Comprehensive survey on Blackhole attack with various Detection/Prevention techniques in Ad-hoc network

Ayasha Malik1 Vishal Gupta2

1Department of Computer Science & Engineering, Ambedkar Institute of Advanced Communication Technologies and Research, New Delhi, 110031 India.
2Department of Computer Science & Engineering, Ambedkar Institute of Advanced Communication Technologies and Research, New Delhi, 110031 India.

Abstract
The flying evolution in communication technology has triggered to sturdy research interest on Wireless Networks. Ad-hoc networks are inherently very prone to number of security threats. Lack of fixed infrastructure, use of wireless link for communication and mobility of nodes make Ad-hoc networks extremely receptive to rival’s hostile attacks blackhole attack being one among them, which can be implementing effortlessly. This paper includes a brief description of black/dark hole attack and presented a comprehensive survey of its prevention techniques as given by some researchers. The main aim is to find how, when, and why an Ad-hoc network was compromised or involved in commitment with blackhole attack.

Keywords: Ad-hoc networks, blackhole attack, security, malicious, prevention, detection, RREQ- route request, RRES/RREP-route response/ route reply

I. INTRODUCTION
A. AD-HOC NETWORK
An Ad-hoc network is a group of autonomous nodes that are capable to self-organise, self- configure and self-arrange. These networks do not require any pre-existing or fixed infrastructure; therefore can be setup dynamically on demands. “Anytime, Anywhere, Any-condition and Anybody: communication is ready” is the goal fulfilled by Ad-hoc network due to its mobility, flexibility and dynamical change in topology.

Along with so many pros there are some cons also:- such as no safe borders, attack from malicious nodes into network, no centralized management facility, limited power supply, scalability, protection less channels, dynamic change in topology etc. but security is being a serious issue among them[1]

The communication between nodes in Ad-hoc network is done via radio waves. In an Ad-hoc network, a node can operate as sender, receiver and router as well. Communication/transmission in Ad-hoc network is done by means of memo/messages, Node can send the data to its nearest node through the messages. And these nodes don’t have any information about any other node i.e. whether the node is malicious or genuine. They all are stranger to each other. [7]

The ad-hoc/wireless networks are exceedingly unguarded to rival’s bitter attacks due to their essence. The open links of Ad-hoc network have to face much type of attacks [10] - blackhole attack is one among them. [16]

The rest of the paper is classified as: Section (B) discusses the route selection and communications between nodes. Section (C) elaborates the blackhole attack. Section (D) presents a detailed description of the communication/route establishment in Ad-hoc network in presence of blackhole node via flowchart. Section (E) classifies the nature of blackhole attacks. Section (II) provides the overview of the detection and the prevention methods of blackhole attack as proposed in the literature. Section (III) represents a table with a brief description of detection and prevention techniques of blackhole attack on the basis of their nature and limitations. Finally the paper concludes with section (IV) and then followed by references.

B. ROUTE SELECTION AND COMMUNICATION BETWEEN NODES IN AD-HOC NETWORK

Table 1: Network representation

<table>
<thead>
<tr>
<th>Node</th>
<th>Representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Source/initial node</td>
</tr>
<tr>
<td>D</td>
<td>Destination/goal node</td>
</tr>
<tr>
<td>A, B, C, E, F</td>
<td>Intermediate nodes</td>
</tr>
</tbody>
</table>
In figure-1 S wants to make relation with D, by means of communication. S broadcasts its RREQ packets along with the address of D to A and C, and wait for the RRES. Neighbours of A and C do the same until D get the RREQ packets. Whose RRES is received first by the S, that route get selected. As the route S-A-B-D is shortest route (with respect to hop count) as compare to route S-C-F-E-D from S to D, so RRES of route D-B-A-S is received by the S first and route S-A-B-D get selected. But as we know, Due to sudden change in network topology, it is possible that when S is communicating with D, suddenly A moves out from the range of S so that connection establishment goes OFF and now the network or S has to find a new/alternative path for communication. (S-C-E-F-D in this case)

C. BLACKHOLE ATTACK

A blackhole attack is one of the well-known serious security threats in Ad-hoc network. It is a kind of security attack. In this attack a malicious (fake) node, called a blackhole node, able to capture all data by conveying false routing direction, falsely holding an up-to-date or latest path to goal node, and then let fall them without delivered to the goal node. Blackhole attack degrades the performance of whole network, like packet delivery rate, payload, control packets and throughput, because of their simultaneously packet dropping behaviour and payload because of frequently route reorganisations. [14] It is a type of active attack, which attracts the node to become victim i.e. blackhole node forces the genuine node to make a communication relation with them.

