SIMULATION OF IEEE 802.11b INTRANET FOR CAMPUS BASED VOTING USING OPNET

Nathan David, Elizabeth OkaforNjideka, Fortune OkerekeOnyekachi, Augustine OforChikwado
Department of Electronic Engineering, University of Nigeria

Abstract— With the increased adoption of electronic voting in several campuses in Nigeria, greater emphasis has been placed on the voting GUI's and security devices (such as biometric scanners) as opposed to the network structure. However, establishing connectivity to a network which is both secure and ensures very high quality of service is inarguably of major importance to the voting exercise. This paper proposes an intranet solution based on IEEE 802.11b WLAN structure to improve on the dysfunctional network structure within the campuses. It also presents some tests for a performance evaluation of the proposed solution. The 802.11b intranet is simulated using OPNET Modeler 14.5 Educational Version and tested against real life conditions made available by the simulation tool.

Index Terms— *WLAN, OPNET, electronic voting, intranet*

1.0 INTRODUCTION

Voting is the expression of our commitment to ourselves, associations, this country and this world.Since manual voting systems have been primarily characterized with high incidences of electoral malpractices and irregularities, [1] electronic voting has quickly gained popularity amongst masses.

Elections allow the populace to choose their representatives and express their preferences for how they would be governed [2]. Electronic voting (simply referred to as e-voting) is a method of casting votes electronically over a network. E-voting is usually characterized by high level of security and ease of access.

Internet technology has continued to revolutionize our global community. It has positively affected every facet of human endeavour ranging from the way we live to how we carry out our activities and communicate [3].

To successfully conduct an election of this nature, with respect to ensuring a very high integrity of votes, careful attention must be paid to ensuring a secure, stable and reliable network is created. The challenge therein lies in the ability to implement a secure network upon which data will be transmitted and communicated effectively to the concerned parties in real-time regardless of their locations.

E-voting can be handled primarily in two ways – internet voting and intranet voting, the latter being the preferred option due to its high level of security. The term *Intranet Voting* is used to describe an electoral process that will enable voters to cast a secure and secret ballot over a computer network within an organization [4]. For this work, an additional wireless feature to enhance flexibility and mobility is also included. The WLAN (IEEE 802.11b) allows users to connect to the LAN wirelessly via radio transmission without additional or intrusive wiring of a wired network [5].In spite of the convenience of mobility, the performance of the Wireless Local Area Networks remains of great importance prior to its adoption as intrinsic part of an enterprise network.

1.1 OBJECTIVE

This paper borders on verifying the various network performance parameters with respect to the actual overall network performance of IEEE 802.11b intranet based Wireless LAN through controlled simulations and tests using OPNET.

The remainder of this paper is organized as follows:

- Section II discusses background information on IEEE 802.11b WLAN (intranet – put/remove).
- Section III describesthe simulation setup and methodology for our work.
- Finally,results are outlined and future work is described in Section IV.

2.0 CASE STUDY:

For the scope of this work, we have designed an intranet for faculty elections in six faculties within the University of Nigeria, Nsukka campus to span across 16 kilometre square area.

In the Nsukka campus, the bulk of the buildings occupy the western half of the site leaving the gently sloping valley, lying between the northeast and southern hills relatively free of buildings [6].

Nevertheless, the 802.11b WLAN intranet can be scaled to cover much larger projects.

3.0 SIMULATION ENVIRONMENT AND EXPERIMENTS SETUP

In this work, we used the OPNET Modeler 14.5 educational version. OPNET provides a wide-ranging development environment for modelling and routine evaluation of communication networks and distributed systems [7]. It is a network simulation software which can be used to build various network configurations and test their performance with simple drag-and-drop actions and a few clicks of a mouse [8]. It provides a simple and user friendly graphical user interface and is well suited for network simulation novices.

A network is constructed by graphically connecting network nodes via communications links [9]. OPNET comes with a huge model library, including application traffic models (e.g., HTTP, FTP, E-mail, Database) and protocol models (e.g. TCP/IP, IEEE 802.11b, Ethernet) that simulate most of the existing hardware devices and cutting-edge communication protocols. It also contains a broad set of distributions for random variable generation (e.g., exponential, Erlang, lognormal, Weibull, Pareto). Among other features, one has the ability to vary the node's data rate, the RTS threshold, the fragmentation threshold and the packet reception threshold (i.e. the receiver's sensitivity). OPNET provides a geographical scale feature which enables us to model networks on a variety of scales (world network, entreprise network, campus network, office network, logical network or even any specific area of interest on the map). This was suitable for us to effectively design a campus network.

