University of Ibadan
Journal of Science and Logics in ICT Research

Analytical Perspective: Failures in Telecommunication Networks in Africa and Deployment of Ant Colony System (ACS) Survivability Technology

[1]Ayoade Akeem Owoade, [2]Kazeem Idowu Rufai and [3]Bolanle Latifat Abimbola

[1,2,3]Department of Computer Science, Tai Solarin University of Education, Ijagun, Ijebu Ode.
[1]owoadeaa@tasued.edu.ng, [2]rufaiki@tasued.edu.ng, and [3]abimbolabl@tasued.edu.ng

Abstract
A failure in a telecommunications network, such as the loss of a link or a node, can occur for a variety of reasons. Accidental cable cuts, hardware malfunctions, software errors, natural disasters (e.g., fire), and operator mistakes are common causes of failures in Africa (e.g., incorrect maintenance). Because many of the causes of failure are outside the control of developing-country telecom operators, there is growing interest in the design of survivable networks. With the telecommunications network gaining traction, it is critical that telecommunications network-related issues such as node-to-node failures be resolved as soon as possible in order to maximize network resource utilization while minimizing failure rate. Many researches have been done on single failure points in telecommunications network, but very little on multiple network failures. This study suggests an Ant Colony System (ACS) survivability model based on capacity effectiveness and quick restoration to quickly resolve multiple node failure problems to improve service quality. The swarm model's resilience was tested using a node-to-node failure at the network's edges. Along with its working path, each communication flow seeks a survival path in order to protect multiple intermediate node-to-node failures. The survival solution path from this scenario demonstrates that the proposed swarm technology is feasible for current business applications in Africa that require high speed/broadband networks.

Keywords: *ICT4D, Telecommunication Network, Network Failure Model, Africans Network, Network Survivability, Ant Colony System*

1. Introduction

Large-scale telecommunications networks are vulnerable to a variety of failures, including natural catastrophes, glitches, and malicious attacks. Total failure failures are those that can result in a wide-area outage and impair network performance [1]. A disaster failure on both nodes and links can severely impede network operation. Communication systems are vulnerable to a range of failures, from solitary failures like fiber cuts and inline equipment malfunctions to simultaneous failures that can hinder a significant portion of the network [2].

There are already numerous past reports of network outages in telecoms and interconnected devices. Such occurrences caused significant outages, and their slow detection and diagnosis exacerbated their impact in terms of active service, financial loss, and human factors like trust in innovation [3]. Table 1 summarizes network outages in various countries.

In the literature, various methods for failure recovery have been suggested. They vary in the network structure being used, and while researches have been conducted on multiple network system outages, as well as the application of the Ant Colony System (ACS) in outage recovery are pretty recent. This inspires the research topic. The following identified gaps in the literature as the foundation for improving the current survivability approaches: (i) there are numerous failures in traffic flow in Africa that requires further consideration. (ii) In order to maintain a stable network, additional capacity distribution problems with multiple failures of African network systems must be addressed more thoroughly.

Ayoade Akeem Owoade, Kazeem Idowu Rufai and Bolanle Latifat Abimbola (2022). Analytical Perspective: Failures in Telecommunication Networks in Africa and Deployment of Ant Colony System (ACS) Survivability Technology, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 7 No. 2, pp. 20 - 32

Table1: The list consists of some of the world's particular network outages.

Date	Country/ Continent	Company	Cause	Implications for Cost
2011 till date	Nigeria [4]	Nigeria GSM operators: Airtel, MTN and Glo.	Power supply instability, inter-network integration issues Congestion on the network Failure to establish a call and subsequent call drop.	Reduced service quality and poor performance of a telecommunications network, resulting in a loss of income.
2010	Spain [5]	Power Company	A fault in a high tension power cable was caused by heavy snowfall in Spain.	220,000 people in and around Girona, Catalonia, were left without power. As a result, the telecommunications network fails.
2008	Europe [6]	Air Traffic Control at European Airports (ATC)	Network Interface Cards (NICs) hardware failure (NIC)	Loss of track of planes or ancillary flight data over multiple time periods
2006	Taiwan [7]	Telecoms firm	Undersea fiber optic lines in Taiwan were obstructed by an earthquake.	Banks from South Korea to Australia experienced significant disruption.

Authors categorize telecommunication network failures into three kinds, namely: (i) 1-link outages/failures, (ii) multiple-link outages, and (iii) disaster failures that include both a single node and multiple outages [8]. In a telecommunications network, single and multiple outages are the most common kinds of outages. As a result, protection against these two types of failures should not be overlooked [9].

The node failure in a disaster failure includes (i) outage of the transmitter or receiver node and/or (ii) failure of an intermediate node for a specific connection. In most cases, device outage on the transmitter/receiver is irreversible [10]. A connection that loses its transmitter/receiver node will be terminated. However, a service that has been disrupted owing to a receiver device outage could be recovered by obtaining distributed storage at a remote location.

The aim of this article is to demonstrate the survivability of the effect of various failures of telecom networks in African countries using an ACS model. This article's significant contributions are as follows: (i) the creation of a new suggested capacity-efficient ACS model, as well as rapid recovery, can indeed help Africa's telecoms in withstanding numerous failures. (ii) Generation of knowledge and methodical illustrations of study scenarios as a standard guideline for African telecoms researchers to understand connectivity issues survival. To the best of the researchers' understanding, the study appears as one of the first to demonstrate that an ACS technique can be easily put in place and applied to the survival of African telecommunications networks.

Because of their collaborative interaction, Ants are social insects that feed in colonies and are able to handle complex behavioural patterns and challenging situations from an ant's point of view. A fascinating aspect of ant behavior is their ways to identify the most direct routes between their nesting sites and sources of food. Some ant species deposit a chemical called pheromone when moving between their nest and sources of food. In the absence of pheromone trails, ants transition at random; however, in the presence of pheromone trails, they usually follow the trail [11]. In broad sense, the ACS technique tried to address an optimal control problem by executing the following the 2 steps below: (i) A pheromone model, which is a parametric probability density function over the solution space, is used to generate optimal solutions. (ii) The solutions are used to change the pheromone values so that future sample size favors high-quality solutions.

