Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network

[1]Arnab Mitra, [2]Rajib Ghosh, [3]Apurba Chakraborty, [4]Debleena Srivastva

[1,2]Dept. of CSE, Adamas Institute of Technology, India-700 126

[3] Dept. of MCA, Siliguri institute of Technology, India-734 009

[4] Dept. of IT, Guru Tegh Bahadur Institute of Technology, India-110 064

Abstract*— This research work reports on Alive and Black Hole node detection if it exists in any Mobile ad hoc networks (MANETs). The dynamic topology of MANETs allows nodes to join and leave the network at any time instance. This general feature of MANET has exposed to major security attacks including existence of black hole nodes, which adversely affects the entire routing practice. To deal with this routing mess, we have proposed an Artificial Neural Network (ANN) based automated Black Hole node detection tactic, which is capable of detecting the existence of Black hole node(s) in the MANET and thus helps to minimize the smash up in reliable routing procedure. Experimental results in network simulation confirm the hazards caused by presence of Black hole node(s) in MANET, which is same as our earlier research on black hole node detection using Cellular Automata (CA) [1].

Keywords*— Mobile ad hoc networks (MANETs), black hole node detection, network security, dynamic routing, Artificial Neural Network (ANN)

I. Introduction

Ad-hoc networks [1] are used in huge number of potential applications: from military uses to domestic uses. Ad hoc networks provide a solution to real life problem for creating an infrastructure, which is potentially impossible or very expensive in nature. In MANET [2], each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.Three major routing protocols for ad hoc networks are presently being used: a table driven routing protocol i.e. Destination-Sequenced Distance Vector routing (DSDV) protocol [3], on-demand routing protocol i.e. Dynamic Source Routing (DSR) protocol [4], and a source initiated on-demand routing protocol i.e. Ad-hoc on demand Distance Vector routing (AODV) protocol [5]. In MANET communication [7], communicating mobile nodes maintain a routing table to store the next hop node information for a route to the destination node.

When a source node wishes to send a packet to a destination node, it uses the specified route available in its routing table. Otherwise, it starts to build up a new routing table by initiating route discovery process by broadcasting the Route Request (PREQ) message to its neighbours, which is promoted to nest node until it reaches an intermediate node with a brand new route to the destination node specified in the PREQ, or the destination node itself. Receiver of the PREQ makes an entry in its corresponding routing table. The destination node or the intermediate node with a new route to the destination node, forwards this Route Response (PREQ) message to the neighbouring node. An intermediate node makes an entry for the neighbouring node from which it received the PREQ, forwards this PREQ in the reverse direction. Upon receiving the PREQ, the source node updates its routing table with an entry for the destination node, and the node from which it received the PREQ. The source node starts routing the data packet to the destination node through the neighbouring node that first responded with a PREQ. Fig. 1, Fig. 2 and Fig. 3 describes this communication methodology.

MANET is composed of two major components: Cluster Routing Centre (CRC) and Tiny Transmitter-receiver (TTR).

Definition 1: *A CRC (Cluster Routing Centre) routes digital data packets from one cluster to another cluster in MANET [1].*

Definition 2: *A TTR (tiny transmitter-receiver) is a major component in MANET serving as a source or destination of communication [1].*

A black hole [7] is a node that always responds positively to every PREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the PREQ in most cases.

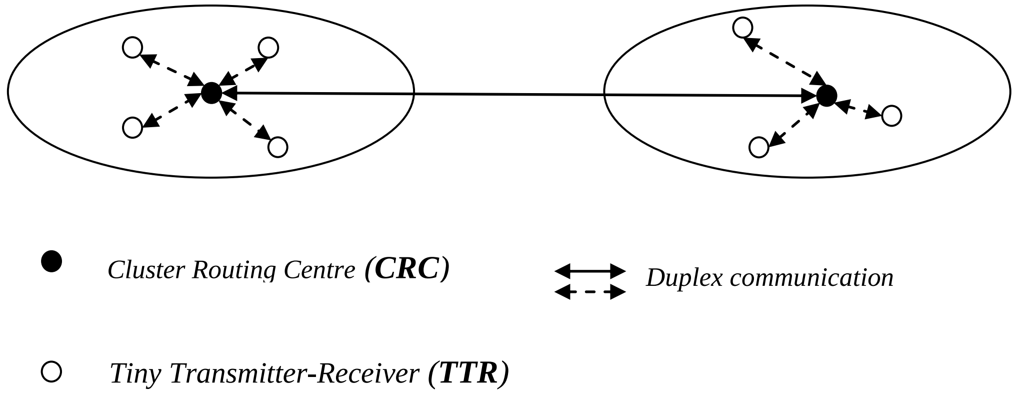


Fig. 1. Schematic representation for MANET communication

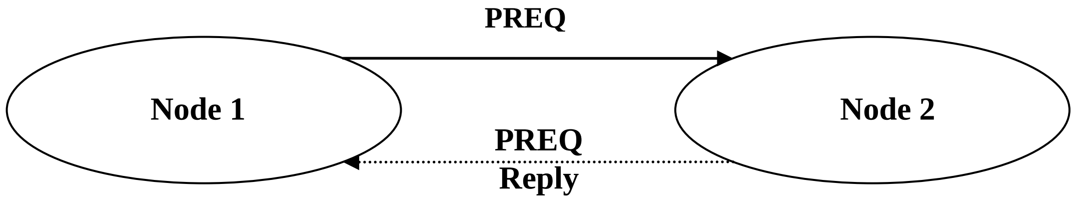


Fig. 2. Basic MANET communicating clusters

When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Fig. 3 explains the behaviour of WANET in presence of Black Hole node.

