CHAPTER 3

MULTI-PATH ENCRYPTED DATA SECURITY ARCHITECTURE FOR MOBILE AD HOC NETWORKS

3.1 INTRODUCTION

A Mobile Ad Hoc Network is a collection of wireless mobile computers that are rapidly deployable. It has neither fixed infrastructure nor managed infrastructure and is self-configuring in nature. Mobile ad hoc networks have proved their efficiency in the deployment of different fields. But they are highly vulnerable to security attacks. This aspect seems to be more challenging in wireless networks.

Ping Wang and Weihua Zhuang (2009) provided routing in ad hoc network as a highly insignificant task because of the frequent movements of hosts’ causing successive topology changes. In which requires flexible methods to find and manage the routes. In the modern era, there arises the requirement for security. Anyhow, the present trend in internet has a varied number of security issues to be discussed. In the absence of confidentiality and integrity of data transferred over the network as illustrated in Figure 3.1.
Security is a critical issue in a Mobile ad hoc network because the primary applications of Ad hoc networks are the military applications, such as the tactical communications in a battlefield, where the environment is hostile and the operation is security-sensitive. As compared with a fixed or a wired network, the characteristics of an ad hoc network pose many new challenges in security. The wireless channels are more susceptible to various forms of attacks such as passive eavesdropping, active signal interference, and jamming. The co-operative nature of ad hoc protocols makes it more vulnerable to data tampering, impersonation, and denial of services.

The lack of fixed infrastructure restricts the applicability of certain conventional security solutions. For example, a public key infrastructure which completely relies on centralized trusted authority and intrusion detection model. This PKI requires a central point to collect data inspected. The limited resources of mobile devices, such as the battery power, also restrict the practical deployment of more comprehensive security schemes in an ad hoc network. Finally, the continuous and unpredictable ad hoc mobility clouds the distinction between normal node and anomaly it results in the difficulty of detection of the malicious behavior.

Providing security for such type of network is the most significant and important issue in the world. Ad hoc networks are widely prone to security due to their distinctive features of frequent mobility in node characteristics and the absence of a pre-existing or foremost administering nature of framework. The techniques and methodologies that have been governed and adopted for the purpose of security in wired networks do not directly apply to ad hoc networks. Existing types of networks do not provide absolute security in the sense that they do not restrict the leakage of information. An exemplary method used to hamper data from falling into erroneous hands is encryption.
The most prevailing approach in providing security across unsecured channel is essential to implement encryption/decryption standards on the data diffused over the networks. Some of the encryption algorithms prominently used for this purpose range from Data Encryption Standard, which comprises a 64-bit block cipher to RSA types of encryption standards. It comprises of popular public-key algorithm. The forthcoming section discusses the attack types in MANET and subsequently the multi-path encryption mechanism is followed in order to provide security in an ad hoc network.

3.1.1 Active and Passive attacks in MANETs

Mobile ad hoc networks are interesting and appropriate for military applications that arise mainly in adverse battlefield conditions. In such scenarios, the competency arises accurately to split the obscure information in the presence of malicious nodes. Malicious nodes may endeavor both passive and active forms of attack to provide accessibility to unauthorized access for the classified information. Malicious modes update the information or rattle the information flow. Passive attacks do not disturb or rattle the operation of the network as the adversary snoops network traffic without making any changes.

On the other hand, active attacks can convincingly affect the network operation because the malicious nodes intrude with network data and positioning. Subsequently, it is easy to identify the possibilities of various active attacks. However, it is a very challenging task to identify passive attacks. An example of passive attack is the probability of eavesdropping on network data flows. Some examples of active attacks comprise black hole attacks, Byzantine attacks, routing attacks, wormhole attacks and so on. These are illustrated in Figure 3.2.
Figure 3.2 Attack types in MANET

In MANET communications, it is necessary to contemplate the problem of sending an obscure message from a source node P to a destination node Q in a protected manner. In that way, data confidentiality, data availability, and data integrity are accomplished. Data integrity is provided using Message Authentication Code whereas providing data confidentiality and data availability in MANET communication is much more essential and at the same time involves a significant task.

Mueller S. et al. (2004) presented a research work to gear up the advantage of multiple paths between different nodes analytically to enhance data confidentiality and data availability in MANET. Existing research carried out provides authentication, confidentiality, availability, secure routing and intrusion detection in ad hoc networks. Ad hoc network characteristics should be taken into consideration to design efficient data security along its path of transmission. The work carried out provides security by suggesting multi-path encryption
mechanism as illustrated in Figure 3.3, which is discussed in detail in next section.

