International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
http://ijcjournal.org/

Evaluating the Perfomance of the Modified Dynamic Hose Model for Virtual Private Networks

Egbonwonu E. L[a*], Onoh G. N[b], Okorogu V. N[c], Eze N.Christian[d]

[a,b,d]*Enugu State University of Science and Technology, Enugu State, Nigeria*
[c]*Nnamdi Azikiwe University, Awka, Anambra State, Nigeria*

Abstract

This paper is designed to model a Modified Dynamic Hose Algorithm for data traffic management. The Virtual Private Network (VPN) under study was characterized and the data for transmission was modeled. Then Algorithm for Modified Dynamic Hose Model to handle varying traffic rates was developed and simulated using MATLAB. The results obtained from network characterization shows that variation in window size and packet size affects the throughput in a VPN as an increase in window size from 50kb to 100kb improved the throughput generated from 15 for the Conventional Hose Model to 28.3 for the Modified Dynamic Hose Model resulting in 13.3 throughputs, which translate to 47% improvement. Also variation in window size and packet size affects the throughput in a VPN as an increase in window size from 10kb to 50kb resulted to a maximum throughput of 3.01 for the Conventional Model as against 15 for the Modified Dynamic Hose Model resulting to additional 11.99 or improvement of 79.93%. The Modified Dynamic Hose Model algorithm, unlike the Conventional Hose Model, determines whether to drop a particular packet or to queue it thereby improving the bandwidth utilization, minimize latency (delays) and Virtual Private Network Throughput.

Keywords: Dynamic Hose; VPN; Hose Model; Algorithm.

1. Introduction

Managing the performance of computer networks involves optimizing the way networks function in an effort to maximize capacity, minimize latency and offer high reliability regardless of bandwidth availability and occurrence of failures. Network performance management consists of tasks like measuring, modeling, planning and optimizing computer networks to ensure that they carry traffic with the speed, capacity and reliability that is expected by the applications using the network or required in a particular scenario [1]. The term QoS, in the field of networking, refers to control procedures that can provide a guaranteed level of performance to data flows in accordance to requests from an application/user using the network [2].

---

* Corresponding author.

Virtual Private Network services have been offered in various forms over a period of time and have recently received considerable attention within the Internet Protocol (IP), frame-relay, MPLS, and ATM networking communities [3]. VPNs are likely to be used by Customers as a replacement for Networks constructed using private lines and should therefore, at the very least, provide a comparable service. Substantial progress in the technologies for IP security enable us to improve on the security and privacy provided in existing VPN service offerings based on private lines or frame-relay. Other works on IP-based VPNs has mainly dealt with group membership, routing protocols and tunneling [3]. Much less attention has been paid to resource management issues related to VPNs. However, supporting a variety of mission-critical functions requires a VPN service to provide performance assurances, backed by Service Level Agreements (SLAs). Private lines isolate the performance seen by a VPN from other flows and provide guaranteed bandwidth, loss and delay characteristics. A VPN service must offer comparable performance assurances. This paper focused on the performance issues related to VPNs.

Due to the progress in security and the overwhelming success of IP networking technologies, the number of end points per VPN is growing, and communication patterns between end points are becoming increasingly difficult to forecast. We expect that users will be unwilling to, or simply unable to predict loads between pairs of endpoints. Similarly, it will become increasingly difficult to specify QoS requirements on a point-to-point basis, using the Conventional approach. The solution, which we call the Hose Model, serves as both a VPN service interface (that is, the way a customer thinks of a VPN) as well as a performance abstraction (that is, the way a provider thinks of a VPN). A Hose offers performance guarantees from a given endpoint to the set of all other endpoints in the VPN, and for the traffic to the given endpoint from the set of all other endpoints in the VPN. The Hose is the customer's interface into the Network, and is the equivalent of the Customer having a "link" into the Network. The Hose service interface allows the Customer to send traffic into the Network without the need to predict point-to-point loads. Though the Hose Model provides Customers simpler, more flexible SLAs, the Model appears to present the Provider with a more challenging problem in resource management. Under the Conventional point-to-point Model for specifying QoS, there is uncertainty about temporal variation in the traffic between the two points. Under the Hose Model, there is also spatial uncertainty; that is, uncertainty about traffic sinks. To cope with these uncertainties, we develop mechanisms that allow Providers to use the Hose Model to achieve significant multiplexing gains in the Network, by the use of signaling to dynamically size Hose and Network Capacity. A Hose is a service level assurance for a point to cloud VPN. This paper considers essentially the incapacitated design problem, that is, how much capacity is needed to support the Hoses. In particular, we wish to determine the cost incurred by the Provider in providing sufficient capacity to accommodate traffic whose matrix is not completely known. We evaluate the Proposed Hose VPN service Model by performing a number of trace driven experiments. In particular we show that significant multiplexing gains may be achieved for both the Customer and the Provider when the Network is capable of exploiting the Hose Model. Two sets of traces were used for these experiments. The first was voice traffic traces from the AT&T backbone Network. The second was data traffic traces from a large corporate backbone Network. The International Standard Organization (ISO) defines, clarifies and standardized the terms referring to Quality and defines it as the "the totality of features and characteristics of a product or service that bears its ability to satisfy stated or implied needs" [4]. Generally speaking, when we say 'quality', we think about the service from the

perspective of Users, comprising of an end-to-end view as show in Figure 1.

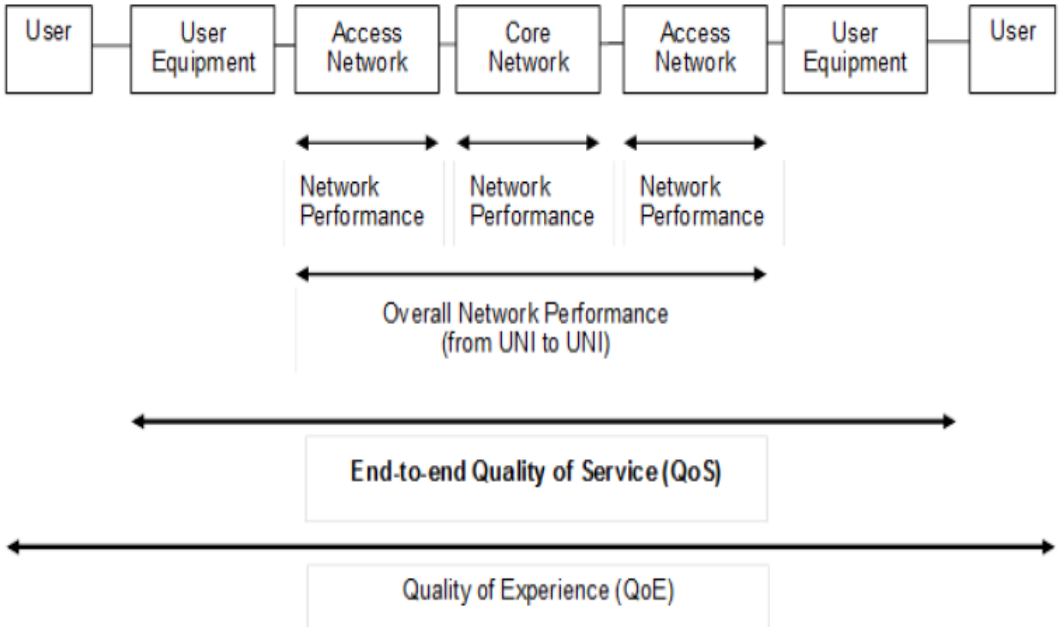

Figure 1: End-to-End Quality Experience [5].

