CHAPTER 6

SECURE CLUSTER-BASED MULTIPATH ROUTING SCHEME

6.1 INTRODUCTION

Communication between mobile nodes is the most problematic issue for forwarding packets between mobile nodes in a MANET. Each node can forward data packets for other nodes using open media, which makes it possible for the malicious nodes to launch various attacks, such as a black hole attack, wormhole attack and rushing attack. It causes great security challenges and makes it difficult to design secure routing in a MANET. Secure routing plays a vital role in forwarding packets in critical applications. And also, the reliable routing of packets between the nodes becomes very challenging in MANET because its dynamism of topology changes. Multipath routing is also a great challenge in MANET due to the dynamic network environment.

A MANET is at a greater risk by allowing the extended presence of security attacks, but is more likely to have preinstalled security mechanisms to detect these security attacks (Aarti & Tyagi 2013). Malicious nodes in sparsely populated networks can be more harmful than malicious nodes in a densely populated network since these nodes can effectively not only disrupt communication but also disconnect the network. The level of effort required of resource constrained devices to monitor, detect, and diagnose malicious activity in a dynamic ad hoc network may be too costly when compared to the
cost of simply rerouting packets through an alternative path. In a densely populated network where several alternative paths are typically available, selecting an alternative route may be a more judicious use of limited resources. Diffie-Hellman key exchange protocol (Shobana & Suresh 2013) is a suitable mechanism for obtaining secure communication in MANET. But sharing the keys between the source and destination is an issue owing to the unreliable communication offered in a critical environment. Further, to establish multiple node disjoint routes in a route discovery attempt and exclude unreliable routes before transmitting packets, multipath routing scheme (Abbas & Jain 2010) is determined as a suitable mechanism for effective routing in MANET. This mechanism is followed in the proposed scheme for achieving energy-efficient secure routing.

Existing secure routing protocols (Yujun et al 2014) (Burmester & Medeiros 2009) designed for a MANET face a number of problems. The problems include the fault detection mechanism that is not considered into the network by data transmission strategy. It depends on the acquisition of network topology which points out the necessity of hiding topology in designing the routing protocols in MANET. To address these issues, it is desirable to design an efficient and secure cluster-based multipath routing scheme for MANET. Further, designing secure multipath routing protocols requires a detailed knowledge about technology followed in a MANET and their peculiar features relevant to security aspects. Thus, effective secure multipath routing and reliability are quite essential to protect nodes from anonymous behavior. In order to enhance the security and reduce the attacks, a Secure Cluster-based Multipath Routing Protocol (SCMRP) is proposed to establish multiple node disjoint routes and to enhance security.

The SCMRP consists of three phases such as cluster formation, establishment of multipath routing and secure path selection. A hierarchical
cluster formation technique is used to form the clusters. A cluster head is selected based on cluster weight factor that is considered as the highest remaining energy, mobility factor and transmission range. SCMRP creates multiple paths between source and destination that eliminate unreliable routes. SCMRP also used Dynamic Secret-based Encryption (DSE) to enhance security. During the routing establishment, dynamic encryption key is updated by the retransmission sequence. The simulation reveals that the SCMRP protects the nodes against eavesdropping by updating the dynamic encryption key with retransmission sequence in routing even when the attackers know the details of DSE scheme and obtain the encryption key at some time.

6.2 NEED FOR SECURE ROUTING FOR MANET

The communication between mobile nodes is the most problematic issue for forwarding packets between mobile nodes in a MANET. Each node can forward data packets to the other nodes using open media, which makes it possible for the malicious nodes to launch various attacks, such as a black hole attack, wormhole attack and rushing attack. It causes great security challenges and makes it difficult to design secure routing in MANET.

The main problems are: node mobility and link failure. However, node mobility provides dynamic change topology, and route breaks occur frequently providing degradation of upstream on wireless network because of not only high loss of packets but also delay to search new routes. One of the most important aspects of the secure communication process (Papadimitratos & Haas 2006) is the design of the routing protocols used to establish and maintain multi-hop routes to allow the communication of data between nodes. While this might be sufficient for a certain class of MANET applications, it is not adequate for the support of more demanding applications such as multimedia audio and video. MANET is vulnerable to many passive and active attacks. Considering passive attacks, the attacker can only eavesdrop or
monitor the network traffic (Goyal et al 2010) (Wu et al 2007) and try to achieve valuable information. But in active attacks, the attacker is not only able to listen to the communications but also it is able to alter or manipulate it. Primarily, MANET is vulnerable to the following active attacks:

