International Journal For Technological Research In Engineering
Volume 4, Issue 12, August-2017 *ISSN (Online): 2347 - 4718*

A NOVAL TECHNIQUE TO ANALYSIS THE MITIGATION OF BLACK HOLE NODE FOR RAPID ENERGY DISSIPATION IN WSN

Kundan Pandit[1], Prof. Anas Iqbal[2]
[1]M.Tech. (Digital Communication), [2]Dapartment Of Electronics And Communication Engineering,
All Saints' College Of Technology, Bhopal (M.P)

ABSTRACT: Mobile ad hoc network faces various security challenges due to its nature. Hence, more packet delivery ratio is achieved. This approach identifies and avoids black hole node in the path discovery phase and hence path chosen by the source node will be secured for data transmission. This approach also has a high point that it does not depend upon the relationship between the nodes. The simulation is carried out in MATLAB thus, we have a tendency to evaluate that our algorithmic rule shows higher routing performance than associate existing approach in terms of finish to finish delay. Security in WSN may be a terribly huge space of research; we've simply touched the surface of this field. In our algorithmic rule, we've managed to mitigate solely packet dropping attack. This algorithmic rule will be additional expanded to mitigate additional alternative attacks. Thus, we have a tendency to evaluated that our algorithmic rule shows higher routing performance than associate existing approach in terms of finish to finish delay. Security in WSN may be a terribly huge space of research; we've simply touched the surface of this field. In our algorithmic rule, we've managed to mitigate solely packet dropping attack. This algorithm can be further expanded to mitigate more other attacks. After completion of simulation approx 3000 rounds of communication energy level of node is been observed. During the attack of black hole the rapid downfall of network energy is being observed. But with proposed EODV algorithm it has find out and removed from the network and ultimately improve the network life. The sort out of the black hole node is another typical work with can also be performed during the proposed work execution which counts energy.

Key Word: Black Hole, WANET, WSN, AODV, MATLAB, EODV

I. INTRODUCTION

Wireless communication has many problems over the wired networks. Wireless Ad-hoc Network (WANET) has gained lot of popularity over wired networks due to their unique characteristics. The word adhoc has Latin roots and means temporary. WANET is a particular network for a particular application. WANET requires no fixed infrastructure for its working. Network devices (nodes) are mobile and communicate over a wireless medium. Also, there is no central controlling authority that manages the network. The participating nodes do network management and routing of data. The participating nodes of the network have limited resources. This difference from the wired network, WANET faces various challenges such as battery constraints, dynamic topology, and bandwidth constraints [1].Wireless network faces various security challenges due to its nature. A lot of vulnerabilities arise due to no central authority and wireless medium of transmission. Route establishment and data transmission are two important functions of routing algorithm in WANET. These two phases need to be secured from attackers. The routing technique must be so flexible that it can work with various attacks. Hence, good communication implies secure routing algorithm.In this thesis work, we consider energy based securing route management phase of the routing protocol to mitigate a particular type of malicious attack called as Black Hole Attack [2]. In this attack a malicious node forces to route the data traffic through it by not following the actual algorithm and then drops the data packets without forwarding them to the destination node. This attack will result in denial of service to the destination node. Before transmitting the data, we make sure that data packets won't be routed via a malicious node. This technique has a better packet delivery ratio when under attack than the original routing technique.

II. PROBLEM STATEMENTS

It is hard to find the method of rapid fall in energy in WSN. Which problem is occurring due for reason for this occurred situation? Since the sensor nodes are battery-powered and are expected to operate without attendance for a relatively long time. But in most cases it is difficult and even impossible to change or recharge batteries for the sensor nodes. Therefore the network lifetime is depends on the life of sensor node battery which makes effective data routing as an especially challenging task in WSNs. This is due to fact that the size of a sensor node is expected to be small and this leads to constraints on size of its components i.e. battery size, processors, data storing memory, all are needed to be small. So any optimization in these networks should focus on optimizing energy consumption in the network. Occurring of malicious node may do have the cause for rapid energy fall. So most research work in finding the energy analysis of this fall due to malicious nodes.

