ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

CHAPTER 4

PROPOSED METHODOLOGY

The first two steps of the proposed research design are discussed in this chapter in detail.

The primary objective of the thesis is to detect the known and unknown cyber attacks with improved accuracy without compromising the Quality of Service(QoS). The entire cyber attack detection process is discussed for known cyber attacks and unknown cyber attacks separately. For detecting the known cyber attacks, monitoring the network traffic is the first and foremost step. This chapter discusses the detection of known cyber attacks through network traffic monitoring by enhancing PCA (Principle Component Analysis) with SVM (Support Vector Machine). The proposed approach shows significant improvement in attack detection rate.

4.1. Network Traffic Monitoring

The term traffic monitoring [54] describes the method by which all the data that are sent and received by a network are identified, thereby faults and harmful events may be detected and the genuine data packets can be allowed to pass through the network. The monitoring operation can take place using two methods, namely, proactive scanning and reactive scanning. Proactive scanning is the process that analyses the network to find anomalies with a predefined time interval, whereas the reactive scanning takes place when an event occurs. Proactive monitoring seems to be better than the reactive, because in proactive scanning, the administrator has to inspect the movement of the traffic, consequently the functioning of entire networks and the level of security in the network. Out of the traffic methods discussed in chapter 2, the router based monitoring is discussed in this thesis. Router based monitoring technique is a proactive scanning, which is identified to be suitable for this study because it offers multi-functionality and it adapts by itself. The very nature of monitoring helps in eliminating the issues in the process of forwarding packets and it does not require any operating infrastructure individually. Among the three router based monitoring techniques, SNMP performs better, but still needs some improvements. The present research work aims to add a new feature for SNMP.

In this proposed work, the performance of route based network traffic monitoring techniques such as SNMP, RMON & Netflow. The implementation of these techniques is carried out to ascertain the most effective monitoring technique among the three. The best among three is improvised to improve the quality of service of the network. The proposed system aims to provide efficient and time saving monitoring system which helps to achieve reduced packet losses, end to end delay and higher throughput. In the network there will not be any route to the destination node from the source node. The source node will broadcast a route request about the data packets to all the nodes whenever it is in a position to send a packet. The source node that does not have a route to the destination when it has data packets to be sent to the destination, it initiates a route request packet, the route request is sent to all the nodes on that network. Each node, upon receiving a route request packet, rebroadcasts the packet to its neighbors if it has not forwarded it already to avoid the retransmission of data. The proposed system aims to send the NACK (Negative Acknowledgement) which helps the node the learn about the neighboring routes travelled by data packets which provides reliability to the existing technique SNMP and helps to save time where as the proposed system provides better results comparatively.

The following steps clearly state the improvement done with SNMP. The processing flow of the proposed system is depicted in figure. 4.1. Proposed traffic monitoring is a router based, that aims to fulfill the need for the administrator in monitoring and handling the resources of the network. The data flow to the host through the router will be generated.

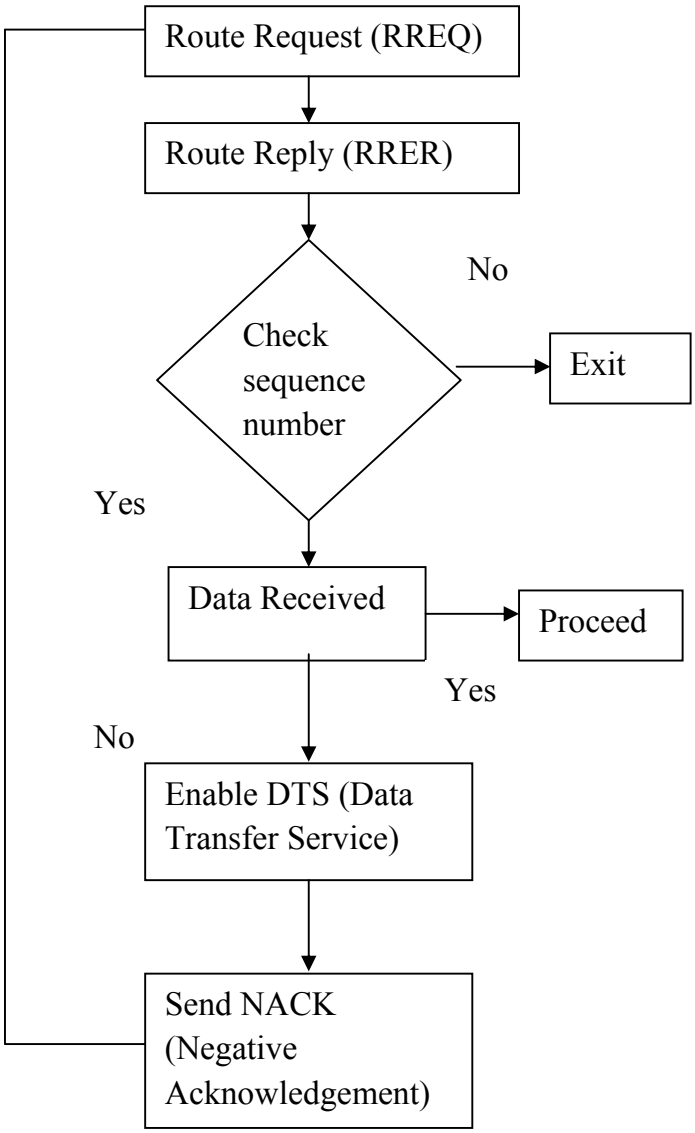

Figure.4.1 Processing steps of proposed network traffic monitoring technique

Processing Steps:

Step.1

The RouteRequest (RREQ) will be initiated throughout the network, when there is a data packet that is to be sent from source to the destination.

Step.2

After receiving the RouteRequest every node will rebroadcast to its neighbor node to ensure that particular node is not a destination node.

Step.3

Each node checks for the sequence number generated by the source in the data packet to ensure that it is not a duplicate packet.

Step.4

To avoid the creation of a loop and multiple transmissions of the route request to the same node through multiple paths, a sequence number is generated.

Step.5

Except the destination node, every open node forwards RouteRequest packet during the process of constructing the path from the source to the destination. There is a chance of failure so DTS (Data Transfer Service) message is assigned to recover the failure data so that the retransmissions can be avoided.

Step.6

NACK (Negative Acknowledgement) helps to reduce bits in the control message format. Nodes will also learn about the routes of the neighbors by which the data packets are traversed.

Algorithmic Steps of Improved SNMP are given in Table.4.1

Table.4.1 Improved SNMP Algorithm

```
Input:S-> CommandGenerator, R->CommandResponder
repeat
  for each neighbor  node in the network
     if route exists then
          send Pdu to dispatcher
          send DTS outgoing Message prepared to generate RequestMsg
          security model prepares RequestMsg
          R registers engine ID with acknowledgement from S
     end if
          response Pdu processed  { The Command responder Sends Response message back}
     if   response Pdu returned by R then
          security model generates responseMsg
          dispatcher prepares response Msg
    end if
          S sends a RREQ to all nodes
          check sequence number
   for all neighbor nodes in the network
        if TTL (Time To Live) is exceeded then
            STOP
       else
            assign DTS message to recover failure data
           send NACK to control message format bits
      end if
   end
    RRER reaches S
    S starts a new RREQ
  end
until the last  node in the network
```

Simulation Methodology

The entire experiments are conducted in a simulated environment using NS2. The number of nodes communicating in different terrain area is considered for experimentation. Specific traffic models and routing protocols are considered. Initially, the source node broadcasts the route request to all other nodes in the network. The packets are sent to the nodes that sent a reply to the route request. The packets will be sent from the source node to the nodes that have sent a reply. On receiving the packet, the nodes send an acknowledgement to the source. The other nodes that have not received the packets will send the NACK (Negative Acknowledgement) to the source. The packets are resent to those nodes once again. The values of the parameter, end to end delay, packet loss and throughput are calculated for all the different simulated models.

The experimental results indicate that irrespective of the data transfer rate, network surface area, the proposed method gives desirable results to preserve the quality while vigorous monitoring.

Simulation Parameters

In order to show the efficiency of the proposed system, it is tested in various surface areas starting from 200m x 200m up to 1500m X 1500m for 100 nodes and the simulation parameters used for those surface areas are depicted in Table.4.2. Apart from that, the proposed system is also tested with various routing protocols say DSR, TORA and OLSR (Figures.4.8 to 4.10). Moreover, the simulation is performed for 10,30, 50 and 80 nodes (Figures.4.11 to 4.14). The Traffic model is also changed to VBR and the results also shown (Figures4.15 to 4.19).

The different parameters used for simulation are shown in table4.2.

Table.4.2 Simulation Parameters

S.No	Parameters	Values
1	Simulator	NS2 (nsallinone2.35)
2	Channel Type	Wireless Channel
3	Number of Nodes	10,30,50,80,100
4	Node Placement Strategy	Random
5	Propagation Model	Two way Ground
6	Traffic Model	CBR, VBR
7	Terrain Area	200mx200m till 1500mx1500m
8	Transmission Range	150m – 250m
9	MAC Protocol	802.11
10	Routing Protocol	AODV,DSR,RIP, TORA,OLSR, OSPF
11	Observation Parameter	End to end delay, Packet loss and Throughput

The metrics used for evaluation are

i. End to End Delay
ii. Packet Loss
iii. Throughput

End to End Delay

The performance of the proposed method is evaluated in terms of end-to-end delay. Total time utilized to transmit the data from the source to the destination.

$$delay_i = \frac{1}{nbx} \sum_{i \in x} \sum_{i \in y} \frac{delay_i}{nby}$$

x: is the set of destination nodes that received data packets.

nbx: is the number of receiver nodes

y: is the set of packets received by node i as the final destination.

Packet Loss

In digital communications, usually there is a chance for three errors. they are packet loss, bit error and spurious packets. The Packet lost is calculated as the number of packet received at the destination will be deducted with the number of packet sent from the source.

$$Packetloss = no.of\ packetsreceived - no.of\ packetssent$$

Throughput

The network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in data packets per second or data packets per time slot i.e. number of bytes of data that is transferred per second between source and destination.

$$\text{Throughput} = \frac{Number\ of\ bits\ received\ per\ second}{Number\ of\ bits\ sent\ per\ second}$$

