CHAPTER – 3
REVIEW OF LITERATURE

"The artist is nothing without the gift, but the gift is nothing without work"

-- Emile Zola

This chapter discusses the literature survey of the present investigation and presents a comprehensive overview of related work in the area of MANET intrusion detection and prevention. The study covers the different protocol approaches for route discovery, encryption approaches as both preventive and IDS, acknowledgement methods and cross layer approaches. The review on these topics exactly shows how the developed technique encapsulates all of these features to develop a robust defensive mechanism to identify and correct network layer attacks to evaluate the performance of the network.

3.1. Introduction

Ad hoc networks are by nature very open to anyone. Their biggest advantage is also one of their biggest disadvantages; basically anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate the network and carry out attacks on its participants with the purpose of stealing or altering information.

3.1.1 Security Goals

Security is a very important factor for MANETs due to its sensitive applications. However, the characteristics of MANETs create each challenges and opportunities in achieving security goals that requires making sure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

Confidentiality: The objective of confidentiality is to carry on the information send undecipherable to unauthorized users or mobile nodes. MANETs make use of an open medium; therefore typically all nodes at intervals the transmission range will acquire the information. A technique to stay information secret is to encrypt the information, or use directional antennas.
Authentication: The goal of authentication is to ensure that a communicating entity is communicating with another legitimate entity. Without authentication an attacker can impersonate an authenticated node and thus gain control over the entire network. There is possible to implement a central point in wired networks and infrastructure-based wireless networks. The central point like a router, base station, or access point. However there is no central point in MANETs and additionally it is difficult to validation an entity.

Integrity: It is able to maintain the message send from being criminally changed or destroyed within the transmission. Once the information is send throughout the wireless medium, the information may be changed or deleted by malicious attackers. The integrity can be achieved by hash functions in order to be certain that changes to a transferred message are done by authorized entities through authorized mechanisms.

Non-repudiation: The objective of non-repudiation is expounded to a proven fact that if a node sends information, the node cannot reject that the information was send by him. By creating a signature for the message, the node cannot later reject the message. It is particularly useful for detecting a compromised node.

Availability: The aim of availability is to stay the network service or resources accessible to approved nodes even supposing there is potential issue within the system. Lack of availablleness ensures Denial of Service (DoS) attacks.

Access control: The goal of access control is to avoid illegal use of network services and system resources. In commonly, the access control is the attention of service in both network communications and individual computer systems [53].

3.2. Background of attacks

In link layer, the protocol to give connection between various mobile nodes so as to make sure one-hop connection by using multi-hop wireless channels. If extend connection between various mobile nodes then uses the network layer protocol. Within coordination process distributed protocols usually imagine that each mobile node are
cooperating with admiration to communication however really this assumption is not potential in hostile mobile networks environment as a result of cooperation is not implemented in MANET. The question occurs why? The explanation is as a result of malicious nodes behavior violating protocol specification so as to disrupt network operations. There are a variety of attacks on networks and can be grouped based on their characteristics.

External and Internal Attacks:

✓ External attacks are dedicated by parties that produce officially part of the network.
✓ Internal attacks are sourced from inside a particular network. A compromised node (known as malicious node, whose actions compromise the security of the whole ad hoc network) which is accessible to all other nodes within its range poses a high threat to the functional efficiency of the whole network.

Passive and Active Attacks:

✓ Passive attacks do not involved any disruption of the service, they are merely intended to steal information and to eaves drop on the communication within the network.
✓ Active attacks can actively alter the data, with the intent of overloading the network, obstructing the operation or to cut off certain nodes from their neighbours so that they cannot use the network services effectively anymore.

3.2.1. Attacks on OSI Layers:

In MANET, the attacks are generally classified into two main categories such as passive attacks and active attacks, in step with the attack suggest that [54]. A passive attack does not disrupting the data exchange operation of the network. An active attack tries to involve destroy the information being exchanged in the network. Table 3.1 shows the common classification of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.
Passive Attacks | Eavesdropping, Traffic analysis, Monitoring
---|---
Active Attacks | Jamming, Spoofing, Modification, Replaying, DoS

**Table 3.1: Security Attacks Classification**

The attacks can be classified into 2 categories, specifically external attacks and internal attacks, according to the domain of the attacks. A number of papers talk over with outsider and insider attacks [56]. External attacks are administrated by nodes that don’t belong to the domain of the network. Internal attacks are from compromised nodes that are literally a part of the network. Internal attacks are a lot of severe when put next with outside attacks since the corporate executive is aware of valuable and secret information, and possesses privileged access rights.

