Detection and Removal of Co-Operative Black Hole\Black Hole Attack in Manet

Raja Karpaga Brinda .R
II ME (CS),
Sri Shakthi Institute of Engineering and Technology Coimbatore, India

Chandrasekar.P
Asst Professor (S) ECE,
Sri Shakthi Institute of Engineering and Technology Coimbatore, India

ABSTRACT
Advancement in the research field has with witnessed a rapid development in Mobile Ad-hoc Networks. The distributive nature and the infrastructure less structure make it an easy prey to security related threats. In this paper, we propose a secure routing protocol for DSR called as BDSR (Baited Black Hole Attack) for the detection and the removal of Black Hole and Co-operative Black Hole attack in MANET. A black hole is a malicious node which replies the route requests that it has a fresh route to destination and 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. The BDSR scheme merges the proactive and reactive defense architecture. In the initial stage it uses a proactive architecture, i.e. uses a Bait id concept for the detection of malicious nodes present in the network. Upon the completion of initial stage it switches to reactive defense strategy. The secure routing protocol resulted in increased packet delivery ratio and reduced overhead ratio. The extended defense routing protocol worked efficiently for the malicious node detection and removal in case of Co-operative Black Hole attack resulting in increased network performance.

Keywords: Black Hole, Co-operative Black Hole, DSR, MANET.

1. INTRODUCTION
Revolution in technology seems to increase mankind demand to access things at a faster rate at their will and wish. Wireless network is one such boon that enables users to access, communicate and transfer data with each other irrespective of their geographic location. Wireless Local Area Networks (WLANs) acts as a backbone behind these wireless applications and devices.WLAN's operation can be broadly classified on the basis of presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. An ad-Hoc network is an infrastructure less network. The operation mode of such network is stand alone, or may be attached with one or multiple points to provide internet and connectivity to cellular networks [3].

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. Nodes in a manet can act as either a host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. Mobile Ad-Hoc network is an autonomous system, such that there is no restriction and nodes can join\leave a network freely. Mobile Ad-Hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology. MANETs have several salient characteristics [4]:

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 greatly 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.

2. SECURITY ISSUSES IN MANET
Infrastructure less nature of Mobile Ad-Hoc Network (MANET) makes it easily prone to security threats. is the most important concern for the basic functionality of network. Lack of security in MANET is often because of its features like open medium, dynamic topology, distributive nature monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body

that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below [3]:

Non Secure Boundaries: Lack of clear secure boundary makes manet vulnerable to different kinds of attacks. MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity.

Compromised Node: Nodes in manet are free to move, join or leave the network in other words the mobile nodes are autonomous .This nature makes it difficult to detect the presence of malicious node within its network.

Lack of Centralized Monitoring: MANET is a self-configurable network, where communication among mobile nodes occurs by its distributive management.

Scalability Problem: In manet due to its mobile nature predicting the numbers of nodes in the future is difficult. The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable.

3. SECURITY ATTACK

Due to various factors like lack of infrastructure, absence trust relationship in between different nodes and its dynamic topology, the routing protocols are vulnerable to various attacks The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

3.1 External and Internal Attack:

External attackers are nodes outside the networks which try to get access to the network and upon receiving access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. Prevention of these attacks can be done by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

Internal attacker will have normal access to the network as well as participate in the normal packet transmission of the network. Internal attack is more severe attacks then external attacks.

3.2 Active and Passive Attacks:

In case of active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. Active attacker in strong can modify, fabricate and replays the messages.In case of passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

4. DESCRIPTION OF DSR

Dynamic Source Routing protocol abbreviated as DSR.It is a reactive protocol. DSR use to update its route caches by finding new routes. It updates its cache with new route discovered or when there exist a direct route between source and destination node. When a node wants to transmit data, it defines a route for the transmission and then starts transmitting data through the defined route.

4.1 Route Discovery Process: When a source node wants to start data transmission with another node in the network, it checks its routing cache. When there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, RREP is generated. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

4.2 Route Maintenance Process: When the transmission of data started, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The node generates a route error message, if it does not receive any confirmation to the originator node. The originator node again performs new route discovery process.

5. 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. When a number of malicious nodes join together they act as a group, forming a Cooperative black hole attack. In general two types of Black hole are present [1]:

5.1 Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

5.2 External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in manet.

6. 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 blackhole attack are given. Kozma, and L.Lazos, "REAct: resource-efficient for node misbehavior in ad hoc networks based on random audits," [5] 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," [8] 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," [6] 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. Latha Tamilselvan and Dr. V Sankaranarayanan," Prevention of Co-operative Black Hole Attack in MANET"[7] designed an approach for detection of co-operative black hole attack, based on the Fidelity table where presence of 0 indicates a malicious node. But it failed for the case of DSR. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol" [2] proposed a simple scheme which depends on the details of intrusion detection from local nodes rather than from the source node. This scheme is used only for the case of AODV as it has the advantage of sequence number.

7. 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.