These Blackhole nodes may perform various harmful actions on the network such as-

- Behaves as a Source node by falsifying the RREQ packet.
- Behaves as a Destination node by falsifying the RREP/RRES packet.
- Decrease the number of hop count, when forwarding RREQ packet. [14]

D. NATURE OF BLACKHOLE ATTACK

<table>
<thead>
<tr>
<th>Nature of Blackhole attack</th>
<th>Single blackhole attack</th>
<th>Cooperative blackhole attack</th>
<th>Grey hole attack</th>
</tr>
</thead>
</table>

In figure-2 Suppose A is a malicious/blackhole node, route S-A-B-D is selected for communication between S and D as it is the shortest (on the basis of hop count). After the connection establishment, S starts to send the data packets to A, when A receive the data packets then all the data packets are dropped by node.

These Blackhole nodes may perform various harmful actions on the network such as-
E. PROCESS OF BLACKHOLE ATTACK VIA FLOW CHART

In the present day of communication/connections, security is the pre-eminent study. It is really very important to prevent network from blackhole attack and provide safe communication in Ad-hoc network. These are the various methods/approaches which have been proposed to prevent from blackhole attack:

1. **PBHA (Prevention of a Blackhole Attack)/ Fidelity Table**: It is based on fidelity table/value, which is provided to every genuine user by default, when RREQ is broadcasted, source node has to be wait until it received RREP/RREP from adjacent nodes, then only that node is selected which have highest fidelity value, hence the threshold value also increases, for transmission of data. The
2. Blackhole attack detection using threshold value: - It is a detection method which is based on the Destination Sequence Number (DSN). In a network every node has a Threshold Value (TV) attach to it. When a RREP packet is received by the node, and then the comparison between DSN and TV is done. If the value of DSN is greater than TV then the node from where the RREP packet comes is said to be a blackhole node. But the drawback of this method is that, no regular updation in TV is done. The lower fake detection rate and higher true detection rate is achieved by regular updation in TV. [14]

\[ DSN > TV \quad //\text{Blackhole node} \]

3. Blackhole attack detection using dynamic threshold: - It is the extension of blackhole attack detection using threshold value method. This method is used to overcome the limitation of blackhole attack detection using threshold value method. In this approach, TV is lively update by intermediates node which is based on all live nodes of network and the time elapsed after it knows the last DSN. [14]

4. Recheck the blacklist: - It is a detection method based on membership time of blackhole node. That means every blackhole node in blacklist hold a membership time, which means only for that particular time it works as a blackhole node, after that it become a genuine node. So that, recheck the blacklist method is used to check this type of node from blacklist and make them free from blackhole node to make communication faster, but only when the membership time get expired and the node is not behaving like blackhole node. [14]

5. IDS (Intrusion Detection System): - The characteristic of Ad-hoc network is completely different as compared to wired network. So that we can’t able to apply IDS in ad-hoc network directly as we can use it in wired network. Before implementation of IDS in Ad-hoc network a kind of modification is applied on IDS. It is concluded that, because of distinctive features of Ad-hoc network intrusion detection is challenging. Prevention/Detection by using IDS can be implemented by using some approaches in Ad-hoc network. These are as follows:

- **IDAD (Intrusion Detection using Anomaly based Detection):** To prevent network from blackhole attack, host-based IDS is used by the IDAD. It is based on normal activities. IDAD presume that, it can scan every single activity of end user and system too; to identify abnormal activities throws by attacker from a pool of normal activities. Therefore, by uncovering abnormal activities of an attacker/blackhole node, the blackhole attack is detected. For this, pre-collected box of abnormal activities is required, named as audit data. After assembling of audit data, it is hand-over to IDAD system, and then a comparison is done between each activity of node with audit data on a fly. If the activities of both are matched up, the IDAD system checks that node first properly and if it found to be genuine then allows making further relation. Working of this system is based on principle “trusts no peer” i.e. nodes don’t depend on another node to prevent network from intrusion. It can detect novel attack (variations of blackhole attack) also. But it is time consuming and requires more computational resources. [1][11]

