RESEARCHERID
THOMSON REUTERS

[Islam, 6(5): May 2019]
DOI- 10.5281/zenodo.2949949

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES
EXTENDS LIFE TO THE MOBILE AD-HOC NETWORK BY DETECTING MALICIOUS NODES AND REDUCING ENERGY CONSUMPTION USING ROUTING PROTOCOL

Md Minhajul Islam[*1] & Dr. Ravindra Kumar Gupta[2]

[*1]Student, Dept. of Computer Science Engineering, SRK University Bhopal, Madhya Pradesh, India
[2]Asst. Professor, Dept. of Computer Science Engineering, SRK University Bhopal, Madhya Pradesh, India

ABSTRACT

The incidence of malicious nodes in an ad-hoc network worsens the performance of the network. A novel approach to detect increasing intrusion of malicious nodes is proposed to protect against attack on MANET vector route protocol. These malicious nodes can reduce overall data access in the network, with the increase in query delays. However some nodes can only decide to support partially or not at all with other nodes. Those mobile nodes that take their own packets but do not send neighbors to packets are known as the unfaithfully nodes. This type of malicious nodes can reduce overall data access in the network. Due to this kind of problem, the overall process of MANET was affected.

The proposed approach employs a technique for determining the conditions less than which the first stage is based on the *secure malicious nodes detecting method (SMND)* to the network and the second step is based on the smallest route to *reducing energy consumption using AODV (REC-AODV).*

In accumulation to identifying malicious nodes, it have been experiential that in this approach, ad- hoc routing has less security and less communication breaks. MANET has many issues that attract researchers to work in these areas. Experimental outcome show that the proposed methodology is to successfully detect malicious nodes, and with the help of routing protocol, the shortest route reduces the energy consumption of the packets in the network, which will be for long life in the network. By keeping these parameters in mind we calculate the packet delivery ratio, throughput, energy usage, congestion control and routing overhead.

Keyword: *SDMN, AODV, Reducing Energy Consumption, Routing, Packets Delivery ratio, Congestion Control & MANETs.*

I. INTRODUCTION

MANET is a collection of wireless mobile node framing a transitory system without the guide of any stand-alone infrastructure or centralized organization [1]. MANET are self-sorting out and self-designing multi-host remote systems, where the structure of the framework changes capably. This is generally a direct result of the compactness of the node. Node in these systems uses a comparable discretionary access remote channel, organizing in an enticing method to associating with them in multi-host sending. The system switches nodes in the form of host and router as well, which every node kept the routing information of various nodes in the system. [3].

In mobile ad-hoc networks where framework is not supported in the case of remote systems, and since the circular transmission of circular node parcel may be outside the scope of the node; A directive method is constantly invented to further the packets between sources and targets. Inside the cell, the base station can achieve every single versatile node without steering via communication like every kind of remote system. Due to specially designated systems, each node should probably advance information for different nodes. It creates additional issues with dynamic topology issues, which have unexpected connectivity changes [4].

[Islam, 6(5): May 2019]
DOI- 10.5281/zenodo.2949949
ISSN 2348 – 8034
Impact Factor- 5.070

