Preventing Manets from Blackhole Attack using Blackhole Node Detection Monitoring System

Parita Jain
Krishna Institute of Engineering & Technology
UPTU, INDIA

Puneet Kumar Aggarwal
Bharat Institute of Technology
UPTU, INDIA

ABSTRACT
Mobile Adhoc networks are prone to number of security threats due to unavailability of centralized authority. It incorporates various malicious activities within the network. This research focuses on single Blackhole attack but our design principles may be applicable to wide range of attacks. So, this proposed approach of Blackhole comprises of active routing misbehavior and forwarding misbehavior. This can be defined by modifying existing DSR protocol with the functionality of single Blackhole node in highly mobile and sparse network without affecting the overall performance of the network.

General Terms
Securing MANETS, DSR algorithm, Behavior of Blackhole node.

Keywords
MANETS, DSR routing protocol, Blackhole attack, Blackhole Monitoring System

1. INTRODUCTION
A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time; therefore, the limited wireless transmission range of each node gets extended by multihop packet forwarding. This kind of network is well suited for the mission critical applications such as emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited.

Ad hoc networks (multi-hop wireless networks) are expected to revolutionize wireless communications in the next few years by complementing more traditional networking paradigms (Internet, cellular networks, satellite communications); they can be considered as the technological counterpart of the concept of 'ubiquitous computing'. However, in order for this scenario to become reality, several issues must be adequately addressed. One of these issues is how to stimulate cooperation among the network nodes. In fact, the nodes of an ad hoc network are usually owned by different authorities (private users, professionals, companies, and so on), and a voluntary and 'unselfish' participation of the nodes in the execution of a certain network-wide task cannot be taken for granted. Concepts borrowed from the theory of Mechanism Design can be used to tackle this problem. Mechanism Design is the branch of Game Theory that studies how to design protocols that stimulate players (in our case, network nodes) to behave 'unselfishly', cooperating to the achievement of a global goal. A distributed protocol with this feature is called strategy-proof.

One of the fundamental tasks any ad hoc network must perform is routing. Since the network is in general multi-hop, a routing protocol is needed in order to discover and maintain routes between far away nodes, allowing them to communicate along multi-hop paths. Unless carefully designed, routing protocols are doomed to perform poorly in presence of 'selfish' node behavior. In general, a network node has no interest in forwarding a packet on behalf of another node, since this action would only have the effect of consuming its resources (energy, and available bandwidth). Thus, if many of the nodes act selfishly (as may well be the case when nodes are owned by different authorities), only a few multi-hop communications will take place, and the network functionality is compromised. Thus, the definition of strategy-proof routing protocols for ad hoc networks is of fundamental importance.

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message, which effectively builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.

Due to inherent characteristics of mobile adhoc network, it can be accessed by any authorized or unauthorized users. Among these most important issue is protection of Network layer. Network layer is vulnerable to various attacks named as Blackhole attack, Wormhole attack and many more.

2. BLACKHOLE ATTACK
MANETS are vulnerable to several different types of attacks. On the basis of many characteristics the attack on network is classified as passive and active attacks. Attacks against the routing messages are the important part in MANET and one such attack is Blackhole attack. It is an interception attack which is injected to get the unauthorized access to routing

messages in networks that are unintentionally sent towards them. It violates the integrity and confidentiality of packets as packets are analyzed and modified before sending to the next node.

A Blackhole node can behave in two ways while defining its existence in the network. [3]. Firstly, it can behave as an intermediate node in the path and the malicious node can intentionally perform absorption, dropping or delaying of message packets that pass through it. Secondly, the malicious node can send a forged route reply (RREP) to the source nodes (RREQ) advertising it as having the shortest route path to the intended destination.

In our research we employ second type on Blackhole attack to detect malicious Blackhole node in the mobile adhoc network.

3. PAPER OUTLINE

The rest of the paper is organized into different sections. Existing work is discussed in section 4. The DSR protocol is discussed in section 5. Our Proposed approach is discussed in section 6. And Conclusion and Future work in section 7. Finally References at last in section 8.

4. EXISTING WORK

During the study of Mobile Adhoc networks we have gone through various articles, research papers and web contents that are relevant to networks, algorithms and various approaches. All these materials gave me broader view about providing "security in MANETS". We have studied some research papers that were relevant to the security and gathered fruitful information how each and every element in MANETS play their role to provide a consistent model.

