IMPROVED COOPERATIVE BAiT DETECTION SCHEME FOR DETECTION AND PREVENTION OF BLACKHOLE ATTACKS IN MANETS

Ravinder Kaur Gill 1, Simardeep Kaur 2

1,2Department of computer Science &Engineering, 1,2GZS Campus College of Engineering&Tech. Bathinda, Punjab, India

ABSTRACT:

MANETs are autonomous networks having mobile nodes that are self-configuring and self-organizing communicating with each other in an infrastructure-less environment. MANET often suffers from security attacks due to its lack of trusted centralized authority, open medium, dynamic topology, multi-hop routing etc. In between these attacks blackhole attack is dangerous active attack on ad hoc networks that can breach the security through routing misbehaviour and packet forwarding. CBDS is blackhole detection scheme, it works on the idea of bait destination address to find malicious nodes. In this paper, we propose an Improved CBDS (Cooperative bait detection scheme) for detection and prevention of black hole attack in network. This scheme detects both single blackhole attack and cooperative blackhole attacks in MANETs. This is done by observing the Sequence number and Neighbours of replying nodes. Our proposed technique has been simulated in NS2.35 by using DSR routing protocol. The effectiveness of proposed scheme is compared with CBDS approach.

Keywords: Cooperative blackhole attacks, Dynamic Source Routing (DSR), Mobile ad hoc network, Sequence number.

[1] INTRODUCTION

Mobile ad hoc networks (MANETs) are wireless networks composed of mobile nodes that communicate with each other in ad hoc manner without having to create any fixed infrastructure for deployment of nodes. Nodes in MANETs acts as host as well as router, therefore each node is responsible for relaying packets to each other through routing protocols. These networks are dynamic, having the capabilities of real time network for random motion of nodes to move in any direction to join or leave the network frequently or change their links by self-configuration. There is no centralised administration to provide authentication in network. MANETs faces various challenges such as dynamic changing network topologies, limited bandwidth, battery lifetime and computation power of nodes etc. These networks includes specific security concerns that may not be present in wired networks because of its open medium, scalability and portability. This makes network more vulnerable to attackers. There are various type of attacks that occurs at different
layers of network in MANETs. One such type of attack is Blackhole Attack occurs in the network layer. In this type of attack, malicious nodes tend to send fake route reply message to source node for having an optimal shortest path to the destination node. These malicious nodes reply quickly to source node, therefore sometimes source node choose their path without using any security mechanism and sends data packets through these malicious nodes. These nodes may either consume or drop data packets sent by source node rather than forwarding them to desired node. There are several schemes to detect blackhole attack in ad-hoc networks. Cooperative Bait Detection Scheme (CBDS) has been analyzed that detects blackhole attack. This scheme comprises three phases to detect malicious blackhole nodes in network. In the first phase of CBDS, Source node chooses address of its adjacent node as bait destination address and broadcasts Route Request message to bait malicious nodes to send replies. In the second phase of CBDS, reverse tracing phase is executed in which source node sends test packets. Nodes that drop these packets are considered as malicious. The route request phase is executed again with the address of the original destination. In last phase of CBDS, packet delivery ratio is determined if it falls to threshold value then the detection procedure would be triggered again to monitor the network. The bait destination broadcasting phase as well as reverse tracing phase tends to drop the packets and consumes large amount of energy of the nodes.

In our work, the proposed scheme detects blackhole nodes in network by considering the location of the nodes that has replied to the source node and sequence number of replying nodes in response to route request (RREQ) message. Nodes with exceptionally high sequence number than other replying nodes are also considered as malicious nodes. The proposed scheme has been implemented on NS2.35 to perform simulation. The performance of proposed scheme is determined in terms of energy consumption, packet delivery ratio and throughput. Rest of the paper is organized as follows: Section II presents the related work, Section III describes proposed Approach, Section IV presents Simulation results and Performance evaluation. Finally Conclusion and future scope are drawn in Section V.

