CHAPTER 3

SECURE DSR PROTOCOL FOR DETECTION AND EXCLUSION OF SELECTIVE BLACK HOLE ATTACK IN MANET

3.1 INTRODUCTION

Mobile Ad-hoc Network (MANET) has gained a considerable attraction in the recent times. It is a set of wireless nodes which can be dynamically placed at any place and anytime with no pre-available network infrastructure. The routers are independent to move in random and arrange themselves in an arbitrary manner: therefore, the network’s wireless topology may vary quickly and in an unpredictable manner. Every device in a MANET can move randomly in any direction, and hence, will modify its links to other devices often. MANETs are generally configured in emergency situations for temporary operations or only if there exists no resources to have big networks set up. These kinds of networks function without any fixed infrastructure that renders them easy to be deployed. The characteristics of these networks are as below:

- Inherent mutual trust
- Dynamic network topology
- Periodic routing updates

In this work, the Secure Dynamic Source Routing Protocol (SDSR) proposed is utilized for the detection and prevention of selective black hole attack in a more accurate manner. An Intrusion Detection System (IDS) is introduced in which the IDS nodes are configured in promiscuous mode just
when it is needed, for detecting the irregular difference in the number of data packets that is being forwarded by a node.

### 3.1.1 Dynamic Source Routing Protocol

The Dynamic Source Routing Protocol (DSR) is a simple and effective routing protocol which is specifically designed for usage in multi-hop wireless ad-hoc networks of mobile nodes. DSR permits the network to be entirely self-organizing and self-configuring, with no available network infrastructure or administration. The protocol consists of two mechanisms of route discovery and route maintenance that operates together in order to permit the nodes to find and maintain the source routes to random destinations in the ad-hoc network. The usage of source routing lets the packet routing to be loop-free trivially, prevents the necessity for up-to-date routing information in the intermediate nodes through which the packets are forwarded, and permits the nodes forwarding or overhearing of packets for caching the routing information in them for their own future utilization. All the aspects of the protocol work fully on-demand, permitting the routing packet overhead of DSR for automatically scaling to only that is required to provide reactions to variations in the routes which are presently in use.

This work is employed for establishing a route by means of flooding Route Request packets in the network.

### 3.1.2 Black Hole Attack

Black hole attack is susceptible to security in MANET routing protocol. In the case of Black Hole attack, a malicious node sucks all the data packets in itself, identical to a hole that absorbs in everything. In this manner, all the packets in the network are discarded. A malicious node which drops all the traffic in the network uses the vulnerabilities of the route discovery packets
of the on demand protocols, like Ad-hoc On-Demand Distance Vector (AODV), Perkins et al. (2003).

The effective methodologies are proposed for the detection of black hole attack, Shraddha Raut & Chede (2012). The first technique uses the concept of the paths redundancy which is available to the source node to arrive at a certain destination. As the redundant paths to arrive at a destination are more, the source node after making the request for a route by means of the RREQ packet waits for a response from more than one node to have a secure route verified. On the receipt of a RREP (Route Reply) the source node does the extraction of the path and compares the two routes, it is seen that in MANET that two paths to the same destination have some hops that are common, therefore in case the two responding nodes have some common hops, they are treated to be secure and robust for the transmission of the data. In the second technique, the conventional sequence number comparison is carried out to guarantee the authenticity of the path. These techniques can mitigate a single black hole attack though it cannot deal with the collaborative black hole attack, where several malicious nodes coordinate together to conduct the network attacks.