Attacks can be classified based on the network protocol stacks. Table 3.2 shows a some example of taxonomy of security attacks; a few attacks can be launched at several layers. Some security attacks use secrecy [55], by which the attackers endeavor to secrete their actions from either an individual who is monitoring the system. However different attacks like DoS cannot be invented secrecy. All attacks are related to non-cryptography related, and cryptography primitive attacks. In table 3.3 shows an example of cryptography primitive attacks.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>Repudiation, Data corruption</td>
</tr>
<tr>
<td>Transport layer</td>
<td>Session hijacking, SYN flooding</td>
</tr>
<tr>
<td>Network layer</td>
<td>Wormhole, Black hole, Byzantine, Flooding, Resource consumption, Location disclosure attacks</td>
</tr>
<tr>
<td>Data link layer</td>
<td>Traffic analysis, Monitoring, Disruption MAC (802.11), WEP weakness</td>
</tr>
<tr>
<td>Physical layer</td>
<td>Jamming, Interceptions, Eavesdropping</td>
</tr>
<tr>
<td>Multi-layer attacks</td>
<td>DoS, Impersonation, Replay, Man-in-The middle</td>
</tr>
</tbody>
</table>

**Table 3.2: Security Attacks on Protocol Stacks**
### Table 3.3: Cryptography Primitive Attacks

<table>
<thead>
<tr>
<th>Cryptography Primitive Examples</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pseudorandom number attack</td>
<td>Nonce, Timestamp, Initialization vector (IV)</td>
</tr>
<tr>
<td>Digital signature attack</td>
<td>RSA signature, ElGamal signature, Digital signature standard (DSS)</td>
</tr>
<tr>
<td>Hash collision attack</td>
<td>SHA-0, MD4, MD5, HAVAL-128, RIPEMD</td>
</tr>
<tr>
<td>Security handshake attacks</td>
<td>Diffie-Hellman key exchange protocol, Needham-Schroeder protocol</td>
</tr>
</tbody>
</table>

#### i. Physical Layer Attacks

Eavesdropping is that the interrupting and reading of information and exchanges by involuntary receivers. In MANET, all mobile nodes are used to share the information through wireless medium. The RF spectrum is help to transfer the information in most of the wireless communications and its broadcasting the information is naturally. Always very easily to intercept the broadcasting messages through airwaves with proper tuned frequency [57]. Therefore, most of the transmitted messages can be listened, and false messages can be easily injected into network.

In additionally, a radio signal can be blocked, which reason the information to be corrupted or lost [57]. If the attacker contains a controlling transmitter, a signal can be generated very strong sufficient to overcome the targeted signals and interrupt communications. This is form in signal jamming like random and pulse. Jamming tools is quickly accessible. Additionally, jamming attacks may be mounted from a location remote to the target networks.

#### ii. Data link layer attacks

The MANET is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer’s protocols.
iii. Network layer attacks

In MANETs, connectivity extended from neighboring nodes to all other nodes in the network by using network layer protocols. The communication links are established between mobile nodes over a possible strong multi-hop wireless link depends on cooperative reactions among all other network nodes.

A range of attacks pointing the network layer are known and strongly studied in research papers. By means of attacking the routing protocols, attackers can understand network traffic, insert themselves into the link between the source and destination, and therefore manage the network traffic flow, as shown in figure 3.1 (a) and (b). Here, “S” is a source node and “D” is the destination node. The node “M” is act as malicious node with analysis network traffic through S to D. A malicious node M will insert itself into the routing path between node S and D.

![Figure 3.1: Routing attack](image)

The traffic packets can be forwarded to a non-optimal and nonexistent path that may introduce large delay and get packet lost. The attackers will produce routing loops, introduce strict network congestion, and channel conflict into certain areas. Multiple collaborative attackers might even stop a source node from finding in the least route to the destination node, inflicting the network to separation, that triggers excessive network to manage traffic, and additional intensifies network congestion and performance degradation.
iv. **Transport layer attacks**
The purposes of transport layer protocols in MANET consist of flow control, creating and clearing of end-to-end connection, delivery of packets with reliable, flow control, congestion control. Like TCP protocols in the web, the node is defenseless to the typical SYN flooding attack or session hijacking attacks. However, a MANET contains a higher channel error rate when evaluate with wired networks. As a result of TCP doesn’t have any technique to differentiate between whether or not a loss was caused by malicious node, random error or congestion, TCP multiplicatively reduces its congestion window upon experiencing losses that degrades network performance considerably [58].

v. **Application layer attacks**
The following attacks are occurs in application layer level of attacks.

- **Mobile virus and worm attacks:**
The application layer consists of user information, and it generally supports several protocols like FTP, HTTP, and SMTP. Malicious code, which incorporates viruses and worms, is relevant across operating systems and applications.

    Since mobile users know, malicious programs are extensively extended in networks. There are a variety of mechanisms by that a worm will discover new machines to take advantage of. For example, IP address scanning system used by internet worms. This technique creating probe packets to a susceptible UDP/TCP port at several various IP addresses. Hosts that are strike by the check respond, accept a duplicate of the worm, and thus get infected. One of the scanning warms is a code red worm [59].