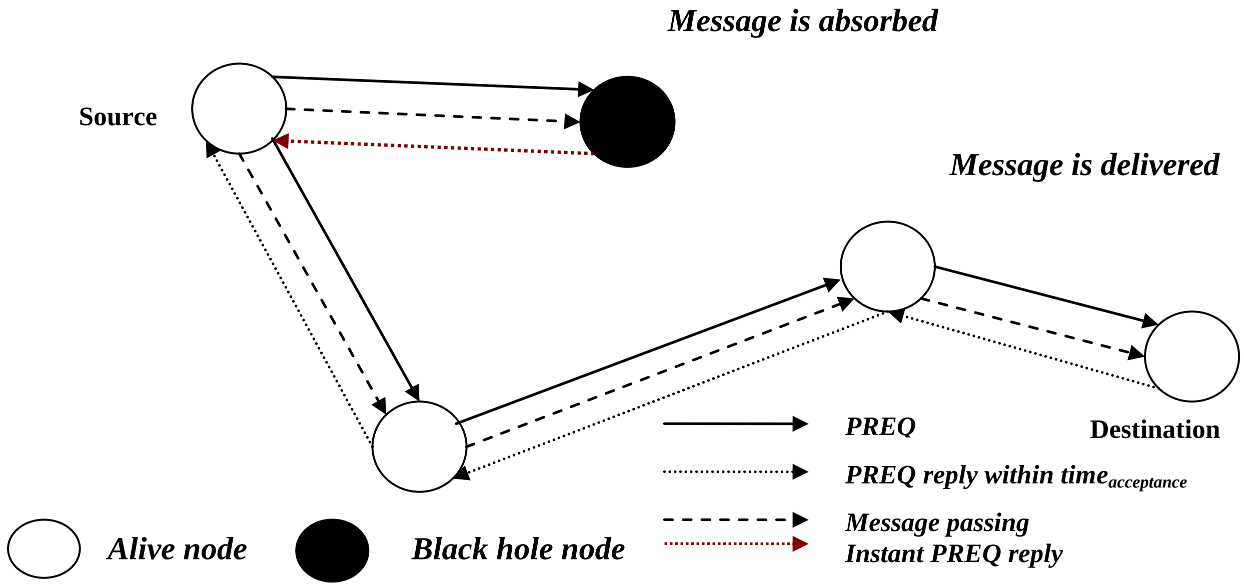


Fig. 3. Schematic representation of Black Hole Problem

For solution of several computational problems, nature inspired computing has been followed in computer science. One of major solving methodology uses “artificial neurons”, which is very much similar to biological neurons. These are called artificial neural networks (ANNs). Natural neurons obtain signals through “synapses” situated on the dendrites or membrane of the neuron. When the signals acknowledged are strong enough (surpass a certain “threshold”), the neuron is “activated” and emits a signal though the “axon”. This signal might be sent to another synapse, and might activate other neurons [17].A typical diagram for neuron network is described in Fig. 4[19].

Complexity of real neurons is exceedingly abstracted at the time of modeling of artificial neurons. They are basically consist of “inputs” (like synapses), which are multiplied by “weights” (strength of the respective signals), and then computed by a mathematical function which determines the “activation” of that concerned neuron.

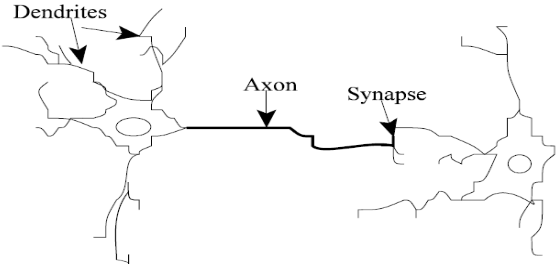


Fig. 4.[19]

Another function (which may be the identity) computes the "output" of the artificial neuron (sometimes in dependence of a certain "threshold"). ANNs combine artificial neurons in order to process information. A typical flow chart for neuron data processing is described in Fig. 5[19].

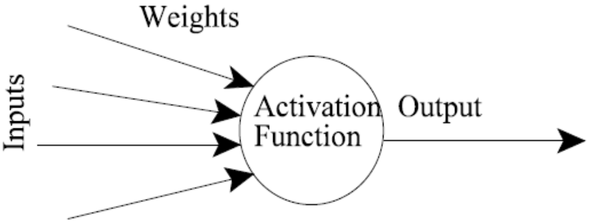


Fig. 5. [19]

Weights may be negative, so a signal is "inhibited" by the negative weight. Depending on the weights, the computation of the neuron will be different. By adjusting the weights of an artificial neuron, the output is obtained for the specified set of input. But in a network of an ANN of hundreds or thousands of neurons, it would be quite complicated to find by hand all the necessary weights. For that scenario, there exist algorithms which can adjust the weights of the ANN in order to obtain the desired output from the network. This process of adjusting the weights is called "learning" or "training" [18]. The number of types of ANNs and their uses in real life computing problem is very high. Since the first neural model by McCulloch and Pitts (1943), there have been rapid developments of hundreds of different models considered as ANNs. The differences in them might be the functions, the accepted values, the topology, the learning algorithms, etc. Also there are many hybrid models where each neuron has more properties. Since the function of ANNs is to process information, they are used mainly in fields related with it. There are a wide variety of ANNs that are used to model real neural networks, and study behavior and control in animals and machines, but also there are ANNs which are used for engineering purposes, such as pattern recognition, forecasting, and data compression [17-20].