A black hole attack on a MANET indicates an attack by a malicious node that gets the route from a source to a destination by means of falsifying the sequence number and the hop count of the routing message, Mitrokotsa & Dimitrakakis (2013). A selective black hole is actually a node which can selectively and alternatively carry out a black hole attack or serve as a normal node. Different IDS (intrusion detection system) nodes are implemented in MANETs for the purpose of detecting and preventing the selective black hole attacks.
IDS nodes must be configured in sniff mode for performing the ABM (Anti-Black-hole Mechanism) functionality that is chiefly utilized for estimating a suspicious value of a node in accordance with the abnormal difference between the routing messages which are sent from the node. If a suspicious value goes beyond a threshold, an IDS will broadcast a block message, warning every nodes present on the network, requesting them to collaborate separate out the malicious node, Lacey et al. (2014). Because of the intrinsic vulnerabilities of wireless networks, novel security measures have to be designed to safeguard them efficiently. This technical work is focused over the detection of suspicious activities in MANETs.

In this work, selective black hole attack detection is carried out by employing secure DSR protocol.

3.1.3 Overview of Grey Hole Detection

The effect of grey hole attack detection is studied over ad-hoc network. Exchange of Information happens in a network of mobile and wireless nodes with no infrastructure support and such networks are referred to as ad-hoc networks. A MANET is a mobile, multihop wireless network that has the capability of independent operation. A Grey hole is actually a node which drops and then forwards data packets selectively once after advertising itself to have the shortest path to the destination node in reply to a route request message. Some technique assists in protecting the network by the detection and reaction towards malicious activities of any particular node. The results facilitate to reduce the attacks over integrated MANET-Internet communication in an efficient manner. Simulation will be conducted by employing a network simulator tool so that the issue of detection and prevention of grey hole attack is addressed in mobile ad-hoc network.
Grey hole attack can act as a slow venom in the network side which indicates the probability of losing the data. In grey hole attack, Vishnu et al. (2010) a malicious node denies to forward few packets and just drops them. The attacker then drops the packets coming from a single IP address or a range of IP addresses selectively and thereafter forwards the other packets. Grey hole nodes present in MANETs are very efficient. Each node maintains a routing table which stores the next hop node information in order to route a packet to the destination node. When a source node wants to route a packet to the destination node, it makes use of a particular route when such a route is present in its routing table. Else, the nodes initiate a route discovery process through the broadcast of the Route REQuest (RREQ) message to its neighbors. On the receipt of RREQ message, the intermediate nodes do the updating of their routing tables for a reverse route to the source node. A Route Reply (RREP) message is transmitted back to the source node once the RREQ query arrives either the destination node itself or some other node which possesses a current route to destination.

The grey hole attack, Sukla Banerjee (2008), on MANET’S is explained employing this protocol. The grey hole attack consists of two significant stages, In the first stage, a malicious node uses the AODV protocol to announce itself to have a valid route to the destination node, with the intention of intruding or damaging the packets, even though the route is false as shown in the Figure 3.1. In the second stage, nodes discard the interrupted packets along with a certain probability. Grey hole Detection is a hard process. In few other grey hole attacks, the attacker node does behave maliciously for the time till the packets are dropped and thereafter switched to their normal behaviour. Because of this behaviour, it is very hard for the network to find out such type of attack. Grey hole attack is also called as node misbehaving attack. Once, variation of black hole attack is the grey hole attack, where the nodes either selectively drop the packets (e.g. dropping every UDP packet when
forwarding TCP packets) or drop the packets statistically (e.g. dropping 50% of the packets or dropping them with a probability distribution). Both kinds of grey hole attacks try to interrupt the network without getting detected by the security measures that are in place, Oscar et al. (2008).

When the source node is observed to behave similar to a grey hole, it is separated from the network by invoking the global alarm detection process as explained later in this section. The periodicity of invocation of the detection algorithm is significant for assuring the necessary throughput in the network and a grey hole may rapidly modify its phase from ‘good’ to ‘bad’. The frequency of invocation of the algorithm must be on the basis of the maximum percentage of packet drop which the network application is able to afford. In the worst case scenario, a grey hole will simply vary its phase from ‘good’ to ‘bad’ immediately once the invocation of one round of the detection algorithm is finished and will then switch back to ‘good’ phase just prior to the next invocation. Even though such a condition may be quite not possible, the invocation periodicity must be on the basis of the estimation of the number of packets which the grey hole might drop during that time period and also the maximum number of packet drops which might be permitted when still keeping up the wanted quality of service (QoS).