3.1.2 Multi-path Encryption Mechanism

Multi-path Encryption Mechanism provides a multi-path encrypted approach for the security in an ad hoc network. The fundamental idea behind multi-path encrypted approach is to break the data that is to be transferred over the network into many packets as shown in Figure 3.4 where $P_1$, $P_2$, $P_3$, $\ldots$, $P_n$ represent the packets transferred over a network. These packets, transferred over network when put together in a well-organized manner, form the whole data, only if performed in a particular manner, just like solving a complicated puzzle. The packets are sent to the intended recipient by way of using multi-path encrypted routing. This minimizes the possibility of capturing all the packets in an intermediate manner by an adversary.
**Figure 3.4 Multi-path Encryption Mechanism**

The working of multi-path routing incorporates the transmission of data adopting more than one path from the sender to the receiver. It minimizes the risk of an adversary supervising all the traffic in all the paths emerging from the sender. This is generally based on the principle that an adversary cannot supervise all the paths at the same time due to the involvement of pragmatic infeasibility.

The researcher has incorporated an efficient mechanism to further enhance the security, and at the same time make expedient the desired features. In this work the problem of routing data over multiple paths is considered in an ad hoc manner. The researcher work proposes to present a data security architecture, which improves the data transmission confidentiality in an ad hoc
network, based on multi-path routing. It utilizes the multiple paths between nodes in an ad hoc network to increase the confidentiality robustness of transmitted data.

![Diagram showing Multi-path Encryption, Security, Diversity Coding, Fault Tolerance, Load Balancing, Improves Reliability, Reduces redundancy]

**Figure 3.5 Data Security Architecture Incorporation**

The original message to be secured is split into parts that are transmitted in multiple paths. The parted messages are encrypted on their course of transmission which improves the security to the next level. One of the well-known approaches to multi-path routing is diversity coding that achieves fault tolerance in ad hoc networks. In this work, a simulation study is performed on multi-path encrypted data security approach in ad hoc networks as illustrated in
Figure 3.5. The motivation of this work is to explore the DSA in ad hoc networks and present the benefits. Experimental simulations are conducted for the DSA approach and compared with existing ad hoc multi-path security solutions. It shows that DSA performs better than the existing security solution up to 6% to 8%.

3.2 MULTI-PATH ROUTING IN AD HOC NETWORKS

In order to disseminate the portions of data to multiple paths, Obaidat M. et al. (2011) designed an efficient algorithm for identifying multiple paths with minimum overlay. The routing protocols adopted in today's Internet are based on the destination node and rely on single shortest path algorithms. The existing Internet routing protocols maintain very limited multiple paths routing in ad hoc networks. When multi-path in an ad hoc network occurs, the packets will be disseminated via multiple paths to the same destination. This is mainly performed for achieving load balancing, congestion control or reliability.

Previous researchers have carried out the work by utilizing the mobile nodes and concentrated on the routing efficiency alone. However, malicious event or security threats may be posted on the data forwarding stage. The routing path security is done through the selection process of reliable multi-path routing which is prone to negligible attack rates. So, multi-path routing is a very promising alternative to single path routing as it provides higher resilience to path breaks. It also alleviates network congestion through load balancing and reduces end-to-end delay.

Multi-path routing is the routing technique which uses multiple alternative paths throughout a network. It can give a diversity of reimbursement such as fault tolerance, increased bandwidth and improved security. The multiple paths might be overlapped, disjointed edge and node-disjointed with each other.
Thus the multi-path routing can be highly suitable for multimedia streaming over wireless ad hoc networks. Multimedia streaming is a technique for transferring data so that it can be processed as a steady and continuous stream.

Streaming technologies like multimedia streaming are becoming increasingly important with the growth of the Internet because most users do not have fast enough access to download large multimedia files quickly. With multimedia streaming, the client browser displays the data before the entire file is being transmitted.

In this work, a multi-path approach for ad hoc networks by adopting diversity coding is presented. The load arising in source-destination pair is disseminated over multi-paths toward reducing the drop rate involved in packets to attain load balancing and to improvise the delay factor arising over packet transmission in source-destination pair. The routing criterion is illustrated in Figure 3.6, where four distinctive paths are implemented in order to send data from a source-destination pair.