    Some worms utilize a loophole of the system. For example, Worm Blaster and Worm Sasser [59] each use a various loophole such as Worm Blaster uses a system RPC DCOM loophole, and Worm Sasser uses the system LSASS (Local Security Authentication Subsystem Service). In MANET, used any loophole system to find an attacker can to make a worm attack.
• **Repudiation attack:**

  In the network layer, firewalls can be installed to keep packets in or keep packets out. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications. For example, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system.

vi. **Multi-layer attacks**

  Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multi-layer attacks are Denial of Service (DoS), man-in-the-middle, and impersonation attacks.

• **Denial of Service (DoS):**

  Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

• **Impersonation attacks:**

  Impersonation attacks are just the first step for most attacks, and are used to launch further sophisticated attacks. For example, a malicious node can precede an attack by altering its MAC or IP address.
• **Man-in-the-middle attacks:**

An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

3.2.2 Network Layer Attacks

In the past few years there is a rapid development in the area of mobile computing. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of MANET. A MANET is an autonomous collection of mobile nodes that can change locations dynamically. Since the nodes are mobile, the network topology changes rapidly and randomly. The MANET network is decentralized. The examples can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. As MANETs are dynamic in nature, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. Security is the aspect not to be treated lightly. This is the most desired feature of communication. According to layered architecture there are different attacks on each layer of MANET but this section insight the network layer attacks in MANET and their countermeasures to prevent those attacks for security purpose. Network layer is affected by various security threats. These attacks may be passive or active. Various network layer attacks are listed below in the figure 3.2.
3.2.2.1 Black hole attack

Security in MANETs can be often usually classified into route security and information security. In information security, information is protected against any form of unauthorized speech act, disruption and destruction. In route security, routing (packet forwarding) is protected against any form of deception. Solving all vulnerabilities associated with each route and information securities notice each information integrity and confidentiality. Typical attacks that may be simply performed against MANETs include: region, Denial of Service (DoS), Impersonation, Disclosure, Spoofing, and Sleep deprivation attacks [67].

A single part attack is definitely happened within the mobile ad hoc networks [60]. It’s a nature of denial of service attack wherever a malicious node offers false data of getting shortest route to the destination so as to induce all the information packets and drop it [62]. In black hole attack, [66] a malicious node (or stingy node) takes advantage of route discovery procedure of routing protocol, to point out itself as having the shortest path to the destination node or to the node whose packet it desires to intercept. This hostile node advertises its convenience of recent routes regardless of checking its routing table. During this manner assaulter node can perpetually have the supply in replying to the route request and so intercept the information packet and retain it [65]. Therefore, all traffics are routed through the assaulter, and thus, the assaulter will misuse or discard the traffic [64].
There are unit varied mechanisms are projected for finding single part attack in recent years. However, several detection schemes are unit unsuccessful in discussing the cooperative part issues. Some malicious nodes collaborate along so as to beguile the conventional into their unreal routing data, moreover, hide from the present detection theme. As a result, many cooperative detection schemes area unit projected preventing the collaborative black hole attacks [61]. The part attack has two properties. First property is, the node exploits the painter protocol, like AODV (Ad hoc On-demand Distance Vector) to advertise itself as having a legitimate path to a destination node, even if the path is invalid, with the intention of intercepting packets. Second property is, the assaulter consumes the intercepted packets while not forwarding to the other node [63]. Some major destruction generated by part is listed below:

1. It will increase network overhead; thanks to unwanted transmission.
2. It decreases the network’s time period by boosting energy consumption unnecessarily.
3. It destroys the network by dropping the crucial knowledge packets over the present communication.

*Single Black Hole Attack:*

In single part attack solely single node behaves as malicious node inside a network. It’s conjointly called part attack with single malicious node. An example is shown as figure 3.3, node 1 stands for the source node and node 4 represents the destination node. Node 3 may be a misconduct node who replies the RREQ packet sent from source node, and makes a false response that it’s the fastest route to the destination node. Thus node 1 mistakenly judges the route discovery method with completion, and starts to send knowledge packets to node 3.
As what mentioned above, a malicious node in all probability drops or consumes the packets. This suspicious node is thought to be a black hole node in MANETs. As a result, node 3 is ready to misroute the packets simply, and also the network operation is suffered from this downside. The foremost important influence is that the PDR diminished severely.

**Collaborative Black Hole Attack:**

In collaborative black hole attack multiple nodes within a network behave as malicious node within a network. It is also known as black hole attack with multiple malicious nodes. Here node 1 is the source node and 6 is the destination node. Nodes are 2, 3, 4, 5 and 7 acts as the intermediate nodes. Nodes are 3 and 5 acts as the cooperative black holes. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ.
Since the black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the black hole node 3 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 3.4. Now on receiving the RREP from node 3, the source starts transmitting the data packets. On the receipt of data packets, node 3 simply drops them, instead of forwarding to the destination or node 3 forwards all the data to node 5. Node 5 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

**Defense against Black Hole Attack:**

There are three defense levels to counter an attack, namely, preventive, incentive and detective-corrective. The preventive level forbids the malicious nodes from taking part in packet forwarding. The inducement level seeks to stimulate the cooperation among the router nodes via an economic model. The detective-corrective level aims to reveal the identity of the malicious node and to exclude it from the network.