However, this view includes a collective effect of individual performances, such as the network, the terminal and customer service process performance. Given the above, there are many notions and standards that should be clarified in this ecosystem that are both subjective (User perceptions) and objective parameters.

From the user's perspective, we refer to Quality of Experience (QoE), as a subjective dimension of the service. This view varies according to each user as influenced by the environment, the terminal and QoS [5].

At a different analysis level and through its recommendation G.1000, the International Telecommunications Union (ITU) explains that there are four different perspectives to analyze 'quality' [6], all the way from the perspective of the provider to the customer's. This is a comprehensive vision that helps conceptualize the two sides mentioned to QoS [7].

1. The quality standard that a customer claims to have experienced (perceived)

3. The quality standard that the service provider expects or declares to offer based on their network planning

4. The quality standard truly achieved and attained by the provider.

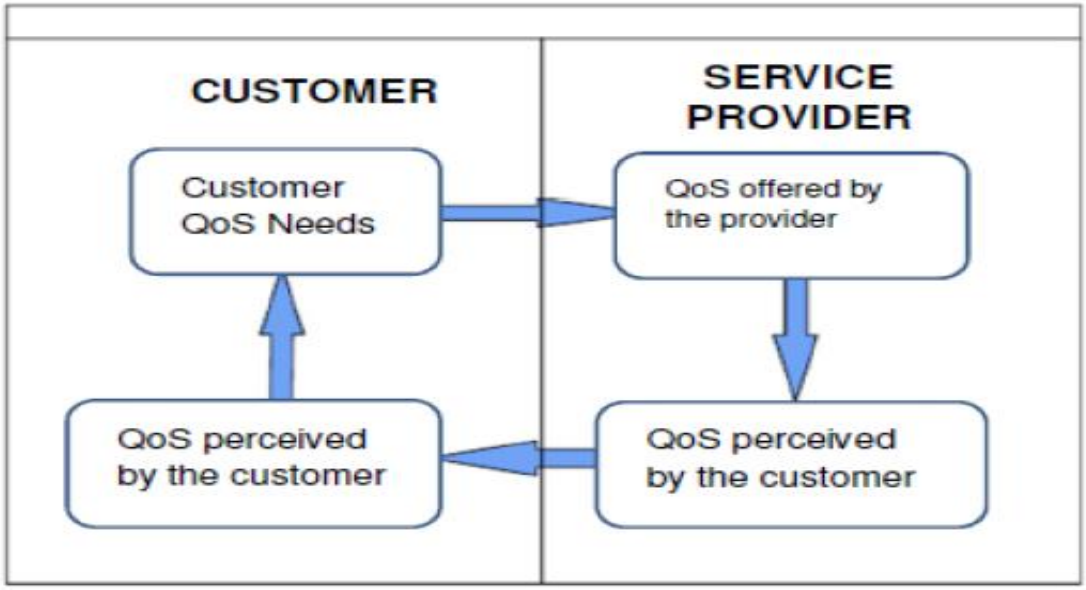

Figure 2: Four Perspectives on Quality as Defined by the ITU [7].

As we have already mentioned, an internet service provider (ISP) can only control the quality they expect to offer, which is determined based on design parameters and network features. Conversely, the quality standard achieved or attained is that which is assessed ex-post after a given period of time and depends on specific elements over which the ISP does not have full control, such as behavioral and climatic aspects. This vision of the ITU includes all aspects impacting the quality offered and attained by the provider while acknowledging the perceptions and needs of the customer [7]. Focusing on the provider, the objective dimension of QoS may be understood and analyzed at different layers: terminal equipment, access network, core network and processes. There is an intrinsic relationship between Quality of Service and quality of network performance—two notions which are sometimes confused. The Figure below shows the relationship between the two notions:

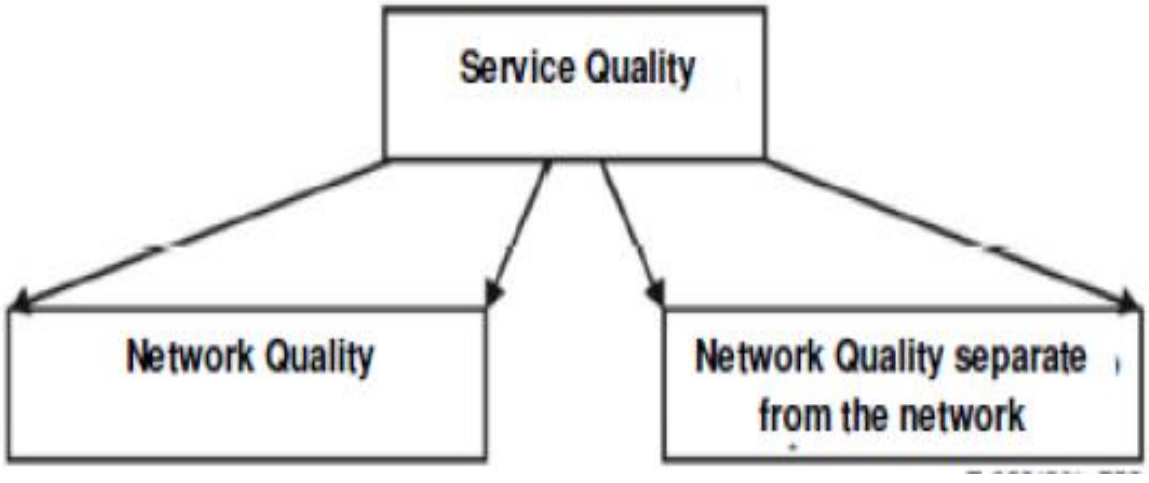

Figure 3: Relationship between Quality of Network Performance and Quality of Service [7].

