Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Approach to Detect Black Hole Nodes in Wireless Network Using Cellular Automata

[1]Arnab Mitra, [1]Rajib Ghosh, [2]Apurba Chakraborty, [3]Santanu Kr. Sen
[1]Dept. of CSE, Adamas Institute of Technology, India-700126
[2] Dept. of MCA, Siliguri institute of Technology, India-734009
[3] Dept. of CSE, Guru Nanak Institute of Technology, India-700114

Abstract— In this research work, we have put an emphasis on 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 black hole node problem, which affects the entire routing process. To deal with this routing disorder, we have proposed Cellular Automata (CA) based Black Hole node detection methodology, which is capable of detecting & removing Black hole node(s) in the MANET. The proposed methodology is easy to implement in hardware and also a cost effective solution in terms of production cost.

Keywords— Mobile ad hoc networks (MANETs), black hole node, network security, routing, Cellular Automata (CA)

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.

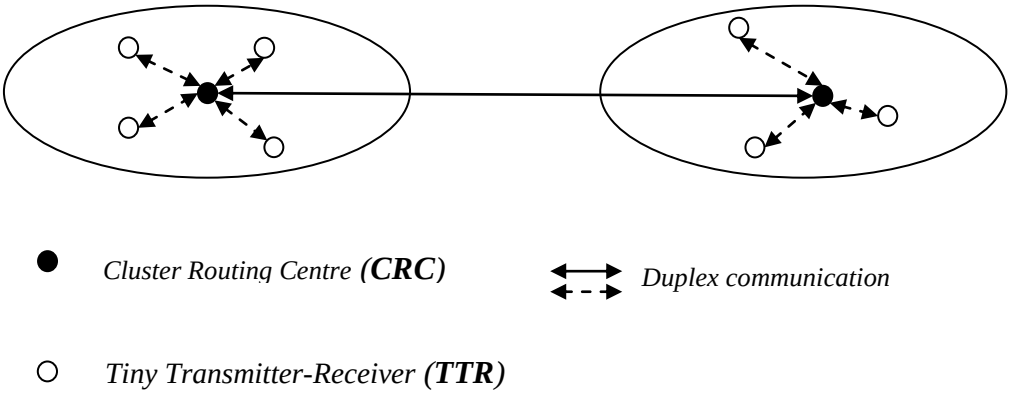

Fig. 1. Schematic representation for MANET communication

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.

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

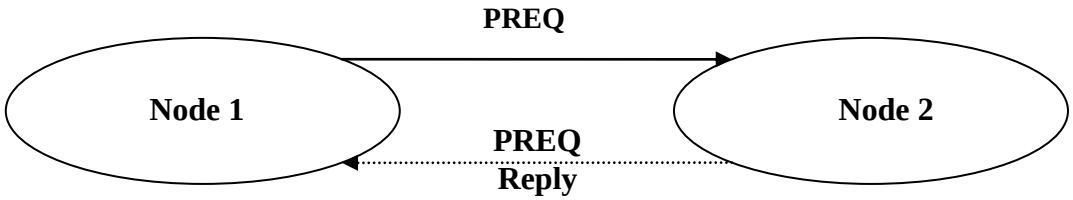

Fig. 2. Basic MANET communicating clusters

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. 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.