3.1 WLAN CONFIGURATION

To setup the WLAN, all the nodes within a particular subnet were grouped into a single Basic Service Set (BSS) and assigned a unique Basic Service Set Identifier (BSS ID) which ranged from 1-6 for the six subnets. An example is shown in figure 1. All the nodes with the same basic service set ID can communicate with each other and the access point(AP) functionality for the routers were auto-enabled. However, the AP functionality for all other nodes within the same BSS were disabled, because each BSS can have at most one AP.

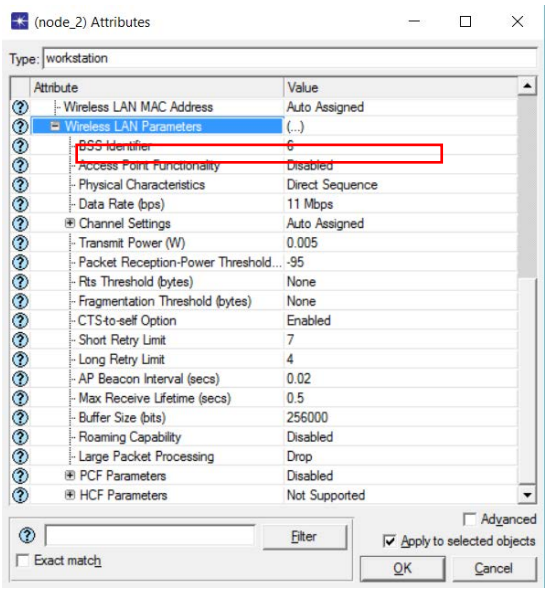


Fig. 1: Basic Service Set Configuration

3.1.1 THE PHYSICAL LAYER

We deployed the 802.11b physical layer standard with a data transmission rate 11Mbps and applied this setting across all the nodes in the network as shown in figure 2.

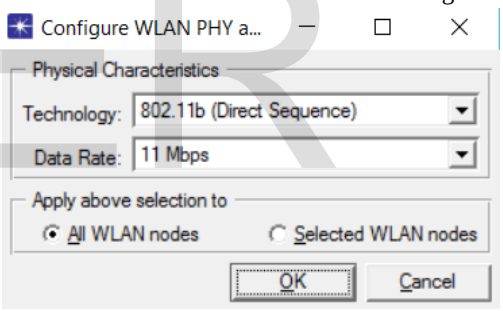


Fig. 2. Physical Characteristics Configuration

4.0 OBJECT UTILITIES CONFIGURATION

4.0.1 PROFILE CONFIGURATION

In order to define the network users' needs and also add background traffic to the network we set up an e-voting profile within which we defined heavy file transfer and heavy database access applications for the profile users. This is shown in figure 3 below:

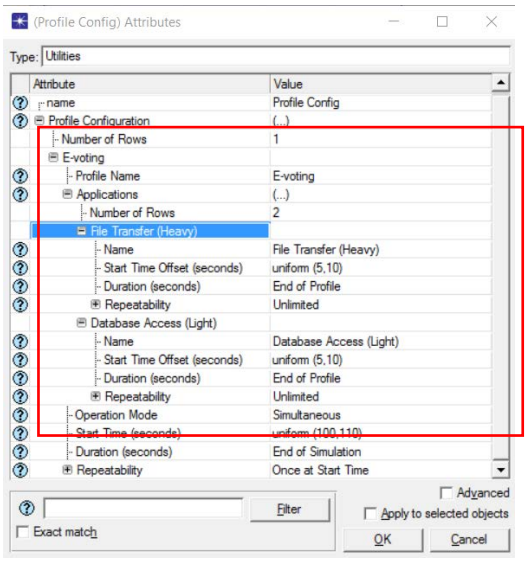


Fig. 3: Profile Configuration

The applications will run simultaneously from 5-10 seconds after the user profile has started up till the end of the profile. The start time for the user profile was set to 100-110 seconds after the network has started up to create room for the start of other nodes (the servers, switches and routers) in the network. The profile was set to run till the end of the simulation.

