CHAPTER 4

AN EFFICIENT SECURE ROUTING MECHANISMS FOR
PREVENTING WORMHOLE AND BLACK HOLE ATTACKS IN
TRUST DTN ENVIRONMENT

4.1 INTRODUCTION

A mobile ad hoc network (MANET) is an autonomous system of mobile stations connected by wireless link to form a network [64]. The ad hoc is connect to other devices with low power, low cost and ability to high speed networking [25]. The challenging fields of network environments are the mobile ad hoc networking and delay-tolerant networking due to the node mobility, high latency, unstable links, temporary disconnection, and the lack of infrastructure. For those purposes, the routing protocol is acting as a cornerstone of communication. This transmits the message end-to-end over multiple hops. In wireless communications, Delay/Distribution Tolerant Networks (DTNs) is identified as one of the key area and it is a class of networks there may be no contemporaneous between the source and destination. Specifically, it is more useful in providing the mission critical services like emergency situations and battlefield applications. This network do not provide the continuous connectivity between the nodes and due to lack of connectivity, it cannot able to exchange their packets regularly.

Hence, it regularly follows the store carry forward approach for routing. In this network, the nodes can misbehave by dropping the received packets and reports that it has not received anything. Moreover, the selfish node do not provide the available resources like buffer and memory for packet forwarding. This type of nodes misbehave by dropping the packets even if the node has a sufficient power and
buffer for storage. Generally, the DTNs are more vulnerable to wormhole attacks wherein the malicious nodes record the packets at one location and tunnels them to another scheming node. So, detecting wormhole attacks is important in DTN, because it significantly disturbs the performance of network. Moreover, it is heavily depends on the normal operations of ad hoc routing protocols. The wormhole attack is defined as a type of tunneling attack, where two or more nodes are collaborated to exchange the message between them via the existing routes. Figure 4.1 shows the framework of the DTN architecture.

![Figure 4.1 Framework of Delay Tolerant Network (DTN)](image)

The main intention of this work is to prevent the DTN from wormhole and black hole attacks. The overall flow of the proposed attack detection system is shown in the following Figure 4.2. Here, the DTN can allow the intermittent connectivity and assures data delivery with limited knowledge.
Figure 4.2 Overall flow of the proposed system

The advantages of DTNs are illustrated as follows,

- **Router Free** – It does not need the wireless router for connecting to the internet.
- **Mobility** – The wireless nodes present in the network can move at the same time in different locations.
- **Speed** – It does not need any additional hardware or software for network creation.
- **Fault Tolerance** – In this network, the routing and transmission protocols are designed to manage the connection failures.
• Connectivity – The use of centralized points or gateways are not necessary for the communication.

• Fast Installation – It does not require any previous installation or infrastructure for setting up the MANET.

• Cost – It eliminates the fixed infrastructure cost and reduce the power consumptions at mobile nodes.

The security goals of DTNs are as follows:

• Availability
• Confidentiality
• Integrity
• Authentication
• Non-Repudiation
• Anonymity
• Authorization

4.1.1 Availability

Availability means that the properties are accessible to only authorized users at appropriate times. It applies to both data and services and it ensures that the survivability of network service despite DoS attack.

4.1.2 Confidentiality

The confidentiality certifies that the computer related resources and properties are accessible to only an authorized users. There is a need to keep the confidentiality of the information from all entities to maintain some confidential information. Moreover, the unauthorized users do not have any privileges to access those information and it is sometimes called as secrecy or privacy.
4.1.3 Integrity

Integrity means that the properties can be altered by only the authorized parties, which includes creating, writing, changing status, and deleting. It ensures that a message being transferred is never corrupted.

4.1.4 Authentication

In DTN, the user authentication enables the identity of the node and it assures that the members in communication are authorized and not impersonate. The user authenticity is ensured because, the sender can create a message that will decrypt properly with the help of shared key.