Rest of the paper is organized as follows: Section II briefs about the related work; Section III describes proposed work; Experimental observations and result analysis are shown in Section IV and Conclusion is reflected in Section V.

II. Related Work

Different ideas and studies have been discussed for the Black Hole node problem and its effects on the routing process [7]. Researchers have proposed solutions to identify and eliminate Black Hole nodes [10-16]. In their researches, they have focused several methodologies to detect Black Hole nodes. Some methodologies are simply graph-based method. But they have not considered the cooperative black hole attacks. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attacks on MANETs. Important efforts have been established for automation of tasks using ANN [17]. Some well known efforts have been targeted using perceptron model [18].The perceptron, the simplest form of a neural network, is able to classify data into two classes.

III. Proposed Work

We have proposed a ANN based "alive node" detection methodology that is easier to implement in hardware circuits and less expensive. Perceptron model based computation has been used for Black Hole and alive node detection. Fig. 6 shows state diagram design for Dead (Black Hole) node with a biased to be in "alive" state. This design is applicable for any node participating in a MANET communication. Fig. 6 represents this design technique.

Proposed methodology is implemented at both end of a cluster based MANET communication architecture as described in Fig. 2. Two simultaneous Black Hole detection algorithms are running on CRC and TTR side. Fig. 7 [1] and Fig. 8 [1] respectively illustrate the basic flowchart at CRC and TTR side. Following fact has been considered that a PREQ reply must arrive to its sender node within a range of acceptance time ($time_{acceptance}$) as described in following Equation 1.

$0 < time_{acceptance} < infinity$ ………(1) [1]

In practice waiting time for PREQ reply ($time_{acceptance}$) should be discarded as soon as the next PREQ is send by sender after a considerable amount of time.

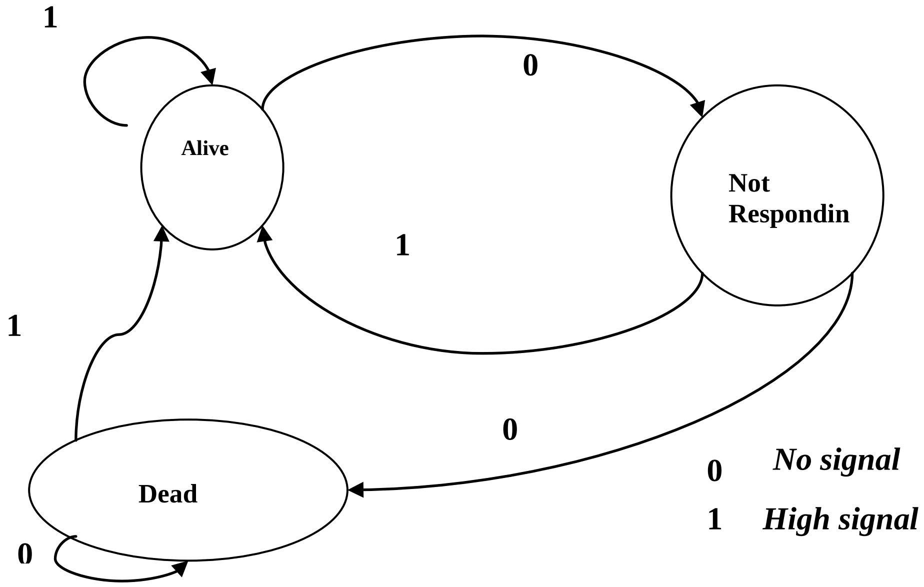


Fig. 6. A biased design for Dead Node detection [1]