4.0.2 Application Configuration

To increase the flexibility of the user profile, the application profile was set to default as seen in the figure 4 below.

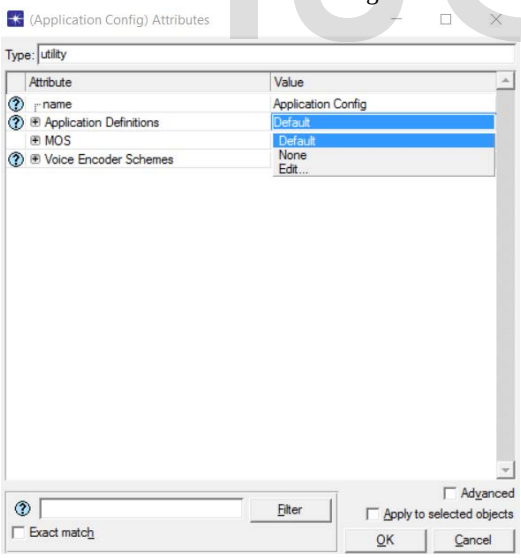


Figure 4: Application Configuration

The application and profile configuration settings were finally deployed on the nodes and set to be supported on the server.

5.0 Results and Analysis

Following the configurations, we ran the simulation for a period of 24hours to obtain the global statistics for the evaluation of the WLAN performance. We also conducted a flow analysis test and survivability test.

We set the result presentation tostacked statistics and time average mode for easy understandability.

5.0.1 Global Statistics

Ethernet Delay:

The ethernet delay obtained for the network remained fairly constant at 0.18 milliseconds over the 24hour period.

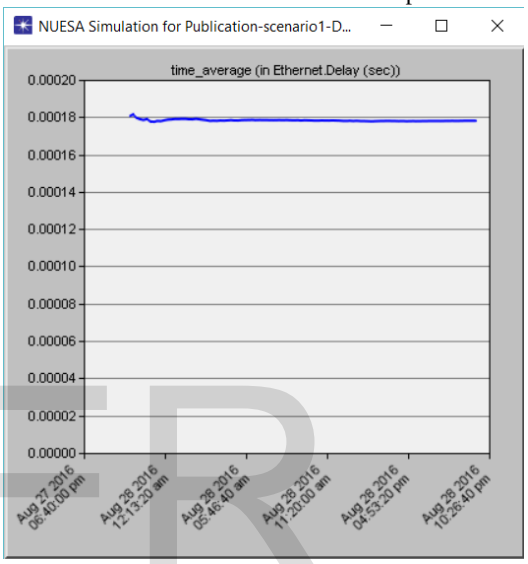


Fig. 5. Ethernet Delay

WLAN Delay:

The end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer was 5.8 milliseconds(ms). This delay includes medium access delay at the source MAC, reception of all the fragments individually, and transfer of the frames via AP.

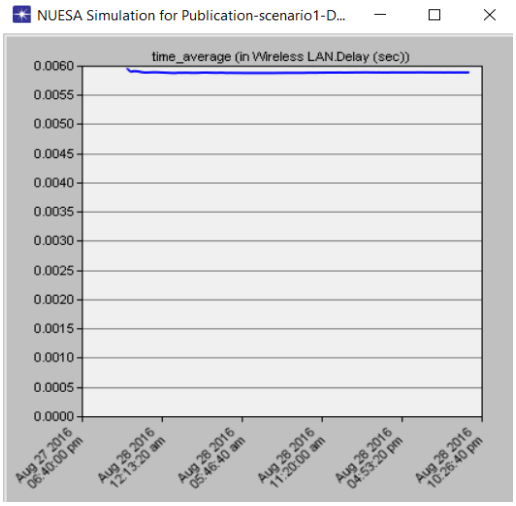


Fig. 6. WLAN Delay

WLAN Load:

The WLAN could send an initial load of 101Kbps to the WLAN layers. However, there was a sharp drop in the load for a period of 80minutes after which it became fairly constant, sending a load of 70Kbps to the wireless LAN layers.

