International Journal of Electrical Communication Engineering
Vol. 1: Issue 1
www.journalspub.com

# Intrusion Detection of Packet Dropping Attacks by Using Cryptographic Hash Function in Mobile Ad-hoc Networks

***Amol Dange*, Rupali Jadhav, Supriya Phatak***
Department of Computer Science & Engineering, Shivaji University, Kolhapur, Maharashtra, India

***Abstract***

*A Mobile Ad-hoc Network (MANET) is an autonomous system of nodes (MSs) (also serving as routers) connected by wireless links. There is no infrastructure existing in a MANET. The network's wireless topology may change dynamically since nodes are free to move and each node has limited transmitting power. In MANETs two types of packet dropping attacks are present: (1) Gray hole and (2) Black hole. In gray hole, attacker node drops part of the data and cheats the previous node and in black hole, attacker node drops all data packets and cheats the previous node. In this paper we present a proposed mechanism to detect and isolate these attacks in network.*

***Keywords****: Black hole; gray hole; AODV; Intrusion Detection Technique; malicious node; monitoring node; cryptographic hash function*

****Author for Correspondence*** *E-mail: amol.dange@gmail.com*

## INTRODUCTION

A mobile ad-hoc network (MANET) is a self-organized multi-hop system comprised of mobile wireless nodes [1]. Wireless network consists of mobile nodes without any physical connection to each other. Such networks use a transmission power to send and receive data. MANETs have some special characteristic such as unreliable wireless links used for communication between hosts, changing network topologies, limited bandwidth, battery power, low computation power etc. Each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network.

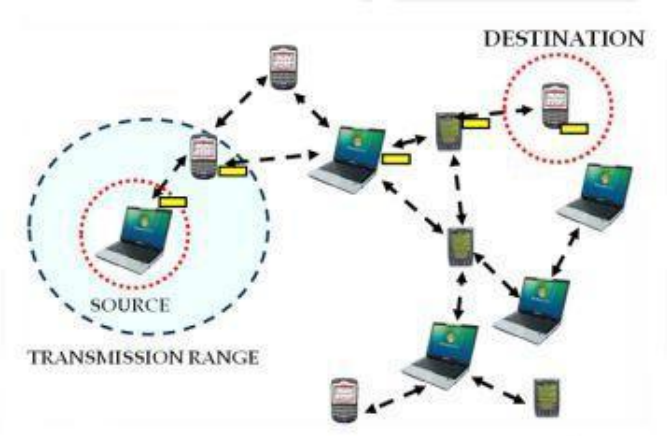


***Fig. 1:*** *Mobile Ad-hoc Network.*

  

**Two Transmission Scenarios Presents in MANETs**

1. The nodes which are in direct transmission range of each other they directly send and receive message or any data packets from each other.
2. The nodes which are not within transmission range of each other, they depend on intermediate nodes for delivery of message or any data packet.

Due to their dynamic and cooperative nature, MANETs demand efficient and effective security mechanisms. As part of risk management we must be able to identify these risks and take appropriate action. In some cases we may be able to design out particular risks cost-effectively. In other cases we may have to accept that vulnerabilities that exist and seek to take appropriate action when we believe someone is attacking us. As a result, intrusion detection is an indispensable part of security for MANETs.

The following part of the paper presents; significance of proposed approach, summary of the related work done previously, proposed work with problems in previous approaches and solutions enlisted in this approach and finally the conclusion.

## SIGNIFICANCE

In MANET, routing and packet forwarding are performed by nodes themselves. For these, security becomes very important issue in MANET. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1. Availability: It implies that network is accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service.
2. Confidentiality: Confidentiality ensures that network services and data are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against eavesdropping or unauthorized reading of message attack.
3. Integrity: Data can be modified only by authorized parties or only in authorized way. It assures that a message being transferred is not destroyed.
4. Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The resources of network should be accessed by the authenticated nodes.
5. Authorization: The network nodes should be able to identify other nodes to prevent impersonation.
6. Freshness: It ensures that malicious node does not resend previously captured packets.
7. Access control: Nodes which are in the network have set of permission for accessing shared network resources.
8. Efficiency: Efficiency of mobile ad-hoc network depends on computation and energy consumption of resources that are available in network

## RELATED WORK

Tseng proposed a method by which we can find malicious nodes present in the network and establish a correct path to destination; this method is called Neighborhood based method. Another one is Multiple Route Replies, in which source node waits for more than two reply packets coming from network after receiving multiple replies it simply verifies the common hope in path. If common hope is there then it simply states that route is safe.