2. OVERVIEW OF SELECTED AFRICAN TELECOMS NETWORKS

2.1 Structure of the Telecommunication Markets

In South Africa, the market is structured around the traditional Public Switched Telephone Network (PSTN) operators, Telkom. There are three major mobile operators, and yet two are incumbents with a monopoly: Sentech, a provider of multimedia networks with an international hub. A carrier of carriers' license is also available, as well as seven licensed inadequately area licenses, six of which are functional, and 344 benefit active network licensees, as well as approximately 250 ISPs. Prior to the new Electronic Communications Act of 2006, all network licenses and related components were constrained to licensed existing firms. Telkom has an overwhelming influence on the PSTN market, while Vodacom and MTN continue to control the mobile market, limiting the potential for competitive rivalry for Cell C [12].

The Federal Government of Nigeria (FGN), the Ministry of Communications, the Nigerian Communications Commission (NCC), and telecommunications service providers are the main players in the Nigeria telecommunications sector. In Nigeria, the FGN's role in telecommunications has been very direct; it is the owner and operator of the incumbent PSTN public telecommunications firm. This changed with the deregulation of the telecommunications sector in 1992, when the NCC was established as a regulatory body. Since then, the NCC has been in charge of telecom, issuing licenses to private mobile telephone operators, allowing them to provide telephone services. This resulted in the issuance of GSM licenses to the first group of GSM operators: MTN, EWN (Econet Wireless Nigeria, which was renamed Vee Networks of Nigeria in 2004). Vmobile was acquired by Celtel in 2006 and is now owned by Airtel Nigeria. M-Tel (Nigerian Mobile Telecommunications Limited, the mobile subsidiary of Nigerian Telecommunications Plc, NITEL) joined in 2001, followed by Glo (Globacom Limited) in 2003 [13]. MTN was Nigeria's largest mobile telecoms operator as of June 2020, accounting for 38% of the market. Globacom and Airtel followed closely behind, with 27 percent and 26 percent of the market share, respectively.

2.1.1 Nigeria Perspective

Between 2001 and 2011, the deregulated market entry initiatives resulted in an impressive 53 percent compound annual growth rate in overall mobile telephone penetration. Despite the fact that annual growth rates are beginning to fall from a high of 160 percent in 2002. The telephone industry was still the fastest growing economic sector in the country. The sector grew at a 35 percent annual rate in the third quarter of 2011, and at a slower but still strong rate of 31.57 percent in 2012 [14]. With the collapse of the state fixed line carrier NITEL, the mobile GSM operators MTN, Globacom (Glo), Airtel, and Etisalat now dominate the telephony market, offering mobile voice and data connections throughout the country. At the end of September 2012, mobile operators controlled 96.5 percent of the market share for mobile subscriptions in Nigeria.

2.1.2 South African Perspective

The market is organized around a traditional PSTN operator and three mobile operators, but there are two dominant incumbents. Despite the fact that South Africa's policy and regulatory environment may have not been favorable to fixed network license investor, world telecom operators clearly see South Africa as the hub to the African region [14]. South African mobile companies are growing to be major players on the continent. They always had the necessary knowledge and skills to find success in challenging situations, and they are used to functioning in situations that advanced operators would believe often too difficult. Nevertheless, the combination of high profits offered by mobile operators such as Vodacom and MTN, fixed-mobile interconnectivity, and telecom sector interconnectivity may motivate the African market in the near future.

2.2 Failures in Telecommunication Networks

Telecom networks that span large areas are prone to a variety of failures. There are three types of failures: Single-link failures, Multiple-link failures, and Disaster failures that include both node (single) and link (multiple) failures [15]. The node failure in disaster failures for a specific connection includes I the source or destination

node failing, and (ii) one of its intermediate nodes failing.

2.2.1 Failures of a Single Device

A single node outage happens when the device is unable to route traffic. These events can be caused by a number of factors, including a device being turned off for maintenance or crashing due to hardware errors. A single node failure, for example, may result in multiple node failures if the failed node is a central node that controls other nodes on the network. Failure of a node Figure 1 depicts a scenario: Switches, routers, and concentrators are examples of connection nodes that connect servers to storage nodes. They only serve as a means of communication and do not store any data. outages affecting the entire router/switch are more damaging to network connections than link outages because a number of links connected to the switch or router are disrupted at the same time, but having lost communication access points does not directly result in data loss [16].

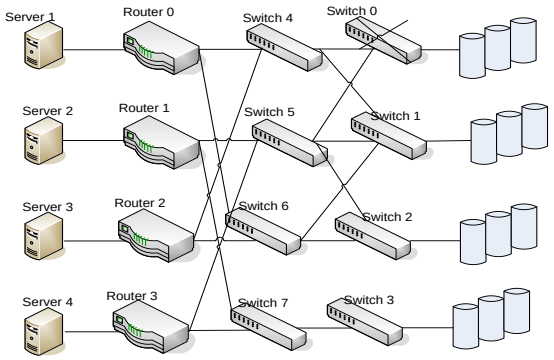

Figure 1: A Failure on Switch 0 Disconnects several Devices [16]

2.2.2 Single Link Failures

Any connection between two components in a system can be severed; if there is only one path between two components, a system is jeopardized if any link along that single path is severed. A reliable network interconnection must be resilient to link failures. Multiple paths between two components reduce the vulnerability of a single point of failure while also effectively balancing input/output workload [16].