- Sybil attacks that the adversary presents more than one identity to network nodes (Ssu et al 2009).
- Replay attack that the adversary replays the previously transmitted messages.
- Spoofed data attack that the adversary intercepts, alters data and transmits them to the destination.
- Wormhole attack: that an attacker receives packets at one point, tunnels them and replays them into another point in the network. This tunnel between the two colluding attacks is known as a wormhole.
- Black hole attack that the attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. Then it drops all packets that receive instead of forwarding those (Su 2011).
- Gray-hole attack which is a routing misbehavior that leads to the dropping of messages. This attack consists of two phases. Regarding the first phase, the attacker advertises as having a valid route to destination and in second phase, the attacker drops received packets occasionally.
- Sinkhole attack that a compromised node tries to attract and drops data from all neighbouring nodes (Tseng & Jack Culpepper 2005).
• Denial of service attacks that are aimed to complete disruption of ad hoc network.
• Selfish nodes which use network for their advantage and do not participate in operations to save energy.

6.3 NEED FOR MULTIPATH ROUTING FOR MANET

Generally, multipath routing is established in order to increase the reliability of data transmission that provides load-balancing among the nodes. The use of multiple disjoint paths transferred the data in parallel that significantly increases the packet delivery ratio. Multipath routing for transmission is very prone to the security threats. It is necessary to provide the secure based multipath routing schemes for the reliable transmission of packets. However, the presence of malicious nodes on the selected multipath affects the efficiency of network performance by decreasing the packet delivery ratio. Multipath routing schemes have attracted a lot of attention recently in a MANET for their unique capability in supporting load-balancing and improving routing reliability in high dynamic scenarios.

However, multipath routing protocol may become vulnerable for the malicious nodes to explore and launch various attacks. Moreover, it almost turned the multipath routing scheme to increase network lifetime. Multipath routing scheme reduces the routing overhead significantly. There are several schemes to find multiple loop-free paths in a route discovery, Ad hoc On-demand Trusted-path Distance Vector (AOTDV) (Li et al 2010), Enhanced Multi-Path Dynamic Source Routing algorithm (EMP-DSR) (Asl et al 2009), energy-efficient secure multipath AODV (Jain & Sharma 2014), TOpology-Hiding multipath Protocol (TOHIP) (Yujun et al 2014), Dynamic Secret Encryption Scheme(DSES) (Ting et al 2014) that enhancing network lifetime.
TOHIP analyzed the threats of topology exposure. It provides the capability to find better routes. TOHIP has more routing overhead than SRP when it is measured in bytes. The authors did not use any efficient security algorithm to prevent the attacks. DSES applied the concept of dynamic secret to design an encryption scheme for smart grid wireless communication. It has good compatibility, which could be integrated with many wireless techniques and applications. Since the length of retransmission sequences is used to generate the secret key, the attackers can hack that secret key very easily. It is applied on wireless smart grid network.

Secure multipath routing protocol (SMRP) (Burmester & Medeiros 2009) proposed a discovery algorithm with a security proof. This algorithm is vulnerable to a hidden channel attack. SMRP analyzed the security framework used for route discovery. An Authenticated Anonymous Secure Routing (AASR) (Wei Liu & Ming Yu 2014) defends against potential active attacks without unveiling the node identities. In this scheme, the route request packets are authenticated by a group signature. AASR used a key-encrypted onion routing with a route secret verification message to prevent intermediate nodes from inferring a destination. It causes routing overhead by using more control packets to ensure the security.

From the previous works, it is essential to design the multipath routing protocol. And also, it is necessary to select the best path for secure routing in MANET. TOHIP is not considered the best path among multiple paths in MANET. The proposed scheme enhances security in multipath routing and to detect the best path among multiple paths by considering energy, link quality and minimum distance between nodes.
6.4 THE PROPOSED SECURE CLUSTER-BASED MULTIPATH ROUTING SCHEME

The proposed scheme purposely observed the issues of secure cluster-based multipath routing in MANET which allows multiple paths between a source and a destination. The proposed scheme used a Dynamic Secret-based Encryption mechanism in multipath that provides the security during the transmission of packets. And also, it is very important to select a path with no malicious node from the multiple paths to achieve secure routing. The better path is selected by considering the metrics such as energy, distance and link quality. The proposed scheme consists of the following phases:

