International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-02, May 2018

Detection and Prevention of Malicious Nodes Using Tree Based Method in Mobile Ad Hoc Network

Shilpa Vijay, M.Tech Student, NITM, Gwalior & India, shilpavijay12@gmail.com
Abhishek Dubey, Assistant Professor, NITM, Gwalior & India, abhishek2be1989@gmail.com

Abstract: **A Mobile Ad-Hoc Network (MANET) is a foundation significantly less or a self-designed aggregating of mobile nodes that can aimlessly control their geographic places such that those networks have dynamic topologies and random mobility with restricted assets. It commonly works by broadcasting the statistics. Its nature is broadcasting so there's a threat to disrupt community via attacker. The variety of attack can be performed in MANET. Wormhole attack is one of the active internal attacks in which or extra attacker nodes tunnel the traffic from one place to some other territory inside the network. Every hub in the system goes about as a number notwithstanding a switch and, advances movement to different nodes. In previous work, they used additional storage for each route response packet to identify the malicious node. This computation requires calculation of the energy of each node and unstable routes which increase routing overhead. This method is very time consuming and it is not possible to store the details of each node is difficult. For discovering wormhole attacker in MANET, we proposed tree-based method to distinguish and avoid an attacker. Construct a tree of network in which source node behaves as a root node and other neighboring nodes are as children. When source send data to destination it search for the paths which should be shortest path. We consider that malicious node always reply first for the shortest path to traverse all the traffic towards itself. By the proposed work, it can be illustrated that the performance of the network improved in the form of various parameters.**

Keywords —MANET, Wireless Technology, Wormhole Attack, Hub, Ad Hoc network, Energy, Route and Malicious Node

I. INTRODUCTION

Wireless technologies for example, Bluetooth or the 802.11 benchmarks empower mobile devices to build up a Mobile Ad-hoc Network (MANET) by interfacing progressively through the wireless medium with no incorporated structure [1]. MANETs offer a few favorable circumstances over customary systems including diminished framework costs, simplicity of foundation and adaptation to internal failure, as directing is performed independently by hubs utilizing other moderate system hubs to forward bundles, these multi-jumping decreases the shot of bottlenecks, however the key MANET fascination is more noteworthy versatility contrasted and wired arrangements [2].

There are various issues which influence the unwavering quality of Ad-hoc systems and cutoff their reasonability for various situations; absence of concentrated structure inside MANET requires that every individual node must go about as a switch and is in charge of performing packet routing tasks; this is finished utilizing at least one basic routing protocols over the MANET. Performing directing errands requires memory and calculation control, however cell phones include physical size and weight impediments basic for their mobility, this lessens the accessible memory and computational assets and additionally restricting battery control [3]. MANETs containing more nodes require more noteworthy preparing force, memory and data transfer capacity to keep up exact routing data; this brings traffic overhead into the system as nodes convey steering data, this thusly utilizes more battery control [4].

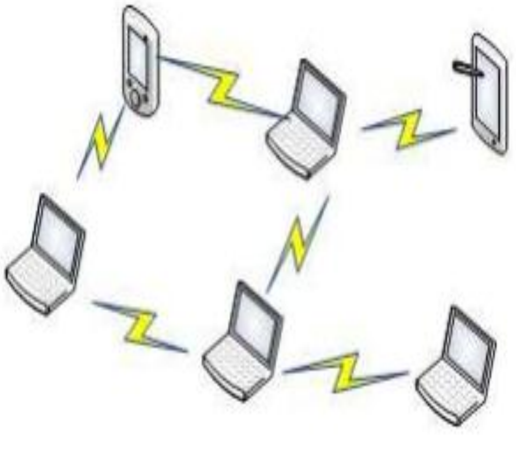

Fig 1. Ad-Hoc Wireless Networks

II. WORMHOLE ATTACK

A Wormhole Attack is the most serious among the security dangers in the MANET since it doesn't abuse any hub of the system. It has the most obliterating sway on the system as it stops the general execution of the system by diminishing the throughput by dropping the packets. In Wormhole Attack nodes mask themselves the as the most brief course in the system than the first directing way. This prompts false origination with respect to the routing ways that are to be chosen in view of the separation of the courses in the