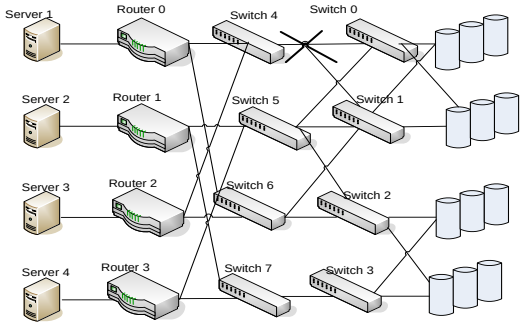

Figure 2: A failure on Links between Switches and Devices [16].

For example, if the link between switches 0 and 4 fails, as seen in Figure 2, a number of storage devices lose their connections to the system. However, other active links and nodes in the system become overburdened as all requests to storage devices attached to switch 0 are now routed through it. It also necessitates the purchase of more expensive switches with more ports for spare links. Furthermore, additional link outages on the path from a server to a storage device may disrupt the connection [17].

2.2.3 Multiple Nodes Failure

Several Nodes Failure occurs when two or more nodes fail at the same time. A node on the network may fail, and before that failure is resolved, another node fails, resulting in a multi-node failure sequence. Wireless Sensor and Actor Networks provide an example of multiple node failure (WSAN). A WSAN has two nodes: an Actor and a Sensor. (WSANs) are networks of sensors and actors that are linked by a wireless medium to perform distributed sensing and activation tasks. Sensors in such a network gather information about the physical world, while an actor makes decisions and performs appropriate actions on the environment. This enables machine-controlled and remote interaction with the environment. Because actors must coordinate their movements in order to be approachable by every node, a well-connected network is required at all times. However, if an associated actor fails, the network may partition into disjointed blocks, violating such a connectivity requirement. [18].

2.2.4 Multiple Links Failure

Multiple link failures can occur as a result of two scenarios. (i) A network link could fail at any time, and before that link can be fixed, one other link fails, actually results in a multi-link failure

series. (ii) Two separate links might well be channeled through common channel in practice. When multiple links fail, a communication could end up losing recovery ability in the first failure by becoming highly susceptible or unprotected in the second failure [19]. The real-world example of multiple link failures occurs (i) when two or more distinct fiber links share similar outage structures, which are commonly termed as Shared-Risk Link Groups. (ii) Furthermore, with Wavelength Division Multiplexed (WDM) technology, fiber link can support multiple light paths once they are routed on the physical topology. Two or more light-paths could potentially share the same physical link. A physical link failure may result in the outage of multiple links in the logical topology.

2.3 Networks Failure Survivability Mechanisms and their Laxities

This section discusses various failures and techniques for dealing with failures in the literature so that service continuity is not jeopardized in the first place or is quickly restored. As an example:

(i). *The Proactive Protection technique***,** One of the proactive mechanism's strengths is the fact that backup guarantees the information reaches the target whenever there is an outage. This mechanism's weakness is its inability to scale. This is due to the use of failover resources that are used to transport duplicate units, which provides survivability. The resilience of multi gateway wireless networks is an excellent example of proactive strategy [20].

(ii). *In Reactive Protection technique*, Reactive protection can be used if the number of packets generated during a proactively secured data transmission is reduced (a condition which normally necessitates the use of energy). The tendency to anticipate multiple routes just before data transmission procedure starts is a great feature of a reactive survival tactic. The paths, moreover, were never used until there is a fault in the primary path, and the weak point is the duplication created in memory space. SMR (Split Multipath Routing) [21] is a good example.

(iii). *For the Adaptive Restoration technique*, Each layer's restoration algorithms will be appropriate for immediate initialization by networking devices, giving rise in a self-configuring system capable of adapting to different outage situations. It has the ability to recover faults at multiple layers. Because recovery communications are not allotted, they are not assured in adaptive recovery. Multi-layer networks are an example [22]. The majority of these techniques make the assumption that only one failure is active at any given time, which is known as the Single-failure assumption. Real-world networks, on the other hand, may experience multiple-failure events due to a variety of causes, such as natural disasters or virus outbreaks affecting software components, all of which have the potential to disrupt a large number of network elements at the same time [23].

The Sprint research group's series of reports is perhaps the most study recently on the classification and recovery of an functional network based on the measured chosen to take over a 6 time frame. They made a significant assertion: "outages are part of day-to-day activities and influence a wide range of links" [24]. Due to the fact that the servicing dialog box was only about 5percent of the time per week, they revealed that 20 percent of outages occurred during planned servicing operations. The remaining failures were split into 30 percent shared failures (16.5 percent router-related and 11.4 percent optical-related, affecting multiple IP network links), and the rest were individual link failures. They also reported that 50 percent of the failures lasted less than a minute, 81 percent lasted less than ten minutes (which they classify as "transient" failures), and only 10percent lasted more than 45 minutes.

3. PROBLEM STATEMENT

To comprehend the reasoning behind this study and the result depicted in Figure 3. We conducted an empirical survey by sequentially sampling various network survivability strategies from articles in the Science Direct and IEEE journal databases. The most relevant and promising survivability strategies were discovered to have four key characteristics during the survey: I speed of restoration, (ii) capacity overbuilding, (iii) flexibility/selectivity, and (iv) standardization [25]. A good survivability technique should capitalize on the strengths of the various technologies and survivability schemes. Facts were obtained from these articles based on expert or judgmental opinion. The majority of network failures were attributed to survivability strategies,

with the investment cost for recovery at the highest layer being up to 20% higher than the costs for recovery at the lowest layer [26]. The studies conducted by Alison Gillwald [27] show that a single-layer survivability strategy is less expensive for networks with low (up to 50%) bandwidth utilization. Moreover, the authors clearly illustrate that multilayer survivability strategy becomes a much more appealing option for high utilization networks (75 percent and above of spare capacity in the transport layers). In our study, 60% of journals confirmed that most network failures are caused by laxity in survivability strategies [28, 29, 30, 31, 32, 33, 34, 35, 36, 37] and are based on both single and multiple failures, 35% of articles did not mention anything relating to survivability strategy, thus the status "Undecided," and 5% of articles stated that no such survivability strategy was used. Based on the results of the survey, we determined that we require an intelligent survivability strategy to address the previously mentioned multiple failure problem. These findings highlight the need for additional research to improve the presence of survivability strategies in telecommunication networks.