3.2.2.2 **Routing attack**

There are several attacks which can be mounted on the routing protocols and may disrupt the proper operation of the network. Brief descriptions of such attacks are given below:

**Routing Table Overflow:**

In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. In the case of proactive routing algorithms, it need to discover routing information even before it is needed, while in the case of reactive algorithms we need to find a route only when it is needed. Thus main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.
Routing Table Poisoning:

In routing table poisoning, the compromised nodes present in the networks send fictitious routing updates or modify genuine route update packets sent to other authorized nodes.

Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

Packet Replication:

In the case of packet replication, an attacker replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

Route Cache Poisoning:

In the case of on-demand routing protocols (such as the AODV protocol [69]), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

Rushing Attack:

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [70]. An attacker which receives a route request packet from the initiating node floods the packet quickly throughout the network before other nodes which also receive the same route request packet can react. Nodes that receive the legitimate route request packets assume those packets to be duplicates of the packet already received through the attacker and hence discard those packets. Any route discovered by the source node would contain the attacker as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the attacker. It is extremely difficult to detect such attacks in ad hoc wireless networks.
3.2.2.3 Sybil attack

A faulty node or an adversary may present multiple identities to a network in order to appear and function as multiple distinct nodes. After becoming part of the network, the adversary may then overhear communications or act maliciously. By presenting multiple identities, the adversary can control the network substantially. Above figure 3.5 shown as example of Sybil attack.

3.2.2.4 Fabrication

In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [71]. In figure 3.6, where fabrication attacks is explained by an example. In the example where the source node $S$ wants to send data towards the destination node $X$, so therefore at start it sends broadcast message and request for route towards the destination node $X$. An attacker as a malicious node $M$ try to pretends and modify route and returns route reply to the node ($S$). Furthermore, an attacker’s nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV routing protocols.
3.2.2.5 Modification

In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

Route sequence numbers modification:

In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

Hop count modification attack:

In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

Source route modification attack:

In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In figure 3.7 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-DX). Which shows that node S and the node X cannot communicate each other directly, and in the scenario (Fig. 3.7) where the node M which act as a malicious node which are going to attempt a denial-of-
service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try to send the packet towards the distention X which is not possible because the node C can’t communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

Figure 3.7: An example of route modification attack

3.2.3 Security steps to avoid Attacks in MANET

3.2.3.1 Secure Multicasting

Multicast is a mechanism where any user become the part of multicast group and even send traffic to the multicast users as well as receive traffic, but due to this procedure it can easily fall into denial of service attacks (DoS). There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for DIstributed Policy enfOrceMent Architecture which is use to protect or secure end user services as well as network bandwidth. Audio and video traffic usually fall into the category of multicast traffic which is usually use by militaries as well as disaster backup plans (teams). There are some of the major responsibilities of DIPLOMA architecture which are given below [72].

- It gives solution for both sender and receiver whenever they access to the multicast group.
- It also used to limit the bandwidth.
DIPLOMA integrates with common multicasting routing protocols like PIM-SM and ODMRP.

It also uses to provide (allocate) network resources in a fair manner during attacks.

3.2.3.2 Secure routing

MANET is a self organized wireless network, due to the fact it has vulnerable attacks that can easily damage the whole network; that’s why there should be some solutions which works even some of the mobile nodes compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication. There are some of the major responsibilities of secure routing which are given below.

- It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
- Routing protocol responsiveness itself provide safety among different routing attacks.

In section [73] there is detail description of secure routing mechanism and in our simulation work is also based on the authentication mechanism in MANET.

3.2.3.3 Privacy-aware and Position Based Routing (PPBR)

MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that's why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbors. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.
3.2.3.4 Key management

Certified Authority (CA) is one of the mechanisms which provide key management; if it is compromised then entire network can easily be damaged. One of the major functionality of key management and distribution for MANET, it provide solutions for mobility related issues. In section [74] writers discuss different aspect of key management and distribution for MANET. In the paper, the approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

3.2.3.5 Intrusion detection System

Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behavior. IDS use to detect critical nodes and then analyze its data traffic, critical node also degrade network performance. There are different IDS systems which has some specific features, some of them are given blow

- Cluster based voting
- Neighbor-monitoring
- Trusts building for detail description of these IDS system see section [75].

3.2.3.6 Multi-layer Intrusion detection technique

Multi-layer intrusion detection technique is a technique in which an attacker attacks at multiple layers in order to stay below the detection threshold so that they will escape easily whenever a single layer impropriety detects. These type of attacks mainly attack at cross layer which are more alarming and frightening as compare to single layer attack and they can easily be escaped. Although these type of attacks can be detected by a multiple layer insubordination detector, where with respect to all network layer’s input are use to combine and examine by the cross-layer detector in a detailed fashion. There is also another way to detect these kinds of attacks by working together with RTS/CTS and network layer detection with respect to dropped packets.
3.3 Analysis and discussion for different solution in black hole attack

Alem Y.F., et al.,[117] have proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD), which is detect both single and multi black hole nodes. In this system monitored every user node activities and anomaly activities of an intruder can be easily identified from normal activities. To identify malicious node, IDAD system to be pre-collected set of anomaly activities, called audit data. Once audit data is collected and it is very easy to detect malicious node, which is able to compare every activities with audit data. If any irregular activity is finding, IDAD system segregate the particular node from the network. The decrease of the number of routing packets, which is minimize network overhead and faster communication.

