Enhancing the Computer Network Security in Data Centre Networks using QoS Metrics

[1]Ohaneme, L.C., [2]Ibiejugba, M.A, and [3]Adejo, B.O.

[1]Department of Computer Science, Federal Polytechnic, Oko Anambra State
[2, 3] Department of Mathematical sciences, kogi State University, Anyigba kogi State

Abstract:- The ever increasing demand for computer based data transfer has made it necessary that computer network users' demand for optimal transfer of information from their desired customers. The most worried aspect of these demands is that most times unauthorized users tend to tamper with the transmitted data within the network. However, the importance of network security in computer network centre cannot be over emphasized in recent times. This work therefore deals with enhancing the computer network security and deployed a measure to checkmate the ever increasing hacking or attacking of data in the network thereby rendering the security system of the computer network to be vulnerable and inefficient. The Quality of Service (QoS) used in the work include, throughput, data delay and utilization factor. Here, the real-time system survey technique is deployed to actualise the analysis of the computer network. The result obtained shows that the deployment of the models developed enhanced security for Data Centre Networks (DCN).

Keywords: *QoS, network security, data centre network,*

*****

1.0 Introduction

Network security has become more important to personal computer users, organizations, and the military. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does things as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. With the advent of the data centre networks vis-a-vis internet, security has become a major concern for the enterprise market segments. The internet structure itself allows for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attacking methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an intranet to remain connected to the internet but secured from possible threats [1].

There are currently two fundamental different networks viz: data networks and synchronous network comprising of switches. However, the internet itself is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as trojan horses, planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet [1]. When developing a secured network, the following need to be considered [2]:

- Access Control– Authorized users are provided with the means to communicate to and from a particular network
- Confidentiality– Information in the network remains private
- Authentication – Ensure the users of the network are who they say they are
- Integrity – Ensure the message has not been modified in transit
- Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, are taken in this research.

To lessen the vulnerability of the computer to the network there are many products available as discussed by [1]. The tools used in tackling security are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Networks running businesses throughout the world are using a combination of some of these tools to combat network security vulnerabilities. In most cases, Intranets are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network when closely observed. Understanding the security issues of the data centre and internet design greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

Besides, the types of attacks through the data centre and internet need to also be studied to be able to detect and guard against them. Intrusion detection systems (IDS) are established based on the types of attacks most commonly used on these networks. Essentially, network intrusions consist of packets that are introduced into these networks to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks.

The last reason for a network security is to guard against intrusion motives.

Typical security currently exists on the computers connected to the network for the enterprise market segments. In existing works, security protocols sometimes usually appear as part of a single layer of the Open System Interconnection (OSI) network reference model. The use of traditional passwords has its drawbacks with respect to authentication in data centre networks, etc, [3] viz:

- User password difficult to memorize.
- User cannot freely choose is password
- User cannot change his password
- It cannot withstand forgery attack

2.0 Review of Related Literatures

2.1 Network Security: History, Importance, and Future

According to [1], system and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. In essence, there exists a communication gap between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interconnect (OSI) model. The OSI model has several advantages when designing networks [4]. The Open Systems Interconnect (OSI) model was developed in 1981 by the International Standards Organization (ISO).

The OSI model comprises seven functional layers, which provide the basis for communication among computers over networks. The seven layers of the OSI model, from highest to lowest, are Application, Presentation, Session, Transport, Network, Data Link, and Physical layers [4].see Figure 2.1. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed in a network design by making other adjustments, and allowing flexibility in development. There could be various methodologies to manage the complexity of security requirements. Secured network design does not contain the same advantages as network design.

