CHAPTER 5

RELIABLE DATA SECURITY ALGORITHM FOR MULTI-PATH MULTIMEDIA STREAMING IN MANET

5.1 INTRODUCTION

The developing technology of mobile ad hoc network is widely dependent on wireless multi-hop architecture, without pre-existing framework and preceding configuration of the nodes in network. The drawbacks of this new networking prototype comprise the following.

(i) Absence of admin node in the network.

(ii) Lack of a central authority over the network.

As a result, a node in mobile ad hoc network cannot make any hypothesis about the integrity of its peer nodes. They help the node with its communication and do not maintain their credentials.

Moreover, with a breakthrough in the bandwidth of wireless channels and computational capability of mobile devices, multimedia applications are apprehended to become more obtrusive in mobile ad hoc networks in the immediate future. Some of the examples of multimedia streaming transmission over mobile ad hoc networks include multimedia streaming of audio or video file.

Several routing protocols such as Dynamic Source Routing, Ad hoc on-demand Distance Vector are widely used in mobile ad hoc network. However, the unreliable nature of the wireless technology and the random change in
topology due to the mobility of the node, pose severe threats in communication over single path routing for certain applications such as multimedia streaming and Voice over Internet Protocol.

In a mobile ad hoc network, multi-path routing is extensively adopted to provide multiple paths between source and destination. As an alternative, a multi-path routing provides a very significant approach when compared to single path routing. The multi-path routing provides with higher flexibility by mitigating congestion occurring due to burst in network. This is achieved through load balancing and in turn reduces the delay due to end-to-end transmission. Thus providing multi-path routing over MANET is of paramount importance for streaming multimedia transmission.

However, security factor prevail an important aspect that encumber the precipitate implementation of multimedia streaming transmission over Mobile ad hoc networks. Security issue must be dispatched in multi-path streaming of multimedia transmission over mobile ad hoc networks. In this work, a generalized architecture is provided for reliable and data secure architecture, for streaming multimedia transmission over multiple paths. The aim of this chapter is to arrange and implement a reliable and secure multi-path routing arrangement that can be smoothly handled for streaming multimedia transmission over MANET.

5.1.1 Mobile ad hoc networks

In mobile ad hoc network, each node is represented by grey and dark grey circles as in Figure 5.1. It is a representation of nodes in mobile ad hoc networks which can interact and disseminate information with their neighbors within its bounded range of communication. Two communication nodes, say, ‘S’, source node and ‘D’, destination node communicate with each other, using the
nodes in between them to establish a path channels for delivering data over mobile ad hoc network.

![Diagram of mobile ad hoc network]

**Figure 5.1 Classical Mobile ad hoc networks**

Hence, each node in the network not only acts as a sender or destination node but also as a router which helps to identify the path in between them and also to forward the data for other intermittent nodes. MANETs as designated by Chowdhury C. et al. (2011) provided with multi-hop technique due to the changing network topology in MANETs. These inherent features require suitable algorithms for routing, methods determining the path from source node to destination node, to be progressive and robust to the frequently changing network structure. The dynamic changing topology and minimum computation power of mobile nodes in mobile ad hoc network make it very challenging for high data volume applications such as streaming multimedia files.
5.1.2 A Multi-path Multimedia Streaming transmission over MANETs

Multimedia streaming transmission over MANETs for multi-path transmission is modelled as shown in Figure 5.2. The figure makes it evident that the source node performs the operations such as initiate routing, encoding the input media and finally selects the path for data transmission purpose. The intermediate nodes are used to help forward the data to the destination node which receives the data and regenerates the multimedia file with the help of the multimedia decoder.

![Diagram](image.png)

**Figure 5.2 Multimedia Streaming Transmission using Multi-path**
Several factors in the above model have to be discussed in order to support a secure and reliable multimedia stream transmission, using multi-path over mobile ad hoc networks. The remainder of the section is organized as follows. Section 5.2 describes the general framework used for streaming multimedia transmission and the faults involved in the work where reliability is not being provided. It proceeds with the inclusion of reliability factor and the paths followed in DSA.