DOI : 10.18231/2454-9150.2018.0125

system. The attacking node does not need any earlier learning of the system and the security components actualized on it. In this compose assault, the two attacking nodes are associated with each other through a connection known as passage. The malicious node display on either side catches the parcel from the legitimate node and by epitomizing the packet, transmits it to another malicious nodes in the network. In given figure, wormhole attack is portrayed. The nodes 2 and 9 are the malicious nodes in the network. These nodes will attempt to get the RREQ [5] message packets. node 9 will send a packet which conveys the false route of node 9 to node 2.But, in actual it is not the original path. The original path follows from node 9-8-6-5-4-2.

The way from node 9 to node 2 is the wormhole link / tunnel made by the malicious nodes.

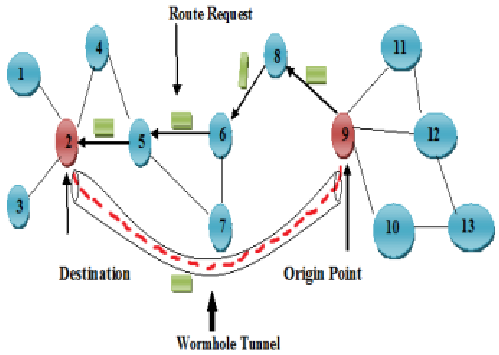

Fig.2. Wormhole Attack

Classification of Wormhole Attack Recent examinations has characterized the wormhole attack on different ways; these attacks are ordered based on these ways they are recorded beneath [6].

- Implementation of these nodes.
- The medium chosen by these nodes.
- Way of attack.
- On the basis of visibility of attacks.

On the basis of visibility these are classified as given below:

- Open wormhole attack / exposed
- Half open wormhole attack
- Closed wormhole attack /covered up
- Open Wormhole Attack/Exposed.

The two wormhole nodes are visible in the network. In this the attacking nodes includes themselves (their identity) in the packet header and then follows the normal route discovery mechanism. Every one of the nodes in the network know about the nearness of malicious nodes however they would carry on as though the malicious nodes are their immediate neighbors.

A. Closed Wormhole Attack / Hidden

Here the source and destination nodes don't know about the nearness of the malicious nodes. The packet headers are not refreshed in the route discovery component. The noxious hub toward one side catches the bundle from the true blue node and passages it into another malicious node. Along these lines, the opposite end attacking node will either dispose of the bundle or specifically disposing of the parcels or modifying the packets.

B. Half Open Wormhole Attack

In this kind of attack the malicious node at one side of the system refresh its personality in the packet header at the season of course disclosure process. Here one malicious node is unmistakable and other is undetectable to the honest to legitimate nodes in the network [7].

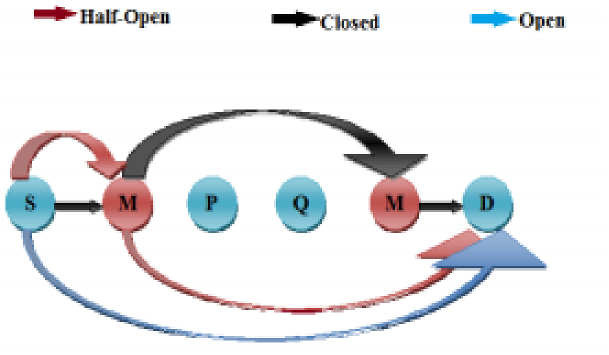

Fig.3. Types of Wormhole Attacks

III. Literature Survey

Jagtar Singh, Natasha Dhiman [8] exhibited that, Mobile means moving and ad hoc means transitory with no settled foundation so mobile ad hoc networks are a sort of transient networks wherein nodes are transferring without any constant infrastructure or centralized administration. Deployed in 1990's, MANETs were broadly inquired about for a long time. Ad-hoc network is a collection of nodes this is linked via a wireless medium forming hastily changing topologies. The infrastructure much less and the dynamic nature of those networks demands new set of networking techniques to be carried out which will provide green end-to-end communication Wireless devices are continuously growing in communique area having more computing pace and some of capabilities, while shrinking in weight and size. MANETs represent to confounded conveyed structures that include wireless mobile nodes that can unreservedly and powerfully self-get ready into subjective and transitory vs topologies.