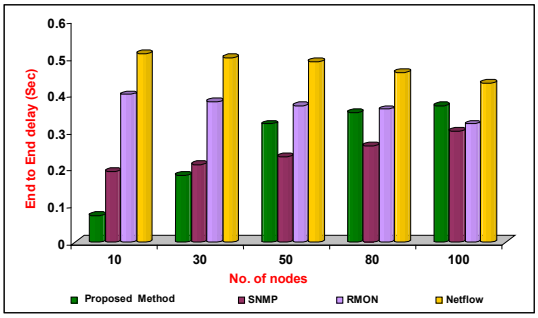

Figure.4.2(a) 200m x 200m

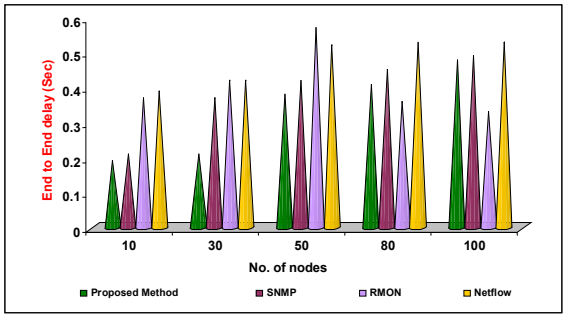

Figure.4.2(b) 400m x 400m

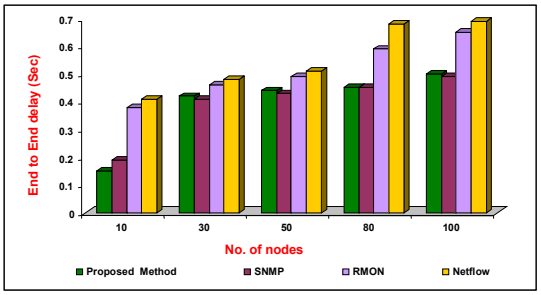

Figure.4.2(c) 600m x 600m

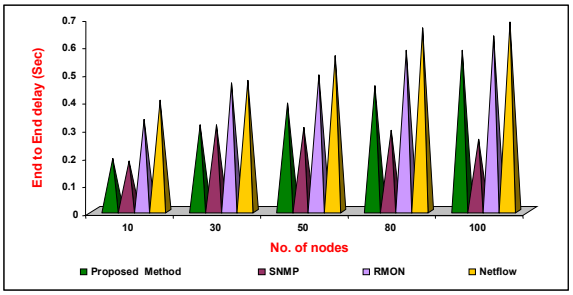

Figure.4.2(d) 800m x 800m

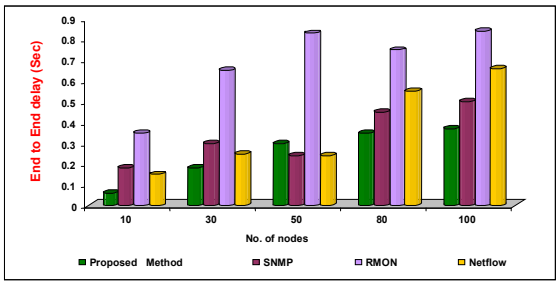

Figure.4.2(e) 1000mx1000m

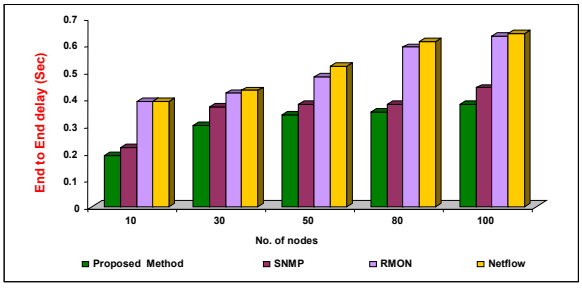

Figure.4.2(f) 1200mx1200m

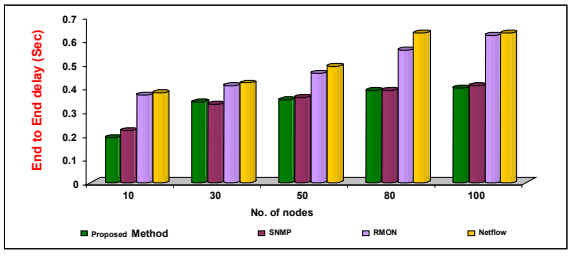

Figure.4.2(g) 1400mx1400m

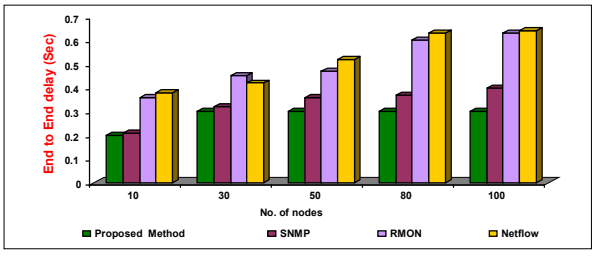

Figure.4.2(h) 1500mx1500m

Figure.4.2 Comparative result for End to end delay based on Data Transfer Rate using AODV for Network Surface areas 200 m x 1500mx1500m

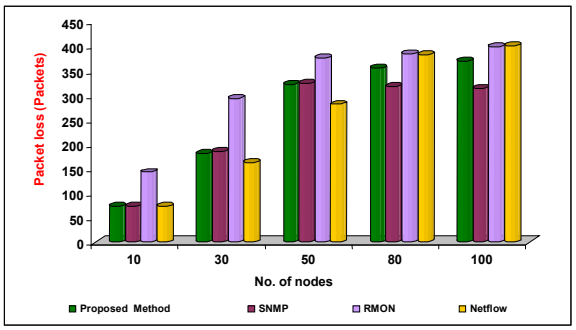

Figure.4.3(a) 200mx200m

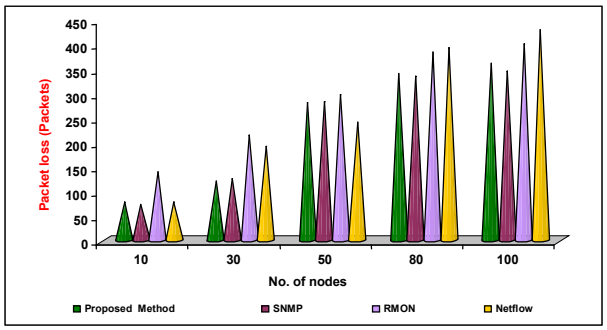

Figure.4.3(b) 400mx400m

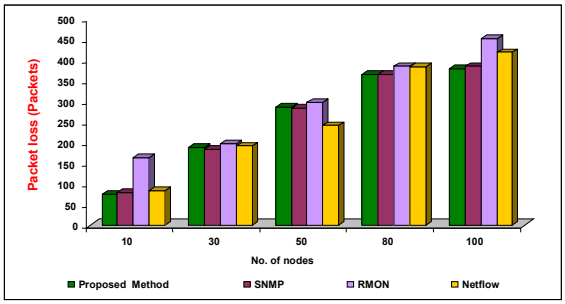

Figure.4.3(c) 600mx600m

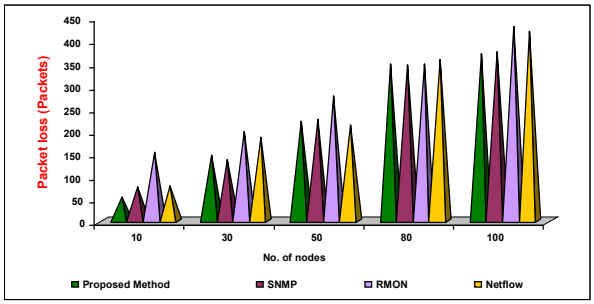

Figure.4.3(d) 800mx800m

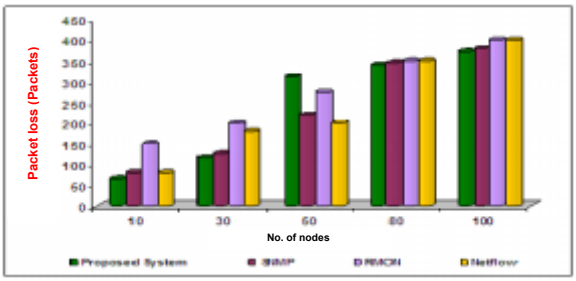

Figure.4.3(e) 1000mx1000m

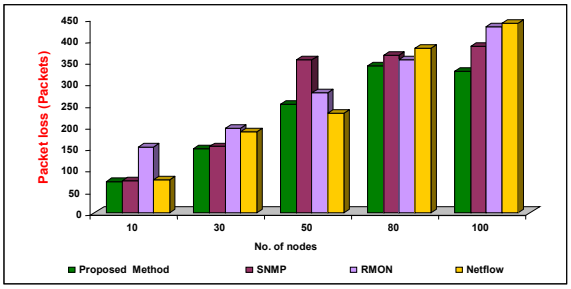

Figure.4.3(f) 1200mx1200m

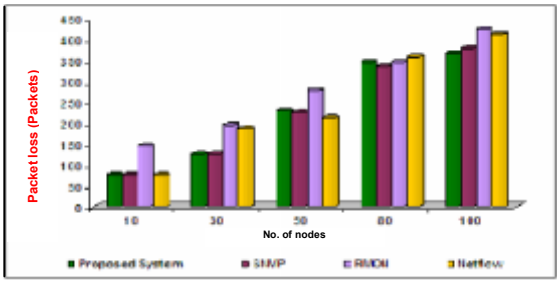

Figure.4.3(g) 1400mx1400m

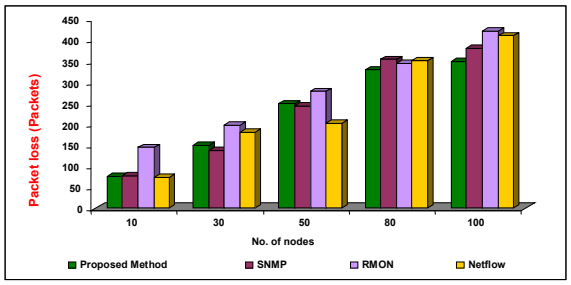

Figure.4.3(h) 1500mx1500m

Figure.4.3 Comparative result for Packet loss based on Data Transfer Rate using AODV for Network Surface areas 200 m x 1500mx1500m

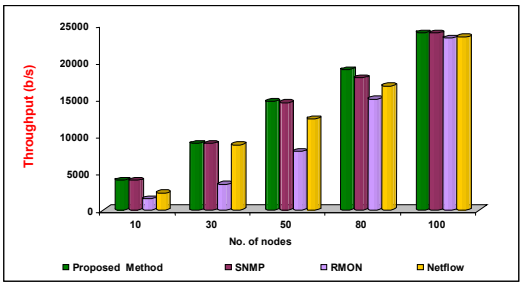

Figure.4.4(a) 200mx200m

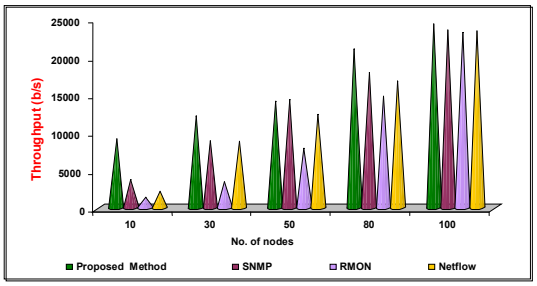

Figure.4.4(b) 400mx400m

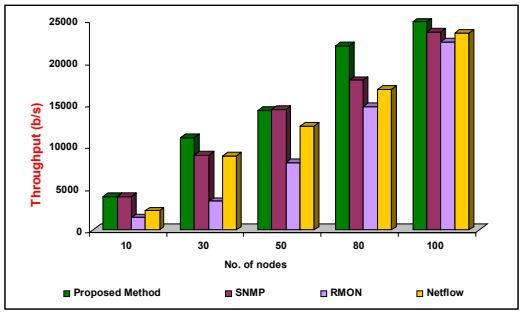

Figure.4.4(c) 600mx200m

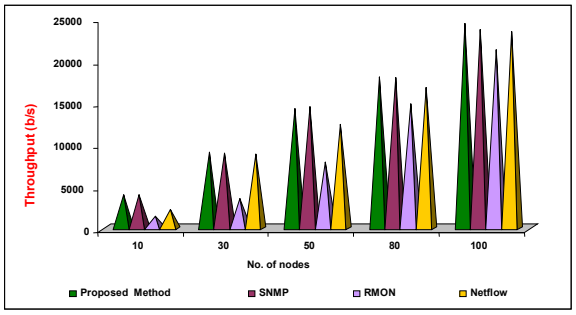

Figure.4.4(d) 800mx400m

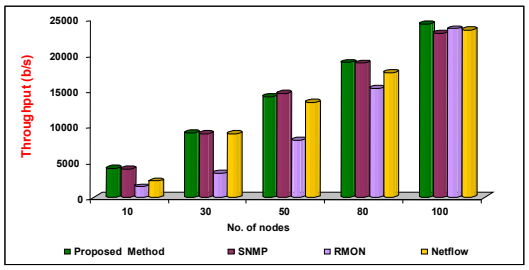

Figure.4.4(e) 1000mx1000m

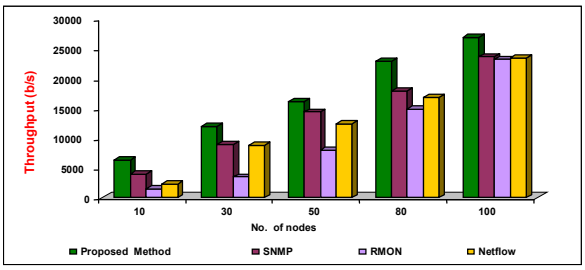

Figure.4.4(f)1200mx1200m

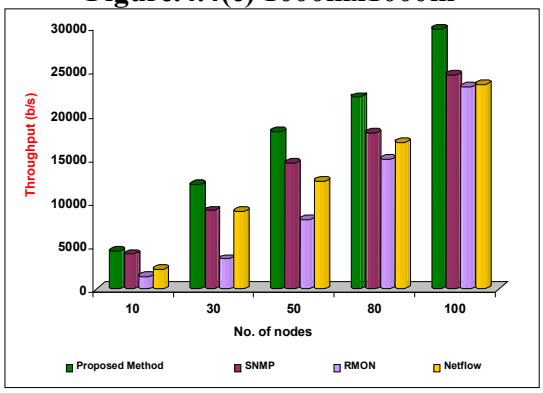

Figure.4.4(g) 1400mx1400m

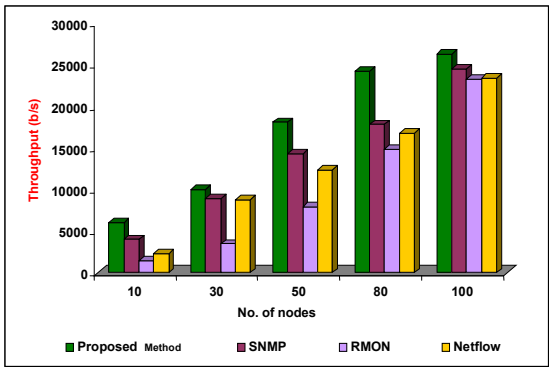

Figure.4.4(h) 1500mx1500m

Figure.4.4. Comparative result for Throughput based on Data Transfer Rate for Network Surface Areas 200m x 200m to 1500m x 1500m