- **IDM/SD (Intrusion Detection using Misuse/Signature based Detection):** Intrusion Detection using Misuse based Detection method is also called as Intrusion Detection using Signature based Detection. It is based on pattern of attacks, i.e. for detection of blackhole node/attacker node in Ad-hoc network pattern of known attack is used. It is a very accurate method i.e. it have power to expose the attack immensely reliable in near real-time. This method has a limitation that it can’t be able to uncover the novel attack whose signature is not known as compared to another IDS method but the other side is, this method is better than other IDS method in computation and delay. It requires more time and more computational resources to identify the blackhole attack/blackhole node. [11]

- **IDSD (Intrusion Detection using Specification based Detection):** This method combines the strength of IDAD and IDM/SD method to uncover the blackhole/malicious node in network by using set of rules. It is quick as well as accurate. This approach is based on legal nature, generally succeed statements are used to differentiate legal program’s nature. It generates alarm only for illegal program’s nature which encountered in network, not for unusual (but legitimate) program’s nature. So that, false positive rate of IDSD reduces as compared to IDM/SD. This system can also detect unknown attacks [11][18]

- **fidelity value is regular updated by source node after receiving ACK from destination node. When destination node received data, it responded by an ACK packets to source node, and the source node has to add 1 to the holding fidelity value of the adjacent node. If no ACK is received by the source node then 1 is subtracted from the holding fidelity value, that means a possibility of malicious/ blackhole node on established path which dropped the data and prevent them to reached destination.[15][9]**
6. D-MBH (Detection of Multiple Blackhole) & D-CBH (Detection of cooperative Blackhole): - These are two algorithms which proposed in paper [11]. These algorithms can detect both nature of blackhole attack (single & collaborative). In first algorithm, source node sends a false RREQ with DSN of non-existent node to the all remaining nodes of ad-hoc network. The attacker node sends the RREP/RRES with high DSN because higher DSN represents fresh path. Then the second algorithm create the list of multiple blackhole/malicious node after calculating the average of DSN of all fake RRES/RREP, and found that RRES/RREP comes from blackhole/malicious node/s has/ve higher DSN in comparison to genuine RREP. This method reduces the routing overhead and computational overhead. [9][3]

7. BBN (BackBone Nodes) and RIP (Restricted IP):- BBN nodes are honest and strong in terms of battery power and range. Initially when the source node wants to make a data transmission, it requests the nearest BBN for a RIP. When BBN received the RIP request from source node then it answers with a fresh IP address, selected randomly from unemployed IP addresses. Then initial node broadcast RREQ to goal and to RIP concurrently. Now if the initial node received RREP/RRES only for goal node and not from that RIP, then there is no malicious node in network. And if source node received RRES/RREP for RIP, then it is clear, network has a/multiple malicious node. [9][19]

8. DRI (Data Routing Information) table and cross checking using FREQ/FREP: - This methods are introduced to identify blackhole attack. Each node in network maintains a DRI table. The DRI table keeps the record of each node that the node did transfer and receives the data with its neighbour nodes. If initial node has not path entry to goal node then initial node will forwards a RREQ message to its neighbour nodes to found a secure and fresh path to goal node. When any node gets this RREQ message then node may respond or may broadcasts it to whole network. If destination node replies for the route request, then every intermedial nodes reform or insert routing details for that goal node. When initial node get RREP from goal node then it will begin to forward packets with received route and update its DRI table on the basis of destination node and intermediate node. The proposed solution raise the graph in terms of performance and throughput rate including less amount of packet loss but mobility of node is to be considered as it should be low. [9]

9. RRT (Router Request Table) table and sequence numbers: - In this method, SN of source node or intermedial node are examine and a comparison done between existing DSN with the source node’s SN, if there is huge amount of difference between SNs, that means it is attacker node. This solution instantly removes that attacker node from the RRT. [9]

10. Protocols for preventing network from blackhole attack: - There are some protocols which help to keep secure the network from blackhole attack by providing secure routing between nodes-