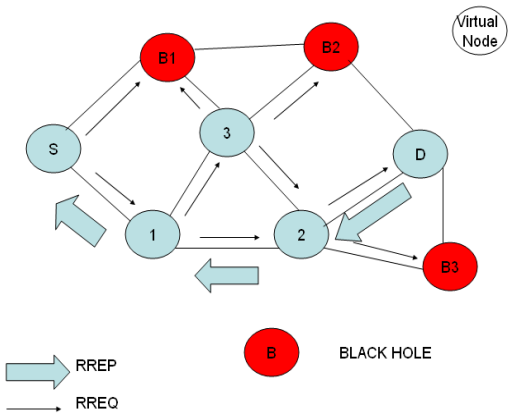

Fig 1: BDSR Mechanism

In case of Co-operative black hole attack, number of malicious node cooperate together and work as a network. This eases the task of detection. When a single malicious node is detected, based on the details of its next hop, we can easily find the remaining malicious nodes present within the network. This scheme performance clearly depicts that it has a greater packet delivery ratio as well as high throughput and it has reduced overhead ratio.

8. SIMULATION RESULTS

The simulation is done using GloMoSim (Global Mobile Simulator), to analyze the performance of the network by varying the nodes mobility. The metrics used to evaluate the performance are given below:

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Routing Overhead: This is the ratio of number of control packet generated to the data packets transmitted.

Network Throughput: Throughput is the number of data packets delivered from source node to destination node per unit of time.

The simulation area is a square field of 2000m X 2000m size, where nodes are placed uniformly. Mobility is chosen to be random way point, where each node chooses a random point and move towards that point with a random speed chosen between minimum and maximum values specified. The node then waits there for the specified pause time and continues it movement as described above. The bandwidth of shared wireless channel is assumed to be 2 MHz.

Table I: Simulation Parameter

Parameter	Value
Application Traffic	CBR
Radio Range	250 m
Packet Size	64 bytes
Transmission Rate	6 packets/sec
Speed	Random (0 – 20 m/s.)
Simulation Time	100 S
Number of Nodes	30
Area	2000m*2000m

Fig 2 shows the graph between packet delivery ratio and mobility of the network. The graph clearly depicts that Co-BDSR has greater packet delivery ratio compared to the DSR.

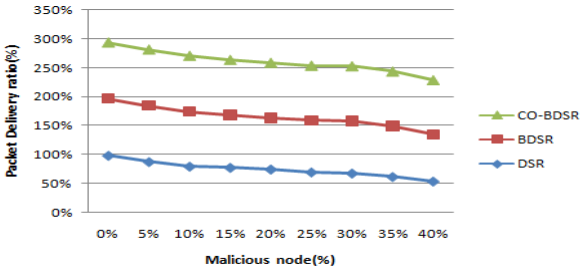

Fig 2: Packet delivery ratio

Fig 3 shows the graph between throughput and mobility of the network. The performance shows that our scheme provides better performance in case of Co-BDSR andBDSR.That is it ensures that packets are successfully delivered to the destination.

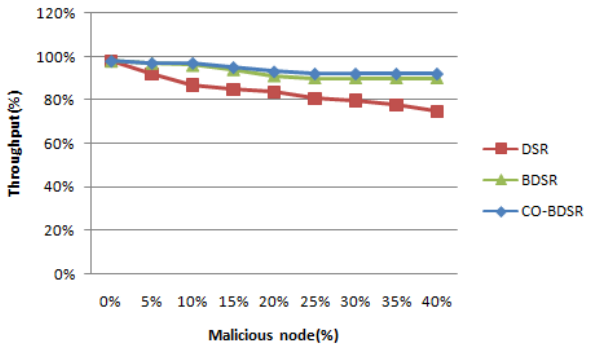

Fig 3: Network Throughput

Fig 4 shows the performance of the network in terms of overhead ratio. Graph is plotted between overhead ratio and mobility of the network. The performance analysis shows that our scheme reduced overhead ratio for Co-BDSR and BDSR.

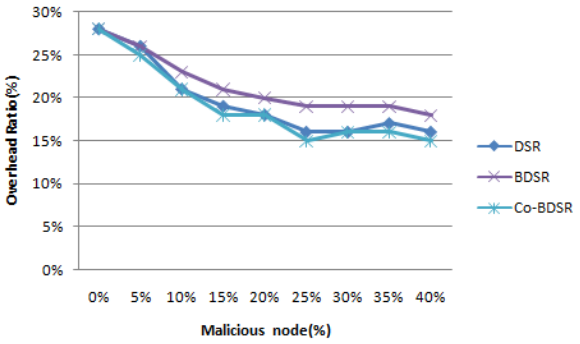

Fig 4: Overhead ratio

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.

9. 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, Co-BDSR and BDSR offers a greater packet delivery ratio and reduced end to end delay.In future work, it can be extended for the detection of gray hole attack thereby increasing the packet delivery ratio and reducing the end to end delay in the network.

10. 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] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol," Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145, 2011

[3] Irshad Ullah and Shoaib Ur Rehman," Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols," 2010

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

[5] 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.

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

[7] Latha Tamilselvan and Dr. V Sankaranarayanan," Prevention of Co-operative Black Hole Attack in MANET," Journal of Networks, VOL. 3, NO. 5, MAY 2008.

[8] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Security, volume (2) issue (3)