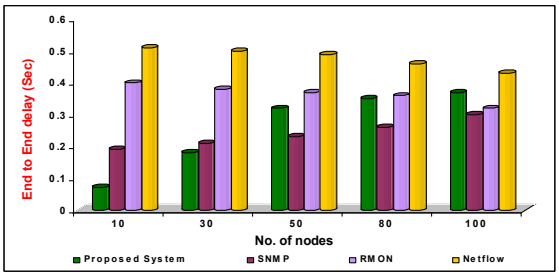

Figure.4.5(a) 200m x 200m

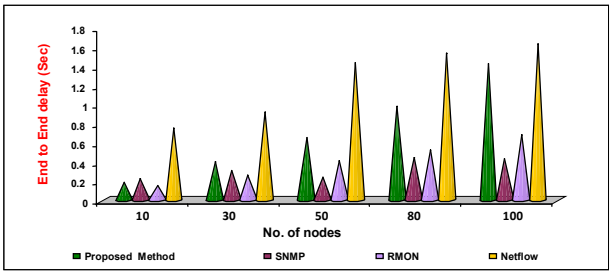

Figure.4.5(b) 400m x 400m

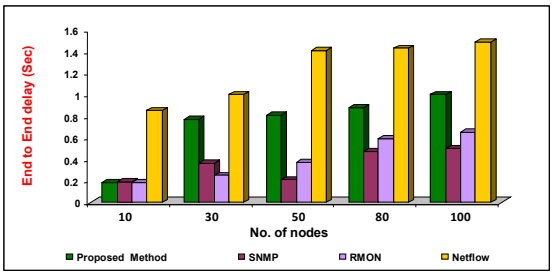

Figure.4.5(c) 600m x 600 m

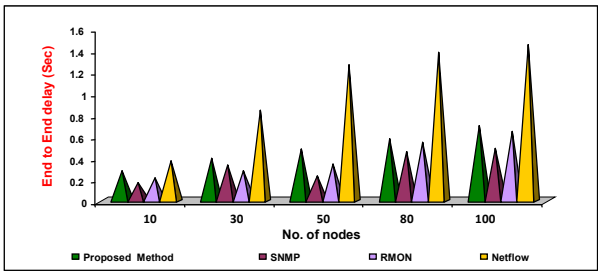

Figure.4.5(d) 800m x 800 m

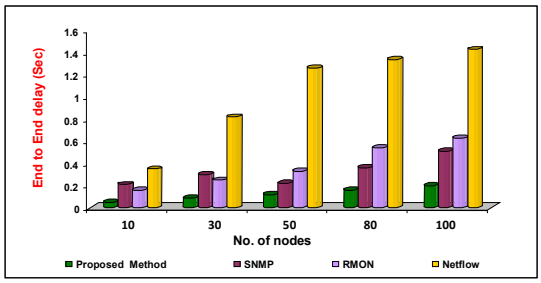

Figure.4.5(e) 1000m x 1000m

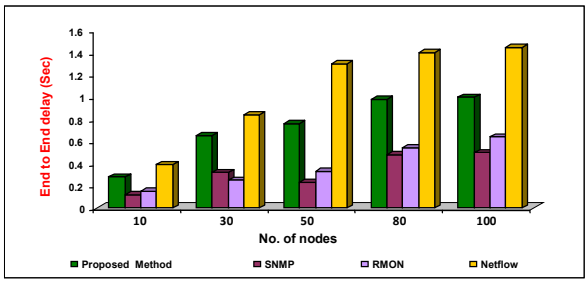

Figure.4.5(f) 1200m x 1200m

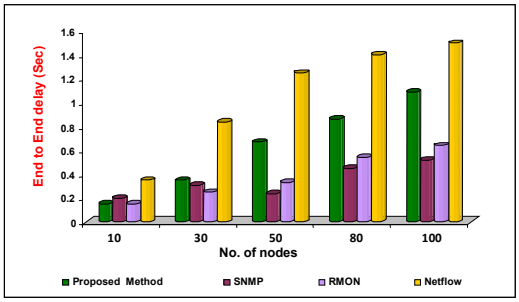

Figure.4.5(g) 1400m x 1400m

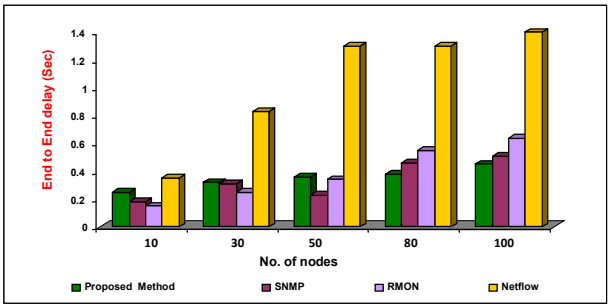

Figure.4.5(h) 1500m x 1500 m

Figure 4.5 Comparative results for End to End Delay based on Time for Network Surface Areas 200m x 200m to 1500m x 1500m

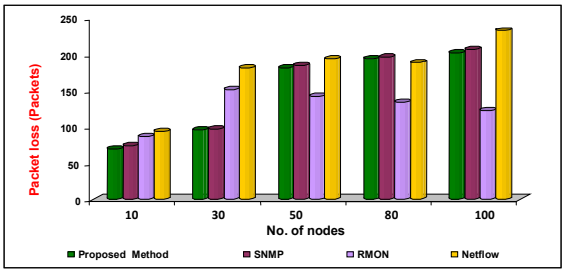

Figure.4.6(a) 200mx200m

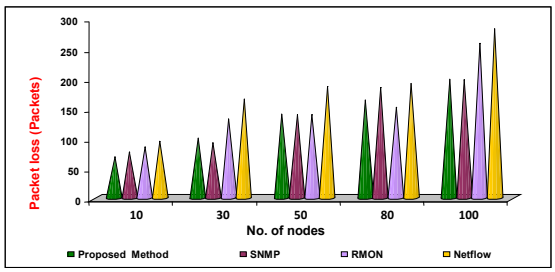

Figure.4.6(b) 400mx400m

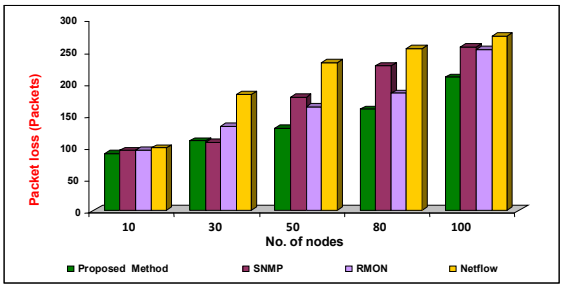

Figure.4.6(c) 600m x 600m

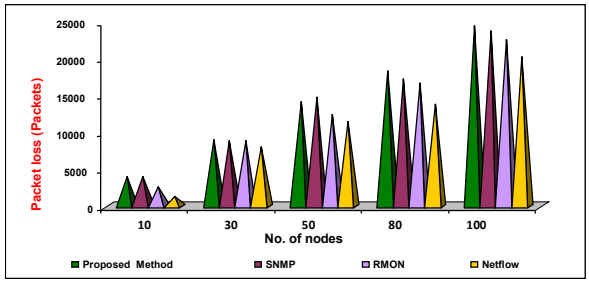

Figure.4.6(d) 800m x 800m

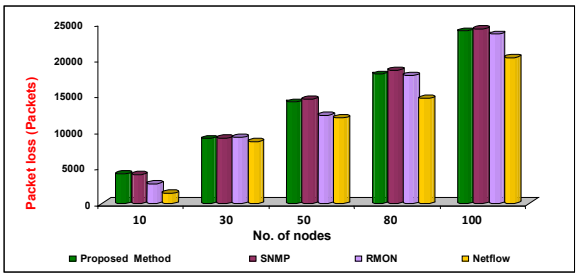

Figure.4.6(e) 1000m x 1000m

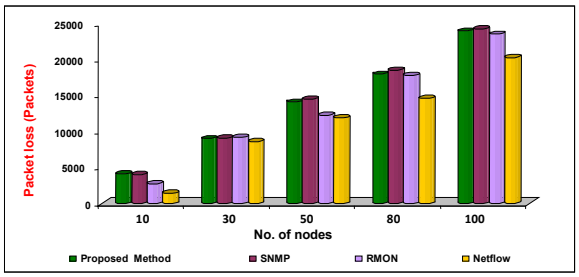

Figure.4.6(f) 1200m x 1200m

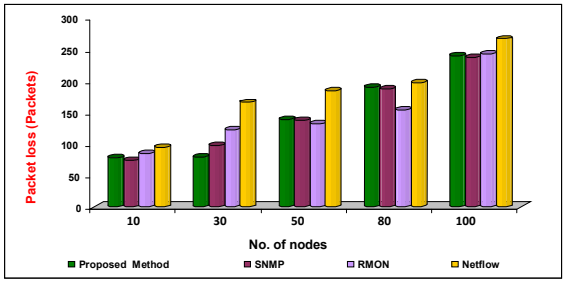

Figure.4.6(g) 1400m x 1400m

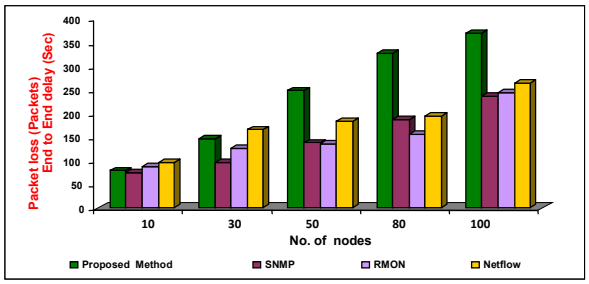

Figure.4.6(h)1500m x 1500m

Figure 4.6 Comparative results for Packet Loss based on Time for Network Surface Areas 200m x 200m to 1500m x 1500m

