International Journal of Electronics Communication and Computer Engineering
Volume 8, Issue 2, ISSN (Online): 2249–071X

Automated Fault Detection and Identification System for Computer Networks

John-OtumuAdetokunboMacGregor
Information & Communication Technology Directorate
Ambrose Alli University,Ekpoma, Nigeria

Ojieabu Clement Eghosa
Department of Electrical/Electronic Engineering
Ambrose Alli University, Ekpoma, Nigeria

Abstract — **This paper examines challenges faced by network administrators with respect to detecting and identifying faulty network components like cables or nodes in a computer network environment. Several research works on techniques used in building fault detection and identification mechanisms for local area networks reviewed. Dependency matrix was used in designing and building the active probing station internal mechanism for the fault detection and identification. The proposed system was tested in a non-production computer network, and the test results revealed that the proposed system is able to detect and identify faulty node/link is 0.22 seconds based on the processor speed and memory capacity. The proposed system is recommended for usage in any local area network.**

Keywords — **Probing Station, Fault Detection, Identification, LAN, Dependency Matrix**

I. INTRODUCTION

Network fault detection mechanism is a system designed to actively or passively monitor targeted network system in order to look for signs of malfunctioning or failing behavior of network devices or components. In order for the fault detection mechanism to effectively and successfully manage or monitor a given computer network, a large number of data about the network devices needs to be continuously obtained and processed. According to [1, 2, 3, 4, and 5] data about the network devices can be acquired using diagnostic tools or could be gotten in form of network alarms [6, 7, 8, and 9].

Fault detection techniques or system is of two types: (a) Active system or probe-based system (b) passive system or alarm correlation-based system [10]. Both classes can address certain challenges in the network and also proffer alternative solutions to faulty situations.

Classification of Network Faults

Network fault detection systems rely solely on network alarms to decide the causes of component failure, and therefore classified network faults based on their time duration in the network into three categories [11].

(i) **Permanent faults:** are faults that exist in a computer network until they are fixed or repaired e.g. malfunctioning network interface cards (NIC), switch / hub, or broken network cable.
(ii) **Intermittent faults:** are faults that occur in the network in a discontinuous and periodic manner, which causes failure of current running processes.
(iii) **Transient faults:** are minor degradation in service often masked by management utilities.

II. LITERATURE REVIEW

Many techniques have been discussed in different literatures to detect faults in computer networks. The following are some reviewed literatures on different techniques for detecting and identifying faults in computer networks.

Network Fault Management Techniques

Network fault management system gathers data about a given network, and analyzes the data using different techniques to detect and identify faulty network component. This section discusses some well-known existing techniques using four key areas.

Artificial Intelligence (AI) Based Techniques

Studies by [12, 13 and 14] are of the opinion that expert system is one of the most commonly used fault management techniques. Expert system uses a rule-based method to mimic the human knowledge or thought process of an expert.

An expert system according to [12] consists of four loosely coupled components, namely:
(i) A monitor
(ii) A problem clearing advisor
(iii) A trouble ticket creation system, and
(iv) A collection of network databases

In [7] a Kohonen Self Organizing Map (SOM) neural network is trained for alarm clustering in computer network fault detection. The training process of neural network is to tune its weights which may take long sessions, and there are no particular rules to guide the selection of number of layers and the number of neurons in each layer.

Intelligent Probing-Based Techniques

A probe is usually a dedicated program or network application installed in one of the nodes in a computer network. This can sometimes be referred to as a probing station which is sent to examine a set of nodes in the network on a periodic basis.

A special matrix referred to as dependency matrix was used to construct probing station for locating faulty nodes in a computer network [1, 2 and 3] , but [10] developed a new intelligent probing model for reducing the total number of probes for detecting and identifying fault in a computer network using fuzzy constraint satisfaction problem (FCSP) technique. Their findings show that the model is effective and efficient in terms of fault detection and identification in computer networks.