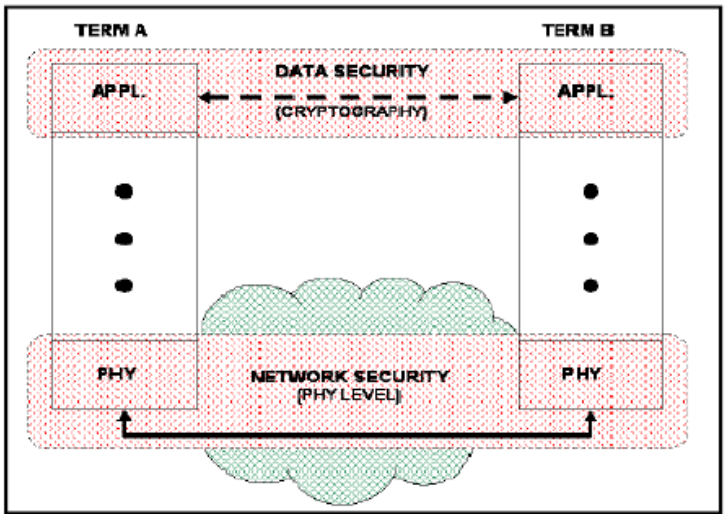

Figure 2.1: OSI model data security and network security functions [5].

When considering network security, it must be emphasized that the whole network needs to be secured. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data, the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

Recent interest in security was fuelled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in United State (US) history [6]. The losses were eighty million dollars in US intellectual property and

source code from a variety of companies [6]. Since then, information security came into the spotlight. Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies nowadays emphasizing the security for the intellectual property. Internet has been a driving force for data security improvement. Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secured.

Conversely, data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Though, strong cryptography in the past can be easily broken today, cryptographic methods have to continue to advance due to the advancement of the hackers as well. When transferring cipher text over a network, it is helpful to have a secured network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secured network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks [5]. The relationship of network security and data security to the OSI model is shown in Figure 2.1. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. The user can possibly choose different methods of data security.
Network security is mostly contained within the physical layer. Layers above the physical layer is also used to accomplish the network security required [5]. Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent counter measure strategies [5].

2.2 Data Centre Computer Networks

According to [6] a data centre is a server farm or a computer room where majority of enterprise servers and storage systems (such as Enterprise Resource Planning solutions (ERPs), Application servers, E-commerce servers, Security systems (IDS)) are located, operated and managed. It is also referred to as the consolidation point for provisioning multiple services that drive enterprise business processes. For example, financial institutions like banks, educational institutions like universities, Internet Service Providers (ISPs), internet-based organizations such as Google, twitter, face book etc, and oil and gas industries, all have data centres where their data are stored, operated and managed. Some of them have and manage their own data centres while others outsource to bigger data centres due to high cost of owning, managing and maintaining a data centre networks [6].

The design of data centre network has been a very interesting area and many research groups have proposed several architectures for computer data centre network. This section reviewed some selected architectures viz: Fat-tree, Monsoon, BCube, MDCube, VL2, DCell, and Synthesis VLAN architectures as discussed in [7].

3.0 System Models and Analysis

Considering computer networks, DCN_1..... DCN_N for parallel broadcast links as shown in figure 3.1, the total indexed throughput Model for channel i in the proposed DCN is given as :

$$S = T_o \sum_{i=1}^{M} S_i / T_i \tag{1}$$

where,

T_o = time needed to transmit a packet on a Parallel broadcast channel in proposed DCN

M = Parallel Broadcast Channels in the in the proposed DCN

i = $\overline{1, N}$

T_i = time needed to transmit a packet on an i broadcast channel in the proposed DCN

$$S_i = \lambda T_o \tag{2}$$

where,

λ = packet/s according to Poisson process

For a DCN with non-persistent channel path, the throughput is given as:

 ISSN: 2321-8169
3737 - 3745

$$S = S_i = \frac{G_i e^{-aG_i/M}}{\left(1+G_i\left(1-\frac{a_o}{M}-\frac{\sigma}{MT_o}\right)\right)e^{-aG_i/M}+G_i\left(3\frac{a_o}{M}+\frac{\sigma}{MT_o}\right)} \quad (3)$$

where,

G_i = Offered traffic in the *ith* channel

M = Numbers of parallel link channels

σ = Length of jammed time after collision

a_o = Normalized propagation delay

T_o = time needed to transmit a packet on a single broadcast channel with bandwidth W_i

If $G_i = G$, then the throughput of a random choice Carrier Sense Multiple Access with Collision Detection CSMA-CD-RC is given by

$$S = S_i = \frac{Ge^{-aG/M}}{\left(1+G\left(1-\frac{a_o}{M}-\frac{\sigma}{MT_o}\right)\right)e^{-aG/M}+G\left(3\frac{a_o}{M}+\frac{\sigma}{MT_o}\right)} \quad (4)$$

