Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.4 Issue 2 (2018) 26 - 32. Submitted 25/04/2018. Published 27/06/2018

Electronic Error Exposure and Recognition System for Computer Networks

R.Venkatesh, N.Khadar Basha
Department of Electronics and Communications Engineering
Dhanalakshmi Srinivasan Engineering College, Tamil Nadu, India

Abstract — This paper examines challenges faced with the aid of network directors with appreciate to detecting and identifying misguided network elements like cables or nodes in a pc network environment. Several lookup works on methods used in constructing fault detection and identification mechanisms for neighborhood location networks reviewed. Dependency matrix was used in designing and building the lively probing station interior mechanism for the fault detection and identification. The proposed device used to be examined in a nonproduction computer network, and the test outcomes published that the proposed device is able to become aware of and perceive inaccurate node/link is 0.22 seconds based on the processor pace and reminiscence capacity. The proposed machine is endorsed for usage in any local vicinity network.

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

I. INTRODUCTION

Network fault detection mechanism is a device designed to actively or passively reveal centered network gadget in order to appear for symptoms of malfunctioning or failing behavior of community gadgets or components. In order for the fault detection mechanism to effectively and efficaciously manipulate or screen a given laptop network, a giant range of facts about the community gadgets needs to be consistently got and processed. According to [1, 2, 3, 4, and 5] statistics about the community gadgets can be received the usage of diagnostic tools or ought to be gotten in form of community alarms [6, 7, 8, and 9]. Fault detection strategies or system is of two types: (a) Active system or probe-based gadget (b) passive machine or alarm correlation-based device [10]. Both instructions can address positive challenges in the network and additionally proffer alternative options to faulty situations. Classification of Network Faults Network fault detection structures depend entirely on community alarms to figure out the motives of issue failure, and therefore categorized network faults based totally on their time length in the network into three categories [11]. (i) Permanent faults: are faults that exist in a pc network until they are constant or repaired e.g. malfunctioning community interface cards (NIC), swap / hub, or broken network cable. (ii) Intermittent faults: are faults that happen in the community in a discontinuous and periodic manner, which motives failure of present day strolling processes. (iii) Transient faults: are minor degradation in carrier frequently masked by way of management utilities.

II. LITERATURE REVIEW

Many strategies have been mentioned in different literatures to realize faults in laptop networks. The following are some reviewed literatures on one of a kind techniques for detecting and figuring out faults in pc networks. Network Fault Management Techniques Network fault

administration machine gathers data about a given network, and analyzes the statistics the use of distinctive techniques to detect and become aware of erroneous network component. This area discusses some universal existing techniques using 4 key areas. Artificial Intelligence (AI) Based Techniques Studies with the aid of [12, 13 and 14] are of the opinion that professional machine is one of the most often used fault management techniques. Expert gadget uses a rule-based approach to mimic the human expertise or idea manner of an expert.

An specialist device in accordance to [12] consists of 4 loosely coupled components, namely:

(i) A monitor

(ii) A problem clearing advisor

(iii) A hassle ticket introduction system, and

(iv) A collection of network databases

In [7] a Kohonen Self Organizing Map (SOM) neural community is educated for alarm clustering in computer community fault detection. The coaching technique of neural community is to tune its weights which might also take long sessions, and there are no unique guidelines to guide the determination of variety of layers and the range of neurons in every layer.

Intelligent Probing-Based Techniques

A probe is usually a devoted application or network application hooked up in one of the nodes in a pc network. This can sometimes be referred to as a probing station which is despatched to observe a set of nodes in the community on a periodic basis.

A one of a kind matrix referred to as dependency matrix was once used to construct probing station for finding faulty nodes in a laptop network [1, 2 and 3] , but [10] developed a new smart probing model for lowering the whole number of probes for detecting and figuring out fault in a computer community the usage of fuzzy constraint delight problem (FCSP) technique. Their findings show that the mannequin is superb and environment friendly in terms of fault detection and identification in laptop networks.

Model-Based Technique

A model-based approach explains the physical and purposeful properties of the community component, which is an abstract model of a managed network. The model works by gathering some enter parameters from the network and then predicts the community performance. Network fault is detected if the observation acquired is at variance with the prediction.[15, 16, 17 and 18] used the finite state computing device (FSM) mannequin to obtain their fault detection schemes in a managed laptop 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 nation algorithm is that they do no longer require learning.

III. METHODOLOGY

We useda different matrix referred to as a dependency matrix to diagram our proposed lively probing station for locating inaccurate nodes in a pc network. Fault management has grow to be a primary trouble in any communication network. This is due to the range of units on the community and the price of monitoring the device's fame actively against the tournament of down time or factor failure.