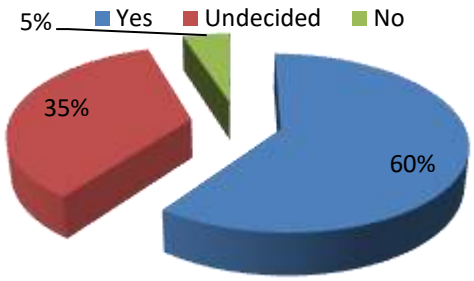

Figure 3: Failure due to Laxity of Survivability Strategies

4. PROPOSED DEPLOYMENT OF ACS SURVIVABILITY TECHNOLOGY

4.1 Technology Intervention

The suggested ACS framework is depicted in Figure 4 as a method for developing a survival telecommunication network model. The framework represents the model's layers, and the swarm intelligence technique is used.

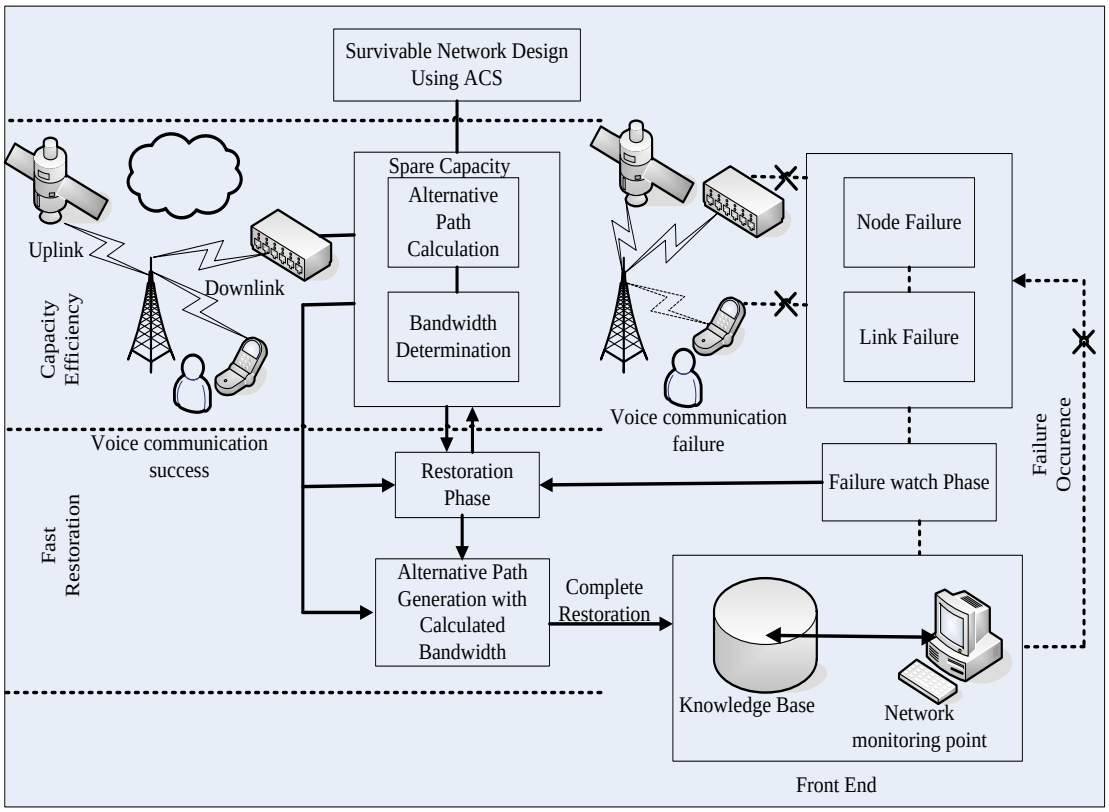

Figure 4: A Framework of Telecommunication network Survivability Strategy

At the network failure phase, the network is being monitored at the front end and the failure report is directed to the restoration phase for prompt survivability. Fast restoration is accomplished by combining the ACS model for generating an alternate path with an added heuristic for calculating the bandwidth required to reroute messages over an alternate path in real time. The system is efficient in terms of capacity due to the use of bandwidth and path calculation mechanisms. The benefits of the proposed model are (i) proactive tracking failures: the basic idea is to draw conclusions about upcoming failures based on the occurrence of previous failures, (ii) multipath routing - the ability to generate multiple paths between pairs of nodes, and (iii) fast route recovery - if the primary path fails, packets can be easily sent to the alternative path by re-calculating next hop probabilities.

Telecommunication protocol standardization goes beyond the techniques for protecting and restoring survivable networks. The development of standardized frameworks for implementing interoperable systems with survivability properties both independently and collaboratively as networked systems is becoming critical for the global community. The European Telecommunications Standards Institute (ETSI) recently announced the launch of a project Standardization, long - term survival, adaptability, fault detection, and access controls are all goals. Because every network device is procedure sensitive, this section of the benchmark was included in the suggested model.

4.2 Multiple Failures at Network Edges and Survivability Intervention

Figure 5 depicts a telecommunication network with switches representing nodes and failed nodes indicated by a cross sign in nodes C and F. The transmission link is the line that connects one node to another. The transmitting node is node A, and the receiving node is node E. If there is a device outage/devices outage along the transmission path when a message is sent from transmitting device A to receiving device E, the message will not be sent and must be rerouted along the alternative path generated by the ACS model.

Figure 6 is a representation of Figure 5's transition diagram. It shows the node labels and link cost used to determine the alternative path.