Now, $D_o = \left(\frac{G}{S}P_{ii}-1\right)\left(M+X_o+\tau_o+2a_o\right)+\left(\frac{G}{S}P_{ii}-1\right)X_o+M+a_o$ (5)

Where,

D_o = Average Packet Delay Normalized to T_o

G = offered traffic in the ith channel

S = Throughput

P_{ii} = The probability that a station senses the chosen channel idle

M = Numbers of Parallel link Channels

X_o = Average transmission delay normalized to T_o

τ_o = Acknowledgement time normalized to T_o

a_o = Normalized Propagation Delay

The architectural model of the indexed throughput is presented in figure 3.1 which serves the proposed DCN in this work

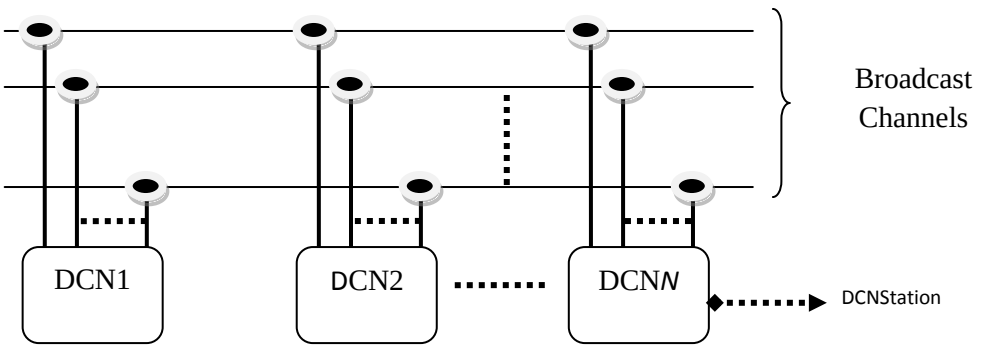

Figure 3.1: Indexed Throughput Architectural Model

3.1 Queuing Model

A continuous time CSMA/CD (carrier sense multiple access with collision detection) system with a finite number of homogeneous Stations, each possessing an infinite buffer was considered in [8], [9], [10], and [11] respectively. The system was decomposed and approximately treats each station as an independent *M/G/*1 queuing system. With this analysis, the mean message delay can be numerically obtained. Conclusively, the stability of the system becomes more sensitive to the retransmission interval as the number of stations increases. The M/G/1 queuing system model is adopted to perform this task and consequently, the expression is illustrated thus:

$$\frac{1}{\gamma} \leq \frac{1}{\lambda} - (T + D) \tag{6}$$

where,

γ = exponential distribution parameter

λ = Poisson process parameter

T + D = service time

The Laplace-Stieltjes transform (LST) of service time distribution function

$$G_1^*(S) = b_1 \exp[-S(T + D)] + (1 - b1)\, G^*(s) \tag{7}$$

where,

b_1 = the probability that a station senses the channel idle and succeeds in transmission

T = transmission time of a message

D = maximum propagation delay

The probability generating function of the stationary queue length distribution at arbitrary constant is given as:

$$L(z) = P_0 \frac{zG_1^*(\lambda - \lambda z) - G_2^*(\lambda - \lambda z)}{z - G_2^*(\lambda - \lambda z)} \tag{8}$$