The major position of energetic fault management utility is to make certain high availability of community and resources. Our proposed fault mechanism method consists of the functionality to robotically monitor nodes popularity in order to discover and perceive inaccurate nodes in a pc network the usage of probing-based technique. A probe is a approach of acquiring facts about objects (O). We considered probe as a diagnostic software tool for trying out objects in order to decide whether or no longer they are active or inactive. Thus a probe is viewed as a subset $p \subseteq O$. The occurrence of a fault may affect some probes [2], while different probes may additionally stay unaffected as the case can also be.

A probe P is affected through a fault F if P exams any of the factors of F
i.e. there are some elements in F that are also in P:
A fault F affects a probe P if $F \cap P \neq \emptyset$
In a computer community underneath consideration, “objects” may also be considered as bodily entities such as switches, computers, and links.

Probes are despatched from the computer in which the fault detection mechanism is established to other computers on the computer network; in order to check the availability and overall performance of the various computers.

A fault might also occur, if a particular node or link is inactive or both the nodes and hyperlinks 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 = {n1, n2,n3, n4, n5, …,nn}, whilst the set of processing hyperlinks is denoted as L = {l1, l2, l3, l4, l5, …, ln}. 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 manifest in both 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. {n1, n2, n3, n4, n5, …,nn}

Fault (F) ⊆L i.e. {l1, l2, l3, l4, l5, …,ln}
We introduced a dependency matrix strategy to seize the relationship between faults and probes in order to observe and discover a erroneous node as encouraged via [1]. Given any set of faults F = {f1, f2, f3, …,fn} and
Probes P = {p1, p2, p3, ….,pn}
The dependency matrix DP, F is given by: DP, F(i, j)= {1 iffault *F*j impacts probe *P*i zero if in any other case

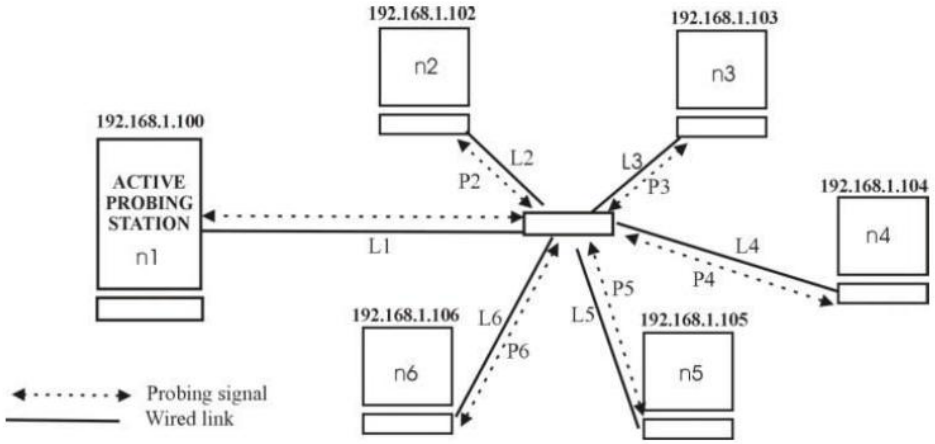

Figure 1:Active probing station for fault detection

Figure 1 suggests the graph of our proposed active probing station for fault detection and identification in a pc network. The energetic probing station is designed to consistently ship diagnostic command to all the profiled computer systems or nodes on the community and additionally receive the nodes health popularity if reachable and active again to the active probing station the use of the ping command. The fault mechanism is also designed with some reasoning ability the use of rule-based approach to classify the return message from the ping command as node reputation "inactive" if the laptop or node is down by way of producing a signal "0" or node reputation "active" if the laptop or node is on by way of 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 indicates the interior fault lively probing mechanism the use of the low degree ping diagnostic tool. Here, the ip_address 192.168.1.100 is the resident server machine, which always and routinely pings all the profiled nodes on the community with ip_addresses 192.168.1.102 – 192.168.1.110.

Immediately any of the nodes is grew to become off or the community cable is pulled off the node's port or swap port; the diagnostic ping device robotically returns a zero feature name indicating node is down, and the fault agent will interpret the zero code to be node inactive and shortly flag a message "fault detected" with the specific node information displayed "node name, ip address, mac tackle and device name".