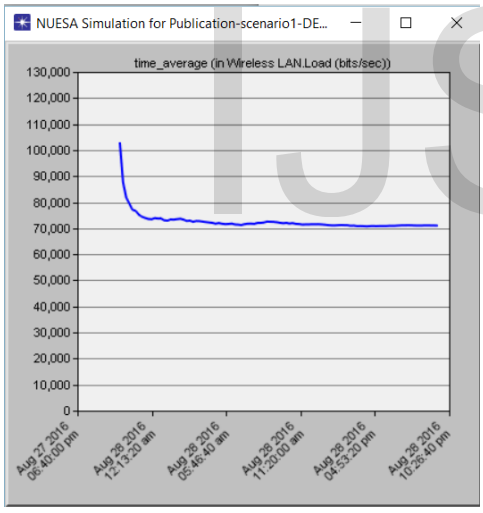


Fig.7. WLAN Load

WLAN Throughput

Similarly, like the WLAN load, we obtained a throughput of 70Kbps. This represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network as shown in figure 4.3 below.

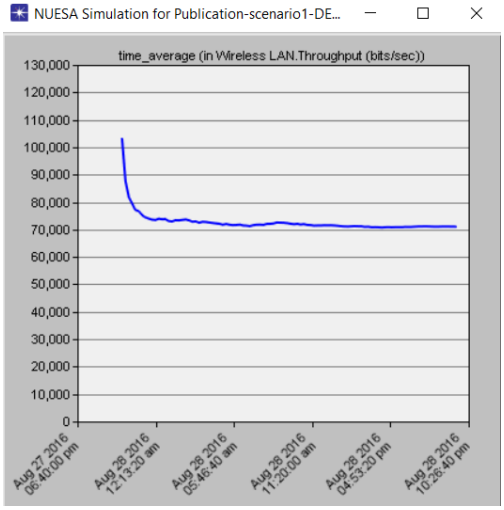


Fig. 8. WLAN Throughput

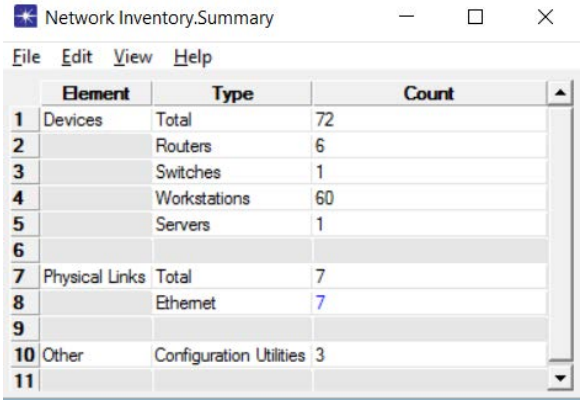
5.0.2 Simulation Setup

To setup the intranet, 6 faculties within the campus were represented as subnets. Each subnet contained one router and ten 802.11b aware workstations giving a total of 60 workstations and 6 routers within the network.

The routers were connected to an advanced ethernet16 switch which supports up to 16 Ethernet interfaces of 100Mbps. The switch also implements the Spanning Tree algorithm in order to ensure a loop free network topology within our network. Finally, the switch was linked to a central ethernet server running TCP/IP and UDP/IP protocols, set to operate in full duplex. Interconnectivity within the network was achieved using 100BaseT duplex links operating at a data rate of 100Mbps.

The application definition and profile definition utilities were also included. The user profile is a mechanism for specifying how standard and custom applications will be used by an end user during a simulation [10].

The network inventory summary is shown in fig. 9 below.



	Element	Type	Count
1	Devices	Total	72
2		Routers	6
3		Switches	1
4		Workstations	60
5		Servers	1
6			
7	Physical Links	Total	7
8		Ethernet	7
9			
10	Other	Configuration Utilities	3
11			

Fig. 9 Network Inventory

Figure 10 shows an overview of the entire network and figure 11 highlights a cross-sectional view of a subnet within the network.