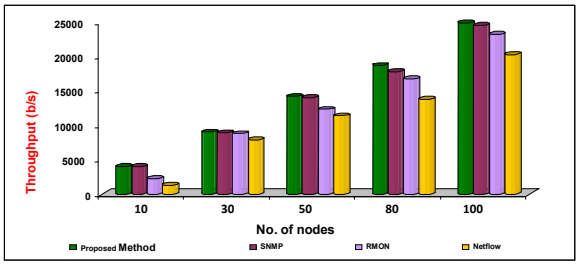

Figure.4.7(a) 200m x 200m

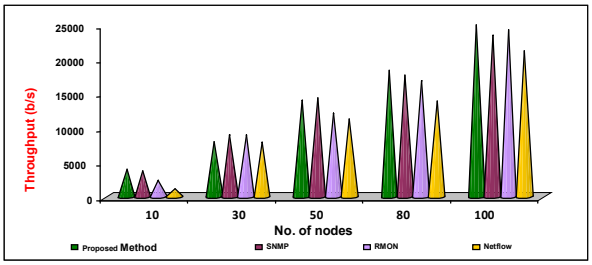

Figure.4.7(b) 400m x 400m

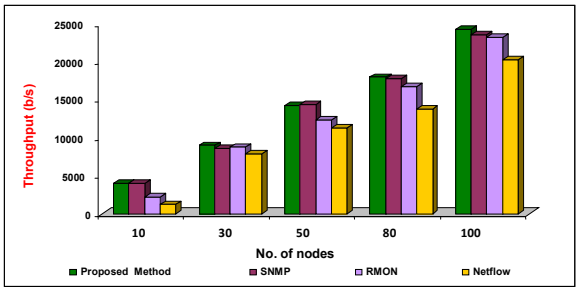

Figure.4.7(c) 600m x 600m

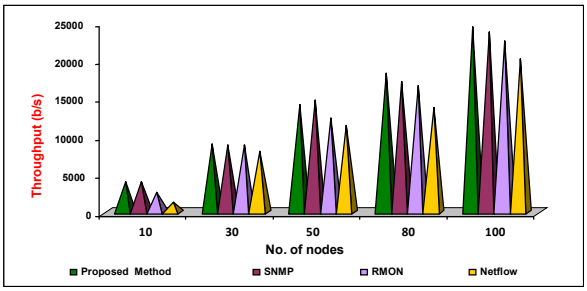

Figure.4.7(d) 800m x 800m

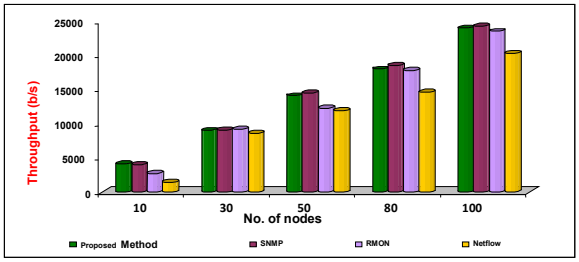

Figure.4.7(e) 1000m x 1000m

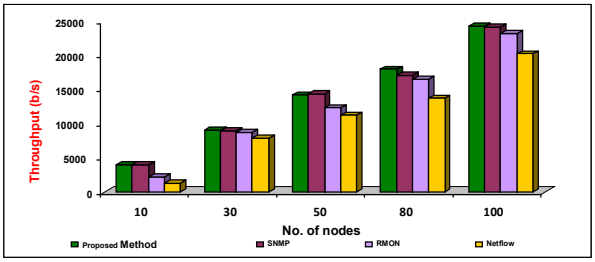

Figure.4.7(f) 1200m x 1200m

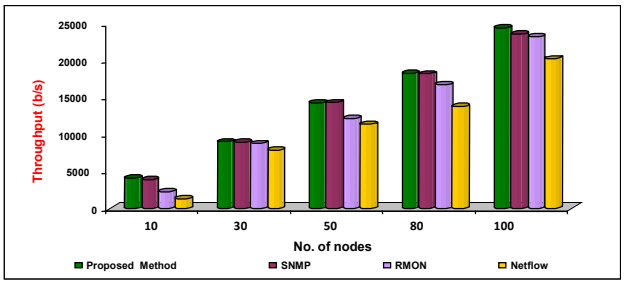

Figure.4.7(f) 1400m x 1400m

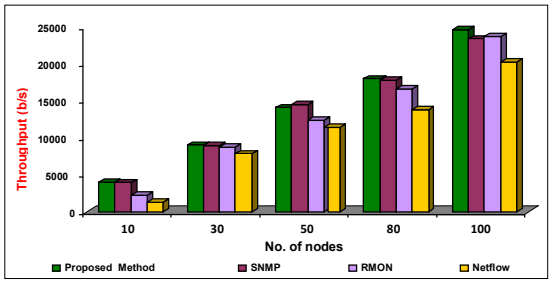

Figure.4.7(g) 1500m x 1500m

Figure 4.7 Comparative results for Throughput based on Time for Network Surface Areas 200m x 200m to 1500m x 1500m

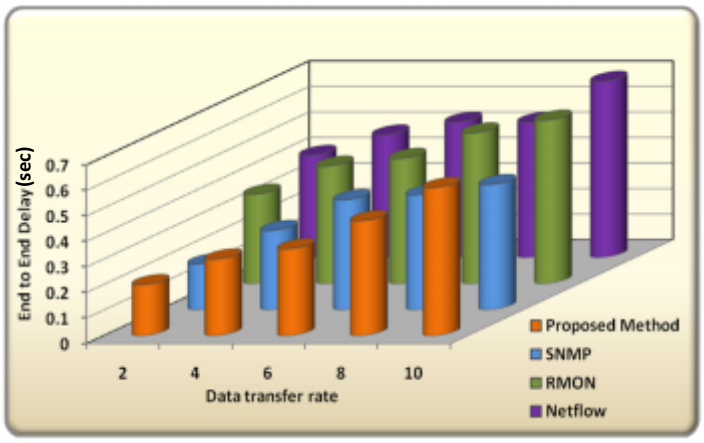

Figure. 4.8(a) End to End Delay using DSR Protocol

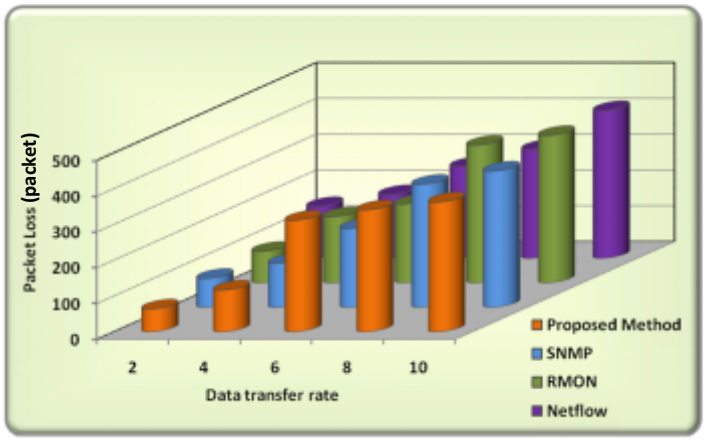

Figure.4.8(b) Packet loss using DSR protocol

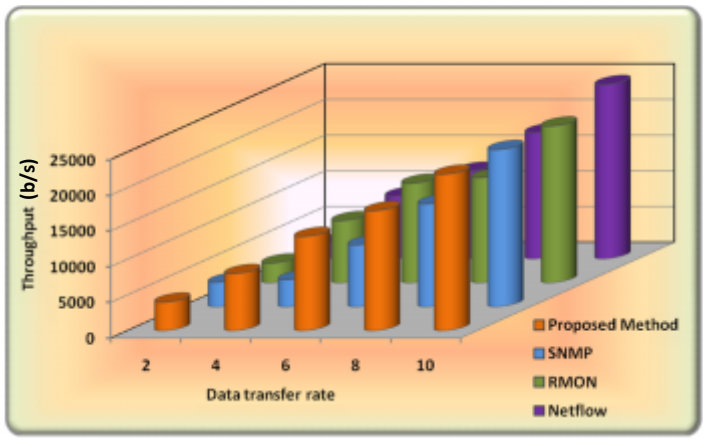

Figure.4.8 (c) Throughput using DSR protocol

Figure. 4.8. Simulation Parameters for 100 Nodes with different secure routing protocol – DSR

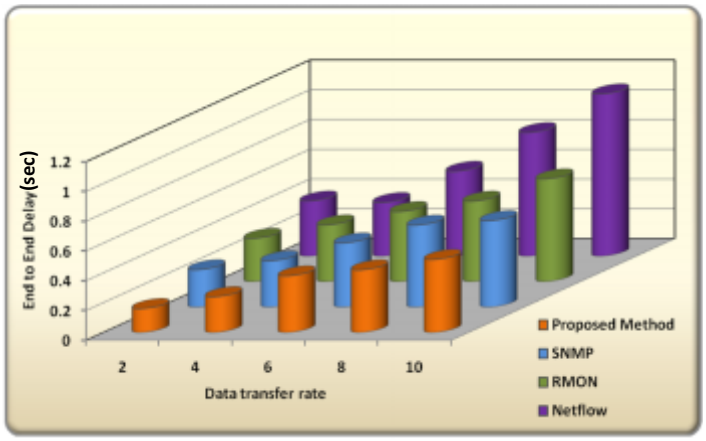

Figure.4.9 (a) End to End delay using TORA protocol

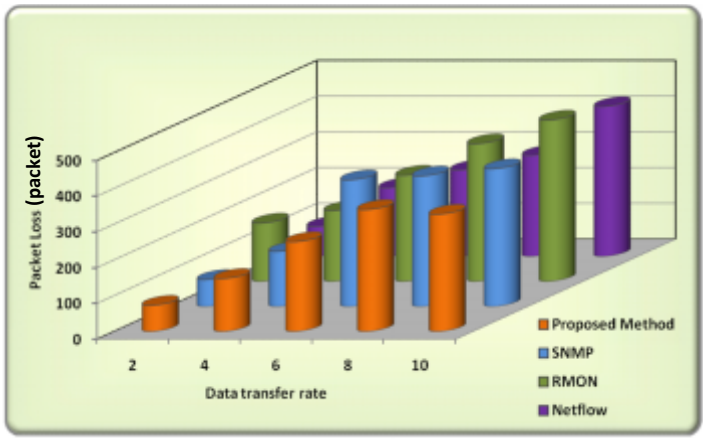

Figure.4.9 (b) Packet Loss using TORA protocol

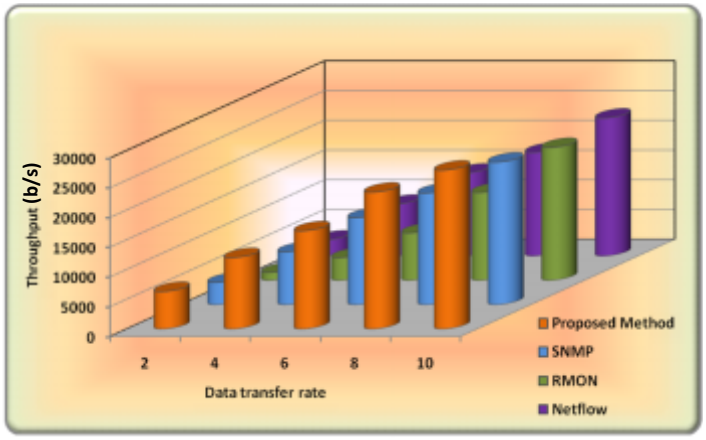

Figure.4.9(c) Throughput using TORA protocol

Figure.4.9.Simulation Parameters for 100 Nodes with different secure routing protocol – TORA