where,

P_o = probability of no client in the system at arrival instant

Hence,

$$R = L / \lambda \tag{9}$$

where,

R = mean response time

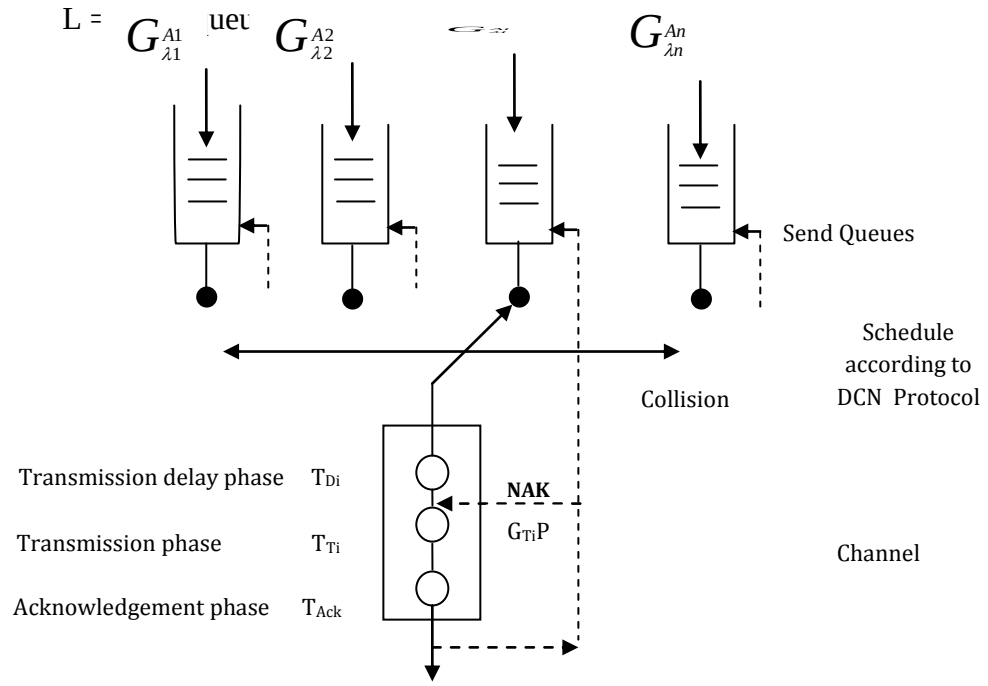

Figure 3.2: Queuing Model of a Computer Network

From figure 3.2, let ***N*** = number of connected network access stations, G_A = general arrival process, G_T= general transmission process, ***λ*** = arrival rate, and ***i*** = index of station number

 ISSN: 2321-8169
3737 - 3745

Hence, Service time per transmission in the model is given as:

$$T = T_T + T_D(X) + T_{ACK} \quad \text{(J)}$$

where, T_T = transmission time, $T_D(X)$ = random transmission delay, T_{ACK} = acknowledgement time.

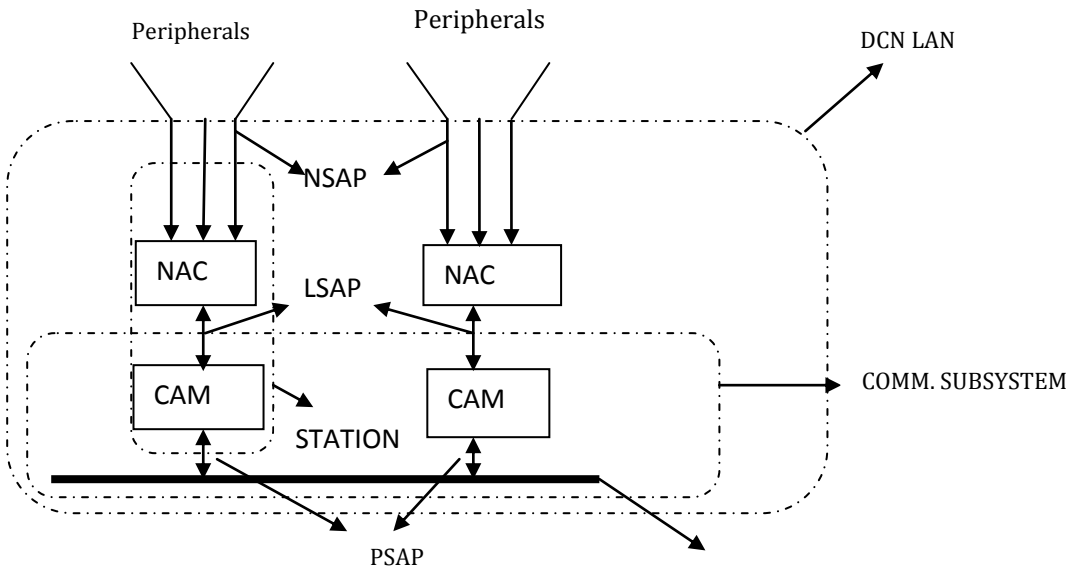

Figure 3.3: Architecture Model of a DCN Server

' represents
Network Service Access Point, ***L-SAP*** represent Link Service Access Point, and ***P-SAP*** represents Physical Service Access Point.