Ming – Yang Su et al., [118] authors discussed a mechanism is Anti – Black hole mechanism. It used to calculate approximately the mistrustful value of a node according to the amount of irregular difference between RREQs and RREPs transmitted from the node. When the value is greater than the threshold value, immediately broadcasted an alert message with id of that node. The malicious node identified at that time will place on their black lists to segregate the malicious node in the network cooperatively. The merit of this mechanism detects cooperative black hole attack and demerit is to maintain extra databases for training data and its updating information, and routing table.

Nital Mistry et al., [119] have a feasible solution for the black hole node. The source node store all the RREPs message in the table called Cmg_RREP_Tab until receiving first RREP packet waits for MOS_WAIT_TIME. At the same time, the source node checked all the nodes RREPs message from the Cmg_RREP_Tab table and discard very high sequence number of the nodes in a network. Each node have Mali_node table for storing the malicious node information to segregate that node in the network. In besides of removing a RREP message in the Cmg_RREP_Tab table, in order to maintain a new freshness table. This solution downside doesn’t seem to be observing of cooperative black hole attack and its high processing delay.
In paper [120] authors K.Lakshmi et al. have projected and mentioned a possible resolution for the black hole attacks that may be enforced on the AODV protocol. During this resolution, compare the primary destination sequence number with the supply node sequence number, it here exists way more variations, between them, sure range as shooting that node is that the malicious node, in real time take away that entry from the RR-Table. Final method is choosing consequent node id that has the upper destination sequence number, is obtained by sorting the RR-Table consistent with the DSEQ-NO column, whose packet is distributed to receive reply technique to continue the conventional AODV method.

The authors Sen J et al. have planned mechanism [121] for relying against a cooperative part attack. This planned mechanism modifies the AODV protocol by introducing two concepts, like (a) information Routing info (DRI) table and (b) cross checking. Within the planned theme, the nodes that reply to the RREQ message of a supply node throughout route discovery method send 2 bits of extra info. Every node maintains a further DRI table. within the DRI table, the bit one stands for ‘true’ and also the bit zero stands for ‘false’, the primary bit ‘From’ stands for the information on routing data packet from the node, whereas the second bit ‘Through’ stands for information on routing data packet through the node, during this mechanism source node (SN) broadcasts a RREQ message to get a secure route to the destination node. The intermediate node (IN) replies with Next Hop and also the DRI of Next Hop Node (NHN) to the source node. Upon receiving the replies from the IN, the supply node checks its own DRI table for the dependableness of the IN node, it's gift within the DRI table, SN starts causing the information packets through the IN node, otherwise SN sends FREQ to the NHM for the reliable IN. When receiving the DRI of its NHN and DRI of IN, the supply node once more checks its own DRI table for the reliable IN, the supply node once more checks its own DRI table for the reliable IN. if reliable IN presents, the supply node (SN) starts causing information packets through that IN node. Otherwise, once more supply node sends an additional request for the reliable intermediate node. However, this mechanism cannot observe black hole nodes fully that act as hand and glove.
Yaser Khamayesh et al., [122] supposed protocol and changed the performance of the initial AODV by introducing a data structure referred as trust table at every node. This table maintain for holding the addresses of the reliable node. A replacement field is superimposed to route reply packets is named trust field. Accordingly, nodes to be superimposed to a different node trust table, it wants of initial to pass the behavior analysis filter. The broadcasting node behavior is incredibly traditional then it's superimposed to the trust table of the receiving node. Route reply packet is overload with an additional field to point the responsibility of the replying node. The worth of the trust field is initialized to zero by the replying node and can be changed by its previous hop throughout the trip of the RREP. The worth of the trust field might be changed either to two if the replying node is that the destination however still exists within the trust table. Upon the RREP is received by the supply node, it decides whether or not to send the information or to attend for any route. Just in case the trust field worth equals to one or two, the supply node sends, otherwise the supply node waits for any route. Though the planned methodology provides reliable routes however consums high network delay.

Rajib Das, et al, [123] during this paper authors provide an algorithmic approach to analyzing and rising security of AODV against region attack. The answer is often applied to characteristic single and cooperative region nodes within the network; and ascertains secure ways from supply to destination by excluding region nodes acting in cooperation. In region attack all network traffics area unit redirected through malicious node foundation of damaging the network. The detection of this attack still thought-about terribly difficult problems. In the simulation showed that impact of the packet delivery quantitative relation and through place has been decreases impact of attacks. The planned resolution is capable of police investigation and removing attack node in the MANET at the beginning.