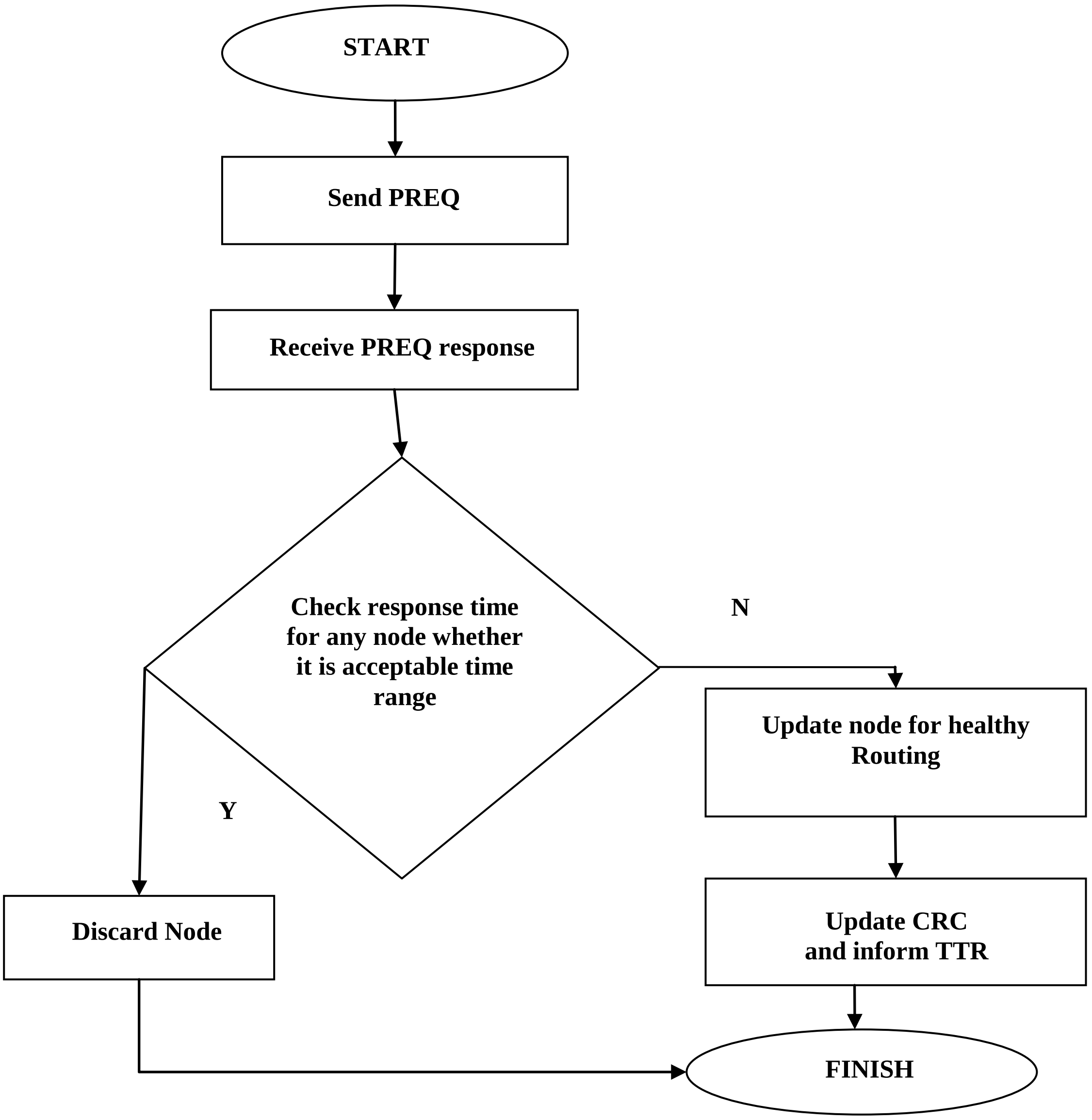

START
Send PREQ
Receive PREQ response
Check response time for any node whether it is acceptable time range
N
Y
Update node for healthy Routing
Update CRC and inform TTR
Discard Node
FINISH

Fig. 7. Flowchart for Black Hole Node detection at CRC [1]

Based on flowchart as reflected in Fig. 7, Algorithm 1 is implemented at CRC side to detect Black Hole node(s) in MANET.

Algorithm 1: CRC_side_black_hole_node_detection [1]

```
Input: nodes (cells)
Output: alive nodes, restricted nodes

Step 1: Start

Step 2: Initialize a cell

Step 3: Check if signal connectivity exists in node, then follow Step 4 else follow
          Step 7

Step 4: Mark the corresponding cell as "Alive Node"

Step 5: Allow particular node for participation in routing

Step 6: Inform sender TTR with updated information of alive- nodes

Step 7: Update node status as "Not Responding"

Step 8: Search if signal connectivity is found latter in "Not Responding" node then
         follow Step 4 else follow Step 9

Step 9: Change "Not Responding" node status into "Black Hole Node"

Step 10: Search if signal connectivity is found latter in "Black Hole Node" node then
         follow Step 4 else follow Step 9

Step 11: Stop
```

Based on flowchart as reflected in Fig. 8, Algorithm 2 is implemented at TTR side to detect Black Hole node(s) in MANET communication.

Algorithm 2: TTR_side_black_hole_node_detection [1]

```
Input: nodes (cells)
Output: alive nodes, restricted nodes, routing table

Step 1: Start

Step 2: Initialize a sender cell

Step 3: Send PREQ to all surrounding nodes in "alive" status

Step 4: Receive PREQ response

Step 5: Check if PREQ response time is within acceptance time, then follow Step 7
          else follow Step 6

Step 6: Mark the corresponding cell as "Black Hole Node" and go to Step3

Step 7: Update node for healthy routing

Step 8: Update CRC

Step 9: Stop
```