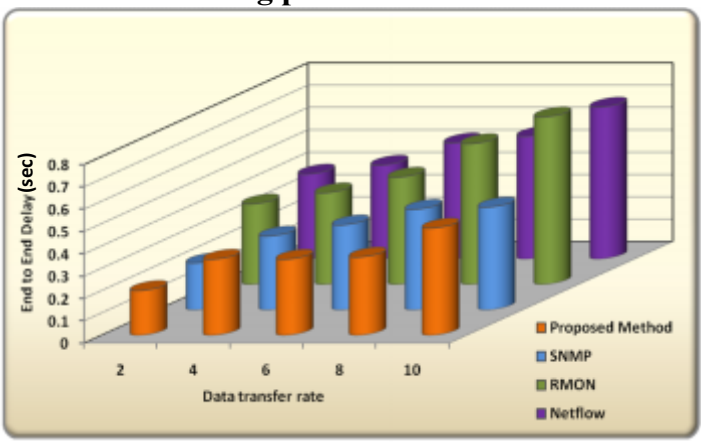

Figure.4.10(a) End to End deay using OLSR protocol

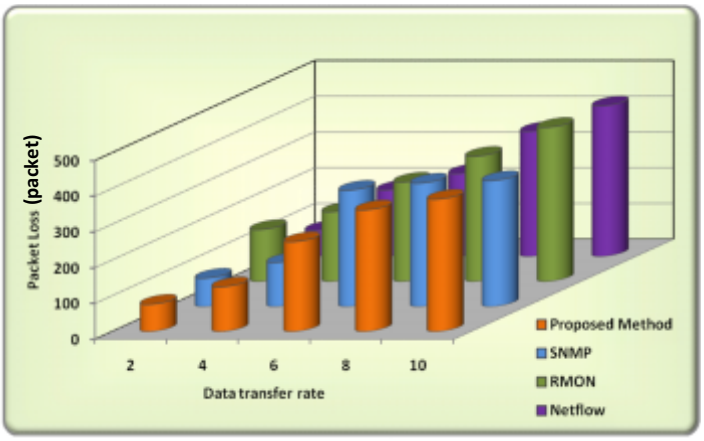

Figure.4.10(b) Packet Loss using OLSR protocol

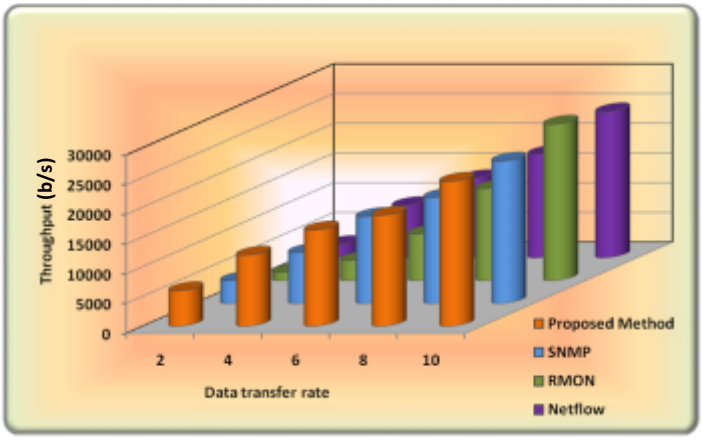

Figure.4.10 (c) Throughput using OLSR protocol

Figure.4.10. Simulation Parameters for 100Nodes with different secure routing protocol – OLSR