3.2 Maximum Throughput and Maximum Delay Equations

In [11], a novel media access protocol CSMA/CD with deterministic contention resolution (DCR) for a local area network was reported and an analytical comparison with the conventional CSMA/CD network and implicit token passing such as express net LAN was considered. This work concluded that the efficiency of DCN will be derived from the throughput of express net LAN and its robustness from CSMA/CD in Ethernet. By modifying the maximum throughput for figure 3.4 maximum throughput and delay models will be realized. Basically, the Maximum Throughput is generally given as:

$$S = \frac{(\text{Number of successful transmissions})*(\text{Message length})}{(\text{Total transmission time}} \quad (10)$$

$$S_{MAX} = \frac{P}{(P+F)} \quad (11)$$

where, P = time length of a message, F = time length for an interface time fill.
Hence, for express net DCN, the maximum throughput is given as:

$$S_{MAX} = \frac{N*P}{2D+(r+P)+(N-1)*(F+r+P)} \quad (12)$$

where,

N = number of stations

P = time length of message

D = end-to-end propagation delay

$2D$ =period after collision detection

r = reservation signal time length

F = reservation signal time length

 ISSN: 2321-8169
3737 - 3745

Let the Maximum Delay Equation for DCN be given as:

$$MD_{MAX} = (2D + J + F) + (N-2)*(2t + F + r + P) + (2D + F + r) + (2D + J + F) + P + (N-1)*(2t + F + r + p) \quad \text{(N)}$$