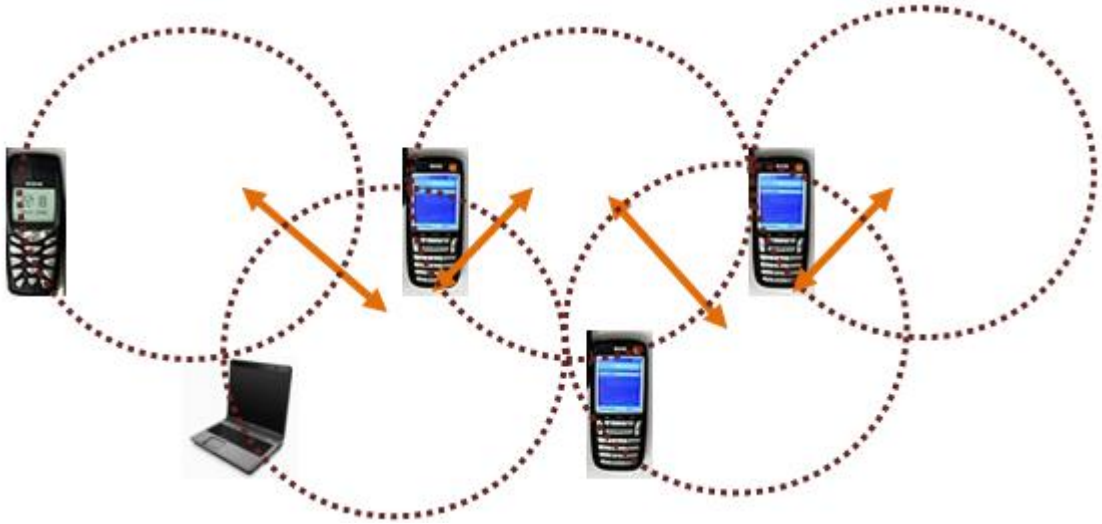

Figure 1:- Ad hoc Network

II. PROBLEM STATEMENT

Our challenge is to find the shortest route for MANET, reduce energy efficiency and detect malicious nodes, in which the mobile nodes of non-responsive-based environments are not included.

The Mobile Ed-Hawk network has attracted much interest due to the recognition of cell devices and the advancement of wireless communication technologies. A MANET is a peer-to-peer multi-hop cell Wi-Fi network that has neither a hard and fast infrastructure nor an important server. Each node in MANET acts as a router and shares packets with each fraction. Many types of MANET applications have been developed. In the field of MANET, there are several research zones that can focus large-scale focus together with the network's overall performance, reliability, Proposed detect malicious node and congestion control.
In addition in our MANET, to develop a simulation to deal with other challenges, the following challenge has been included:

i. **Firstly:** how to increase the network life availability of data by reduces energy consumption?
ii. **Secondly:** how to improve the data security by malicious node detection?
iii. **Finally:** how improver packet losses by network congestion control?

III. DETECTING MALICIOUS NODE

A node is defined as a malicious node which is refusing to provide services and data to other nodes in the network. And the node that modifies the data during or after the Trust Detection Transmission in MNET is known as the malicious node.

Security in the mobile ad-hoc network is that the most important aspect of the network's fundamental practicality is Mobile Ed Hawk Networks (MANET) are wireless networks that feature dynamic topology and do not have any mounted infrastructure. Finding the security of the responsive neighbour node can be a requirement.

Current mobile ad hoc networks allow for many different types of attacks. Although the wired network also executes similar tasks, it is easy to fix the infrastructure in such a network. Current MANETs are basically unsafe for two different types of attacks: active attacks and passive attacks. An attack on the node is to attack the danger to attack. On the other hand, passive attacks are mainly due to the lack of support for the purpose of energy saving. The attacks have been classified as modification, cloning, construction, work-hole and lack of cooperation.

Within the routing protocol known as "**Quality of Service Good Neighbourhood Node Detection Algorithms" (QOS-GNDA),** the purpose of complete disruption of the service attack routing function and therefore the full operation of the ad hoc network. Typical examples of denial of service attacks include overlapping routing tables and lack of sleep. The malicious node attacks on the routing table overflow so that the network can be filled with fake routing construction packets to consume resources of the participant node and disrupt the establishment of legitimate routes. The purpose of sleeping increment is to maintain specific node battery consumption in continuous routing decisions [5].

MANETs name as **Improved Good Neighbourhood Node Detection Algorithms (IGNDA)** to reduce the information. In the estimated system, we have a tendency to find reliable neighbour nodes such as secure information transmission only at the time of link installation. Different parameters like Transmissions are different, the power of the node, the power of the signal, the ability of the node for higher information, the position of the node square measure is used to find equally higher information measurement packet forwarding and reliable neighbour node is. These parameters provide the flexibility to reduce the delay and reduce the packet dropping magnitude connection. This extra removes the setting in the network and improves the performance of the routing protocol and thus improves the performance of the network.

Regardless of all these leads, MANET is susceptible to security ultimatum, energy deficiency and encroachment by malicious nodes. Camouflage malicious nodes in sensor networks can badly distort the normal functioning of wireless sensor networks. Once the malicious nodes start attack, it is difficult to identify the incisions. If the network presents malicious nodes and if it makes an entry in the routing path, then it causes security threat to sensitive information. This approach tries to avoid packet packets and avoid packet tempering attacks.