Sen *et al.* summarized a method in which every node listens to the next node for identifying misbehaving node present in the network [2,3]. If any node drops the packet more than threshold value then source node is notified.

Cai *et al.* summarized a method which keeps a rate for every node in network; such as a node is decreased when the node is detected as malicious or misbehaving node [4].

Approach referred by Uyyala and Naik in their paper has provided a method in which monitoring nodes are used for detecting the attacks and intrusion detection algorithm is used for improving network performance [5–10]. This method detects and isolates the gray hole and black hole attack if the attacker drops the packet.

## PROPOSED WORK

### Prevent Fake Reply Packets

In neighborhood based detection scheme we are able to find out misbehaving node in the network and route recovery. The source node sends a modified route entry packet to destination node so that source re-routes and send packets to destination node. But this method fails when the attacker sends any fake reply packets.

To solve this problem proposed approach involves the use of monitoring nodes in the network where monitoring node monitors all incoming and outgoing packets of active node.

### Prevent Collision Occurs At Receiver Node

If any node present in active path is dropping packets more than threshold value then source node notifies that there is malicious activity present in the network. But it fails in identifying malicious node if destination does not receive any packets because of collision present at node destination and intermediate node is not re-transmitting packets.

To solve this problem proposed approach involves observing the behaviours of neighbouring node by using anomaly intrusion detection mechanism.

### Avoiding Dropping or Modifying the Packets

If any node acts as a malicious node in the network it simply drops the packet in active route or modifies that packet data and retransmits that packet to the destination.

To solve this problem monitoring node broadcasts alert message to its neighbours in the network when any monitoring node identifies misbehaving node in its neighbours.

### Maintaining Data Integrity of the Data Packets

Sometimes malicious node in the network sends a number of fake reply packets and treats that they are having shortest route path to destination. When sender sends any data packet from that route, malicious node alters that message or packet by simply adding or dropping of that packet. So data packet does not reach the destination.

Here, there is a requirement for maintaining the integrity of data packets to overcome this problem. We extend anomaly intrusion detection mechanism by using cryptographic hash function. Cryptographic hash algorithms are necessary to keep a system secure, particularly when communicating through an untrusted network.

### Intrusion Detection System

Intrusion is a sequence of related actions performed by malicious node which gives a result in compromising the activity of system and it disturbs the given security policy of that system or network.

Intrusion detection is a process of identifying and isolating malicious activities which target computing and network resources.

Intrusion detection systems are the software application which detects the intrusion present in the target network.

Anomaly or behaviour based techniques used in IDS in which historical data about system activity of intended behaviour of user are used to build a normal profile. The detection process identifies the malicious activity from normal profile.

These anomaly based IDS system is used for detecting packet dropping attack but if packet is modified or altered then we extend IDS using cryptographic hash function which provides integrity of data packets [6–10].

**Cryptographic Hash Function**

A cryptographic hash function is a hash function, in which an algorithm takes a block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) modification to the data will modify the hash value. The data that has to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digests.

For providing integrity on data packets one-way-hash function H is used to generate MAC for RREP packet. Cryptographic Hash Function is the only possible way to generate MACs.

A Message Authentication Code (MAC) is a small part of information, which is used to authenticate and to provide integrity on the message.

A MAC algorithm, accepts a variable length message as input, and outputs a fixed length MAC.

There are so many cryptographic hash functions, such as Message-Digest algorithm (MD5) or Secure Hash Algorithm (SHA-1).