• Cluster formation
• Establishment of Multipath Routing
• Secure path selection

6.4.1 Cluster Formation

The SCMRP used a Hierarchical-based cluster formation technique to partition the group over a variety of scales. It used a methodology for selecting energy-efficient cluster head. A cluster weight factor is calculated for the mobile node based on the metrics such as highest remaining energy, mobility factor and Transmission range. The highest remaining energy of all nodes is calculated by Equation (6.1)

\[ E_{HR} = E_T - (E_{ideal} + E_{Tx} + E_{Rx}) \]  

(6.1)

where \( E_{HR} \) is the highest remaining energy of a node, \( E_T \) is the total energy of a node, \( E_{ideal} \) is the initial energy of node, \( E_{Tx} \) is the transmission energy of a node, and \( E_{Rx} \) is the receiving energy of a node. The mobility of the node is
calculated as the rate of position of a mobile node with respect to time. Nodes update packets frequently at high speed during travel. Here, node with less mobility is considered as a factor. Source node knows the mobility of all nodes. The mobility of a node is expressed by Equation (6.2)

\[ M_f = \frac{1}{T} \sum_{t}^{T} \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \]  

(6.2)

\( M_f \) mobility of a node \( \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2} \) is the distance between sender and all nodes. \( T \) is the time. During the route request phase, the sender node calculates the distance between sources’ nearest nodes. Transmission range \( TR \) of a node is calculated by Equation (6.3)

\[ TR = \prod_{i} \sqrt{(x_i - x_{i-1})^2 + (y_i - y_{i-1})^2} \]  

(6.3)

A node with the highest weighted factor is selected as a cluster head that is based on a weighted factor such as the highest remaining energy, the less mobility and the large transmission range. The aim of clustering process is to eliminate far away nodes from participating in the routing process. Figure 6.1 shows the scenario of secure cluster-based multipath routing in a MANET. In this scenario, nodes 4, 8, 9 and 21 are not involved in the routing phase. This process also increases the network lifetime.

6.4.2 Establishment of Multipath Routing

This section presents the establishment of multipath routing in MANET. Multipath routing possesses three phases: route request phase, route reply phase and route probe phase.

- Route request phase creates a reverse route which is used in route reply phase. In this phase, route request messages are
transmitted from source to destination. After receiving the route request message, every intermediate node creates a reverse route and rebroadcasts them if the message is not received before.

- Route reply phase finds many node disjoint routes as possible in route message. In this phase, route reply messages are transmitted from destination to source node. After receiving a reply message, an intermediate node picks the neighbour, which is close as to the source node, and therefore multiple node disjoint routes are established.

- Route probe phase detects the unreliable route and excludes it before sending out the packets. The source node sends a route probe message through every exposed route in route reply message to the destination node. By performing this action, the unreliable route is detected and eliminated.

In these three phases, every node maintains two tables. One is Sequence Number Table (SNT) which is used to prevent nodes from unnecessary route messages. The other is a Routing Table (RT) that includes the node through which to reach the destination and determine the number of hops to the destination.

### 6.4.3 Secure Path Selection

The best path is selected from the multipath by considering the matrices such as energy, link quality, and distance. The shortest distance of a routing path is calculated by Equation (6.4)

\[
SR_{min} = \sqrt{(x_t - x_{t-1})^2 + (y_t - y_{t-1})^2}
\]  

(6.4)
The energy of a route is calculated by Equation (6.1). The link quality between nodes is measured by radio signal strength that is found by Equation (6.5)

\[ l_q = \frac{s_p}{s_{max}} \]  

where, \( s_p \) is the signal strength of a path, and \( s_{max} \) is the maximum signal strength available of a path. Finally, a path with minimum distance, efficient link quality and maximum energy is selected as a better path for transmission. Security mechanism is applied in the selected path for enhancing secure data transmission. It detects three security attacks such as wormhole attack, black hole attack and rushing attack during the communications between the nodes in a selected path.

![Scenario for secure multipath routing](image)

**Figure 6.1 Scenario for secure multipath routing**
Figure 6.1 shows the secure multipath routing scenario. Initially, the source (S) initiates Route Probe Phase (RPRO) by sending a route probe message to the destination (D) through every route that has been established in Route Reply Phase. In every RPRO, D is required to send an RPRO message back to S through a reverse route. In RPRO phase, S detects the secure routes. If there are malicious nodes present in the path p1 that may drop the packets, S may not receive the returning RPRO message on that path p1. Immediately, S selects another path like p4 or p2 according to Figure 6.1.