Figure 3.6 describes the flow of packets in multi-path ad hoc networks followed with the routing topology.

Figure 3.6 Designs of multi-paths in Mobile Ad Hoc Networks
3.2.1 Design and description of multi-path in ad hoc networks

This proposed model maneuvers the multi-path to provide maximum security against link or path downfall. The packets containing data are transmitted in source-destination pair over multi-path, by adopting diversity coding as mentioned in 3.1.2. In the design of multi-path, presume that $MP_{max}$ paths are available for data transmission from a source node to destination node. All paths in ad hoc network are cooperatively dislocated, as they do not share a node in common. Each and every path is indexed as $i = 1,\ldots, MP_{max}$. The probability of path failure is denoted by $\text{FailProb}_i$ which denotes the probability that path ‘$i$’ is de-linked at the time when the source node tries to transmit.

The probability of failure packets from available paths are constructed in the vector form as $\text{FailProb} = [\text{FailProb}_i]$, where $i = 1,\ldots, MP_{max}$. Given $\text{FailProb}$, also define the probability of success packets from path availability which is given as, $\text{SuccProb} = [\text{SuccProb}_i]$, where $\text{SuccProb}_i = 1 - \text{FailProb}_i$, where $i= 1,\ldots, MP_{max}$. Suppose that the work Multi-path Encrypted Data Security Architecture for Mobile Ad Hoc Networks has to send a packet of ‘A’ information bits by using the accessible paths in such a way that the probability of reaching the destination is to be maximized. This is represented as $P_{max}$. This goal is attained by designing channel coding approach, called diversity coding where B extra bits are inserted as overhead. The concluding C bits are denoted as $C = A + B$.

The major decision to be arrived is about how the ‘B’ bits have to be distributed to the available paths. Some paths may even perform poor by which using those paths does not result in optimality. In such cases, it will have no use for utilizing those paths. Hence, define vector $\vec{v} = [\vec{v}_i]$. If $n$ is the total number of paths to adopt in order to maximize $\text{SuccProb}$, it would be advantageous to derive the block allocation vector $\vec{v}$ as a variable size $v$, instead of determining its
size to the total available paths \( (\text{MP}_{\text{max}}) \). Based on these, the appropriation vector has the following form, ‘\( \mathbf{v} \)’ = \([V_1, V_2, V_3, \ldots V_n] \) where \( n \leq \text{MP}_{\text{max}} \).

### 3.2.2 Multi-path Routing Topology

The originality of the proposed approach is that it does not modify the existing lower layer protocols. The constraint applied in the security protocol is both the sender 'A' and the receiver ‘B’ is authenticated. Session key and Message key are used for the encryption and decryption of frames at MAC layer. The authentication of the terminals is performed efficiently in multi-path routing topology. This routing protocol supports multi-path routing by using Link Status Multi-Path Routing protocol.

#### 3.2.2.1 Link Status Multi-Path Routing Protocol

Like the notorious Open Shortest Path First algorithm, the multi-path routing protocol is based on a link status database. Each and every node maintains a copy of nodes in the network that is frequently refreshed. Figures 3.7(b) and 3.7(c) illustrate the copy of the network sketch stored in router databases. Figure 3.7(b) describes a conventional data structure used by OSPF. The example shows that the conventional data structure consumes relatively much more memory than the data structure used by LSMTPR.

In contrast to OSPF, in LSMTPR, each node has an area code for each destination. The area code is similar to the shortest distance which is represented in terms of the availability of number of nodes on a passage to a destination. By assuming that node Q is the destination, Figure 3.8(a) presents the area codes to Q stored in the other nodes in the network. In the same way, Figure 3.8(b) illustrates the table kept in node Q, in which the middle column presents the area
code from Q to every other node and the last column shows the coinciding interfaces.

When node Q receives a packet whose destination is determined to be of U, it forwards it to its neighbors with the smallest area code to the destination. That is, Q would forward the packet to the interface coinciding it to node T or node R. In this manner the routing table in every node for each destination from the link status database is illustrated in Figure 3.7(c) using the algorithm given in Figure 3.9. For example node Q generates and keeps a routing table shown in Figure 3.8(b). The core idea behind the algorithm is to determine the neighbors for each node.

