Review on Prevention and Detection of Black hole Attack in MANETs

Sampada H K[#1],Dr.Shobha K R[*2],Rakhi S[*3]

[#]*Assistant Professor, Electronoics and Communication, Atria I T, Bangalore,India*

[*]*Associate Professor, Telecommunication Engineering, MSRIT, Bangalore,India*

[*]*Assistant Professor, Electronoics and Communication, Atria I T, Bangalore,India*

***Abstract*—MANET(Mobile Ad-hoc NETwork) is an infrastructure less, dynamic, decentralized network. Any node can join the network and leave the network at any point of time. Due to its simplicity and flexibility, it is widely used in military communication, emergency communication and academic purpose. In MANET there no infrastructure hence each node acts as a host and router. They are connected to each other by peer-to-peer network. Due to the dynamic nature of Mobile Ad-hoc Network, it is more vulnerable to attacks. Since any node can join or leave the network without any permission the security issues are more challenging than other types of network. One of the major security attacks in Ad-hoc networks is the black hole attack. It occurs when a malicious node referred as black hole joins the network. The black hole conducts its malicious behavior during the process of route discovery. For any received RREQ, the black hole claims having route and propagates a faked RREP. The source node responds to these faked RREPs and sends its data through the received route. Once the data is received by the black hole, it is dropped instead of being sent to the desired destination. This paper discusses some of the techniques put forward by researchers to detect and prevent Black hole attack in MANETs. Further a comparison table is made for the existing solutions to black hole attacks in MANETs.**

***Index Terms*—MANET; MANET Architecture; Black Hole; Security; Attacks; DoS**

I. Introduction

The growth of smart electronic gadgets since 1990's like laptops PDA's, WI-FI networks have made MANETs a popular research topic.

Mobile Ad-hoc[1], networks are temporary and short range networks formed when all the devices use the same protocol, without any subscription service. They are also infrastructure less wireless networks. That is they don't require a base station to communicate and can be deployed very fast in any of the remote places. Usually form a LAN network and communicate through WI-FI (802.11 Standards). They do not have a central control hence the nodes are free to move in any direction wirelessly. This leads to unique routing and communication challenges in MANETS. For example, each node should have full knowledge of the topology changes and need to constantly communicate topology information when a node leaves or enter the network. The mobile nodes in MANETs keep exchanging their topology changed information which may lead to additional traffic in the network. MANETs[2], are called the peer-peer network in which the nodes can communicate with each other only if they are in each other's range. MANETs are also self-configurable and self-healing networks. They don't have clear boundaries. Each node should perform three duties a host or a router or an intermediate node. Intermediate nodes will participate in communication even if the traffic is not intended to them. A node can be a computer, phone, laptop etc. They can form instant networks as they are self-configuring. A MANET can act as a standalone (Fig. 1) network or can be connected to the internet through a router or a gateway(Fig. 2). MANETs have their applications[3], in almost each and every field like in education field as virtual classrooms, in military as automated battle field, in automation

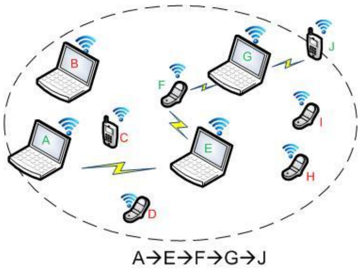

Figure 1: Example standalone MANET

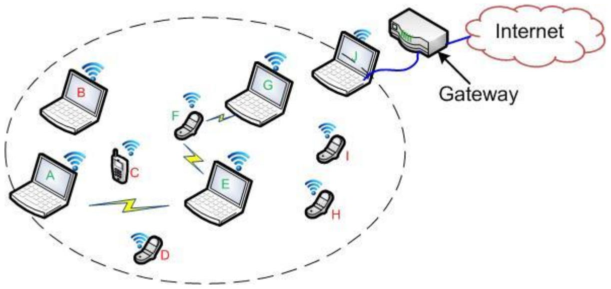

Figure 2: Example MANET connected to internet

industry as VANETs. Also for a common man for remote billing purpose, in rescue systems usually where the entire infrastructure is demolished. Thus MANETs are an important research topic.