4.1.5 Non-Repudiation

Non-repudiation assures that both the sender and receiver of a message cannot deny that they have ever sent or received the message. It is used to discriminate that if a node with some undesired function is compromised or not.

4.1.6 Anonymity

It means all information that can be used to find both the owner and a current user of a node should be private and not be distributed by node itself.

4.1.7 Authorization

It assigns various access rights to different users, for instance, only a network administrator can manages the network.

4.2 Delay/Distribution Tolerant Network (DTN) Formation

A dynamic mobile ad hoc network (MANET) on-demand routing in DTN is based on the reactive routing protocol mechanisms. In route discovery, the destination
node alone reply to the route request. If the destination node is unavailable, then the frequent node closer to the destination node will serve as the message carrier. The message carrier manages the forwarded messages and it will later deliver the message to the destination. Figure 4.3 illustrates a delay tolerant routing in MANET. When an end-to-end path may fail between the source and destination, the MANET and standard routing protocols are used. The modest routing protocols used in DTN are flooding and epidemic flooding.

![Figure 4.3 A delay tolerant routing in mobile ad hoc networks](image)

Figure 4.3 A delay tolerant routing in mobile ad hoc networks

In this scheme, the messages are copied from a single node to another node and it do not already have a copy of the message. Due to mobility and other reasons, the new nodes becomes reachable, where the additional copies are made. In DTN, the retransmission can be done at any time, because the nodes hold the message and it tolerates the intermittent connections. It uses scheduled, opportunistic and predicted connectivity to support the heterogeneous environments.

The main aim of using DTN is, it overcomes the problem of lack of connectivity, asymmetric bidirectional data rate and irregular delays. Normally, the DTN follows the node store and forward approach due to the lack of consistent connectivity. The node store and forward approach in DTN is shown in Figure 4.4.
This method is very analogous, where each data is processed and forwarded before reaching the destination.

![Diagram of Node Store and Forward in DTNs](image)

**Figure 4.4 Node Store and forward in DTNs**

In DTN, routing is considered as one of the important operation and a successful breakthrough has a direct impact on the performance of the ad hoc network. This is the major reason for the routing is being targeted by various types of attack. Moreover, the DTN is suffered from various security attacks due to its features such as, open medium, topology changing, lack of central monitoring, management, cooperative algorithms and no clear defense mechanism. The DTN routing schemes are categorized into such as, probabilistic/history based routing, model-based routing and node movement control based routing.

- Routing schemes that utilizes the deployed nodes, namely, message ferries.
- It makes use of history based information for estimating the delivery probability of peers.
• Then, it passes the message to the peer that can best deliver the message.

• If the source sends multiple copies to various relay nodes, the routing scheme uses 2 hop relay forwarding.

• If it encounters the destination, the routing schemes have the relay nodes deliver to the destination.

In this method, each node in the network is associated with a persistent storage device that stores the message for indefinite amount of time. The persistent storage is more useful for the following situations:

• When the data rate of the incoming messages is higher than the data rate of the outgoing messages.

• When the neighboring node is not available for a long time.

4.3 ATTACK MODEL

In MANET, an adversary can support various threats against DTNs for reducing the performance of the network. Here, the attacks are categorized into two types such as, external attack and internal attack. In external attacks, the intruder can cause congestion in routing to disturb the nodes from providing services. In internal attacks, an intruder needs to gain normal access based on its malicious behavior.

In DTN, the attacks are classified based on the followings:

• Attacks on routing protocols

• Attacks on packet forwarding

The DTN can be attacked from any direction at any node in the network that is completely dissimilar from the fixed hardwired networks. In this network, every node should be prepared to meet an attacker either directly or indirectly. The mobile nodes which refuse to share its resources to other nodes are known as malicious nodes. These type of nodes are from both inside and outside of the network. In DTN, it is
very difficult to detect the attacks from an affected node. Moreover, it indicates that every node in the network should not trust any node immediately.