![Node Structure](a)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q</td>
<td>1</td>
</tr>
<tr>
<td>P</td>
<td>S</td>
<td>3</td>
</tr>
<tr>
<td>Q</td>
<td>P</td>
<td>1</td>
</tr>
<tr>
<td>Q</td>
<td>R</td>
<td>2</td>
</tr>
<tr>
<td>Q</td>
<td>T</td>
<td>4</td>
</tr>
<tr>
<td>R</td>
<td>Q</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Node</th>
<th>Neighboring node</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q,S</td>
</tr>
<tr>
<td>Q</td>
<td>P,R,T</td>
</tr>
<tr>
<td>R</td>
<td>Q,U</td>
</tr>
<tr>
<td>S</td>
<td>P,T,V</td>
</tr>
<tr>
<td>T</td>
<td>Q,S,U,W</td>
</tr>
<tr>
<td>U</td>
<td>R,T,X</td>
</tr>
<tr>
<td>V</td>
<td>S,W</td>
</tr>
<tr>
<td>W</td>
<td>V,T,X</td>
</tr>
<tr>
<td>X</td>
<td>U,X</td>
</tr>
</tbody>
</table>

![Source-Destination link](b)
![Router Database](c)

**Figure 3.7(a)** Node Structure  **(b)** Source-Destination link  **(c)** Router Database
Figure 3.8 (a) Area codes from other nodes to Q (b) Table kept in node Q

3.2.2.2 Algorithm - Link Status Multi-Path Routing Protocol

The algorithm in Figure 3.9 advances in the path of breadth first searching over a network on the source node. The complexity arising due to space in BFS is O(|V|) whereas the complexity arising due to space in conventional Dijkstra algorithm is O(n^2) where V represents the vertices and N denotes the available links in the path. The main drawback in using the conventional Dijkstra algorithm is the profound efficiency in sporadic networks. The algorithm LSMPR shows fine improvement in this type of networks.
TN: Number of nodes
S: Set of nodes evaluated
FinalS: Set of nodes added into S finally
PresS: Set of nodes discussed at present
ac: area code
Int: Set of interfaces
Source: Source node
Destn: Destination node
node1: Incoming node
node2: Node already present in the network
For each nodes (Node.ac = 0; Node.Int = 0)
{
    Int = AccessNeighbor(Source ,S);
    FinalS = Int;
    S = S U Int;
    For (node1CPresS)
    {
        node.ac = 1;
        PresS = AccessNeighbor(node1,S);
        node2.ac = (node.ac + 1);
        node2.Int = (node2.Int U node1.Int);
    }
}

Figure 3.9 Algorithmic representation of Link Status Multi-Path Routing Protocol
3.3 MULTIPLE PATH MESSAGE TRANSMISSION

With the knowledge of network topology the proposed security model will use n routes (the message will be divided into n - 1 share). One path is used for signalling, the second one is used to transmit a plain text with a key share (randomly chosen) and the others (n -2 paths) are used to transmit the different shares of the original message. Therefore the proposed data security multi-path protocol should have at least 3 links. If there exists <=2 links multi-path message transmission does not provide the data security.

This section discusses about the algorithm for multi-path message transmission with the basic set of assumptions and uses diversity coding in order to achieve QoS.

3.3.1 Algorithm for Multi-path Message Transmission

Multi-path routing allows the establishment of multiple paths between a single source and single destination node. This proposal increases the reliability of data transmission and provides load balancing by way of providing reliability, load-balancing, energy-conservation, and Quality-of-Service. The algorithm for Multi-path Message Transmission is illustrated in Figure 3.11 with the basic assumptions given below in Figure 3.10.

**Step 1:** Dividing m into n - 1 parts gives P (m) = {P₁, P₂, ..., Pₙ₋₁}

Where, m is the message to be sent securely between A and B.

**Step 2:** Tp (ntwk): Function invoked periodically to discover topology of the ad hoc network. It returns true if adjustment in topology exists, otherwise it returns false.

**Step 3:** Symbolize the frequency of topology refreshing.

**Step 4:** N (A, B) number of links between A and B where n is an integer; 3 <= n <= N (A, B)

**Figure 3.10 Basic assumptions**
Input: (network topology, m)
Tp(ntwk)=true
While (connection is active)
{
if Tp(ntwk)==true)
{
if (N(A,B)>=3)
{
take n links among N(A,B)
divide m into n-1 parts to form p(m) = \{ P_1, P_2, ..., P_{n-1} \}
generate x randomly
}
if (N(A,B)==2)
{
take one path as data path
take one path as control path
generate x randomly
}
if (N(A,B)==1)
{
one path is used as control and data path
generate x randomly
}
}
Output: P(m) = \{ P_1, P_2, ..., P_{n-1} \}, x

Figure 3.11 Algorithmic representation of Multi-path Message Transmission
The original message $m$ is divided into $(n-1)$ share and each of them has a unique identifier. The algorithm generates path numbers of appropriate message parts to be sent on the signal channel. The path numbers assigned for the message parts are selected randomly and sent along appropriate paths of multi-path routing protocol. During the next message transmission, different paths are used for parted messages, generated through pseudo random model.