II. Requirements, Characteristics, Advantages and Challenges of MANETs

A. *Requirements*

In MANETs, security is a key requirement as it is infrastructure less decentralized network of mobile nodes and the nodes have to trust each other for communication. In addition:

- Reliability: Each node should rely on its neighboring node to communicate because there is no central checking point.
- Availability: As the topology is dynamic and nodes are free to join or leave the network availability of nodes for communicationis an important requirement.
- Scalability: The MANET should also be scalable i.e., more number of nodes should be able to communicate efficiently.
- Quality of Service: Is a major requirement of any network either wired or wireless network i.e., the efficient usage of the available bandwidth, Packet Delivery Ratio etc.

B. *Characteristics*

Following are the primary characteristics of MANETs:

- Distributed Operation: Unlike traditional networks, MANETs do not have centralized control. Nodes are autonomous and participate as hosts and also as routers. Thereby, nodes must trust each other, communicate and route the packets to destination.
- Multi-hop Routing: If a node wants to communicate with other node which is not in its communication range the message should be relayed through the intermediate nodes.
- Dynamic topology: As the nodes move continuously with different speeds the topology of network changes.
- Shared Physical Medium: The medium for communication is wireless hence cannot be restricted to any user.
- Power Limitation: Nodes are small and are light weight thus having limited memory. They have to keep moving, search for the routes and also send and receive packets, so the battery gets drained off very fast.

C. *Advantages*

Following are the primary advantages of MANETs:

- Do not require any dedicated packet routing infrastructure.
- Allows for establishing communication in areas where it is challenging to build/install traditional network infrastructure.
- Significantly reduce cost and maintenance effort needed.
- Since nodes dynamically establish connection with new nodes, there is no setup/configuration requirement for adding new nodes.
- Highly scalable with greater resilience against link failures due to dynamic nature of the network.

D. *Limitations*

As discussed above, MANETs have several advantages and can be game changing in enabling next generation network technologies. However, the dynamic nature of the network and inherent dependence of nodes for transmission poses unique challenges to enabling such networks. These are some of the major challenges for MANETs:

- Reliability: Each node should rely on its neighboring node to communicate because there is no central checking point.
- Hidden terminal: The hidden terminal problem refers to collision of packets at the receiver end. The receiver might be in the communication range of multiple transmitting nodes which might themselves be invisible to each other. This could potentially lead to simultaneous transmission of packets from both transmitting nodes at the same time leading to collisions at the receiver.
- Packet Loss: Ad hoc networks experience a much higher packet loss due the very dynamic and continuously changing topology, frequent node movements, interference etc.
- Mobility induced route changes: Dynamic topology tend to change the routes very often.
- Security: Although security is an important concern for all types of communication networks wired or wireless, Ad-hoc networks are much prone to security attacks due to their inherent nature of dependency on other nodes.

III. Routing Protocols in MANETs

Routing protocols play an important role in selecting an optimal route from the source to the destination with minimum overhead and less bandwidth. There are some of the popular routing protocols found in literature:

Proactive or Table driven[7]: The entire information of the different nodes connected in the network is stored with each node and periodically the nodes update information of the topology changes in their routing table e.g. DSDV, OLSR, WRP, CGSR, FSR. Advantage is immediate route selection with increased bandwidth but more overhead.

Reactive or On Demand[4]: As the name indicates routes are discovered on demand. If a source wants to communicate with some other node, the route selection starts by route request flooding packets. So does not require continuous updating of the topology changes.AODV, DSR, ABR, ACOR are popular examples. While these protocols require lesser bandwidth, increased latency is a major challenge.

Hybrid[4][5]: Can be proactive or reactive depending on the application or the requirement of the user. E.g. TORA, ZRP, LANMAR, OORP, ARPAM, HSR etc.

A. AODV Protocol Overview

AODV routing protocol is a reactive routing protocol and hence routes are determined only when needed [13][14][15]. Fig. 3 shows the message exchanges of the AODV protocol. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message to all its neighbors. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) to that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the node has not received this RREQ before or if it not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, initiating the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it validates the route and reinitiates route discovery if necessary.

Advantages:

- Having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination.
- The connection setup delay is lower.

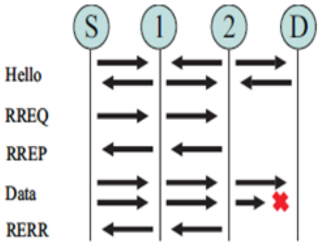

Figure 3: AODV protocol messages.