In wormhole attack, an attacker records packets or bits at one location in the network, tunnels them to the selected location, and retransmits them into the network. Wormhole misleads to consider a route that is shorter than the original one within the network; this can confuse the routing mechanism which relies on the knowledge about the distance between nodes. The attacking node captures the packets from one location and transmits them to other distant located nodes which distribute them locally. The tunnel is either wired link or a high frequency links. This creates the false impression that the two end points of the tunnel are very close to each other which leads to routing disruption.

In a MANET, a black hole attack is a type of denial-of-service attack in which a router is supposed to relay packets instead discarding them. Black holes refer to places in the network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its planned receiver. When investigating the topology of the network, the black holes themselves are hidden, and can only be identified by observing the lost traffic.

When a node sends a route request packet (RR) to another node in the network, if there is an attacker present, then it accepts the RR packet and
sends it to their neighbours with higher transmission speed as compared to the other nodes. Because of this high transmission speed, the packet forwarded by the attacker first reaches to the destination node. Destination node accepts this RR packet, and discards the other RR packets which reached later. The receiver found this route as a valid route and used it for further communication. This way the attacker successfully gains access in the communication between the sender and the receiver.

In order to prevent attacks, the proposed scheme used a Dynamic Secret-based Encryption mechanism (DSE). The DSE is applied in a selected path to enhance the security and reduce the attacks during communication. A dynamic secret concept is applied to design an encryption scheme for node communication. Between two nodes of communication, the previous packets are coded as retransmission sequence, where the retransmitted packet is marked as ‘1’, and the other is marked as ‘0’. During the communication, the retransmission sequence is generated on both sides to update the dynamic encryption key. Any missing retransmission sequence would prevent the adversary from achieving the keys. Considering the limitation on computational power, the hash functions are used in the Dynamic secret generation that is expressed by Equation (6.6)

\[ ds(k) = f_1H(\varphi_1(L,Rs)) \]  

(6.6)

where \( ds(k) \) is the dynamic secret key, \( f_1H \) is the hash function, and \( Rs \) is the re-transmission sequence. The new dynamic secret is applied to update the Dynamic Encryption Key (DEK) that is calculated by Equation (6.7)

\[ DEK(k) = Ds(k) \oplus DEK(k-1) \]  

(6.7)

A DEK is generated on both sides of communication synchronously. The sender applies it to encrypt the message, and the receiver applies it to
decrypt the same. XOR function is applied to update the DEK that is used to encrypt or decrypt the data on both sides. Encryption and decryption are expressed as follows.

\[ D \oplus Dek^*(k) = C_D \]  \hspace{1cm} (6.8)

\[ C_D \oplus Dek^*(k) = D \]  \hspace{1cm} (6.9)

If DEK is shorter than the data, it is replicated and padded circularly to generate whose length is equal to the raw data or cipher text. DSE scheme is an appropriate solution for securing wireless communication. It can prevent eavesdropping and forging by utilizing the inevitable errors in communication.

6.5 SECURITY ANALYSIS

In this section, security of SCMRP is analyzed in the presence of different attacks. Thus, the potential damages incurred by malicious nodes are greatly reduced or even eliminated. The security of SCMRP is analyzed in resisting the following attacks when the attacks are launched from different situations.

6.5.1 Black Hole Attack

A black hole attacker disrupts route discovery by forging a route to the destination. A typical attack is launched when Source broadcasts a route request to search a route to destination, attacker replies and advertises a route from itself to destination. If source sends packets to destination through the same route, the attacker can intercept and discard the packets. Since SCMRP does not allow intermediate nodes to send route reply messages, it can resist the black hole attack.
6.5.2 Spoofed Route Signaling

Route discovery packets are encrypted by a source and destination using either an asymmetric or shared key. Only the source and destination have the right keys to decrypt them. Thus, the impersonation attacks are completely prevented.

6.5.3 Fabricated Routing Messages

In SCMRP, each routing message is verified at an intermediate node. The message reaches the destination using multiple paths. By using message and route redundancy, an intermediate node will be detected if the message is modified. Later, a lower trustworthiness value will be given to that node. When the trust value of the node is below a threshold, the node will be labeled and removed from the routing table. Therefore, the fabrication of routing messages can be prevented.