Section 5.3 deals with the characteristics of the building block involved in the design of RDSA, the EIDA algorithm and the components involved in the RDSA. Some of the components included in the work are multimedia encoder, encryption and decryption mechanism, path allocator, re-ordering buffer, feedback proxy and finally providing multi-path routing with the help of a neat diagram. Section 5.4 illustrates the different steps involved in RDSA for multimedia stream transmission over Mobile ad hoc network. Section 5.5 and 5.6 provide the results and discussion. Finally, section 5.7 draws the conclusion.

5.2 SECURITY MECHANISM IN MOBILE AD HOC NETWORK

Most of the routing protocols designed for mobile ad hoc networks proceed on the assumption that the nodes in the network cooperate in a well behaved manner. Abusalah L. et al. (2008) did not hold security hypothesis in many cases, in which the information regarding routing is vulnerable while misbehaving nodes could easily disrupt the network and thus change the routing information. Therefore, a number of routing protocols have been proposed to counteract a set of attacks. They make it possible to compromise the discovery of route.
There are certain limitations in the routing protocols where intermediary nodes are not authenticated and no prevention mechanism is provided for the man-in-middle attack as illustrated in Figure 5.3.

![Routing Protocols Diagram]

**Figure 5.3 Routing Protocols**

### 5.2.1 Multimedia Multi-path Stream Transmission

The inherent increased bandwidth utilization of wireless networks and computational power of mobile devices in MANET, multimedia stream transmission over ad hoc network are getting demand. Henceforth, the execution of multimedia stream transmission suffers from the bandwidth quality variations profound in mobile ad hoc network. Furthermore the quality of multimedia streaming transmission is deprived. The noisy communication channel causes interference errors in the transmission.
It therefore necessitates either additional redundancy or retransmissions and finally minimizes the performance of bandwidth. Moreover, failures in link occur due to the interferences and fluctuations in the signal received. Dhurandher S.K et al. (2011) emphasized the arrangement of multimedia multi-path streaming as a significant task. To alleviate these issues in streaming multimedia transmission over mobile ad hoc network, the research work proposes multi-path encrypted mechanism in Chapter 3 using Link Status Multi-Path Routing Protocol.

This work “Reliable Data Security Algorithms for Multi-path Multimedia Streaming in MANET” enhances security for multimedia streaming, which provides further protection to the existing architecture in a mobile ad hoc manner using multi-path routing mechanism. The multi-path encryption mechanism is used as a security mechanism over mobile ad hoc network.

The basic principle discussed in Chapter 3 provides multi-path encrypted approach which breaks the data, which are to be transferred over network into many packets. These packets are transferred over the network. It is put together in a well-organized manner to form the whole data. The packets are transmitted to the intended recipient using multi-path encrypted routing, reducing the possibility of capturing of the packets by an adversary.

The general framework of multimedia streaming transmission using multi-path over Mobile ad hoc network is illustrated in Figure 5.4. At the sender, the raw multimedia stream is compressed by a multimedia-stream encoder into S streams, consisting of stream1, stream 2, …, stream n. The encryption mechanism used for streaming multimedia transmission is performed using WEP encryption scheme, already discussed in chapter 3. Then the streams sent are partitioned and allocated to P paths consisting of path1, path 2, …, path n using path allocator in multi-path environment over mobile ad hoc network.
The paths are preserved by a multi-path routing protocol. When the flows arrive at the receiving end, they are first arranged into a re-ordering buffer to recover the actual ordering. Finally, the multimedia stream transmission is extracted from the re-ordering buffer to be decoded and revealed.

**Figure 5.4 Framework of RDSA for Multi-path Multimedia Streaming**
As the general framework, for the multi-path multimedia streaming transmission over MANET depicted in the Figure 5.4, does not consider reliability factors, the research work has integrated reliability improvement in the framework for multi-path multimedia streaming transmission over Mobile ad hoc network. The architecture of RDSA for multi-path multimedia streaming over Mobile ad hoc network is demonstrated in Figure 5.5.

5.2.2 Reliable Multi-path Multimedia Streaming

![Image: Architecture of Reliable Multi-path MST](image_url)

Figure 5.5 Architecture of Reliable Multi-path MST
This section proposes a reliable framework for multi-path Mobile ad hoc networks that provide end-to-end reliability between the source-destination pair. The main goal of this framework is to provide reliability not only on the multi-path routing protocol between the source and destination nodes but also on data transmission using these multiple routes. The RDSA introduces a set of features that can be incorporated with low overhead without modifying lower layer protocols.