Disadvantages:

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.
- Multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead.
- Periodic beaconing leads to unnecessary bandwidth consumption.

B. Dynamic Source Routing

It is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Determining source routes requires accumulating the address of each device between the source and destination during route discovery [15]. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply).

To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used[12]. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route.

Dynamic source routing protocol (DSR) is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on-demand routing protocols is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. The destination node, on receiving a Route Request packet, responds by sending a Route Reply packet back to the source, which carries the route traversed by the Route Request packet received.

Consider a source node that does not have a route to the destination. When it has data packets to be sent to that destination, it initiates a Route Request packet. This Route Request is flooded throughout the network. Each node, upon receiving a Route Request packet, rebroadcasts the packet to its neighbors if it has not forwarded it already, provided that the node is not the destination node and that the packet's time to live (TTL) counter has not been exceeded. Each Route Request carries a sequence number generated by the source node and the path it has traversed. A node, upon receiving a Route Request packet, checks the sequence number on the packet before forwarding it. The packet is forwarded only if it is not a duplicate Route Request. The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same Route Request by an intermediate node that receives it through multiple paths. Thus, all nodes except the destination, forward a Route Request packet during the route construction phase. A destination node, after receiving the first Route Request packet, replies to the source node through the reverse path the Route Request packet had traversed. Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself). This route cache is also used during the route construction phase.

Primary Advantage: This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach.

Primary Disadvantage: In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as in proactive routing is not required.

IV. Security Concerns

Security in MANETs is a major concern because of the wireless links, unreliable nodes, node dependence for communication, bandwidth limitation and dynamic topology.

Any network's goals are authentication, confidentiality and integrity. Attack on a network can be either passive or active. Passive attacks can be further classified as release of message contents and eaves dropping. Active attacks are masquerade, replay, denial of service, modification of messages. Different OSI layers have different attacks; black hole attack is one of the network layer attacks.

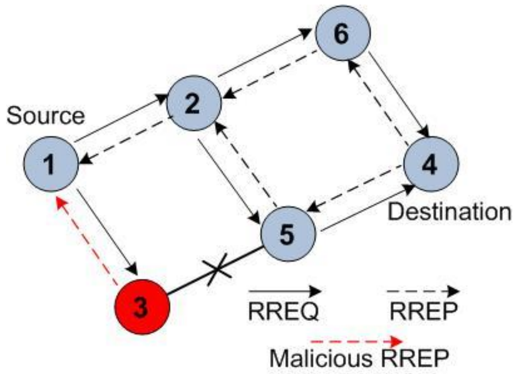

Figure 4: Example of black hole attack

V. Black Hole Attack

It is one of the network layer attacks also called denial of service attack where the actual node is denied of its service. A router or an intermediate node which had to forward the packet to the destination actually drops or discards the packet [8][9]. Because the MANET nodes are prone to packets loss due to various reasons it is very hard to detect a malicious node/router.

The malicious node (Fig. 4) can discard all the packets which can be detected by neighboring nodes and can further discard it from the network. But if the malicious node discards specific packets at specific time in specific routes it is very difficult to detect and discard the malicious nodes as the traffic still flows. Usual routing procedure from source to destination, is the source floods the route request packets to all the nearest neighboring nodes[10], the node which has the nearest path to destination will reply first and the source chooses that path. But a malicious node will send the reply before any other node in the network so that the source chooses that path and it can drop all the packets and create a black hole in the network. There can be collaborative attacks where more than one malicious node will join and launch the attack together and they are very dangerous and cannot be very easily detected.

VI. Related Work

In this section, we provide a detailed survey on related work. A summary of approaches and solutions proposed so far is provided in Table 1.

Piyush et.al [9] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

Chen et al. [10] presented a solution consisting of two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. According to their solution, each node involved in a session must create a proof that it has received the message; when source node suspects some misbehavior, Checkup algorithm checks intermediate nodes and according to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm. This solution may generate high traffic and computational cost of detection algorithm due to the basic limitations of gossip protocol and aggregate signatures.

An approach is discussed by Lathaet. al [11] in which the requesting node waits for a specific time for replies from neighbors that include the next hop details. After the specific time, Collect Route Reply Table is verified to know whether there is any repeated next-hop-node or not. Existence of repeated next-hop-node in the reply paths indicates the truthful paths or limited chance of malicious paths. Though, the process of finding repeated next hop node increases overhead.