People and devices are permitted to flawlessly internetwork in zones without a pre-display discussion framework, e.g., disaster recovery environments. Routing in Mobile Ad-hoc Networks is a testing undertaking because of its incessant changes in topologies. We examine in this paper routing protocol, difficulties and security of ad-hoc networks.

Aarti, Dr. S. S. Tyagi [9] presented that, MANETs is a framework a great deal less, dynamic network comprising of a gathering of wireless mobile nodes that discussion with each other without the utilization of any unified specialist. Because of its fundamental attributes, together with remote medium, dynamic topology, dispensed collaboration, MANETs is defenseless to diverse kinds of protection strikes like worm hole, black hole, rushing attack and various other. In this paper we concentrate mobile ad-hoc network and its attributes, challenges, application, security objectives and distinctive sorts security attacks at various layers.

Gurpinder Singh, Jaswinder Singh [10] displayed that, Mobile Ad hoc networks (MANET) are described by multihop wireless connectivity, Infrastructure less environment and as often as possible converting topology. The nodes acts as router and talk to each different. This paper goals to offer a method of knowledge the problems and protocol (OSPF, DSR, AODV, TORA.OLSR.DSDV) of MANET and examining behavior of DSR, AODV, and TORA protocol the utilization of measurements Throughput and Network Load. The Behavior analysis has been finished by utilizing simulation tool opnet 14.5 which is the fundamental simulator [9].

L Raja, S Santhosh Baboo [11] introduced that, Advancement in the field of web because of wireless networking technologies offers ascend to numerous new applications. MANET is one of the most extreme promising fields for research and change of wireless network. As the recognition of mobile device and wireless networks notably extended during the last years, wireless ad-hoc networks has now become one of the maximum vibrant and active discipline of conversation and networks. A MANET is an self sustaining series of mobile devices (laptops, smart phones, sensors, and many others.) that speak with each different over wireless hyperlinks and cooperate in a dispensed way with the intention to offer the vital networks capability inside the absence of a fixed infrastructure. This sort of network, running as a stand-by myself network or with one or a couple of factors of attachment to mobile networks or the Internet, paves the way for a few new and energizing applications. This paper presents understanding into the capacity packages of ad hoc networks, different attacks and talks about the innovative requesting circumstances that protocol architects and network developers are gone up against with.

M. Rmayti et al. [12] In this paper, our propose a novel detection model to allow a node to check whether a presumed shortest path contains a Wormhole tunnel or not. Our approach is based on the fact that the Wormhole tunnel reduces significantly the length of the paths passing through it.

IV. PROPOSED WORK

In previous work, they used additional storage for each route response packet to identify the malicious node. This computation requires calculation of the energy of each node and unstable routes which increase routing overhead. This method is very time consuming and it is not possible to store the details of each node is difficult. It is difficult to store the energy and routes of all nodes so this technique is not efficient for the large and scalable network.

For discovering wormhole attacker in MANET, we proposed tree-based method to distinguish and avoid an attacker. When a node in the network has a few data which is to be securely spread to the destination. Then we construct a tree of network in which source node behaves as a root node and other neighboring nodes are as children. When source send data to destination it search for the paths which should be shortest path. We consider that malicious node always reply first for the shortest path to traverse all the traffic towards itself. So we check the left and right children of malicious node or who reply first on the basis of tree which we formed earlier. Then request the neighbours that are this path is suitable or not. Then all neighbour which is child node check this and reply root node if it is valid then send data otherwise all child update that information and protect the data from getting into the wormhole channel.