Both the sender and the receiver should implement DSA layer to be able to use this protocol. Before sending data between sender (A) and destination (B), the topology is provided in order to calculate the different routes ‘n’ between A and B. If n is<3, a message error is generated. Otherwise if n=1 or n=2 routes that will be used to transmit data securely will be chosen from the ‘n’ existing routes according to a cost function.

The purpose of each building block of the above mentioned architecture is explained as follows:

5.2.3 Multimedia Encoder

In the proposed architecture, a multimedia encoder is designed for multimedia stream transmission over mobile ad hoc network. The proposed work applies Enhanced Information Dispersal Algorithm as illustrated in Figure 5.6, which uses redundancy in order to achieve reliability. With this EIDA algorithm, the data and data redundancy are broken up into A streams, such that any B streams can be used to reconstruct data D where A and B are positive integers, with A always less than or equal to B. If agreeable numbers of streams are received at the destination, the destination advances to regenerate the packets, otherwise it waits.
Figure 5.6 Data dispersal using EIDA

5.2.3.1 The Enhanced Information Dispersal Algorithm

The basic principle behind designing Enhanced Information Dispersal Algorithm is to provide reliable storage or transmission of packets over mobile ad hoc network based on multi-path systems. EIDA parses a whole file into predefined subsets with the help of matrix multiplication. This again splits the data into new matrices, where the original matrices are reassembled. The idea of EIDA is to transact a source file F, by introducing some amount of redundancy and partitioning the resultant into ‘x’ pieces.

These packets are then transmitted. Restoration of F is possible with any combination of y pieces, where $y \leq x$. Each distributed piece is of size $F / y$, which provides the mechanism that the methodology is optimal. The algorithm for Enhanced Information Dispersal Algorithm is illustrated in Figure 5.7.
Let y1, y2 be the subsequences of length n
n, r are integers
m denotes the matrix

**Initialization process**
Step 1: Choose an integer n such that m = n + r where m/n ≤ 1
Step 2: Choose m vectors xi = (x_{i1}, x_{i2}, ..., x_{in}) such that 1 ≤ j ≤ m

**Partitioning of files**
Step 3: Let File F be partitioned into sequences of length n
Step 4: F = (y_1, y_2 ..., y_n), (y_{n+1}, ..., y_{2n})
Step 5: Let partitioning denote P_j = (y_1, y_{2}, y_{m}) where j = 1, 2, ..., m,
Where z_j = x_j * P_r = x_{i1} - y_{(r-1)} + ... + x_{jn} * y_m
Such that F_j = |F_j| / n

**Applying distribution**
Step 6: Let P = [P_i] 1 ≤ i, j ≤ m denote m * m matrix
Step 7: Apply inverse to P

**Perform modulus operation to obtain output file**
Step 8: Let i = j mod n
Step 9: Let r = [j / n]
Step 10: Output generated

**Figure 5.7 Algorithm EIDA**
5.2.4 Encryption and Decryption

In the proposed framework, encryption at the sender side and decryption at the receiver side are performed using WEP, mainly for providing reliability. Here, reliability is maintained not only for the route discovery but also for the data transfer.

5.2.5 Path Allocator

In this architecture, a path allocation scheme is used, which assigns the packets to the multi-paths using the Link Status Multi-Path Routing algorithm as already discussed in chapter 3. The list of paths for the flow of multi-path routing is maintained in the path set (PS) table, along with the path rating of each path. The path rating ‘pr’ is decreased by a constant ‘c’ each time a transmission failure is reported, and it is increased by a constant ‘c’ for each successful reception. If the rating of path gets reduced below a threshold factor ‘f’, (the value being 0.15 borrowed from TCP-LP suggested by A. Kuzmanovic and E. W. Knightly (2003), the path is removed from the PS table.