DPRAODV protocol is proposed by Payal et al. which is based on maintaining a list of blacklisted nodes [12]. A pre-determined threshold is set to determine when a given node needs to be blacklisted. Also an ALARM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. The protocol has higher routing overhead due to addition of the ALARM packets.

Ruthvij H et al. [18] have proposed a new routing algorithm MR-AODV which is an improvement over R-AODV for the detection of malicious node. The author has made an attempt to improve the MANET performance by modifying the node functionality receiving the RREP from a malicious node in R-AODV to modified R-AODV. The process of detecting a malicious node is same as in R-AODV by detecting the PEAK value periodically which has the destination sequence number of the received packet. In R-AODV if a malicious node is detected by any node, the respective node will attach a *DO_NOT_CONSIDER* tag to the reply and resends the reply back to the source through the intermediate nodes so that all the intermediate nodes also will update in their routing table that node as malicious node. But in MR-AODV, when the malicious node is detected by a node, it updates the routing table as a malicious node and discards the RREP from the malicious node. Here it does not put the tag as *DO_NOT_CONSIDER*and the RREP [13][14], is not sent back to the source. Instead in the next RREQ the malicious node list will be attached so that the intermediate nodes will not receive any reply from the malicious nodes, only the genuine replies will be accepted.

Tamilselvan et al. [19] have proposed a solution for the black hole attack using AODV routing algorithm. It will wait and check the replies from the various neighboring nodes before choosing the preferred route for the destination. The source node sends request to all the neighboring nodes, if the neighboring node is the destination node it will reply or will send the request further to its neighboring nodes. The source node then receives reply along with the sequence numbers and the time of packet arrival from various nodes makes an entry in another table called ‘Collect Route Reply Entry Table’ (CRRT). After receiving the first reply it sets the ‘Timer Expiry Table’ for collecting the further requests from the various nodes. After the time out it will check the various replies from all the neighboring nodes to find if there are any repeated next hop nodes in the replied paths it assumes that the path is less prone to malicious nodes and chooses that path for reaching the destination.

MoitreyeeDasgupta et al. [20] has given a very new approach called ABM (ANTI BLACKHOLE MECHANISM).The idea is to isolate the black hole nodes from the network. New set of nodes called IDS (intrusion detection system nodes) are deployed throughout the network. IDS nodes are placed at places where they can see and observe the maximum neighboring nodes. IDS nodes keep observing the traffic being exchanged between various nodes; it maintains two tables called RQ(route request) table and SN(suspicious node) table. In RQ table the various request messages RREQs from various nodes and to whom the neighboring nodes further send requests are maintained. In SN table suspicious node table, the replies from various neighboring nodes are maintained. If a node behaves suspiciously that is, it never forwards any of the RREQs and only replies RREPs for the requests it may be a black hole behavior and such nodes are entered into SN table. After this block messages are flooded into the network indicating the malicious nodes from the SN table and the suspicious nodes are eradicated from the network.

In [21] Isaac et al. gives a novel method to detect and prevent the black hole attack. The scheme can identify two things black holes nodes and also checks all the existing routes by acknowledgement mechanism between the source and destination hence find the authenticated route to destination. The algorithm DBA-DSR is a modified DSR algorithm. The DSR request and reply packets have various field like source address, destination address, hop count etc. The algorithm modifies The DSRs request and reply packets to having a new field in the packet called the RREP initiator field and the fake RREQ which tells the address of the node sending the reply for the request. This is a little different from the regular DSR, the source node initiates the fake RREQ to a fake destination address which does not exist with a fake sequence number. If the intermediate node is not malicious node it simply sends the RREQ to its neighboring node. But if it is a malicious node it creates a fake RREP with a created destination address and sends the reply to the source node. The source node traces back the replied node and records the address in the black hole node list.Then the regular DSR algorithm starts where the source sends the original RREQ packet to all the neighboring nodes, if the reply is from the destination node then the node is authenticated node but, if the RREP comes from an intermediate node, the RREP will be checked by sending an ACK packet again to the destination node.If the destination node sends back the ACK to the source node then the route is safe or if some malicious action is noted then that route is avoided further.

