Defense Strategy for the Detection of Black Hole Attack in Dsr

Raja Karpaga Brinda.R[1], Chandrasekar.P[2]

[1] *II ME (CS), Sri Shakthi Institute of Engineering and Technology, Coimbatore, India*

[2] *Assistant Professor (S), Dept of ECE, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India*

brind222@gmail.com , chasek_2002@yahoo.co.in

Abstract: *Mobile Ad-hoc Networks are an emerging area of mobile computing. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Mobile adhoc network are prone to security threats. The lack of infrastructure and dynamic structure makes them easy prey to security attacks. The security threats may vary from active impersonation attacks to passive eaves-dropping. A black hole is a malicious node that replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The damage will be serious when they work as a group. This type of attack is called cooperative black hole attack. This proposed model includes a secure routing mechanism for DSR. We use the BDSR (Baited- Black-hole DSR) to detect and avoid black hole attack and extend the concept to the detection of co-operative black hole attack. The BDSR merges the proactive and reactive defense architecture in MANET by using the virtual and non-existent destination address to bait the malicious node to reply RREP.The performance graph is simulated for the packet delivery ratio and end to end delay.*

Keywords: *Black hole, cooperative black hole, DSR, Manet.*

I. Introduction

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic,sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links. A MANET consists of mobile platforms referred to as "nodes" which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. Manet nodes are equipped with wireless transmitters and receivers using antennas. At a given point in time, depending on the nodes positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters. MANETs have several salient characteristics [3]:

Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology which is typically multihop may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications often much less than a radio's maximum transmission rate.

Energy-constrained operation: Nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping is carefully considered.

II. Security issues in MANET

Due to infrastructure less, security is a major concern in mobile adhoc networks. Following is the various vulnerabilities that exist in wireless ad-hoc networks [3]:

Open Medium – Owing to open medium i.e. being distributed, eavesdropping is much easier in manet

Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network. They dynamically change their topology. This allows any malicious node to join the network without being detected.

Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security.

Lack of Centralized Monitoring - There is absence of any centralized infrastructure that prohibits any monitoring agent in the system.

Lack of Clear Line of Defense - The only use of Line of defense - attack prevention may not secure. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link.

In addition to prevention, we need two line of defense – detection and response. Realizing security in ad hoc environments is exceedingly difficult since many different types of ad hoc networks exist. Any variation is possible ranging from predominantly static sensor networks to highly mobile vehicular network scenarios. So, it is necessary to design specialized security solutions adapted to the underlying ad hoc network. Not only has the network architecture had to face security threats, also the services and protocols used within the network have to withstand many different attacks.

III. Security Attack

Various ways are found to classify the security attacks. Adhoc network are susceptible to link attacks ranging from passive eavesdropping to active

impersonation. Eavesdropping might give an attacker illegal access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and no repudiation. In this subsection we will discuss to type of categorization.

Behavior based attacks:

Passive attacks include packets containing secret information might be eavesdropped, violating the confidentiality principle. It obtains data exchanged in the network without disrupting the operation of the communication. Active attacks include injecting packets to invalid destinations, deleting packets, modifying contents of packets, and impersonating other nodes. Active attacks can be internal or external. These attacks are carried out by an external advisory or internal node involving actions such as impersonation.

Location based attacks:

External attacks in which the attacker aims to cause congestion propagate fake routing information or disturb nodes from providing services. Internal attacks are those in which the adversary wants to gain the normal access to the network and it participates in the in network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. Internal attacks are more severe and hard to detect.

IV. Description of DSR

Dynamic source routing (DSR) protocol is an on-demand routing protocol that is based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does

not have such a route, it initiates route discovery by broad- casting a route request packet. This route request contains the address of the destination, along with the source node's address and unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record. A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

V. Problem Definition

MANET is composed of a number of autonomous nodes that are self-managed each node acts as a host and it discovers its path and transmits its packet through the network. One of the most important security attacks is the black hole attack. A black hole is a selfish node which tries to capture the packet transmission and just drops the packet. In general two types of Black hole are present [1]:

Internal black hole attack:

The malicious node is actually not present within the network. But in case a chance occurs it tries and includes itself within the network. The damage caused by an internal malicious node is very severe.

External black hole attack:

The malicious node is an external node. It tries to fit itself in the network by overhearing the networks activities and starts participating in the actual transmission.

