Grayhole Attack Prevention Using a Cooperative Mechanism Based On Hybrid Defense Architecture in MANET

PATEL BRIJAL, Pg Student, Parul Institute Of Technology, India
HIREN MER, Assistant Professor Department of CSE, Parul Institute Of Technology, India

Abstract
In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malicious nodes, this necessity may lead to serious security concerns; for example, such nodes may disturb the routing process. In this context, preventing or detecting malicious nodes launching gray hole or collaborative blackhole attacks is a challenge in mobile adhoc network. In this paper attempts to resolve this issue by designing a routing mechanism in which MD5 (Message Digest 5) technique is used. This method will help in achieving the stated goal. In proposed work we will try to achieve packet delivery ratio and routing overhead will be considered and chosen as performance metrics.

Keywords: MANET, Gray hole/collaborative black hole attacks, Malicious node, MD5.

Introduction
A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes in wireless network without any fixed infrastructures. In this network, intermediate nodes cooperate and act as a router and send messages from one node to another.

MANETs is rapidly deployable and it also highly adaptive in nature. Nodes have high mobility and communication is done via shared wireless network. MANETs are widely used in applications such as military communication by soldiers, Emergency rescue service, Disaster Recovery, etc. In MANETs have some particular characteristics such as unreliable wireless links used for communication between many host, limited bandwidth, constantly changing the network topology, enumeration power and low battery power etc.

In Mobile Ad hoc Networks there is no infrastructure support as in case with wireless networks. Since a destination node might be instead of the range in a source node sending packets; a routing process is at all times needed to find a path so as to forward the packets suitably among the source node and the destination node. In a cell, a base station can reach all mobile nodes without routing by means of broadcast in generic wireless networks. In the process of ad-hoc networks, each node should be able to forward data to the other nodes.

The lack of any infrastructure, mobile nodes are dynamically changing the network topology in infrastructure less network makes MANET more vulnerable to various types of routing attacks than a typical wireless network. The attacker would perform different types of attacks such as Black hole, Collaborative Blackhole and Gray hole attack.

Blackhole Attack
In a blackhole attack, a malicious node sends a fake RREP packet to the source node that has initiated a route discovery process and in order to show itself as a destination node or an intermediate node to the actual destination node to the route. In such a case the source node would send all of its data packets to the malicious node and the malicious node then intercepting the packets. A result of source node and destination node will not be able to communicate with each other.

Also a malicious node does not need to check its routing table when sending a false message; its response is more likely to diffuse the source node first. This makes the source node consider that the route discovery process is complete and that is ignore all other reply messages and begin to send data packets. As a result of this process, all the packets through the malicious node are discarded without forwarding them to the destination.

Co-Operative Blackhole Attack
The malicious node could be said to form a black hole in the network. In sometimes these malicious nodes are cooperate with each other with the same aim of dropping packets these are known as cooperative Black Hole nodes and the attack is known as Cooperative Black Hole attack.

Gray Hole Attack
Gray hole attack is a variation of black hole attack, in which the malicious node’s are more difficult to detect. The gray hole nodes can perform the attack in three different ways:

a) The malicious node may drop packets from certain nodes while forwards all other packets to the network.
b) A node may behave maliciously for a certain time and dropping packets selectively.

c) The malicious node may drop packets from specific nodes for precise time only, but later on, it behaves as a normal node. Since, due to these characteristics, the detection of gray hole attacks is very hard. A gray hole attack can disturb the route discovery process and degrade the network's performance.

Related Work

Nowadays Mobile Adhoc Network is emerged as a very active research area because there are lots of mobile devices are connected to each other without an infrastructure. Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative black hole attacks.

In ordinary, detection mechanisms that have been proposed so far can be grouped into two broad categories. Proactive detection schemes in many cited paper Jian-Ming Chang[1], A. Baadache and A. Belmehdi[6], H. Weerasinghe and H. Fu[7] are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage. Reactive detection schemes[1][8][9] are those that trigger only when the destination node detects a significant drop in the packet delivery ratio.