The quality of network performance comprises technical parameters that are measured objectively and describe the performance of part of the network. These include: throughput rates, latency, variable delay, etc. On the other hand, network-independent factors comprise delivery time, processes and repair times among others. The relative weight these have on QoS depends on the nature of the service. Considering the above, this research work focuses on the quality of network performance that ISPs can manage (i.e. the quality they expect to offer on their network) which is determined mainly by elements that depend on the access and core networks.

2. A Practical Approach to VPN Resource Management using a Dynamic Hose Model

The Multi-commodity Flow Problem (MFP) solver was deployed to carry out bandwidth allocation [8]. In other to avoid producing bottleneck links in VPNs, they employed traffic predictor to ensure that any inaccuracy would cause the links not to have enough Capacity and violate the linear constraints on the commodities for each link is avoided. They proposed the L-PREDEC for Forecasting Virtual Network dynamic link usage, while employing a linear predictor. Traffic predictor adjusted the link with the largest occupation (bottleneck link) by periodically monitoring the traffic rate of a user link and adjusting the reserved bandwidth based on the forecasting made from traffic history. A scheme was proposed for enhancing VPN QoS using a method called "Log-infinitely Divisible Cascades" [9]. They proposed that the scheme would enable Several VPN traffic between two Provider Edge routers and of the tag stack using Multi-Protocol Label Switching (MPLS) VPN data also they allowed different transmission to share a LSP tunnel. The VPN multiplicity reduces the signaling load and the scale of forwarding table of routers to bring high system scalability. MPLS based load balancing was proposed for VoIP flows, it was implemented with an effective flow classification technique which prioritized the Voice packets based on their flow arrival rate and bandwidth utilization using probing techniques. They were differentiated as responsive, unresponsive and dataflow. Whenever the network experienced unbalanced load conditions due to link failure or system failure in the IP network, default routing policy would be overridden by multi-path routing policy. The data rates of unresponsive flow were estimated and marked based on their data rates using Rainbow Fair Queuing (RFQ) mechanism. In order to perform multipath dispersion and alleviate the problem of congestion, the core router looks for congestion free paths and reroutes the flows into best multiple paths that satisfies the given QoS requirements. Otherwise, it drops some of the low priority packets from those unresponsive flows Quality of Service (QoS) requirements of next generation IP-based backbone networks for managing multiple VPN was considered for services offered by a VPN Service Providers. In their paper, they proposed a programmable Tempest frame-work for Class of Service (CoS) Based Resource Allocation (CBRA) in MPLS tunneled VPNs. Switchlet based resource partitioning concept were used to create, build and provision multiple VPNs on demand. Furthermore, a distributed algorithm is proposed by using the primal decomposition method. The algorithm through the coordination of the global coordinating algorithm operate in the network while through the local adjusting algorithm operate in the individual virtual private networks.

3. Methodology

This research work is aimed at characterizing the VPN network and designing a model of a Modified Dynamic Hose Algorithm for data traffic management that will optimize the Data Throughput so as to enhance and

improve the Quality of Service (QoS) delivery in VPN Networks

3.1 Design Adopted

This research characterized Virtual Private Network and examined the resource management in the Network. During the Network characterization, a test bed was setup to monitor traffic and bandwidth utilization on the Network. The traffic generation and monitoring tools used was Iperf. The metric used in the experiment is Throughput (measured in Mbps). Also large files were used for testing workloads on all the VPN servers.

After the characterization of the VPN, a Model of Virtual Private Network was developed and simulated. The Modified Dynamic Hose Model was designed after Algorithm of the Modified Hose Model was developed

3.2 Develop Algorithm for Modified Dynamic Hose Model to Handle Varying Traffic Rates

The Virtual Network was represented by an undirected graph G (V, E), where V and E are the set of substrate Nodes and the set of physical links, respectively. It was assumed that k number of VPNs co-existed on the substrate Network. A set of k VPN was represented by a set of virtual links, denoted by

$$E^{(k)} = \left\{\left(s_1^{(k)}, t_1^{(k)}\right), \ldots, \left(s_{lk}^{(k)}, t_{lk}^{(k)}\right)\right\} \qquad 3.1$$

Where (s, t) is a virtual link connecting Node s and t, and l_k is the number of Virtual links of the k-th VPN.

Let $S^{(k)}$ denote the set of Nodes of the k-th VPN, By using the Hose Model constraints, all the Virtual Links connected to the Node i will have an upper bound bandwidth constraint of $\beta i^{(k)}$for the k-th VPN. Therefore the traffic demands of the k-th VPN from the link is dij $^{(k)}$

$$\sum_{\forall(i,i)\vee(i,j)\epsilon E^{(k)}} d_{il}^{(k)} \leq \beta_i^{(k)}, \qquad \forall i \in S^{(k)} \qquad 3.2$$

$$\beta_i^{(k)} = \mu \sum_{(i,j)\in E^{(k)}} \alpha_{ij}^{(k)} \qquad 3.3$$

Where $\alpha ij^{(k)}$ is the upper bound of the traffic demand of Virtual Links. And

μ can be adjusted from 0 to 1but was set as 0.8 for optimal performance.

If $cl^{(k)}$is the allocated bandwidth to link l

And $vl^{(k)}$is the link weight of a Node in the VPN.

The algorithm for the dynamic bandwidth allocation system is shown below

1. Given $c_l^{(k)}, \forall l \in E$ for each VPN
2. $v_l^{(k)} \leftarrow c_l^{(k)} - \theta_i \cdot \lambda_i^{(k)}$;
3. Send $v_l^{(k)}, \forall l \in E$, to the global coordinating algorithm;
4. Wait for receiving $c_l^{(k)}$, from the coordinating algorithm;
5. Receive $v_l^{(k)} \forall l \in E$, from each VPN
6. Solve min $\left\{\sum_k (c_l^{(k)} - v_l^{(k)})^2 : \sum_k (c_l^{(k)} \leq c_l\right\}, \forall l \in E$
7. For $^{\forall k, sendbandwidth c_i^{(k)}, \ \forall l \in E, tothek-thVPN}$

The bandwidth allocated to each VPN is guaranteed by rate limiting of other VPN connections, this algorithm allows busy VPN traffic to take more bandwidth beyond its guaranteed bandwidth by "borrowing" the underutilized bandwidth from idle VPNs, thus better bandwidth utilization can be achieved. Such extra bandwidth, that is, bandwidth allocated beyond the guaranteed bandwidth, would be fairly allocated among Virtual Ports or VPN connections from different tenants with the weight proportional to the guaranteed bandwidth they purchased. Although the algorithm was designed for both traffic transmitted from the sites into the Network and for traffic received from the Network, only the algorithm for transmitted traffic was used for this work. The work was modeled to satisfy Pareto Efficiency, that is; when there is enough free bandwidth, any machine sharing the bandwidth could be able to use it by exceeding its own SLA.