IV. SYSTEM TESTING

The proposed active probing station experiment used to be conducted and tested on a non-production pc network of about eight (8) systems. The machine processor and reminiscence potential 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 mostly targeted on the Detection Time (DT). The system performance in phrases of time it takes to discover a erroneous hyperlink or node and the mean time of notifying or reporting the node to be inactive via the screen alert message to the network administrator is considered. We found out that the mean time for our proposed device to file a fault incidence in a near real-time state of affairs on the display screen is about 0.32 seconds on a system with Intel Core i3 processor with four GB reminiscence area as compared to a suggest time of 0.22 seconds on a gadget with Intel Core i7 processor with 4 GB memory space. It, therefore, reveals that the greater the gadget specifications in terms of processor velocity and memory capacity, the shorter in time (seconds) it will take the detection mechanism to analyze, realize and file fault occurrence.

VI. CONCLUSION

The trouble of effective community management is quite interesting and challenging. Several lookup works on network management viz-a-viz fault detection and localization were reviewed in order to virtually tackle the challenges in designing the detection and identification mechanism in a LAN surroundings with appreciate to node energetic repute or LAN connection. Dependency matrix approach was used in the building the lively probing station mechanism for detecting and locating faulty nodes/links in a Local Area Network. Results printed that there is a

high-performance detection rate, however the detection time is based on the velocity of the microprocessor and memory hooked up on the laptop machine used as the lively probing station.

REFERENCES

[1] Brodie, Mark, Irina Rish, and Sheng Ma. "Optimizing probe selection for fault localization." (2001).
[2] Khanna, Gunjan, et al. "Distributed diagnosis of failures in a three tier e-commerce system." Reliable Distributed Systems, 2007. SRDS 2007. 26th IEEE International Symposium on. IEEE, 2007.
[3] Natu, Maitreya, and Adarshpal S. Sethi. "Active probing approach for fault localization in computer networks." End-to-End Monitoring Techniques and Services, 2006 4th IEEE/IFIP Workshop on. IEEE, 2006.
[4] Natu, Maitreya, and Adarshpal S. Sethi. "Efficient probing techniques for fault diagnosis." null. IEEE, 2007.
[5] Khanna, Gunjan, et al. "Distributed diagnosis of failures in a three tier e-commerce system." Reliable Distributed Systems, 2007. SRDS 2007. 26th IEEE International Symposium on. IEEE, 2007.
[6] Yemini, Shaula Alexander, et al. "High speed and robust event correlation." IEEE communications Magazine 34.5 (1996): 82-90.
[7] Gardner, Robert D., and David A. Harle. "Alarm correlation and network fault resolution using the Kohonen self-organising map." Global Telecommunications Conference, 1997. GLOBECOM'97., IEEE. Vol. 3. IEEE, 1997.
[8] Bouloutas, Anastasios T., George W. Hart, and Mischa Schwartz. "Fault identification using a finite state machine model with unreliable partially observed data sequences." IEEE Transactions on Communications 41.7 (1993): 1074-1083.
[9] Wang, Clark, and Mischa Schwartz. "Identification of faulty links in dynamic-routed networks." IEEE Journal on selected Areas in Communications 11.9 (1993): 1449-1460.
[10] Andre O., Marc Paye, and Howard I. Maibach. Handbook of cosmetic science and technology. CRC Press, 2014.
[11] Deng, Robert H., Aurel A. Lazar, and Weiguo Wang. "A probabilistic approach to fault diagnosis in linear lightwave networks." IEEE Journal on selected areas in communications 11.9 (1993): 1438-1448.
[12] abie, Sameh, Andrew Rau-Chaplin, and Taro Shibahara. "DAD: a real-time expert system for monitoring of data packet networks." IEEE Network 2.5 (1988): 29-34.
[13] Marques, Todd E. "A symptom-driven expert system for isolating and correcting network faults." IEEE Communications Magazine 26.3 (1988): 6-13.
[14] Fuller, Wayne. "Network management using expert diagnostics." International Journal of Network Management 9.4 (1999): 199-208.
[15] Chao, Chi-Shih, Don-Ling Yang, and An-Chi Liu. "A LAN fault diagnosis system." Computer Communications 24.14 (2001): 1439-1451.
[16] Rouvellou, Isabelle, and George W. Hart. "Automatic alarm correlation for fault identification." INFOCOM'95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People. Proceedings. IEEE. Vol. 2. IEEE, 1995.

[17] Wang, Clark, and Mischa Schwartz. "Identification of faulty links in dynamic-routed networks." IEEE Journal on selected Areas in Communications 11.9 (1993): 1449-1460.
[18] Mohamed, Abduljalil A., and Otman Basir. "An adaptive multi-agent approach for distributed alarm correlation and fault identification." Proceedings of the 9th IASTED International Conference. Vol. 676. No. 072. 2010.