International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Computer Network Reliability Analysis of a Dual Ring Network: Federal University of Technology, Minna (Gidan Kwanu Campus) As a Case Study

Godwill Udoh, Caroline Alenoghena, and Bala A. Salihu
Department of Telecommunication Engineering, Federal University of Technology Minna, Nigeria
godwilludoh@gmail.com-mail,carol@futminna.edu.ng, salbala2000@hotmail.com

Abstract—**In the reliability analysis of computer networks there are different approaches to tackling the task. For dual ring networks, k-terminal reliability is preferred and used in this work. A concise description of the campus network studied is given. In this work a reliability analysis of a computer network is done using K-terminal reliability measure to give an index for comparison and define network performance indicators that affect the reliability of the computer network. .In the reliability evaluation, the terminal stations/nodes are seen as to be made up of different critical components and is treated as such. Plots of reliability index against these components of the stations show very low values when priority is placed on only one node as is the case in the understudied network. Different parameters affect the reliability of the network and are evaluated in the work.**

Keywords-reliability analysis; computer network; reliability index; network reliability; k-graphs; dual rings

I. INTRODUCTION

Present day communication is centered on computer networks, thus, the design of reliable computer networks is much needed. Reliability analysis of a computer-communication network gives “worthiness test” of the infrastructure or relevant components that constitute the computer network and as such, seeks to evaluate the relevance of the computer network to its intended design expectations.In evaluating the relevance of a computer network, service indicators like Quality of Service (QoS) often come into consideration. Reliability is a prominent index in achieving high QoS performances of telecommunications networks. Effective reliability design also aids resource managements. Effective reliability design technologies in developed countries employ “end-to-end reliability” measure. In catering for factors shaping the distribution of economic activities, progress process of network facilities and disparity of reliability at inter-regional level, “one-to-all” measure is employed in developing countries

Most computer network reliability problem is primarily resolved by calculatingthe probability that some specific set of nodes in understudied network can “talk” to one another at a given time.

Different set of algorithms are employed in reliability analysis of computer networks. The algorithms used can be grouped into two:

A. Path/Cut Enumeration:

This entails the listing of all the simple paths that exist between the end nodes. This represents a complete set of favorable non-disjoint events. Simple paths are links in the network that connect set of nodes while prime cut sets are links in the network which when disconnected cause the network to fail. The simple paths are considered as sets of favorable events while the prime cuts as set of unfavorable events. Reliability analysis entails summing the terminal reliabilities of these paths which is an indication that each node communicates with a designated node. To obtain the computer network reliability, the inclusion-exclusion techniques of path and cuts is carried out. Boolean algebra also offers efficient techniques that can be used to do this.

B. Case analysis:

Case analysis uses the method of graph decomposition. This entails the creation of subsets from the pathsets, either around a reference edge or around a number of edges/links/paths. A reference edge is simply the node from which the factoring is referenced. When more than one edge is considered, graph decomposition is restricted to a conservative policy as against an exhaustive one. Using a conservative policy minimizes the number of disjoint events in the analysis. Disjoint events are simple paths that are not connected or have common node. This decomposition simplifies the analysis and helps cancel out occurrence of parallel links.

II. REVIEW OF RELATED WORKS

Most of the works reviewed evaluate the reliability of understudied Networks by the methods of minpaths and mincuts. A minpath is the shortest distance/path/ number of hops between nodes needed to keep them up and communicating while mincut is the smallest break in the link/network that renders the link/network ineffective. An aggregation of paths between nodes is called pathsets while an aggregation of cuts in the network is called cutsets.

As a network enlarges and nodes increase, the number of minpaths and mincuts increase exponentially. Effective analysis of these sets needed to keep the network up or down via optimization methods help in estimating the reliability of understudied networks.

Genetic algorithm as an optimization tool was used in evaluating the reliability of networks [1]-[3] [4].

Wei-Chang Yeh [5] in his work used Particle Swarm Optimization and Monte Carlo Simulation in analyzing the pathsetsinorder to evaluate the reliability

Monte Carlo simulation was also employed in [6] [7] [8] to analyze the pathsets/cutsets inorder to evaluate the reliability understudied network.

Wei Hou [9] in his thesis, analyzed the reliability of networks with software and hardware failures. He developed models; MORIN – Modelling Reliability for Integrated Networks and SAMOT – Simplified Availability Modeling Tool, with which he used in analyzing the Network.

Boolean reduction technique was also used in evaluating the reliability of understudied network [10] – [14]

Mathematical Analysis are also employed in the reliability analysis of networks [15] – [17].