$$\sum_{i \in hostk} t_{ij} \geq B \Rightarrow \sum_{i \in hostk} b_{ij} = \eta B \qquad 3.4$$

Where $\eta$is the overall bandwidth utilization and B is total bandwidth of the link

$$\forall i, j \sum_{j \neq i} t_{ij} \geq A_i^t \Rightarrow \sum_{j \neq i} b_{ij} \geq A_i^t \qquad 3.5$$

$$\sum_{i \in hostk}^{n} A_i^t \leq B_k \qquad 3.6$$

$$\forall i \sum_{j \neq i} G_{ij} \leq A_i^t \qquad 3.7$$

Ti represents the traffic sending request of VPN i, based on the Model above,

$$T_i = \sum_{j \neq i} b_{ij} \qquad 3.8$$

3.2.1 Modified Dynamic Hose Model on Virtual Private Network to Enhance Resource Management Using MATLAB/SIMULINK

MATLAB program and SIMULINK model were developed and used for the simulation analysis of resource management in virtual private network were carried out using Modified Dynamic Hose Model to handle varying

traffic rates. The monitoring technique will use dynamic host model system to detect congestion on the VPN.

In the simulation, data Packets are generated by the input box. Each data has attributes representing the Packet size. The data Packets are then transmitted on the data Network. Figure 3.4 is the MATLAB/SIMULINK Model for Resource Management in Virtual Private Network. It mainly consists of traffic source modules, Node access control module, ingress committed rate, Dynamic Hose Model, resource assignment, Network sink, logic module (if else), parameter input box, display box and scope.

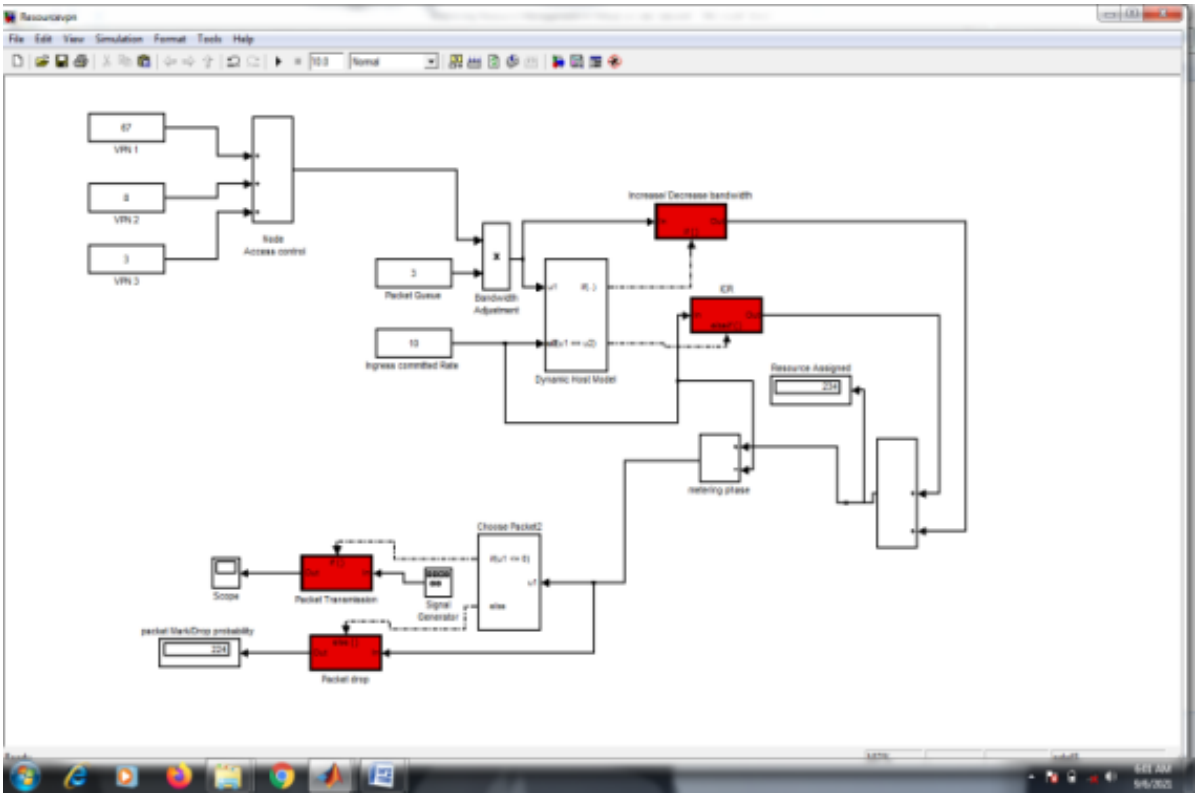

Figure 4: MATLAB Model of Modified Dynamic Hose Model on Virtual Private Network.

3.1 Design Adopted

This research examined and evaluated the resource management in the Network. During the Network characterization, a test bed was setup to monitor traffic and bandwidth utilization on the Network. The traffic generation and monitoring tools used was Iperf. The metric used in the experiment is Throughput (measured in Mbps). Also large files were used for testing workloads on all the VPN servers.

After the characterization of the VPN, a Model of Virtual Private Network was developed and simulated. The Modified Dynamic Hose Model was designed after Algorithm of the Modified Hose Model was developed.

3.2 Fieldwork Experimental Measurement

Bandwidth utilization was measured and the experimental tool used to verify bandwidth utilization is net-box

software (Net-box) which **is** simply a software used by MTN (Service Provider) in Nigeria to monitor customer performance, and data usage on the network. The procedure used in carrying out the experiment when appropriate Password was logged is as follows:

VLAN : 1061

IP : 197.210.185.26

GATEWAY: 197.210.185.25

JITTER & BANDWIDTH OF CLIENT ⇒ 20Mb/s

Customer details retrieved were test- run. After the test was run there was a graphical display on the screen or monitor of the Laptop. The nature or the characteristics of the graph shows data performance as in Figure 5.

Figure 5: Graph showing over Utilization of Bandwidth.

From the nature of the Graph; at some points in the Graph below 20mbps, the Graph was smooth and this shows that the network congestion level is still within tolerable limit as Subscriber have not started over stressing the network by exceeding the allocated bandwidth. When the data indicator goes beyond 20Mbps, the network becomes overstretched and congestion sets in if the excess bandwidth is not shed or redistributed to other VPN networks that need more bandwidth

4.3 Simulation Results

4.3.1 Network Characterization Result

In the network characterization, we have used large files for testing workloads as all the VPN servers used have moderately high bandwidths around 20Mbps therefore file sizes of at least 15MB were used to allow the network activity to settle and collect more realistic data. The following two tables show the Throughput analysis done on each of Client VPN servers individually.

Table 1: Simulation Parameters.