The message share will be transmitted in plain text. The final part is sent in plain text on one of the $n$ paths. It will be the starting point for the receiver to find other parts. Concerning the manner of dividing messages, a channel coding approach called Diversity Coding is used to recover from link failures. Finally, the $n-1$ parts of $m$ pairs are combined using pseudo random operation related to final path. On the $n$th link, which is considered as signalling channel, send values of pseudo random number and number of path in which message parts are transmitted. The algorithmic representation of Multi-path Message Transmission is expressed in Figure 3.11.

Once the message transmission through multi-path is appropriated, the work proceeds with the encryption of messages to be followed in a multi-path manner. The briefing of the encryption of messages is discussed in the forthcoming section.

3.4 MULTI-PATH ENCRYPTION OF MESSAGES

The message parts on every data channel are sent encrypted by WEP to strengthen discretion. The chosen WEP for encryption in the proposed simulation offers efficient security to be swallowing in the multi-path routing protocol. Wired Equivalent Privacy is a security algorithm which uses the stream cipher. Here, two authentication methods are used. They are Open System authentication and Shared Key authentication for encryption purposes.
In Open System authentication, WLAN client need not provide its qualifications to the Access Point during authentication. Any client can authenticate with the AP and then attempt to connect. In effect, no authentication occurs.

Subsequently WEP keys can be used for encrypting data frames as shown in Figure 3.12. At this point, the client must have the correct keys. In Shared Key authentication, the WEP key is used for authentication in a four step challenge-response handshake as illustrated in Figure 3.13.
**Step 1:** The client sends an authentication request to the Access Point.

**Step 2:** The Access Point replies with a clear text message

**Step 3:** The client encrypts the text message using the configured WEP key, and sends it back in another authentication request.

**Step 4:** The Access Point decrypts the response. If it matches the text message the Access Point sends back a positive reply.

**Figure 3.13 Four step Challenge-Response Handshake**

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames. Even if an attacker achieves something to obtain one part or more of the transmitted message, the likelihood of renovating the message is low. The attacker should possess all the parts, aware of the joint function and also to decrypt the WEP encoding. As a result, security can be achieved using data security architecture which is explained in the forthcoming section.

**3.5 DATA SECURITY ARCHITECTURE**

The motivation behind the data security in multi-path routing by Stephen Dabideen J.J and Garcia Luna Aceves (2012) helped to divide the initial message, ready for transmission into parts and then to encrypt and combine these parts by pairs. An increase in robustness of confidentiality is attained using the characteristics of prevalent multiple paths between nodes in an ad hoc network. This robustness is achieved by sending encrypted combinations on the different existing paths between the sender and the receiver. In the solution, even if an
attacker succeeds to have one part or more of transmitted parts, the probability
that the original message can be reconstructed is low.

The next step is to design an application layer situated on top of the
network (IP) layer that will manage the use of proposed two level data security
solution to send data securely. In order to ensure security, a specific header,
called DSA header, is added. DSA layer is situated between two important
layers. The first one is the IP layer that will provide the protocol with important
information about routing, number of available routes, quality of routes,
depending on the routing protocol used. The second layer is the Transport layer
(TCP/UDP) that is able to manage retransmission, if needed, especially when
topology has changed after the data transmission had started. The detailed
illustration of the two layers is demonstrated in Figure 3.14.

Figure 3.14 DSA Layer
The Data Security Architecture introduces a set of features that can be incorporated with low overhead without modifying lower layer protocols. Both sender and 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’ routes between A and B.

3.5.1 Paths selection in DSA

In an ad hoc network, the topology changes frequently, this makes wireless links unstable. Sometimes packets might be dropped due to the bad wireless channel conditions, the occurrence of collision on multi-path routing, or because of out of date routing information. When packet loss does occur, non-redundant share allocation will disable the reconstruction of the message at the intended destination. To deal with this problem, the work introduces redundancy in Data Security Architecture to improve the reliability. The decision of using the redundancy is to find the average mobility of the network's nodes.