In [22] Mehdi Medadianet. al has given a simple yet very effective way to determine the malicious nodes in the network. Activities in the node show the honesty of the node. If the node has to participate in any communication in the network it has to give a honesty test. As soon as the source node sends the request for the route to the destination, many nodes reply that they have the shortest route to the destination, if a node replies first its honesty is tested by asking the neighboring nodes, if they give the positive response like yes the node has delivered many packets to the respective destination then the node is said to be honest. If the reply is, it has received many data packets but never forwarded them either to the destination or to its neighboring nodes then the behavior is considered malicious

In [23] Ms Monika et al. has studied the various environments of the MANETs with and without the malicious nodes and come up with a new algorithm called SRD-AODV (Secure Route Discovery for AODV). The algorithm is purely based on the destination sequence numbers for a small, medium and large scale network of MANET nodes. Some calculations are provided for say a small network what can be the maximum and minimum allowable sequence numbers similarly for a medium and large network with and without the malicious nodes.

In [24] Keechan et al., a method for detecting black hole attack has been proposed with two main concepts i) Maintaining the routing table. ii)Checking the reliability of the node. Maintaining the routing table is to record the information of from the node through the node and to the node. This information is stored as bits. For example, if the RIT (Routing Information Table) says 111. The node is reliable as all three fields are true. A value of '1' indicates *true* and '0' indicates *false*. The node has participated as a source node or intermediate node or as destination node. The reliability check is that at least 2 of the three bits have to be true for the node to be a legitimate node.

In[25] Gayathri et al. gives a new method called real time monitoring system was developed. When a source node wants to send some data to the destination node it sends RREQs to all its neighbors. If a node is the destination node it sends the RREP to the source node. If it is not the destination node it forwards the RREQ to its neighbor again. In real time monitoring system if a node's behavior is found malicious it instructs its neighbors to overhear/listen to what the suspected node is doing whether it forwards the packet [26]. To do this the neighboring node of the suspected node puts itself in the promiscuous mode and keeps a watch on the suspected node it maintains *'fcount*' and a*'rcount*'. Finally neighboring node will forward packets to suspected node until *'fcount*' reaches a threshold value; thereafter if the '*rcount*' is still 0 then the malicious behavior is confirmed.

In [28] Saurabh Gupta et al.have proposed BAAP: Black Hole Avoidance Protocol for wireless network is a protocol which successfully avoids black holes in wireless MANET network. It uses AODV protocol for route discovery. When the neighboring nodes respond to the source about the path to the destination on one of the several paths are chosen by the source. In BAAP every node maintains a legitimacy level of their neighbors. There are additional fields added to the AODV packet like the *first_hop* field containing the IP address of the first hop after the source. In addition to this, the reply packet in BAAP has the source IP address information [27]. Legitimacy table contains three fields: Node ID, PathCount and SentCount. Node ID field stores the IP address of the node whose legitimacy is being recorded. PathCount field specifies the number of times the node has been chosen in the route and the SentCount field describes the number of times connection to destination have been successful node through the Node ID. These two count field are also used to define the Legitimacy Ratio [SentCount/(PathCount+1)] of a Node ID which indicates the confidence of node in performing its intended function of correct routing. A higher legitimacy ratio means higher possibility of a node being non-malicious.

In [29], Fidel Thachil has proposed that every node keeps track of the trust value of its neighbors. This is required for detection of malicious node which is doing selective packet dropping. Each node listens to its neighbor silently to know whether the node is receiving and sending the packets or not. A caching mechanism is implemented at every node to collect the packets forwarded by the neighboring node, if the node cannot tap the same packet as sent it decreases the trust value if the trust value reduces below a threshold value the node is determined to be a malicious node and will be avoided eventually.

In [30] authors have planned for the modified Extended Data Routing Information (EDRI) [31] algorithm and Negative Acknowledgement (NACK) algorithm. The work is in three steps i) Design a modified EDRI algorithm. ii) Design of NACK algorithm. iii) Remove the black hole and gray holes from the network. The EDRI table has a FROM and THROUGH fields. FROM field indicates the node has acted as a source. THROUGH field indicates that the node acted as intermediate node. These fields help in knowing the nodes better. The NACK indicated negative acknowledgement, the source after receiving the RREP from the neighboring nodes, the source node after sending the data will ask for acknowledgement back to source for further confirmation.