III. LITERATURE SURVEY

[1] Md. Zair Hussain1, M. P. Singh2 and R. K. Singh3 1Maulana Azad faculty of Engg. & Tech., Patna, India projected the routing protocols take issue on the premise of application and spec. With awareness could be a mandatory style criterion, several new protocols are specifically designed for routing, power management and information dissemination. Economical routing during a sensing element network needs that routing protocol should minimize

network energy dissipation and maximize network period.[2] Aswini Kavarthapu Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India. Narasimha Rao Sirivella proposed a method faulty sensor node is detected by discrete path selection technique by compare the actual RTT with present RTT. This method is simulated in NS2 on WSNs with eight sensor nodes designed using circular topology.[3] Abderahmane Baadache et. al. have steered AN approach that uses acknowledgments to evidence and to properly forward packets on the trail. During this technique, every packet receiving node sends a reply to the sender node to mark the eminent reception of the message. The communication is attested victimization hash values. This approach is incredibly computation intensive. Every node on the trail needs to recomputed the hash worth and check. Also, there's communication overhead because of lack being sent by every node on the route.[4] Anuj Rai suggest that the wsn has the routing algorithm that has capable to form a of detection a region node within The methodology involves causing a entice route request message, before causing associate actual route request. Sender's of all the reply messages square measure blacklisted as malicious nodes. This approach introduces a major quantity of delay, and it doesn't address the co-operative region under the region attack. [5] Nabarun Chatterjee et. al. recommended a technique involving cryptography toavoid region node throughout the trail setup section. Sender node sends some plain text to the destination node with the route request message, and the destination node sends the encrypted text with the reply message. This methodology permits solely destination node to reply to route request [6] S. Sankara et. al. have used the hash-based technique to avoid part attack. every node encompasses a distinctive Id that it uses whereas causing back the reply. The response message is hashed, and the hash worth is saved within the message to make sure that reply reached tamper unengaged to the supply node. supply node collects all the response messages for a amount, and therefore the then correct route is known. [7] Anand Aware et. al. planned to discard the primary reply to achieve sender node, and realize the second optimum reply message to hold out the info transmission. This technique fails if the network size is giant.[8] Debarati Roy Choudhury et. al. have given associate degree approach that prevents any alteration of the traditional behavior of the AODV protocol. The supply node maintains 2 tables, one to store the received replies and different to avoid wasting the malicious node's data. [9] Satoshi movie maker et. al. has given another approach to avoid part attack. During this approach, a threshold price of the valid sequence variety is calculated exploitation feature vector. The mean price for the feature vector is calculated at every mounted measure

IV. PROPOSED METHODOLOGY

This Dissertation investigates the WSN scenario and the working behaviours of from MATLAB and rapid energy fall due to unwanted node like black hole. For this research it needs to implement 50 nodes in the area of WSN. This research has been focused on adhoc communication network so it will work for WSN. Simulation provides the two stages containing one is simple work and other is the black hole node.

4.1 Simulation Parameter and Removal Technique of Black hole

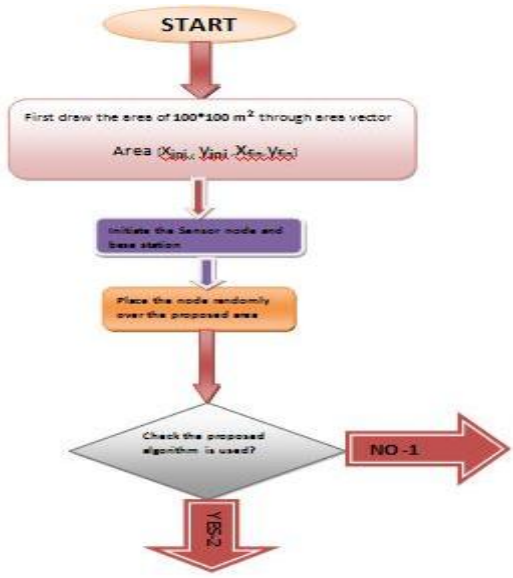
Table 4.1: Important Proposed parameter

Parameter	Value
Area	1000*1000 CM2
Number of Nodes	50
Initial Network Energy	1J
Simulation Round	3000 equivalent to
Transmission Rate	Efs=10*10^(-12); Emp=0.0013*10^(-12)
Data Aggregation Energy	EDA=5*10^(-9)
Mobility Model	Random Way-point
Probability of converting Black hole node	Automatic

It has not a clear that how much black hole node is being converted from the ordinary node. It is totally dependent on the automatization of proposed work that how much number of black hole nodes formed during or before the simulation formed. It is just for attending the actual scenario so that in real situation can be bitterly analyzed.

4.2 Work flow of proposed work

Step1: First take a MATLAB 2010b.
Step2: go the command prompt.
Step3: type guide.
Step4: use default GUI.
Step 5: drag and drop two buttons.
Step6: one is for basic and other is for proposed.
Step 7: name both button from property inspector.
Step8: the right clicks the button again.
Step 9: the go to call back and press the basic code which is discussed below.
Step 10: similarly same process will be follow for other but for proposed work.