DSA is based on multi path routing in ad hoc networks. The question is how to find the desired multiple paths in a Mobile Ad hoc Network and how to deliver the different message parts to the destination using these paths. Routing in an Ad hoc network presents great challenge because the nodes are capable of moving and the network topology changes continuously and unpredictably. The Dynamic Source Routing protocol is capable of maintaining multiple paths between the source-destination pair. This on-demand protocol works by broadcasting the route inquiry messages throughout the network and then gathers the replies from the destination. Even though DSR is able to find multiple disjointed paths, these paths might not be optimal for Securing Data based MultiPath routing in ad hoc networks (SDMP). This is because of the path selection which is usually based on the hop count or propagation delay in these
routing protocols. Security is an essential parameter in choosing different paths in such a way that the message security is maximized.

Therefore, elucidate a path which is compromised when any one or more of the nodes along the path is compromised. For each path, consider that if it is compromised, all the shares allocated to it would be compromised. Otherwise, if the path is not compromised, all shares on that path will be safe. As paths are node disjointed, it is assumed that the probability that one path is compromised is independent of others.

Assume that there are \( n \) disjointed paths: Path1, Path 2, \ldots, Path \( n \), available from the source to the destination. Use the vector to denote the security parameters of paths, where \( P_i \) (\( i = 1, 2, \ldots, n \)) is the probability that the path \( i \) is compromised. Assume also that: \( P_1 \leq P_2 \leq \ldots \leq P_n \). The paths are ordered from more secure one to less secure one. Note that the path security information \( P \) is obtained at the source from the used multi-path routing protocol. Assume that if one node is compromised, all the shares traveling through that node will be compromised. The probability \( P_i \) does not include the probability that the source or the destination node is compromised. The source and the destination are both reliable.

The maximum security provided only depends on the chosen paths and \( P_i \) is a probability satisfying \( 0 \leq P_i \leq 1 \). The less probability and the more secured path are used to deliver the message. It is intuitive that non-redundant secret sharing scheme provides the maximum security to the message, because it gives fewer chances to an adversary to obtain all message parts. However, it requires the successful reception of all the parts and the knowledge of used combination function.
In an ad hoc network, wireless links are not stable and redundancy is a common way to improve the reliability. It is based on the idea of sending more information than minimum requirement, so that the original message can be reconstructed if any loss happens in the network. So, the path selection criteria is to choose, at least, the first m most secure paths among the n existing ones (while m is the number of message parts). It is assumed also that the signalling information should be sent on the most secure selected path because of sensitive data it contains.

With probability \( q_i \) that node \( n_i \) is compromised, then, the probability that a path from A to B consisting of node A, \( n_1, n_2, \ldots, n_i, B \) is compromised and equal to \( p = 1 - (1 - q_1, 1-q_2, \ldots, 1-q_i) \). The probability \( q_i \) indicates the security level of node \( i \) and the feedback is estimated on the basis of some security monitoring software or hardware devices such as firewalls and intrusion detection devices.

### 3.6 EXPERIMENTAL EVALUATION

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 usually vary in different simulations with the transmission ranges 100 m and 1000 m. In order to factor out the effect of routing protocols in the simulations, it is assumed that the network topology is known. Routes considered are disjointed.

In the 1\textsuperscript{st} and 2\textsuperscript{nd} evaluations (eavesdropping and overhead), node mobility is randomly defined between the interval \([0, 2 \text{ m/s}]\). In the first set, all nodes are assumed equally likely to be compromised with probability \( q_i \), 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. It solely depends on the network topology although using the Secure Data based Multi-path routing in ad hoc networks algorithm to select paths to be used for sending message parts is different for different link costs.

Using the characteristics of 1st simulation set, it is not necessarily true that more paths imply higher security because that depends on security level of used paths. To derive the results two cases are experimented: equal costs and different costs at every time. The probability to find multiple disjointed paths in an ad hoc network is pretty high. This justifies the achievability of the DSA based on the use of multiple paths in ad hoc networks. There are one or more chances to find multiple paths when using set1 conditions (all nodes are assumed equally likely to be compromised with probability $q_i$) and the more is transmission range, more are existing disjointed paths.