(Source: Oscar et al. 2008)

**Figure 3.1 Grey Hole Attack in Mobile Ad-hoc Network**
In this work, grey hole attack is detected by employing secure DSR protocol with efficiency over MANET.

3.1.4 Overview of Trust Based Security Mechanism

Aravindh et al. (2013) proposed a trust based technique for the detection and separation of malicious nodes in MANET. This technique makes use of the trust values to assist in the packet forwarding by keeping a trust counter for every node. When the trust counter value goes below a trust threshold, the respective intermediate node is tagged to be malicious and separated from the network, thereby maximizing the performance of the network.

Trust is referred to as the confidence of a node $i$ that a node $j$ will conduct itself as anticipated, i.e. on the node’s $j$ cooperation. In order to assess the reliability of its neighbors, a node not just monitors their behaviour (direct observations) but might also communicate with the rest of the nodes to have their opinions exchanged. The techniques for getting the trust information and describing every node’s reliability are called as trust models. A trust model is generally utilized not just for higher layer decisions such as routing and data aggregation, though also cluster head selection and, more astonishingly, for the purpose of key distribution. Its goal is about improving the security and thereby increasing the throughput, the lifetime and also the resilience of a network.

Gupta et al. (2013) proposed a concept of trust factor in (initialization phase), for choosing the most effective route along with a routing path. In this strategy, Constant trust factor is utilized for evaluating the reliable and shortest path for communication in the network. In order to avoid the attack by malicious node, the identity information such as IP address and Trust factor value has been employed. This identity information is allocated to every node in initialization phase or at the time the node is configured.
With the characteristic of self-organization and the restriction of individual resources, MANET usually faces security and attacks problem. In this work, a trusted routing protocol is developed by making use of trusted frameworks and secure protocol for MANET. When carrying out the discovery of trusted routing, dissimilar to those cryptographic approaches which carry out signature generation or verification at each routing packet, it simply combines the recommended opinions altogether and carries out a routing judgment on the basis of every element of the new opinion. In this manner, the computation overhead can be hugely minimized, and the reliability of the routing procedure can be also assured in MANET.

The trust analysis is carried out here on the basis of the honesty, reliability and the efficient parameters. In order to depict the usability of the routing protocol, it is applied to a network that has black hole attack. For every node, it detects the best trust composition and creation for maximizing the application performance. The technique is an efficient and trustworthy communication technique which can make the decision over next hop selection under the trust vector. Just a trustful node has the eligibility of transmitting data over the network.

Pirzada et al. (2006) transformed Dynamic Source Routing (DSR) protocol so that the intermediary nodes function as trust gateways which keep trace of trust levels of the nodes for preventing the malicious nodes. Every node monitors its neighbors and then sustains a direct trust value for them. Source node employs this trust information for computing the path that is the most trustworthy. The technique for the computation of trust is dependent only on the forwarding behaviour of the nodes. The node which execute the trust gateway might itself be malicious.
In this work, the trust based security model proposed is employed for guaranteeing the black hole and grey hole detection with efficiency.

3.2 METHODOLOGY FOR SELECTIVE BLACK HOLE AND GREY HOLE ATTACK DETECTION

System Model

In this section, the heterogeneous network is taken into consideration which comprises of various nodes with multiple resources. Heterogeneous MANET consists of mobile devices which have diverse communications capability like radio range, battery life, data transmission rate, etc. In the recent times, few schemes are utilized for developing the routing protocols for accommodating heterogeneous MANETs. In this work, each node is responsible for both the detection of events and serving as a router for forwarding the packets. It comprises of nodes from various manufacturers or service providers. The malicious nodes might not entirely collaborate with one another.