a

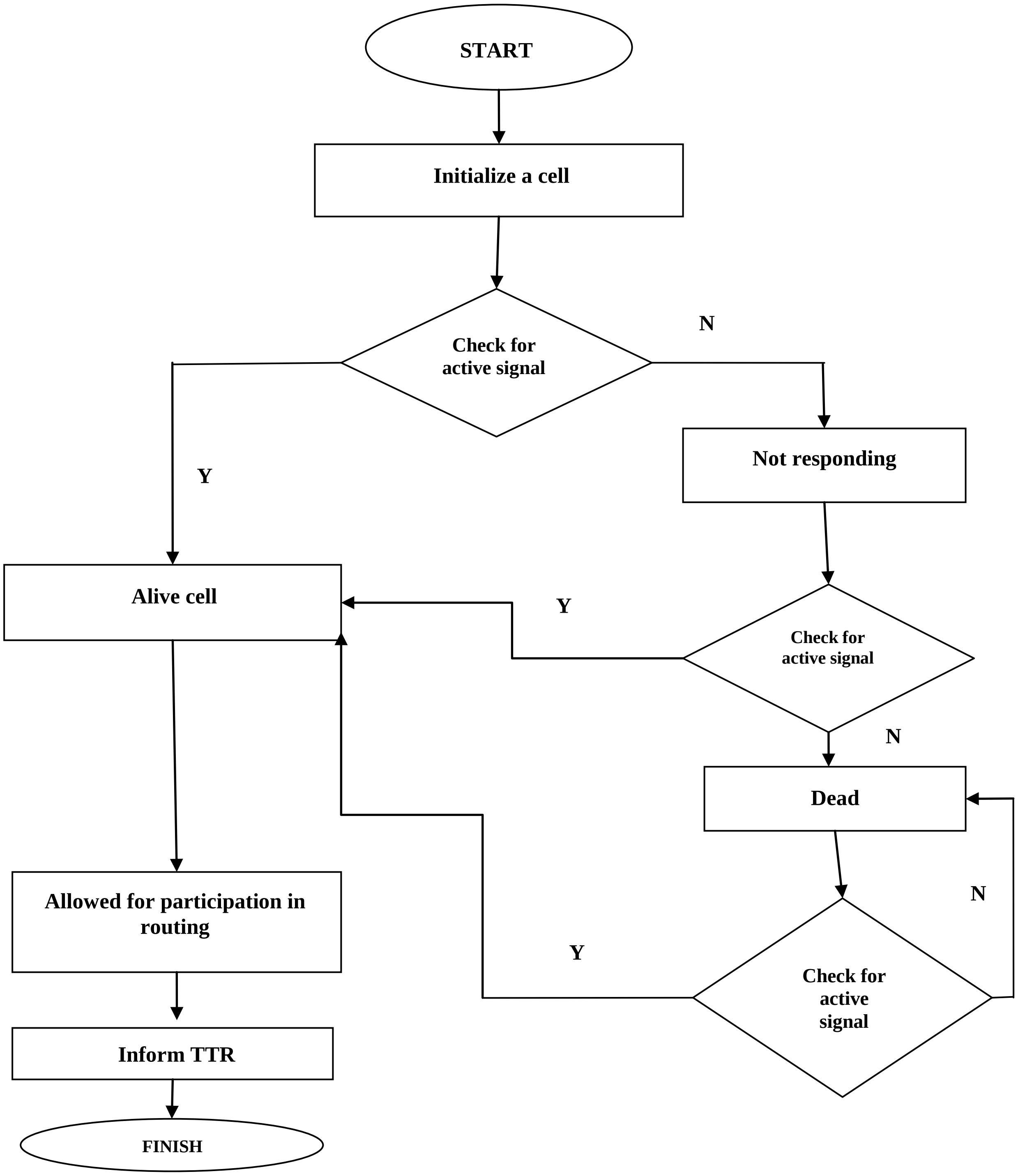


Fig. 8. Flowchart for Black Hole Node detection for TTR [1]

Using Algorithm 1 and Algorithm 2, our proposed methodology thus updates the routing table with the fact of newly detected Black Hole node in MANET. Thus proposed system becomes dynamic in nature. Proposed ANN based design for detecting Black Hole nodes is further described in Fig. 9.

TABLE1: POSSIBLE STATE CONFIGURATIONS AND REMARKS

Alive Node (A)	**Not Responding Node (B)**	**Black Hole Node (C)**	**Result (Z)**
0	0	0	Black Hole Node (0)
0	0	1	Black Hole Node (0)
0	1	1	Black Hole Node (0)

0	1	0	Not Responding Node (0)
1	1	0	Not a valid configuration for Node (0)
1	0	0	Alive Node (1)
1	0	1	Not a valid configuration for Node (0)
1	1	1	Not a valid configuration for Node (0)

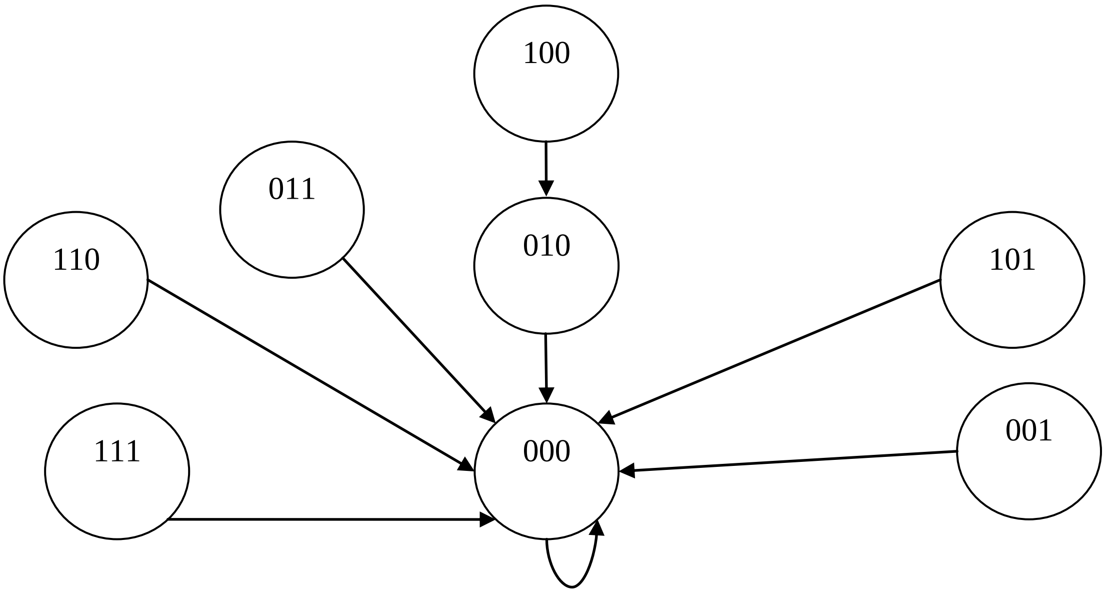


Fig. 9 (a). Proposed State transition diagram for Black Hole Node detection System

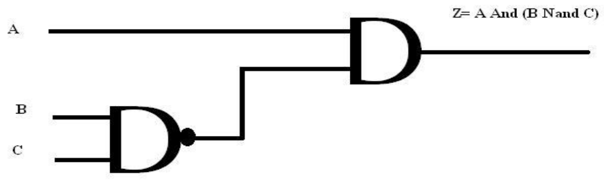


Fig. 9 (b). Proposed logic diagram for Black Hole Node detection System

Achieved relation for perceptron training described in Fig. 9 (b) is described in Equation 1.