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. This proves the efficiency of using the multi-path in DSA. It is also observed that when nodes have different security levels, DSA selects more secure paths. In the 2nd simulation set, the same message length and vary path number are used. Redundancy and nodes are considered as random mobility (max 2 m/s). If a message is considered as dropped, then the destination does not find all its parts to be able to reconstitute it. Using multiple paths allows taking profit from redundancy. In this way it decreases the probability of dropping messages. Here notice that high transmission range is an important factor in decreasing the probability of dropped messages.
3.6.1 Bandwidth

Bandwidth describes the maximum data transfer rate of a network. It measures how much data can be sent over a specific connection in a given amount of time.

**Table 3.1 No. of Nodes vs Bandwidth efficiency**

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>Bandwidth Efficiency (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed multi path transmission</td>
</tr>
<tr>
<td>100</td>
<td>78.1</td>
</tr>
<tr>
<td>200</td>
<td>79</td>
</tr>
<tr>
<td>300</td>
<td>80.3</td>
</tr>
<tr>
<td>400</td>
<td>82</td>
</tr>
<tr>
<td>500</td>
<td>84</td>
</tr>
<tr>
<td>600</td>
<td>83.2</td>
</tr>
<tr>
<td>700</td>
<td>84.1</td>
</tr>
<tr>
<td>800</td>
<td>88.5</td>
</tr>
<tr>
<td>900</td>
<td>90.2</td>
</tr>
<tr>
<td>1000</td>
<td>92.6</td>
</tr>
</tbody>
</table>

Table 3.1 describes the bandwidth efficiency obtained when the number of nodes increases in the mobile ad hoc network environment. The
outcome of the proposed multipath transmission in MANET is compared with an existing single path DSA Scheme.

Figure 3.15 shows the simulation results for the Bandwidth efficiency compared with the multipath transmission and single path DSA framework. In ad hoc networks, the link level bandwidth is used in multi-path provisioning for end-to-end flows. If an end-to-end flow traverses numerous hops in the link layer, then the bandwidth assigned to such flow is measured by the ability of the bottleneck link. To provide multi-path routing and be able to carry out tasks such as data control, an end-to-end flow’s requested bandwidth is verified against the link layer bandwidth hop-by-hop to discover a possible path.

![Graph](image)

**Figure 3.15 No. of Nodes vs Bandwidth efficiency**

So, multi-path routing relies on the ability of the system in quantifying link layer bandwidth. It can be seen that the multi-path framework achieves much better Bandwidth efficiency compared with the Single path DSA Scheme.
Multi-path routing achieves approximately 40 % to 45% bandwidth efficiency and this is more than that of single path DSA Scheme.

### 3.6.2 Delay

The Delay of a network identifies how long it receives a bit of data to move transversely in 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 3.2 Mobility vs Delay**

<table>
<thead>
<tr>
<th>Mobility (m/s)</th>
<th>Delay (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed Multi path transmission</td>
</tr>
<tr>
<td>10</td>
<td>2.5</td>
</tr>
<tr>
<td>20</td>
<td>4.8</td>
</tr>
<tr>
<td>30</td>
<td>5.9</td>
</tr>
<tr>
<td>40</td>
<td>11.1</td>
</tr>
<tr>
<td>50</td>
<td>14.1</td>
</tr>
<tr>
<td>60</td>
<td>15.5</td>
</tr>
<tr>
<td>70</td>
<td>15.4</td>
</tr>
<tr>
<td>80</td>
<td>15.8</td>
</tr>
<tr>
<td>90</td>
<td>16.2</td>
</tr>
<tr>
<td>100</td>
<td>16.3</td>
</tr>
</tbody>
</table>

Table 3.2 describes the delay that occurred when more number of data increases in the mobile ad hoc network environment. The reliability of the
The proposed multi-path transmission scheme in MANET is compared with the existing single path DSA Scheme.

![Graph showing Mobility vs Delay]

**Figure 3.16 Mobility vs Delay**

Figure 3.16 depicts that mobility also increases the average packet delay. The average packet delay increases roughly 50 percent at 20 m/s compared with 10 m/s. When compared within multi-path transmission and single path DSA Scheme under mobility, the advantage of multi-path transmission increases. Because the multi-path transmission uses different routing scheme for individual flows, when one of the routing breaks, it goes for the other route to reach its destination.