The trust-based approach takes the impact of both trust and QoS trust over the trustworthiness or maliciousness. The trust may consist of honesty, privacy, similarity, between centrality, and strengths. QoS trust may comprise of competence, protocol conformance, reliability, high packet delivery ratio, bandwidth consumption, lesser delay, task finishing capability, etc. In this work, it adapts honesty as a measure for trust obtained from heterogeneous networks and adapts the energy (for the measurement of competence) and collaboration for measuring QoS trust which is obtained from communication networks, since these can be regarded to be the indicators of trustworthiness. The component of honesty trust is measured by means of evidences of dishonesty like false self reporting, trust fluctuation and abnormal trust recommendations. The energy trust component yields a piece of evidence
as a compromised node generally conducts energy-consuming attacks, like the dissemination of bogus messages. Finally, a compromised node generally depicts itself to being uncooperative due to selective forwarding or message dropping attacks for disrupting the message routing in MANETs.

Black hole attack: a malicious node drops all the packets that it must forward.

Grey hole attack: an attacker discards particular kind of packets (routing packets, data packets from a designated node, etc.) and forwards just a portion of them.

In a civilian scenario, a set of people who are not familiar with one another may be inspired for cooperation to form a networked environment. Such a kind of an environment will anticipate fair play from all the participants when ‘using’ and ‘providing’ network service. A necessary feature of security scheme is to monitor that the participants meet their social commitment practically, and to form a distributed rating system, that refuses ad-hoc network services to a socially dishonest node, and simultaneously offers better services to the honest nodes through the detection of the attacks in an efficient manner.

The issues of rendering security in MANET mostly lies in the possibility to solve the black hole and grey hole attacks in heterogeneous network. In order to create a heterogeneous system, two sub-problems must be resolved, namely: a) the detection of an intruder, and b) the exposing of this information to the ad-hoc community studied by Paul et al. (2002). The procedure of revelation of information needs that the system supports at least the scheme of non repudiation. This needs a certification authority that is tedious to be rendered for a dynamic community in which any entity can take part and requires to be detected by any other entity. In addition, because of the
‘transient’ characteristic of attacks (like dropping packets) even this scheme is inadequate, since it results in a question of ‘belief’ for the ad-hoc community like whom is to be trusted, either the accusing node or the accused. In this work, it focuses primarily on the detection of certain complex attacks and its initiator, and secondly, on how to expose this information to at least few of the nodes of the system ‘believable’ way. It depends on the attacks that results in an advantage for the attacker. They have chances in either route finding stage or data-forwarding stage. This technical work, specifically, detects the attacks over Secure Dynamic Source Routing (SDSR) protocol for ad-hoc routing by utilizing only the shared secret between source and destination.

3.2.1 Trust Based Security Model

Generally, the MANET nodes are hugely constrained with respect to computational power, energy, memory, and bandwidth, hence modelling of the security schemes for MANETs is a great challenge. It initially introduces a lightweight computation technique for the evaluation of the trust value of nodes in WSNs based Duan et al. (2013).

\[
\tau(i, j)^t = \alpha \times d\tau(i, j)^t + \beta \times \frac{\sum_{(k \in \mathcal{C}_j \cap \mathcal{A}_i)} \alpha(k, j)^l}{n-1}
\] (3.1)

Inclusion of \(\alpha + \beta = 1, \alpha > 0, \beta > 0\). \((i, j)\) indicates the trust value of node \(j\) for node \(i\). \((i, j)\) refers to the direct trust value. \((k, j)\) indicates the recommendations obtained from node \(k\) that belongs to the neighbor set \(\mathcal{C}_j\) of node \(j\). \(n\) represents the number of neighbors and \(l\) indicates the order number of the evaluation records. \(\alpha\) and \(\beta\) refer to the weighed factors that are related to the security policies.