Z= A And (B Nand C) …………..(1)

IV. Experimental Observations and Result Analysis

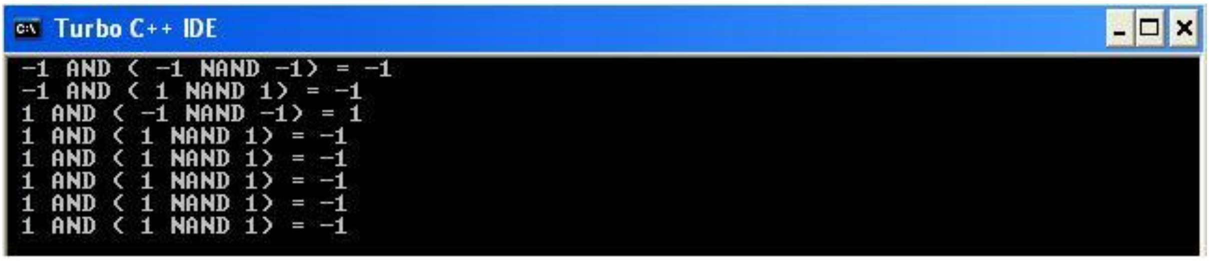
Figure 9 has been further implemented in supervised learning module for perceptron training model as reported in Table 2.

TABLE 2. TRAINING DATA SET USED IN PERCEPTRON MODEL

Training No.	A	B	C	Z = A And (B Nand C)
1.	-1.0	-1.0	-1.0	-1.0
2.	1.0	-1.0	-1.0	1.0
3.	-1.0	-1.0	1.0	-1.0
4.	-1.0	1.0	-1.0	-1.0

5.	-1.0	1.0	1.0	-1.0
6.	1.0	-1.0	1.0	-1.0
7.	1.0	1.0	-1.0	-1.0
8.	1.0	1.0	1.0	-1.0

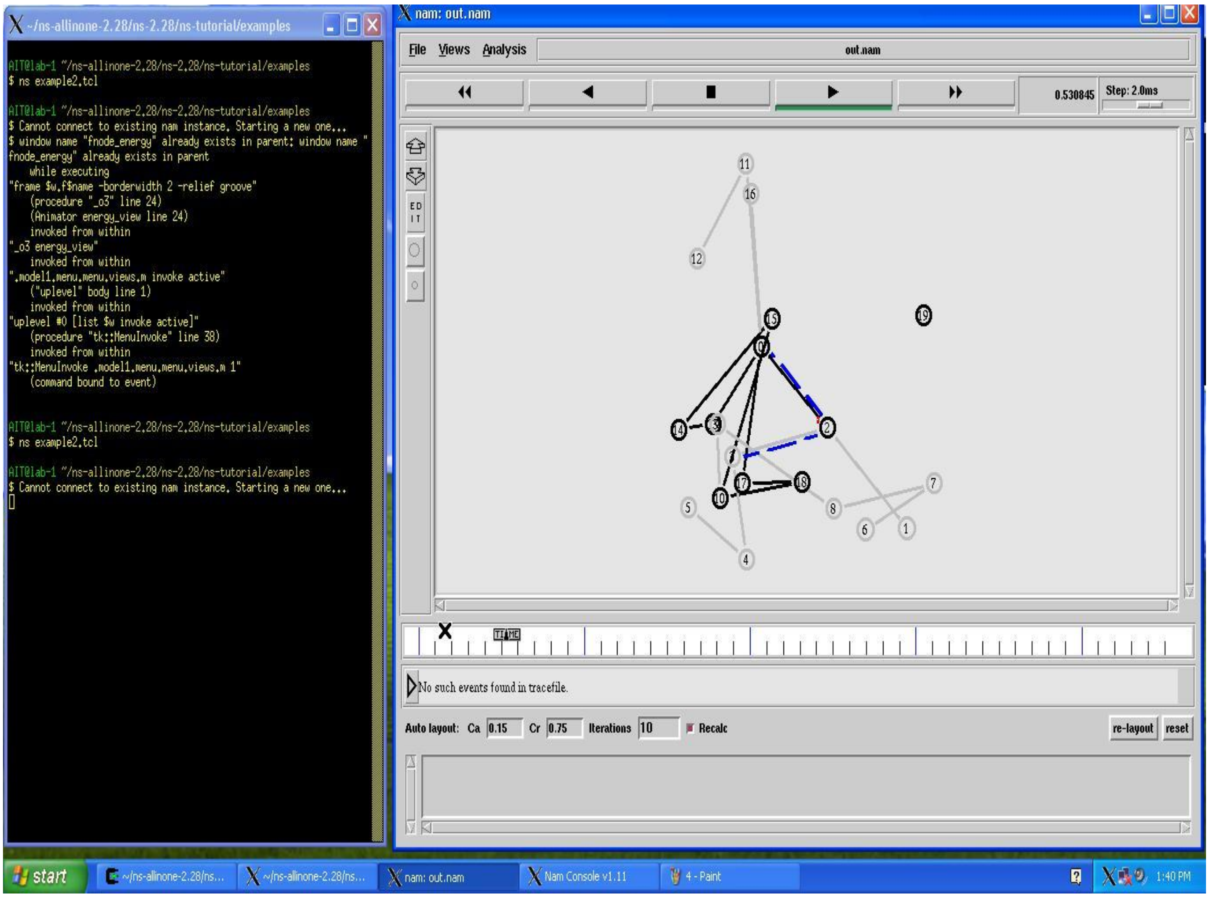
High impedance value and low impedance value for any input and processed output is represented by "1.0" and "-1.0" respectively in Table 2. Learning outcome based on Table 2 is reported in Fig. 10. Thus the perceptron model helps to check out "alive nodes" in MANET.



```
-1 AND ( -1 NAND -1) = -1
-1 AND ( 1 NAND 1) = -1
1 AND ( -1 NAND -1) = 1
1 AND ( 1 NAND 1) = -1
1 AND ( 1 NAND 1) = -1
1 AND ( 1 NAND 1) = -1
1 AND ( 1 NAND 1) = -1
1 AND ( 1 NAND 1) = -1
```