An overview of works reviewed shows that little has been done on reliability analysis of Ring topology networks (this might be a ripple-effect from the fact that most computer networks implement the mesh topology for its obvious advantages).

Earlier works seem to use survivability, availability, susceptibility, connectivity and reliability interchangeably. These mentioned parameters are distinct and a field of study on themselves.

Modern communication networks are made up of reliable components and failed components are quickly repaired. Multiple connections which allow for rerouting of messages in the event of a network failure is also a common feature. With the afore-stated in mind, it is important to take into account the connection ports, links and state of the nodes (this should cater for issues of power supply, equipment malfunctioning and working environment) in the reliability analysis of computer networks.

III. MODELING THE NETWORK

Models used to describe computer networks help to define a frame in which the network could be studied. From papers researched, the common model used for Computer Network is the Stochastic Model.

A stochastic network [18] describes a physical system in which each node and/or each edge (directed or undirected) fails statistically independently with a number representing the non-failure probability such that failures of any network elements do not affect another network element in same network. With this model, the network reliability analysis problem consists of measuring the probability given failure/operation probabilities for edges/nodes and the link connectivity [19].

In the Reliability analysis of Computer Networks (especially Ring Networks), the following assumptions are made (depending on the number of components understudied):

- Components are either operative or failed at any given time. Component state is a random event, s, independent of the state of any other component
- The reliability of a network component is the probability that it is operative at any given point in time.
- The Channel Capacity, C, is fixed and C » B (where B is the provisioned Bandwidth/Capacity for the Network).
- Failure of any electronic component in a station, including the power supply, causes the station to fail
- Network reliability does not include the probability for failure of attached hosts since they are external to the understudied communication ssubnetwork.

The components used to define the node in the understudied network are the link, port and station itself. The station define the system health and caters for power issues in the node. Failure/success probabilities of these component are independent of each other but have an overall effect on the state of the node.

The port comprises the transmitter, receiver and the inbound/outbound link used in effecting self-healing when a fault occurs.

A. *Describing the Understudied Network*

The School’s campus network understudied (Federal University of Technology, Minna; GidanKwanu campus), as at time of research has 9 nodes (RAD ETX-1002) and 11 terminal stations (RAD ETX-201). All the nodes have a port/Terminal station/leaf that serves the complex they are located. The nodes (which are basically DAS –Dual Attachment Station) form the backbone of the network. The terminal stations or leafs on the branches are basically SAS – Single Attachment Station. The Campus Network is a Dual Core, full-Duplex, Bi-directional Ring Network. For the purpose of analysis, we are considering it as a dual ring network having 9 DAS as nodes. We implement the K-Terminal Reliability measure in evaluating the reliability of the dual ring.

B. *K –Terminal Reliability*

A good index for measuring the utilization of a computer network reflects the fact that network usually fails gradually and that some nodes and/or links are more important than others. The measure also should not be based on traffic patterns. Terminal, “capacity-related”, and “travel-time related” reliability measures are possible measures that satisfy the stated prerequisites.

Terminal Reliability is the probability that there is an end-to-end connection between atleast two nodes in a computer network needed to keep the network up and running. There are basically 3 variants; K-Terminal, 2-Terminal and All-Terminal Reliabilities.

The common measures of reliability problems when applied to computer networks are mainly specialized cases of k-terminal reliability. This is defined as the probability that a path exists which connects k terminals (nodes) within the network.Reliability here is gotten by summing the probabilities of disjoint success paths. The complexity of identifying all disjoint success paths is exponential and as such determining K -terminal reliability for a network could be very time-consuming. Most existing researches on K–terminal reliability speed up calculations by reducing the computation efforts as much as possible.

C. K – Terminal Reliability of Ring Networks

A ring can be defined by a network graph; G = (V, L), whose vertices (V) and directed edges (L) are connected in a cycle(circuit). The vertices represent nodes and the directed edges represent fiber path from one NAP (Network Attachment Port) transmitter to another NAP receiver. Whenthe primary ring is operative, then the vertices and edges comprising the subgraph of these elements are traversed exactly once, forming an Eulerian circuit. If a link or a station should fail on the primary link, it is eliminated from G and self-healing is invoked. Consequently a new subgraph is formed which comprises operative stations on both the primary and secondary links. This constitute the needed Eulerian circuit. The derivedsubgraph provides communication among operative stations and links in a ring network. It also provide communication among stations that can communicate using the ring network protocol. [20]