A bigger value for \(\alpha\) shows that the node in MANET is more confident about its own judgment. In the same way, a huge value for \(\beta\)
indicates that the QoS rendered by other nodes have more trustworthiness in the trust evaluation process. Moreover, the trust value varies between $0 \leq t \leq 1$. Usually, it is believed that the greater the trust value of the node is, the more trustworthy it is. The impact of conflicting behaviour attacks can be minimized by configuring sufficient values of $\alpha$ and $\beta$. Just because the behaviour of nodes gets monitored by its neighbors in the network, in case a malicious node behaves in a different manner to various nodes, it could be detected by taking the combination of direct trust and indirect trust into consideration.

The direct trust computation is expressed by

$$dt(i,j)^l = \gamma_1 \times dt_{P(j)}(i,j)^{l-1} + \gamma_2 \times dt_{N(j)}(i,j)^{l-1}$$

(3.2)

Where $dt_{P(j)}(i,j)^{l-1}$ indicates the direct trust value of node $j$ for node $i$ dependent on node $j$’s past well-behaved behaviour, while $dt_{N(j)}(i,j)^{l-1}$ refers to the direct trust value of node $j$ for node $i$ dependent on node $j$’s past malicious behaviour.

$T_{ij}^{honest\ node}(t)$: This indicates the belief of node $i$ that node $j$ is honest on the basis of node $i$’s direct observations toward node $j$. Node $i$ can monitor node $j$’s dishonesty evidences inclusive of abnormal trust recommendations, false self-reporting, and trust fluctuation over the time span $[0, t]$ for estimating $T_{ij}^{honest\ node}(t)$ node.

$T_{ij}^{energy}(t)$: This refers to the percentage of energy that remains in node $j$ that node $i$ directly sees at time $t$. In the role of a neighbor, node $i$ can overhear and also monitor node $j$’s packet transmission activities over the time span $[0, t]$ for estimating $T_{ij}^{energy}(t)$ node.
The degree of cooperativeness of node $j$ as assessed by node $i$ on the basis of direct observations over the time span $[0, t]$ is denoted by $T_{ij}^{\text{cooperative node}}(t)$. Node $i$ can use overhearing in order to find uncooperativeness behaviours like packet dropping or selective forwarding and might provide recent interaction experiences a larger priority over the old experiences in the estimation of $T_{ij}^{\text{cooperative node}}(t)$.

The throughput of node $j$ as assessed by node $i$ on the basis of the direct observations over the time span $[0, t]$ is denoted by $T_{ij}^{\text{throughput}}(t)$. Node $i$ can use technique for detecting a greater throughput in nodes such as packet selective forwarding and may provide recent interaction experiences a larger priority over older experiences in the estimation of $T_{ij}^{\text{throughput}}(t)$.

### 3.2.2 SDSR Protocol

DSR is actually a reactive protocol and is an instance of an on-demand routing protocol on the basis of the concept of source routing. It is referred to be used in multi hop ad-hoc networks of the mobile nodes. It lets a network to be self-organizing and self-configuring with no network infrastructure/management. DSR routing protocol finds the routes and sustains information concerned with them from one node to other by making use of two schemes defined by Singh et al. (1998): (i) Route discovery – finds the route between source and destination and (ii) Route maintenance –if a route fails, it evokes another destination route. The benefit of DSR is source routing.
Route Discovery

It is the time when a node S wishes to transmit a packet to a destination node D, it obtains a source route to D. Route Discovery is utilized solely while S begins to transmit a packet to D and is not aware of a route to D before.

Route Maintenance

It is a technique in which the node S detects whether the network topology had changed when utilizing a source route to D, so that it can no more make use of the route to D in the form of a link on the route which does not work. When the Route Maintenance exposes that a source route is damaged, S tries to make use of any other route it is aware to D, or initiates the Route Discovery again to find a new route. Route Maintenance is utilized actually when S transmits packets to D. Route Discovery/Route Maintenance work on demand. Dissimilar to other protocols, DSR requires no periodic packets at any level within a network. DSR does not use frequent routing advertisement, link status sensing, or neighbor detection packets. It also does not depend on these functions from any other network protocols. The on-demand behaviour and absence of periodic activity in DSR lets several overhead packets to be scaled down to zero, while the nodes are nearly stationary with regard to each other and routes necessary for the present communication have been discovered already.

