecting and Blocking the Black Hole

This model also illustrates the process of detecting and blocking the black hole. The model has six nodes one of these nodes is a black hole node, in order to detect the black hole the message with virtual address used, when the black hole

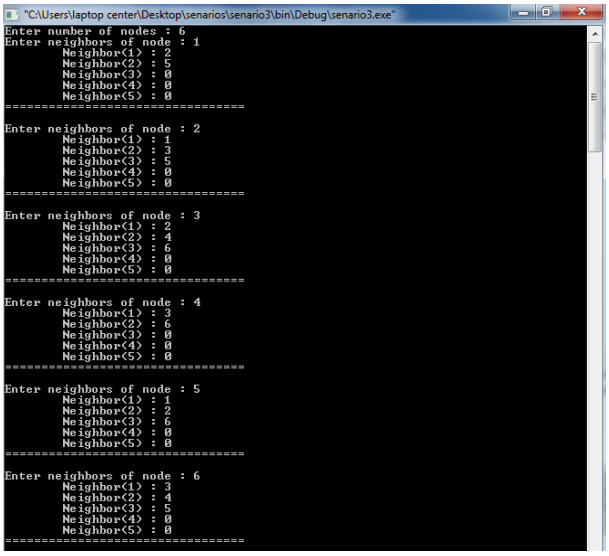


Fig 5: Configuring nodes and routing tables of MANET

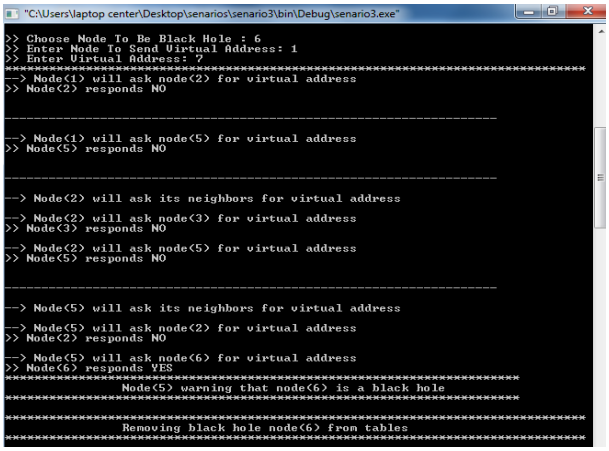
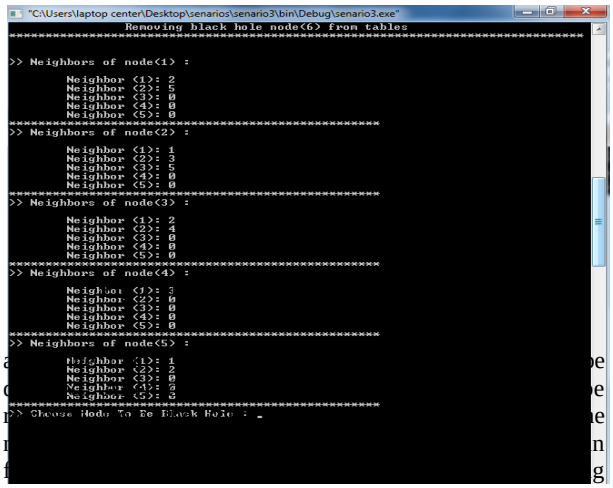


Fig 6: Detecting and blocking BH



process instead of the source node (NODE 1). This operation will enhance the network performance.

6.2 Hardware Model

6.2.1 PCB circuit design and working procesure

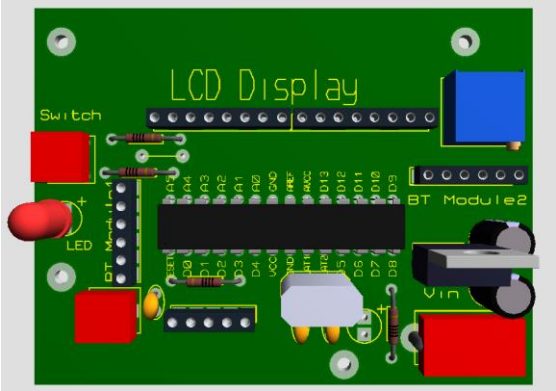


Fig 8: PCB circuit design

- We have two circuits in our network to simulate node 2 and node 3
- Node 1 is (mobile or pc) and it is connected to node 2.
- Node 4 (mobile or pc) is connected to node 3.
- Both of them - circuit (1) and circuit (2) - are connected to each other.
- The connection in this network based on Bluetooth media using Bluetooth modules called HC-05 which has 10m connection range and band rate of 9600 bit/sec.
- The connection between the two circuits based on BT module1 in each circuit by configuring the two modules to be connected to each other, when power is on as master and slave. We configured one of them as a master, and the other as a slave, then getting the MAC (media access control) address of the slave. The master will connect to this MAC address when see it around.
- The two circuits use atmega328 microcontroller as the brain that will control the data flows from a node to another by getting the data from each Bluetooth module. The atmega328 communicates with these modules over UART serial protocol.
- The switch is used to give the microcontroller an order to simulate as a black hole node.
- The red LED (Light Emitting Diode) is used to indicate that this node is a black hole node.
- LCD (Liquid Crystal Display) is used for monitoring the procedure and steps of the software that implemented through the microcontroller.