Case 1-No
No result will come out because no any energy count technique has been executed.
Case 2-Yes

- First assigning the energy of each node
- Make one node as base station who behaviors take as a sink like behaviors.
- This node is for the data aggression of all nodes and broadcast and assigning the task that will for each round.
- As the communication round increase the energy being decrease because the each round need some energy for send transmission and reception of signals.
- A malicious node has been introduced which has very similar behavior like base station.
- It will raise more communication to rest of nodes.
- It has sink the essential data and force the node to more communication so the energy become rapidly finish.
- The count the energy of each nodes and the sum of total node as per the round increases.
- Due to malicious node called black hole it is quite easy to detect the energy used differentiation in present case or without black hole.
- At the end of simulation it has been come out figure of approx 3000 round.

V. SIMULATION RESULT

This result comes out after the proposed work code executed in MATLAB. Which is designed through guide mechanism provided in MATLAB and makes it a GUI that contains two buttons and having one has the simple work not having algorithm and other has executed to proposed algorithm.

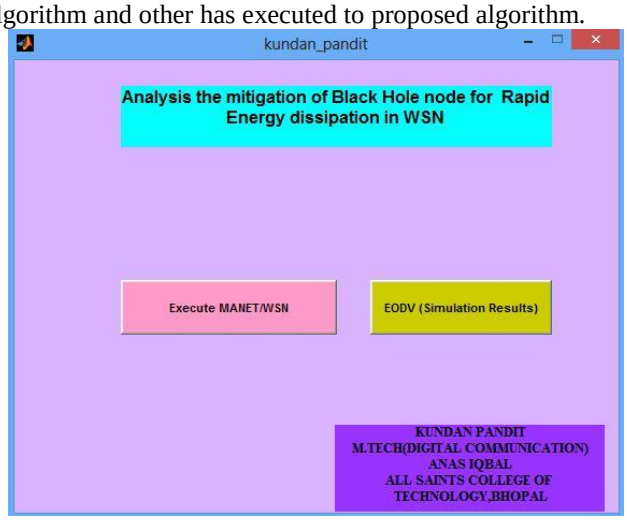


Fig 5.1: Basic layout of proposed GUI designed in MATLAB 2010

This is the first layout that has been created in MATLAB 2010.It has two button created on front layout, one has the simple WSN contains that is showing basic showing the node placement. Other is the proposed work button based on energy dissipation of WSN.

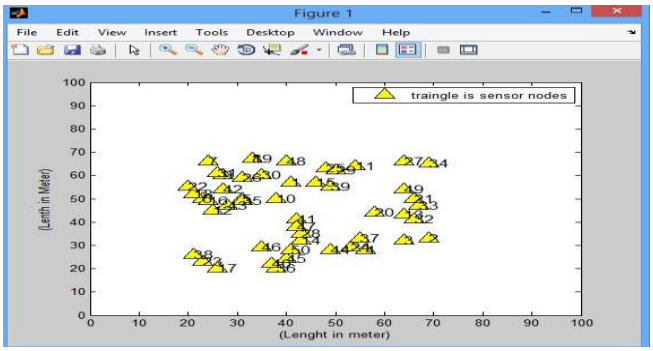


Fig 5.2: Executing the 50- black hole nodes in proposed area

This layout come after the pressing the first button. Here the triangle is the node of WSN and it is 50 in number within the proposed area 150*150.It can be varies as our requirements. This implementation just shows that how the communication node inserted by placing the node in random manners.

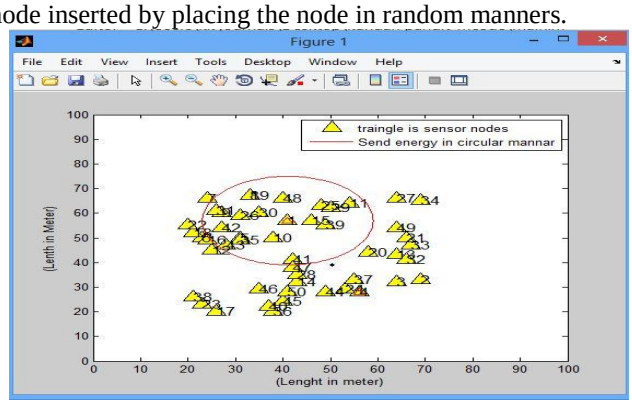


Fig 5.3: Figure shows the nodes transmitting the energy for communication

As we see in above figure nodes transmission signal as shown in circle. This is the wave that has some range in distance measure. As the distance increases the energy goes down radically. So it is required to take small energy dissipation during the one round of communication. With the minimum energy dissipation we found more longevity of network. But for reception side it has to be reaching the single with minimal loss of packets. So same time it is quite necessary to do take both conditions. Means it has to minimize the energy for one round considering the need to reach the base station via nodes.