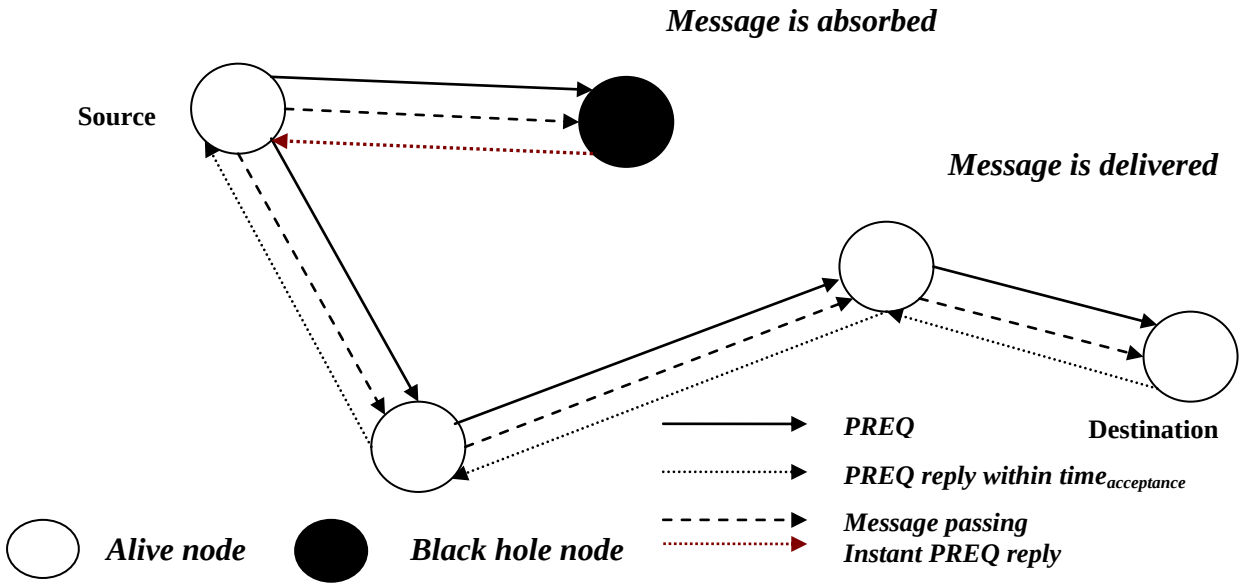

Fig. 3. Schematic representation of Black Hole Problem

Cellular Automata [8] is used to represent a dynamic mathematical model. A Cellular Automaton (pl. cellular automata, in short CA) is a discrete model studied in computability theory and complexity science for any dynamic system or modelling. A regular grid of cells, each in one of a finite number of states, such as "1" for ON and "0" for OFF, produces CA cell framework. This framework might be in multi-dimensions. For each cell, a set of cells called its neighbourhood (usually including the cell itself) is defined relative to the specified cell. A new generation is created (advancing time by 1), according to some predetermined mathematical function that determines the new state of each cell in terms of the current state of the cell and the states of the cells in its neighbourhood.

The simplest CA is one-dimensional with only two neighbours defined at the adjacent cells on either side of it. This combination forms a neighbourhood of 3 cells, with 2^3=8 possible patterns for this neighbourhood. There are then 2^8=256 possible rules. These 256 CAs are generally referred to by their Wolfram code. Wolfram code is a standard naming

convention invented by Wolfram; it gives each rule a number from 0 to 255. A number of papers have analysed and compared these 256 CAs, either individually or collectively [9].

CA has a significant role for computation, as it is easy to implement through hardware components. Following Fig. 4 shows a rough outline of CA implementation and Fig. 5 describes the hardware implementation of CA through flip-flop.