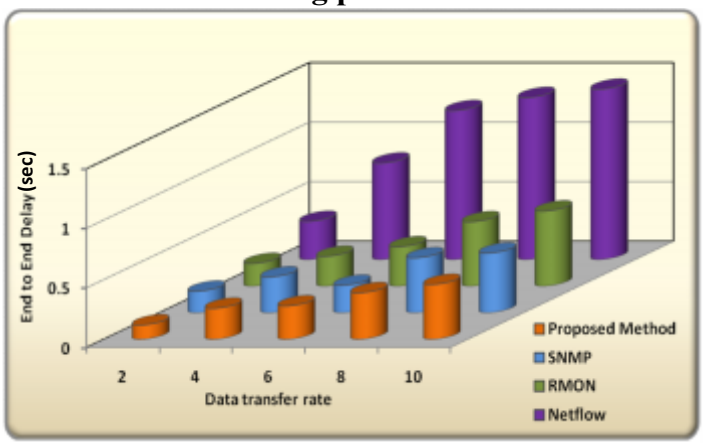

Figure.4.11(a) End to End delay

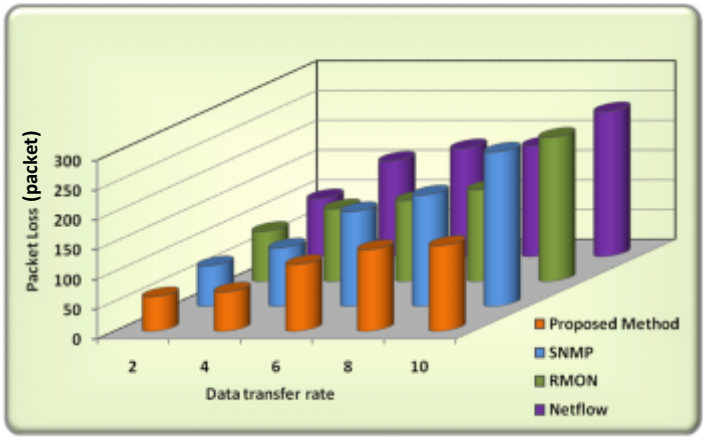

Figure.4.11(b) Packet Loss

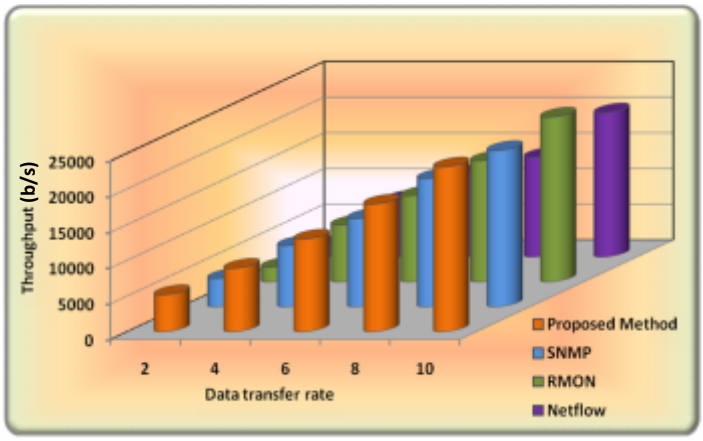

Figure.4.11(c) Throughput

Figure.4.11 Simulation Parameters for 20 Nodes

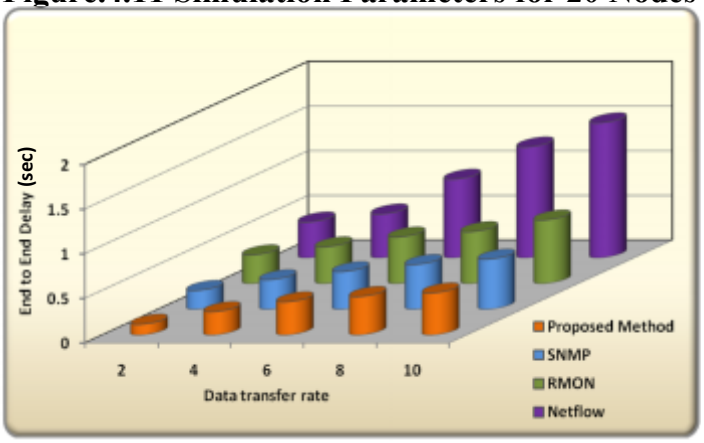

Figure.4.12(a) End to End Delay

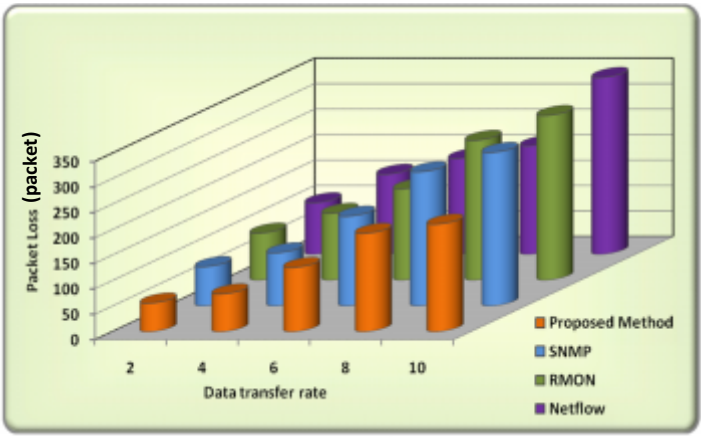

Figure.4.12(b) Packet Loss

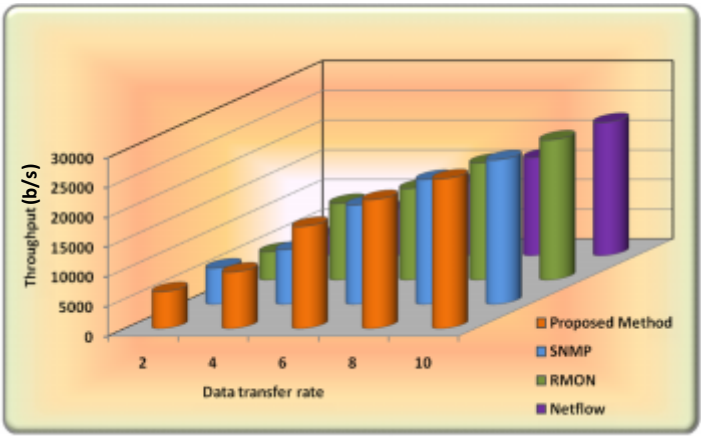

Figure.4.12(c) Throughput for 40 nodes

Figure.4.12. Simulation Parameters with 40 nodes

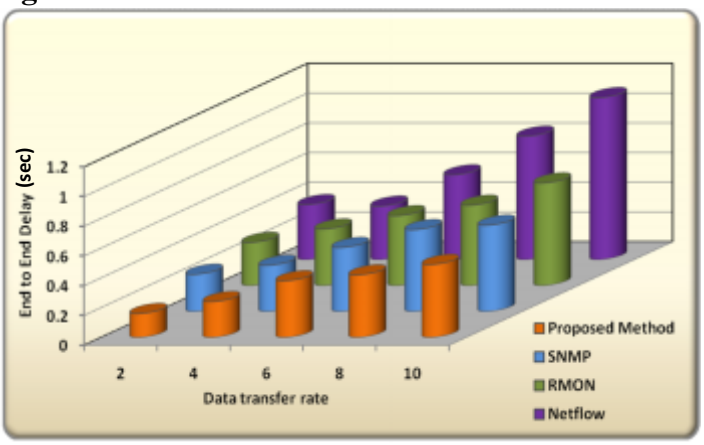

Figure.4.13(a) End to End Delay

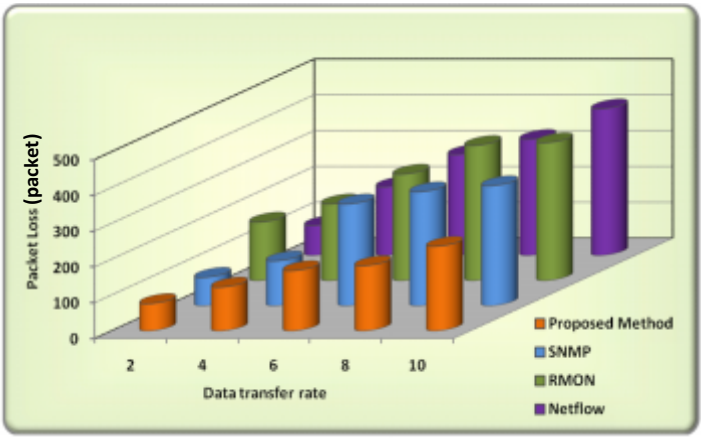

Figure.4.13(b) Packet Loss

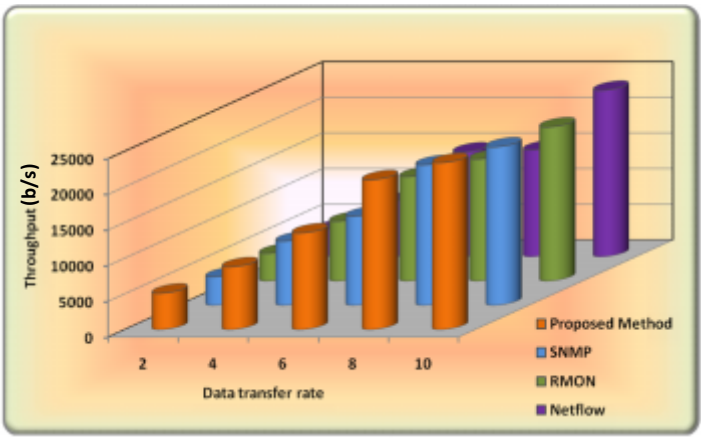

Figure.4.13(c) Throughput

Figure.4.13 Simulation Parameters for 60 Nodes

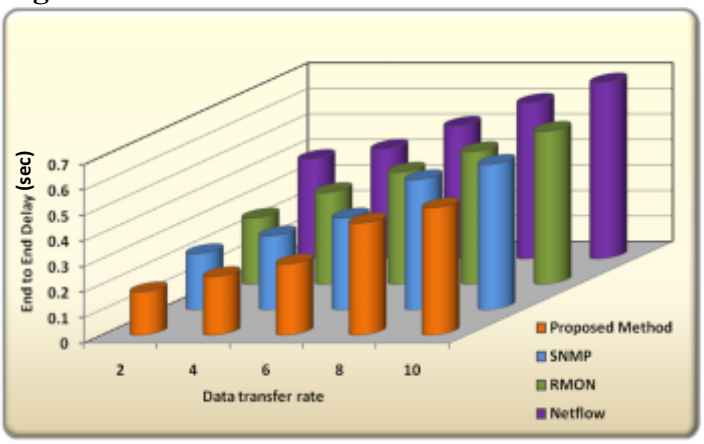

Figure.4.14(a) End to End Delay

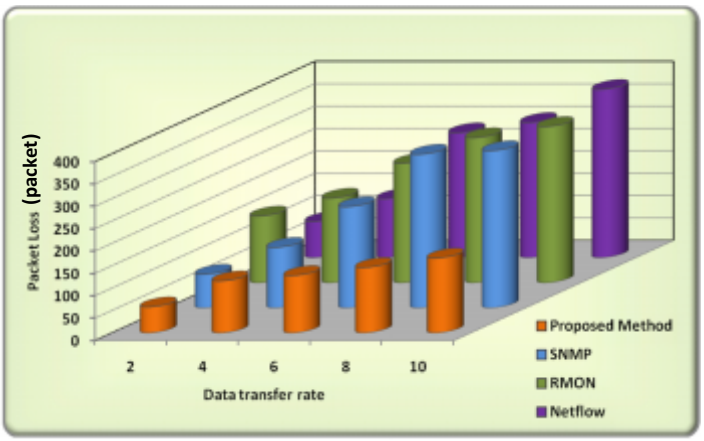

Figure.4.14(b) Packet Loss

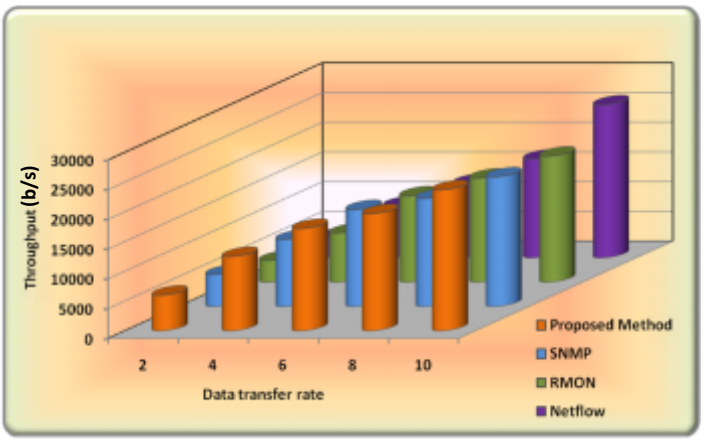

Figure.4.14(c) Throughput

Figure.4.14 Simulation Parameters for 80 Nodes

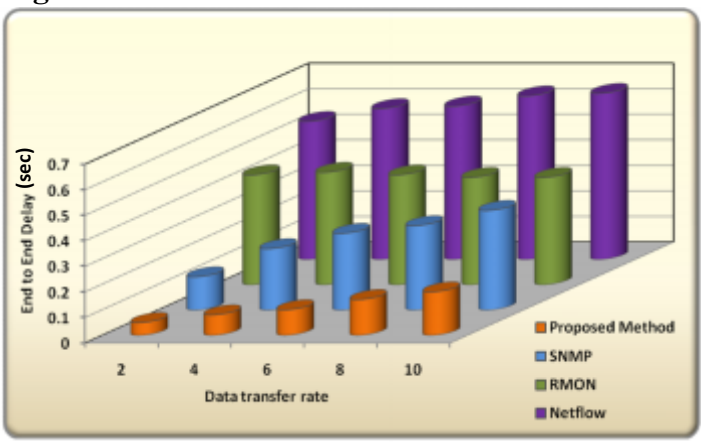

Figure.4.15(a) End to End Delay

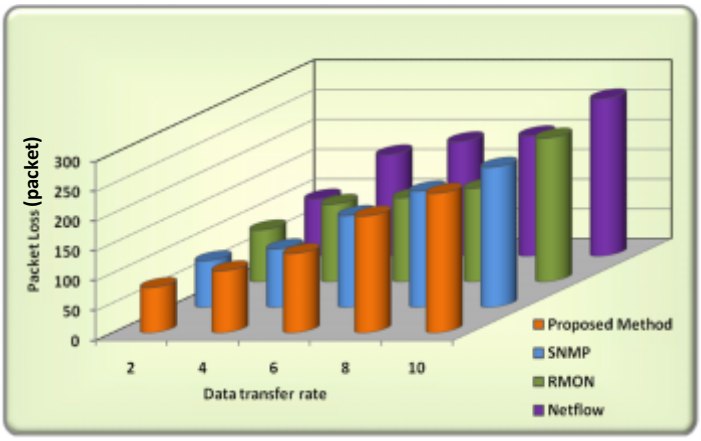

Figure.4.15(b) Packet Loss

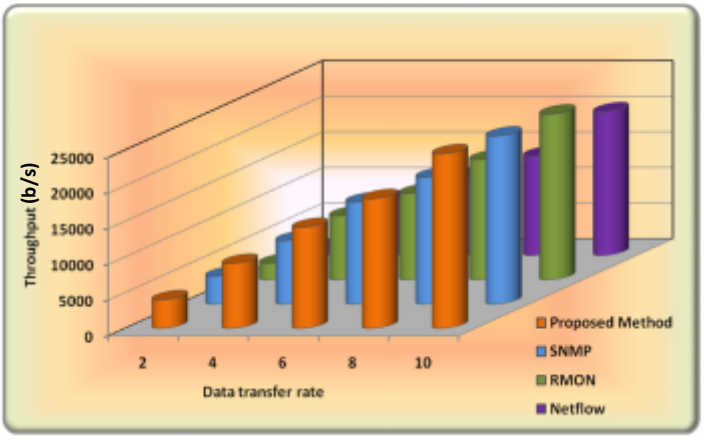

Figure.4.15(c) Throughput

Figure.4.15.Traffic Model – VBR - Simulation Parameters with 20 nodes

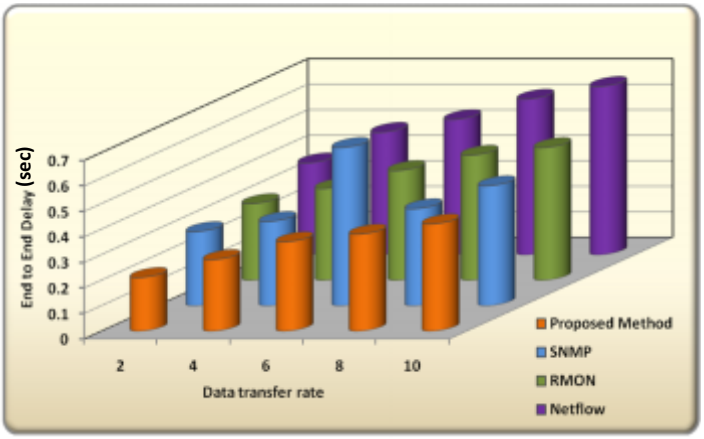

Figure.4.16(a) End to End Delay for 40 Nodes

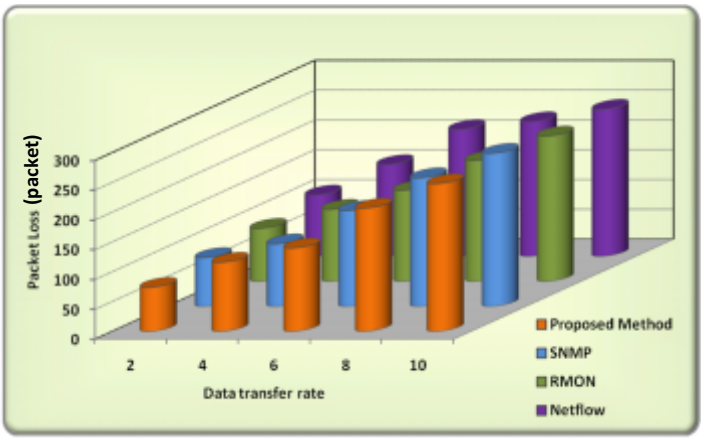

Figure.4.16(b) Packet Loss for 40 Nodes

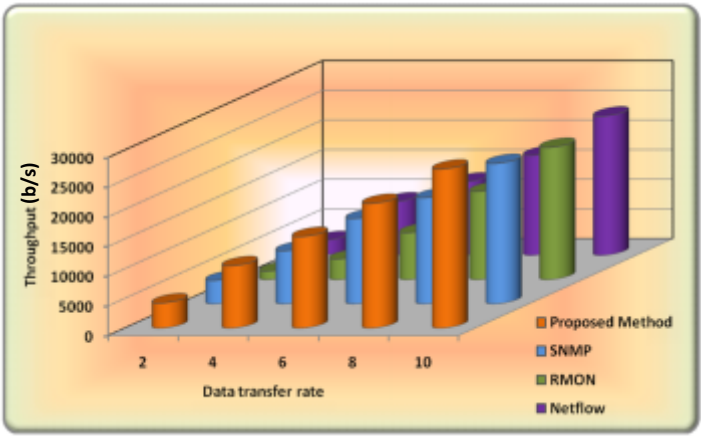

Figure. 4.16(c) Throughput for 40 Nodes

Figure.4.16.Traffic Model – VBR - Simulation Parameters with 40 nodes

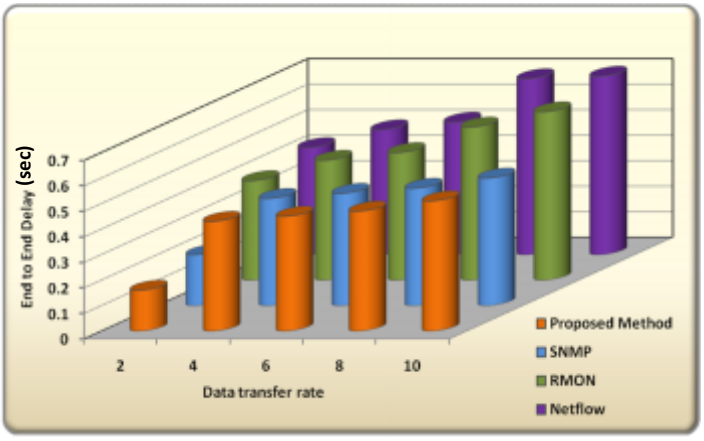

Figure.4.17(a) End to End Delay for 60 Nodes

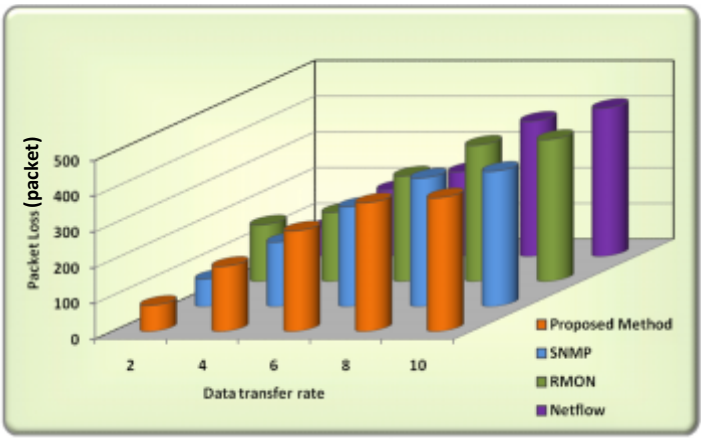

Figure.4.17(b) Packet Loss for 60 Nodes

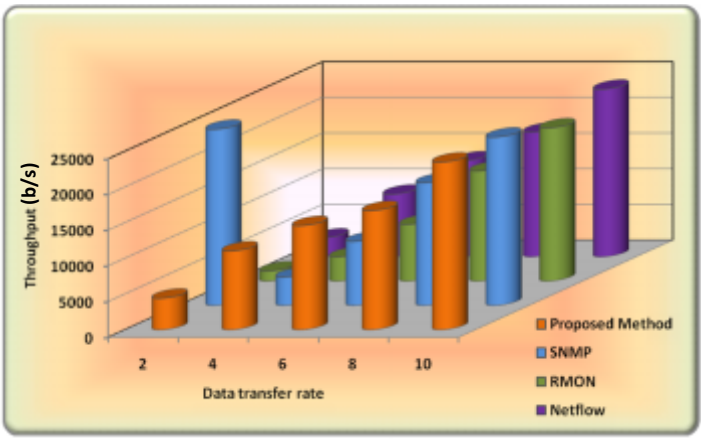

Figure.4.17(c) Throughput for 60 Nodes

Figure.4.17.Traffic Model – VBR - Simulation Parameters with 60 nodes

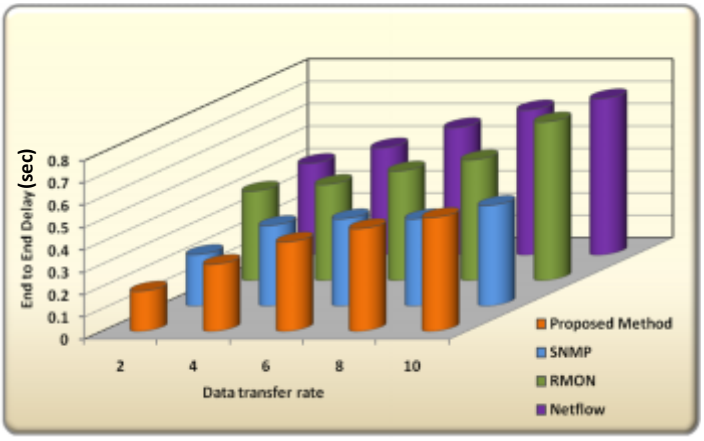

Figure.4.18 (a) End to End Delay

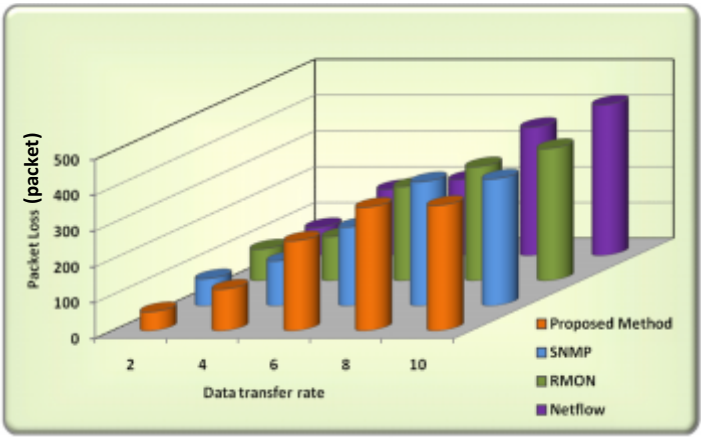

Figure.4.18 (b) Packet Loss

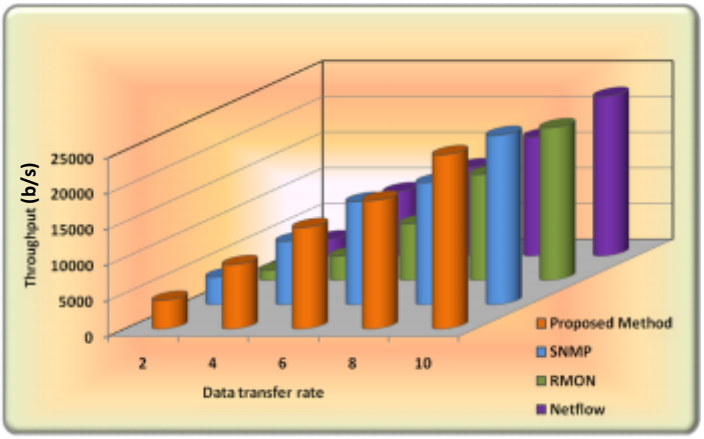

Figure.4.18 (c) Throughput

Figure.4.18.Traffic Model – VBR -Simulation Parameters with 80 nodes

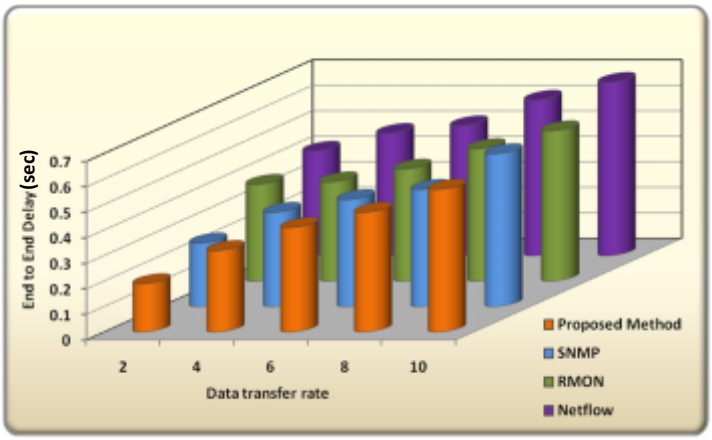

Figure.4.19(a) End to End Delay

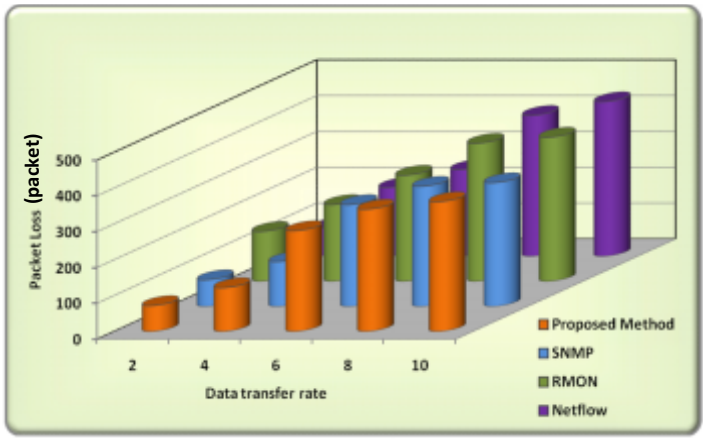

Figure.4.19(b) Packet Loss

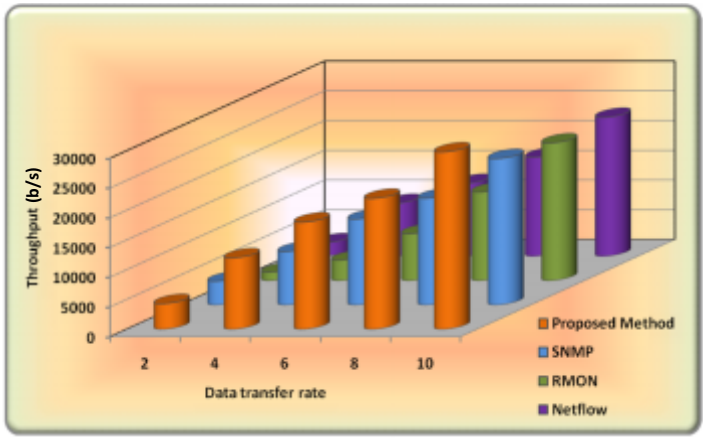

Figure.4.19 (c) Throughput

Figure.4.19.Traffic Model – VBR -Simulation Parameters with 100 nodes

Figure.4.19.Traffic Model – VBR -Simulation Parameters with 100 nodes

From the results shown in figures.4.2 to 4.19, it is obvious that the proposed method has outperformed the other methods.

4.1.1. Numerical Comparison of the Performance Metrics