Hence, it is very difficult to validate all the route information due to the mobility and constant changing of topology. The modification is also a type of attack and it will occur, when the malicious node can redirect the network traffic and conduct DoS attacks by changing the message fields and forwarding the route messages. In this work, there are two different attacks such as, wormhole and black hole are detected to improve the performance of the network. The framework of selfish node detection is shown in the Figure 4.5.

![Figure 4.5 Selfish node detection](image)

Different attacks severely affecting the delay tolerant networks are diagrammatically shown in Figure 4.6 and the risks in DTNs are noted as:

- Denial-of-Service (DoS) attacks
- Black hole attacks
- Wormhole attacks
- Gray hole attacks
- Confidentiality attacks
Insider attacks may cause important difficulties in networks, for example, the adversary uses the nodes to promote a specific harmful attack called black hole attack. In black hole attacks, a node presented itself as a valid node by forming forged packets and at that time it drops the packet. The malignant node is acting as the black hole in packet dropping technique. It is also said to be the packet dropping attack, as it is having the shortest path to the destination node. In wormhole attacks, a malignant node forwards the packet at one location and replays them at another location in the network.
### 4.3.1 Wormhole Attack

The wormhole attack is a severe attack as it copies the packet at one location and responses them at various locations or among the similar network. Such an attack consists of two malicious nodes. For instance, if a source node $S$ needs to communicate with a destination node $D$, then the route request will initialize by $S$ to its neighbor nodes $B$ and $C$. Figure 4.7 describe the wormhole attack in delay tolerant networks. Then, $B$ and $C$ will forwards the route request to its neighbors. $M_1$ and $M_2$ are the pair of malicious nodes, where its presence does not declare by $C$. While $M_1$ obtains the packet, it will forward or tunnels the packet to the $M_2$. Through multiple paths, the route request packets are forwarded in on-demand routing protocols.

![Figure 4.7 Wormhole Attack in DTNs](image)

### 4.3.2 Blackhole Attack

A black hole attack is a type of DoS attack that is a serious problem in network, which means that one malicious node utilizes the routing protocol. In this attack, a malicious node has the best path to reach the destination during the process of route discovery. Moreover, it sends a fake RREP message to the desired source, when it receives the RREQ from the sender. Then, the malicious node drops all the packets instead of forwarding, when the source starts the data transmission in the
network. Black hole attack is the suspicious attack in the MANET and the source node receives the fake routing information. A single black hole can easily happened in the DTN an example of black hole detection is shown in Figure 4.8.

![Figure 4.8 Black hole Attack in DTNs](image)

**Figure 4.8 Black hole Attack in DTNs**

Here, the node A is the source node and node D refers the destination node. Node C is the misbehavior node, who responses the RREQ packet that sent from the node A. It make a false reply to the source node and has the fastest route to the node D. Hence, the source node erroneously chooses the route discovery procedure. The data packets are started sending to the misbehavior node, say, node C. A malicious node may drop or consumes the packet. This problem can be regarded as the black hole as shown in Figure 4.9.
4.3.2.1 Local Monitoring in Blackhole Attack

To detect the blackhole attack in the network, the local monitoring process is carried out, it includes:

- **Packet Fake**: The outgoing packets don’t have the corresponding incoming packet.
- **Packet Alteration**: The difference between the fields of incoming and outgoing packets is calculated.
- **Wilful Packet Delay**: If the packet is forwarded between the nodes after a threshold time instead of immediately, the delay can occur.
- **Packet Lost**: If the packets are not forwarded within a maximum time, it will be lost.

This attack forges the sequence number and hop count of a routing message to obtain the desired route in the network. After acquiring the path, the attacker eavesdrop all the packets and impersonates a destination by sending a RREP to the
corresponding source node, which initiated the RREQ. Figure 4.10 shows an example scenario for black hole attack packet dropping.