Parameter	Value
Protocols	UDP
Number of VPN	3
Data rate	10 Mb, 50 Mb, 100 Mb
Packet Size	512kb Bytes, 1024 Bytes, 2048 Bytes
Simulation Time	13s
Traffic Pattern	CBR, FTP
Ingress committed rate	10

Table 2: Throughput Testing VPN servers 1.

Number of Users	Throughput (KB/sec)	Per User (KB/sec)	Bandwidth utilization
1	3638.19	3638.19	16.12
2	5769.92	2884.96	25.57
4	12042.24	3010.56	53.36
8	19288.32	2411.04	85.48
10	20722.33	2072.23	91.83
12	22564.14	1880.34	100
16	22355.36	1397.21	99.07

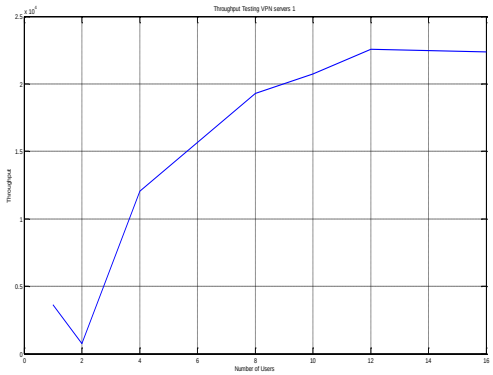

Figure 6: Number of Users versus Throughput Testing VPN servers 1.

Figure 6 shows that the Throughput increases with an increase in the number of Users showing that more Packets are transmitted and delivered on the Network.

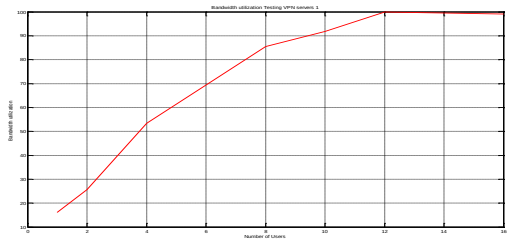

Figure 7: Number of Users versus Bandwidth Utilization Testing VPN servers 1.

Figure 7 shows that the bandwidth allocated to each User keeps degrading as the number of Users keeps increasing. But we notice that a maximum bandwidth is approached around 12 Users per Client. Another observation made here is that the bandwidth utilization increases as we load the Client with more number of Users. This is a drawback in the files system because it should be aiming to maximize bandwidth utilization at all possible times.

Table 3: Throughput Testing VPN servers 2.

Number of Users	Throughput (KB/sec)	Per User (KB/sec)	Bandwidth utilization
1	3723.05	3723.05	14.72
2	5739.89	2869.945	22.70
4	13883.89	3470.97	54.92
8	24454.57	3056.82	96.74
10	23722.33	2372.23	93.84
12	25278.57	2106.54	100
16	22355.36	1397.21	88.43

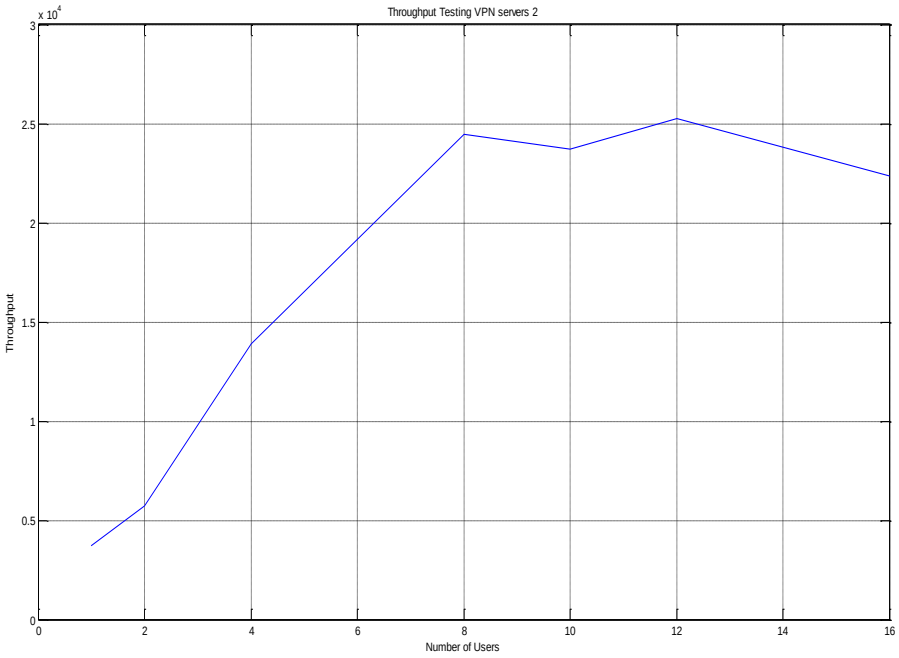

Figure 8: Number of Users versus Throughput Testing VPN servers 2.

Figure 8 shows that the Throughput increases with an increase in the number of Users showing that more Packets are transmitted and delivered on the Network. This shows that VPN server 1 and VPN server 2 has similar characteristics in terms of Throughput and it is equally applicable to any VPN Network.

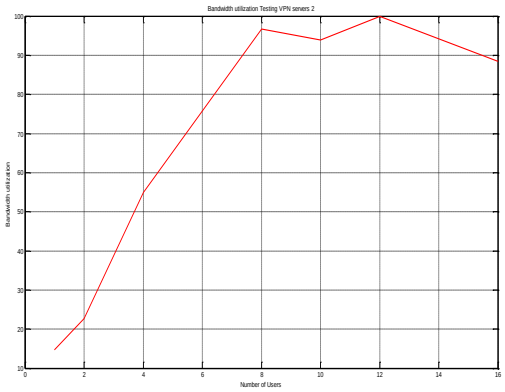

Figure 9: Number of Users versus Bandwidth Utilization Testing VPN servers 2.

Figure 9 shows that the bandwidth allocated to each User keeps degrading as the number of Users keeps increasing. But we notice that a maximum bandwidth is approached around 12 Users per Client. Another observation made here is that the bandwidth utilization increases as we load the Client with more number of Users. This is a drawback in the files system because it should be aiming to maximize bandwidth utilization at all possible times. This also shows that VPN server 1 and VPN server 2 has similar characteristics in terms of Bandwidth Utilization and it is equally applicable to any VPN network.

Various tests are alternately run using different aspects of Transfer rates and Packet size. With CBR sitting on UDP protocol, the simulation results are presented in Table 4,

Table 4: CBR Throughput for different Packet sizes at the CBR transfer rate: 10 Mb, 100 Mb and 1000 Mb.