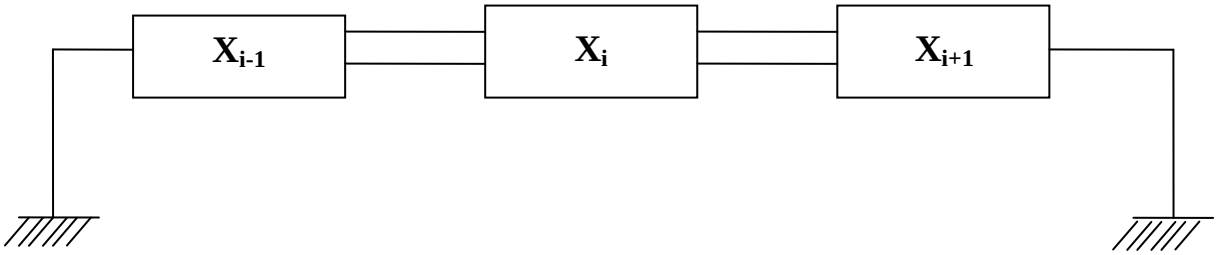

Fig. 4. Typical representation of 3-cell Null Boundary CA

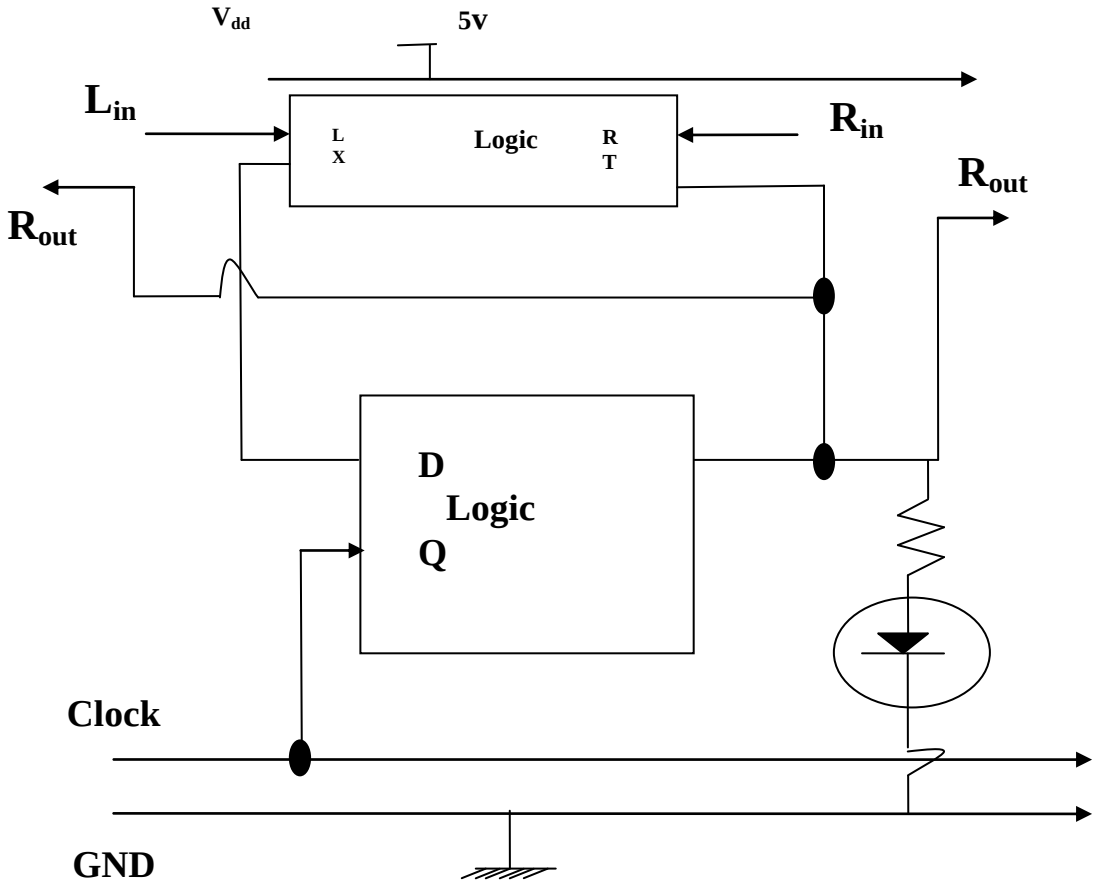

Fig. 5. Typical hardware implementation of CA cell

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 [10-17]. 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. Besides these research works on detection of Black Hole nodes for MANET, some efforts have been made to realize ad hoc network using CA [18]. The easy to implement feature and cost effectiveness of CA has thus initiated a search for a solution if exists for detecting Black hole nodes in MANET using CA.

III. PROPOSED WORK

We have proposed a CA based Black Hole node detection methodology that is easier to implement in hardware circuits and less expensive. Flip-flop based basic nature of CA facilitates the memory based computation for Black Hole 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.

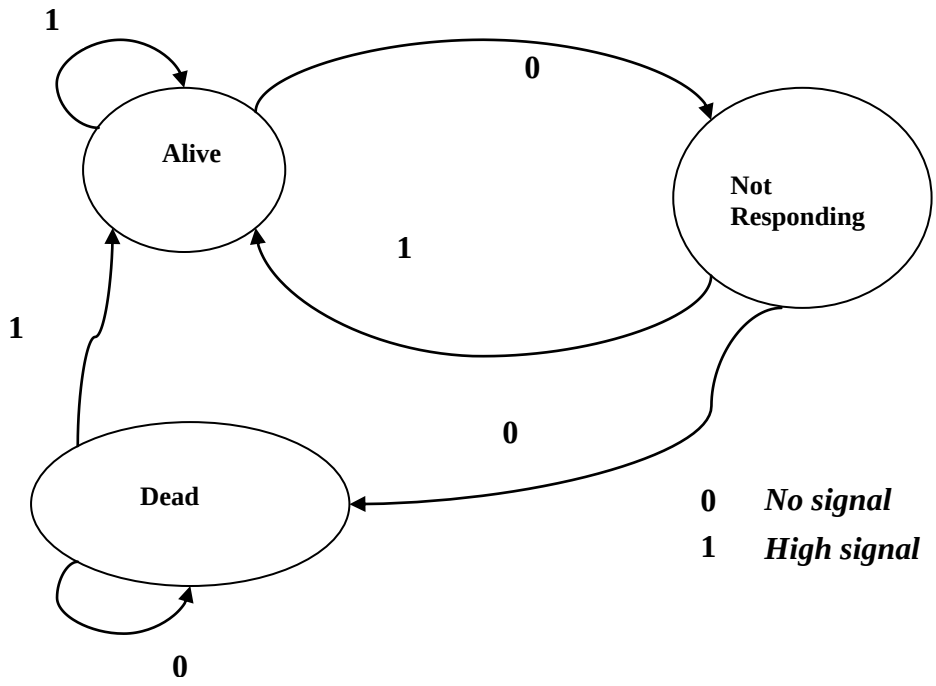

Fig. 6. A biased design for Dead Node detection

Proposed methodology is implemented at both end of a cluster based MANET communication architecture as described in Fig. 2. Two simultaneous Black Hole detection algorithm is running on CRC and TTR side. Fig. 7 and Fig. 8 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)

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.