Lalit Himral et al. [124] have planned methodology to search out the secured routes and stop the black hole nodes within the MANETs by checking whether or not there is giant distinction between the sequence range of supply node or intermediate node who has sent back initial RREP or not. Generally, the primary route replies are going to be from the malicious node with high destination sequence range, that is hold
on because the initial entry within the RR-Table. Then compare the primary destination sequence range with the supply node sequence range, is there exists rather more distinction between them, sure it's from the malicious node, in real time take away that entry from the RR-Table. The planned methodology cannot realize multiple region attack.

Herminder Singh et al. [125] have mentioned the AODV protocol stricken by black hole attack and planned a feedback answer that relatively decreases the quantity of packet loss within the network. The black holes by examining the quantity of sent packets at that node which can invariably be adequate zero for many of the cases. Once the malicious nodes are detected, it will adopt a feedback methodology to avoid the reacceptance of incoming packets at these black holes. The packets returning at the immediate previous nodes to black nodes area unit propagated back to the sender and also the sender follows another safer route to the destination. However, it cannot find region nodes once they worked as a bunch.

Elisha, et al, [126] authors are performed black hole attacks are established by involved malicious node that consent to forward data packets to destination but eavesdrop or drop the packets purposely, which not only compromise the network, but also reduce the worth of the network performance. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. A requirement basis the route update information is shared on a periodically. The malicious node regularly broken a control packets are susceptible. This paper auxiliary analyzes to help power of making a strong detection of black hole attack in AODV and improve the performance of routing protocol.

The proposed design AODVR [127] has introduced many modules like Packet Classifier, Extractor, Black list Tester, RREP sequence variety Tester, threshold tester and ALARM broadcaster. Because the packet arrives within the system, Packet Classifier classifies it to be RREQ, RREP secure, RERR, ALARM and HELLO packet. AODVR modifies the content and format of RREP and embody a brand new kind of packet ALARM. Extractor extracts needed contents of all sorts of packet apart from HELLO. However, the procedure of formulating the threshold could be a bit
overwhelming, therefore it results network delay. Formulations of correct threshold vary keep malicious node from intrude; whereas a wrong formation might prohibit associate authentic node thereby disgrace it to be a part.

A rule bestowed in [128] to notice the black hole attack in a MANET supported the preprocessor referred to as Pre_Process_RREP and it's easy and doesn't amendment workings of either intermediate or destination node. It doesn't even modify the operating of traditional AODV. The method continues to simply accept RREP packets and calls a process referred to as Compare_Pkts (packet p1 and p2) that really compare the destination sequence range of two packets and selects the packet with higher destination sequence range if the distinction between two numbers isn't considerably high. Packet containing exceptionally high destination sequence range is suspected to be a malicious node associate degreed an ALERT message containing the node identification is generated that is broadcasted to neighbor nodes in order that it are often isolated from the network and may maintain a listing of such malicious nodes. This resolution has additional network delay and can't notice cooperative part nodes.

In [129] Kamarularifin Abd et al. have designed associate ERDA resolution to enhance AODV protocol with minimum modification to the prevailing route discovery mechanism recvReply() operate. There square measure 3 new parts introduced in changed recvReply() operate namely: table rrep_table to store incoming RREP packet parameter mali_list to stay the detected malicious nodes identity and parameter rt_upd to regulate the method of change the routing table. Once RREQ packet is shipped out by the supply node S to search out a contemporary route to the destination node D. RREP packet received by node S are captured into RREP_tab table. Since the malicious node M is that the primary node to response, the routing table of node S is updated with RREP information from node M since the value of parameter rt_upd is ‘true’ node S accepts subsequent RREP packet from completely different node to update the routing table although it arrives later and with a lower destination sequence vary than the one inside the routing table. The present route entry in routing table is overwritten by the later RREP returning from different node. ERDA technique offers an easy resolution by eliminating the false route entry and replaced the entry with later RREP. However, it cannot find cooperative part attack.
All the above approaches will solely check whether or not the route to the destination node is valid or not. But, they can't check the standard of the route. In paper [130] delineate an answer to counter black hole attacks to the ETX metric acquisition method that is predicated on the standard of the routes between the supply and also the destination nodes. The answer is named the Secure ETX (SETX) protocol. The protocol, rather than permitting individual nodes to advertise their individual delivery ratios it'll, permits nodes to live neighbors’ delivery ratios directly. The algorithmic program makes use of the ETX metric price to search out a detection threshold price ($d_{\text{thresh}}$). The most plans utilized in the planning of the SETX protocol is to let a causing node to calculate each $d_r$ and $d_f$ values themselves, instead of relying their neighboring nodes to calculate the $d_f$ price. To permit this, a causing node known as an initiator (I), generates and broadcasts probes to its neighboring nodes. Every of those probes contain a stream of random value. The neighboring nodes can get to come back the probes received back to the initiator. The probes that are sent back to the initiator are known as acknowledge probes. The leader calculates the $d_f$ value by figuring out the magnitude relation between the number of authentic acknowledge probes received and also the number of probes that were broadcast. Within the SETX protocol, two styles of buffers is introduced, an Advertised Probe Buffer (APB) and Received Probe Buffer (RPB). An APB may be a probe buffer wont to store probes that are publicized, and a RPB is employed to store the probes received from a given neighbor node. The dimensions of APB and RPB are denoted because the $\text{PROBE\_BUFFER\_SIZE}$, and its default price is ten probes to keep up solely the newest probes within the buffers. The SETX protocol doesn't enable neighbors to send their individual $d_f$ values to its leader. Rather, the neighbors ought to remit the leader all the probes they receive from the leader. These came probes is the proof of the equality of the link involved. Because the probes contain random numbers, if a neighbor node has not received a sound probe, it'd be troublesome for the node to forge one that would pass the verification so as to forge up the $d_f$ price for the link. Therefore, it has a tendency to may say that with the SETX protocol, it's troublesome for a neighboring node to launch region attacks by fabricating the $d_f$ value.