   - DSDV (Destination-Sequenced Distance-Vector Routing):- It is a protocol, which is used widely in Ad-hoc network. It uses a DSN and dynamic TV to discover a current route to the destination node. It detects as well as prevents the blackhole attack in network. It required a regular updation in its routing worktables, which consume battery/cell power and bandwidth too; while the network remains inactive. Whenever the network change its infrastructure, a fresh succession number is required prior for network re-convergence; that’s why it is not suitable for huge lively networks [4]

   - AODV (Ad Hoc On-Demand Distance Vector):- This routing protocol used widely in Ad-hoc network. In AODV initial node initiates the path disclosure activity by posting a RREQ to entire network. Intermedial node participates in this activity by further scattering this RREQ to the way of destination node. Hence the process takes some time to sends RREP from destination node. A blackhole/malicious node does not aware and instantly post back a false (wrong) RREP/RRES packet to the initial node after make-believe that it has best path to goal. Hence, the initial node is able to know about blackhole node and ignore it as well. [6]

   - EAODV (Enhancement Ad Hoc On-Demand Distance Vector):- It is an enhancement on AODV. The main strategy of EAODV is that, the goal node will convey the RREQ/RREP to initial node at any point of time during data transmission. That’s why; when the current/new incoming RREP/RRES received to network from goal node then the entire existing path listed encircling blackhole/malicious nodes will be override by current RRES/RREP. Simultaneously, the testing of all accepted RRES/RREPs is done by the help of a heuristic approach taken from [14] in which a kind of detection and isolation is done over received RRES/RREP. EAODV protocol is an updation over AODV routing process. It uses two procedures to remove the blackhole attack; change
and update the logic expression of routes and secondly, add process detection and process isolation methods but the whole process takes some extra delay and extra energy usage. [6]

- **IDS-AODV/Switch the route**: IDS-AODV is a prevention method. The main strategy is that originally the data is travelled along with first organised path but if the second RREP/RRES appears then the data transmission is shifted to the second path. As this approach believes that the first RREP/RRES that received by source node is from blackhole/malicious node, therefore pay no attention to that RREP/RRES. This approach upgrades the packet delivery ratio but there is another side too. For example, if the second RRES/RREP received by initial node arrives through blackhole/malicious node, it is not avoided and the path selected which includes blackhole/malicious node. It is also called switch the route. But there is a problem, when destination node is nearer as compare to attacker/blackhole node then the first RREP/RRES received by initial node is from destination node not from attacker/blackhole node. In this case, the data send by source through the path which is established by malicious/blackhole node.[6]

- **IIDS-AODV (Improved IDS-AODV)**: It is the modification of IDS-AODV. This method was introduced to overcome the limitation of IDS-AODV. It is based on the checking of second RREP message. Initial working is same as that of IDS-AODV. The difference between IDSAODV and IIDS-AODV is, In IIDS-AODV when second RREP/RRES received by source node; firstly a test is performed using the BSN and RDSN. In the test of second RREP/RRES, difference between the BSN and RDSN is considered and then relate to the 50% of highest successive number (HSN) and result have to be less or equivalent to (HSN/2). Only if current/second RREP/RRES fulfilled the condition of test, then source node will move to this route. If this test fails, the source node will continuously to sending its packets along with the route that is selected by first RREP/RRES. [6] Broadcasted sequence number (BSN) is one of the fields of RREQ message and has been encountered earlier by the source for any kind of path which is on the way to destination and Received destination sequence numbers (RDSN) is a sequence number that is received from RREP message.

\[
\text{BSN} - \text{RDSN} \leq \frac{\text{HSN}}{2} \quad \text{//Route selected}
\]

- **WAODV (Watchdog AODV)**: In this method every node has a watchdog set with it to check neighbours node as the neighbours have to dispatch packets to their neighbours. If the packets didn’t dispatch by the neighbours node then it detected by the watchdog and that neighbour node declare as a misbehaving node/malicious node. This approach cannot able to uncover the malicious nodes in existence of equivocal and collisions of destination side, finite transferring power, directional antennas, false or mischief behaviour and imperfect dropping. [8][12]

- **REP (Recommendation Exchange Protocol)**: In this protocol each node can convey and take recommendations from neighbour nodes. REP protocol is based on trust which is developed by experiences and suggestions of nodes. [8]