VI. Related Works

A number of researches are being carried for enhancing the security in Manet. Since there is no particular line of defense, security for manet is still a major concern for man. Some of the researches for the detection of black hole attack are given. W. Kozma, and L.Lazos,"REAct:resource-efficientfor node misbehavior in ad hoc networks based on random audits," [3] Based on Audit Procedure. When destination node detects a heavy packet drop, it triggers the source node to initiate the audit procedure. Source node chooses an audit node and it generates behavioral proof. Similarly source node prepares it behavioral proof .On the basis of comparison of results malicious nodes are detected. Drawback was that it is a reactive approach .Only if there is a drop in packet delivery ratio, the mechanism is triggered. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," [4] Introduced the concept of route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack in AODV. The intermediate node along with RREPs sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node checks in its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. It was dependent on the intermediate nodes reply. Also it was able to detect only single black hole.W. Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," [5] Introduced the approach of hash based function in REAct system. Enabled the data traffic and forward path detail available in behavioral proof. Upon drop in the packet delivery ratio initiates the blackhole detection. Based on the reactive detection.

VII. Proposed Method

The DSR based secure routing protocol that we are using detects and avoids the black hole attack. BDSR (Baited Blackhole DSR) uses the concept of sending bait id and attracts black hole to reply the fake routing information. Initially it sends a virtual and random address as its destination address. Proactive detection is used initially. In case presence of any malicious node is detected, it is included in the black hole list. We use the proactive detection only in our initial stage. Thereby reducing the routing extra overhead. As soon as the initial stage is over, it becomes reactive detection. Normal packet transmission takes place. Upon the completion of the process it checks the packet delivery ratio. If drop in packet delivery ratio is found, destination node sends alarm to the source which triggers the black hole detection. Our mechanism merges the advantage of proactive detection in the initial stage followed by superiority of the reactive detection.

In BDSR scheme the packet format of the RREP and RREQ is modified. In case of DSR routing, the source will have all the information about the intermediate nodes participating in its mechanism. Upon the reception of the RREP, it will know details of the nodes participating in packet transmission but it will not know exactly which the malicious node is. The packet format of RREP is modified such that Reserved field is used as Record address. The record address enables to trace the malicious node. In addition it has RREQ' packet which has a virtual and non-existent address as its target address. Route discovery is initiated with the source sending RREQ' to all the nearby nodes. The target address of the RREQ' is a fake id i.e. a virtual non-existing random id is given .When a malicious node receives RREQ', it replies itself as the shortest path to the destination. Upon the reception of the RREP, from the record address field, the source will know which the malicious node is and removes it from its network, in its initial stage. Thus the malicious node is detected and is recorded in the blackhole list. Thus the proactive detection detects the presence of blackhole.Also all the nodes are made aware of the blackhole.

The proactive detection makes use of the record address and the false id to perform the detection of the malicious node. Upon detection of the malicious node it is removed from the network by triggering alarm to all the nodes in the network about the malicious node. Thus future responses from the malicious nodes are discarded.

After the initial proactive stage, it becomes reactive detection. Source sends the route RREQ to the nearby nodes. The intermediate node sees to the target address. If it is the shortest path to the destination it adds its address to the field and forwards the packet to the destination.

In case it has already received the packet it just discards the packet. If it is the target address it sends RREP to the source and normal packet transmission starts. Upon the completion of the process, the destination checks the packet delivery ratio. BDSR scheme uses the advantage of both the proactive and the reactive detection. In the initial stage it reduces the chance of malicious node. In later stage it becomes reactive detection thereby reducing the overhead.

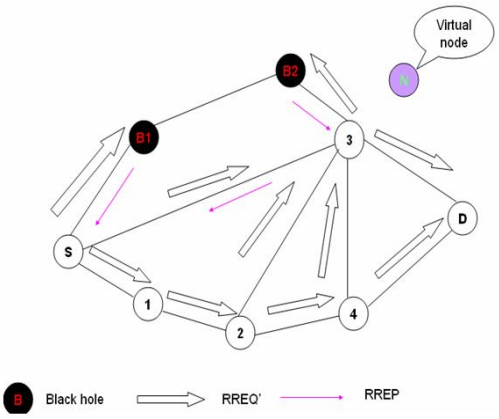

Fig 1: BDSR Mechanism

VIII. Simulation Results

The simulation is being carried out using Glomosim network simulator .

Based on the simulation parameters graph is plotted between DSR and BDSR.A number of parameters can be used to determine the performance.

The set of parameters over which the simulation is done are given below. The table gives the overall details of the environment condition at which the simulation is carried out.

Here we compare the packet delivery ratio and the end to end delay of BDSR and DSR .Based on the value in the statistics table the graph is plotted.