For K stations, at least one component is not in any other K-MEC. Each of its K-MEC (minimal eulerian circuit) is distinct in graph.Edges and vertices in G that are not in these circuits are irrelevant and contribute nothing to K-terminal reliability for this subset. The reliability of the ring network having k nodes, R_k(G), then becomes the probability that a set of K-MEC is operative. The sum of probabilities of this set, using inclusion-exclusion to evaluate the K-terminal reliability of a ring network containing the set of K-MEC, Ei, for i = 1. . . m, is given in equation 1

$$pr\{A\}=\sum_i Ai-\sum_{i<j}(Ai\ \cap\ Aj)+\sum_{i<j<k}(Ai\ \cap\ Aj\ \cap\ Ak)+\cdots+(-1)^{m-1}.Pr\{Ai\ \cap\ Aj\ \cap\ Ak\ldots Am\} \tag{1}$$

Where A*i* is a MEC having *i* nodes and Aj has *j* number of nodes.

From the analysis, a K-graph is derived. A K-graph is a circuit formation containing one or more K-MECand is a subgraph of G. A particular K-graph can correspond to several different circuit formations which might have many repeated terms. Some of these have a positive coefficient $(-1)^{k-1}$corresponding to an odd number k of K-MEC and some have a negative coefficient $(-1)^{k-1}$corresponding to an even number k of K-MEC in the formation. Statedcircuit formations are odd or even formations respectively. The combination of these positive and negative coefficients on repeated terms cancels out some of the terms in the final expression. The net number of noncanceled terms which is also the net number of noncanceled K-graphs of type Hi, viz, the net number of noncanceled circuit formations is termedthe domination value d_{Hi}. To reduce the number of repeated terms in the final expression we introduce the denomination value as given in (2).

$$\Pr\{Ai\}=\sum_{i=1}^{n} d_{Hi}.Pr\{k_i\} \tag{2}$$

Where K*i* is the K-MEC derived at *i*

Computational complexity of the decomposition is dependent on the number of K-graphs in the network.

In order to apply this to the Ethernet ring network topology deployed in the Campus (FUT MINNA)**,** the number of K-MEC in each topology is first determined. We assume that the K stations of interest are sorted in token-passing order and are renumbered with an additional index from 1 to K. We refer to the station pair ***(ij)*** in this renumbered K element subset as consecutive stations if j = $(\boldsymbol{i}\pm\mathbf{1})$ mod K. [24]

D. K – MEC in Dual Rings

A dual ring has two sets of K-MEC.

Set #1 consists a circuit which contains all the stations and links in the operative primary ring.

Set #2 comprises other circuits that are formed by using two consecutive stations of the K given stations;having the self-healed end stations. Since there are K end-station pairs, there are K K-MEC in set #2, making the total number of K-MEC in a dual ring K+ 1.

Using the concept of case analysis (stated in introduction); we effect graphical decomposition around a single keystone. The keystone chosen here was the node at ITS-InfoTech Studies center.

IV. COMPUTING THE K-TERMINAL RELIABILITY OF THE NETWORK

For K ordinary DAS and K =9

Notation

P	Station Reliability
D_l	Link/ Fiber path Reliability
D_p	Port Reliability
$\oplus$	Addition modulo K
t_j	($(t.x)_j$, 0, *), j = 1... K; addresses of the K stations of interest in a dual ring (These addresses are sorted in token-passing order on the fault-free ring)

s_j (($(t.x)_{j\oplus 1}$ - $(t.x)_{j\oplus k}$).mod N-station-separation distance.

In order to determine the probability that stations t_j, j = 1. . . K, can communicate with each other in a dual ring, the noncanceled K-graphs are derived and Pr {Ki} is computed.

A. Case l

K-graph H_1 results from circuit formation F_1 and contains all DAS and links on the primary ring. This occurs for all K in the noncanceled graphs at k=0 in the derived k-MEC.

$$R_{DR1}=p^N.D_l^N.D_p^{2N} \tag{3}$$

B. Case 2

K-graph H_j results from circuit formation F_j, j = 2... K, and contains all DAS and links connecting the K specific stations in both primary and secondary ring segments with self-healed end stations $t_{j\oplus k}\ and\ t_{j\oplus 1}$. This is formed from the nodes under consideration in the network.

$$R_{DRj}\ =\ p^{N-S_j+1}.D_l^{2(N-S_j)}.D_p^{2(N-S_j+1)} \tag{4}$$

C. Case 3

K-graph H_{j+k} results from circuit formationF_{1j}, j = 2... K, and contains:

- all DAS and links connecting the K specific stations in both primary and secondary ring segments with self-healed stations $t_{j\oplus k}$ *and* $t_{j\oplus 1}$
- all DAS and primary ring

$$R_{DR1j} = p^{N}.D_{l}^{2N-S_j}.D_{p}^{2N} \tag{5}$$

K –terminal Reliability of a dual ring network having N = 9 nodes and $1 \leq S_j \leq 8$ is obtained by summing the probabilities in cases 1, 2 and 3 after multiplying by the appropriate domination coefficient gives [24]

$$R_K(G)_{DR} = R_{DR1} + \sum_{j=2}^{K+1}(R_{DRj} - R_{DR1j}) \tag{6}$$

V. RESULTS

Applying the above stated equation to the K-graphs for the understudied network, we have

TABLE I. RESULTS FOR RELIABILITY INDEX COMPUTATION FROM K = 1 TO K = 9

Skeleton	**Given Rules**
$R_1(G)_{DR}$	$p^9.D_l^9.D_p^{18}$
$R_2(G)_{DR}$	$p^9.D_l^9.D_p^{18} + p^7.D_l^6.D_p^{14}(1-p^2.D_l^1.D_p^4) + p^4.D_l^3.D_p^8(1 - p^5.D_l^4.D_p^{10})$
$R_3(G)_{DR}$	$p^9.D_l^9.D_p^{18} + p^7.D_l^6.D_p^{14}(1-p^2.D_l^1.D_p^4) + p^7.D_l^6.D_p^{14}(1-p^2.D_l^1.D_p^4) + p^7.D_l^7.D_p^{14}(1-p^2D_l^1D_p^4)$
$R_4(G)_{DR}$	$p^9.D_l^9.D_p^{18} + 2\{p^7.D_l^6.D_p^{14}(1-p^2D_l^1.D_p^4)\} + p^8D_l^7D_p^{16}$
$R_5(G)_{DR}$	$p^9D_l^9D_p^{18} + 4\{p^8D_l^7D_p^{16}\}$
$R_6(G)_{DR}$	$p^9D_l^9D_p^{18} + 4\{p^8D_l^7D_p^{16}\}$
$R_7(G)_{DR}$	$p^9D_l^9D_p^{18} + 2\{p^8D_l^7D_p^{16}\}$
$R_8(G)_{DR}$	$p^9D_l^9D_p^{18} + p^8D_l^7D_p^{16}$
$R_9(G)_{DR}$	$p^9D_l^9D_p^{18}$

p, D_l , D_p are the operative probabilities (and hence, reliability) of the nodes, links and ports respectively.

To calculate $p, D_{l\ and}\ D_p$ we use

$$1 - R_{failure} = 1 - e^{-\lambda t} \tag{7}$$

Where λ the failure rate of the component under discussion,$R_{failure}$ is the failure probability of component and t is the time frame used to understudy the component in the link.

The accepted probability for fiber failures in the distribution part of the new ITU-T G.657 proposal document (in Annex I) is around 1/100000 over 20 years per fiber per network element.

This gives $R_{failure}$ = 1/100000=0.00001

D_{fl} = 1- $R_{failure}$ = 1- 0.00001= 0.99999

$D_t = 1 - R_{failure} = 1 - e^{-\lambda t}$

From [21] [22],

FIT (/10^9 hours) = 958; hence FR = 958/ 10^9 = 0.958 x10^{-6}

$D_t = 1 - e^{-\lambda t} = 1 - e^{-0.958\text{ x}10^{-6}\times 20\times 365\times 24}$ = 0.1545123

$D_r = 1 - R_{failure} = 1 - e^{-\lambda t}$

From [21] [22],

FIT (/10^9 hours) = 130; hence FR = 130 / 10^9 = 0.13 x10^{-6}

$D_r = 1 - e^{-\lambda t} = 1 - e^{-0.13\text{ x}10^{-6}\times 20\times 365\times 24}$ = 0.02251858

$D_l = D_t\,.\,D_r\,.\,D_{fl}$ = 0.99999×0.1545123×0.02251858 = 0.003479

From [23],

FIT (/$2.92\text{x}10^6$hours) = 1;

Hence, $FR = \lambda = \frac{1}{2.92\text{x}10^6} = 3.424658\text{x}10^{-7}$

This gives the Reliability of the port as $D_p = 1 - e^{-\lambda t}$ over a time frame of 20 years as

$1 - e^{-\lambda t}$ = 1 - $e^{-3.424658\ \text{x}10^{-7}\ \times 20\times 365\times 24}$ = 0.0582354

Readings taken from the campus shows an average of 128 failures in 1month; (30×24) hours on the nodes. High rate of failure here is due primarily to the erratic power supply in the campus and the absence of working standby power banks.