- **OCEAN (Observation-based Coordination Execution in Ad hoc Networks)**: This protocol implemented to overcome the limitation of DSR routing protocol. It is an extension over DSR protocol. It uses two systems to detect malicious/blackhole nodes; first is monitoring system and second one is reputation system. But OCEAN fails to predict accurate result i.e. can’t able to uncover all malicious nodes. [12]

- **ODMRP (On Demand Multiple Routing Protocol)**: It depends on authentication i.e. for secure communication, first the routing messages authenticated by localized certificate chain method then broadcasted to neighbours node. [12] (For more kindly Refer 13)

- **BHS-ODMRP (Blackhole Secure-On Demand Multiple Routing Protocol)**: It is supplement of ODMRP. It is been applied over the top of the path invention procedure of ODMRP in which the safety favour is divided in more than one nodes and each node certify one another with in a self and well-ordered manner. [12]
<table>
<thead>
<tr>
<th>Methods</th>
<th>Type of attack</th>
<th>Limitation</th>
<th>Detection/prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBHA / Fidelity Table</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Routing overhead and end to end wait/delay is slightly higher than AODV.</td>
<td>Detection</td>
</tr>
<tr>
<td>IDM/SD</td>
<td>Sole blackhole</td>
<td>This method unable to detect novel attacks whose signatures are unknown. It required more time and more computational.</td>
<td>Detection</td>
</tr>
<tr>
<td>BBN and RIP</td>
<td>Cooperative/multiple blackhole and gray hole</td>
<td>Work only when total number of malicious node are higher than numbers of genuine nodes</td>
<td>Detection</td>
</tr>
<tr>
<td>RRT and sequence numbers</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Malicious/blackhole node act as source node and break security.</td>
<td>Prevention</td>
</tr>
<tr>
<td>DSDV</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>It is not for highly vibrant networks.</td>
<td>Prevention</td>
</tr>
<tr>
<td>AODV</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Extension in storage overhead, routing overhead and end to end wait/delay.</td>
<td>Detection and prevention</td>
</tr>
<tr>
<td>EAODV</td>
<td>Sole blackhole</td>
<td>The end-to-end wait/delay increases</td>
<td>Detection and prevention</td>
</tr>
<tr>
<td>IDS-AODV/Switch the route</td>
<td>Sole blackhole</td>
<td>Attackers upgrade tables when they listen channels</td>
<td>Prevention</td>
</tr>
<tr>
<td>WAODV</td>
<td>Sole blackhole</td>
<td>Failed in company of equivocal and acceptor smashing, restricted conveyance power, directional aerial</td>
<td>Detection</td>
</tr>
<tr>
<td>REP</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Failed when attackers capture the neighbour node to forge the fake reply packets</td>
<td>Detection</td>
</tr>
<tr>
<td>OCEAN</td>
<td>Cooperative/multiple blackhole</td>
<td>Fails to deal with misbehaving/blackhole nodes properly</td>
<td>Detection and prevention</td>
</tr>
<tr>
<td>ODMRP/BHS-ODMRP/Certificate chaining</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Overhead in implementing Private keys, issuing and checking certificate makes it costly and difficult and causes delay of about 15%</td>
<td>Detection and prevention</td>
</tr>
<tr>
<td>BDSR</td>
<td>Cooperative/multiple blackhole</td>
<td>The communication overhead is slightly higher than DSR.</td>
<td>Detection and prevention</td>
</tr>
<tr>
<td>Banned RREP</td>
<td>Sole blackhole</td>
<td>Failed when attackers capture the destination node to forge the fake reply packets</td>
<td>Prevention</td>
</tr>
<tr>
<td>Acknowledgment of RREQ</td>
<td>Sole and Cooperative/multiple blackhole</td>
<td>Blackhole node can dispatch a reply message if the key of some/a node are open to remaining nodes.</td>
<td>Prevention</td>
</tr>
<tr>
<td>ACO</td>
<td>Cooperative/multiple blackhole and gray hole</td>
<td>Failed when optimal route captured by the attacker.</td>
<td>Detection</td>
</tr>
<tr>
<td>CONFIDANT</td>
<td>Sole blackhole</td>
<td>It does not address partial packet dropping</td>
<td>Detection</td>
</tr>
<tr>
<td>DCM</td>
<td>Cooperative/multiple blackhole</td>
<td>Control overhead is higher than AODV</td>
<td>Detection and prevention</td>
</tr>
</tbody>
</table>
• BDSR (Baited-Black-hole DSR): - It is an extension of DSR and it can detect and avoid the blackhole attack. In this technique bait forwarded to attract blackhole node/malicious node to respond by false route direction. Therefore, it can achieve proactive detection and trace back the route to exact position of existing blackhole. That can minimize the opportunity to suffer blackhole attack after the establishment of the route. [17]