Proposed algorithm Steps to secure detect malicious node (SDMN) for communication
Step 1: N_T- Total number of nodes in the network

Step 2: $N_1, N_2, N_3, \ldots\ldots\ldots\ldots N_r$, Initialize of the network

Step 3: Broadcast "Hello" in packet message across the network.

Step 4: Sender node is ready to broadcast routing packet and establish the route**.**

Step 5: Destination node received the request from source node.

Step 6: Compute remains energy E_i after opening irregular data transmission and faithfull node value Y through the Acknowledgement got amid information transmission utilizing AODV.

Step 7: The node with similarly high faithfully node values and residue energy are elected are chosen as the provisional essential sender head node and its neighbors are chosen as bunch part to shape a set.

Step 8: The probably chosen sender node communicates the message (hello_msg) to its neighbor node to node member.

Step 9: Determine time= T, of success Hello message

Step 10 : If (existing time < T) then
If (Hello message is overhear from the tentatively Selected Node NT[i]) then
While (during broadcasting of Hello message by tentative selected nodes) do
selected Node NT[i] is secured primary.

Step 11: Compare $NT_{[i]}$ and T

ISSN 2348 – 8034
Impact Factor- 5.070

Step 12: if ($NT_{[i]}$>T) then increase the NT[i] and go to step: 10

Step 13: else go to step 11

Step 14: determine faithfully node using signal quality

Step 15: If signal quality > = Threshold after that go to step: 14

Step 16: else it is a feeble signal so go to step: 14

Step 17: Calculate stream limit

Step 18: If stream limit is equivalent to CBC at that point store node address (Good node)

Step 19: else Bad node Source node keeps up way boycott.

Step 20: Send RREQ through great node

Step 21: Source node begins the course revelation process if any way coordinates that way boycott and incorporates nodes from node boycott than source node disposes of the course.

Step 22: If the way is alright at that point source node begins sending packets to the goal node.

Parameter in AODV

In this situation a few parameters with a particular esteem are considered. Those are as appeared in table 4.3.

Table 1: Parameter 1 for implementation of AODV

Parameter	**Value**
Number of nodes	40
Range Size	800x600
Communication range/radios (m)	10 to 30
Simulation Time	100 sec
Pause Time	5ms
Transmission Range	250 m
Traffic Size	CBR (Constant Bit Rate)
Packet Size	512 bytes
malicious node %	0 to 100
The velocity of a node (Maximum) m/s	1
Routing Protocol	AODV

[Islam, 6(5): May 2019]
DOI- 10.5281/zenodo.2949949
ISSN 2348 – 8034
Impact Factor- 5.070

IV. RESULT & DISCUSSION

Packet delivery ratio

It very well may be characterized as the proportion of number of packets effectively conveyed to goal to the quantity of parcels transmitted by source node.

PDR= (Total number of packets effectively received)/(Total number of packets send)

Table 2: Packet Delivery Ratio (%)

Number of nodes	Packet delivery ratio (%)		
	With malicious node	Without malicious node	Proposed model
10	80.2	85.6	88.9
20	71.6	75.9	81.6
30	65.2	69.5	74.2
40	72.5	75.6	80.1