5.2.6 Re-ordering Buffer

One major factor when using multi-path multimedia streaming transmission over mobile ad hoc network is the increased re-ordering delay. As packets sent on different paths using multi-path transmission over Mobile ad hoc networks suffer from different set of delays, the appearance of packets at the receiving side suffers from out-of-disposal. Thus the receiver uses a re-ordering buffer to temporarily store the packets received and puts them in line using the sequence number patterns.
5.2.7 Feedback Proxy

The main function of this feedback proxy agent is to provide reliability in multimedia streaming transmission on multi-path over mobile ad hoc network. It further amalgamates the information received from the receiver and sends a feedback message to the sender about the stature of data. The information of the received data from the receiver side comprises the following:

(i) Successfully received.
(ii) Unsuccessfully received due to modification or out-of disposal.
(iii) Never received because of packet loss due to congested traffic.
(iv) Error occurred due to wireless channel.
(v) Failure of link.
(vi) Nodes misbehavior.

5.2.8 Multi-path routing

This method provides better transmission performance and fault tolerance by providing:

- Simultaneous, parallel transport over multiple carriers.
- Load balancing over available assets.
- Avoidance of path discovery when re-assigning an interrupted stream.

Classical multipath routing has been explored for two reasons. The first is load balancing in which the traffic between a source-destination pair is split across multiple (partially or completely) disjoint paths. The second is use of multipath routing is to increase the possibility of reliable data delivery. In these
approaches, multiple copies of data are sent along different paths, allowing flexibility to failure of a certain number of paths.

Both these uses of multipath are applicable to wireless sensor networks. Load balancing can spread energy utilization across nodes in a network, potentially resulting in longer lifetime. Duplicate data delivery along multi paths can result in more accurate tracking in surveillance applications, at the possible expense of increased energy.

5.4 BASIC OPERATIONS INVOLVED IN RDSA FOR MST

The three basic operations involved in RDSA for multimedia stream transmission are (a) Route Request (b) Multimedia Stream Transmission and finally (c) Route maintenance as illustrated in Figure 5.8.

![Diagram of RDSA Multimedia Stream Transmission Operations]

**Figure 5.8 RDSA Multimedia Stream Transmission Operations**
Before discussing the proposed framework further, it is imperative to provide some of the assumption made for this scheme:

(i) Assume that a source node (S) and a destination node (D) share the packets or files in a cooperative manner.

(ii) Follow bidirectional transmission on each link. This assumption is justified, as many wireless Media Access Control (MAC-layer) protocols using ad hoc sensor networks, including IEEE 802.11, require bidirectional transmission.

(iii) Assume that a mobile node communicates with only neighboring nodes and maintains the list of all its immediate neighboring nodes. Henceforth, secure neighbor discovery would only serve to strengthen the security and further enhance the reliability of RDSA for multimedia stream transmission.

5.4.1 Route Request

Route Analysis for multimedia streaming using multi-path routing over mobile ad hoc network is as follows:

The path for the source node S to be followed to reach the destination node D is obtained by processing the flooding operation along with the route request (RouteREQ) packets, elucidated in Figure 5.9. Next, whenever a node receives a RouteREQ packet along with source address S and destination address D, the node immediately views its intermediate node table for references. The objective of intermediate node table is to preserve the list of RouteREQ received for any source destination pair and the intermediate nodes required for the request to be processed. The processing state consists of either “discard” or “rebroadcast”. The result of processing state is dependent on the behavior of intermediate nodes. If the packet arriving from a source has a list of intermediate
nodes which act as a superset, the packet is discarded; otherwise the node rebroadcasts it.

Suppose an intermediate node ‘a’ receives the RouteREQ packet directly from source node S. When the same RouteREQ packet with intermediate nodes {b} arrive from ‘b’, ‘a’ discards it. Upon receiving the RouteREQ, node ‘a’ appends its address in route table and then rebroadcasts it. In case of node ‘d’ the node will accept RouteREQ from neighbors and ‘b’, and subsequently discard that from node ‘e’. Henceforth upon receiving the RouteREQ from node ‘a’, node ‘d’ verifies the encryption mechanism using WEP as discussed in Chapter 1.

Figure 5.9 Route Request Process

When D receives RouteREQ packets from its neighboring nodes, it is responsible for discovering multi-paths to be traversed for multimedia streaming transmission over mobile ad hoc network from all the received routes. When receiving the first RouteREQ, the destination verifies whether the packet
complies with the data security architecture using WEP encryption mechanism as described in Chapter 1 and caches the route list. Further, it decrypts and stores session key and message key from S. Then D generates route reply (RouteREP) packet, which comprises gathered route as obtained from RouteREQ, a session key and message key of the D on the entire message.