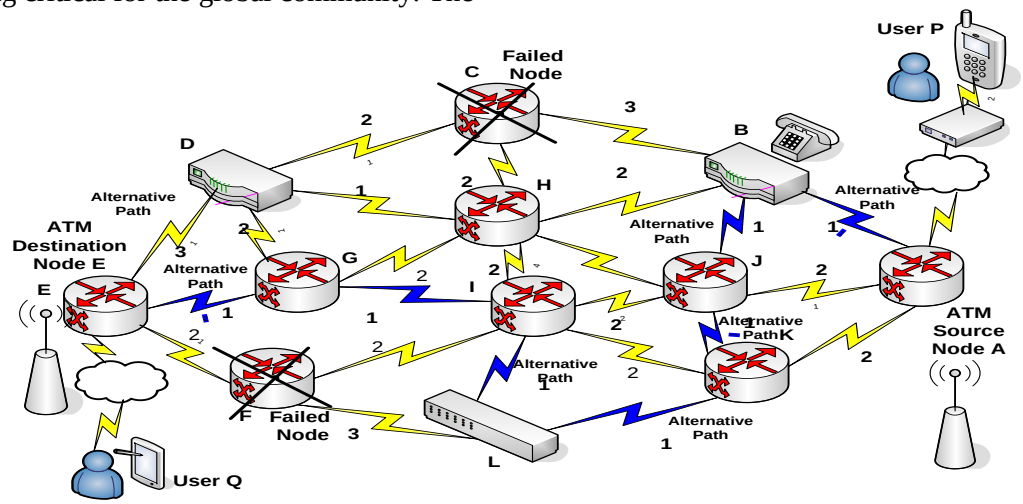

Figure 5: Node-Node Failure on Telecommunication Network [38].

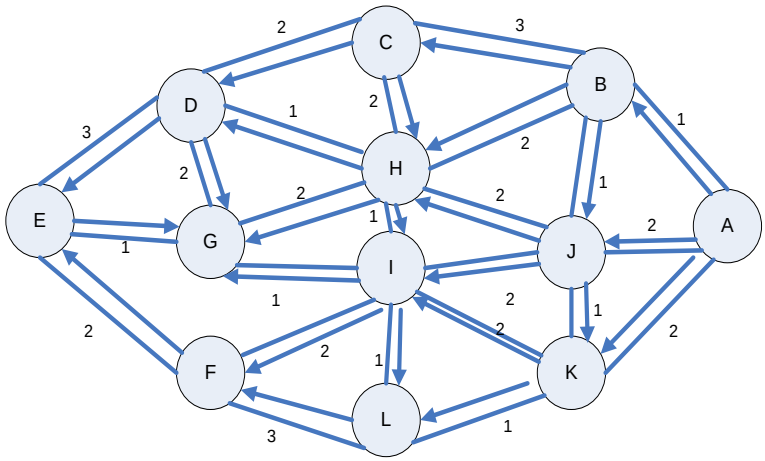

Figure 6: Figure 5's State Transition Diagram

4.2.1 Algorithmic and Mathematical Analysis

To model survivability, the ACS model is described below. Pheromone concentration at the start:

$$\tau_0 = \frac{1}{n\, L_{nn}} \qquad (1)$$

'n' is the quantity of devices in the graph and L_{nn} equals length of the link between two devices.

Local pheromone update:

$$\tau_{ij}(t+1) = (1-\rho).\tau_{ij}(t) + \rho.\tau_0 \qquad (2)$$

$\tau_{ij}(t)$ equals the quantity of pheromone at the edge (i, j) at period t; ρ is a parametric values controlling pheromone decay, ρ=0.1 which was adopted from best practices in the literature such that $0 < \rho < 1$; and τ_0 is the preliminary pheromone value on all edges.

Computation of edge attractiveness

$$\eta_{ij} = \frac{1}{d_{i,j}} \qquad (3)$$

Where d is the distance between nodes i and j.

Edge Probability Computation

$$P^k_{i,j}(t) = \frac{[\tau_{i,j}(t)]^{\alpha}[\eta_{i,j}]^{\beta}}{\sum_{i \epsilon J^k_i}[\tau_{i,j}(t)]^{\alpha} * [\eta_{i,j}]^{\beta}} \qquad (4)$$

α *and* β are two factors that govern the comparable importance of the pheromone trail. τ_{ij} equals the quantity of pheromone concentration on the connector between devices i and j. α= 2 and β=1 were taken from the literature, since $\alpha > 0$.

This subsection examines the process of determining an alternate route to the failed devices in Figure 5. Figure 7 depicts the first and last two iterations to minimize space.

The model produced alternate solution network paths A –B – J –K – L – I – G – E through which voice packets will flow when nodes C & F are down. Table 2 displays the probability distributions of selected nodes.

4.2.2 The Bandwidth Needed for Voice Message Transmission

Throughput can be used to find the minimum bandwidth needed to transfer a message [27], as shown in equation 5.

$$B_{Req} = \frac{W}{D} \qquad [5]$$

The equation is used to determine the bandwidth needed between two points that are linked. W denotes the capacity of a packet to be transmitted, and D denotes the message delay. Then, for the bandwidth, needed which should consist of two or more devices is determined as in equation 6.

$$B_{Req} = \frac{W}{D\text{-}a} \qquad [6]$$

First Iteration: A is the starting state; B, J, and K are prospective states. At random, distances are generated.