where,

D = end-to-end propagation delay

$2D$ =period after collision detection

J = period of jams

F = inter message time fill length

r = reservation signal time length

P = time length of message

t = station-to-station propagation delay time

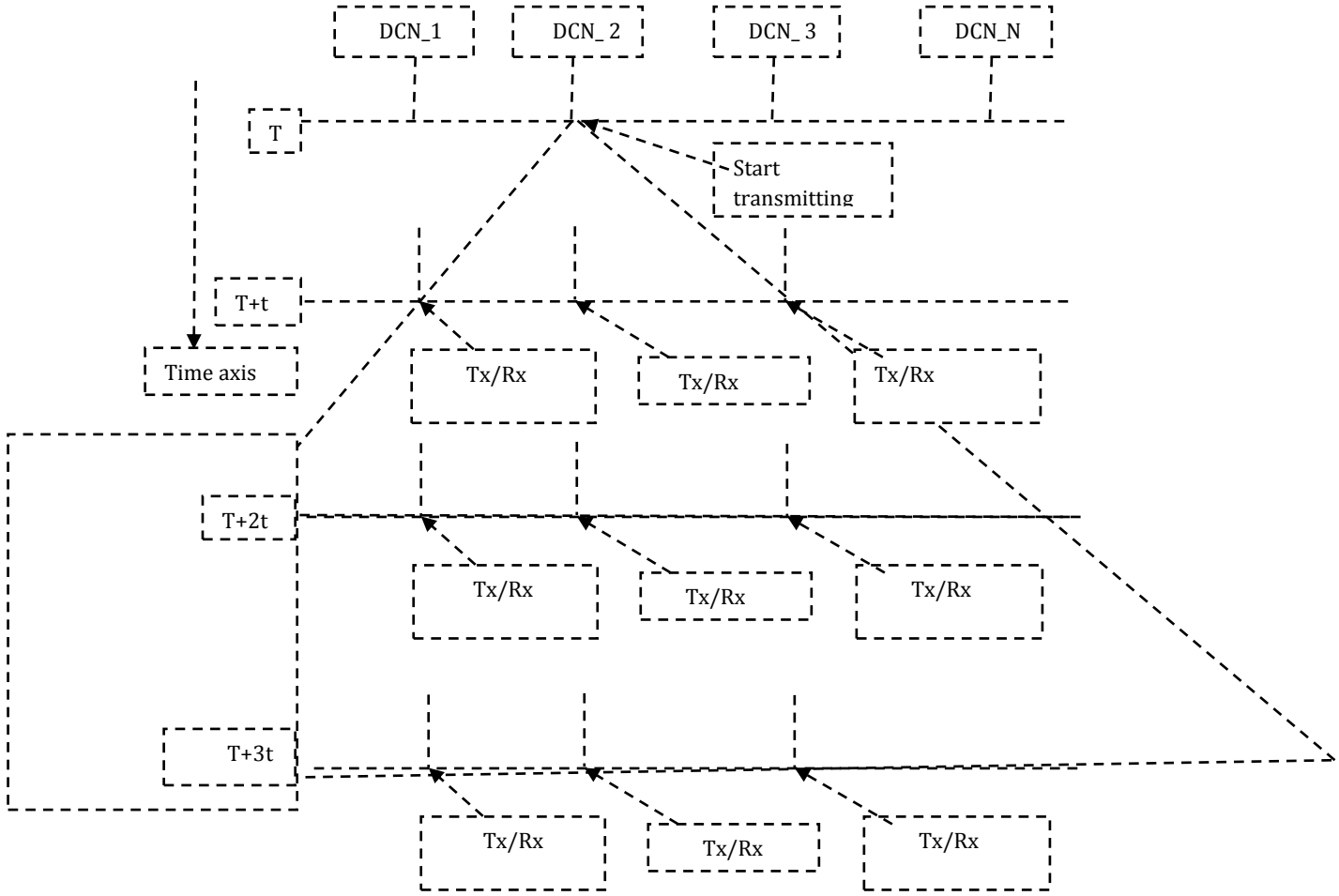

Figure 3.4: Multiple DCN full duplex models

4.0 Results Presentation and Analysis

The simulation of a computer network scenario for QoS studies is carried out with a WLAN network. It was run accordingly and the statistics were collected and displayed on a graph. Results of the system are discussed below. In this work, an evaluation on computer network Hotspot variant is carried out in this section considering their security integrations in the sites for the mobile nodes representing the end users.

(a)Throughput QoS Response

Figure 3.1 shows a secured steady-state throughput response achieved from the scenario computer network environment. The security VLAN algorithm facilitates a better response compared with throughput degradation under hybrid security policy with

 ISSN: 2321-8169
3737 - 3745

time and throughput degradation under dual security policy with time e.t.c, under realistic loads. Interestingly, it was observed that the proposed security algorithm had slightly better throughput behaviour of about 3500 packet/bits compared with TCP plots in throughput degradation under hybrid security policy with time and throughput degradation under dual security policy with time etc. The implication is that transmission of realistic traffic will witness a reliable packet data delivery with active connections transmitting data between the mobile nodes and the backend servers. With an emulated round trip time equal to 100 ms (a near zero packet loss rates), the measures of packet sizes greater than 1200 bytes in the real scenario is validated by the results obtained by simulation and provide a further support on the advantages of proposed VLAN computer network.