Moreover, a black hole attack has two different properties, which are listed as follows:

- It exploits the routing protocol and promotes itself as it has a valid route to a destination, even though the route is fake. The main aim of this attack is to intercept all the packets in the network.
- In this attack, the attacker sends a RREP as soon as it receives the RREQ from the source node without performing any networking operations. In this way, it successively injects the black hole in the network.
4.3.2.2 Types of Blackhole Attack

The blackhole attack is classified into two types, such as:

- Internal attack
- External attack

4.3.2.2.1 Internal Attack

This type of attack has an internal malicious node in between the source and destination. The attacker node gets the information about the neighboring nodes and it attacks the network by starting the data communication. This type of attack is known is as an inner attack, because the node itself belongs to the data route. Moreover, detecting internal misbehavior of the node is difficult, because the internal attack is more accessible to secure. When an individual or group within an organization pursues to disturb the operations, the internal attack will occur. In this attack, the attacker get the admittance to access the network. Hence, this attack handles large number of resources, mechanisms to launch a refined computer attack. One of the best way to protect the network against this attack is to implement secure routing in DTNs.

4.3.2.2.2 External Attack

This type of attack creates congestion in network to disrupt the overall function of the network. It is a kind of internal attack, which take control of internal malicious node in DTNs. The external attacker aims to cause a traffic jam and to disturb the nodes in the network by propagating fake routing information. This type of attack stay outside in the network that reject access to the network traffic. It creates the congestion and disturbs the entire network. It is a type of internal attack that controls the malicious nodes to attack other neighboring nodes in the network.
In this attack, the malicious or intruder nodes find the active path of the destination node.

It spoofs the unknown destination by sending a RREP, which includes, the destination address field.

Here, the sequence number is set to the highest value and the hop count is set to the lowest value.

If the desired route is available, the malicious node sends the RREP to the nearest available node that belongs to the active path.

Once the RREP is received by the nearest available node, the malicious node will relay the established inverse route to the data of the source node.

After that, the new route is selected for data forwarding and the malicious node will drop all the packets, which belongs in the route.

4.4 TRUST EVALUATION IN NETWORK

In DTN, the concept of trust is very important for communication and protocol designing, where the trust relationship is enabled between the nodes in the network. These relations are enabled based on the sign generated by the earlier interactions of entities in a protocol. Hence, the trust will be accommodated between these entities, if the interactions have been faithful to the network protocol. The main characteristics of trust in DTN are illustrated as follows:

- Generally, the trust is not static, is dynamic.
- It is subjective, and not necessarily transitive.
- It is asymmetric, but not reciprocal.
- In DTN, the trust management framework should not assume that all nodes in the network are co-operative.
- It must be determined in a highly customized manner without any communication and computation load.

Moreover, the trust management is necessary for DTN, because it is a special case of risk management. Generally, the trust management includes the followings:

- Trust generation
- Trust establishment
- Trust evidence
- Trust distribution
- Trust discovery
- Trust update
- Trust revocation

In this work, a trust management technique is presented for black hole and wormhole attack detection. The trustiness among the nodes in the network can be estimated directly and indirectly based on the equation (1) and equation (2). Consider $T_x$ is the global reputation of the $x^{th}$ service provider (SP), $T_{xy}$ is the rating of the peers about the SP, it is calculated whenever the transaction is completed among two nodes.

$$T_{xy} = R_x \cdot W (\delta_{sc} + \delta_{tt} + \delta_{tc}) + ICT_{xy}$$  \hspace{1cm} (1)$$

$$ICT_{xy} = \sum_{v \in S} \frac{D_{v,y} D_{x,v}}{D_{x,y}}$$  \hspace{1cm} (2)$$

Here, $R_x$ refers the rating trustiness of peer $x$, $\delta_{sc}$ is the total number of successful communications, $\delta_{tt}$ mentions the total number of times the transmission occurs, $\delta_{tc}$ is the number of trust communications, $W$ denotes the weight, $T_{xy}$ states the trust value between the node $xy$, $D_{x,v}$ and $D_{v,xy}$ are the number of nodes located on
the path, v is the intermediate node, S refers the set of nodes, and $ICT_{xy}$ denotes the indirect communication trust.

