A TWO TIER APPROACH FOR PREVENTING BLACK HOLE ATTACK AND IMPROVING EFFICIENCY

Avinash Gada[1], Praveen Naik[2]

[1]*M.Tech, CS&E, Acharya Institute of Technology, karnataka, India*
[2]*Assistant Professor, Acharya Institute of Technology, karnataka, India*

Abstract

One of the most emerging and trending in the field of networking is secure routing to overcome many hindrances that are occurring in day to day lives. Thus providing efficient mechanisms for such networks is the most challenging one. MANET's (Mobile Adhoc Networks) are a combination of several independent nodes without any fixed infrastructure, dynamic topology, battery constraints, and lack of centralized mechanism, because of its architecture/outlier they are more vulnerable to various kinds of passive and active attacks, such as black hole attack, grey hole attack, wormhole attack. Providing/Implementing a multi tier/two tier security mechanism helps in elevating such kinds of active attacks to some extent.

Keywords: *Black Hole attack, MANET, Clustering, Encryption.*

----------***----------

1. INTRODUCTION

A MANET consists of several independent nodes that are aimed to perform specific tasks Ad hoc networks offer minimal operating costs, higher flexibility, good coverage and better throughput due to the involvement of individual nodes. since each node in a MANET is self configured without any centralized control mechanism, infrastructure less, readily configured, the MANETs are deployed in vast kind of applications such as military operations, rescue operations, weather fore casting and many more in our day to lives. Because of its behavior and its infrastructure, its became a boom for many attackers to exploit it in many ways and making it more vulnerable, since the MANETs are more susceptible to various kinds of attacks providing an efficient and effective mechanisms to combat several attacks is the most challenging one. This paper aims at improving the security mechanism by providing two tier architecture such that to some extent the efficient performance and attack free network could be visualized.

2. A SURVEY ON BLACK HOLE ATTACKS

2.1 Prevention of Black Hole Attack in MANET

An ad hoc network is a collection of individual mobile nodes dynamically forming a temporary network. It operates in the presence of non centralized infrastructure. One of the dominant protocols used in ad hoc networks is AODV (Adhoc on demand distance vector) protocol, meant to provide a wide range of services for many mobile users by means of good structured architecture. Energy depletion, channel errors, loss of packets is some of the limitations of MANETs. The AODV protocol is being compromised by security of the Black hole attack. The Black hole attack is a kind of the attack that causes diversion of the data packets to an unknown node which is not a part of the network, the malicious node advertises as having a shortest path from the node with which it want to intercept. In this paper it the faster message verification, black hole identification, safe routing and black hole routing is being avoided.

2.2 Removal of selective Black Hole Attack in MANET by AODV Protocol

Mobile AdHoc networks are independent and self forming wireless networks. A MANET is composed of several independent users communicating over constrained bandwidth. Because of the independent mobile nodes the topology of the network keeps on changing indigenously. A black hole attack on MANET refers to an attack by falsely advertising sequence number, hop count and acquires a routing message from source to the destination. This paper focuses on preventing the selective black hole by activating the trusted nodes and preventing the data loss and analyzing the performance of the trusted nodes after inserting them into the network. The trusted nodes are replaced with the nodes that are being attacked and hence loss of energy is being preserved.

2.3 Detection and Prevention of Black-Hole Attack in MANETS

In this the authors have proposed the concept of clustering and clustering head, because of fewer requirements and quickly deployable, MANETs are most suitable for a various kinds of applications such as Rescue operations, Military operations and Day to Day applications. A black-hole attack in MANET occurs due to the presence of malicious nodes of malicious nodes in the network attracts several data packets by advertising a fake route to the destination before the actual route reaches the source. The concept of clustering approach is proposed in AODV protocol for detecting and preventing black hole attack. In this approach each and every member of the cluster ping to the cluster head to detect any difference between the number of data packets sent and received by the node, if any ambiguity is observed all the nodes discard the malicious node from the network. The analysis is being carried in terms of Packet Delivery ratio, Detection Rate, Throughput

and the simulation results are being obtained using NS2 simulator tool.