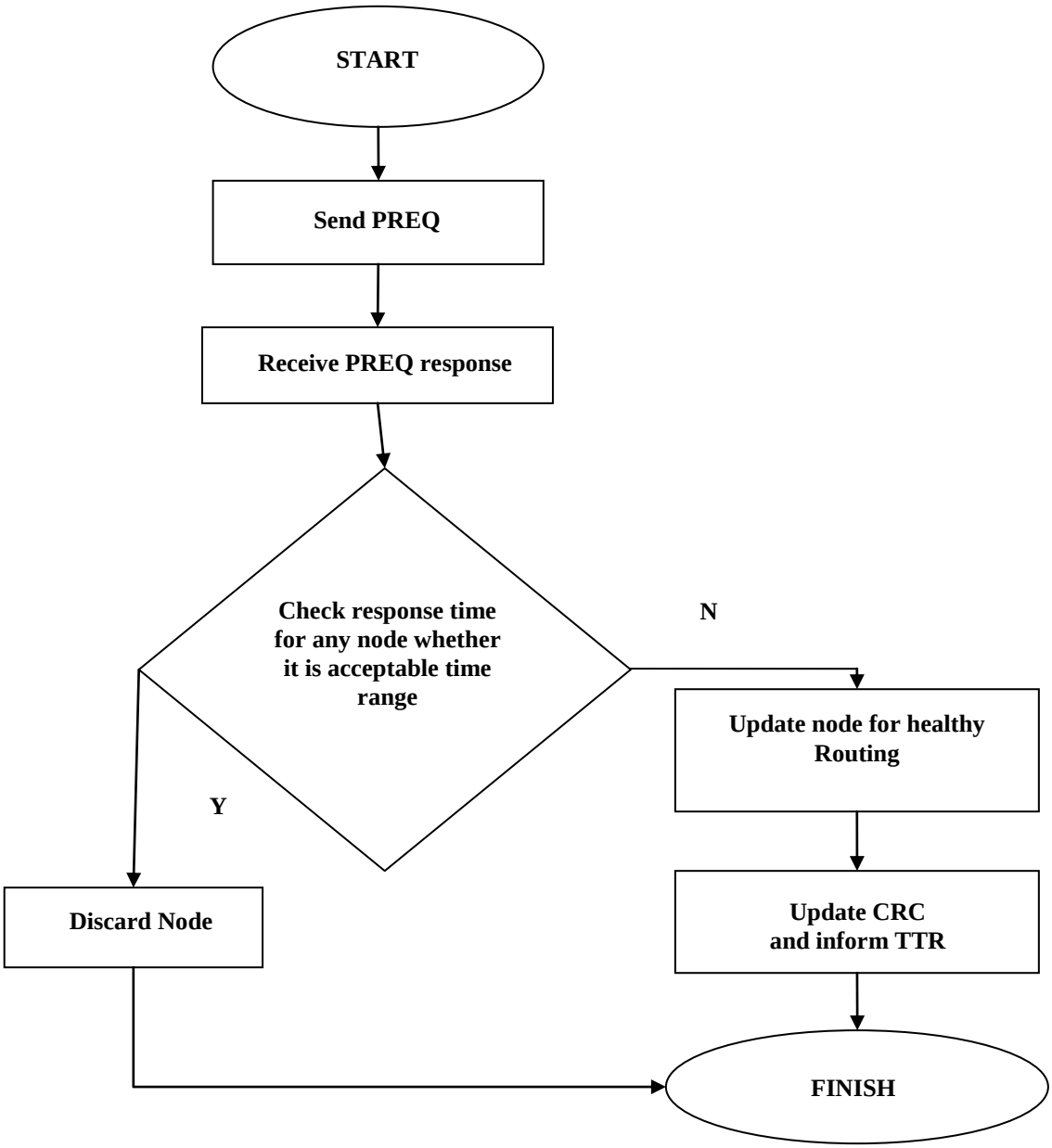

Fig. 7. Flowchart for Black Hole Node detection at CRC

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

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

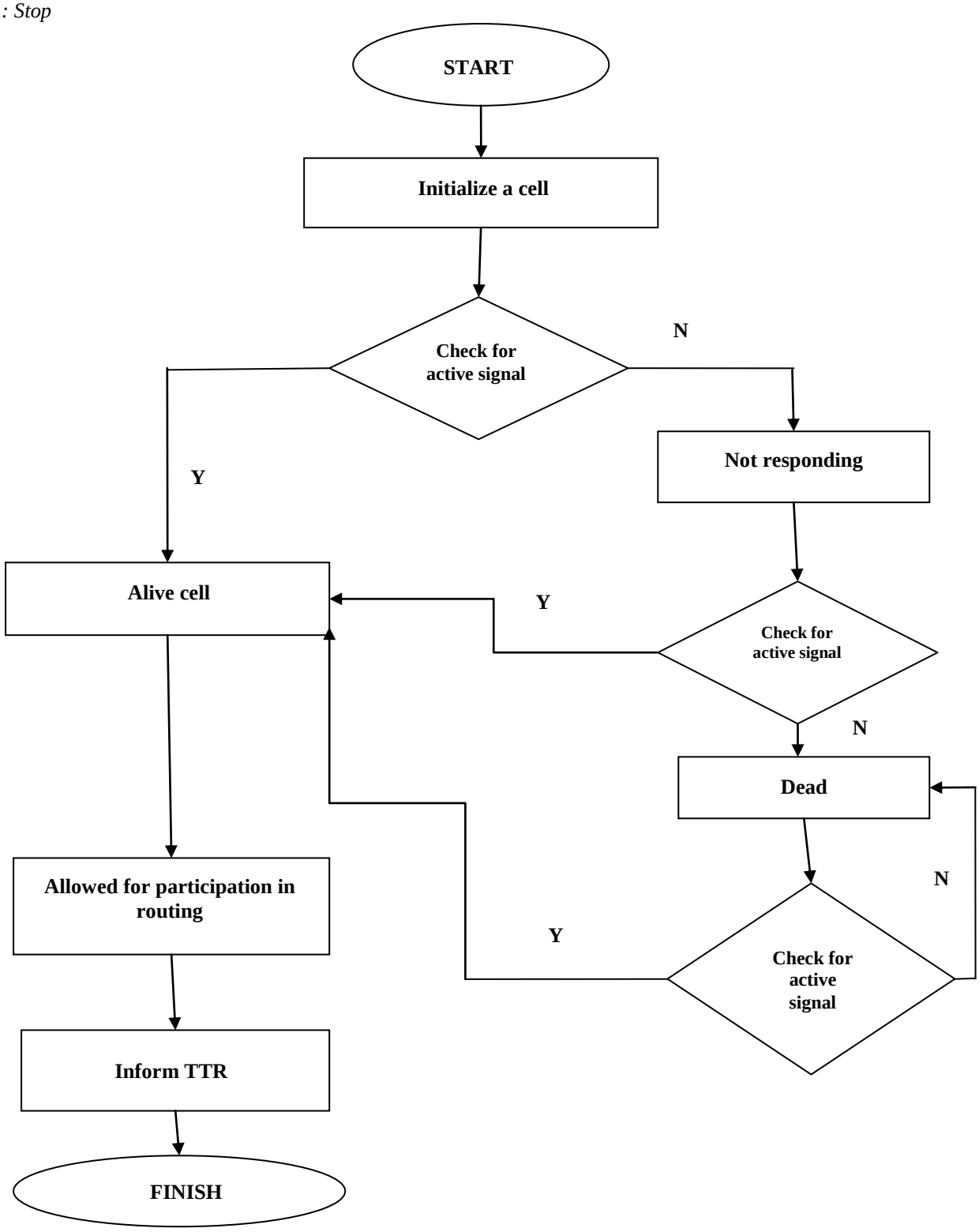

Fig. 8. Flowchart for Black Hole Node detection for TTR

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

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

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 CA based design for detecting Black Hole nodes is further described in Fig. 9. The design achieved in Fig. 9 indicates the possible state values for a three cell null boundary CA are "Alive" is either 0 or 1, "Not Responding" is either 0 or 1 and "Dead or Black Hole" is either 0 or 1. Value 1 indicates about the active status of that corresponding cell/state. Details of these facts are shown in Table 1. Fig. 9 shows the proposed transitions based on Table 1.