Many researches had been conducted by developing new enhanced routing protocols then the existing ones to solve the Blackhole attack problem in the mobile adhoc networks [4]. As the hosting and routing operations in the network mainly depends on the wireless nodes so, it requires a investigation mechanism hosted by the source for the detection of malicious Blackhole node in between the path, claiming that the path to the destination is a reliable path.

In [8] Marti et al proposed a watchdog/path-rater approach to detect Blackhole node in the network. When a source node wants to send a packet to the destination node having number of nodes in between the path. Then the source watchdog checks whether the next hop node forwards the packet or not. If the next node does not forward the packet within a predefined threshold then that node is defined as a Blackhole node in the network. But the cons of this approach is that if a node which is located at two or more hops from the source node, it is difficult to identify for Blackhole node because for that one have to trust on the information given by other nodes which allow the malicious node to be defined as good behaviour node. Also, the watchdog defined with the source node is not that powerful that it able to differentiate between misbehaviour by receiver collisions, ambiguous collisions, collusion partial dropping and controlled transmission power.

In [5] Seong Moo Yoo proposed different approaches to solve the Blackhole node attack. 1) In his first approach he allows the source node to check whether the intermediate node is authorized node or not by utilizing the network redundancy. That is the source node buffer all the route reply (RREP) that it gets until the shortest and reliable path is identified. And after that transmits the entire buffer packet. This leads to time delay in sending the message packet through that shortest path. 2) In his second approach, each node stores sequence number of last sent packet and last received packet. When a RREP packet is received by the node, it checks both the sequence number; if they are not matching then it initiates an alarm defining the existence of malicious node. The shortcoming is that if we have a large scale network then the difference in these sequence numbers will not able to define the existence of malicious node in the network.

In [6] the author Weili et al, proposed an approach in which each intermediate node is required to send the next hop information with the request reply (RREP) packet to the source node such that the source node extracts the information of next hop send by the intermediate node and then again sends the route request to the neighbouring nodes to verify whether the intermediate nodes who have earlier send the route reply have the route to the destination or not.

In [9] Jian Chen proposed an approach in which he defined an assumption that the neighbouring node set difference of one node at different time instance is less than or equal to one, and the probability that the neighbour set difference of two nodes at the same time instance is very small. That is, he defined two control packets for extracting information about the neighbouring nodes.

In [12] H.Yang uses cryptographic approach to protect network layer attacks by providing collaborating localized voting against Blackhole malicious nodes and named this approach as SCAN.

In [16] Rajib Das et al, defines an approach by discovering two routes one for the destination node and other for the intermediate node. If the next hop node sends a reply (RREP) with defining that it has a route to the destination but not for the intermediate node than the source node will discard the route reply and further again starts the fresh route discovery process. Also after finding the malicious node in the network it sends out an alarm message to all the neighboring nodes in the network with information about that malicious node.

Many other various solutions are introduced to address this wireless network attacks problem and still there are many researches are going on. But if we initiate the routing protocol in this network, then it will lead to degradation of performance and less throughput for those networks.

5. DYANMIC SOURCE ROUTING PROTOCOL (DSR)

In wireless networks with infrastructure support a base station always reaches all mobile nodes. But in adhoc network a destination node might be out of range of a source node transmitting packets, routing is needed to find a path between source and destination. The greatest problem for routing arises is that of from the highly dynamic topology. This results in frequent changes in topology. In adhoc networks routing tables reflect these frequent changes in topology.

Dynamic source routing (DSR) divides the task of routing into two separate problems.

5.1 Route Discovery

A node only tries to discover a route to the destination if it has to send something to this destination and there is currently no known route.

5.2 Route Maintenance

If a node is continuously sending packets via a route it has to make sure that the route is held upright. As soon as node detects problems with the current route it has to find an alternative.

The basic principle of source routing is also used in fixed networks, for example token rings. DSR eliminates all periodic updates and works as follows: If a node needs to discover a route it broadcasts a route request with a unique identifier and the destination address as parameters.

Any node that receives a route request does the following: 1) if a node has already received the request (identified using the unique number), it drops the request packet. 2) If the node recognizes its own address as the destination then the request has reached its target. 3) Otherwise the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

Using this approach the route requestor collects a list of addresses representing a possible path on its way towards the destination. As soon as the request reaches the destination it can return the request packet containing the list to the receiver in reverse order. But this possible only when links should work bidirectionaly.