The fundamental mechanism of the proposed SDSR protocol during the phase of route discovery is the establishment of a route through the flooding of Route Request (RREQ) packets in the network. The destination node, on the receipt of a RREQ packet, replies by transmitting a Route Reply (RREP) packet back to the source by doing a reversal of the route information which is stored in the RREQ Packet. On getting the RREQ, any intermediate
node can transmit the RREP back to the source node when it possesses the route to arrive at the destination. During the phase of Route maintenance, the link breaks are dealt with. A link breakage happens when any intermediate node that is involved in the packet forwarding process gets out of the range of transmission of its upstream neighbor. When an upstream node detects a link breakage while forwarding a packet to the next node present in the route path, it transmits back a Route ERRor (RERR) message to the source warning it regarding that link break. The source either attempts an alternative path that might be available or once again originates the route discovery process.

3.2.3 Black Hole Attack Detection

Black hole attack in MANETs is a critical security issue that has to be solved, where the attacker drops in falsified routing information in the routing packets received for advertising itself to have the best route to the destination. When the attacker in BHA wins in getting the route, it can interrupt the coming and conduct eavesdropping, denial-of-service, or man-in-the-middle attacks. For instance, in Figure 3.2 node N1 desires to transmit data packets to node N6 and starts the route discovery process. It is assumed that the node N2 is an attacker node with no sufficiently fresh route information to the destination node N6. But the node N2 advertises directly that it possesses the route to the destination each and every time it gets RREQ packet from node N1 and transmits the response to the RREP packet directly to the source node N1. Here, the node N2 creates a black hole in the network. Node N2 can do the misrouting of the network traffic easily to itself and then create an attack over the network.

Since Black hole attack attempts to drop the packets rather than forwarding it to its destination or eats up the interrupted packet in a silent manner, it tends to become a very serious Denial of Service (DoS) attack for a network. The effect of the attack is dependent over the kind of protocol which
is utilized by a network. Therefore, performance of the network parameters is assessed through implementing various black hole nodes. In addition, the performance is analysed by changing the pause time and various node speeds along with implementing the black hole nodes.

(Source: Mary & Vasudevan 2010)

**Figure 3.2 Black hole attack detection**

In MANET, the nodes also operate similar to a Black hole where it denies to forward each packet. The malicious node might forward the messages to the incorrect path, generating unreliable routing information in the network. Another method of selective forwarding attack is referred to as Neglect and Greed. Still it can take part in lower level protocols and might even accept the receipt of data to the sender though it discards the messages in a random manner. A node such as this is negligent. When it also provides excess priority to its own messages it also becomes greedy. Also, another type of selective forwarding attack is delaying the packets transmitting through them, generating the incorrect routing information between the nodes.

The trust-based routing guarantees a technique of message security. Nodes that are less trusted in this mechanism are provided with a message that is lesser self-encrypted parts thus rendering it hard for the malicious nodes to
have access to minimum information necessary to break through the encryption technique. Trust routing protocols must recognize the trustworthy nodes and find a reliable/trustworthy route from the sender to destination node in a few seconds or better yet in a tenth of seconds, based on the mobility of the nodes and the hops present in the route.

![Overall Block diagram of Black hole and Grey hole detection using Trust based SDSR](image)

**Figure 3.3** Overall Block diagram of Black hole and Grey hole detection using Trust based SDSR
Trust based routing preserves the messages against changes. Trust evaluation in all the network nodes- based on a new solution - was dependent on parameters such as node stability specified by mobility/pause time and the rest of the battery power. Node trust forms the basis for choosing a trustworthy transmission route. The entire block diagram is illustrated in Figure 3.3.