[2] RELATED WORK
Many research works have been proposed for detection and removal of malicious nodes in MANETs. These existing studies deals with single blackhole node detection or some methods may require to cost much time and resources to detect cooperative blackhole attacks in networks. Some of these methods may require specific environments or assumptions to operate. In this paper we introduce various mechanisms used for detecting malevolent nodes in MANETs. We briefly illustrate different strategies related to our work.
Jian-Ming Chang et al. [1] Proposed a methodology to defend against grayhole and collaborative blackhole attacks performed by malicious nodes in MANETs by CBDS approach. Cooperative bait detection scheme (CBDS) integrates the advantages of both reactive and proactive architectures. In CBDS approach, source node selects its adjacent node stochastically to cooperate with this node with the intuition of using address of this node as bait destination address. An alarm is sent by destination node back to the source node when there is significant drop in packet delivery ratio. This method implements reverse tracing technique in order to detect and prevent malicious nodes from participating in routing procedure. After performing these operations of blackhole and grayhole detection data is transmitted in network through specific path selected by source node. Shivani Uyyala et al. [2] proposed a mechanism that detect and isolate blackhole attacks in MANETs through anomaly based intrusion detection scheme. This method uses monitoring nodes for detecting attacks in network, these monitoring nodes have unique id for distinguishing itself from other nodes. Monitoring nodes covers all its neighbours in network and observes their behaviour at network layer using anomaly based intrusion detection scheme. Golok Panda et al. [3] proposed an approach by using key authentication method which leads to prevent the inducer that carry black hole node.

Neelam Khemariya et al. [4] proposed an efficient approach for the detection and removal of the Black hole attack in the MANETs. Proposed approach is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. This mechanism detects both the single Black hole attack and the Cooperative Black hole attacks in network. It detects attacks when node is idle as well as in case when a node is not idle, threshold value for communication interval is used to check whether node is idle or not. Firoz Ahmed et al. [5] proposed an Encrypted Verification Method (EVM) to effectively detects blackhole attack in MANETs. In this mechanism detection node that receives reply (RREP) from suspicious node sends an encrypted verification message to destination node directly along with path for verification. This approach detects blackhole nodes and also reduces control overhead. This approach resolve problem through two steps: Firstly Identify suspicious node and then verify that suspicious node through an encrypted verification message, therefore malicious behavior of nodes such as dropping or absorption of message is detected significantly.

Nabarun Chatterjee et al. [7] proposed a technique to avoid blackhole node behaviour in AODV routing protocol by using Triangular Encryption in NS2. In this technique there is per agreement between sender and receiver of data on partition and the key of triangular encryption. Destination node in this method encrypts the plain text sent along with request (RREQ) packet from intermediate node by pre agreed partition and key along with reply (RREP) packet. The intermediate node update their index and hop count on receiving packet. So if the packet contains cipher text it reaches
destination node as blackhole node sends reply without consulting routing table. The sender node checks whether the packets has matching cipher text. Prachee N. Patil et al. [12] proposed a new approach for preventing blackhole node attack in DSR based route caching that makes use of normal time caching. On detection of blackhole node in MANET during the path construction, the blackhole node id is passed to path function of DSR. Paths are ready to be added in route cache in this function but before adding to cache these paths are parsed to verify presence of blackhole node id, if blackhole node appears that path is eliminated and rest of the paths are added.