Fig. 10. Snapshot of Learning Procedure

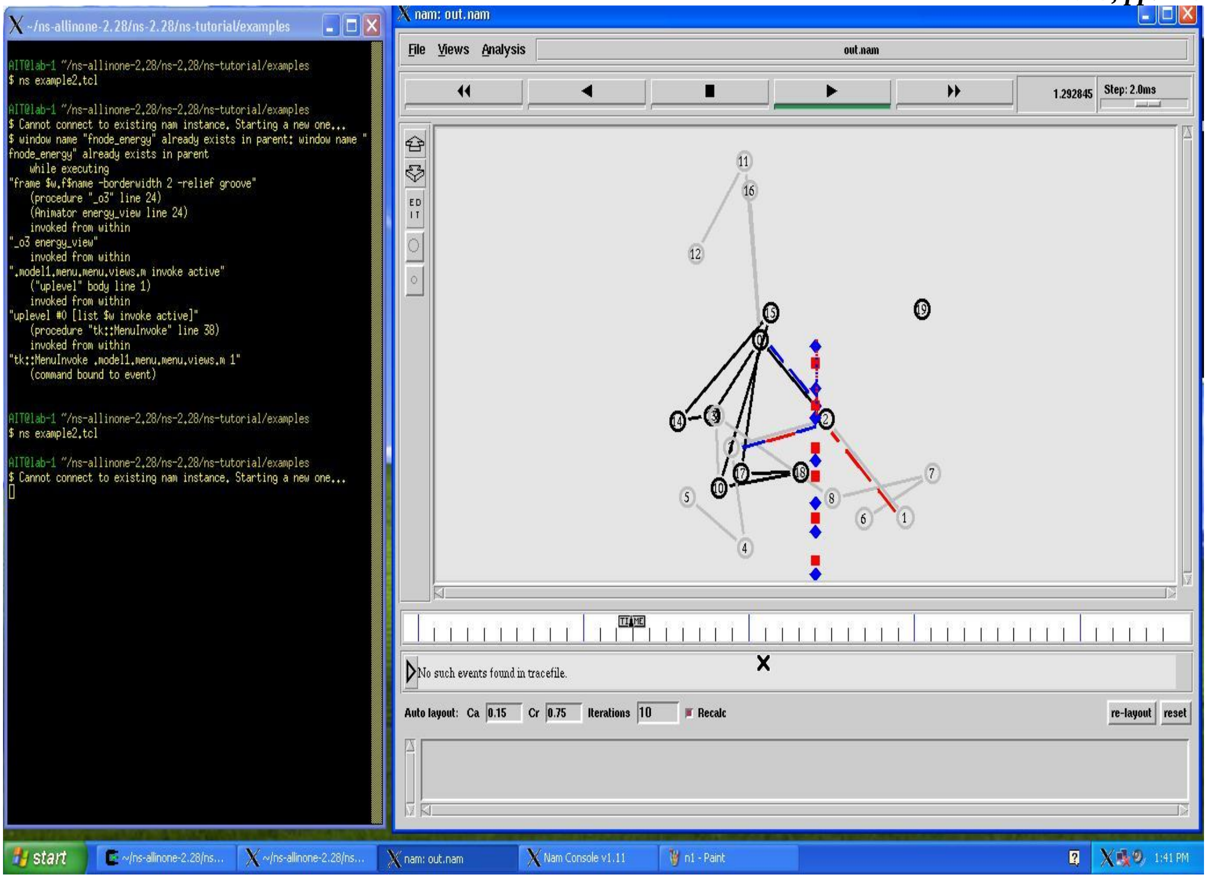
To show that MANET transmission is affected by the presence of Black Hole nodes, we have implemented Black Hole node attack in an ns-2 simulator. For our simulations, we have implemented CBR (Constant Bit Rate) application, TPC/IP (full duplex communication), IEEE 802.11b MAC and physical channel based on statistical propagation reproduction. The replicated network consists of 20 arbitrarily owed wireless nodes in a flat freedom. In our experimental situation we have allowed 20 nodes in which nodes 1, 5, 6, 12 and 19 are Black Hole nodes responsible for nasty behaviour. Subsequent metrics that have been used to assess the performance are shown in Fig. 11 and Fig. 12.



```
AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ ns example2.tcl

AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ Cannot connect to existing nam instance. Starting a new one...
$ window name "fnode_energy" already exists in parent: window name "
fnode_energy" already exists in parent
    while executing
"frame $w.f$name -borderwidth 2 -relief groove"
    (procedure "_o3" line 24)
    (Animator energy_view line 24)
    invoked from within
"_o3 energy_view"
    invoked from within
".model1.menu.menu.views.m invoke active"
    ("uplevel" body line 1)
    invoked from within
"uplevel #0 [list $w invoke active]"
    (procedure "tk::MenuInvoke" line 38)
    invoked from within
"tk::MenuInvoke .model1.menu.menu.views.m 1"
    (command bound to event)


AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ ns example2.tcl

AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ Cannot connect to existing nam instance. Starting a new one...
```

No such events found in tracefile.