Proposed Algorithm:

```
Step 1: Initialize the network
Step 2: Select sender S and destination D nodes
Step 3: if source has data to send to the destination
        Then construct a tree T in which source node is a
        root node
Step 4: if it has neighbours
        Then make all neighbour nodes as a child node
        Else tree has no child
Step 5: request for shortest path
Step 6: if we get reply from the node
        then we  traverse  T.left and T.right
        else request again
Step 7: if path is valid
        Then neighbours check and reply to source node
Step 8: update the routing table
Step 9: Exit
```

DOI : 10.18231/2454-9150.2018.0125

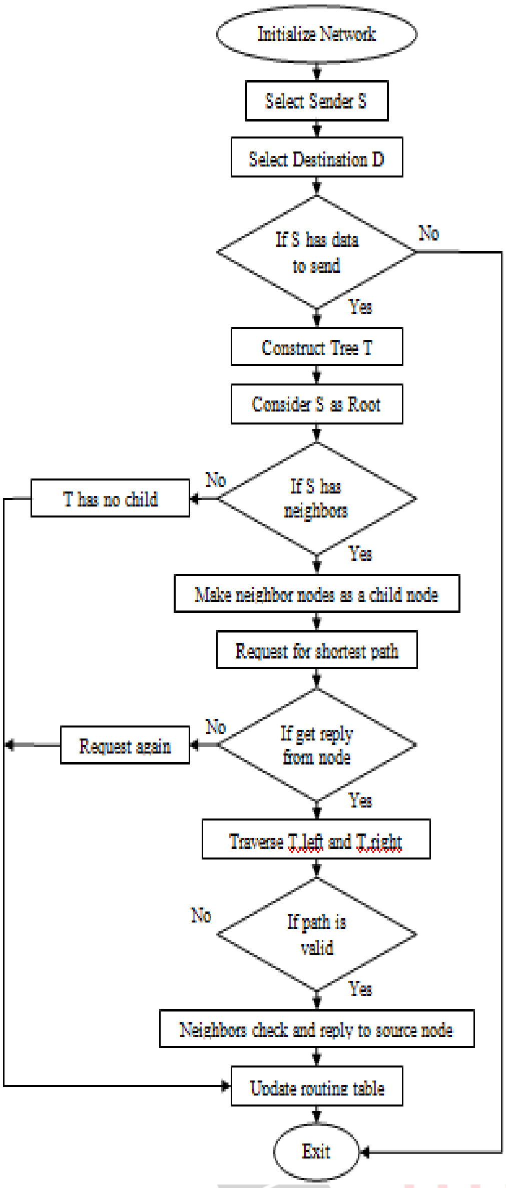

Fig.4. Flowchart of Proposed Algorithm

V. Result Analysis

Network For the implementation of the proposed work, we used NS2 for the simulation and the above mentioned techniques are applied to show the work.

Table 1: Parameter Table with their Values

Parameters	Values
Simulation Used	NS2
Network Size	1526m x 135m
Number of Nodes	50
Simulation Time	50s
Antenna Used	Omni directional Antenna
Packet Size	1500 bytes
MAC Protocol	IEEE 802.11

There are three tables which show throughput values, PDR values and Packet drop values at different time period

A. *Trace file*

The file written by an application to store coverage data or overall network data and in NS2, it's referred to as Trace File. Trace files log each packet, each event that occurred within the simulation and used for analysis.

Output:

```
s 1.000000000 _44_ AGT  --- 0 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [0] 0 0
r 1.000000000 _44_ RTR  --- 0 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [0] 0 0
s 1.000000000 _44_ RTR  --- 0 AODV 48 [0 0 0 0] -------
[44:255 -1:255 30 0] [0x2 1 1 [49 0] [44 4]] (REQUEST)
s 1.008000000 _44_ AGT  --- 1 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [1] 0 0
r 1.008000000 _44_ RTR  --- 1 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [1] 0 0
s 1.016000000 _44_ AGT  --- 2 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [2] 0 0
r 1.016000000 _44_ RTR  --- 2 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [2] 0 0
s 1.024000000 _44_ AGT  --- 3 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [3] 0 0
r 1.024000000 _44_ RTR  --- 3 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [3] 0 0
s 1.032000000 _44_ AGT  --- 4 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [4] 0 0
r 1.032000000 _44_ RTR  --- 4 cbr 1000 [0 0 0 0] -------
[44:0 49:0 32 0] [4] 0 0
```

B. *AWK file*

AWK Scripts are great in handling the information from the log which we acquire from NS2.