### 4.5 WORM HOLE AND BLACK HOLE ATTACK PREVENTION

The RREQ packets are sent by estimating the Message Authentication Code (MAC) in secure Variable Bit-rate On-Demand Routing (VBOR) protocol. After adding the address of the source and destination, relay set, hop count, and number of security associations with regard to the RREQ. The shared secret key of the source and destination cannot able to verify the packet after the source sends RREQ packet via intermediate routers. Until reaching the destination, the MAC value and its neighbor are being transmitted via intermediate routers. The destination node can acquire several routes from several paths and has MAC value, where the message was transmitted between source and destination. The wormhole attack can be prevented using MAC value with the secret key of two users. Wormhole attacker (colluding attacker) does not find the MAC value as it cannot able to get the secret key.

The following are the steps for the encryption and decryption in the proposed approach. The inputs taken are source node S, destination node D, relay set R, hop count Hc, secret key for sender SEK_s, and the public key for both sender and receiver. The type of message for sending and receiving is taken as the data. Initially, the data is encrypted and the key is right shifted based on the destination or hop count. Hc decides how much nodes transmit and relay computation helps to choose the optimal node or path estimation. The key is generated by the value of the MAC without packet loss using MD5 for data and the final encrypted key.
4.5.1 MD5-MAC Description

Initially, the MANET is formed with the collection of wireless mobile hosts, which does not have the aid of any centralized administration or support. Then, the Message Digest (MD) 5 algorithm is employed to generate the code after authenticating the valid neighbors. The authentication service verifies the user’s identity and assures the recipient. The MD5 is a digital signature mechanism that is mainly used to verify the data integrity. The hash function MD5 can be converted into a MAC algorithm with a key K up to 128 bits. MD5 refers the MD5 algorithm without padding and the 128-bit secret key is lengthened to 128-bit subkeys K₀, K₁, and K₂. The MD5-MAC is achieved by the following modifications in MD5.

- The first value of MD5 is swapped by K₀.
- The key K₁ is divided into four 32-bit words represented by K₁[n] where (0 ≤ n ≤ 3). These are added to the constants for each MD5 iteration in round n respectively.
- The leftmost j bits of the hash value is the MAC value.

Sender Message Formation

Inputs

Source node: S
Destination node: D
Relay set: R
Hop count: Hc
Secret key for sender: SEKₛ
Public key for sender: PUKₛ
Public key for receiver: PUKᵣ
Message: Data
**Data Encryption Key**