Model-Based Technique

A model-based technique explains the physical and functional properties of the network component, which is an abstract model of a managed network. The model

works by gathering some input parameters from the network and then predicts the network performance. Network fault is detected if the observation obtained is at variance with the prediction.[15, 16, 17 and 18] used the finite state machine (FSM) model to achieve their fault detection schemes in a managed computer network. In the (FSM) model, the computer network, and its behaviors in terms of faults are represented as a set of states. The disadvantage of the state algorithm is that they do not require learning.

III. METHODOLOGY

We useda special matrix referred to as dependency matrix to design our proposed active probing station for locating faulty nodes in a computer network. Fault management has become a major issue in any communication network. This is due to the number of devices on the network and the cost of monitoring the devices status actively against the event of down time or component failure.

The main role of active fault management application is to ensure high availability of network and resources.

Our proposed fault mechanism approach includes the capability to automatically monitor nodes status in order to detect and identify faulty nodes in a computer network using probing-based technique.

A probe is a method of obtaining information about objects (O). We considered probe as a diagnostic software tool for testing objects in order to determine whether or not they are active or inactive. Thus a probe is regarded as a subset p⊆O.

The occurrence of a fault may affect some probes [2], while other probes may remain unaffected as the case may be.

A probe P is affected by a fault F if P tests any of the elements of F

i.e. there are some elements in F that are also in P:

A fault F affects a probe P if F∩P ≠ Ø

In a computer network under consideration, "objects" may be regarded as physical entities such as switches, computers and links.

Probes are sent from the machine in which the fault detection mechanism is installed, to other computers on the computer network; in order to test the availability and performance of the various computers.

A fault may occur, if a particular node or link is inactive or both the nodes and links are inactive.

Our proposed fault detection mechanism is modeled as follows:

S = N, L

Where S = Switch

N = Nodes (Computers)

L = Link (Wired)

The set of processing nodes is denoted as N = {n_1, n_2, n_3, n_4, n_5, …,n_n}, while the set of processing links is denoted as L = {l_1, l_2, l_3, l_4, l_5, …, l_n}

We assumed that there is a finite set (O) of objects which can exist in one of two states i.e. Node (N) and Link (L).

(N) => "Active" or "1" = {functioning correctly}

(N) => "Inactive" or "0"={Not functioning}

(L) => "Active" or "1" = {functioning correctly}

(L) => "Inactive" or "0" = {Not functioning}

A fault (F) can occur in either Node (N) or Link (L) or both the Node (N) and Link (L).

i.e. a fault can be in any subset of the following:

Fault (F) ⊆N i.e. {n_1, n_2, n_3, n_4, n_5, …,n_n}

Fault (F) ⊆L i.e. {l_1, l_2, l_3, l_4, l_5, …,l_n}

We introduced a dependency matrix approach to capture the relationship between faults and probes in order to detect and identify a faulty node as recommended by [1].

Given any set of faults F = {f_1, f_2, f_3, …,f_n} and

Probes P = {p_1, p_2, p_3, ….,p_n}

The dependency matrix $D_{P,F}$ is given by:

$$D_{P,F}(i,j) = \begin{cases} 1 \text{ iffault } Fj \text{ affectsprobe } Pi \\ 0 \text{ if otherwise} \end{cases}$$

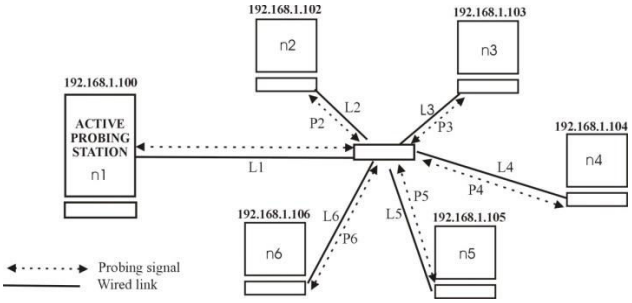

Figure 1: Active probing station for fault detection

Figure 1 shows the diagram of our proposed active probing station for fault detection and identification in a computer network. The active probing station is designed to continuously send diagnostic command to all the profiled computers or nodes on the network and also receive the nodes health status if available and active back to the active probing station using the ping command.