6. PROPOSED APPROACH

In Our proposed approach, we are basically carrying our investigation for detection of Blackhole node and preventing the network from this type of attack by modifying existing Dynamic Source Routing Protocol (DSR). Proposed DSR algorithm also addresses all kinds of misbehaving nodes such as selfish or malicious nodes. Our main aim with this approach is:

- To present the various significance of MANET networks.
- To present detailed study over MANETS.
- To analyze the Blackhole attack in MANETS.
- To present approaches to provide security to the Mobile Adhoc networks from Blackhole attack.

In our approach, there exists a source node or we can call it a requester who request to its neighboring nodes that are within the transmission range of it for the route identification to the destination node. The detection Monitoring System consist of the requestor acting as a monitoring node within the network for the identification of Blackhole node.

The approach on which this monitoring system nature relies assures that if a provider in the network sends back the RREP packet to the requestor more than one or two times for having route to different destinations from the same requested node and assuring that it has a shortest path to the destination than that providing node is accused as an Blackhole node. And after discovering malicious node all other neighboring nodes are informed by sending a data information packet that a particular provider is suspected as an Blackhole node in the network. So, that no other source node makes a path to the destination with this malicious node as an intermediate node.

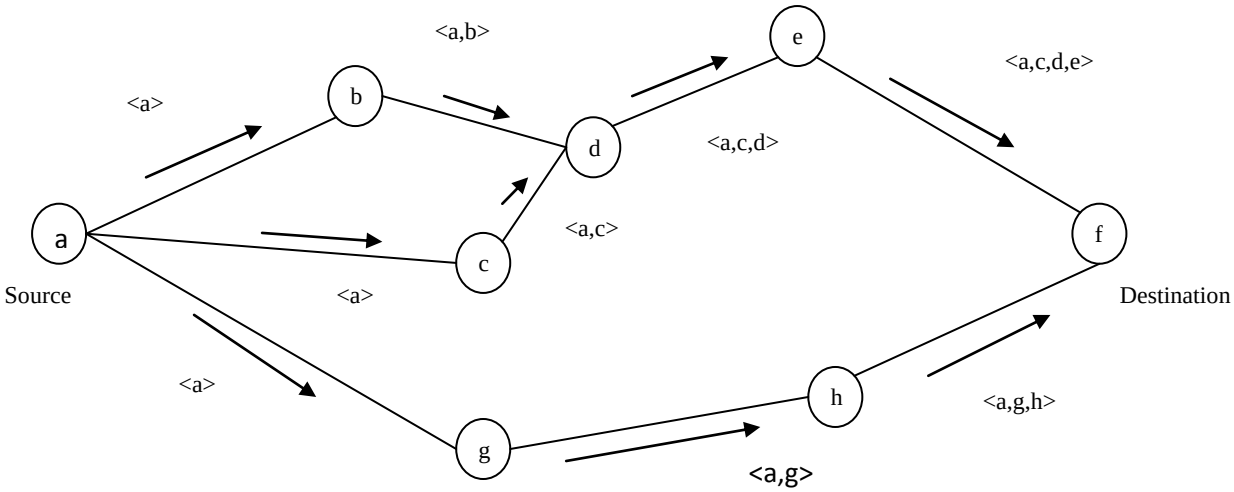

Fig 1: Route Discovery.