Jathe S.R, Dakhane D.M, [131] review paper exposed communication without a network infrastructure. Due to security vulnerabilities of the routing protocols,
however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this review paper authors studied the details about black hole attack and comparison of detection of different black hole attacks techniques. These techniques analyze help to choose best techniques for detection of black hole attacks.

Ramod Kumar Singh and Govind Sharma [132] planned technique uses promiscuous mode to notice malicious node (black hole) and propagates the knowledge of malicious node to any or all the opposite nodes within the network. It doesn't need any information, further memory and a lot of process power. The simulation results show the effectively of the planned technique as throughput of the network doesn't depreciate in presence of the black holes.

Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala [133] planned an algorithm that detects and removes malicious nodes throughout the route discovery part. Nodes receiving RREP verify the correctness of routing information; supply node broadcasts an inventory of malicious nodes once causation RREQ. Nodes update route tables after they get any info of malicious nodes from received routing packets. As there’s no further management packet value-added within the planned rule, there would be negligible distinction in Routing Overhead that is that the magnitude relation of the quantity of routing connected transmissions to the quantity of knowledge connected transmissions. Moreover, because the malicious nodes would be isolated, Packet Delivery magnitude relation (PDR) would be improved greatly; PDR is that the magnitude relation of range of received knowledge packets to the quantity of sent knowledge packets. If the node receiving RREP from a malicious node doesn’t have the node marked as malicious within the routing table, the planned rule adds a little process overhead thereto node because it needs to calculate the height price.

Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang ,and Arjun Agrawal [134] planned that tackles black hole attacks by maintaining an Extended Data Routing Information (EDRI) Table at every node additionally to the Routing Table of the AODV protocol. The mechanism is capable of police work a malicious node. It additionally maintains a history of the node’s previous malicious instances to account for the grey behavior. Refresh packet, Renew Packet, BHID Packet, more request and
more reply packets are employed in addition to the present packets (RREQ and RREP). Our technique is capable of finding chain of cooperating malicious nodes that drop a major fraction of packets. A limitation of this resolution is that the malicious nodes got to be consecutive whereas acting in cooperation (which is that the most typical scenario) to be known by the algorithm.

In this paper [135] authors have given fuzzy primarily based trust value routing algorithm to handle black hole and cooperative black hole attack that are caused by malicious nodes. Fuzzy management technique to find and mitigate a kind of attack, particularly malicious packet dropping in ad hoc network. A malicious node will promise to forward packets however drop or delay them. During this technique, each node within the mobile ad-hoc network sends the route request and waits for the acknowledgement. The requesting nodes analyze the behavior of unknown node mistreatment fuzzy technique and on basis of result the node take this node within the route of the packet. After, node state data may be utilized by the routing protocol to bypass those malicious nodes. The projected methodology shows that during a moderately dynamic network, this method will find most of the malicious nodes with a comparatively high positive rate. The packet delivery rate within the painter can even be raised consequently.

In authors [136], projected algorithmic rule can give the answer of packet loss and rate against the black hole attack in network. The traffic will increase over the mobile ad hoc network it'll results in range of issues that's congestion and packet loss. This congestion and packet loss issues happens owing to the attack in mobile ad hoc network. The purposed work can first notice the black hole attack by means of the fuzzy logic. The fuzzy logic is enforced on packet loss and rate at time of node communication. Currently during this it'll send the packet from neighbor nodes. This algorithmic rule can give the higher resolution.