$$\text{DEK} = \text{PUK}_s \text{ XOR SEK}_s$$

**Shifted Key**

$$\text{Shk} = \text{RightShift}_{n\text{_bit}} (H_c, \text{DEK})$$

$$\text{FEK} = \text{Shk XOR D} \ // \text{Final Encrypted Key}$$

**Encrypted Data**

$$\text{Ed} = \text{Encryption} (\text{FEK}, \text{Data})$$

$$\text{MAC} = \text{Using MD5 for Data, and FEK}$$

**New Packet Formation**

$$\text{M}(S, D, H_c, R, \text{Ed, PUK}_s, \text{MAC})$$

**Receiver Message Formation**

**Received Message**

$$\text{M}(S, D, H_c, R, \text{Ed, PUK}_s, \text{MAC})$$

**Request for Secret Key**

$$\text{SEK}_s = \text{REQ}(S, \text{PUK}_s);$$

**Data Decryption Key**

$$\text{DDK} = \text{PUK}_r \text{ XOR SEK}_s$$

**Shifted Key**

$$\text{Shk} = \text{RightShift}_{n\text{_bit}} (H_c, \text{DDK})$$

$$\text{FDK} = \text{Shk XOR D} \ // \text{Final Decrypted Key}$$

**Decrypted Data**

$$\text{Dd} = \text{Decryption} (\text{FDK}, \text{Ed})$$

$$\text{MAC} = \text{Using MD5 for Data, and FDK. The hash key is generated based on the concept of a hash function and it transforms a given input of arbitrary length to a value of a fixed length, which is known as a hash value. The hash functions are very}$$
efficient that does not require any heavy computations. It is mainly applied in the area of security for message authentication and integrity checks. The proposed MD5 is a widely used cryptographic based hash function that produces 128 bits (i.e. 16 bytes) hash value. This algorithm generally expresses the hash value in the form of a hexadecimal number (32 bits). Moreover, it processes various messages with variable length and it produces a fixed length message of 128 bits.

Here, the input message is split into chunks of 512 bit blocks (i.e. sixteen 32 bit words). The attackers in black hole receive the RREQ packets and it has the latest and a fresh route to the destination. The decryption process is initialized by requesting the secret key. It is difficult for the attacker to generate the secret key as it can be shared between the nodes. Depending on the value of the MAC, the RREQ packets are decrypted. The key is then right shifted based on the hop count and the final decrypted key with MD5 is used for decrypted data. The sender can decrypt and estimate a new MAC value by receiving the message of MAC values from the destination. The comparison of the new MAC value with the receiver side message are analyzed by the sender. If the values are same, then the sender guarantees that there are no modifications in the transmission. Otherwise, the message will be dropped and it is said to be packet dropping.

4.6 PERFORMANCE ANALYSIS RESULTS OF SECURE ROUTING MECHANISMS

The second phase of the research work proposed Secure Routing Mechanism (SRM) [4] to prevent the data from the attacks in the DTN environment. Using the relay details, a novel key generation mechanism is introduced. As a consequence, the generated key provides security for the DTN network. The main contribution of this research work is prevention from the wormhole and black hole attack in the trust DTN.
environment. The experimental results exhibit higher packet delivery ratio with respect to the number of nodes, number of hop counts, and lower latency in terms of number of nodes than the existing techniques.

The Secure Routing Mechanism (SRM) [4] and the Repetitive Trust Management (RTM) [3] are proposed in consecutive phases of this research. The performance of the SRM approach is evaluated by comparing it with the used RTM technique for an adversary detection and prevention of black hole and wormhole attacks on the trust DTN environment. The proposed method outperforms the existing RTM in terms of packet delivery ratio (with respect to the number of nodes and the number of hop counts), latency, and average delay. Table 4.1 describes the configuration parameters for the proposed work.

Table 4.1 Configuration Parameters

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTN Area</td>
<td>1000 m x 1000 m</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>20</td>
</tr>
<tr>
<td>Number of Holes (Black/Worm)</td>
<td>2</td>
</tr>
<tr>
<td>Communication Range</td>
<td>100 m</td>
</tr>
<tr>
<td>Node Speed</td>
<td>2.5 m/s</td>
</tr>
<tr>
<td>Packet Generation</td>
<td>1 packet/s</td>
</tr>
<tr>
<td>Number of Runs</td>
<td>10</td>
</tr>
</tbody>
</table>
The following metrics are measured as:

**Number of nodes**

The number of nodes denotes the number of system or devices that are connected to a network. Each device on the network has a network address such as the Message Authentication Code (MAC) address for the unique identification of each device.

**Latency**

Latency is a measure of amount of time taken by the data packets to travel between multiple points without any delay. The network latency includes propagation, transmission, routing, and other storage delays. Lower latency shows the effective communication of the data packets.

**Average delay**

The average delay is defined as the time interval between the generations of message and transferred to the final receiver. It is estimated as the average of all the received messages along with acknowledgements. The reduction in the average delay indicates the effective receiving of the messages is done at the receiver side. The average delay must be equal to 0 in the ideal situations.