2.4 Detection and Prevention Of Black Hole Using Clustering in MANET using Ns2

A MANET consists of wireless independent nodes that communicate with each other without the need of any fixed infrastructure or any base station. That's why MANETs have a lot of applications where fixed infrastructure is no more used. Nodes in the MANET are independent and are capable of functioning on its own in the absence of fixed infrastructure. MANETs are susceptible to various kinds of attacks due to their dynamic behavior, and since each node is independent and can join/leave the network at any instant of time. Black node is a kind of node that causes drop in packets by replying false route requests and doesn't contain any path to the destination. The author proposed the concept of eradicating black node at a distributed level.

2.5 A Novel approach for preventing Black-Hole Attack in MANETs

A Black-Hole attack is a type of attack in MANET occurs due to the presence of malicious nodes, that falsely advertises the fake fresh route to the destination. This paper presents a clustering approach for detection and prevention of Black-Hole attack in the presence of AODV protocol. In this approach every member of the cluster will ping to the cluster head to detect the peculiar difference between the number of data packets that are sent and received by the node. If any invariance is seen then , all the nodes will obscure the malicious node from the network. In this the authors have proposed a light weight solution which is based on simple acknowledgement to scheme to prevent Black Hole attack it can be merged with any existing on demand adhoc routing protocols, with this approach the mobile check-points detect the presence of several black hole nodes. The detection and throughput rates are improved by 4 and 1.5 times respectively.

3. RELATED WORK

This section describes the previous works that are being carried out and how it could be related to our proposed work. According to various considerations MANET security is the prime concern in every aspect. Moreover the security schemes have a vast impact on throughput, delay, and other hindrances. They need some overhead and consume network resources and thus decrease throughput significantly, earlier works considered throughput and security separately in designing a MANET with which the overall optimization of the network could not be achieved in terms of performance. By jointly designing upper layer and physical layer security schemes related to channel conditions and relaying cooperativeness ensures the optimal throughput.

To analyze the Black hole various approaches have been proposed. Accordingly a MANET is used in wide applications, for example communication between the nodes through insecure links arises a security problem, MANET is susceptible to various kinds of attacks such as black hole attack, worm hole attack, grey hole attack, Sybil attack, flooding attack and route table alteration attack. To overcome black hole attack intrusion detection system, sequence number comparison, trust based routing approach, sequence number comparison have been proposed in the earlier studies. Trust base routing mechanisms identifies and decreases the number of malicious nodes and dangers in the path.

In order to detect and identify the black hole a trust based mechanism is proposed, in which the nodes in the network calculate the trust value of the neighboring nodes, if any node is found to be less than the calculated trust value, and then it's treated as a malicious node and avoided in the data communication paths. This ensures that the AODV protocol is being secured and the MANET is being avoided with Black hole attack.

The black hole attack in a MANET is a serious issue and various steps must be taken to overcome such issue. In a black hole attack more than one node is malicious identifying and detecting is cumbersome. Several approaches have been proposed to overcome the black hole in the presence of AODV protocol. Forced Routing information modification prevents the attack by automatic error correction that leads the node to select the correct path in the routing path, thus securing the network from attack and also providing the communication link between the server and access point, and thus making it more secure by transferring the data flow through the trusted nodes between server, access points, and the nodes.

Since every node in the MANET has to rely on another for data transmission, cooperativeness among the nodes must be maintained. However, it is hard to encourage cooperativeness among the nodes, each node has limited resources that need to be secured and the nodes become selfish and could not help in data transmission process, such nodes are known as selfish nodes. It leads to several issues such as Quality Of Service (QoS), routing, security, auto-configuration and resource management. A highly reliable cooperativeness must be established to attain a significant data transfer without compromising the network resources.

The structured classification of these clustering schemes enables us to better understand and make significant changes. In MANET the movement of nodes change the topology quickly resulting in increased overhead in message transfers. The protocols try to keep the number of nodes within the cluster so as to attain the better functionality. The cluster head is selected on-demand so as to improve the communication costs.