The performance of the proposed method is also evaluated numerically based on the properties of the metrics are additive, multiplicative and concave. Additive is used to delay and multiplicative for packet loss. The formula used is given below:

$$Additive \quad : d(p) = d\ (n_1, n_2) + d\ (n_2, n_3) + ... + d\ (n_{m-1}, n_m)$$

$$Multiplicative : d(p) = d(n_1, n_2) \times d\ (n_2, n_3) \times .... \times d\ (n_{m-1}, n_m)$$

Let $d(n_i,n_j)$ be a metric for the link (n_i,n_j) and $p = (n_1,n_2,...,n_m)$ be a path between nodes n_1 and n_m

$$Throughput : T = \frac{K(P+H)}{D}$$

K ----> No.of packets per window

P ----> No.of payload bits per packet

H ----> No.of header bits per packet

D ----> Delay of link

Table.4.3. Numerical Comparison results of the performance metrics

Performance Metrics	**Enhanced SNMP**	**SNMP**	**RMON**	**Netflow**
End to End delay(Sec)	**89**	90.0002	90.0007	90.0004
Packet loss(Packets)	**9477**	10120	10635	10022
Throughput(bits/sec)	**1902**	1678	1337.5	611

Router based monitoring techniques SNMP, RMON and Netflow are implemented using NS-2 simulators in different surface areas varying from 200m x 200m to 1500mm x 1500mm surface area based on data transfer rate and time using the three performance metrics end to end delay, packet loss and throughput which are the most important parameters to evaluate the network performance.

The analysis of the data by comparison of metrics such as Packet loss, Throughput and End to End Delay conclusively proves the use of Enhanced SNMP that shows a great deal of consistency and accuracy in traffic monitoring and suggests that Enhanced SNMP is the best tool for monitoring networks among the four routers based techniques. It is also proved numerically by using the mathematical formula.

After monitoring the network traffic, the next step in the proposed methodology is known cyber attack detection.

4.2. Detection of known Cyber attacks

Dimensionality reduction [87] techniques are generally used to transform the original high dimensional data into consequential description of reduced data. The dimensionality reduction techniques[85] are mainly classified as linear and nonlinear techniques and they are clearly discussed in chapter 2. The process of assuming that the data will be placed on or near a linear subspace of higher dimensional space is termed as linear technique [4]. Following are the linear dimensionality reduction [48][76] techniques applied to reduce the dimension[96] of the traffic data. They are Principal Component Analysis[88], Linear Discriminant Analysis, Independent Component Analysis[2][3] and Enhanced PCA.

The work flow of an enhancement of PCA with SVM is given in figure.4.20

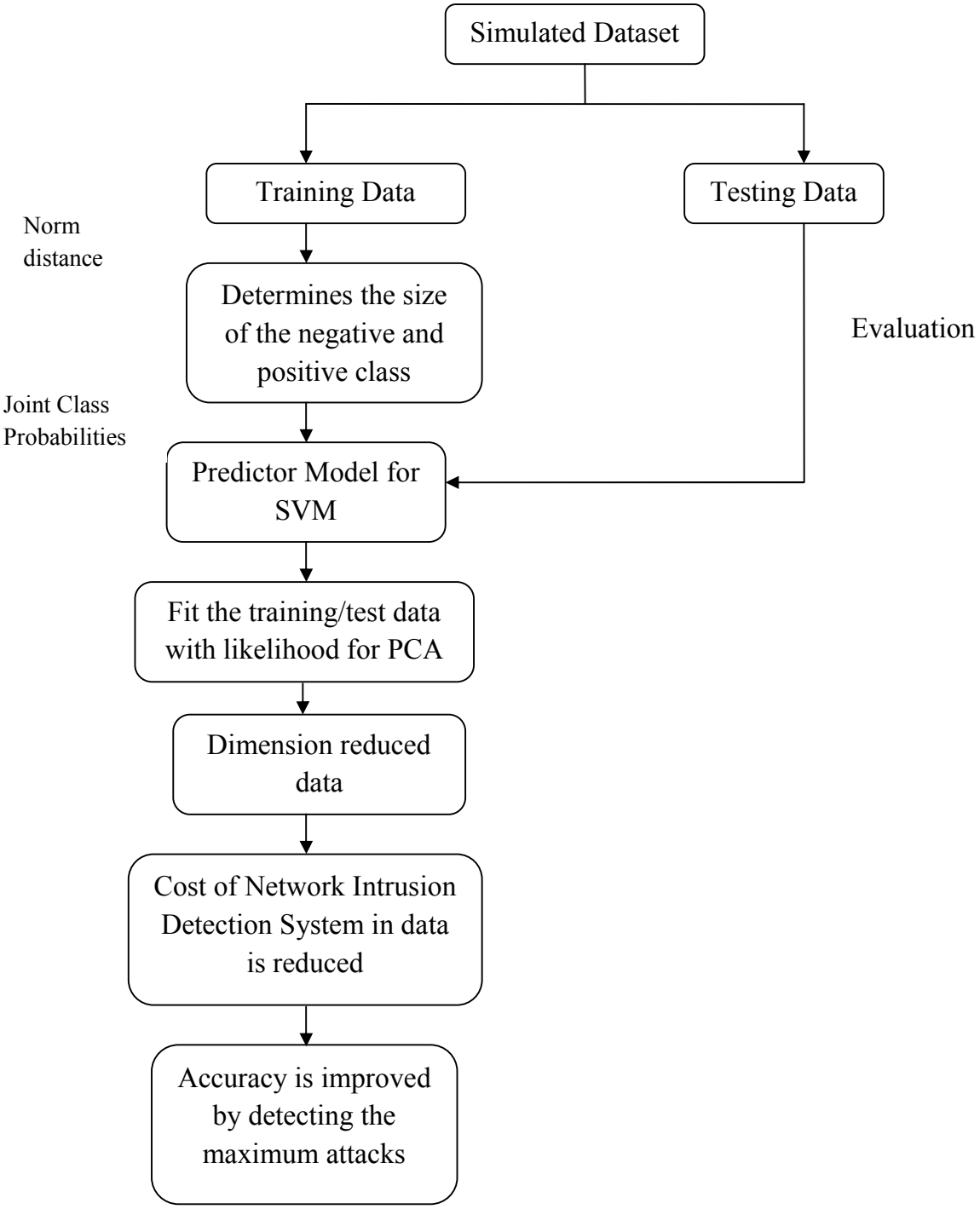

Figure.4.20 Enhancement of PCA with SVM

This integration is used to detect outliers in a given data set. This algorithm can accurately detect anomalies in non-Gaussian data.