Time	**Packet size: 512 Bytes**	**Packet size: 1024 Bytes**	**Packet size: 2048 Bytes**
2	0	0	0
2.5	0.008	0.016	0.033
3	0.008	0.016	0.033
3.5	0.008	0.016	0.033
4	0.008	0.016	0.033
4.5	0.008	0.016	0.033
5	0.008	0.016	0.033
5.5	0.008	0.016	0.033
6	0.008	0.016	0.033
6.5	0.008	0.016	0.033
7	0.008	0.016	0.033

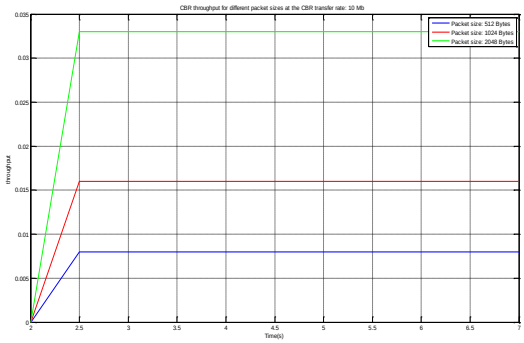

Figure 10: Time versus CBR Throughput fordifferent Packet sizes at the CBR Transfer rate: 10 Mb, 100 Mb, and 1000 Mb.

From the characterization of VPN Throughput, it uses two parameters which are Packet size and Transfer rate. It is seen from Figure 10 that Packet size affects the VPN Throughput. As the three Transfer rates provide same Throughput; it follows that Transfer rate does not affect the Throughput in a VPN.

Tests are run using different aspects of Window sizes and Packet sizes with FTP using TCP protocol, the experimental results are presented in Table 5, Table 6 and Table 7.

Table 5: FTP Throughput with FTP Window size: 10 Kb.

Time	Packet size: 512 Bytes	Packet size: 1024 Bytes	Packet size: 2048 Bytes
8	0	0	0
8.5	0.48	0.92	1.8
9	0.79	1.53	3.01
9.5	0.71	1.36	2.67
10	0.71	1.36	2.67
10.5	0.79	1.36	2.67
11	0.71	1.53	3.01
11.5	0.71	1.36	2.67
12	0.79	1.36	2.67
12.5	0.71	1.53	2.67
13	0.71	1.36	3.01

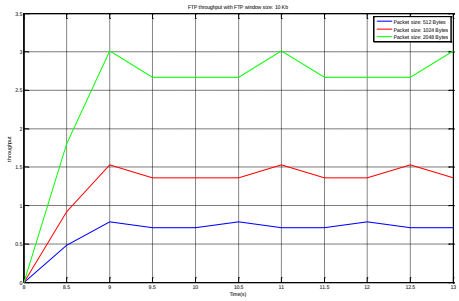

Figure 11: Time versus FTP throughput with FTP window size: 10 Kb.

Figure 11 showed that the window size is used to trigger results in turns with 512 Bytes, 1024 Bytes and 2048 Bytes Packet sizes. This shows that variation in Window size and Packet size affects the Throughput in a VPN.

Table 6: FTP Throughput with FTP window size: 50 Kb.

Time	Packet size: 512 Bytes	Packet size: 1024 Bytes	Packet size: 2048 Bytes
8	0	0	0
8.5	1.43	2.76	5.41
9	3.97	7.66	13.73
9.5	3.53	6.81	14.67
10	3.53	6.81	13.36
10.5	3.97	6.81	13.36
11	3.53	7.66	14.37
11.5	3.53	6.81	14.03
12	3.65	6.81	13.36
12.5	3.85	7.66	13.36
13	3.53	6.81	15

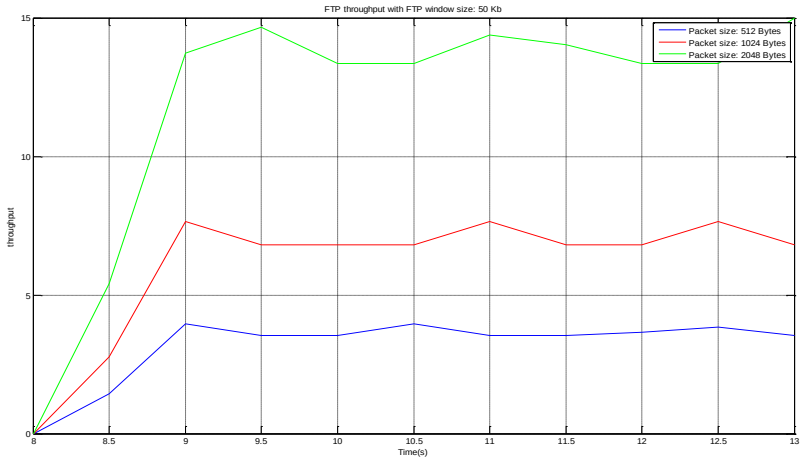

Figure 12: Time versus FTP Throughput with FTP Window size: 50 Kb.

Figure 12 showed that the window size is used to trigger results in turns with 512 Bytes, 1024 Bytes and 2048 Bytes Packet sizes. This shows that variation in Window size and Packet size affects the Throughput in a VPN as an increase in Window size from 10kb to 50kb improved the Throughput generated. Here the maximum Throughput generated was 15 as against 3.01obtain when Window size: 10 Kb was used. The improvement obtained here is 11.99 or 79.93%.

Table 7: FTP Throughput with FTP Window size: 100 Kb.

Time	Packet size: 512 Bytes	Packet size: 1024 Bytes	Packet size: 2048 Bytes
8	0	0	0
8.5	1.997	3.85	7.55
9	7.95	14.78	27.09
9.5	7.07	14.16	29.7
10	7.07	13.62	26.73
10.5	7.9	13.62	26.73
11	7.11	15.32	27.73
11.5	7.07	13.62	29.06
12	7.19	13.62	26.73
12.5	7.83	15.32	26.73
13	7.07	13.62	28.3

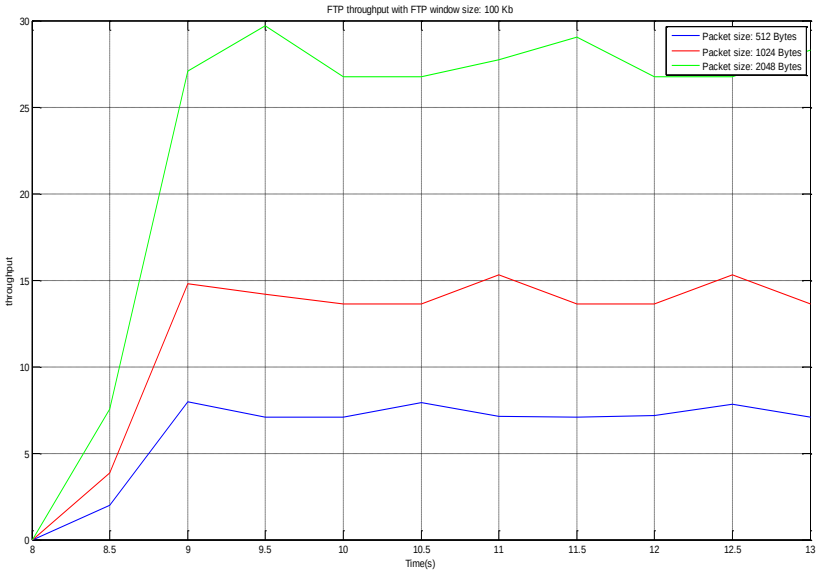

Figure 13: Time versus FTP Throughput with FTP Window size: 100 Kb.