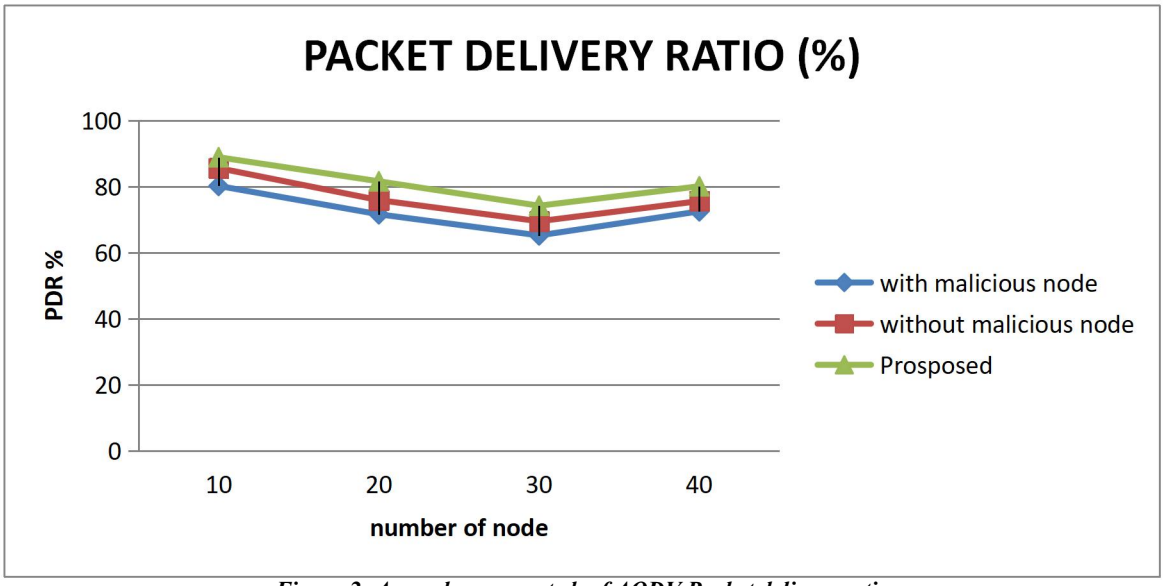

Figure 2: A graph represented of AODV Packet delivery ratio

ISSN 2348 – 8034
Impact Factor- 5.070

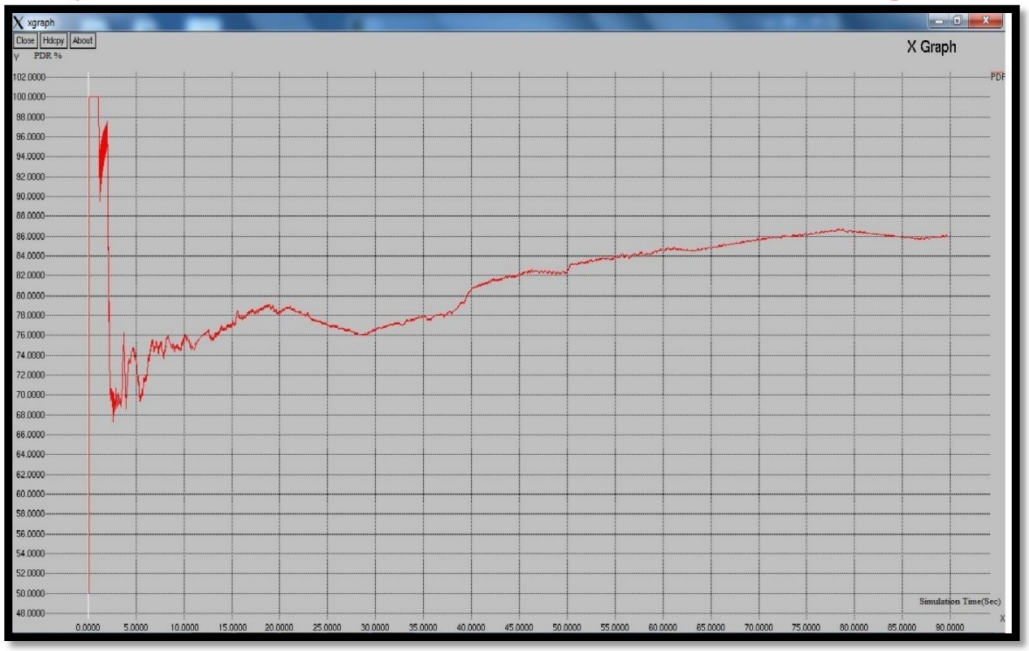

Figure 3: A Screenshot of AODV Packet delivery ratio vs. Simulation time

1.1. AVERAGE END TO END DELAY-

Average End to End Delay the normal time taken by bundles to reach starting with one end then onto the next end (Source to Destination). This postponement incorporates preparing and lining delay in each middle of the road hub. Lesser start to finish defer demonstrates better performance of the networks.