✓ Comparison of Various Solutions to Black Hole Attack

The following table 3.4 shows various solutions to black hole attack in mobile ad hoc network.
<table>
<thead>
<tr>
<th>Techniques proposed by</th>
<th>Techniques / Solutions</th>
<th>Introduce new packets (Yes / No)</th>
<th>Modifies AODV / Routing Tables (Yes / No)</th>
<th>Type of Black Hole Attack</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alem, Y.F., Zhao Cheng Xuan, 2010 [117]</td>
<td>Intrusion detection using anomaly detection</td>
<td>Yes</td>
<td>No</td>
<td>Single black hole attack</td>
<td>Neighbor nodes may give false information</td>
</tr>
<tr>
<td>Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao, 2010 [118]</td>
<td>An anti black hole mechanism using intrusion detection system</td>
<td>Yes</td>
<td>Yes</td>
<td>Multiple black hole attack</td>
<td>Time delay</td>
</tr>
<tr>
<td>Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, 2010 [119]</td>
<td>Compare route replies and discards the high destination sequence number route reply</td>
<td>No</td>
<td>Yes</td>
<td>Single black hole attack</td>
<td>Time delay</td>
</tr>
<tr>
<td>Sen J, Koilakonda S, Ukil A, 2011 [121]</td>
<td>Data routing information table of next hop node</td>
<td>Yes</td>
<td>Yes</td>
<td>Co operative black hole attack</td>
<td>Maintenance of DRI tables apart from normal routing information</td>
</tr>
<tr>
<td>Yaser Khanmayesh, Abdulraheem Bader, Wail Mardini and Muneer Bani Yasein, 2011 [122]</td>
<td>Behavioral analysis filters and trust values</td>
<td>No</td>
<td>Yes</td>
<td>Single black hole attack</td>
<td>Network overhead and time delay</td>
</tr>
<tr>
<td>Rajib Das, Dr. Bipul Syam Purkayastha, Prodipto Das, 2011 [123]</td>
<td>Algorithmic approach to analyzing and rising security of AODV against region attack</td>
<td>No</td>
<td>No</td>
<td>Single black hole attack</td>
<td>Time delay</td>
</tr>
<tr>
<td>Lalit Himral, Vishal Vig, Nagesh Chand, 2011 [124]</td>
<td>Checking SN’s of source node and first route reply</td>
<td>No</td>
<td>Yes</td>
<td>Single black hole attack</td>
<td>Time delay, Co-operative black hole nodes</td>
</tr>
<tr>
<td>Herminder Singh, Shweta, 2011 [125]</td>
<td>Feedback solution based on the number of packets sent from the nodes</td>
<td>Yes</td>
<td>No</td>
<td>Single black hole attack</td>
<td>Always it doesn’t works that is when congestion occurs</td>
</tr>
<tr>
<td>Mohammed Abu Obaida, Shahnewaz Ahmed Faist, Md. Abu Horaira, Tanay Kumar Roy, 2011 [127]</td>
<td>Compares the route reply sequence numbers, with threshold value and selects the routes</td>
<td>Yes</td>
<td>No</td>
<td>Single black hole attack</td>
<td>Cannot detect co-operative black hole attack</td>
</tr>
<tr>
<td>Subash Chandra Mandhata, Dr.Surya Narayan Patro, 2011 [128]</td>
<td>Compares destination node sequence range of more than one RREP’s at source node</td>
<td>Yes</td>
<td>No</td>
<td>Single black hole attack</td>
<td>Network delay, Cannot detect co-operative black hole attack</td>
</tr>
<tr>
<td>Kamarularifin Abd, Jalil, Xaid Ahmed, Jamalul-Lail Ab Manan, 2011 [129]</td>
<td>Enhance route discovery for AODV</td>
<td>No</td>
<td>Yes</td>
<td>Single black hole attack</td>
<td>Cannot detect co-operative black hole attack</td>
</tr>
</tbody>
</table>

Table 3.4: Comparison of various solutions to black hole attack
<table>
<thead>
<tr>
<th>Name and Year</th>
<th>Solution</th>
<th>Co-operative Black Hole Attack</th>
<th>Time Delay and Overhead Due to Much Calculations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Osathanunkul K, Ning Zhang, 2011 [130]</td>
<td>Secured ETX metric</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>P. K. Singh and G. Sharma, 2012 [132]</td>
<td>Uses promiscuous mode to detect black hole node</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>R. H. Jhaveri, S. J. Patel and D. C. Jinwala, 2012 [133]</td>
<td>During route discovery phase to detect malicious node</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>G. S. Bindra, A. Kapoor, A. Narang, and A. Agarwala, 2012 [134]</td>
<td>Maintaining Extended Data Routing Information table, history of nodes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 3.4(continue..): Comparison of various solutions to black hole attack

### 3.4 Summary

As authors tend to already understand why MANET is therefore common in present scenario? It’s some additional normal options attributable to that it's acceptable globally. In line with the distinctive characteristics of MANET, the counseled techniques for victimization within the detection of the black hole attack ought to be light-weight, safe, and correct. In this chapter, simply offer an inventory of solutions in MANET on a selected attack that's black hole attack. There square measure such a large amount of solutions which offer higher security just of single malicious node however these solutions don't seem to be effective in case of multiple malicious nodes. During this paper a quick introduction is offer for every resolution with their enhancements and downsides. However, these techniques consume a lot of power than the restricted computations approaches. Researchers have to be compelled to target up the effectiveness of the protection theme still as minimize the price to create them appropriate for a MANET.