TABLE1: POSSIBILITY FOR STATE CONFIGURATION AND CONCLUSIONS

"Alive"	**"Not Responding"**	**"Black Hole"**	**Decimal Equivalent State Value**	**Conclusion**
0	0	0	0	Black Hole node
0	0	1	1	Black Hole node
0	1	1	3	Black Hole node
0	1	0	2	Not Responding Node
1	1	0	6	Not a valid configuration
1	0	0	4	Alive
1	0	1	5	Not a valid configuration
1	1	1	7	Not a valid configuration

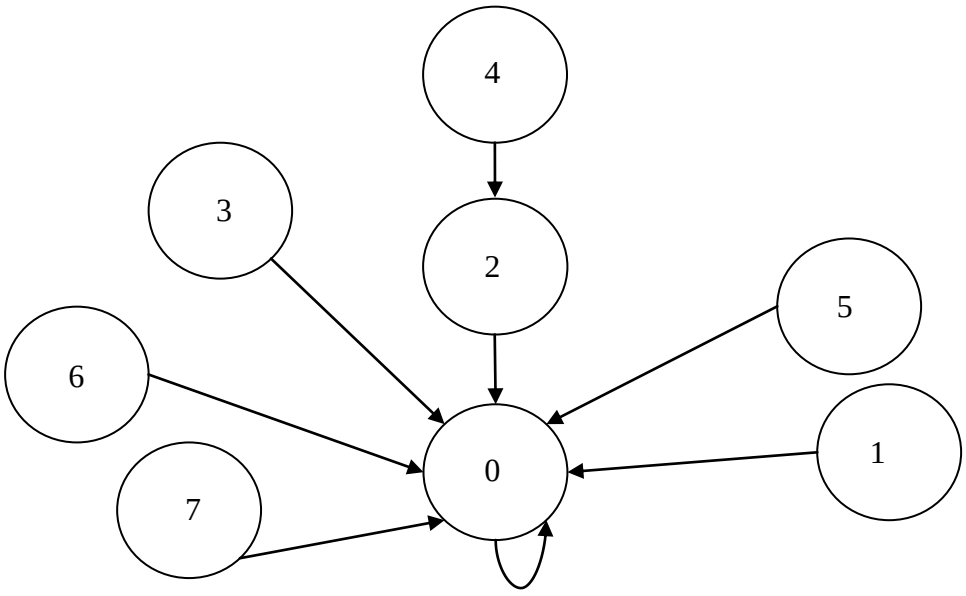

Fig. 9. State transition diagram for CA based Black Hole Node detection System

Based on the state diagram described in Fig. 9, following CA rules are synthesized in RMT generation for CA for a null boundary 3-cell CA as described in Fig. 4. RMT generation process is described as follows:

	X_{i-1}	X_i	X_{i+1}	
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0
	0	0	0	


```
    ------------------------------------
0       0       0       1       0
        0       0       0
    ------------------------------------
0       0       1       1       0
        0       0       0
    ------------------------------------
0       1       0       1       0
        0       0       0
    ------------------------------------
0       1       1       0       0
        0       0       0
    ------------------------------------
0       1       1       1       0
        0       0       0
```

Based on this above calculation for generation for RMT, CA rule calculation is followed in Table 2.

TABLE 2. RMT TABLE

	111	**110**	**101**	**100**	**011**	**010**	**001**	**000**
R0=0	D	D	D	D	D	0	0	0
R1=16	D	D	D	1	0	0	0	0
R2=0	D	0	D	0	D	0	D	0

In Table 2, "D" refers don't care condition for constructing RMT table. From Table 2, rule characteristics for anticipatory CA rules for Black Hole node detection, are reflected in Table 3.

TABLE 3. RULE CHARACTERISTICS TABLE

CA rule in Decimal Representation	**CA rule in 8-bit Binary Representation**	**Boolean Form for associated CA rule for next cell value=($X_i(t+1)$)**
0	00000000	0
16	00010000	$X_{i-1}(t)$ AND (NOT $X_i(t)$) AND (NOT $X_{i+1}(t)$)

IV. EXPERIMENTAL OBSERVATIONS AND RESULT ANALYSIS

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. 10 and Fig. 11.