The RouteREP is then sent back on the reverse route as mentioned by the gathered route in the RouteREQ. The main job of the intermediate node on the reverse route is to verify its identifier, the predecessor and successor nodes identifier in the gathered route. If both comparisons are valid, the intermediate node signs the RouteREP and passes it to the next successive node in the path. As a result, the RouteREP reaches the source node. This node also verifies whether it received the message from its neighboring node and if this neighboring node is the first node on the path.

5.4.2 Route Maintenance

A break in route occurs due to several factors such as dynamic nature of mobile ad hoc network, fast changing rate of mobility and link failure where the neighbor of the node sends a route error to the source node S. The source node S will then eliminate that route from the routing table. If the source node S finds another path to the destination node D, then the source node uses the particular path by avoiding the eliminated route from the routing table.

If the source node S does not have any way to pass or find a route for the destination node D and if the session is still active the source node would initiate a new route discovery through route request RouteREQ mechanism. The authentication of packets is performed in order to authenticate the packet and the route maintenance uses two mechanisms, namely Open System authentication and Shared Key authentication using WEP as discussed in Chapter 3.
5.4.3 Multimedia Stream Transmission

Protecting the routing mechanism from malicious node attacks is only a part of the security and providing reliability mechanisms over Mobile ad hoc network. Usually a malicious node behaves commonly during route discovery process, nonetheless, during multimedia stream forwarding phase the segment packet is either dropped or the content of the packet is modified and then forwarded accordingly.

The proposed scheme using RDSA provides secure multi-path multimedia stream transmission data forwarding over Mobile ad hoc network. While forwarding data, session keys SKS and SKD are used to encrypt and accordingly packets are transmitted. Apart from doing encryption mechanism, the packets are further divided into m fragments which are sent to the destination D on m alternative routes. The various symbols used for providing reliable multimedia stream transmission over mobile ad hoc networks are represented in Table 5.1.

Table 5.1 Symbols used in Multimedia stream transmission

<table>
<thead>
<tr>
<th>Symbols used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ts</td>
<td>Time stamp</td>
</tr>
<tr>
<td>S</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>Hash()</td>
<td>Hash Function</td>
</tr>
<tr>
<td>$E_{Ly^+}(A)$</td>
<td>Encryption of message A with Ly+</td>
</tr>
<tr>
<td>$D_{Ly^-}(A)$</td>
<td>Decryption of message A with Ly-</td>
</tr>
<tr>
<td>SKS, SKD</td>
<td>Session key by Source and Destination node</td>
</tr>
</tbody>
</table>
5.4.4 **Steps involved in Multimedia Stream Transmission**

The following steps are involved when sending the multimedia stream MS from the source node S to the destination node D over Mobile ad hoc network. It comprises the following steps:

1. S splits the packet into m streams \( \{a_0, a_1, \ldots, a_{m-1}\} \) in addition to redundancy R.
2. Hence the length of each multimedia stream is
   a. \( \text{Length} \left( a_i = R \times \text{Length}(MS) \right) \frac{1}{m} \)
      where \( 0 \leq i \leq m \)
3. Perform encryption using session key results in
4. \( E_{ai} = \text{ESKS} (a_i || i || m || S || Ts) \)
5. Compute Hash Function
   a. Hash (\( E_{ai} \parallel \text{SKD} \))
6. Send \( E_{ai} || (E_{ai} \parallel \text{SKD}) \) to destination D
7. S receives an acknowledgement from destination D which comprises
   a. Successful delivery
   b. Unsuccessful delivery
   c. Lost packet
   d. Link failure
8. In case of failure Destination D resends the packet on another path \( i+1 \)
9. Process stops when received successfully by D

5.5 **Experimental Performance**

NS-2 is used to simulate an ad hoc network with 50 nodes randomly deployed in a 500 m by 500 m area. Nodes have equal transmission range in each simulation and can vary in different simulations. Using two different transmission ranges 100 m and 100 m (row and column) the effect of routing
protocols in the simulations is factored and it is assumed that the network topology is known. The routes considered are disjointed. In the 3rd and 4th evaluation in order to determine eavesdropping and overhead, node mobility is defined randomly in the interval [0,2ms].