The fault mechanism is also designed with some reasoning ability using rule-based technique to classify the return message from the ping command as node status "inactive" if the computer or node is down by producing a **signal "0"** or node status "active" if the computer or node is on by producing a **signal "1"**.

```
Active probing(192.168.1.100)>ping 192.168.1.102 -t
Active probing(192.168.1.100)>ping 192.168.1.103 -t
Active probing(192.168.1.100)>ping 192.168.1.104 -t
Active probing(192.168.1.100)>ping 192.168.1.105 -t
Active probing(192.168.1.100)>ping 192.168.1.106 -t
Active probing(192.168.1.100)>ping 192.168.1.107 -t
Active probing(192.168.1.100)>ping 192.168.1.108 -t
Active probing(192.168.1.100)>ping 192.168.1.109 -t
Active probing(192.168.1.100)>ping 192.168.1.110 -t
```

Figure 2: Internal active probing mechanism

Figure 2 shows the internal fault active probing mechanism using the low level ping diagnostic tool. Here, the ip_address 192.168.1.100 is the resident server machine, which continuously and automatically pings all the profiled nodes on the network with ip_addresses 192.168.1.102 – 192.168.1.110.

Immediately any of the nodes is turned off or the network cable is pulled off the node's port or switch port; the diagnostic ping tool automatically returns a zero function call indicating node is down, and the fault agent will interpret the zero code to be node inactive and quickly flag a message "fault detected" with the exact node information displayed "node name, ip address, mac address and system name".

IV. System Testing

The proposed active probing station experiment was conducted and tested on a non-production computer network of about eight (8) systems. The system processor and memory capacity specifications are revealed in Table 1.

Table 1: System specifications

S/No	Processor	Memory	Quantity
1	Intel Core i7	4GB	1
2	Intel Core i3	4GB	1
3	Intel Core i3	2GB	1
4	Intel Duo Core	2GB	3
5	Pentium IV	2GB	2

V. Performance Evaluation

In evaluating the performance of our proposed fault detection and identification mechanism, we mainly concentrated on the Detection Time (DT).

The system performance in terms of time it takes to detect a faulty link or node and the mean time of notifying or reporting the node to be inactive through the screen alert message to the network administrator is considered.

We found out that the mean time for our proposed system to report a faultoccurrence in a near real-time situation on the screen is about 0.32 seconds on a system with Intel Core i3 processor with 4 GB memory space as compared to a mean time of 0.22 seconds on a system with Intel Core i7 processor with 4 GB memory space.

It therefore reveals that, the higher the system specifications in terms of processor speed and memory capacity, the shorter in time (seconds) it will take the detection mechanism to analyze, detect and report fault occurrence.

VI. Conclusion

The problem of effective network management is quite an interesting and challenging. Several research works on network management viz-a-viz fault detection and localization were reviewed in order to really address the challenges in designing the detection and identification mechanism in a LAN environment with respect to node active status or LAN connection.

Dependency matrix technique was used in the building the active probing station mechanism for detecting and locating faulty nodes / links in a Local Area Network. Results revealed that there is a high performance detection rate, but the detection time is based on the speed of the microprocessor and memory installed on the computer system used as the active probing station.

References

[1] Brodie, M., and Rish, S. (2001). *Optimizing probe selection for fault localization*, In 12th International Workshop on Distributed Systems Operations Management.

[2] Brodie, M., Rish, S., Odintsova, N., Beygelzimer, A., Grabarnik, G., and Hernandez, K. (2002). Adaptive diagnosis in distributed systems, Technical Report International Business Machine.

[3] Natu, M., and Sethi, A. S. (2006). *Active probing approach for fault localization in computer network*, In E2EMON' 06, Vancouver, Canada.