This gives 30 × 24hours = 128

$Pr_{failure}$ = 128/ (30 × 24)

P = 1 − $R_{failure}$ = 1 - 128/ (30 × 24) = 0.82222

$1 - R_{failur\ e} = 1 - e^{-\lambda t} \rightarrow R_{failure} = e^{-\lambda t}$

1 – 0.82222 = $e^{-\lambda\times 20\times 365\times 24}$

0.18888 = $e^{-\lambda\times 175200}$

λ = In 0.18888 ÷ -175200 = 9.512805×10^{-6}

SAS reliability = D_{SAS} = p. D_p = 0.82222×0.0582354 = 0.04788231

DAS reliability = D_{DAS} = p.D_p^2 = 0.82222×0.0582354^2 = 0.002788446

Determining the Mean Time before Failure, MTBF, entails summing the mean time to fail (MTTF) and the mean time to detect and repair (MTTR) [24]

$$\text{MTBF} = \text{MTTF} + \text{MTTR} \tag{8}$$

For the equipment in this research (RAD SWITCHES), the repair time (actually, negligible since there have been no faults since their provisioning) is quite small compared to the MTBF, so this work approximates the MTBF to be equal to the MTTF.

With the afore-stated and considering the Time frame for data collection, we assume the average time between power outages to be the MTBF of the RAD Switches.

MTBF = 1 ÷ (128/ (30×24)) hours
= 1 ÷ 0.178 = 5.625 hours

The average time taken to restore power supply to the Station via alternate sources is around 15 minutes and supply by the Generator set lasts about 4 hours.

MTTR = 15 minutes = 15/60 = 0.25hours

Unavailability of the Network, q = MTTR/MTBF = 0.25/5.625 =0.0444444

MTBF ≈ MTTF= 5.625 hours

Availability and unavailability are often expressed as probabilities. For the equipment understudied (RAD Switches and Fiber Links), all of the failure rates were based on field data or assumptions that devices of comparable complexity and exposure should have similar failure nodes.

$A = MTBF/(MTBF + MTTR)$= 5.625 / (5.625 + 0.25) = 0.95744681

For the Optic Fiber Link, cuts/failures are usually due to excavation or construction works on fiber path and attacks by rodent. Data gotten from the ITS shows there have been no fiber cut/failure since the provisioning of the facility, and considering the layout and terrain of the campus, there is likely to be none for the next 2years.

The RAD Switches employed in the Network design have not failed since provisioning too. Inoperability of the devices is due primarily to challenges of erratic power supply to the Station.

The average time taken to restore power supply to the Station via alternate sources is around 15 minutes and supply by the Generator set lasts about 4 hours.