6.2.2 Practical Model

The practical system is shown in figure 9, to illustrate the working procedure of the system there are two proposed scenarios:

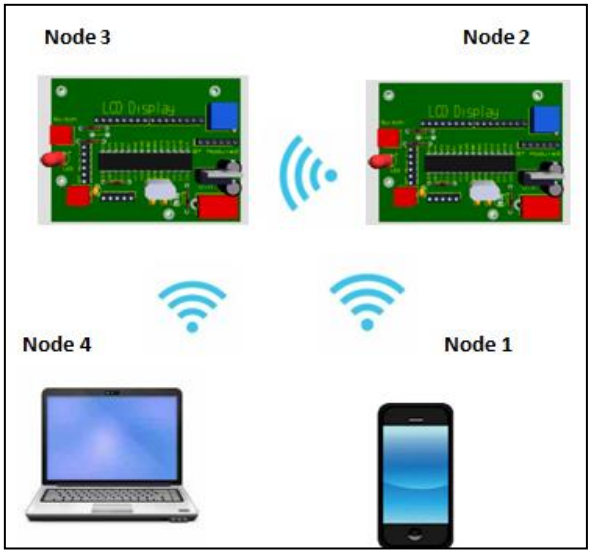


Fig 9: System diagram

First scenario assumes that node 1, node 2 , and node 4 are honest nodes, but node 3 is a black hole node. The message will be sent from node 1 to node 4 as in figure 9. The network has the following scenario:

- Node 1 wants to send message (hello) to node 4 (4:hello)
- Node 1 will send message to node 2 asking about node 4, node 2 is not neighbor of node 4, so node 2 will ask its neighbor (node 3) about node 4.
- Node 3 will immediately responds (YES), and it will send the path to node 2, then to node 1.
- According to the path, node 1 will send the message to node 4, node 3 will receive the message but instead of delivering it to node 4 it will drop the massage. The message will not be delivered to node 4.
- LCD will show the data message is not received by node 4.

Fig 10: First scenario

Second scenario assumes that node 1, node 2 , and node 4 are honest nodes, but node 3 is a black hole node as in figure 11. The message sent from node 1 to node 6, in order to detect and block the BH. The source will send a message with virtual address which is not belonging to any of nodes. In the normal behavior each node must broadcast the message to the neighbors because the destination address is virtual, but black hole node will respond that it has a path to the virtual destination, in this case it will be detected, the assumed virtual address is node 6, the network has the following scenario:

- Node 1 wants to send message (hello) to node 6 (6:hello)
- Node 1 will send a message to node 2 asking about node 6. Node 2 is not neighbor of node 6, so node 2 will ask its neighbor (node 3) about node 6
- Node 3 will immediately respond (YES).
- Node 2 will detect the black hole node .
- Node 2 will remove node 3 from routing table, and it will send warning message to node 1.
- This detection is done locally by node 2, not by node 1. By this way we will maintain the performance of network.
- LCD will show that node 3 is blocked and it will show the warning messages as in figure 11.

Fig 11: Second scenario

7. CONCLUSION

This paper has proved that black hole is a kind of intrusion node which is working in the network seriously. In this paper, a software model and hardware model are implemented. The models introduced a clear perception of how AODV routing protocol and black hole node are working, the models also proved that the proposed solution had the ability to detect and block BH node in a visible way. This way started from detecting and blocking BH and ended with removing BH from network and from routing tables. Each step is notarized by LCD in the hardware model and by the output form of software model.

All steps are performed with observing the network performance, such as the previous node took over the blocking process instead of the source node, at the same time we keep the shortest path. These options have been added to enhance the network performance.

REFERENCES

1- Imad I. Saada, et al, "Local Intrusion Detection by Bluff Probe Packet (LIDBPP) in A mobile Ad Hoc Network (MANET) ", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 11, No. 11, November 2013.

2- Imad I. Saada, et al, "Implementing and Comparing LIDBPP (Local Intrusion Detection by Bluff Probe Packet)", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, August 2016.

3- Anumeha, et al, "Introducing Efficient AODV Routing Protocol for MANET", International Journal of Computer Applications Vol. 124, August 2015.

4- S. Ramaswamy et al, "Prevention of cooperative black hole attack in wireless ad hoc networks", International Conference on Wireless Networks (ICWN'03), USA, 2003.

5- S. Marti et al, "Mitigating routing misbehavior in mobile ad hoc networks," in 6th ACM International Conference in Mobile Computing and Networks, August 2000.

6- Deng, H et al, "Routing security in wireless ad hoc networks". IEEE communications magazine, 40(10): 70-75, 2002.

7- Pradish Dadhania, et al, "Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks", (IJERA) Vol. 3, Issue 1, 2013.

8- Firoz Ahmed et al, "An Efficient Black Hole Detection Method using an Encrypted Verification Message in Mobile Ad Hoc Networks", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

9- Imad I. Saada, et al, "Various Solutions of Black Hole Attack in A mobile Ad Hoc Network (MANET)" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 8, August 2014.