Using equation 1:$\tau_0 = \frac{1}{n\,L_{nn}}$

For distance AB, $\tau_0 = \frac{1}{12*1}=0.08$

Local update

Using equation 2: $\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{AB}=(1-0.1)*0.08+0.1*0.08=0.08$

For distance AJ, $\tau_0 = \frac{1}{12*2}=0.04$

$\tau_{AJ}=(1-0.1)*0.04+0.1*0.04=0.04$

For distance AK, $\tau_0 = \frac{1}{12*2}=0.04$

$\tau_{AK}=(1-0.1)*0.04+0.1*0.04=0.04$

distance BH, $\tau_0 = \frac{1}{12*2}=0.04$

From equation 3

$\eta_{AB}=\frac{1}{1}=1.0$, $\eta_{AJ}=\frac{1}{2}=0.5$, $\eta_{AK}=\frac{1}{2}=0.5$

Using equation 4:

$w(A,B)=[\tau_{A,B}]^{\alpha}[\eta_{A,B}]^{\beta}=(0.08)^2(1)^1=0.0064$

$w(A,J)=[\tau_{A,J}]^{\alpha}[\eta_{A,J}]^{\beta}=(0.04)^2(0.5)^1=0.0008$

$w(A,K)=[\tau_{A,K}]^{\alpha}[\eta_{A,K}]^{\beta}=(0.04)^2(0.5)^1=0.0008$

Sum=0.0064+0.0008+0.0008=0.018, probability:

$P^k_{AB}=\frac{0.0064}{0.008}=0.8$, $P^k_{AJ}=\frac{0.0008}{0.008}=0.1$, $P^k_{AK}=\frac{0.008}{0.0084}=0.1$

Node B is chosen as the next node because it has the greatest chance.

2ND Iteration: Current state: B, Potential State: C, H, J

L_k=(B-C)=3,L_k=(B-H)=2, L_k=(B-J)=1

Using equation 1: For distance BC, $\tau_0 = \frac{1}{12*3}=0.03$,

For distance BJ, $\tau_0 = \frac{1}{12*1}=0.0833$

Local update

Using equation 2: $\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{BC}=(1-0.1)*0.03+0.1*0.03=0.03$

$\tau_{BH}=(1-0.1)*0.04+0.1*0.04=0.04$

$\tau_{BJ}=(1-0.1)*0.08+0.1*0.08=0.08$

Using equation 3:

$\eta_{BC}=\frac{1}{3}=0.3$ $\eta_{BH}=\frac{1}{2}=0.5$, $\eta_{BJ}=\frac{1}{1}=1.$

Using equation 4:

$w(B,C)=[\tau_{BC}]^{\alpha}[\eta_{BC}]^{\beta}=(0.03)^2(0.3)^1=0.00027$

$w(B,H)=[\tau_{BH}]^{\alpha}[\eta_{BH}]^{\beta}=(0.04)^2(0.5)^1=0.0008$

$w(B,J)=[\tau_{BJ}]^{\alpha}[\eta_{BJ}]^{\beta}=(0.08)^2(1)^1=0.0064$

Sum=0.00027+0.0008+0.0064=0.00747

Probabilities

$P^k_{BC}=\frac{0.00027}{0.00747}=0.36$, $P^k_{BH}=\frac{0.0008}{0.00747}=0.11$,

$P^k_{BJ}=\frac{0.0064}{0.00747}=0.86$

Device J is chosen as the next device because it stands greatest chance.

5th Iteration: Current state: L

Potential State: F, I

L_k=(L-F)=3 , L_k=(L-I)=1

Using equation 1: $\tau_0 = \frac{1}{n\,L_{nn}}$

For distance LF, $\tau_0 = \frac{1}{12*3}=0.03$,

distance LI, $\tau_0 = \frac{1}{12*1}=0.0833$

Local update

Consider equation 2: $\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{LF}=(1-0.1)*0.03+0.1*0.03=0.03$

$\tau_{LI}=(1-0.1)*0.08+0.1*0.08=0.08$

Using equation 3:

$\eta_{LF}=\frac{1}{3}=0.3$ $\eta_{LI}=\frac{1}{1}=1.$

Using equation 4:

$w(L,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.03)^2(0.3)^1=0.00027$

$w(L,I)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.08)^2(1)^1=0.0064$

Sum=0.00027+0.0064=0.00667

$P^k_{LF}=\frac{0.00027}{0.00667}=0.04$, $P^k_{LI}=\frac{0.0064}{0.00667}=0.96$

Node I is chosen as the next node because it has the greatest chance, and F is a failed node.

6th Iteration: Current state: I, Potential State: F, G

L_k=(I-F)=2 , L_k=(I-G)=1

Using equation 1: $\tau_0 = \frac{1}{n\,L_{nn}}$

For distance IF, $\tau_0 = \frac{1}{12*2}=0.08$, distance IH, $\tau_0 = \frac{1}{12*1}=0.08$

Equation 2 is used:

$\tau_{ij}(t)=(1-\rho).\tau_{ij}(t)+\rho.\tau_0$

$\tau_{IF}=(1-0.1)*0.08+0.1*0.03=0.08$

$\tau_{IG}=(1-0.1)*0.04+0.1*0.04=0.04$

Figure 7: The ACS computation for generating alternative paths.

Using equation 3: $\eta_{IF}=\frac{1}{2}=0.5$ $\eta_{IG}=\frac{1}{1}=1$ Equation 4 is used: $w(I,F)=[\tau_{LF}]^{\alpha}[\eta_{LF}]^{\beta}=(0.08)^2(0.5)^1=0.0032$ $w(I,G)=[\tau_{LI}]^{\alpha}[\eta_{LI}]^{\beta}=(0.04)^2(1)^1=0.0016$ Sum=0.0032+0.0016=0.0048	$P_{IF}^{k}=\frac{0.0032}{0.0048}=0.67$, $P_{IG}^{k}=\frac{0.0016}{0.0048}=0.33$ Because node F is a failed device, device G is selected as the next node and E as the target device. Routing path: A, B, J, K, L, I, G, E

Figure 7: The ACS computation for generating alternative paths continues.

Table2: A full cycle's probability has been updated.

Present State	A	B	C	J	K	L	I	G	E	
A	1.00	0.80	0.00	0.10	0.10	0.00	0.00	0.00	0.00	1ST Update
B	0.00	0.00	0.36	0.86	0.00	0.00	0.00	0.00	0.11	2ndUpdate
J	0.00	0.00	0.00	0.00	0.80	0.00	0.10	0.00	0.00	3rd Update
K	0.00	0.00	0.00	0.00	0.00	0.89	0.11	0.00	0.00	4th Update
L	0.00	0.00	0.00	0.00	0.00	0.00	0.96	0.00	0.00	5th Update
I	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.33	0.00	6th Update
G	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	7th ,,

E= closing state, and ant has traversed all states

When 'a' is the unidentified feature that depends on 'n' and 'I,' and 'n' is the quantity of devices and $I=\sum_n I_n$, is the total length of transmission path. $a=f(n, I)=\alpha n+\beta I$ [27].