C. *Result in graphical form*

XGRAPH is a universally useful x-y information plotter with intelligent catches for printing, panning, expanding and selecting show choices. It will plot information from any number of documents on a similar chart and can deal with boundless information set sizes and any number of information records.

1) *Packet Delivery Ratio:*

It is the definition in which the total numbers of received packets calculated in terms of send packets. It is in the percentage form which has no unit. The graph shows that a PDR graph among base method as well as proposed method. This PDR rate is best in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

DOI : 10.18231/2454-9150.2018.0125

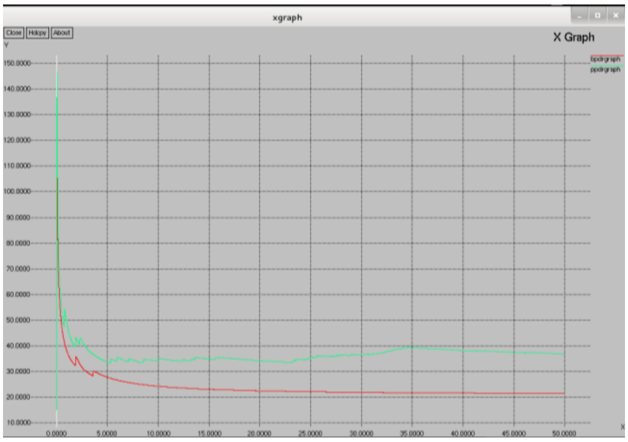

Fig.5 PDR Graph

Table 2: Packet Delivery Ratio

Time (in ms)	Base paper	Propose paper
5	27.7842	33.6752
10	24.2809	34.2244
15	23.1011	34.9555
20	22.5184	34.2719
30	22.1696	35.3149
35	21.9222	36.6829
40	21.7543	39.3583
45	21.6341	38.1568
50	21.5328	37.4701

2) Throughput

The transfer of information lying on information measure is result as output. The graph represents an output graph among base approach moreover as projected approach. The output of the projected approach is better than the present approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

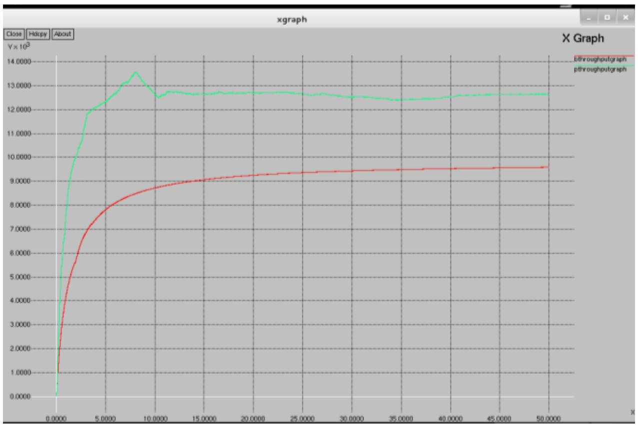

Fig.6 Throughput Graph

Table 3: Throughput

Time (in ms)	Base paper	Propose paper
5	7806.58	12313.6
10	8714.08	12652.6
15	9062.93	12637.9
20	9248.1	12687.7
25	9360.74	12660.2
30	9431.54	12517
35	9485.51	12410.3
40	9527.15	12539
45	9559	12617.8
50	9583.78	12643.1

3) Routing Overhead:

It is the whole wide variety of control packets inside the network at some stage in the transmission of data from source to destination. The graph shows that the routing overhead is less in the proposed work which is greater in existing technique.

