International Journal For Technological Research In Engineering
Volume 4, Issue 4, December-2016 *ISSN (Online): 2347 - 4718*

CLUSTERING OF MOBILE ADHOC NETWORK: AN APPROACH FOR BLACK HOLE PREVENTION

Saiqua Anam[1], Mr. Om Prakash Yadav[2]
[1]Student M.Tech (C.S.E), UCER, Allahabd, U.P, India

ABSTRACT: A MANET holds wireless mobile node that communicates with each other without any infrastructure of network or any central base station. In the absence of infrastructure the nodes in the manet are autonoumous and managed by itself. There is no fixed time in the network that nodes of MANETs can join and leaves.The black hole is the malicious node that pretend itself as having the shortest path to the node to reach the destination. This malicious node drops the packets in the network by giving the wrong replay for any route request and have no path for destination. Here proposed method get rid of the malicious black hole node at distributive level. This approach address the performance issues of MANET.A new cluster oriented concept is proposed to enhance the performance and efficiency of the network .Proposed strategy ensure to bring best performance of manet in presence of black hole attacks.

I. INTRODUCTION

Mobile adhoc network are the self composed network in which it is configure various mobile nodes. MANETs has self properties, as the name mobile nodes are arrange in the dynamic topological infrastructure is also known as MANET. Due to high mobility that affected by the various kind of issues. According to the observation there are two main issues first how to detect the malicious node and second is how to prevent from malicious node to increase the performance of the MANET. Due to study, It is perceive that there are various method available for the performance issues of MANET. Some of them are studied and after that a new strategy is proposed and implemented. This paper presents a cluster oriented infrastructure for observing and communicating the mobile nodes in the networks. Attacks on mobile adhoc network can be classified into two categories. A passive attack does not disrupt proper operation of the network without altering it. The requirement of privacy can be violated if an attacker is also able to interpret the data gather. Discovery of passive attacks is very difficult for the operation of the network itself does not get affected. A way of preventing this kind of problem is to use powerful encryption mechanisms to encrypt the data being coveyed, thus making it impossible for eavesdropped to obtains any useful information from the data overhead. An active attack tries to change or damage the data, then the normal working of the network is interrupt. These can be divided into the two categories: external attack and internal attacks. External attack are the attack in which nodes that do not belong to the network. these attacks prevented by using standard security mechanisms such as encryption techniques and fire wall. In the internal attacks The nodes are the part of network.

II. INTRODUCTION OF BLACK HOLE ATTACK

A black hole is a malicious node that falsely replies for any Route Request (RREQ) without having active route to specified destination and drops all the receiving packets [1]. A Black Hole
node has two properties: (a) the node enters in AODV by represent itself as a valid route for destination. Then it starts receiving the packet from the valid node (b) drops the packet containing valuable information.

- Single Black Hole Attack: In single black hole attack only one malicious node attack on the route[2]. When the source node broadcast RREQ message then the malicious node takes an advantage of vulnerabilities of AODV protocol. It responds with high sequence number to its preceding node in the path. Thus source node assumed malicious node as a destination node and start the process of data forwarding. The malicious node then drop all the packet received.
- Co-operative Black Hole Attack: The number of malicious notes is more than one in the network[3]. The overall result of cooperative is complete decrease in throughput and increase in packet drop ratio in the network. Thus for better security and better performance in MANETS it is very important to eradicate the Cooperative attack.

III. BRIEF LITERATURE SURVEY

MANET is the temporary network in which mobile nodes is independent to move in or out from the network.
MANET is build on temporary wireless network and not required any fixed infrastructure as well as centralized administration. Due to non availability of network infrastructure and autonomous behavior of nodes, network is vulnerable to many attacks. Most commonly found attack, man in middle attack, deniel of service attack, impersonation, eavesdropping attack, black hole attacks, gray hole attack.
AODV routing protocol is a source initiated on demand routing protocol. Each mobile nodes maintains a routing table that maintain the next hop node information for a route to destination. Black hole is responsible for loss in the network by receiving the packet and dropping the receive packet that has to receive by the destination. Therefore there is need to detect and prevent the MANET from the malicious black hole nodes. This lead to improve the performance of MANET by lowering the route of packet drop ratio and increasing the detection rate of malicious node which gives the through put ratio more which enhance the network performance.
Methodology used
1. Start
2. Deploy mobile in the network

3. Organize the network(into cluster) Decided position of every nodes
4. Choose source node
5. Select the cluster head which has lesser distance from the source node.
6. Nodes which will reply to cluster head hello message will become a part of cluster
7. Introduce cooperative malicious node(black hole) in networks
8. Dectection of black hole node node using cluster head.
If (member node ack with data to cluster head)->detection of black hole nodes using cluster header.
Else(Assign node as malicious node)
9. Detection of black hole node using cluster header
If(cluster head does not ack with data pack)->Discovery of new cluster head Else (continues packet forwarding)
10. Dicovery of new cluster head
If(new member ack with cluster header)->Assign that member node as a new cluster head
Else
Assign node as malicious node
11 Continue packet forwarding till destination is reached
12. end

IV. CONCLUSION

Our approach is to detect the malicious node successfully in the entire network and the results will be predicted to be more efficient than the existing approach of safen route method with high packet delivery ratio as well as high detection rate of black hole node nodes.

REFERENCES

[1] Akhlaq, Monis, et al. "Addressing security concerns of data exchange in aodv protocol."World Academy of Science, Engineering and Technology16 (2006): 29-33.

[2] Sowmya, K. S., T. Rakesh, and P. HudedagaddiDeepthi. "Detection and Prevention of Blackhole Attack in MANET Using ACO."International Journal of Computer Science and Network Security12.5 (2012): 2124.

[3] Goyal, Priyanka, VintiParmar, and Rahul Rishi. "Manet: Vulnerabilities, challenges, attacks, application."IJCEM International Journal of Computational Engineering & Management11.2011 (2011): 32-37

[4] Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating Impact of Blackhole Attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

[5] Abusalah, Loay, AshfaqKhokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols."Communications Surveys & Tutorials, IEEE10.4 (2008): 78-93.

[6] Khin, Ei and ThandarPhyu. "Comparative Analysis of Black Hole Attack Solutions in AODV Protocol."IJCCER1.2 (2013): 21-25.

[7] Devassy, Antony, and K. Jayanthi. "Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting."

[8] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks."Communications Magazine, IEEE 40.10 (2002): 70-75.

[9] Weerasinghe, and Kriti. "Discovering a secure path in MANET by avoiding black/gray holes." International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878

[10] Sanjay Ramaswamy, Huirong Fu, Neelam , "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[11] Chavda, Ketan S., and Ashish V. Nimavat. "Master of Computer Engineering, CU Shah College of Engineering and Technology, Wadhwancity." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013