[3] PROPOSED WORK (IMPROVED CBDS)
Our proposed work, aims at detecting and preventing malicious blackhole nodes in single step in MANETs. In this approach, the source node forwards the Route Request (RREQ) messages in the network to find route to destination node. All the nodes forward the RREQ message to their neighbouring nodes to get path for desired node and Route Reply (RREP) messages are being sent to the source node in response to RREQ message with their list of neighbours. The Replying nodes have route to the destination node and these are one hop neighbours of the destination node and these replies also contains reply from the black hole nodes as well. The source node will analyze the received neighbour list. If the replying node does not have destination node as its neighbor list that node is considered as blackhole node. The destination neighboring node can also act as malicious node by increasing its sequence number. As malicious nodes exceptionally increase their sequence number to claim of having fresh route to destination node and then intercept data packets on receiving data packets. So, as a prevention step, the source node will not choose the path containing the malicious nodes and shortest path for eligible nodes is determined by ignoring the path of these malicious node.
Flowchart of proposed Scheme

Algorithm

Nei = Neighbour set of nodes.
Rep = List of nodes that Replied to Source Node Claiming Path to destination node.
for x=1 : Rep
for y = 1: Nei
    if Rep(x), Nei(y) != Dst
        puts node Rep(x) in suspected list S
    end
end
end
for i=1:S # for all the nodes in suspected list
    if seq. no.(i) >> Avg. Seq. No.
        puts node s(i) in malicious list
    end
end

[4] SIMULATION RESULTS

We have used NS2 simulator to show the simulation results of the proposed scheme. The random waypoint mobility model is used for the communication between 50 nodes in the network that are distributed in the area of 1100*1100 m². The specifications of the simulation environment and the processes involved are shown in the table 1 below.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS2(2.35)</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>1100*1100 m²</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>50</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two ray ground model</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni antenna</td>
</tr>
<tr>
<td>Traffic Model</td>
<td>CBR</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250 m</td>
</tr>
<tr>
<td>Basic Routing Protocol</td>
<td>DSR</td>
</tr>
</tbody>
</table>

Energy Consumption

![Energy Consumption Graph](image)

Figure 1. Energy consumption

This factor is indicator of lifetime of the network. The simplicity of the proposed scheme has also been able to reduce the energy consumption in network. Figure 1 depicts that initial energy of 100
Joules is given to the network. The improvement in this factor has been found at 8.34 percent over CBDS. Energy is calculated by default in NS2 through energy dissipation model.

**Throughput**

![Throughput Analysis graph](image)

**Figure 2. Throughput Analysis**

It is the amount of data received at particular node per second. It is used to monitor the efficiency of network. The throughput values have been found to be impressive showing an increase of 49.5 percent over the CBDS.

\[
\text{Throughput} = \frac{\text{No. of packets received} \times \text{Packet size} \times 8}{1000}
\]

**Packet Delivery Ratio (PDR)**

![Packet delivery Ratio graph](image)

**Figure 3. Packet delivery Ratio**
PDR is ratio of number of packets successfully delivered to the number of packets sent. It indicates the efficiency of the scheme in delivering of packets in the network. Higher the packets received rate aggravates the performance of the network as shown in figure 3. The proposed scheme has shown an increase of 8.1 percent for the packet delivery ratio over CBDS.

\[
PDR = \frac{\text{Number of packets received}}{\text{Number of packets received} + \text{Number of packets dropped}}
\]

[5] CONCLUSION
The proposed work aims at detecting the black hole nodes successfully and reducing the packet loss in the network. The performance of the proposed scheme is compared with CBDS. The results were obtained in terms of packet delivery ratio, throughput and energy consumption in the network. All the three parameters showed an improvement over the existing scheme. The packet delivery ratio shows an improvement of 8.1 percent as compared to CBDS. The throughput of proposed scheme shows an improvement of approximately 49.5 percent as compared CBDS. The energy consumption parameter shows an improvement of 8.34 percent over CBDS. Thus it can be concluded that the proposed scheme which detects the black hole nodes by taking into consideration their relative positions with respect to destination has out performed the existing CBDS approach. It has not only detected the malicious node but also consumed lesser energy owing to its simplicity.

In future, this scheme can be applied to detect wormhole attacks that turns malicious at later stages by providing data to other malicious nodes. Also, Cryptographic algorithms described by various authors can also be combined with proposed algorithm to provide more security against the attacker nodes which tend to modify the contents of the data packets.

REFERENCES