MTTR = 15 minutes = 15/60 = 0.25hours

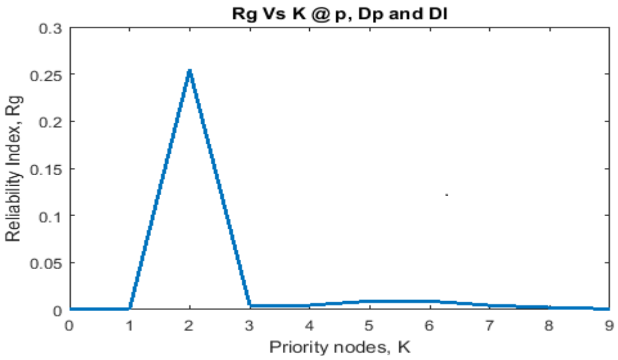

Figure 1. Reliability plot at P, D_l , D_p

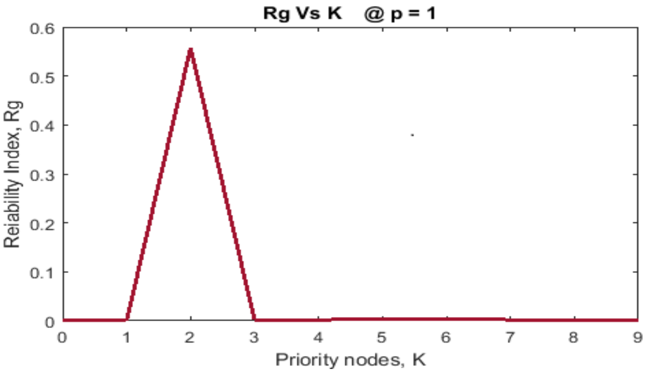

Figure 2. Reliability plot at P negligible

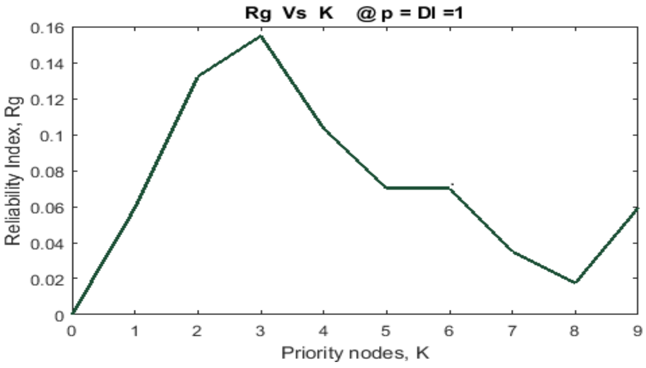

Figure 3. Reliability plot at p, $and\ D_l$ negligible

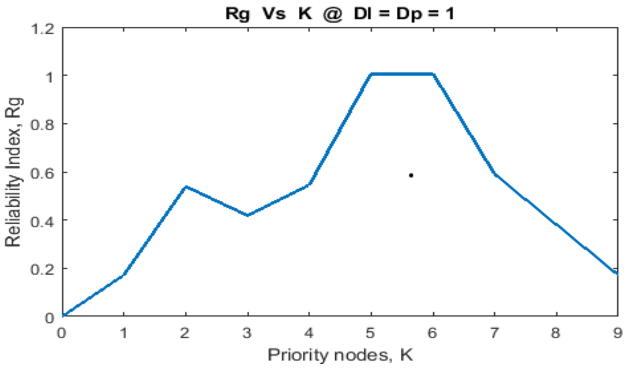

Figure 4. Reliability plot at $D_l\ and\ D_p$ negligible

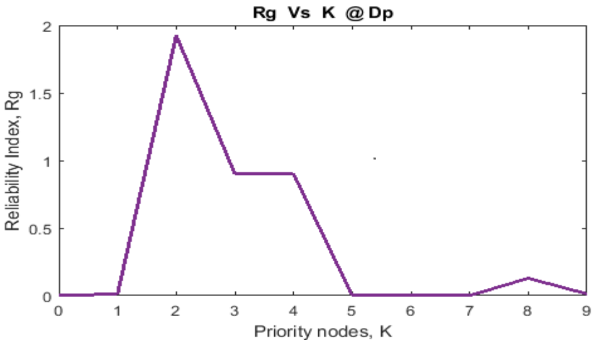

Figure 5. Reliability plot at D_p negligible

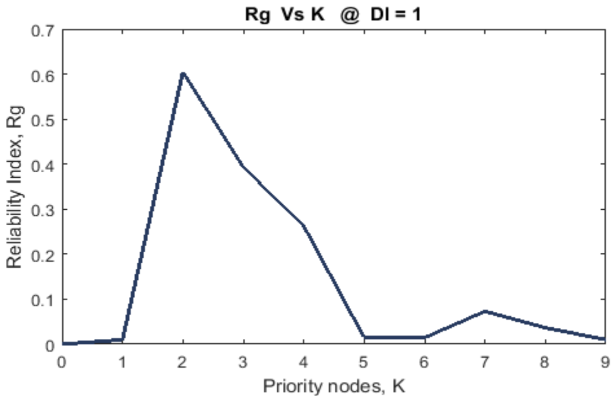

Figure 6. Reliabilit plot at D_l negligible

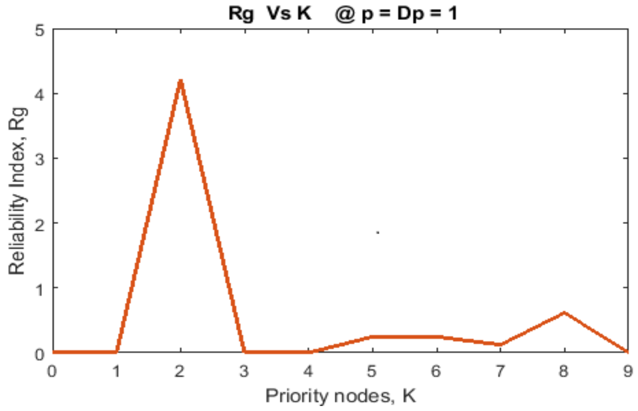

Figure 7. Reliability plot at p and D_p negligible

VI. DISCUSSION OF RESULTS

Plot 1: The best value for reliability Index is at K = 2. This plot shows the effect on Reliability Index when all the variables are considered (fig 1)

When we make any parameter defining the node, port and/or link to be one, we are assuming a perfect parameter, making its influence on the Reliability of the Network negligible. In the computation for node reliability and overall reliability of the network, the events are independent and as such making any of the events to be one simply makes its effect negligible.