This section calculates the bandwidth expected to transfer a packet over the alternate route shown in Figure 6. From equation 6: Assume that the packet capacity is 500bytes, the IP header equals 20 bytes, the real capacity of the packet= (500-20) Bytes=480 Bytes. The delay is computed by dividing the length of the links by the propagation speed. the time it takes the message to reach the first node is 5 seconds, and that there are 8 nodes in the path, the time it takes the message to move from sender to the receiver is=5×8=40 Sec.

From the path A-B-J-K-L-I-G-E,

Total distance= 1+1+1+1+1+1+1=7metres.

$\text{Speed}=\frac{7m}{40}=0.175m/s$

,

$$\text{Delay}=\frac{7m}{0.175m/s}=40s.$$

From equation $a=f(n, I)=\alpha n+\beta I$

$a=8+7=15$, α and β are assumed to be 1,

$B_{Req}=\frac{W}{D-a}=\frac{480}{40-15}=\frac{480}{25}=19.2$Bytes/s.

The bandwidth needed to transmit the message from transmitter A to receiver E on survival path A-B-J-K-L-I-G-E is 19.2Bytes/Sec. This is appropriate to be determined promptly to avoid unnecessary downtime on Africa network failures.

Comparison with other related works are discussed. Awoyemi and Alfa [36] suggested network recovery for next-generation technology and digital systems The authors investigate the most notable network restoration kinds and designs that have been or are being developed for current and next-generation devices and communication technologies, as well as their characteristics and capabilities. Noticeable observations on network recovery for next-generation computers and communication networks are made, and improvements and pragmatic adjustment recommendations are addressed. Finally, future work in developing network recovery models that meet the needs and characteristics of arising next generation

connectivity and data processing systems is suggested. Awoyemi and Alfa's work differs from ours because a model was proposed and implemented.

Mohammad [37] suggested a technique of distributing network capacity after recovery, with MPLS-TE networks employing various telecoms technologies to build backhaul networks. The next generation is depicted in this study by a message transfer network that provides distinct functionalities. The purpose of providing transfer functions in the next generation that used Multi-Protocol Label Switching (MPLS) devices; two major issues have been identified: multi - path data transfer and traffic transfer, which are the subjects of this study. As a result, this study presents a method to these two issues by using optimal solution processes to find the best route. Dijkstra and Bellman-Ford that is distinguished by an increased choice of a single fastest route between the transmitter and receiver, depending on many carefully chosen procedures to the most efficient use of network capacity. Attempting to solve data flows distribution issues in a network with a vast amount of nodes employing the salesman method or possessing NP-completeness results in substantial time lag, implying that the suggested solution is unsuitable for real world applications. As a result, other procedure rely on the use of disparate shortest route are needed for real world applications. By comparing Mohammed's work to ours, it is discovered that the ACS model suggested in our work generates an alternative path in real time, whereas Mohammed's method generates a time delay.

5. CONCLUSION

In this work we proposed a telecommunication network survivability model for African countries which government organizations and private telecommunication network providers can undertake in order to improve on services to subscribers, reduce network failure occurrence, improve business decision-making and customer relationship management. The study suggests the Ant Colony System Survivability model, which is centered on capacity effectiveness and quick recovery, by using the ACS model's analytical solution to resolve telecom network failures, as shown in figure 7. Anytime a failure occurs in the main route, the proposed model resolves failures by generating the alternative path, and the bandwidth required by the alternative path is determined.

The system could assist to survive possible network failures. Amongst others, the intergovernmental systems integration of this model was one of the recommended interventions, with this model put in place, periodic and prolonged telecommunication network failures, and the cost of restoring network failures will be minimized. It is suggested that the suggested Telecom network survival model, depicted in Figure 7, be used by Africa Telecom operators and PSTNs in various African countries to resolve both single and multiple failures.

It would be interesting to focus on other types of failures which are not addressed in this study in the future. More public and private sector research can also improve on the model used in this work.

References

[1] Sheng Huang, Ming Xia, Charles U. (2010). Martel, A Multistate Multipath Provisioning Scheme for Differentiated Failures in Telecom Mesh Networks, Journal of Lightwave technology, vol. 28, no. 11.

[2] Vasseur J. P., Pickavet M., and Demeester P. (2004). Network Recovery: Protection and Restoration of Optical ONET-SDH, IP, and MPLS. San Mateo, CA: Morgan Kaufmann.

[3] Kyle J. S. White, Dimitrios P. Pezaros, Christopher W Johnson. (2012). Increasing Resilience of ATM Networks using the Traffic Monitoring and Automated Anomaly Analysis, University of Glasgow, ATACCS.

[4] Adegoke A.S and Babalola I.T. (2011). "Quality of service analysis of GSM telephone system in Nigeria" American Journal of Scientific and Industrial Research.

[5] Guardian. http://www.guardian.co.uk/ (2010).

[6] Department of Homeland Security, Office of Inspector General. (2007). "Lessons Learned from the August 11, 2007, Network Outage at Los Angeles International Airport".

[7] ITPRO. http://www.itpro.co.uk/, (2006).

[8] Sheng Huang, Ming Xia,Charles U. Martel, and Biswanath Mukherjee. (2010). "A Multistate Multipath Provisioning Scheme for Differentiated Failures in Telecom Mesh Networks" Journal of Lightwave Technology, Vol. 28, No. 11.

[9] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano. (2009). "Assessing the vulnerability of the fiber infrastructure to disasters," presented at

the presented at the IEEE INFOCOM, Rio de Janeiro, Brazil.