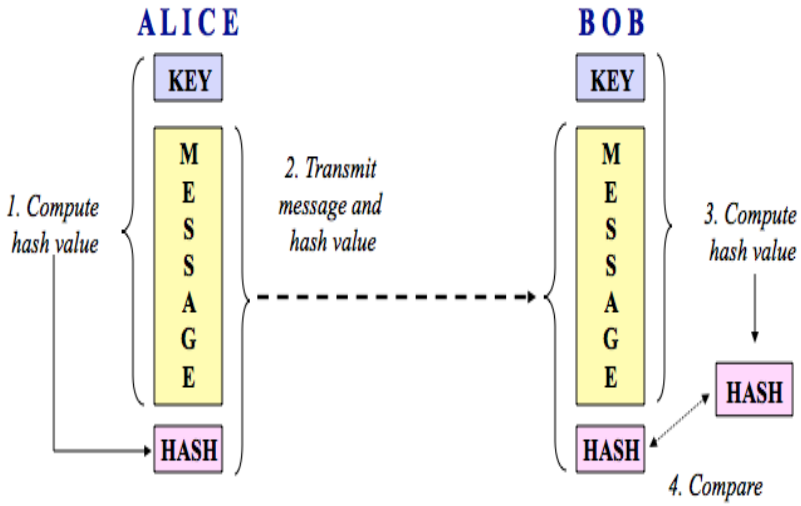


***Fig. 2:*** Message-Digest Algorithm.

**Algorithm for Detecting Packet Dropping Attack using Cryptographic Hash Function**

Step 1: Set or apply the monitoring nodes in the network that will cover the entire network.

Step 2: Monitoring nodes will monitor the network, i.e. it will monitor all incoming and outgoing packets of the nodes which are in active path.

Step 3: If the incoming and outgoing packets are not same i.e. malicious activity is present. Then the monitoring node will intimate it to sender to resend the message by re-routing.

Step 4: There are several malicious nodes in the network. Sometimes malicious node may be the part of second optimal route.
Step 5: Apply the hash function on the message if the malicious node is the part of second optimal route.
Step 6: The hash value is computed at source using cryptographic hash function that is SHA-1.
Step 7: When destination node receives the message or data packet it will compute the hash value of that packet.
Step 8: If the hash values are the same i.e. hash value of data packets at sender node = hash value of data packets at destination node. Then message is delivered at destination node securely.
Step 9: If the hash values are not the same, then monitoring node simply broadcast an alert message in the network.
Step 10: When sender receives that message from monitoring node, it re-routes that message and it will save the route information in routing table. In future it will not send any data packets through this route.

## CONCLUSIONS

In this paper, we have presented an extension mechanism of anomaly based intrusion detection system by using cryptographic hash function for providing security in the network and integrity on data packets against the malicious activities present in the network. This proposed method is extended to detect and isolate the packet dropping attack when attacker modifies or alters the data packets without dropping the packets. If the processing time taken by the nodes for transmission of data packets gets reduced then system can be improved to minimize delay.

## ACKNOWLEDGMENT

The author would like to give thanks to Department of Computer Science and Engg., Annasaheb Dange College of Engineering and Technology, Ashta, for suggesting the line of the research.

## REFERENCES

1. Akanksha Jain. Trust Based Routing Mechanism against Black Hole Attack using AOMDV-IDS in MANETs Format. *International Journal of Emerging Technology and Advanced Engineering,* (ISSN 2250-2459). Apr 2012; 2(4).
2. Fan Hsun Tseng, Li Der Chou, Han Chieh Chao. A Survey of Black Hole Attacks in Wireless Mobile Ad-hoc Networks. *A Springer Open Journal*. 2011.
3. Sen J, Chandra M, Harisha SG, *et al.* A Mechanism for Detect ion of Gray Hole Attack in Mobile Ad-Hoc Networks. *Information, Communications and Signal Processing, 6th International IEEE Conference.* 2010.
4. Jiwen Cai, Ping Yi, Jialin Chen, *et al.* An Adaptive Approach for Detecting Black Hole and Gray Hole Attacks in Ad-hoc Networks. *24th IEEE International Conference on Advanced Information Networking and Applications.* 2012.
5. Shivani Uyyala, Dinesh Naik. Anomaly Based Intrusion Detection of Packet Dropping Attacks in Mobile Ad-hoc Networks. *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).* 2014.
6. Kanthe Ashok M, Dina Simunic, Ramjee Prasad. Effects of Malicious Attacks in Mobile Ad-hoc Networks. *IEEE International Conference on Computational Intelligence and Computing Research.* 2012.
7. Virada Vinay P. Intrusion Detection System (IDS) for Secure MANETs. *International Journal of Computational Engineering Research.*

8. Chandure Onkar V, Gaikwal VT. Detection and Prevention of Gray Hole Attack in Mobile Ad-hoc Networks using AODV Routing Protocol. *International Journal of Computer Applications (0975–8887).* Mar 2012; 41(5).
9. Madhusudhanagakumar KS, Aghila G. A Survey on Black Hole Attacks on AODV Protocol in MANET. *International Journal of Computer Applications*: *(0975–8887).* Nov 2011; 34(7).
10. Kanan S, Kalaikumaram T, Karthik S, *et al.* A Review on Attack Prevention Methods in MANET. *Journal of Modern Mathematics and Statistics.* 2011; 5(1): 37–42p.