This section provides the previously made contributions with respect to MANET security and the dominant black hole attack and its overcoming. The proceeding section describes the proposed methodology to detect and prevent the black hole in a MANET.

4. PROPOSED METHODOLOGY

The proposed approach provides the clustered organization of the nodes where the nodes and the node heads are distributed as following:

1) Cluster nodes: These nodes are a part of the network and participate in data communications, at any instant of time these nodes may leave or may be a part of another cluster.

2) Two Cluster heads: These cluster heads act as a check in point and monitors the incoming/outgoing data flow path in a cluster, these two cluster heads act as a double layer security mechanism in which if the inspection is not done at the first node then it could be carried out in second node, and these are also responsible for establishing communication among other clusters , and also keeping the profile information of all the nodes under it such as trust value, data transmitted/received by individual nodes and the node behavior.

3) Monitoring node: This node acts as a centralized node, responsible for managing all the tasks carried out in a MANET, such as monitoring all the nodes, inspecting the data flow routing, pinging all the cluster heads to ensure its involvement in the network monitoring.

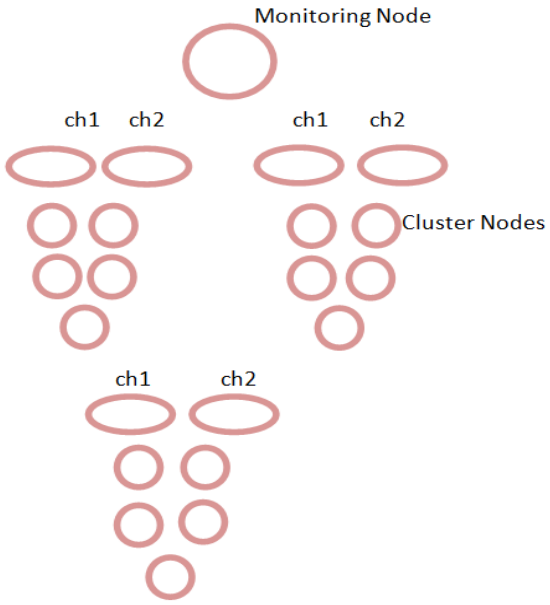

Fig -1: Schematic organization of cluster nodes, cluster heads and monitoring node

Once the cluster formation is done the nodes in a cluster interact with each other and ping to cluster head and start establishing communications with it. The nodes in a cluster are assumed to be trusted nodes such that their profile information is maintained at the cluster head and monitoring node, this enables secure routing in a MANET and limits the probability of vulnerability. After establishing the communications between the cluster nodes, cluster head and the monitoring node, the nodes in MANET are distributed with public keys by a monitoring node, if the nodes need to establish a communication with other nodes/cluster head/monitoring node, then they must exchange the private keys and if they are matched then secure communication takes place between them.

Initially all the nodes are kept with the profile information of all the nodes, such that upon receiving a private key the nodes must ensure proper data exchange by checking the profile information of other node and upon matching the desired information the data exchange takes place.

When a black hole is found to exist, and try to establish a network connection upon receiving a public key if it tries to act as a part of the network and start communicating with other nodes in the network. communication with it hampers, since the profile information of a black hole node is not updated and marked it as a fake node and ping monitoring node via cluster head, and updates the information regarding unknown node, which in turn the monitoring node populates the same information to all the other nodes such that in the future if the same attack exits then it is no longer taken into account. With this approach the advent of Black hole attack is detected and prevented with dual security mechanism. The same approach could be applied for worm hole attack, it involves two unknown nodes and tends to be a part of the network, one node forms a part of the network and transfers all the data flow through a tunnel to the node on the other end, if these nodes are detected through encryption mechanisms they can no longer be a part of the network, the worm hole attack prevention could be visualized to some extent.

By taking throughput into consideration the, maximum throughput could be achieved only in the absence of vulnerable attacks, with this dual secure mechanism an enhanced result could be expected, even if an attack occurs chances of attacking the network could be completely reduced. This results in better QoS, monitoring the dynamic behavior of the nodes, the data flow routing, number of data packets sent or received by an individual node. With these properties a network is assumed to be trust worthy and more efficient as compared with a network having loads of attacks and vulnerabilities in it.