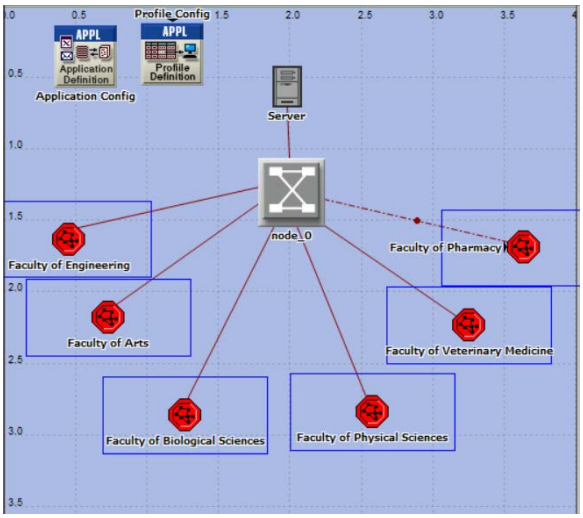


Fig. 10 Overview of the 802.11b Intranet Structure.

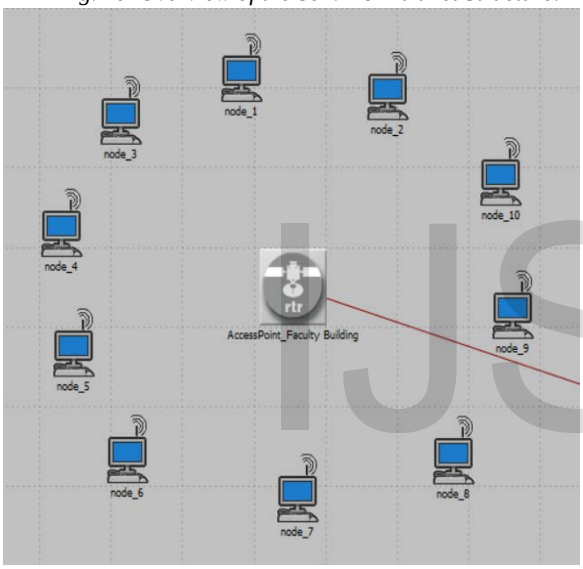


Fig. 11. Cross-Sectional View of a Subnet within the Network

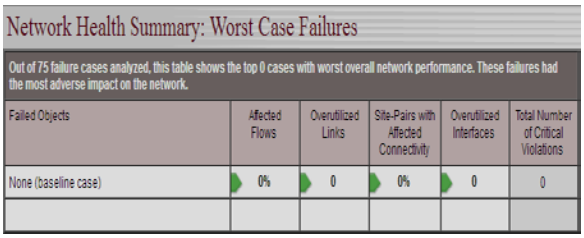
5.1 Survivability Analysis Report

After the network was subject to high traffic and load applications, we conducted a survivability analysis based on 75 failure test cases which obtained an overall network survivability score of 145 out of 180. This score provides an overall measure of the network's abilityto recover from failures. It is the percentage of investigated failure cases which did not result in critical violations of any of the performance metrics.

A score of 145 on the 180 scale indicates that the network is very resilient.

5.1.1 Network Health Summary

Out of the 75 failure cases analyzed, no case was reported with bad overall network performance as seen in fig 4.4a. There was also a zero impact on the performance metrics as shown in figure 4.4b indicating a healthy network.



Network Health Summary: Worst Case Failures

Out of 75 failure cases analyzed, this table shows the top 0 cases with worst overall network performance. These failures had the most adverse impact on the network.

Failed Objects	Affected Flows	Overutilized Links	Site-Pairs with Affected Connectivity	Overutilized Interfaces	Total Number of Critical Violations
None (baseline case)	0%	0	0%	0	0

Fig. 12a Network Health Summary- Worst Case Failures

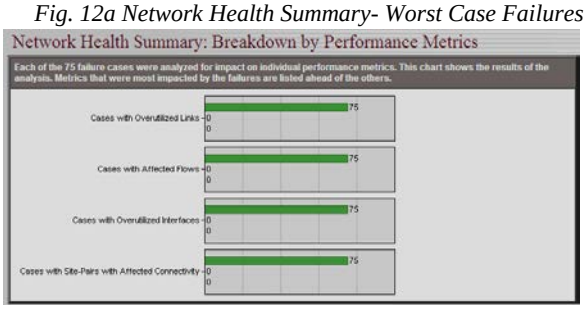
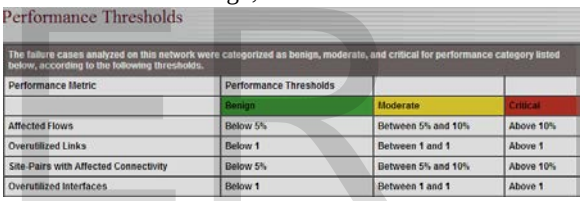