Khattak et. Al[2] proposed solution of using optimal route and hash for preventing black and gray hole attacks on AODV protocol. In this solution second established route has been used for transmission of data packets from source to destination. Xiaoling Zheng and Jidong Jin[3] are used to focuses on the methods of the application safety improvement of MD5 in the passport authentication by switching or interfering with the treatment process of MD5.

In Isaac Woungang [4], Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat proposed a solution for detection Black hole attack in MANETs. In their solution, DBA-DSR scheme, a feasible DSR-based solution to mitigate black hole attacks in MANETs. Simulation results showed that (1) the original DSR heavily suffers from black hole attack in terms of network throughput and packet delivery ratio, (2) the proposed DBADSR scheme performs better than the DSR scheme in terms of network throughput rate and minimum packet loss percentage.

In[5] Zhao Min and Zhou Jiliu proposed Two authentication mechanisms, based on the hash function, the Message Authentication Code (MAC) and the Pseudo Random Function (PRF), are proposed to provide fast message verification and group identification, identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack.

Problem Definition

The existing methods are suffering from protocol dependent methods which in turn can't identify the Cooperative Blackhole / Grayhole attack in more efficient way. In this method is also not more secure and sufficient to react against Cooperative Blackhole / Grayhole attack. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative black hole attacks and gray hole attack.

Proposed Work

The proposed work will give the efficient results compare to existing results which are given in research paper. In proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect gray hole/ collaborative black hole attacks in MANETs. So proposed work will achieve the high throughput and security compare to the existing work.

Proposed Key Authentication Scheme

A source node generates a chain of one-time-use keys using the hash function, e.g., MD5 and shares only that last generated key, K_l, with the receivers. A message can be authenticated only when the used key in the chain is revealed. To verify the authentication key, the receiver recursively applies the cryptographic hash function until reaching K_l. In reality, the receiver can stop when reaching a key that has been used before. A key cannot be used outside its designated time interval and the message will be ignored if the MAC is based on an expired key. Consequently, clock synchronization is required to make sure that the source and destination have the same time reference for key expiration.
Work Flow Of Proposed System

Steps For Proposed System

Initial Bait Step
Step 1: Deploy ‘N’ number of nodes in a 2D plane of wireless network
Step 2: Choose source node ‘S’ and destination node
Step 3: Create TCP/UDP connection among the nodes
Step 4: Assign unique key ‘K’ to all the nodes in the network
Step 5: The source node stochastically selects an adjacent node, i.e., \( n_r \), within its one-hop neighborhood nodes
Step 6: Adjacent node is taken as the destination address and send bait RREQ
Step 7: Source node had sent out the RREQ, there would be other nodes’ reply RREP in addition to that of the \( n_r \) node.
Step 8: This indicates that the malicious node existed in the reply routing

Initial Reverse Tracing Step
Step 9: When a malicious node, for example, \( n_m \), replies with a false RREP, an address list \( P = \{ n_1, \ldots n_k, \ldots n_m, \ldots n_t \} \) is recorded in the RREP
Step 10: \( S = K_1 \cap K_2 \cap K_3 \ldots \cap K_k \)

Step 11: \( T = P – S \), where \( T \) is the list of trusted node for routing

Shifted to Reactive Defense Phase
Step 12: Get \( T \), route the packets through the trusted nodes available in \( T \)
Step 13: Check the unique while forwarding the packets in every nodes along the route
Step 14: Securely transmit packet to destination

Conclusion And Future Work
Proposed detection scheme based on MD5 will try to detect grayhole/ collaborative blackhole attacks in MANETs. The introduced techniques are to identify the grayhole/ collaborative blackhole attack efficiently with high throughput and provide more security.
In future we can propose to mitigate the multiple blackhole attack by applying mitigation technique which provides, enhance the efficiency of existing Method and High throughput against the attacks.

References
[8] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simu-