Since the MANETs are applied in a wide range of applications, it became a boon for many of the attackers to exploit it in various ways; efficient mechanisms must be implemented by taking considerations in all the aspects with respect to resource utilization, QoS, throughput, attacks.

5. DESIGN AND ARCHITECTURE

The clusters are formed randomly by selecting few nodes and from those nodes the cluster head and the monitoring node is selected based on parameters like highest residual energy and the distance parameter, the design part of the network consists of a two cluster heads for each cluster and a monitoring node, such that the cluster head acts a check in and checkout point for the data flow that is transferring within and outside the network, and also monitors the data flow between inter and intra cluster communications, the monitoring node acts as an overall supervision of the

network and also maintains all the information about the cluster heads, cluster nodes, and the data flow path sent/received by each node in a data communication process.

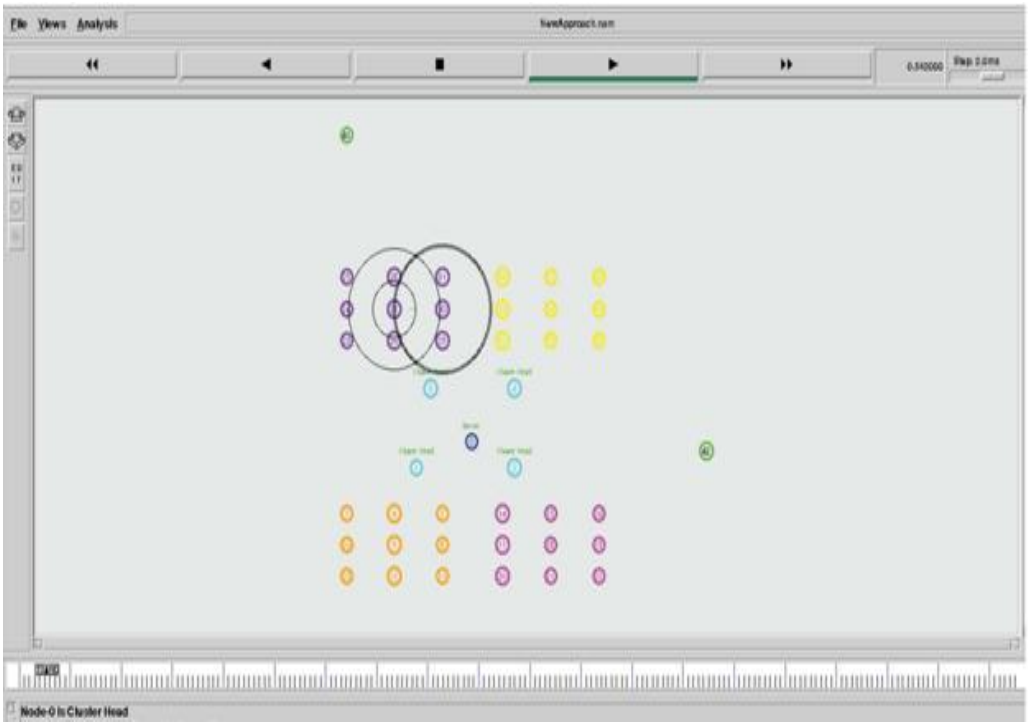

Fig -2: Cluster heads, Cluster nodes and Monitoring node

The efficiency of the network could be improved with respect to performance, throughput and delays, with the two tier mechanism the attacks could be minimized and the normal functioning of the network continues without any interruptions which leads to increased throughput and also lesser end to end delays, that leads to increased performance, with this approach the overall efficiency of the network could be visualized when compared with the earlier works this paper mainly focuses on security parameter with the two tier mechanism the chances of attacking a network could be minimized to some extent and the increase in throughput and performance could be analyzed.