Processing Steps:

Step.1 *The dataset will be trained.*

Step.2 *Determine the size of the negative and positive class using norm distance*

Step.3 *The performance of the SVM system classifier is predicted using Joint class probability, construct D1 (y1) and D2(y2) for each distribution respectively.*

Step.4 *Thus, it calculates the margin, the support vectors, the alpha values and the weights.*

Step.5 *The trained dataset will be tested with likelihood for PCA. Predictor model is constructed and the output is ascertained.*

Step.6 *For the connection of records, class labels are represented as 0 for normal and 1 for anomaly class*

Step.7 *Dimension reduced dataset as output*

Step.8 *Cost of NIDS (Network Intrusion Detection System) in the data is reduced.*

Step.9 *Accuracy is improved in detecting the maximum number of attacks.*

Table.4.4 depicts the algorithmic flow of the proposed research work.

Table.4.4 Algorithm for enhanced PCA with SVM

```
Capture input traffic class label
repeat
    If (class label ≥0) then
            represent class label as normal traffic
            construct predictor model
            construct soft decision boundary for training data
            enable likelihood function to map SVM with posterior probabilities
            calculate margin, alpha values and weights
            represent class label '0' as client request
        else
            represent class label as anamoly class
    end if
until end of the data
```

Support Vector Machine

Support Vector Machine[78] is a popular method for classification which is a supervised learning also helps in finding the decision surface of data points of two classes in order to maximize the margin.

$$\underset{\alpha}{\text{Maximize}} \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j} \alpha_i \alpha_j y_i y_j K(x_i, x_j)$$

Subject to $o \leq \alpha_i \leq 1/\lambda_x$

(x,y) is a point on elliptic curve E

α_i - weight

$x_{i \ldots j}$ - data points *(x=1……l)*

Support Vector Machine is also considered as perceptron, hyperplane which helps to separate data. The hyperplane will be identified with the help of perceptron. Every hyperplane will be monitored rather than its working process.

Experimentation and Comparison

Principal component Analysis, Linear Discriminant Analysis and Independent Component Analysis [2] are compared in detecting the known cyber attacks with the given dataset. Among the three, Principal Component Analysis is found to be the best dimensionality reduction techniques. It detects the 87% of the attacks, whereas LDA and ICA finds only 82% and 74% respectively. In order to increase its efficiency the most popular optimization technique SVM is combined with PCA. Usually the optimization techniques will be used to classify the detected attacks. But in this research work, the dataset is given as input in SVM to make data as an optimized one and the output of it is given as input to PCA for detection. While combining the SVM with PCA it increases the accuracy rate at 94%. The percentage of detection rate is increased to 7%. The results are represented in Table.4.5.

Table.4.5 Detection Rate by Enhanced PCA with SVM

S.No	Methods	Attack Detection Rate
1	Principal Component Analysis	87%
2	Linear Discriminant Analysis	82%
3	Independent Component Analysis	79%
4	**Enhanced PCA with SVM**	**94%**

Results

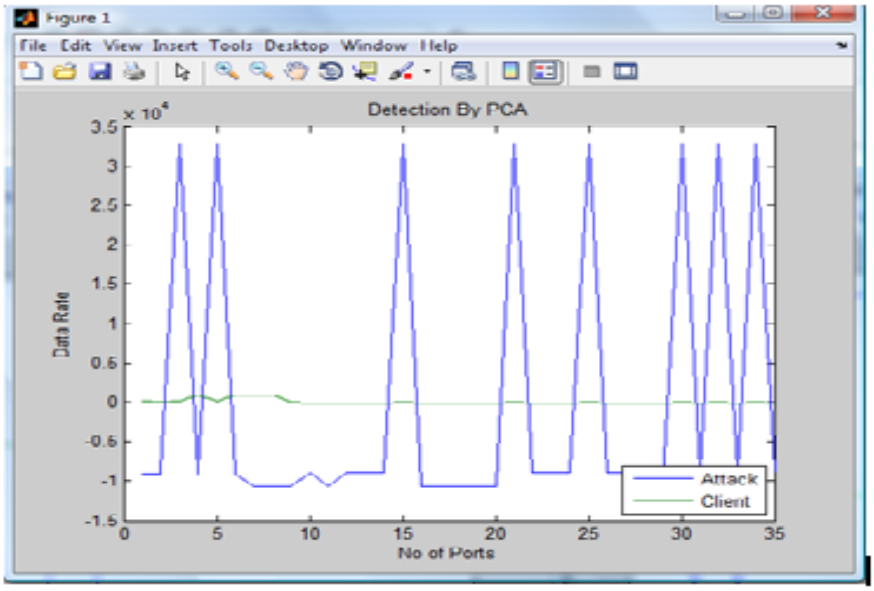

Figure.4.21. Cyber Attack Detection using PCA

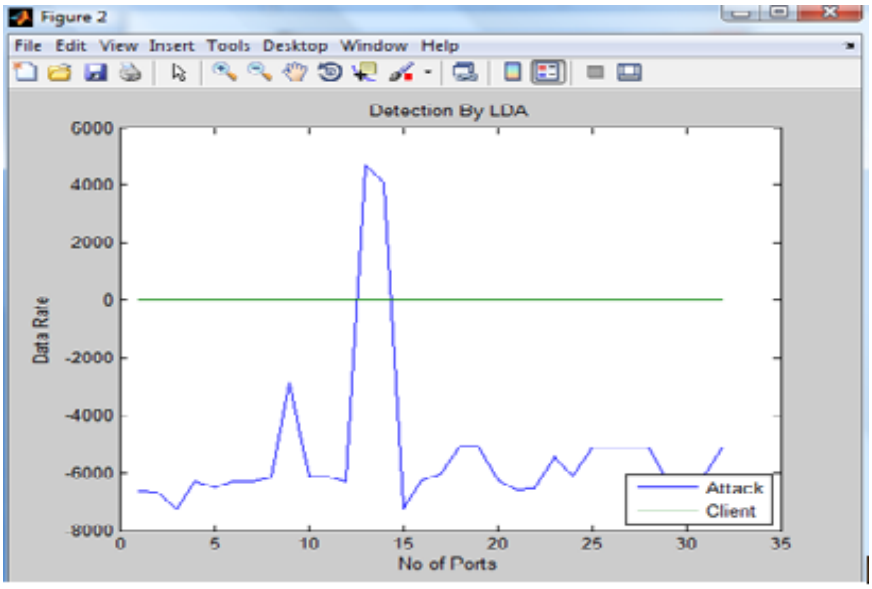

Figure.4.22. Cyber Attack Detection using LDA

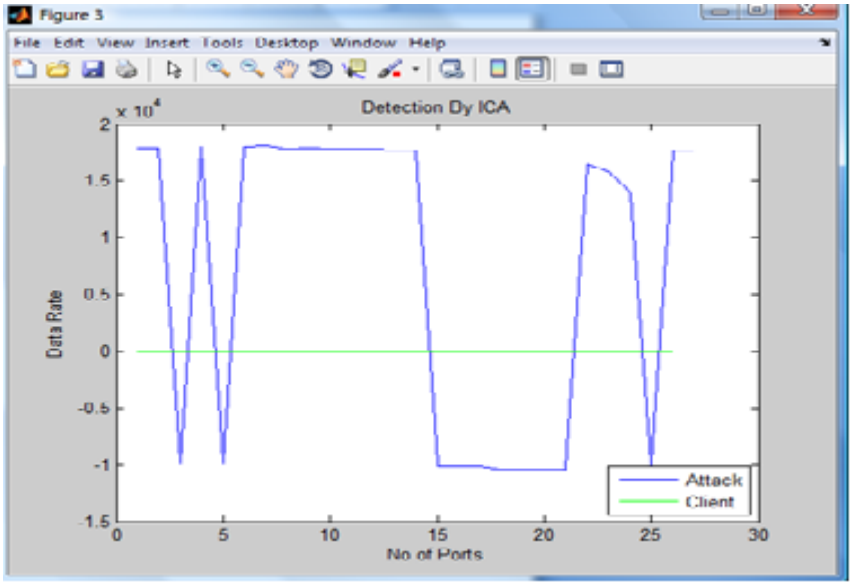

Figure.4.23. Cyber Attack Detection using ICA

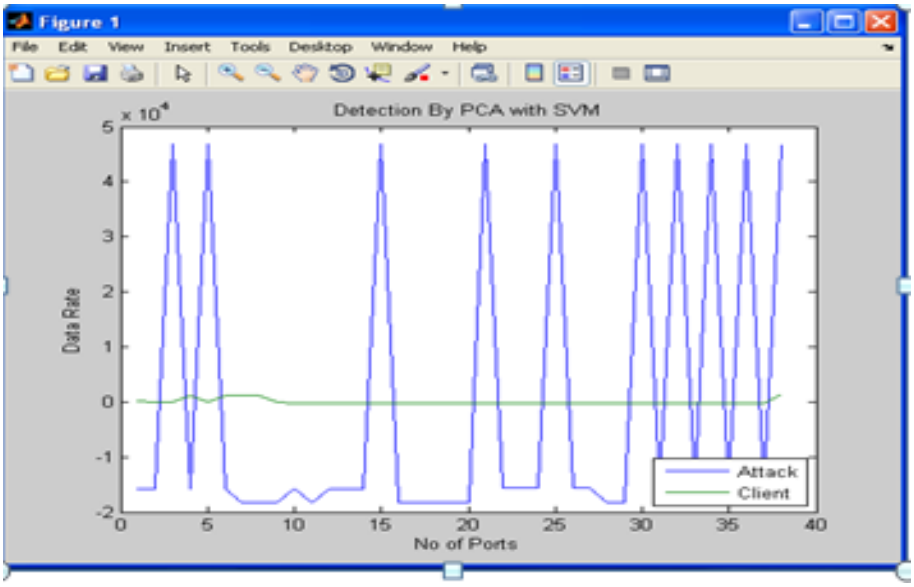

Figure.4.24. Cyber Attack Detection using Enhanced PCA with SVM

4.3. Chapter Summary

Handling known cyber attacks can be done in two steps. Improved traffic monitoring and enhanced PCA with SVM. Improved traffic monitoring gives better efficiency in traffic

monitoring, adaptability for various network sizes, reduced retransmission and also helps in time saving.

This research work helps to find out an efficient method to detect attacks using dimensionality reduction techniques such as Principal Component Analysis, Linear Discriminant Analysis and Independent Component Analysis. The performance of the three techniques is compared with each other to find out the best technique. In future the real time traffic data can be used to study the capability of the techniques used in this research work and the accuracy level can be improved.

The next chapter deals with Enhanced moving target defense mechanisms to handle unknown attacks.