In the first set, all the nodes are assumed equally likely to be compromised with probability qi, so all links are of the same cost. In the second set, each node is assigned a probability randomly. The maximum number of paths the algorithm is able to find is independent of the link costs which is dependent on the network topology. Subsequently, by using Secured Data based multipath routing, the algorithm to select path is different for different link cost.

Using the characteristics of 2nd simulation set, it is not necessarily true that more paths imply higher security, because that depends on security level of used paths. Experiment with two cases: equal costs and different costs at every time. The probability to find multiple disjointed paths in an ad hoc network is pretty high. It justifies the achievability of RDSA that is based on the use of multiple paths in ad hoc networks.

There is one or more chances to find multiple paths when using set1 conditions (all nodes are assumed equally likely to be compromised with probability qi) and more the transmission range, the number of disjointed paths are also high.

5.6 RESULT AND DISCUSSION

In this proposed method the video can be split into five parts and transmitted in multi-path based on the availability of the nodes. The source and the destination for the transmission are visible. Eventually, the video is multicast from source to destination. In this simulation, consider that a message is
compromised if there are at least \( m \) compromised nodes on \( m \) disjointed paths. The probability of compromised messages decreases quickly when increasing path number, especially when using more than 5 paths. That proves the efficiency of using multi-path in RDSA.

Also observe that when nodes have different security levels, RDSA selects more secure paths. In the 3rd simulation set, the same message length is used but the path number is varied. Use redundancy and nodes are considered random mobility (max 2 m/s). A message is considered dropped, if the destination does not find all its parts to be able to reconstitute it. Using multiple paths allows taking profit from using some redundancy. That decreases the probability of dropping messages. High transmission range is an important factor in decreasing probability of dropped messages.

5.6.1 Throughput

**Throughput** refers to how much data are transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections.

Table 5.2 arrays the throughput for the successful delivery of packets varying in size over MANET in a secure way. The table compares the throughput of the Reliable Data Security Algorithm with an existing Data Security Algorithm.
Table 5.2 No. of packets vs Throughput

<table>
<thead>
<tr>
<th>Number of packets (p)</th>
<th>Throughput (%)</th>
<th>RDSA in MANET</th>
<th>DSA in MANET</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>80</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>85</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>87</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>90</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>92</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>150</td>
<td>95</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>175</td>
<td>96</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>97</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>225</td>
<td>99</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>250</td>
<td>99</td>
<td>45</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.10 depicts the throughput for successful delivery of packets in MANET. In the Reliable Data Security Algorithm, the multimedia multi-path transmission is used. The RDSA preferred the routing path based on analyzing two phases, one is route discovery and another is route maintenance by each node in the network. Using those three tables, the nodes in the network efficiently identified a simple and secure path for data communication in MANET.
Figure 5.10 No. of packets vs Throughput

The performance graph of the Reliable Data Security Algorithm in throughput is shown in the Figure 5.10. Compared to the Data Security Algorithm, the Reliable Data Security Algorithm provides the best routing path for nodes in MANET in terms of throughput rate. The variance in the throughput for delivery of packet data from source to destination would be 50-60% high in the Reliable Data Security Algorithm.

5.6.2 Energy Consumption

Energy consumption rate is computed to identify the consumption of energy it needs to execute the task and this is measured in terms of joule (J).

Table 5.3 shows the energy consumption by the nodes for the successful delivery of packets over MANET among the nodes in a secure way. The table compares the energy consumption rate of the Reliable Data Security Algorithm with an existing Data Security Algorithm.
Table 5.3 No. of nodes vs Energy consumption

<table>
<thead>
<tr>
<th>Number of group tasks</th>
<th>Energy consumption ( J )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RDSA in MANET</td>
</tr>
<tr>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td>2</td>
<td>2.3</td>
</tr>
<tr>
<td>3</td>
<td>3.5</td>
</tr>
<tr>
<td>4</td>
<td>3.7</td>
</tr>
<tr>
<td>5</td>
<td>4.1</td>
</tr>
<tr>
<td>6</td>
<td>4.5</td>
</tr>
<tr>
<td>7</td>
<td>4.8</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>5.1</td>
</tr>
<tr>
<td>10</td>
<td>5.2</td>
</tr>
</tbody>
</table>

Figure 5.11 indicates the consumption of energy by the nodes in the network for a secure transaction of packets over the nodes. In the Reliable Data Security Algorithm, the multimedia multi path transmission is used in the MANET. After identifying the routing path efficiently, the secure communication should be done and the nodes in the network are based on their presence in the respective group.