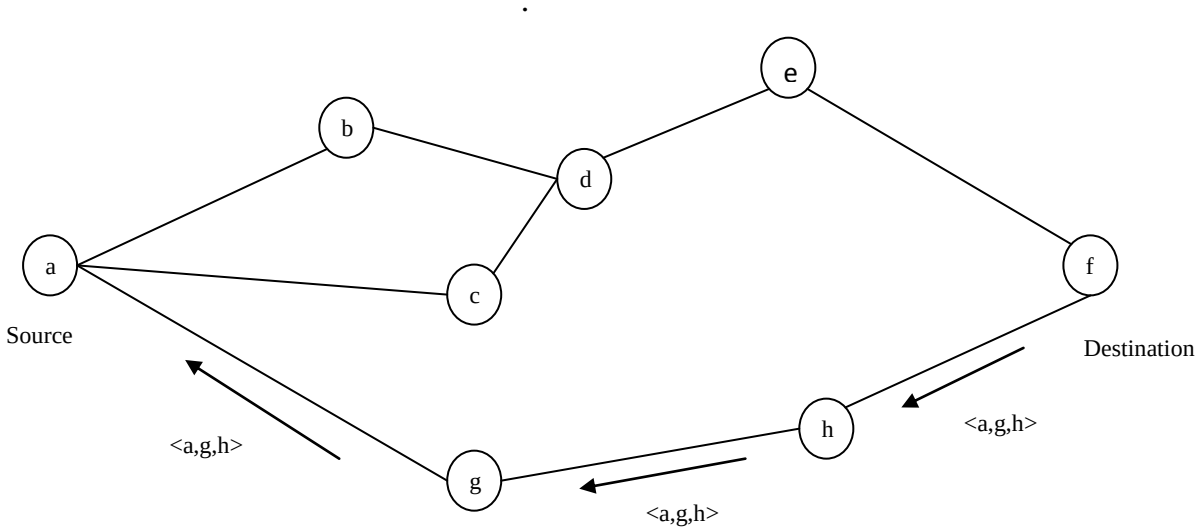

Fig 2: Route Reply

7. CONCLUSION AND FUTURE WORK

Our main focus in this study is to develop the routing protocol which will handle such types of attacks and also maintaining the performance of such networks. Our approach is a new approach for the Blackhole node detection within the network as the property of Blackhole node allows the node to provide an assurance to the requestor of having shortest path to the destination. In this research we define an approach with having different pairs of sources and destination such that we can identify the route from same source node to different destinations.

Future work includes the simulation of this proposed approach by using NS2.34 or any other network simulator tool and also provides its performance analysis in comparison to existing routing protocols.

8. REFERENCES

[1] B. Wu, J. Chen, J. Wu, and M. Cardei. 2008 A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks in Wireless/Mobile Network Security, Springer.

[2] Y. Hu and A. Perrig. 2004 A Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy, pp. 28-39.

[3] Moumita Deb. 2008 A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks in WCECS October 22-24 san Francisco, USA.

[4] E.Royer and C.-K. Toh. 1999 A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine, Vol. 6, No. 2, pp.46-55.

[5] Mohammad AL-Shurman, Seon-Moo Yoo and Seungiin Park. 2004 Black Hole Attack in Mobile Ad Hoc Networks. ACMSE Huntsville,AL,USA.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal. 2009 Routing security in Wireless Ad-hoc Network in University of Cincinnati.

[7] Sonja Buchegger and Jean-Yves Le Boudec. 2002 Performance Analysis of the CINFIDENT Protocol: Cooperation of nodes-fairness in Dynamic Adhoc Networks in Proc of IEEE/ACM MobiHOC.

[8] Santosh Krishna B.V, Mrs. Vallikannu A.L. 2010 Detecting Malicious Nodes for Secure routing in MANETS using Reputation Based Mechanism in IJSER.

[9] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch. 2003 Detecting Black-hole Attack in Mobile Ad Hoc Network in The institute of Electrical Engineers IEEE.

[10] S.Murthy and J. J. Garcia-Luna-Aceves. 1996 An efficient routing protocol for wireless networks. ACM Mobile Networks and Application, Oct. 183–197, 1996.

[11] F. Kargl, S. Schlott, A. Klenk, A. Geiss, M. Weber. 2004 Securing Ad hoc Routing Protocols", EUROMICRO.

[12] H. Yang, et al. 2006 SCAN: self-organized Network-layer Security in Mobile Adhoc Networks. IEEE Networks, vol. 24 pp. 1-13.

[13] D. Djenouri, A. Derhab, N. Badache. 2006 Ad Hoc Networks Routing Protocols and Mobility". Int. Arab J. Inf. Technol. (IAJIT) 3(2):126-133.

[14] J. Broch, D. B. Johnson, and D. A. Maltz. 1998 The dynamic source routing protocol for mobile ad hoc networks, Internet draft.

[15] B. Wu, J. Chen, J. Wu, and M. Cardei. 20008 A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer.

[16] Rajib Das et al. 2011 Security Measures for Blackhole Attack in MANET: An Approach. IJEST.