In [33] it is mentioned that, every IDS node executes a mechanism, called an ABM (Anti-Blackhole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold, a block message is broadcasted by nearby IDS, giving notice to all nodes on the network to cooperatively isolate the malicious node. The Block message contains the issuing IDS [32], the identified black hole node, and the time of identification. Upon receipt of a Block message issued by IDS, normal nodes will place the malicious node on their blacklists, thus, the AODV routing protocol for normal nodes must be slightly revised.There are three assumptions in this paper: i) two neighboring IDS nodes are located within each other's transmission range in order to forward Block messages to each other. ii) An authentication mechanism exists in MANETs, wherein, a node ID cannot be forged, and the block message sent by the IDS node can be modified and counterfeited. iii) Every IDS is set in promiscuous mode in order to sniff all routing packets within its transmission range.

In [34] Jaydeep Sen et al. present detailed analysis and provide experimental details to evaluate the effect of blackhole attack on AODV protocol in MANET.

TABLE I. COMPARISON OF DIFFERENT ALGORITHMS

Algorithm	***Key Features***	***Limitations***
Backbone network	• End-to-end checking between the source and destination. • Backbone network if checking fails.	• End-to-end checking increases delay and overhead.
Key management algorithm	• Gossip protocol. • Detection algorithm based on legitimate signatures.	• Signatures can be fabricated.
CRRT Table	• Repeated next-hop-node.	• Extra table along with routing table, time delay.
DPRAODV	• ALARM packet is sent along with RREP reply packet.	• Cannot detect cooperative black hole attack.
MR-AODV	• Improvement over R-AODV. • PEAK value determined periodically having the destination sequence number of the received packet.	• Destination sequence number can be manipulated.
AODV	• Wait for the replies from all the neighbouring nodes. before choosing the preferred route.	• Waiting time is more, by the time route is discovered topology may change.
ABM	• IDS nodes deployed through the network. • IDS work in promiscuous mode.	• Extra RQ and SN tables have to be maintained.
DBA-DSR	• ACK packets to detect black holes nodes • Determines the authenticated route among the various routes.	• DSR is not a preferred algorithm because of its limitations.
Honesty	• Honesty test for nodes to participate in the network	• Cannot detect cooperative black hole attack.
SRD-AODV	• The algorithm is purely based on the destination sequence numbers for a small, medium and large scale network of MANET nodes	• Need to do analysis before going to the actual algorithm.
Modified routing table	• Routing table check having FROM, TO, THROUGH fields	• Increased overhead.
Real time monitoring system	• overhear/listen to what the suspected node is doing	• Neighbours can lie.
BAAP	• First_hop field contains the IP address of the first hop • Legitimacy level of each node maintained	• False positives.
Trust value	• Caching mechanism is implemented at every node to collect the packets forwarded by the neighbouring node. • If the node cannot tap the same packet as sent it decreases the trust value	• False positives.
Modified EDRI	• Modified extended data routing information algorithm. • NACK negative acknowledgement algorithm.	• Lot of extra fields in the packet needs memory.
EDRI table	• Negative ACK packets with fabricated destination. address sent to detect malicious nodes.	• Not as effective as MEDRI.
Simulation	• Simulation experiments to evaluate the effect of blackhole attack on AODV protocol in MANET. •	• No with the practical scenario.
Association based Routing	• This trust value based on the experiences that the node has with its neighbour nodes.	• False positives.

First the black hole attack is explained in detail with the help of 7 nodes with some mobility speed, different scenarios like the link breakage and how the data gets lost in the network. Next, a black hole node is created and studied and the various performance matrixes are evaluated with and without the black hole nodes. The author has taken four scenarios of defined parameters for the simulation with or without black hole node. Several variations including different types of nodes (black hole or regular), positions and mobility factors are used in the simulations. The metrics used to evaluate the performance are packet loss percentage, throughput and end-to-end delay. The results of the simulation show that the packet loss in the network with a blackhole increases beyond that dropped by the blackhole node. This is due to increased congestion in the routes toward the blackhole node.

Ming Yang et al. [35]: This paper presents the extension of Association based Routing which is to be applied over the DSR protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experiences that the node has with its neighbor nodes [37].

Three types of associations are proposed in[37] are as shown below:

- UNKNOWN: Trust levels between them are very low, Probability of malicious behavior is very high, newly arrived nodes are grouped in to this category.
- KNOWN: Trust levels between them are neither low norhigh; Probability of malicious behavior is to be observed.
- COMPANION: Trust levels between them are very high; Probability of malicious behavior is very less. The Association status depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. The technique proposed a very simple equation for the calculation of trust value.