3.2.4 Grey Hole Discovery Process

Grey Hole attack is very harmful attack against the networks, and leads to the entire network to malfunction, and also impacts the entire networks communication. Grey Hole attack or Selective forwarding attack is easier for implementation, but very hard to detect. In the case of Grey Hole attack, normal node works nasty and shows itself normal and participates in the receipt of the packets sent from the source node, and on the receipt of packets, these nasty nodes discards the packets selected and only sends the remaining packets to the neighbor node. Hence, Selective forwarding attack or Grey Hole attack is very deleterious, that has to decided and eliminated by SDSR protocol in an efficient manner by employing trust based scheme.

If the destination node finds out that the real number of data packets it gets from its previous hop node is considerably lesser compared to the number of data packets the source node has transmitted, it begins the grey hole node discovery process. When the destination node gets the RREQ, it then verifies the number of data packets it got from its previous hop node with that provided in the RREQ. In case it gets lesser number of packets from the neighboring node than the sender node, it supposes that it is grey hole attack and moves to the next module referred to as intrusion detection.
Algorithm Procedure

1. Begin

2. Set nodes \( N = \{n_1, n_2, \ldots, n_\nu\} \)

3. Set path \( P = \{p_1, p_2, \ldots, p_\nu\} \)

4. When Route _ Request _ Packets are acquired by node

5. Update information for all nodes \( n_1, n_2, \ldots, n_\nu \)

6. if trust information in Route _ record then update distance, path and node information

7. Discover attack node using source id, trust value and route _ record information

8. Drop the attack nodes

9. Compute the parameters of node and it must be higher throughput, minimum distance and lower end to end delay

10. Choose the node which meets the condition below

\[
\text{Node} = T_{ij}^{\text{honest node}}(t) + T_{ij}^{\text{energy}}(t) + T_{ij}^{\text{cooperative node}}(t) + T_{ij}^{\text{throughput}}(t)
\]

11. Update route record employing route discovery and route maintenance process

12. End
3.3 EXPERIMENTAL RESULTS AND DISCUSSION

This work uses Network Simulator 2 (NS2) for validating the detection and exclusion efficiency of the newly introduced technique against selective black hole node. The MANETs considered are with dimensional area 1000X1000 m$^2$. A whole of 100 nodes are initialized for the purpose of evaluation. The experimental setup is tabulated in Table 3.1. The assessment of the new Threshold based EAODV is compared with that of DSR, AODV and Trust based SDSR for deciding the efficiency.

<table>
<thead>
<tr>
<th>Table 3.1 Experimental setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Area (Size)</td>
</tr>
<tr>
<td>Network Topology</td>
</tr>
<tr>
<td>MAC Layer (IEEE Standard)</td>
</tr>
<tr>
<td>IFQ Type</td>
</tr>
<tr>
<td>IFQ Length</td>
</tr>
<tr>
<td>Bandwidth</td>
</tr>
<tr>
<td>Application Type</td>
</tr>
<tr>
<td>CBR interval</td>
</tr>
<tr>
<td>No. of Packets</td>
</tr>
<tr>
<td>Simulation Time</td>
</tr>
<tr>
<td>Data Transfer Protocol</td>
</tr>
<tr>
<td>No. of Nodes</td>
</tr>
<tr>
<td>Maximum Transmission range</td>
</tr>
</tbody>
</table>
End-to-End delay

End-to-end delay indicates the time consumed for a packet to be sent across a network from the source to destination usually due to queuing and retransmission because of collision.

![Figure 3.4 Number of nodes vs End to End Delay](image)

Figure 3.4 demonstrates the comparison made for the end to end delay performance for DSR, AODV and Trust based SDSR techniques. The nodes range from 20 to 100 and end to end delay is plotted for these nodes in milli seconds (ms). The number of nodes is plotted along the x axis and the end to end delay is plotted along the y axis. The experimental result indicate that the Trust based SDSR protocol proposed yields a lower end to end delay performance in comparison with the available DSR and AODV protocols.
Packet Delivery Ratio

The ratio of packets is delivered successfully to a destination in comparison with the number of packets which have been transmitted.