[4] Natu, M., and Sethi, A. S. (2007). *Efficient probing techniques for fault diagnosis*.2nd International Conference on Internet Monitoring and Protection, IEEE.

[5] Hernandez, K., Brodie, M., Rish, S., Odintsova, N., Beygelzimer, A., and Grabarnik, G.(2002). Adaptive diagnosis in distributed systems, Technical Report International Business Machine.

[6] Yemini, S. A., Kliger, S., Mozes, E., Yemini, Y., and Ohsie, D. (1996). *High speed and robust event correlation*, IEEE Communications Magazine.

[7] Gardner, R., and Harle, D. (1997). *Alarm correlation and network fault resolution using Kohonen Self Organizing Map*, Globecom '97 Proceeding.

[8] Bouloutas, A. T., Hart, G. W., and Shwartz, M. (1993). Fault identification using a FSM model with unreliable partially observed data sequence, IEEE Transactions on Communications.

[9] Wang, C., and Schwartz, M. (1993). *Identification of faulty links in dynamic-routed networks*, IEEE Journal on Selected Areas in Communications.

[10] Mohamed, A. A., and Bashir, O. (2009). *A New Probing Scheme for Fault Detection and Identification*, IEEE Conference proceedings. pp. 90-95

[11] Wang, Z. (1989). *Model of network faults, Integrated Network Management*, North-Holland, Amsterdam

[12] Rabie, S., Rau-Chaplin, D., and Shibahara, T. (1988). *DAD: a real-time expert system for monitoring of data packet networks*, IEEE Network.

[13] Marques, T. E. (1989). *A symptom-driven expert system for isolating and Correcting network faults.*In Expert System Applications in Integrated Network Management (E. C. Ericson, L.T. Ericson, and Minoli, eds.), Artech Mouse.

[14] Fuller, W. (1999) *Network management using expert diagnostics*, International Journal of Network Management.

[15] Chao, C., Yang, D., and Liu, A. (2001). *A LAN fault diagnosis system*, Computer Communications 24 (14), pp. 1439-1451, Elsevier Science B. V., 2001.

[16] Rouvellou, I., and Hart, G. (1995) *Automatic alarm correlation for fault identification*, Proceedings. IEEE INFOCOM 95, the Conference on Computer Communications.

[17] Wang, C., and Schwartz, M. (1993). *Identification of faulty links in dynamic-routed networks*, IEEE Journal on Selected Areas in Communications.

[18] Li, C. S., and Ramaswami, R. (1995). *Fault detection and isolation in transparent all-optical networks*, IBM research report, RC-220028.

Authors' Profile

John-OtumuAdetokunbois a member of the Nigeria Computer Society (NCS) and a Chartered Information Technology Professional, registered with the Computer Professionals Registration Council of Nigeria (CPN), currently pursuing Ph.D in Computer Science at Ebonyi State University, Abakaliki, Nigeria. He obtained his M.Sc(Info Tech) from National Open University of Nigeria and M.Sc (Computer Science) from Ambrose Alli University, Ekpoma, Nigeria. He is a Senior Technical Officer at the Directorate of Information and

Communication Technology. His research interest includes Computer communication systems, Agent computing and Multi-agent based systems, Network security, Software engineering and Soft computing. He has published over 15 articles in both local and international Journals.
E-mail:*macgregor.otumu@gmail.com*

Engr. (Dr.) Ojieabu Clement Eghosais a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). He has Ph.D in Communication Engineering, M. Eng in Electronic & Telecommunication Engineering and B.Eng in Electrical/Electronic Engineering. He is an Associate Professor of Communication Engineering at the Department of Electrical/Electronic Engineering, Ambrose Alli University, Ekpoma. His research interest includes Computer networks and security, intelligent systems, and satellite communication systems. He has published over 30 articles in both local/international journals and conference proceedings.
E-mail:*bishopeghosa@yahoo.ca*