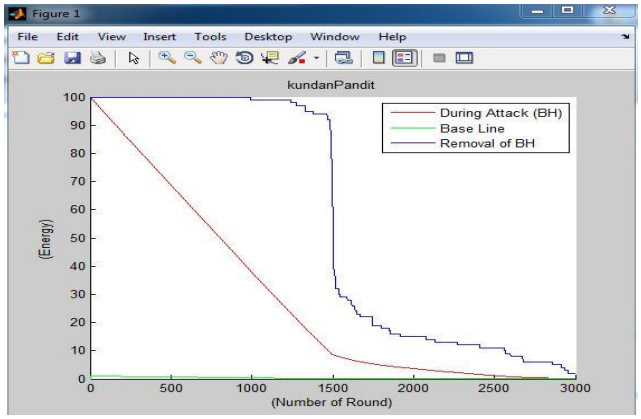


Fig 5.4: This figure comes out after executing the MANET to 2000 rounds.

Figure 5.4 shows the three lines, one of the green line is base line represent the energy base second line in dark pink represent the energy of network during the attack of black hole which is reasonably depicted and merge so quickly to base line. Third line the proposed work of which eliminated the black hole nodes form the WSN that is as per the communication need the level of energy goes down.

5.1 Comparison Table

	Existing Parameters	Proposed Parameters
Simulation Type	NS2	MATLAB
Area	1000*1000	100*100
Node	50	50
Energy in Joule	50J	1J
Energy Model	Battery	Battery
Channel type	Wireless Channel	Wireless Channel
Simulation Time	45 Sec	1.18 min

5.2 Result Comparison (1 round =0.03933 sec)

Time in sec	Energy (Existing Technique)	Energy(Proposed Technique)
0	50	1
10	44	1
20	39	1
30	35	1
40	30	1
50	25	0.99
60	20	0.90
70	15	0.23
80	10	0.08
90	05	0.06
100	Dead	0.04
110	Dead	Contd.

VI. CONCLUSION & FUTURE

This approach additionally incorporates division that it doesn't rely on the link between the nodes. Thus, although a trusty node turns into a malicious node then additionally our approach will stop the attack from happening. In projected algorithmic program, we've got required to mitigate solely packet dropping attack known as the rapacious activity. This algorithmic program may be any expanded to mitigate a lot of different attacks. Result above in comparison found that the proposed work using EODV find better choice for finding the black hole node. In Future it may be simple to deploy the node while not the previous intimation of malicious black hole nodes. Therefore it will deploy military use and any secret activities that ought to be high security demands.

REFERENCE

[1] Md. Zair Hussain1, M. P. Singh2 and R. K. Singh3 1Maulana Azad College of Engg. & Tech., Patna, India 2National Institute of Technology Patna, India 3Muzaffarpur Institute of Technology, Muzaffarpur, India "Analysis of Lifetime of Wireless Sensor Network" International Journal of Advanced Science and Technology Vol. 53, April, 2013.

[2] Aswini Kavarthapu Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India. Narasimha Rao Sirivella "A Failure Node Detection based on Discrete Selection in WSNs": International Journal of Computer Applications (0975 – 8887) Volume 106 – No. 15, November 2014.

[3] Abderrahmane Baadache and Ali Belmehdi. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 73:173–184, 2014.

[4] Anuj Rai, Rajeev Patel, RK Kapoor, and DS Karaulia. Enhancement in security of aodv protocol against black-hole attack in manet. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 91. ACM, 2014.

[5] Nabarun Chatterjee and Jyotsna Kumar Mandal. Detection of blackhole behaviour using triangular encryption in ns2. Procedia Technology, 10:524–529, 2013.

[6] S Sankara Narayanan and S Radhakrishnan. Secure aodv to combat black hole attack in manet. In Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, pages 447–452. IEEE, 2013.

[7] Anand A Aware and Kiran Bhandari. Prevention of black hole attack on aodv in manet using hash function. In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on, pages 1–6. IEEE, 2014.

[8] Debarati Roy Choudhury, Leena Ragha, and Nilesh Marathe. Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack. Procedia Computer Science, 45:564–570, 2015.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. IJ Network Security, 5(3):338–346, 2007.

[10] W. Ye, J. Heidemann and D. Estrin, An energy-efficient MAC protocol for wireless sensor networks, in: IEEE INFOCOM (2002) pp. 1567–1576.

[11] Pavithra B Raj1, R Srinivasan2 PG Student, Department of Computer Science & Engineering, M.S.Ramaiah Institute of Technology, Bangalore "Fault Node Identification and Route Recovery in Distributed Sensor Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014.

[12] Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki. Diagnosing mobile ad-hoc networks: two distributed comparison-based self-diagnosis protocols. In Proceedings of the 4th ACM international workshop on Mobility management and wireless access, pages 18–27. ACM, 2006.

[13] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks: Applications and challenges. Journal-Communications Network, 3(3):60–66, 2004.