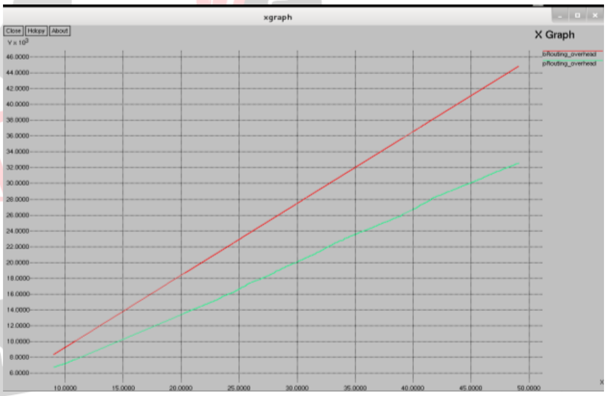

Fig.7. Routing Overhead Graph

Table 4: Routing Overhead

Time (in ms)	Base paper	Propose paper
10	9282	7220
20	18659	13624
30	27487	20103
40	36573	26722
50	44845	32582

DOI : 10.18231/2454-9150.2018.0125

VI. CONCLUSION

Today's Mobile Ad hoc Networks (MANETs) became a popular concern for scientists, and different learning has been made to performance enhancement of ad hoc networks. In MANET, the nodes are compromised for data forwarding to each other for communication with the others node which are away from their communication range. MANET is a sort of network whose dynamic topology, decentralizing organization and particular such limits are when in doubt for some security attacks. The mobile nodes converse with each other not including any infrastructure. One of these attacks called Wormhole Attack that two opposition node collaborate together to transmit the packets in out of band channel. Wormhole attack consists of nodes the attacker nodes which are related to every different with a hyperlink essentially this link is referred to as tunnel. In the proposed work, we enhance the performance of the network by generating the valid path in the form of tree. The result section show the efficiency of the work in the form of PDR, throughput and routing overhead.

REFERENCES

[1] Mobile Ad-hoc Networks (MANET), http://www.ietf.org/html.charters/manetcharter. html. (1998-11-29).

[2] Pallavi Agarwal, Neha Bhardwaj, "Overview of Trust Management in VANET and Various Cryptography Fundamentals", International Journal of Future Generation Communication and Networking. 2016 Jun 30; 9(6):137-44.

[3] Krishna Gorantala, ―Routing in Mobile Ad-hoc Networks‖ , Umea University, Sweden, June-2006.

[4] Geetha Jayakumar and Gopinath Ganapathy, ―Performance Comparison of Mobile Ad-hoc Network Routing Protocol‖ , International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.11, pp. 77-84 November 2007.

[5] Pallavi Agarwal. Technical Review on Different Applications, Challenges and Security in VANET. Journal of Multimedia Technology & Recent Advancements. 2017; 4(3): 21–30p.

[6] R. Maulik and N. Chaki," A comprehensive Review on Wormhole Attacks in MANET", in proceeding of 9th International Conference on Computer Information Systems and Industrial Management Applications, (2010), pp. 233-238

[7] Akansha Shrivastava and Rajni Dubey," Wormhole Attack in Mobile Ad-hoc Network: A Survey" in International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.293-298.

[8] Jagtar Singh, Natasha Dhiman, "A Review Paper on Introduction to Mobile Ad Hoc Networks", ISSN: 2278-621X , Vol. 2 Issue 4, IJLTE

[9] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", ISSN: 2277 128X ,Volume 3, Issue 5, International Journal of Advanced Research in Computer Science and Software Engineering, May 2013,

[10] Gurpinder Singh, Jaswinder Singh, "MANET: Issues and Behavior Analysis of Routing Protocols" ISSN: 2277 128X", Volume 2, Issue 4, International Journal of Advanced Research in Computer Science and Software Engineering April 2012.

[11] L Raja, S SanthoshBaboo, "An Overview of MANET: Applications, Attacks and Challenges", ISSN 2320–088X, Vol. 3, Issue. 1, pg.408 – 417, IJCSMC, January 2014

[12] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi A. Mammeri "Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks (MANETs)" 2016, IEEE.

DOI : 10.18231/2454-9150.2018.0125