11. Banned RREP/RRES: - It is a prevention method that works on the principle of deactivates the entire respond/reply messages which return from the intermedial nodes. In banned RREP/RRES, the intermedial nodes are block to forward out RREP/RRES and therefore, only that reply messages are trusted which comes from actual destination node. In this technique, it is assumed those malicious/blackhole nodes are from intermedial node. That’s why intermedial nodes are prohibited to initiate any RREP/RRES data packet. In this approach, wait for route increases in big networks and may give a power to blackhole/malicious node that it can forward RREP/RRES at the place of destination node. [6]

12. Acknowledgment of RREQ: - In this technique which is based on cryptography techniques, when a node gets RREQ/RRES from third non-believable node then, ARREQ/ACK_RREQ received by initial node which is encoded by its shared key. So now the initial node has to decrypts it first, then performed again an encryption over it but now with destination’s public key and dispatch to initial node. Node is considered as genuine node, when goal node gets same message as sent. Otherwise RREQ/RRES is simply ignored. [8]

13. ACO (Ant Colony Optimization):- As the name indicate, it depends on the real world behaviour of ants and the method they use for finding food. This technique derived from incidental conveyance of colony by normal negotiator, known as artificial ants, when an ant moves along a route; it deposits a chemical called pheromone on it. As more and more ants travel along with that identical route, pheromone concentration of the route grows. The route with the maximum pheromone concentration is then chosen to be the optimal route. The same method is used in network to find optimal and safe route which is free from blackhole node. It is a detection method. [2]

14. CONFIDANT (Cooperative of Nodes, Fairness in Dynamic Ad-hoc Network):- It is a next genre of Watchdog. It uses a method which alike as Pretty Good Privacy for indicating countless amount of faith, secret authorization and authorized documentation. It permits node to do negative ratings to identify fake allegation. But it does not able to capture incomplete packet dropping. [12] For more kindly refer [5]

15. Certificate Chaining: - As the name indicate, certificate means authorization and chaining means number of nodes. In this method authentication is done via a chain of nodes, which is self-assemble and didn’t use any trusted third party. In certificate chaining, a set of digital certificates use to represent authentication that form a chain. The roles and responsibilities are equally divided to each and every node of network and achieved supreme level of node contribution. Each node of the network able to issue stored and distributes certificates to remaining node which lie in their radio communication range. A authorized document/certificate binds with node including its common/shared key and safety framework. Every single certificate is saved two times in a network, one for the issuer node and the other for whom it is issued. Neighbours of a node are responsible to update certificates and adding new certificates too. If there is clashing in certificates, i.e., one common/shared key to many nodes or one node having many of common/shared keys, then there is chances to found a malicious node in the network who has issued a fake certificate. [12]

16. DCM (Distributed and Cooperative Mechanism):- This solution can avoid, detect and mitigate the multiple blackhole attacks. DCM includes four sub-modules with it. These modules are Assemble the Local Data, Local Identification, Co-operative sub-modules with it. These modules are Assemble the Local Data, Local Identification, Co-operative Identification and Universal Identification, Co-operative Identification and Universal Response. [For more, refer 17]

III. CONCLUSION

The paper opens up with the introduction of Ad-hoc networks, their characteristics and the limitations that make them even prone to various security attacks. In this paper, we have discussed the Blackhole attack in Ad-hoc networks. The paper presents a comprehensive survey on the detection and prevention techniques of blackhole attack in Ad-hoc networks as proposed by different researchers. Finally, the paper concludes with a comparative study of the different prevention and detection techniques on the basis of their limitations and the nature of blackhole attack that they deal with.

REFERENCES