TABLE I: Simulation Parameter

Parameter	Value
Application Traffic	CBR
Radio Range	250 m
Packet Size	64 bytes
Transmission Rate	4 packets/sec
Speed	Random (0 – 20 m/s.)
Simulation Time	100 S
Number of Nodes	30
Area	2000m*2000m

Fig 2 shows the graph plotted between the number of malicious nodes and the packet delivery ratio. It is inferred from the graph that since there is no mechanism available to detect malicious node in DSR, the packet delivery ratio decreases as the no of malicious node increases. In BDSR, the packet delivery ratio is higher compared to DSR .It offers a greater packet delivery rate.

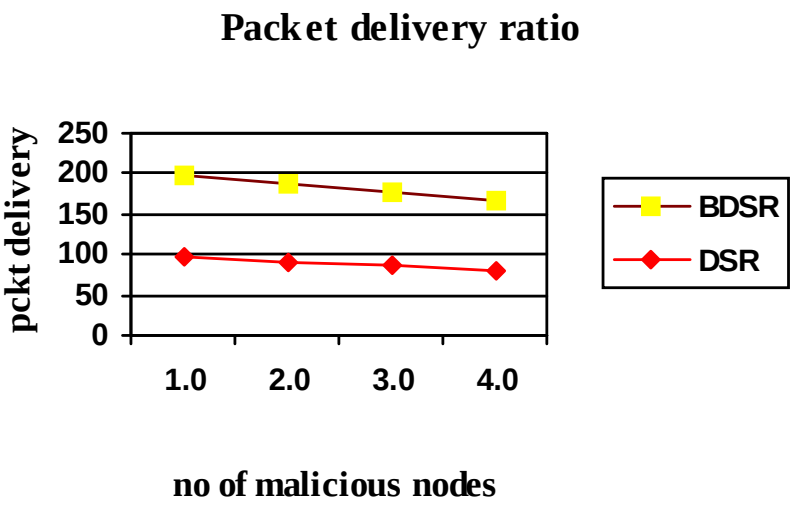

Fig 2: Packet delivery ratio

Fig 3 shows the graph for end to end delay. It is observed that the end to end delay is greater in the case of DSR.Due to the merging of proactive and reactive detection in BDSR; it offers reduced end to end delay.

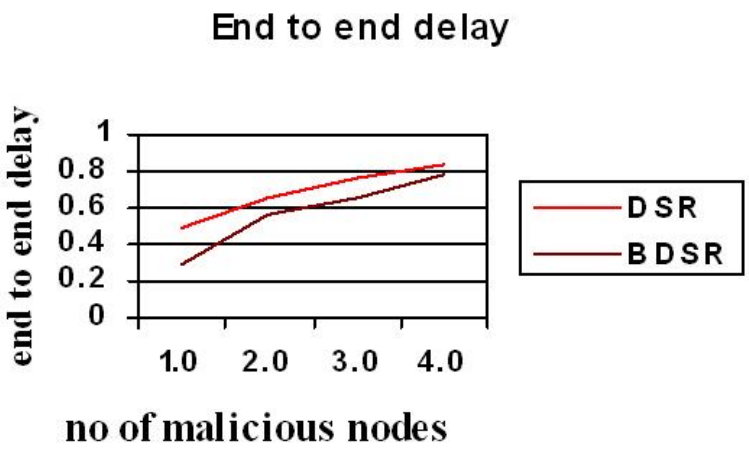

Fig 3: End to End delay

BDSR scheme uses the advantage of both the proactive and the reactive detection. In the initial stage it reduces the chance of malicious node. In later stage it becomes reactive detection thereby reducing the overhead.

IX. Conclusion and Futurework

The BDSR detects and avoids the black hole attack in manet.It uses the proactive detection in its initial stage and reactive detection in the later stage. The proactive detection checks for malicious nodes presence in the initial stage. The reactive detection reduces the overhead and resource wastage. Performance of parameters such as packet delivery ratio and the end to end delay are noted. Compared to DSR, BDSR offers a greater packet delivery ratio and reduced end to end delay.

In future work, it is extended to detect the co- operative black hole attack**.**

References

[1] Po-Chun TSOU,Jian-Ming CHANG, Yi-Hsuan LIN,Han-Chieh CHAO, Jiann-Liang CHEN "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs "ICACT2011.

[2] A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks,"International Journal of Computer Science and Information Security," Vol. 7, No. 1,2010.

[3] Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET," International Journal of Computer Science and Technology

[4] W.Kozma, and L. Lazos,"REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009.

[5] W.Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," 28th International Symposium on Reliable Distributed Systems September 2009.

[6] H. Weerasinghe and H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad hoc Networks: Simulation Implementation and Evaluation," IEEE International Conference on Communication, 2007.

[7] H.Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magazine, Vol. 40, No. 10, October 2002.

* * * * *