Fig. 11. Snapshot 1 for ns2 simulation for an arbitrary MANET



```
~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples

AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ ns example2.tcl

AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ Cannot connect to existing nam instance. Starting a new one...
$ window name "fnode_energy" already exists in parent: window name "
fnode_energy" already exists in parent
    while executing
"frame $w.f$name -borderwidth 2 -relief groove"
    (procedure "_o3" line 24)
    (Animator energy_view line 24)
    invoked from within
"_o3 energy_view"
    invoked from within
".model1.menu.menu.views.m invoke active"
    ("uplevel" body line 1)
    invoked from within
"uplevel #0 [list $w invoke active]"
    (procedure "tk::MenuInvoke" line 38)
    invoked from within
"tk::MenuInvoke .model1.menu.menu.views.m 1"
    (command bound to event)


AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ ns example2.tcl

AIT@lab-1 ~/ns-allinone-2.28/ns-2.28/ns-tutorial/examples
$ Cannot connect to existing nam instance. Starting a new one...
```

nam: out.nam

out.nam

1.292845 Step: 2.0ms

No such events found in tracefile.

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc

Fig. 12. Snapshot 2 for ns2 simulation for an arbitrary MANET

Fig. 11 and Fig. 12 highlight the consequence for established routes from source to destination. For our Experiment we have considered Node 0 as source and Node 10 as destination in an arbitrary MANET. Dark colour line shows an existence of valid route from source to destination where faded lines indicate that the path is affected by presence of Black Hole node and that concerned route is not a proper connection between source and destination. Blue and Red colour indicates the full duplex communication between source and destination in shortest path. Dotted Red and Blue colour vertical line in Fig. 121 reflects a synchronisation point at Node 2.

V. Conclusion

It is observed in experimental results that the communication in MANET is abruptly affected by the presence of Black hole nodes in MANET. Proposed ANN based system is dynamic in nature. Implemented intercommunication methodology for detecting the presence of Black Hole node helps to update routing table more dynamically as it is working at both ends: at CRC side and TTR side. This detection methodology generates a similar result as we have already achieved for Black Hole detection in MANET using CA [1]. Hence ANN based black detection methodology is an efficient way to detect presence of black hole nodes in MANET.

Acknowledgment

Our sincere thanks to IJARCSSE for allowing us to modify template they have provided.

References

[1] Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Santanu Kr. Sen; *An Approach to Detect Black Hole Nodes in Wireless Network Using Cellular Automata*; International Journal of Advanced Research in Computer Science & Software Engineering (IJARCSSE); Volume 2, Issue 9; September 2012

[2] Ad-hoc Network; *http://en.wikipedia.org/wiki/Wireless_ad-hoc_network*

[3] MANET; *http://*en.wikipedia.org/wiki/Mobile_ad_hoc_network

[4] Lecture Notes on DSDV; *www.cs.sunysb.edu/~jgao/CSE370-spring06/lecture10.pdf*

[5] Lecture Notes on DSR; *www.monarch.cs.rice.edu/monarch-papers/dsr-chapter00.pdf*

[6] Lecture Notes on AODV; *www.moment.cs.ucsb.edu/pub/wwan_chakeres_i.pdf*

[7] Lecture Notes on MANET communication; www.cnd.iit.cnr.it/andrea/docs/chap_rman06_p2p.pdf

Fan-Hsun Tseng et al.; A survey of black hole attacks in wireless mobile ad hoc networks; Human-centric Computing and Information Sciences; Springer Open Journal; 2011

[8] Artificial Neural Network; *www.edugi.uni-muenster.de/eduGI.../ArtificialNeuralNetworks240506.pdf*

[9] Rajib Das et al.; *Security Measures for Black Hole Attack in MANET: An Approach*; International Journal of Engineering Science and Technology (IJEST); Vol. 3, No. 4; 2011

[10] Elmar Gerhards et al.; *Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs*; 32nd IEEE Conference on Local Computer Networks; 2007

[11] XiaoYang Zhang ; *Proposal of a method to detect black hole attack in MANET*; This paper appears in: Autonomous Decentralized Systems (ISADS '09) ; 2009

[12] Akanksha Saini et al.; *Comparison Between Various Black Hole Detection*; National Conference on Computational Instrumentation (NCCI); 2010

[13] Hesiri Weerasinghe; *Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation*; Proceedings of the Future Generation Communication and Networking, vol. 02; 2007

[14] Sheenu Sharma et al.; *Simulation study of Black H Attack in the Mobile ad hoc networks*; Journal of Engineering Science and Technology; Vol. 4, No. 2 ; 2009

[15] Sanjay Ramaswamy et al.; *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*; Int’l Conf. on Wireless Networks; 2003

[16] Akanksha Saini et al.; *Effect Of Black Hole Attack On AODV Routing Protocol In MANET*; International Journal of Computer Science and Technology (IJCST) Vol. 1, Issue 2, 2010

[17] Perceptron: www.cs.otago.ac.nz/cosc343/Lectures/L12-perceptron.pdf

[18] Artificial Neural Network: www.amc-app1.amc.sara.nl/EDUwiki/images/f/ff/Nbt_primernn.pdf

[19] Arttificial Neural Network: www. en.wikipedia.org/wiki/Artificial_neural_network

[20] Types of neural netwok: www. en.wikipedia.org/wiki/Types_of_artificial_neural_networks