Table 3:- Average End to End Delay

Number of Nodes	Avg End to End delay (Sec)	
	with malicious node	without malicious node
10	10.52	8.25
20	11.2	9.5
30	9.85	8.8
40	9.4	7.48

ISSN 2348 – 8034
Impact Factor- 5.070

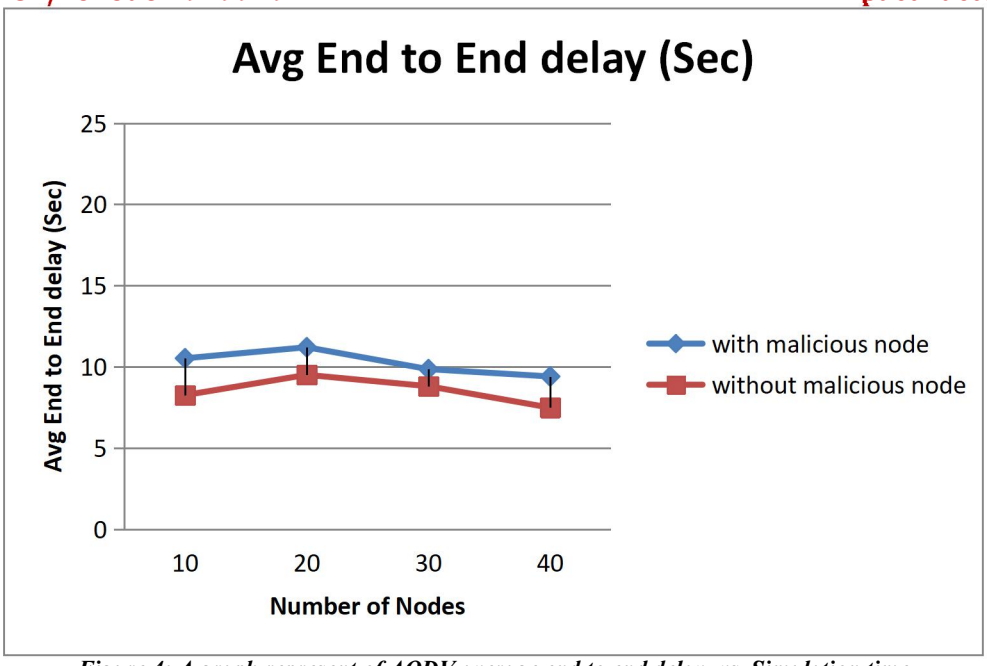

Figure 4: A graph represent of AODV average end to end delay- vs. Simulation time