R1= Ratio between the number of packets actually forwarded and number of packets to be forwarded [38].
R2 = Ratio between total number of packets that are received by node and node should forward and the total number of packets sent by node's 1-hop neighbourhood and are not destined for another neighbour or to itself. If the denominator is not zero and R2 = 1.
A = Acknowledgement bit. (0 or 1)
T = Estimated Trust value
T = *tanh*(R1+R2+A)

As an improvement over DSR[40][41], a novel route cache mechanism was proposed by Prachee et al. for black hole detection [39]. During the process of path construction, the detected black hole node ID is passed to the path function of DSR. This node ID is checked before updating the route cache information and hence paths with malicious nodes are eliminated. The algorithm proposed in [39] uses normal time caching leading to reduced delay. Thereby, this approach is faster than previous black hole detection mechanisms.

VII. Conclusion

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper, we first summarise the pros and cons with popular routing protocols in wireless mobile ad hoc networks. Then, the state-of the-art routing methods of existing solutions are categorized and discussed. According to this work, we observe that both proactive routing and reactive routing have specialized skills. The proactive detection method has the better packet delivery ratio and correct detection probability, but suffered fromthe higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packetloss in the beginning of routing procedure. Therefore, we recommend that a hybriddetection methodwhich combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kind of routing detection used. The black hole problem is still an active research area. This paper will benefit moreresearchers to realize the current status rapidly.

References

[1] Ian D. Chakeres, Elizabeth M. Belding-Royer, "AODV Routing Protocol Implementation Design," IEEE/ACM *24th International Conference on Distributed Computing Systems Workshops* (ICDCSW'04), Vol. 7, pp. 698-703, 2004.

[2] Nadeen A, Howrath M P, "A Suevey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," *Communication Surveys & Tutorials*, Volume 15 Issue 4, pp. 2027-2045, 2005.

[3] Rath M, Patnayak B K, "A methodical Survey on real time applications in MANETs: Focussing key issues," IEEE *International Conference High Performance Computing and Applications(ICHPCA)*, pp. 1-5, 2014.

[4] Patel D N, Patel S B, KothadiyaH R, Jethwa P D, Jhaveri R H, "A Survey on reactive routing protocola in MANET," *International Conference on Infromation Communication and Embedded Systems(IICICES)*. pp. 1-6, 2014.

[5] Sivakumar D, Suseela B, Varadharajan R, "A Survey of Routing Algorithms in MANET," *International Conferenec on Science and Management*, pp. 625-640, 2012.

[6] Venkanna U, Veluswamy R L, "Black Hole attack and their counter measure basd on management," *3rd International Conference on Adavnces in Recent Technologies in Communication and Computing*, pp.232-236, 2011.

[7] Shenbagapriya R, Kumar N, "Survey on proactive routing protocols in MANETS," IEEE *14th International Conference on Science Engineering and Management(ICSEMR)*, pp. 1-7, 2014.

[8] Sarma k j, Shama R, Das R, "A Survey on Black Hole detection inMANET, " IEEE , .pp. 202-205, 2014.

[9] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks," *2nd international conference on Ubiquitous information management and communication*, pp.310-314, 2008.

[10] Chen Wei, Long Xiang, Bai Yuebin and Gao Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks, " Second IEEE *International Conference on Communications and Networking*, pp. 366-370, 2007.

[11] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET," *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, pp. 21-26, 2007.

[12] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based Manet," *International Journal of Computer Science Issues*, Vol. 2, Issue 3, pp: 54-59, 2010.

[13] Charles E. Perkins and Elizabeth M. Royer, "Ad-Hoc On- Demand Distance Vector Routing", *Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[14] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV," *International Journal of Computer Science and Network Security*, vol. 10, No. 4, pp. 12-18, 2010.

[15] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based Manet," *International Journal of Computer Science Issues*, Vol. 2, Issue 3, pp: 54-59, 2010.

[16] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Solution for Grayhole Attack in AODV Based MANETs," Springer, *In Proc. Of Third International Conference on Advances in Communication, Network and Computing*, pp. 60-67, 2012.

[17] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs," INFOCOMP *Journal of Computer Science*, Vol. 11 No. 1, pp. 1-12, March 2012.