[10] D. P. Onguetou and W. D. Grover (2008)., "A new insight and approach to node failure protection with ordinary p- cycles," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 5145–5149.

[11] Shu-Chuan Chu, Hsiang-Cheh Huang, John F. oddick and Jeng-Shyang Pan. (2011). "Overview of Algorithms for Swarm Intelligence" Springer-Verlag Berlin Heidelberg, page 28-41.

[12] Steve Esselaar, Alison Gillword, Christoph Stork. (2006) "Soth African Telecommunication Sector Performance Review", Link Centre Public Research Paper, No. 8.

[13] Fola Odufuwa, (2012). "A Supply and Demand Side Analysis of the ICT Sector", ICT Policy Action, Paper 6.

[14] Lena Wosinska. (2006). "Connection Availability in WDM Mesh Networks with Multiple Failures," ICTON.

[15] GSM World. (2006). GSM operators. coverage maps and roaming information, GSM World website.

[16] Q. Xin et al. (2005). "Impact of failure on interconnection networks for large storage systems". In the Proceedings of the 22th IEEE /13th NASA Goddard Conference, (MSST 2005), Monterey, CA.

[17] G. Siva Kumar, Dr. (2014). I. Santhiprabha, "Node failure Recovery in Wireless Sensor and Action Networks Using ALeDir Algorithm" International Journal of Eng. and General Science" Vol. 2, Issue 6.

[18] Lena Wosinska. (2006) "Connection Availability in WDM Mesh Networks with Multiple Failures" The Royal Institute of Technology KTH, School of Information and Communication Technology (ICT), ICTON.

[19] A. Srinivas and E. Modiano. (2003). Minimum energy disjoint path routing in wireless ad-hoc networks. In the proceedings of the 9th annual international conference on Mobile computing and networking (Mobicom 2003).

[20] S. Lee and M. Gerla.(2001). Split multipath routing with maximally disjoint paths in ad hoc networks. In proceedings of ICC 2001.

[21] R.S.K. Chang, et. Al., "A Multilayer Restoration Strategy for Reconfigurable Networks," in Proc. Of IEEE Infocom'94, pp. 1872- 1878.

[22] R. Pastor-Satorras and A. Vespignani, (2001). "Epidemic dynamics and endemic states in complex networks," Phys. Rev. E, vol. 63, no. 6.

[23] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot. (2004). Characterization of failures in an IP backbone. In Proc. of 23rd IEEE Conference on Computer Communication (INFOCOM'2004), pp. 2307–2317, Hong Kong.

[24] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot. (2004). Feasibility of IP restoration in a tier-1 backbone. IEEE Network, 18(2):13–19, March-April 2004.

[25] Demeester, P.; Gryseels, M.; Autenrieth, A.; Brianza, C.; Castagna, L.; Signorelli, G.; Clemenfe, R.; Ravera. (1999). Resilience in multilayer networks" IEEE Communications Magazine,Vol.37, no.8, pp.70-76.

[26] Bigos W, Cousin B, Gosselin S, Le Foll. (2007). "Survivable MPLS Over Optical Transport Networks: Cost and Resource Usage Analysis" Journal on Selected Areas in Communications, IEEE vol.25, no.5, June 2007.

[27] Alison Gillwald, Mpho Moyo. (2012). What is happening in ICT in South Africa, A supply and Demand side analysis of the ICT sector, Evidence for ICT Policy Action, Research Africa.

[28] A. H Azni, Rabiah Ahmad, Zul Azri Mohamad Noh, Farida Haznani and Najwa Hayaati. (2015). Systematic Review for Survivability in Manets. ScienceDirect, Procedia – Social and Behavioral Sciences 195(2015) 1872 – 1881.

[29] Qingliang Wang, LiFang Zhai, Zheng-Tao JIANG, Yunbing Hou. (2012). Progress and Research of Network System Survivability Scheme with Cooperative Information Management. Journal of Networks, Vol. 7, No. 10.

[30] Go Hasegawa, Masayuki Murata (2009). A New Method of Proactive Recovery Mechanism for Large Scale Network Failures. IEEE Xplore.

[31] A. Daniel, R. Singh, and J. Saini. (2011). "Performance of Routing Protocol for Ad Hoc Network Using Path Survivability Based on Load and Bandwidth Management under Back Pressure Technique," Int. J. Comput. Sci. Eng. Technol., vol. 1, no. 9, pp. 544–549.

[32] M. Lima and H. da Silva. (2008). "Survival multipath routing for MANETs," in IEEE Network Operations and Management Symposium, 2008. NOMS 2008., 2008, vol. 6, pp. 425–432.

[33] T. Wang, C. Huang, K. Xiang, and K. Zhou. (2010). "Survivability Evaluation for MANET Based on Path Reliability," in 2010 Second international Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 378–381.

[34] James, P. G Sterbenz et al (2010). Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. COMNET: Resilient and Survivable Networks.

[35] G. Siva Kumar, Dr. I. Santhiprabha. (2014). "Node failure Recovery in Wireless Sensor and Action Networks (WSAN) using ALeDir Algorithm" International Journal of Engineering and General Science" Vol. 2, Issue 6.

[36] B. S. Awoyemi ,1 A. S. Alfa,1,2 and B. T. Maharaj (2018). Network Restoration for Next-Generation Communication and Computing Networks. Journal of Computer Networks and Communications. Volume 2018, Article ID 4134878, 13 pages

[37] Mohammad Alhihi (2017).Method of Distribution Network Resources after Restoration, the Networks MPLS-TE Use of Various Telecommunications Technologies to Construct Backbone Networks. Int. J. Communications, Network and System Sciences, 2017, 10, 251-260

[38] A. A. Owoade and I. O. Osunmakinde. (2016). "Resilience and survivability of ATM node-node network failures using ant colony swarm intelligent modelling," in *Proceedings of 2016 SAI Computing Conference, SAI 2016*.