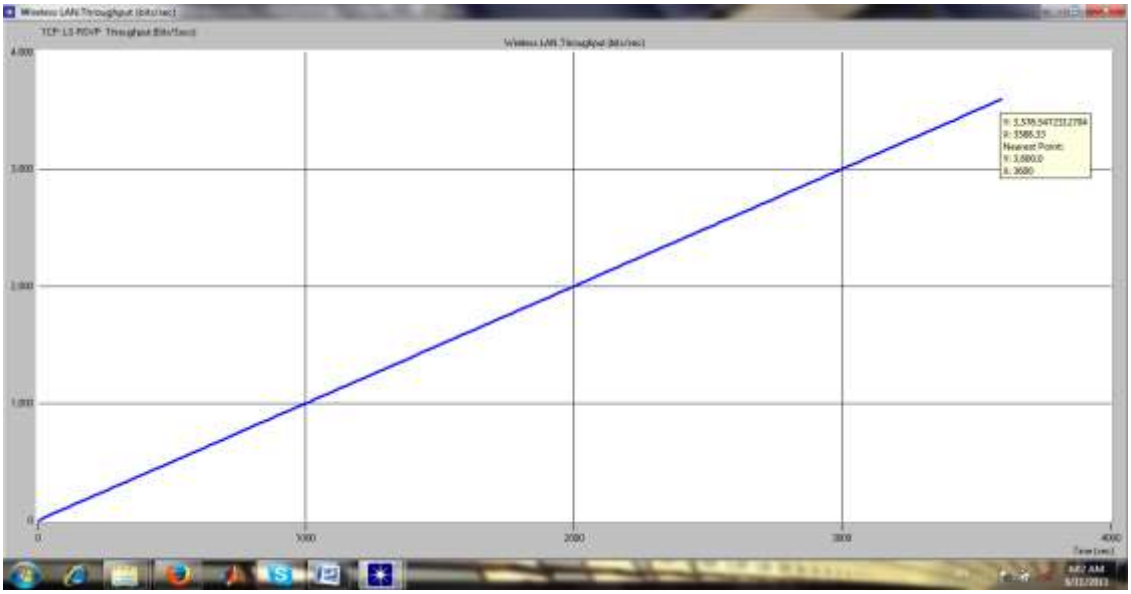

Figure 3.1: Secured Computer Network throughput (VLAN Throughput Plot)

(b) Delay QoS Response

Figure 3.2 shows the latency Plot of computer network with VLAN under realistic load. The proposed TCP/IP variant maintains fast rise latency throughout the transitions as depicted by the trend curve beginning from 0.005s up to 0.04s for the WLAN realistic load scenario. Essentially, the proposed computer network shows a comparative latency response of generic TCP. It maintained a steady rate of about 0.004s relative to generic TCP. Both plots show a similar trend but with Hotspot_VLAN, a lower latency of less than 0.005secs was observed.

Figure 3.2: Computer Network Delay Plot

5.0 Conclusion

The importance of computer network security in recent times cannot be over emphasized as all efforts have been gearing towards protecting transmitted data from imbue and illicit interference. So many data on transit had been tampered with by unauthorized persons for one reason or the other. Maximum security in computer networks is also paramount in all sectors of human endeavours.

Therefore the need arises that maximum protection be given to transmitted data so that high throughput is obtained afterwards.

References

[1] Bhavya Daya, "Network Security: History, Importance, and Future", http://web.mit.edu/~bdaya/www/Network%20Security.pdf.
[2] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, Vol.31, No.9, pp.24-28, Sep 1998.
[3] Behrouz A. Forouzan, and Sophia Chung Fegan "Data Communications and Networking" 4th Edition McGraw-Hill of the Americas, New York
[4] Eric Cole, Ronald Krutz, and James W. Conley "Network Security Bible, Wiley Publishing, Inc. Indianapolis, Indian, 2005
[5] Kartalopoulos, S. V.,"Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference Proceedings, 19-23, May 2008,pp 1469-1473
[6] Udeze Chidiebele. Chinwendu, " Re-Engineering Data Center Networks For Efficient Web Application Integration in Enterprise Organizations" PhD Dissertation Dept of ECE NAU 2013.
[7] Udeze C.C, Okafor K.C, Onwusuru I.M, An Evaluation Of Legacy 3-Tier Data Center Networks for Enterprise Computing Using Mathematical Induction Algorithm, Computing, Information Systems, Development Informatics & Allied Research,Vol. 4 No. 4 Dec. 2013.
[8] Whitner, R.B.an d Balci, O.(1989). "Guidelines for Selecting and Using Simulation Model Verification Techniques," Proceedings of the 1989 Winter Simulation Conference, pp.559- 568, Washington, DC, December 4-6.
[9] IEEE 802-2001, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture" 7 February 2002, pg. 2&3.
[10] Wikhard M. Kiesel, Paul J. Kuehn, 'A New CSMA-CD Protocol for Local Area Networks with Dynamic Priorities and Low Collision Probability' IEEE Journal on Selected Areas in Communications, Vol. SAC-1, No.5, November 1983, p 869-876.
[11] Akihiro Takagi, Shinichi Yamada, Shohei Sugawara, 'CSMA/CD with Deterministic Contention Resolution' IEEE Journal on Selected Areas in Communications, Vol. SAC 1, No 5, November, 1983,pp 877-884.