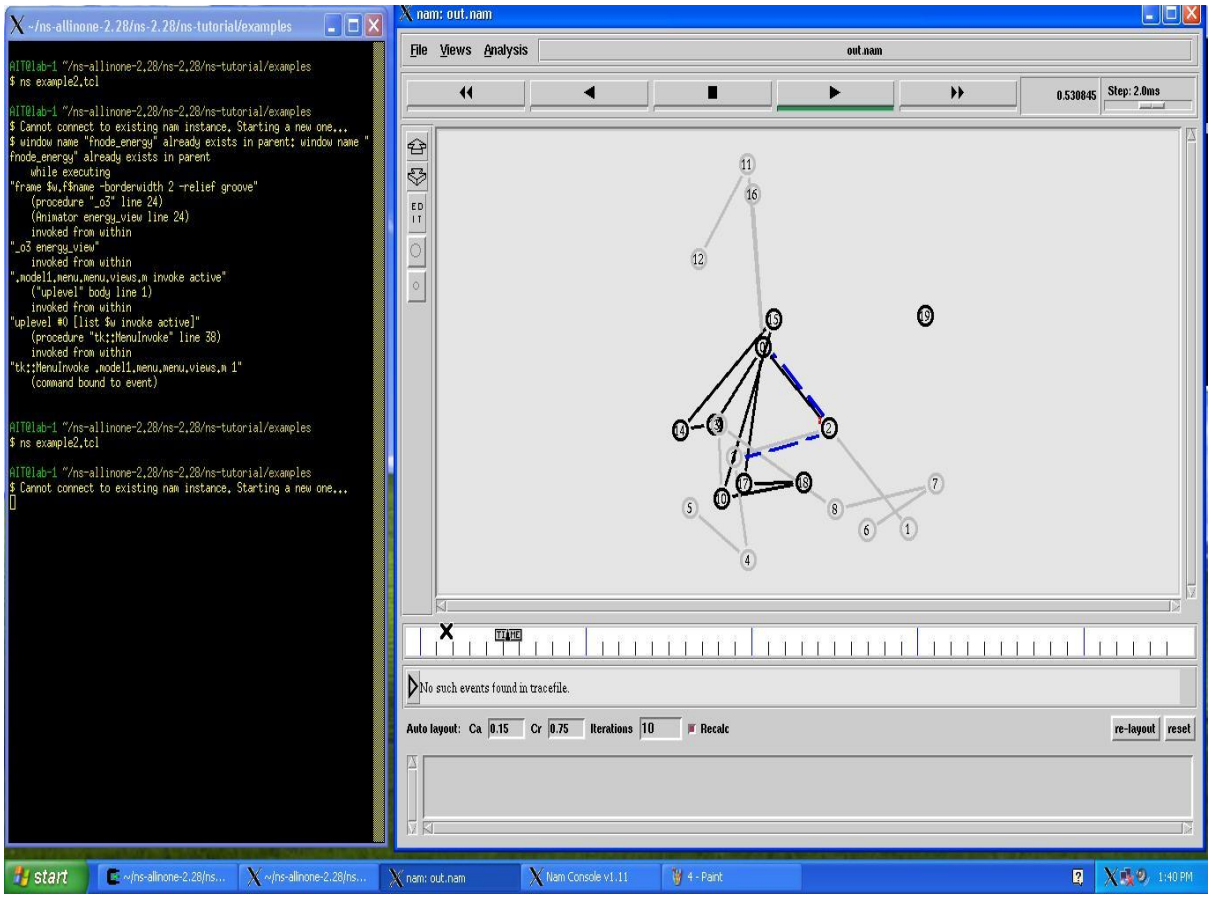

Fig. 10. Snapshot 1 for ns2 simulation for an arbitrary MANET

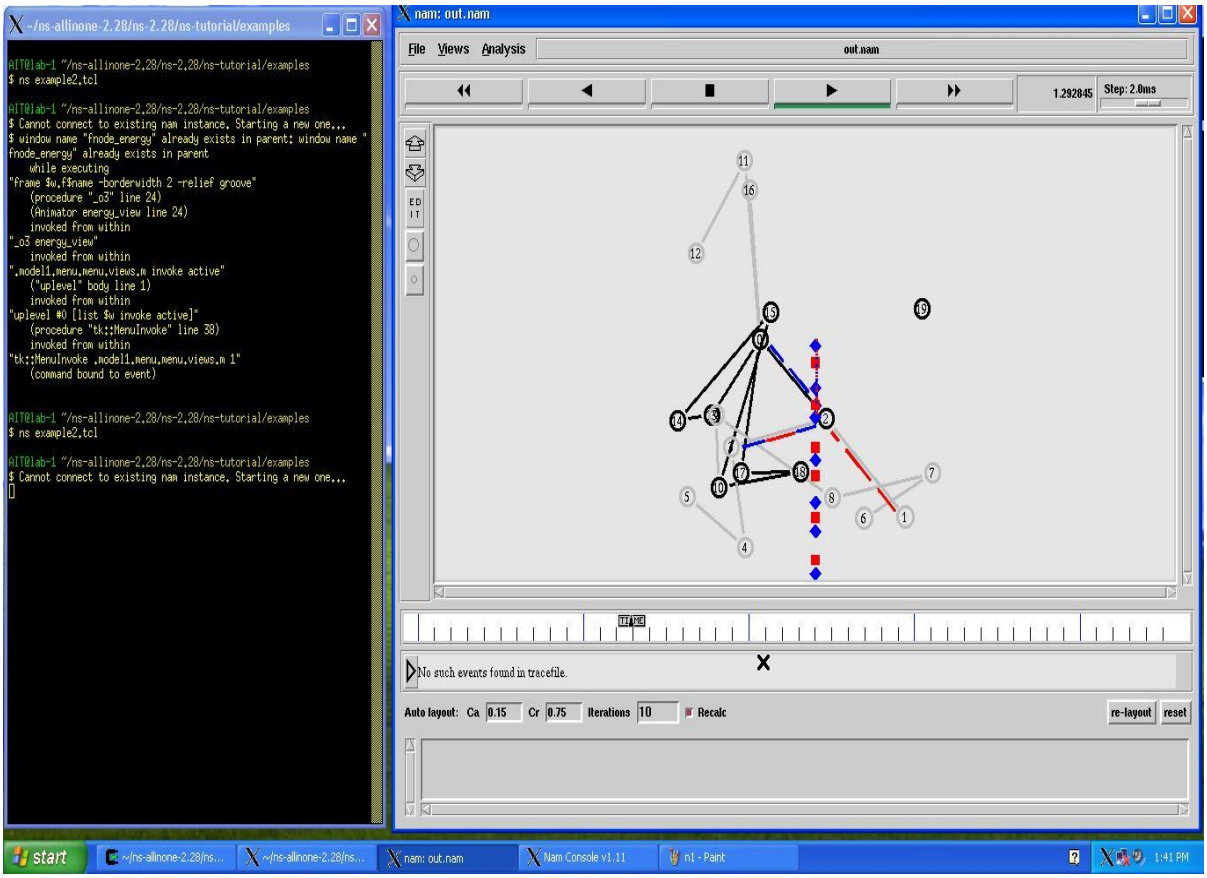

Fig. 11. Snapshot 2 for ns2 simulation for an arbitrary MANET

Fig. 10 and Fig. 11 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. 11 reflects a synchronisation point at Node 2.

V. CONCLUSION

Experimental result analysis reflects that presence of Black hole nodes in MANET affects communication in MANET. Proposed CA based system is dynamic in nature, which is a basic advantage of CA. 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. The cost efficiency for implanting this approach is also facilitating the choice for using CA for Black Hole detection in MANET.

ACKNOWLEDGMENT

Our thanks to IEEE for allowing us to modify template they have developed.

REFERENCES

[1] Ad-hoc Network; *http://en.wikipedia.org/wiki/Wireless_ad-hoc_network*
[2] MANET; *http://*en.wikipedia.org/wiki/Mobile_ad_hoc_network
[3] Lecture Notes on DSDV; *www.cs.sunysb.edu/~jgao/CSE370-spring06/lecture10.pdf*
[4] Lecture Notes on DSR; *www.monarch.cs.rice.edu/monarch-papers/dsr-chapter00.pdf*
[5] Lecture Notes on AODV; *www.moment.cs.ucsb.edu/pub/wwan_chakeres_i.pdf*
[6] Lecture Notes on MANET communication; www.cnd.iit.cnr.it/andrea/docs/chap_rman06_p2p.pdf
[7] 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] S. Wolfram; A *New Kind of Science.* Champaign, IL: Wolfram Media; 2002
[9] S. Wolfram; *Theory and Application of Cellular Automata;* Reading, MA: Addison-Wesley;1986
[10] 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
[11] Elmar Gerhards et al.; *Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs*; 32nd IEEE Conference on Local Computer Networks; 2007
[12] XiaoYang Zhang ; *Proposal of a method to detect black hole attack in MANET*; This paper appears in: Autonomous Decentralized Systems (ISADS '09) ; 2009
[13] Akanksha Saini et al.; *Comparison Between Various Black Hole Detection*; National Conference on Computational Instrumentation (NCCI); 2010
[14] 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
[15] 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
[16] Sanjay Ramaswamy et al.; *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*; Int'l Conf. on Wireless Networks; 2003
[17] 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
[18] Penina Orenstein et al.; *Modeling A Wireless Ad-Hoc Network Using A Cellular-Automaton Approach*; International Journal of Simulation Systems, Science & Technology (IJSSST), Vol. 10, No. 1; 2009