[18] Rutvij H. Jhaveri "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs," IEEE, *Third International Conference on Advanced Computing & Communication Technologies*, 2012.

[19] Latha Tamilselvan , Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET," IEEE, *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 2007.

[20] Moitreyee Dasgupta, Debarpita Santra, Sankhayan Choudhury, "Blackhole prevention mechanism in Mobile Ad-hoc Network," IEEE, *Fourth International Conference on Computational Intelligence and Communication Networks*, 2012.

[21] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, Mohammad S. Obaidat, Fellow of IEEE and Fellow of SCS"Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks," IEEE, *International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2012.

[22] Mehdi Medadian, Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol," *European Journal of Scientific Research ISSN 1450-216X,* Vol.69 No.1, pp.91-101, 2012.

[23] Ms Monika Y. Dangore Mr Santosh S. Sambare ,Detecting And Overcoming Blackhole Attack In Aodv Protocol," IEEE, *International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*, 2013.

[24] Keecheon Kim ,"Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs," IEEE *International Conference on High Performance Computing and Communications*, 2013.

[25] Ms. Gayatri Wahane Ms. Savita Lonare ,"Technique for Detection of Cooperative Black Hole Attack in MANET "IEEE ,*Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013

[26] Durgesh Kshirsagar 1 Ashwini Patil, "Blackhole Attack Detection and Prevention by Real Time Monitoring," IEEE, *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, 2013.

[27] M. K. Marina and S. R. Das, "On-demand multi-path distance vector routing in adhoc networks," *Proceedings of the IEEE Intl. Conf. On Network Protocols(ICNP),* pp. 14-23, 2001.

[28] Saurabh Gupta ,Subrat Kar,S Dharmaraja ,"BAAP: Blackhole Attack Avoidance Protocol for Wireless Network," IEEE, *International Conference on Computer & Communication Technology (ICCCT)*, pp.468-473, 2011.

[29] Fidel Thachil , K C Shet , "A trust based approach for AODV protocol to mitigate black hole attack in MANET," IEEE *International Conference on Computing Sciences*, pp.281-285, 2012.

[30] Vani A. Hiremani, Manisha Madhukar Jadhao "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET," IEEE *International Conference on Green Computing, Communication and Conservation of Energy (ICGCE),* pp.944-948, 2013.

[31] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs," *International Conference on System Engineering and Technology*, 2012.

[32] C. E. Perkins, E. M. B. Royer and S. R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing," *Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt,* 2003.

[33] Seryvuth Tan, Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs," IEEE *International Conference on ICT Convergence (ICTC)*, pp. 1027-1032, 2013.

[34] Jaydip Sen, Sripad Koilakonda, Arijit Ukil ,"Modelling and Simulation A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks," IEEE Second International Conference on Intelligent Systems, *Second International Conference on Intelligent Systems, Modelling and Simulation*, pp.338-343, 2011.

[35] Ming-Yang Su, Taoyuan, Kun-Lin Chiang, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," IEEE *International Symposium on Parallel and Distributed Processing with Applications (ISPA)*, pp.162-167, 2010.

[36] Anu Bala, Munish Bansal , "Analysis of MANET under Blackhole Attack," IEEE *First International Conference on Networks & Communications Performance*, pp.141-145, 2009.

[37] Richard Dawkins. "The selfish Gene. Oxford University press," 1980 edition, 1976.

[38] N.Bhalaji, Dr.A.Shanmugam ,"ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET," IEEE *IFIP International Conference on Wireless and Optical Communications Networks (WOCN)*, 2009.

[39] Prachee N. Patil Ashish T. Bhole "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching," IEEE *Tenth International Conference on Wireless and Optical Communications Networks*, 2013.

[40] Bai,F., Sadagopan, N., Krishnamachar , B.,Helmy, A. "Modeling Path Duration Distributions in MANETs and Their Impact on Reactive Routing Protocols," IEEE *Journal on Selected Areas in Communication*,Vol. 30 Issue 11, pp. 1357-1373, 2004.

[41] Wu, J., Dai,F.,Gao,M.,Stojmenovic, I.(2002), "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks," *Journal Of Communications And Network*, Vol. 4 Issue 1.

[42] Anu Kumari, Arvind Kumar, Akhil Sharma, "Survey Paper on Energy Efficient Routing Protocol in MANET," ISSN: *2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*, Volume 3, Issue 3, March 2013.