Packets of the flow on the broken route are temporarily forwarded using the best-effort route. Here, the protocol performs better at high loads and at high speeds and does better under all conditions. Thus, the multi-path transmission scheme decreases approximately 50 – 60 % of delay occurrence when compared with the single path DSA Scheme.
3.6.3 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>
<thead>
<tr>
<th>Number of packets sent</th>
<th>Number of packets received</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed multi path transmission</td>
</tr>
<tr>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>50</td>
<td>41</td>
</tr>
<tr>
<td>75</td>
<td>65</td>
</tr>
<tr>
<td>100</td>
<td>83</td>
</tr>
<tr>
<td>125</td>
<td>118</td>
</tr>
<tr>
<td>150</td>
<td>137</td>
</tr>
<tr>
<td>175</td>
<td>170</td>
</tr>
<tr>
<td>200</td>
<td>185</td>
</tr>
<tr>
<td>225</td>
<td>220</td>
</tr>
<tr>
<td>250</td>
<td>245</td>
</tr>
</tbody>
</table>

Table 3.3 describes the throughput obtained when more number of packets increases in the MANET environment. The outcome of the proposed
multi path transmission scheme in MANET is compared with the existing single path DSA Scheme.

![Graph showing No. of packets vs Throughput](image)

**Figure 3.17 No. of packets vs Throughput**

Figure 3.17 shows that when mobility increases, the throughputs of all protocols drop. It also shows throughput value at the mobility \( v = 10 \text{ m/s} \). Mobility affects network throughput at both the MAC layer and the routing layer. At the MAC layer, it takes time to determine the collisions caused by node movement and to keep new slots. Basically, a protocol is based on developing a reservation having only limited capability to hold network mobility.

At the network layer, it takes time for the routing protocol to re-establish a route when it breaks. As can be seen, the multipath transmission performs better than the Existing Single path DSA Scheme. The throughput of multi-path transmission is approximately 80-90 % and it is the best when compared with the single path transmission.
3.6.4 Routing Overhead

Routing overhead defined as congestion occurs in the route during the transmission of packets from source to destination path. Here the routing overhead refers to the packet transfer rate.

**Table 3.4 Mobility vs Routing Overhead**

<table>
<thead>
<tr>
<th>Mobility (m/s)</th>
<th>Routing Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed multi path transmission</td>
</tr>
<tr>
<td>10</td>
<td>70</td>
</tr>
<tr>
<td>20</td>
<td>75</td>
</tr>
<tr>
<td>30</td>
<td>78</td>
</tr>
<tr>
<td>40</td>
<td>80</td>
</tr>
<tr>
<td>50</td>
<td>85</td>
</tr>
<tr>
<td>60</td>
<td>88</td>
</tr>
<tr>
<td>70</td>
<td>90</td>
</tr>
<tr>
<td>80</td>
<td>95</td>
</tr>
<tr>
<td>90</td>
<td>97</td>
</tr>
<tr>
<td>100</td>
<td>99</td>
</tr>
</tbody>
</table>

Table 3.4 describes the routing overhead obtained when the mobility rate increases in the MANET environment. The outcome of the proposed
multipath transmission scheme in MANET is compared with the existing single path DSA scheme.

In multipath transmission, four types of control messages are used to maintain neighborhood connectivity, to investigate routes using request messages, to reply for routes requests and to notify route errors. The size of request message dynamically increases as it moves through network toward destination whereas reply message’s size decreases as it moves toward source node. The multi-path transmission satisfies requirements and achieves better performance by maintaining multiple paths along the destinations via these dynamically sized varying messages.

![Figure 3.18 Mobility vs Routing Overhead](image)

**Figure 3.18 Mobility vs Routing Overhead**

Figure 3.18 shows the routing overhead in terms of packets for increasing node mobility. The improved performance achieved in multi-path transmission is at the cost of routing control overhead. The proposed framework,
multi-path transmission shares the nodes visited and delay information through request and reply messages periodically to maintain multiple paths containing the highest control overhead. Thus multi path transmission approximately reduces 50-60 % the routing overhead when compared with the single path DSA scheme.

3.7 SUMMARY

The Data Security Architecture presented is tailored for on-demand multi-path data route, with encryption of parted data messages in MANETs. It represents a better effort toward a formal security model that can deal with levels of security to safeguard the message being transmitted in ad hoc networks. In the context of mobility, DSA requires that route discovery takes place simultaneously with data communication with larger additional bandwidth that is naturally generated. Consequently, in the proposed formal model, it prevents the adversarial nodes to break up routes by inserting alternate paths for the parted messages. The results of the simulation depict that the DSA with encrypted message parts performs better security by 6% to 8% than the conventional security model with simple encryption on the data directly.