Fig. 12b.Network Health Summary- Breakdown by Performance Metrics

5.1.2 Network Performance Details

From the OPNET analysis report generated, figure 13a below shows the Performance References to determine if the network is in Benign, Moderate or Critical State.



Performance Thresholds

The failure cases analyzed on this network were categorized as benign, moderate, and critical for performance category listed below, according to the following thresholds.

Performance Metric	Performance Thresholds		
	Benign	Moderate	Critical
Affected Flows	Below 5%	Between 5% and 10%	Above 10%
Overutilized Links	Below 1	Between 1 and 1	Above 1
Site-Pairs with Affected Connectivity	Below 5%	Between 5% and 10%	Above 10%
Overutilized Interfaces	Below 1	Between 1 and 1	Above 1

Fig. 13a Performance References

In analyzing the affected flows, and site pairs with affected connectivity in the network, the graph report showed that the tested 75 failure cases lay in the green portion of the graph indicating that the network is highly survivable, thus placing the network in a benign state, as shown in figure 13b..

Similarly, when ascertaining for the overutilized links and interfaces, the 75 failure cases lay in the green region of the graph, also indicating a very high survivability of the network. The graph is shown in figure 4.5c.

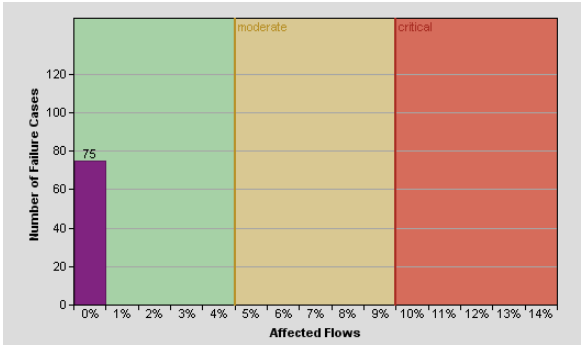
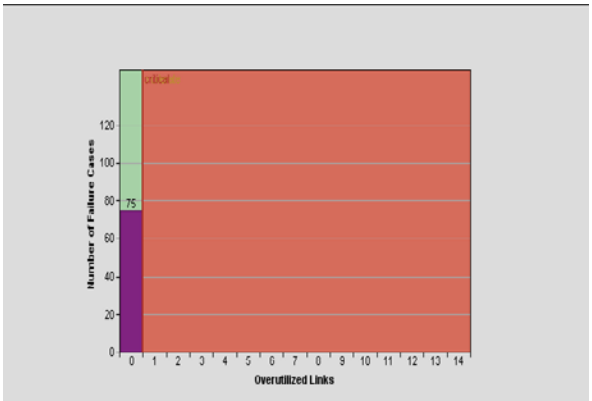


Fig. 13b. Network Performance- Affected flows/ affected connectivity



Fig, 13c. Network Performance- Over-utilized links and interfaces

5.1.3 ELEMENT SURVIVABILITY

This graph lists the distribution of survivability indices of the 7 links and 7 interfaces in the network. The survivability index of an element is defined as the percentage of failure cases that this element survives.

According to the graph the 7 links and 7 interfaces were able to survive 100% of the failures. Figure 14a shows the interface survivability analysis graph and figure 14b shows the link survivability analysis graph.