Figure 13 showed that the Window size is used to trigger results in turns with 512 Bytes, 1024 Bytes and 2048 Bytes Packet sizes. This shows that variation in Window size and Packet size affects the Throughput in a VPN as an increase in Window size from 50kb to 100kb improved the Throughput generated. Here the maximum Throughput generated was 28.3 as against 15 obtain when Window size: 50 Kb was used. The improvement obtained here is 13.3 or 47%.

Table 8: Simulated Data of Mark/Drop probability with different values of Congestion Window using Hose Model Algorithm.

Traffic congestion window	mark/drop probability
2	2.4448
4	1.5758
8	0.8717
16	0.4512
32	0.2283
64	0.1147
128	0.0575

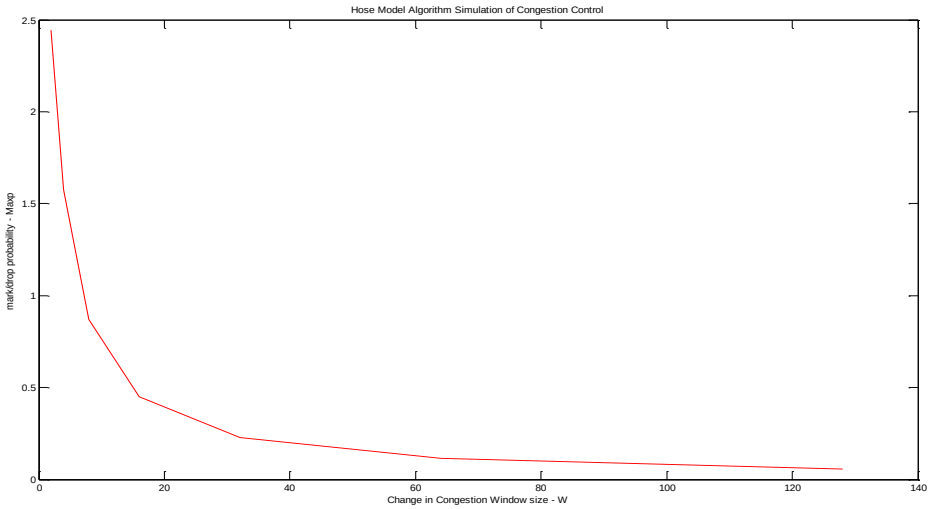

Figure 14: Variations in mark/drop probability *with* different values of Congestion window *W* Packets, for Hose Model Algorithm.

A simulation of Variations in Mark/Drop probability *with* different values of congestion window *W*, Packets, for Hose Model Algorithm as shown in Figure 14 shows that the variations in Mark/Drop probability with different window size W, has a dropping characteristics, which shows that an increase in the window size will reduce Mark/Drop probability as represented in Figure 14

Table 9: Simulated Data of Mark/Drop probability with different values of Congestion Window using Modified Dynamic Hose Model.

Traffic congestion window	mark/drop probability
2	1.6284
4	1.0495
8	0.5806
16	0.3005
32	0.1521
64	0.0764
128	0.0383

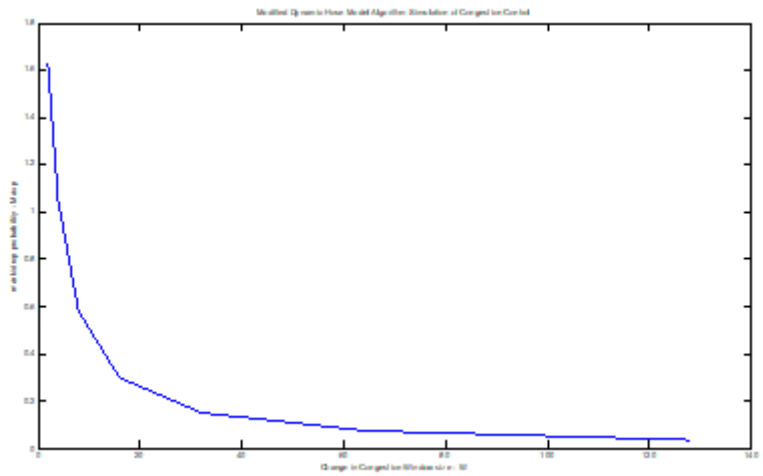

Figure 15: Variations in Mark/Drop probability *with* different values of Congestion window *W*, Packets for Modified Dynamic Hose Model.

A Simulation of Variations in Mark/Drop probability *with* different values of Congestion Window *W*, Packets for Modified Dynamic Hose Model as shown in Figure 15 shows that the variations in Mark/Drop probability with different window size W has a dropping characteristics, which shows that an increase in the window size will reduce Mark/Drop probability but was improved due to differentiated Service. Modified Dynamic Hose Model achieves scalability through performing complex QoS functions such as Classification, Marking, and Conditioning operations using the DiffServ into a limited number of traffic aggregates or classes only at the Edge Nodes. In the Core Routers, Scheduling and Queuing Control Mechanisms are applied to the traffic classes based on the field marking: all traffic conditioning and dropping is intelligently handled at the Network Layer using IPDiffServ QoS mechanisms. A simulation of Variations in Mark/Drop probability *with* different values of Congestion Window W, Packets for Hose Model and Modified Dynamic Hose Model Algorithm shows that the variations in Mark/Drop probability with different window size W, has a more dropping characteristics for Hose Model Algorithm than Modified Dynamic Hose Model Algorithm. So in-profile and out-of-profile Packets will have different drop preference. The Modified Dynamic Hose Model Algorithm then determines whether to drop a particular Packet or to queue it. All the Packets that are not dropped no matter whether they are in or out-of-profile are put into the same queue to avoid out of order delivery.

4.3.2 Packet Delivery Ratio

Table 10: Comparison of Sent (ICR) and Received (ECR) Packets for Existing and Proposed Models.