**Number of hop counts**

A hop is defined as the portion of the transmission path between the source node and destination node. A hop occurs during the passage of packets to the next node through the routers. The hop count is the routing metric that refers the number of routers in the path through which the data packet passes from the source to the destination. Hop count is a rough measure of distance between two hosts. A hop count of ‘n’ means that n routers/gateways separate the source node from the destination.
node. As the hop count does not consider the speed, latency, load and reliability of a hop, it is not useful for determining the optimum network path.

### 4.6.1 Number of Nodes Versus Delivery Ratio

Table 4.2 and Figure 4.11 depicts the delivery ratio of the existing RTM and the proposed SRM with respect to the number of nodes. The delivery ratio decreases while maximizing the size of network area. Due to this fact, the probability is low among two nodes and therefore, the buffers are not empty. The proposed method yields a packet higher delivery ratio than the existing mechanism.

#### Table 4.2 Analysis of delivery ratio with respect to the number of nodes for the existing RTM and the proposed SRM

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>Delivery Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RTM</td>
</tr>
<tr>
<td>1</td>
<td>0.832</td>
</tr>
<tr>
<td>2</td>
<td>0.822</td>
</tr>
<tr>
<td>3</td>
<td>0.801</td>
</tr>
<tr>
<td>4</td>
<td>0.785</td>
</tr>
<tr>
<td>5</td>
<td>0.735</td>
</tr>
<tr>
<td>6</td>
<td>0.698</td>
</tr>
<tr>
<td>7</td>
<td>0.642</td>
</tr>
<tr>
<td>8</td>
<td>0.601</td>
</tr>
<tr>
<td>9</td>
<td>0.556</td>
</tr>
<tr>
<td>10</td>
<td>0.512</td>
</tr>
</tbody>
</table>
4.6.2 Number of Hop-Count Versus Delivery Ratio

Table 4.3 and Figure 4.12 shows the delivery ratio with respect to the number of hop counts for the Existing RTM and Proposed SRM system. The proposed SRM methodology has a higher delivery ratio than the previous RTM.

Table 4.3 Analysis of delivery ratio with respect to the number of hop counts for RTM AND SRM

<table>
<thead>
<tr>
<th>Number of Hop Counts</th>
<th>Delivery Ratio RTM</th>
<th>Delivery Ratio SRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.82</td>
<td>0.92</td>
</tr>
<tr>
<td>2</td>
<td>0.82</td>
<td>0.92</td>
</tr>
<tr>
<td>3</td>
<td>0.81</td>
<td>0.91</td>
</tr>
<tr>
<td>4</td>
<td>0.75</td>
<td>0.91</td>
</tr>
<tr>
<td>5</td>
<td>0.75</td>
<td>0.89</td>
</tr>
<tr>
<td>6</td>
<td>0.68</td>
<td>0.88</td>
</tr>
<tr>
<td>7</td>
<td>0.62</td>
<td>0.82</td>
</tr>
<tr>
<td>8</td>
<td>0.61</td>
<td>0.81</td>
</tr>
<tr>
<td>9</td>
<td>0.56</td>
<td>0.76</td>
</tr>
<tr>
<td>10</td>
<td>0.52</td>
<td>0.71</td>
</tr>
</tbody>
</table>
4.6.3 Number of Nodes Versus Latency

Table 4.4 and Figure 4.13 describes the latency or delay of the existing RTM and the proposed SRM system with respect to the number of nodes. It measures the time that is taken for the transmission of data packets from one point to the other point. The proposed SRM has a higher latency than the existing RTM. The latency of SRM increases gradually for each number of nodes.
Table 4.4 Analysis of latency with respect to the number of nodes for RTM and SRM