6.5.4 Securing Shortest Paths

In SCMRP, multiple paths are built from a source to a destination during route discovery. The destination can choose a path with minimum cost to send back a reply, which can be the most trusted or shortest path with minimum delay, the shortest path with minimum hop counts. Whereas SCMPR may choose a path as the shortest path on which an RREQ packet arrives at the destination first.

6.5.5 Byzantine Attacks

In SCMRP, a node receives multiple copies of the same message, which are forwarded by different nodes and protected by Dynamic Encryption Key at different segments on a route. The node can find discrepancies by comparing these copies. If some of the nodes that forward the message are
more trust worthier than others, it can immediately claim those that do not forward a message correctly as colluding nodes.

6.5.6 Sybil Attacks

A Sybil attacker disrupts route discovery by impersonating multiple legal nodes. To launch this attack, the attacker first obtains the identity of a set of legal nodes and then impersonates some or all of them to participate in multiple route discoveries. SCMRP does not include identity of nodes in the routing messages, because during the communication, the retransmission sequence is generated on both sides to update the dynamic encryption key and thus it is impossible for malicious nodes to obtain the identity information of other nodes. Therefore, SCMRP is resistant to sybil attack.

6.6 SIMULATION AND RESULTS

6.6.1 Simulation Study

The proposed scheme has been implemented in network simulator (NS2). The main objective of the simulation was to enhance energy-efficiency to increase the network lifetime. 200 nodes were randomly deployed in a 1000 m x 1000 m area of interest. The transmission range of the node was 50 m, and initial energy is assigned with 10 joules. Nodes followed the random waypoint model that finds the availability of connection paths in MANET, where nodes are moving at six different uniform speeds ranging between 0 to 30 m/s. The proposed scheme is also evaluated by comparing it with the related TOHIP and SRP protocols in terms of packet delivery ratio, energy consumption, throughput and routing overhead. The simulation results were studied by varying the network size from 50 to 200. Table 6.1 shows the simulation parameter setting for the evaluation of the proposed scheme and the related schemes.
Table 6.1 Parameter settings for simulation (SCMRP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation area</td>
<td>1000m x 1000m</td>
</tr>
<tr>
<td>Number of mobile nodes</td>
<td>50,100,150,200</td>
</tr>
<tr>
<td>Simulation time</td>
<td>1000sec</td>
</tr>
<tr>
<td>Number of source–destination pair</td>
<td>10</td>
</tr>
<tr>
<td>Node movement speed</td>
<td>30 m/sec</td>
</tr>
<tr>
<td>Initial energy</td>
<td>10 j</td>
</tr>
<tr>
<td>Transmit energy</td>
<td>0.5j</td>
</tr>
<tr>
<td>Receiver energy</td>
<td>0.1j</td>
</tr>
<tr>
<td>Ideal energy</td>
<td>0.01j</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Number of attacker</td>
<td>20</td>
</tr>
</tbody>
</table>

6.6.2 Algorithms used for Comparison

The system TOHIP (Yujun et al 2014), AASR (Wei Liu & Ming Yu 2014) and the system SMRP (Burmester & Medeiros 2009) are taken for comparison to evaluate the performance of the proposed scheme.

TOHIP establishes multiple node-disjoint routes in a route discovery and excludes unreliable routes before transmitting packets. TOHIP is loop-free and does not expose network topology. SMRP used a discovery algorithm with a security mechanism. This algorithm is vulnerable to a hidden channel attack. SMRP analyzed the security framework in the route discovery. AASR defends against potential active attacks without unveiling the node identities. In this scheme, the route request packets are authenticated by a group signature. AASR used a key-encrypted routing with a route secret verification message to prevent intermediate nodes. It causes routing overhead...
by using more control packets and routing packets to establish routing and to ensure security. However, this scheme is unable to address secure routing effectively, selective dropping attack and energy consumption caused by a number of attackers in a MANET.

### 6.6.3 Results and Discussion

This section describes the results obtained through simulation of the proposed scheme. The experimentation is performed by varying the count of attackers in the network. The results obtained are analysed by varying the size of the network. The efficiency of the proposed and the related schemes is evaluated using the metrics such as packet delivery ratio, total energy consumption, end-to-end delay, signal strength ratio, and routing overhead. The simulation results show that the proposed scheme achieves maximum efficiency when compared with the other related schemes.