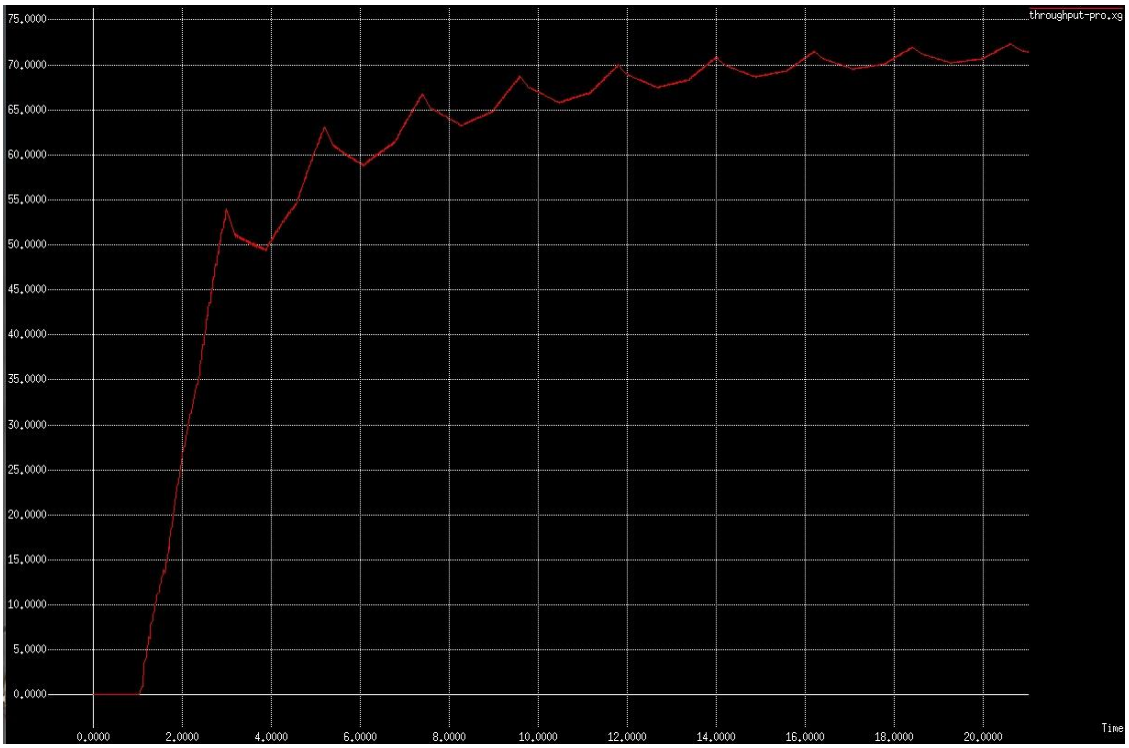

Fig -3: Enhanced Throughput

6. CONCLUSION

In this paper we have presented a complete overview on Black hole attack and its impacts, and an approach to overcome such kind of related attacks such that even under this kind of attacks the operations can be carried out in a hassle free manner, and mainly focuses on secured and efficient mechanism to prevent Black hole attack in such a way that the throughput could be minimized and to increase the performance of the network to some extent.

REFERENCES

[1]. Pooja Jaiswal and Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", IRACST, Vol.2, No5, October 2012

[2]. T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol, IJCIET'14, Volume 3, Special Issue 3, March 2014.

[3]. Gurnam Singh, Gursewak Singh "Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2", IJECS, Volume - 3 Issue -8 August, 2014

[4]. Rashmi, Ameeta Seehra, "Detection and Prevention of Black-Hole Attack in MANETS ", IJCST, Volume 2 Issue 4, Jul-Aug 2014.

[5]. Rashmi, Ameeta Seehra, "A Novel Approach for Preventing Black-Hole Attack in MANETs", IJCSIT, Volume 2, No.3, September 2014.

BIOGRAPHIES

Avinash Gada, M.Tech(IV sem), Computer Science & Engineering, Acharya Institute of Technology, Bangalore.

Praveen Naik, currently working as Assistant Professor, Dept. of Computer Science & Engineering in Acharya Institute of Technology, Bangalore, and having 10 years of experience in teaching and industry and pursuing PhD in the field of Software Engineering.