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>Latency (RTM)</th>
<th>Latency (SRM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.05</td>
<td>0.02</td>
</tr>
<tr>
<td>2</td>
<td>0.14</td>
<td>0.18</td>
</tr>
<tr>
<td>3</td>
<td>0.18</td>
<td>0.11</td>
</tr>
<tr>
<td>4</td>
<td>0.2</td>
<td>0.13</td>
</tr>
<tr>
<td>5</td>
<td>0.24</td>
<td>0.17</td>
</tr>
<tr>
<td>6</td>
<td>0.29</td>
<td>0.2</td>
</tr>
<tr>
<td>7</td>
<td>0.34</td>
<td>0.23</td>
</tr>
<tr>
<td>8</td>
<td>0.36</td>
<td>0.25</td>
</tr>
<tr>
<td>9</td>
<td>0.38</td>
<td>0.27</td>
</tr>
<tr>
<td>10</td>
<td>0.42</td>
<td>0.31</td>
</tr>
</tbody>
</table>

Figure 4.13 The results of latency with respect to the number of nodes for the existing RTM and the proposed SRM
4.6.4 Number of Attacks Versus Delivery Ratio

Table 4.5 and Figure 4.14 shows that the proposed mechanism exhibits better delivery ratio for black hole and wormhole with respect to the number of attacks. For each number of attacks, the delivery ratio calculates the fraction of messages. The network is able to receive the packets during the presence of the black hole and wormhole attacks.

Table 4.5 Analysis of delivery ratio with respect to the number of attacks for the black hole and wormhole

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>Delivery Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Black Hole</td>
</tr>
<tr>
<td>1</td>
<td>0.8</td>
</tr>
<tr>
<td>2</td>
<td>0.71</td>
</tr>
<tr>
<td>3</td>
<td>0.65</td>
</tr>
<tr>
<td>4</td>
<td>0.54</td>
</tr>
<tr>
<td>5</td>
<td>0.4</td>
</tr>
</tbody>
</table>

Figure 4.14 Results of delivery ratio with respect to the number of attacks for the black hole and wormhole
4.6.5 Number of Attacks Versus Average Delay

Table 4.6 and Figure 4.15 shows the average delay of the existing RTM and proposed SRM with respect to the increase in the number of black hole and wormhole attacks. From the graph, it is clearly observed that the average delay for black hole and wormhole increases gradually for each and every number of attacks. The average delay for the black hole attack is relatively lower than the average delay for the wormhole attack.

Table 4.6 Analysis of an average delay with respect to the number of attacks for the black hole and wormhole

<table>
<thead>
<tr>
<th>Number of Attacks</th>
<th>Average Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Black Hole</td>
</tr>
<tr>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>125</td>
</tr>
<tr>
<td>3</td>
<td>136</td>
</tr>
<tr>
<td>4</td>
<td>149</td>
</tr>
<tr>
<td>5</td>
<td>168</td>
</tr>
</tbody>
</table>

Figure 4.15 The results of an average delay with respect to the number of attacks for the black hole and wormhole
4.7 SUMMARY

- In Delay Tolerant Networks (DTNs), the wormhole and black hole attacks are harmful in distracting the operation of typical networks.
- The packet is passed intermediate the source node and the destination node need a trust environment.
- An attacker acquires packet at one location and tunnels them to a different location. Due to the lack of secure routing for finding the valid routes in existence, an efficient secure routing mechanism is proposed in this paper.
- Based on the details of the relay, a novel key generation approach is presented to provide security for the DTN network.
- The wormhole and black hole attack prevention is performed based on the analysis of these mechanisms. The performance analysis of the proposed method shows better delivery ratio and latency in terms of number of nodes.
- The computed trusted value is compared with the threshold value and the decision is made, whether to consider or eliminate the node.
- Timing request is sent to the particular packet and the sender waits for the acknowledgement from the packet.
- The wormhole and black hole attack prevention is performed based on the analysis of these mechanisms.
- The performance analysis of the proposed method shows better delivery ratio and latency in terms of number of nodes.
- The third phase of the research work proposed an efficient approach for enhancing privacy preservation in the DTN.
The proposed scheme effectively detects the malicious nodes and performs better in terms of packet delivery ratio, mean absolute error and execution time.