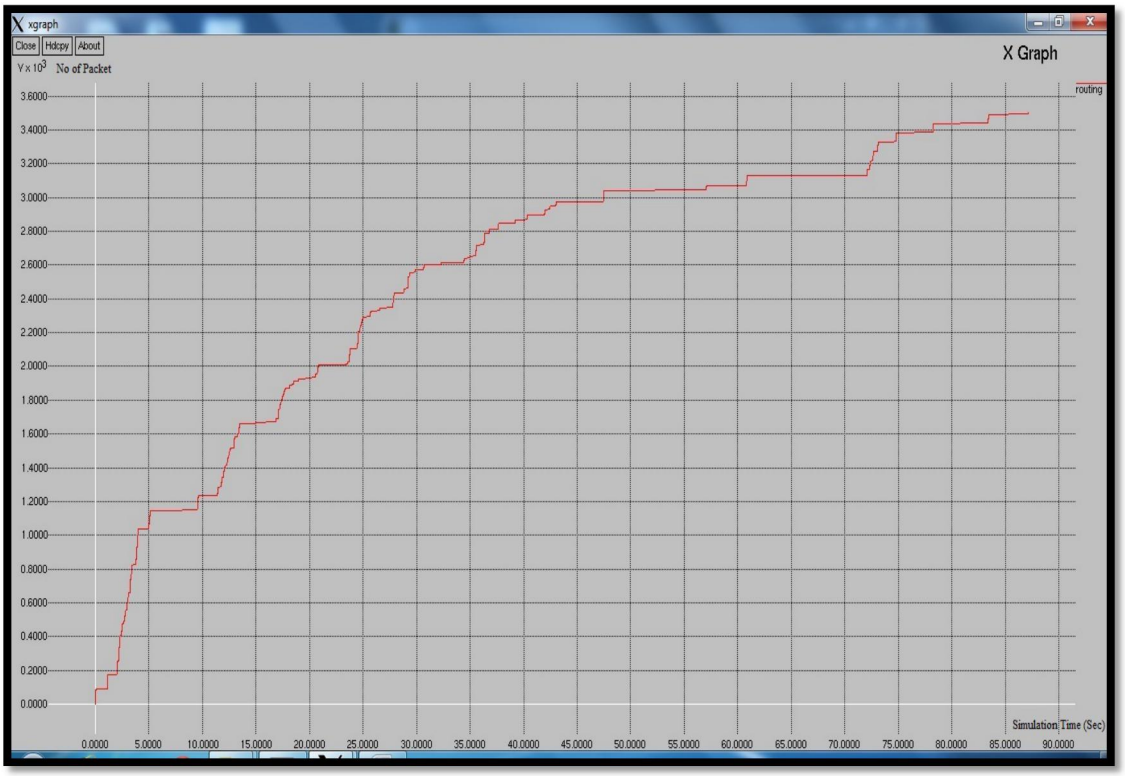

Figure 5: A Screenshot of AODV average end to end delay- vs. Simulation time

ISSN 2348 – 8034
Impact Factor- 5.070

V. CONCLUSION

In this paper, the malicious behavior of the node has been discussed and the security solution has been defined to prevent such behavior. The purpose of this research is to deny the service and data attack which can be caused by malicious nodes by making buffer overflow and malicious bandwidth and make MANET more secure. This letter concludes that with the onset of any attack in any network there is a lack of throughput in the network. Packet delivery ratio also falls and increases in checksum errors and packet loss ratio.

SMND techniques have been proposed to identify the malicious nodes that make packet drops during transmission. In this proposed research, behavioral analysis techniques are proposed to identify malicious nodes. This is a highly effective packet drop detection technique. The possibility of detecting malicious nodes in future work will improve. Due to this, the output parameters such as throughput, packet distribution ratio and the duration of the delay will improve.

REFERENCE

1. *Eiji Nii, Takamasa Kitanouma, "Cooperative Detection for Falsification and Isolation of Malicious Nodes for Wireless Sensor Networks in Open Environment", IEEE proceeding of 2017 Asia pacific microwave conference.*
2. *Zhang y., Lee W.: 'intrusion detection in wireless ad hoc networks'. Proc. Sixth acm int. Conf. On mobile computing and networking (mobicom'00), 2000, pp. 275–283*
3. *KACHIRISKI O., GUHA R.: 'intrusion detection system using mobile agents in wireless ad hoc networks'. Ieee workshop on knowledge media networking (kmn'02), 2002, pp. 153–158*
4. *WYSOCKI B.J., DADEJ A.: 'advanced wired and wireless networks' (springer, 2004, vol. Ix), p. 270,*
5. *HU, Y. , PERRIG, A. , JOHNSON, D.: 'ariadne: a secure on demand routing protocol for wireless ad hoc networks, acm mobicom, september 2002*
6. *MARTI S., GIULI T., LAI K., BAKER M.: 'mitigating routing misbehavior in mobile ad hoc networks', acm mobicom, august, 2000.*
7. *C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TROUVE: A trusted routing protocol for urban vehicular environments," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, 2015, pp. 260–267.*
8. *C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," Tech. Rep., 2003.*
9. *DENG H., LI W., AGRAWAL D.P.: 'routing security wireless ad hoc networks', ieee commun. Mag., 2002, pp. 70–75*
10. *PATCHA A., MISHRA A.: 'collaborative security architecture for black hole attack prevention in mobile ad hoc networks'. 2003, doi: 10.1109/rawcon.2003.1227896*
11. *YAU P.-H., MITCHELL C.J.: 'reputation methods for routing security for mobile ad hoc networks'. 2003, doi: 10.1109/ tic.2003.1249106*
12. *RAZA I., HUSSAIN S.A.: 'identification of malicious nodes in an aodv pure ad hoc network through guard nodes', acm comput. Commun., 2008, 31, (9), pp. 1796–1802*
13. *MEHFUZ S., DOJA M.N.: 'swarm intelligent power-aware detection of unauthorized and compromised nodes in mantes', j. Artif. Evol. Appl., 2008, 2008, article id 236803. P. 16. Doi:10.1155/2008/236803.*