Plot 2: When the effects of p is made negligible, best values for reliability index is at K = 2. This implies that if the other parameters are considered only as variables, considering the present network, it will be better to have priorities placed on two nodes for optimal reliability values. (Fig 2)

Plot 3: When the effects of p and D_l are made negligible on the network, reliability values peaks at K = 3. This implies that if only the port reliability,D_p is considered, three nodes are needed to be given priority for optimal network reliability. (Fig 3)

Plot 4: When the value of D_l – link reliability, is made negligible, the plot peaks at K = 2 for optimal reliability. This implies that if only the station and port reliability are considered, it will take two nodes of priority for optimal reliability (Fig 4).

Plot 5: When D_p $andD_l$ is made negligible, the plot pikes at K = 2 and K = 5 and 6. Optimal values is at K = 5 and 6 approximating one (1). Given that the links (fiber paths) and ports on network devices (SAS and DAS) have not had any fault since their commissioning, it is safe to assume their overall effect on the network reliability is negligible. This plot (fig 5) aptly describes FUT, MINNA; Gidan Kwanu Campus Computer Backbone Network. As such it is imperative to have priorities placed on five or six nodes out of the nine nodes that comprise the backbone network. Keeping priority on only one node (ITS), as it is presently, makes the network very unreliable.

Plot 6: When Dp is made negligible, reliability values peaks at K = 2 (fig 6)

Plot 7: When p andD_l are made negligible, the lot peaks at K = 4 (fig 7)

Where D_l $andD_p$are assumed to be 1, as in the case of the FUT MINNA, GidanKwanu campus network (fig 5), it is observed that 5 to 6 priority nodes are needed to have optimal network reliability when the Network reliability is dependent, primarily, on the station reliability (as it is with FUT MINNA, GidanKwanu campus computer backbone network). . It is observed from all plots that at K = 1 the network reliability is always minimal. Often in the range of 10^{-4} and in some cases 10^{-23} (fig 7).

The value of D_l - composite link reliability, shows that it is the weakest and most vulnerable of the parameters in the understudied network. Hence, adequate protection measures are needed to maintain its workability.

The value of reliability for DAS which comprises the backbone of the understudied network shows it is very low and that the attached hosts (consisting of SAS) are more reliable in the network. This is as a result of epileptic power supply $(p.D_p^2)$ and that the DAS are integral in the design of the network.

The Mean Time before Failures (MTBF) value of 5.645hours when compared to tens of hours for average enterprise networks is low.

The average time taken to restore the network (0.25hours) is much given that current trend in telecommunications is to limit the range to about 20ms.

The availability of the network is good, 0.95744681 (given it is an academic environment) even though it falls short of the “five-nines” (99.999%) property needed of most telecommunications networks.

VII. CONCLUSION AND RECOMMENDATIONS

FUT Minna campus computer backbone Network was analyzed and its reliability index was computed to be around 0.0007 using the K-Terminal Reliability measure.

The following outlined recommendations are given:

- Future studies on the school’s network reliability analysis should go further to incorporate Capacity related and travel time measures of reliability. This would answer questions of packet drops, effective data throughput and transmission delays.
- To improve the network, the station reliability has to be upgraded. For optimal network reliability, priority

should be placed on 5 or 6 nodes out of the 9 nodes that make the network. As observed, priority placed on only one node (as it is presently in the school's campus network with the node at ITS given the highest and only priority) yields a very low reliability for the network; 0.00076 for the school's network understudied.

- Upgrading will entail installing battery/power banks to improve upon power supply to selected 5 or 6 nodes.
- Distributing the servers among these nodes will also be needed (actually better-off) than concentrating the servers at the ITS Node.
- The RAD Switches cannot implement automatic switching in order to effect self-healing on the ring when a cut/fault occurs. Thus, network engineers have to physically unplug and plug back fiber links to through-ports on the ODF (optical distribution frame). The use of layer 3 devices, like Cisco 3550 series, can help eliminate this need and reduce MTTR for the network. They do this by implementing the Hot Standby Router Protocol - HSRP and Gateway Load Balancing Protocol - GLBP. HSRP provides automatic router back-up. GLBP improves on the redundancy of the system.

With these devices, the school can also implement the MPLS (Multi-protocol layer switching) technology. MPLS delivers highly scalable, differentiated, end-to-end IP services with simple configuration, management, and provisioning for providers and subscribers.