**Packet Delivery Ratio:** The packet delivery ratio can be determined as the ratio of the number of packets successfully delivered to the destination of the number of packets sent by the source along the path. It shows the capability of the proposed mechanism to deliver the data to the destination.

**End-to-End Delay:** The end-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

**Routing Overhead:** Routing overhead refers to the total number of routing packets that are transmitted during the simulation time from source to destination. For packets sent over multiple hops, each transmission of the packet counts as one transmission. The proposed scheme has estimated the routing overhead in varying nodes.
**Energy Consumption:** Energy consumption is the total energy that is spent to deliver the packets successfully across a network from source to destination.

**Signal Strength Ratio:** The Signal Strength Ratio displays the ratio of the Vertical path received signal power to the Horizontal path received signal power. This ratio can be useful for determining multipath conditions in ad hoc networks.

### 6.6.3.1 End-to-end delay

Figure 6.2 shows that the proposed schemes SCMRP achieves minimum delay about 0.6sec for forwarding packets to the destination in the presence of 20 attackers because the proposed scheme selected the energy-efficient, secure attacker-free routing path to involve the packet transmission. It has also chosen an alternate path for forwarding packets when the attacker is present. It shows that the SCMRP achieved minimum delay compared to the related schemes because it does not consider the attacker to involve in the routing phase. The proposed scheme and the related schemes TOHIP, SMRP and AASR have the end-to-end delay in the range of 0.6sec, 0.7sec, 0.79sec and 0.8sec respectively in the presence of an attacker. Figure 6.3 shows that this metric keeps minimum delay relatively stable, which proves that the proposed SCMRP does not degrade the efficiency of delivering packets with minimum delay at maximum speed 30 m/sec. It also provides the secure multipath routing with the best path when compared to the existing methods.
Figure 6.2 End-to-end delay vs. number of attackers

Figure 6.3 End-to-end delay vs. speed
6.6.3.2 Routing overhead

The routing overhead is evaluated for SCMRP, TOHIP, AASR and SMRP while varying the number of nodes. It is defined as the number of routing packets transmitted for establishing routing paths that caused minimum routing overhead. Figure 6.4 shows that the routing overhead caused by SCMRP has transmitted less routing packets than the related schemes. SCMRP has transmitted an average of 4500 routing packets for forwarding packets in the selected routing path with scheduled simulation time. The related schemes had required more routing packets for the routing purpose that led to routing overhead.

![Figure 6.4 Routing overhead](image)

6.6.3.3 Packet delivery ratio

Figure 6.5 shows the packet delivery ratio by varying the nodes in the network. The SCMRP scheme is compared with related schemes TOHIP, SMRP and AASR. It shows that the proposed schemes maintained higher
PDR about 98%. An intensive performance evaluation shows that the proposed scheme has better capability of finding routes. When there are malicious nodes, the proposed scheme can greatly improve the packet delivery ratio. The PDR of the proposed schemes gets increased when the number of nodes increases. It shows that the packet delivery ratio increases for the proposed model since it provides the multipath routing with the secure path when compared with the existing methods. It was shown that the performance of the proposed scheme is more efficient than the related schemes. Normally, the value of PDR gets increased in the proposed model since it sends the number of data at a time when compared to the related schemes. It has been shown that the value of PDR increases since it provides secure multipath routing with the best path.

![Figure 6.5 Packet delivery ratio](image)

*Figure 6.5 Packet delivery ratio*
6.6.3.4 Energy consumption of the network

Figure 6.6 shows the total energy consumption of a network while varying number of nodes. It is noticed that the SCMRP consumes minimum energy about 15.52 J while varying the number of nodes. TOHIP has longer convergent time because it tends to establish longer routes and to find as many nodes-disjoint routes as possible in a route discovery attempt to prevent route discovery from being invoked frequently. The other two related schemes such as SMRP and AASR do not consider the energy factor, and also it required more control packets to establish secure routing that causes more energy consumption. The proposed SCMRP selects the shortest path that offers more efficient results with less energy consumption. In the proposing SCMRP, the energy consumption of a node increases slightly as the number of nodes increases. This is because the clustering technique provides the minimum nodes to participate in the routing. Also, this figure shows that SCMRP does not consume more energy. SCMRP based network shows stability with increasing number of nodes..