The performance graph of the Reliable Data Security Algorithm in energy consumption is shown in Figure 5.11. Compared to Data Security Algorithm, the proposed RDSA provides better energy rate by consuming minimum amount of energy for delivery of packet data from source to destination. Energy consumption would be 40-50% lower in the Reliable Data Security Algorithm compared to an existing Data Security Algorithm.
5.6.3 Network Lifetime

Network Lifetime refers to the period of time during which an object, a process and a phenomenon exist or function.

**Table 5.4 Network lifetime**

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Network life time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDSA in MANET</td>
<td>DSA in MANET</td>
</tr>
<tr>
<td>80</td>
<td>65</td>
</tr>
</tbody>
</table>

Table 5.4 shows the lifetime of the network based on the number of the nodes in MANET for data communication. The table compares the values of the Reliable Data Security Algorithm with an existing Data Security Algorithm in MANET.
Figure 5.12 displays the network lifetime to enhance the secure communication over the network for a long period of time. Compared to DSA, RDSA provides a secure routing path for nodes in MANET for a long period of time. For security, the Reliable Data Security Algorithm and the nodes in the network will be assessed and processed.

![Network Lifetime Graph](image)

**Figure 5.12 Network lifetime**

The performance graph of the Reliable Data Security Algorithm in finding the lifetime of network is shown in Figure 5.12. The attack resistance rate is very low, so the network lifetime of the MANET uses the proposed security. It is best and the variance is 30-40% high by providing a secure routing path communication among the nodes present in the network.

### 5.6.4 Delay

The delay of a network identifies how long it receives a bit of data to move transversely along the network from one node to another. It is typically considered in multiples or fractions of seconds. The delay is measured in terms of seconds (sec).
Table 5.5 Mobility vs Delay

<table>
<thead>
<tr>
<th>Mobility (m/s)</th>
<th>Delay (sec)</th>
<th>RDSA in MANET</th>
<th>DSA in MANET</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>20</td>
<td>195</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>25</td>
<td>152</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>35</td>
<td>202</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>52</td>
<td>240</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>60</td>
<td>290</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>65</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>70</td>
<td>320</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>75</td>
<td>350</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>82</td>
<td>360</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.5 arrays the delay that occurred when more number of data increases in the mobile ad-hoc network environment. The delay metric related to the RDSA in MANET is compared with the DSA in MANET.

Figure 5.13 depicts that mobility also increases the average packet delay. The average packet delay increases roughly by 55% at 20 m/s compared with 10 m/s. When comparing the Reliable Data Security Algorithm and the existing Data Security Algorithm under mobility, the advantage of RDSA increases.
Figure 5.13 Mobility vs Delay

Because the Reliable Data Security Algorithm uses different routes for entity flows and if one of the routes breaks, then the route is repaired and others are not affected. Packets of the flow on the broken route are momentarily forwarded using the best-effort route, which will agree with one of the other routes. There is supplementary route redundancy.

The performance graph of the Reliable Data Security Algorithm in delay is shown in Figure 5.13. When the mobility increases, the delay decreases gradually in the Reliable Data Security Algorithm when compared to Data Security Algorithm. The variance in the delay for sending the packet data from source to destination would be good. The Reliable Data Security Algorithm is approximately 60-70% lower with Data Security Algorithm.
5.7 SUMMARY

This work, presents the security framework, RDSA for multi-path multimedia streaming to improve the routing efficiency for secured data transmission. While multiple disjoint paths are used, there occurs a tradeoff between path disjoining and packet reordering. Due to the occurrence of interferences in channel, it tolerates the burst of packet losses in case of route breakage. In the context of mobility, RDSA requires that route discovery takes place simultaneously with reliable data path selection. Consequently, in the proposed formal model, it prevents the adversarial nodes to break up routes by inserting alternate path for the parted messages. The experimental results show that the proposed RDSA for multi-path multimedia streaming gives better result in terms of transmission delay, bandwidth allocation and load factor.