We have been able to perform a reliability analysis of a real time, physical network using K –terminal reliability measure. Since works on real networks is very limited, this could serve as a template (especially for enterprise networks using a ring network) or better still, serve as a reference for future works

VIII. ACKNOWLEDGEMENT

Godwill, U., Dr. Caroline, A., and Dr. Bala, S., thank the department of telecommunications in school ofEngineering of the Federal university of Technology, Minna, for help given in this research.

REFERENCES

[1] R. Dirk, F. Rothlauf, and P. Gmilkowsky. "Designing reliable communication networks with a genetic algorithm using a repair heuristic." *European Conference on Evolutionary Computation in Combinatorial Optimization*. Springer Berlin Heidelberg, 2004.

[2] K. Anup, M. Pathak, and P. Gupta. "Genetic-algorithm-based reliability optimization for computer network expansion." *IEEE Transactions on reliability* 44.1 (1995): 63-72.

[3] A. Fulya, B. Dengiz, and A. Smith. "Reliability optimization of computer communication networks using genetic algorithms." *Systems, Man, and Cybernetics, 1998. 1998 IEEE International Conference on*. Vol. 5. IEEE, 1998.

[4] K. Abdullah, and A. Smith. "A hybrid genetic algorithm approach for backbone design of communication networks." *Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on*. Vol. 3. IEEE, 1999.

[5] Y. Wei-Chang. "An improved sum-of-disjoint-products technique for the symbolic network reliability analysis with known minimal paths." *Reliability Engineering & System Safety* 92.2 (2007): 260-268.

[6] Y. Oliver "Terminal-pair reliability of three-type computer communication networks." *IEEE transactions on reliability* 41.1 (1992): 49-56.

[7] Y. Wei-Chang. "A new Monte Carlo method for the network reliability." *Proceedings of First International Conference on Information Technologies and Applications (ICITA2002)*. 2002.

[8] R. Suresh, A. Kumar, and E. V. Prasad. "Computing terminal reliability of computer network." *Reliability Engineering* 16.2 (1986): 109-119.

[9] H. Wei. *Integrated Reliability and Availability Aanalysis of Networks With Software Failures and Hardware Failures*. Diss. University of South Florida, 2003.

[10] S. Sieteng, and S. Rai. "CAREL: Computer aided reliability evaluator for distributed computing networks." *IEEE Transactions on Parallel and Distributed Systems* 2.2 (1991): 199-213.

[11] R. Suresh, and S. Soh. "A computer approach for reliability evaluation of telecommunication networks with heterogeneous link-capacities." *IEEE Transactions on Reliability* 40.4 (1991): 441-451.

[12] V. Malathi, and K. Trivedi. "An improved algorithm for symbolic reliability analysis." *IEEE Transactions on Reliability* 40.3 (1991): 347-358.

[13] K. Sy-Yen, F. Yeh, and H. Lin. "Efficient and exact reliability evaluation for networks with imperfect vertices." *IEEE Transactions on Reliability* 56.2 (2007): 288-300.

[14] B. Octavian. *An Enhanced Approach to Network Reliability Using Boolean Algebra*. Diss. Lafayette College, 2003.

[15] O.C. Ibe, "Reliability comparison of token-ring network schemes." *IEEE transactions on reliability* 41.2 (1992): 288-293.

[16] A. Satyanarayana, and M. Chang. "Network reliability and the factoring theorem." *Networks* 13.1 (1983): 107-120.

[17] G. Giancarlo. "Reliability evaluation of Common-Cause failures and other interdependencies in large reconfigurable networks." (2010).

[18] L. Yi-Kuei. "Reliability of a stochastic-flow network with unreliable branches & nodes, under budget constraints." *IEEE Transactions on Reliability* 53.3 (2004): 381-387.

[19] S. Akhilesh, X. Liudong, and H. Liu. "Modeling and evaluating the reliability of wireless sensor networks." *2007 Annual Reliability and Maintainability Symposium*. IEEE, 2007.

[20] Y. Jiahnsheng, and C. B. Shin. "K-terminal reliability in ring networks." *IEEE Transactions on Reliability* 43.3 (1994): 389-401.

[21] Reliability Data, Agilent technologies, Inc. 1999, 5968-6620E (11/99),www.semiconductor.agilent.com

[22] C. Nathan and L. Passauer. *Impact of Fiber Optics on System Reliability and Maintainability*. VITRO CORP SILVER SPRING MD, 1988.

[23] S. Flint, " *Failure rates for fiber optic assemblies* ". IIT RESEARCH INST CHICAGO IL, 1980.

[24] P. Chinmayananda, "Node Reliability in WDM Optical Network." (2012).