![Figure 6.6 Total energy consumption of the network](image)
6.6.3.5 Signal strength ratio

Figure 6.7 shows the signal strength ratio (SSR) by varying the nodes in the network. It shows that the proposed scheme maintained more SSI than the related schemes. The SSR of SCMRP gets increased when the number of nodes increases. It shows that the packet delivery ratio increases for the proposed model since it provides more link quality between nodes in selected best path that shows more efficient forwarding packets without loss. The related schemes have less SSR because it does not consider link quality for establishing routing paths. Normally, the value of SSI gets increased in the proposed scheme since it sends the number of data in a time when compared to the related schemes.

![Figure 6.7 Signal strength ratio](image)

Figure 6.7 Signal strength ratio
Table 6.2 Comparative analysis of SCMRP with the existing schemes.

<table>
<thead>
<tr>
<th>Performance Metrics</th>
<th>TOHIP</th>
<th>SMRP</th>
<th>AASR</th>
<th>SCMRP Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-End delay (sec) vs. no of attacker</td>
<td>0.7</td>
<td>0.79</td>
<td>0.8</td>
<td>0.6</td>
</tr>
<tr>
<td>End-to-End delay (sec) vs. maximum speed</td>
<td>0.81</td>
<td>0.87</td>
<td>0.9</td>
<td>0.7</td>
</tr>
<tr>
<td>Total energy consumption (j)</td>
<td>24.23</td>
<td>26.22</td>
<td>27.45</td>
<td>15.52</td>
</tr>
<tr>
<td>Packet delivery ratio (kb/sec)</td>
<td>96.94</td>
<td>95.98</td>
<td>87.91</td>
<td>98.07</td>
</tr>
<tr>
<td>Signal strength Ratio (db)</td>
<td>3897</td>
<td>3678</td>
<td>3456</td>
<td>4213</td>
</tr>
<tr>
<td>Routing Overhead (RTP)</td>
<td>7235</td>
<td>7899</td>
<td>8189</td>
<td>64440</td>
</tr>
</tbody>
</table>

Table 6.2 shows the comparison of SCMRP with the related schemes for different parameters. The parameters may be the End-to-End delay, packet delivery ratio, routing overhead, energy consumption and signal strength ratio. The proposed scheme achieved less energy consumption, delay and routing overhead because it forms stable clusters with multipath in a network. The proposed scheme achieved higher PDR through secure data transmission because it selects the better path which provides malicious-free routing. The proposed scheme shows stability with increasing number of nodes in terms of energy consumption. The proposed scheme makes use of the dynamic encryption scheme to achieve secure packet transmission. In the existing schemes, the entire data can be exposed to the attacker during data transmission. The proposed scheme resists the attacker activities in routing by choosing an alternate path for data transmission and is capable of achieving high packet delivery ratio with increased network lifetime.

### 6.7 SUMMARY OF THE CONTRIBUTIONS

The proposed secure cluster-based multipath routing scheme establishes a secure route to increase the reliability and enhancing security of the network. The objective of the proposed SCMRP is to minimize the
security risk caused by an attacker present in a network. The SCMRP consists of three phases such as cluster formation, establishment of multipath routing and secure path selection. The energy-efficient clusters are formed using a hierarchical clustering technique. The cluster weight factor such as highest remaining energy, mobility factor and transmission range are considered to select a cluster head. The SCMRP also forms the multiple paths between source and destination, and also it eliminates unreliable routes. Then, the best path was selected from the multipath by considering the parameters like energy, distance, and link quality. A security mechanism DSE is applied in a selected path to enhance the security and reduce the attacks during communication. Finally, the performance of the network is evaluated when there is an attacker present in the network.

The major benefits of the proposed scheme are i) secure routing path is established for the data transmission ii) if an attacker is found in a path, alternate path can be selected from the available multiple paths which provides efficient packet delivery ratio. iii) The computation and routing overhead involved in security mechanism is very low compared to the other related schemes.

The achievability of the proposed scheme is evaluated through performance analysis and simulation results. The results show that the proposed scheme outperforms to the existing schemes in terms of the packet delivery ratio, signal strength ratio, routing overhead, end-to-end delay and energy efficiency. Hence, the proposed scheme can achieve high reliability and enhanced security in a vulnerable environment. This scheme is suitable for sensitive data transmission application.