Number of Packet Sent	**Number of Packet Received With Existing Model**	**Number of Packets Received with Proposed Model**
50	36 (0.72%)	46 (0.92%)

The Table.10 represents the Packets delivery ratio which is calculated as the total number of Packet received

successfully at the final destination and total number of Packets sent.

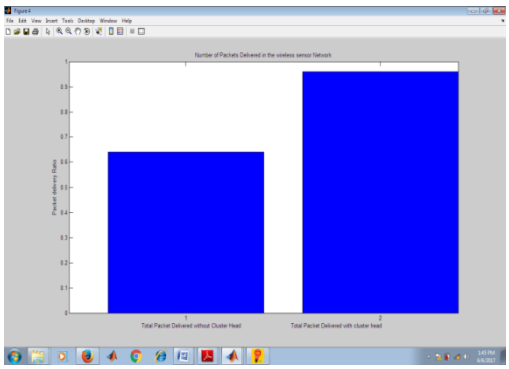

Figure 16: Comparison for Packets delivery Ratio for Existing Pipe Hose and the Proposed Modified Dynamic Hose Technique.

Figure 16 showed the variation in the Packets delivery ratio of the Existing and Proposed Techniques and Comparison of both in terms of Packets delivery performance. The Modified Dynamic Hose Model posted 92% Packet delivery ratio as against the Existing Model that posted 72% Packet delivery ratio.

5. Conclusion

In this paper Simulations were carried out on the Modified Dynamic Hose Model for improving Resource Management in Virtual Private Network. The needed Parameters were sent to MATLAB Workspace from where the results of the generated parameters were obtained for each Simulation time used. Figure 6 and 8 show that the Throughput increases with an increase in the number of Users and that more Packets are transmitted and delivered on the Network. This shows that VPN servers 1 and VPN server 2 haves similar Characteristics in terms of Throughput and it is equally applicable to any VPN Network. Figures 7 and 9 shows that the Bandwidth allocated to each User keeps degrading as the number of Users keep increasing. But we notice that a maximum bandwidth is approached around 12 Users per Client. Another observation made is that the bandwidth utilization increases as we load the Client with more number of Users. This is a drawback in the files System because it should aim to maximize bandwidth utilization at all possible times. This also shows that VPN servers 1 and VPN servers 2 have similar characteristics in terms of Bandwidth Utilization and it is equally applicable to any VPN Network. Various tests are alternately run using different aspects of Transfer Rates and Packet size. With CBR sitting on User Data Protocol (UDP), the simulation results are presented in Table 4. From the characterization of VPN Throughput, it uses two parameters which are Packet size and Transfer rate. It can be seen from Figure 10 that Packet size affects the VPN Throughput and the three Transfer rates provide same Throughput. So Transfer rate does not affect the Throughput in a VPN. Tests are run using different aspects of Window sizes and Packet sizes with FTP using TCP Protocol. The experimental results are presented in Table 5, Table 6 and Table 7. Figure 12 showed that the Window size is used to trigger results in turns with 512 Bytes, 1024 Bytes and 2048 Bytes Packet sizes. This shows that variation in Window size and Packet size affects the Throughput in a VPN as an increase in Window size from 10kb to 50kb improved the Throughput generated. Here the maximum Throughput generated was 15 as against 3.01 obtain when Window size: 10 Kb was used

(Figure 11). The improvement obtained here is 79.93%. Figure 13 showed that the Window size is used to trigger results in turns with 512 Bytes, 1024 Bytes and 2048 Bytes Packet sizes. This shows that variation in Window size and Packet size affects the Throughput in a VPN as an increase in Window size from 50kb to 100kb improved the Throughput generated. Here the maximum Throughput generated was 28.3 as against 15 obtain when Window size: 50 Kb was used (Figure 12). The improvement obtained here is 13.3 or 47%.

The Simulation results as presented in Tables 8 and 9 and Figures 14 and 15 shows the Variations in Mark/Drop probability *with* different values of Congestion Window for Hose Model Algorithm and Dynamic Hose Model as applied to Model Resource Management and Quality of Service Control in VPN using Modified Dynamic Hose Model to provide efficient data rate Throughput in the Network operation, handling varying Traffic rates, and to improve the Mark/Drop probability with different values of Congestion Window. A Simulation of Variations in Mark/Drop probability *with* different values of Congestion Window W, Packets for Hose Model and Modified Dynamic Hose Model Algorithm shows that the variations in Mark/Drop probability with different Window size W, has a more dropping characteristics for Hose Model Algorithm than Modified Dynamic Hose Model Algorithm as shown in Figure 15. So in-profile and out-of-profile Packets will have different Drop preference. The Modified Dynamic Hose Model Algorithm then determines whether to drop a particular Packet or to queue it. All the Packets that are not dropped no matter whether they are in or out-of-profile are put into the same queue to avoid out of order delivery.

Figure 16: Comparison for Packets delivery Ratio for Existing Pipe Hose and the Proposed Modified Dynamic Hose Technique showed the variation in the Packets delivery ratio of the Existing and Proposed Techniques and Comparison of both in terms of Packets delivery performance. The Modified Dynamic Hose Model posted 92% Packet delivery ratio as against the Existing Model that posted 72% Packet delivery ratio.

References

[1] Nigeria Communication Commission – NCC; Retrieved June 12, 2021 from http://www,ncc.gov.ng/index.php

[2] W. C. Y. Lee, ”Mobile communication Engineering”, McGraw-Hill Inc; 1982

[3] Fotedar, S., Gerla, M., Crocetti,P. and Fratta,L. (2015) “ATM Virtual Private Networks,” *Communications of the ACM*, vol. 38, pp. 101–109, Feb 2015

[4] ISO/IEC JTC 1/SC 29/WG 11, “Information technology – coding of audio-visual objects, part 1: systems, part 2: visual, part 3: audio,” *FCD 14496*

[5] Paxson.V. (2017) End-to-End Internet Packet Dynamics. In *Proc. of ACM* SIGCOM*M*, September 2017.

[6] Report ITU-R M.2244 (2011), “ Standards in Isolation between Antennas of IMT Base Station in the Land Mobile Service”, November, 2011

[7] Guerin,R. and Peris, V. (2010) Quality-of-service in packet networks: basic mechanisms and directions, *C*omputer Networks and ISDN, vol. 31, No. 3, pp, 169–179, Feb. 2010

[8] Christian, M., Dotaro, E. and Papadimitriou, D. (2016) A Practical Approach to VPN Resource Management using a Dynamic Hose Model. 2016 2nd Conference on Next Generation Internet Design and Engineering, Valencia, 3-5 April 2016, 147-153.

[9] Lim, L.K., Gao, J., Ng, T.S.E., Chandra, P.R., Steenkiste, P. and Zhang, H.(2017) Customizable Virtual Private Network Service with QoS. Computer Networks, 36, 137- 151