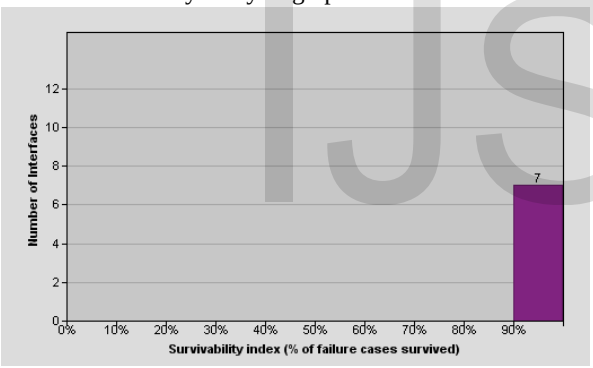


Fig. 14a. Survivability of Interfaces

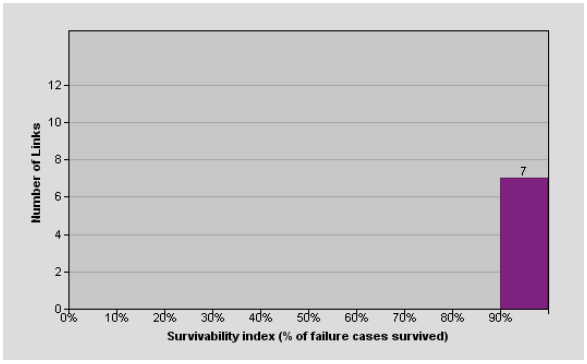


Fig. 14b.Survivability of Links.

6. 0 CONCLUSION AND RECOMMENDATIONS

Throughout this paper, we have observed the different performance parameters for a functional IEEE 802.11b WLAN intranet set up for electronic voting.

The performance measurement results and survivability tests show that this WLAN intranet setup will ensure that e-voting is carried out effectively on a network that is both secure and very reliable. Observing the figures for the WLAN load, throughput and delay show that the load is transmitted with a very high efficiency and little delay. From the Survivability Test, the 75 failure test cases had only benign or no impact on the network performance and the overall survivability score proved thatthe network would be able to withstand and recover from any failure without critical violations in any of its performance metrics. Overall, the proposed IEEE 802.11b WLAN intranet willfunction as anexcellent network backbone for a campus based e-voting exercise. It is therefore recommended for use in such a project or even much larger projects.

REFERENCES

1. F. Ayo, "Election Rigging and the Problems of Electorcal Act in Nigeria," *Afro Asian Journal of Social Sciences*, p. 1, 2011.
2. N David, D Ubachukwu, H Ijomanta, C Ozoudeh, A Biometric based Software Solution for E-Voting using networking, Sch. J. Eng. Tech., 2014; 2(6B):874-881, https://www.researchgate.net/publication/268745860_A_Biometric_based_Software_Solution_for_E-Voting_using_networking?ev=prf_pub
3. Nathan David, Patrick Ocheja, Paschal Udeh, Olisa Okpoko, Design of a University Portal with Biometric Lecture Attendance Monitoring System, Sch. J. Eng. Tech., 2014; 2(6B):847-856. https://www.researchgate.net/publication/268745868_Design_of_a_University_Portal_with_Biometric_Lecture_Attendance_Monitoring_System?ev=prf_pub
4. B. C. Molokwu and M. N. Agu, "Secure Intranet Voting System for Students' Union Elections in Nigerian Tertiary Institutions," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 6, pp. 78-79, Nov - Dec 2014
5. Z. Lu and H. Yang, Unlocking the Power of OPNET Modeler, New York: Cambridge University Press, 2012, pp. chp.1 3-4
6. Nathan David, Campus Wide network for Univesity of Nigeria, Nsukka Campus, NIJOTECH, VOL. 29 NO.1, MARCH 2010, p. 52-60
7. Nathan David, Chukwunonye Anyakoha, Henry Agbo, OPNET based simulation for Rural Educational ICT Connectivity, International Journal of Scientific & Engineering Research, Volume 7, Issue 4, April-2016. P. 1499-1504
8. https://www.researchgate.net/publication/301779184_OPNET_BASED_SIMULATION_FOR_RURAL_EDUCATIONAL_ICT_CONNECTIVITY?ev=prf_pub
9. C. Hilas and A. Politis, Simulations of Various IEEE 802.11b Network Configurations for Educational Purposes.
10. O. O. Elechi, "Design and Simulation of Wireless Local Area Network for Administrative Office using OPNET Network Simulator: A Practical Approach,"
11. S. Sethi and V. Y. Hnatyshin, The Practical OPNET User Guide for Computer Network Simulation, Boca Raton, Florida: CRC Press, 2013, p. 191.