Figure 3.5 Packet Delivery Ratio Comparison

Figure 3.5 illustrates the comparison between the techniques with respect to packet delivery ratio. It is evident from the graph that the new Trust based SDSR techniques yields a better performance with an effective black hole and grey hole attack detection with respect to packet delivery ratio.

Energy Consumption

Energy consumption refers to the average energy necessary for transmitting, receiving or forwarding operations of a packet to a node in the network during a period of time.
Figure 3.6 illustrates the comparison made between the techniques with respect to energy consumption. The node numbers vary from 20 to 100 and the energy is plotted for such nodes in Joule (J). The number of nodes is plotted across the x axis and the energy is plotted across y axis. The experimental results indicate that the Trust based SDSR protocol proposed yields a lesser energy consumption in comparison with the available DSR and AODV protocols. It yields a better performance with effective black hole and grey hole attack detection with respect to energy consumption.

**Throughput**

Throughput refers to the number of packets/bytes obtained by source per unit time. It is a crucial metric for the analysis of network protocols.
Figure 3.7 Throughput comparison

Figure 3.7 illustrates the comparison made between the techniques with respect to throughput. It is evident from the graph that the trust based SDSR techniques yields a better performance with effective black hole and grey hole attack detection with respect to throughput.

Packet drop rate

Packet drop happens while one or more packets of data traversing across a network don’t arrive at their destination. Packet drop rate is measured in the form of a percentage of the packets lost with regard to the packets transmitted.
Figure 3.8 Packet drop rate comparison

Figure 3.8 illustrated the comparison made between the techniques with regard to packet drop rate. It is evident from the graph that the trust based SDSR techniques yields a better performance with effective black hole and grey hole attack detection with respect to the packet drop rate.

Normalized routing load

Normalized routing load is computed to be the DSR control packets sent and forwarded divided by the number of data packets which are received.
Figure 3.9 Network lifetime comparison

Figure 3.9 illustrates the comparison made between the techniques with regard to normalized routing load. It is the proportion of every routing control packets sent by every node over the number of data packets received at the destination nodes. It is evident from the graph that the new trust based SDSR techniques yield better performance with resourceful black hole and grey hole attack detection with respect to normalized routing load. It is the ratio between the total numbers of routing packets that are sent over the network to the total number of received data packets.

Reliability

Reliability is involved with the capability of a network to conduct a necessary operation like “communication”. Figure 3.10 illustrates the association between the reliability over communications and the number of nodes. Trust based SDSR possesses a greater reliability compared to AODV and DSR. Trust based SDSR is yet considerably efficient if the number of nodes is huge.
Figure 3.10 Reliability comparison

Figure 3.10 illustrates the comparison made between the techniques with respect to normalized routing load. It is evident from the graph that the novel trust based SDSR technique gives a greater reliability value compared to AODV and DSR techniques. Trust based SDSR is yet substantially efficient if the number of nodes is huge.

3.4 SUMMARY

The secure DSR protocol is a light weight solution methodology that is basically a simple acknowledgement technique for detecting black hole and grey hole nodes in MANET. By the use of trust based attack detection, this work guarantees the QoS parameters considerably. This chapter offers black hole attack and grey hole attack over MANET in detail. In this work, the proposed technique referred to as Trust based SDSR protocol that is focused over the effective black hole and grey hole attack detections. The comparison made between the experimental results show that the scheme proposed yields
better results with respect to performance parameters. This chapter provides the conclusion that the Trust based SDSR protocol performs in a better manner over black hole and grey hole attack detection and enhances the overall network performance. The futuristic scope is with the implementation of the technique in other on-demand routing protocols and also for the detection of other attacks in MANETs.