A Survey on the Capacity of Network in Locating the Node Failures through End-To-End Path Measurements

Almas K A
M. Tech, Department of CSE, CBIT.
Visvesvaraya Technological University
CBIT, Kolar, Karnataka, India
almaska786@gmail.com

Subhashini R
Assistant Professor, Department of CSE, CBIT.
Visvesvaraya Technological University
CBIT, Kolar, Karnataka, India
subashini050@gmail.com

Mohammed Jameel A Z
M. Tech, Department of CSE, TJIT.
Visvesvaraya Technological University
TJIT, Bengaluru, Karnataka, India
jameelzarzari@gmail.com

Abstract : The capability of confining the node failures in communication networks from the normal/failed states of the end-end paths is been investigated. If a set of nodes are given, confining the failures uniquely, not beyond the given set necessitates that the different visible path states must be associated with the different events of node failure. But, it is difficult to test this condition on larger networks because of the need to list all the possible node failures. The first endowment is a set of ample conditions to identify the number of failures within a random node set. Along with the topology of the network and monitors' locations, the limitations applied by the probing mechanism are also incorporated. Three probing techniques are considered. They are: 1) arbitrarily/randomly controllable; 2) controllable but cycle-free; or 3) uncontrollable (the default routing protocol determines it). Quantifying the potential of failure confinement is the second endowment done through: (i) the maximal failures in the network and; (ii) largest set of nodes inside which failures can be confined uniquely. Using the above ample conditions, the measures (i) & (ii), can be evaluated effectively by converting them into the functions of per-node property. How (i) and (ii) can be used to assess the impact of variety of parameter which includes topology, monitor numbers and probing techniques are demonstrated.

Key Words - Failure confinement, Network tomography, Identifiability condition, Maximum identifiability index.

1. INTRODUCTION

Monitoring of the performance of a network efficaciously is necessary for the operators of the network to build an unfailing communication network that are vigorous to service disturbances. For the sake of achieving this goal, it must be possible for the monitoring infrastructures to spot the misbehaviors in the network and to constrain the sources of the abnormality in a precise and prompt way. Awareness of the inhabitation of the controversial network elements in the network is especially useful for speedy recovery of the service. Anyhow, confining the elements of the network that induces the disturbances in the services can be tough. An effortless viewpoint of monitoring the individual elements' health directly is not always realistic because of the lack of ability of the protocols to exchange and use information. Furthermore, intrinsic monitoring techniques functioning on the elements of the network cannot recognize the difficulties resulting from incorrectly configured or abrupt network layer interactions, where end-to-end transmission is disturbed, but distinctive network elements through the path continue to be working, known as *silent failures* [1]. These restraints call for a disparate way that can identify the network elements' health from the health of the end-to-end communications interpreted amidst the measurement points.

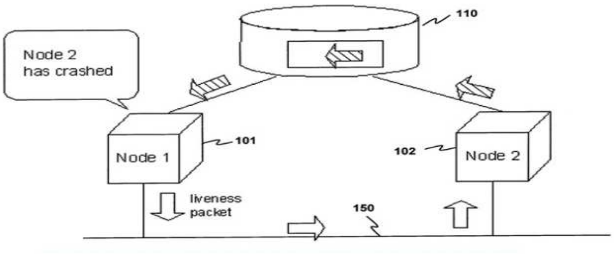

Figure 1: The system structure on locating the node failure.

Network Tomography [2] is one such method, which aims on deducing the internal characteristics of the network, contingent on the measurement of end-end performance from the *monitors.* These are the nodes with the capability to monitor the network. Network tomography depends upon the path connectivity i.e., end-end performance encountered by data packets, different from direct measurement. Hence, it tackles situations like running costs, silent failures, and absence of protocol support. Advancement to the network tomography is the *Boolean network tomography* [3]. In this technique, the interested features are in binary form (i.e., *normal* or *failed*).

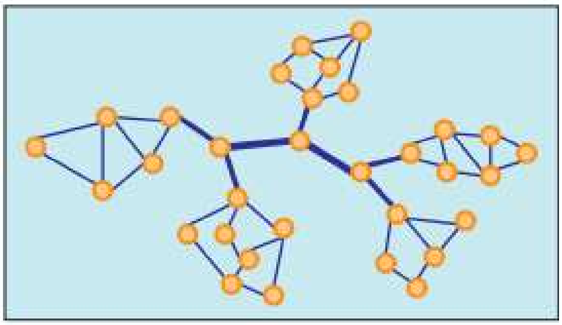

Figure 2: Figure representing the arbitrary network topology. Nodes: Cluster of Computers/Routers Edges: Direct link between two nodes

In this paper, an application of boolean network tomography is studied. This is done to locate the failure of nodes by measuring the path states. By believing that we have a normal path of measurement, only when all the nodes in the path act in normal manner, the problem is put together as a set of Boolean equations. The binary states of nodes denote the unknown variables, and the measurement paths' states which are observed denote the constants that are known. Solving these set of Boolean equations is the objective of this technique.

Since, they are the grainy inspections, uniquely recognizing the state of nodes from path measurements normally becomes inconceivable. For instance, whenever two nodes in a measurement paths appear jointly, having a look on all of these path failures, we can only conclude that any one among or both of these nodes have failed but cannot exactly specify which node. Here, it lacks the consideration of properties like topology, placement of monitor,etc,. It will be feasible to locate the failures in the nodes in sub-networks uniquely even if an uncertainty exists in locating the failures covering the whole network.

Three closely related problems are considered in this paper. A set of nodes of curiosity be denoted by S.

1. Let k represent the bound on the number of simultaneous failures in the node, in what state can the failed nodes in S can be uniquely located?
2. Upto what extent of simultaneous failures in nodes can a failure in S be located uniquely?
3. If k binds the total no. of failures, what is the largest set of nodes in which we can uniquely locate the failures?

The above questions can be answered depending upon the computable paths, topology of the network, monitor positioning and probes' mechanism to route. There exists three probing techniques infer different control levels over probing packets directing and also are viable in different network layouts. These are,

i. Uncontrollable Probing
ii. Controllable Arbitrary-path Probing
iii. Controllable Simple-path Probing.

2. RELATED WORK

We can mainly categorize the existing work as single failure locating and multiple failure locating. It is assumed by the single failure location technique that the multiple failures occurring simultaneously are unimportant.

In [4], the techniques flexible with failures are developed by Bejarno and Rastogi to monitor the delays in links and Service Provider faults. Here, an attempt is made which is of two stages to reduce the costs of monitoring infrastructure and the extra traffic that is caused by the enquiry messages. In the first stage, the locations of the least monitoring station sets are computed to the extent that it covers all network links, even when link failures are present. In second stage, the smallest probe message set is computed which are circulated from the stations for measuring the delays in link and to segregate faults in network.

Horton and Lopez consider the mensurations utilizing the dispersed set of beacons. It is shown that enumerating the least no. of required points of measurement in a network is NP hard. Some inspections are launched which permits us to put forward a comparatively small prospect set of measurement points for the present topology of Internet [5].

Zarifzadeh, Gowdagere and Dovrolis in [6] locates the failures and also finds out the level of congestion. Good and bad links are distinguished in this framework and also an estimation of the range is inferred for every bad link's performance. A framework of Range tomography is applied on the two path performance metrics and an algorithm is proposed for every problem. This framework is applied on three operational networks. This allows finding out the position of the bad links. But in these works a fact that there is frequent occurrence of multiple failures is ignored.

In [7] Markopoulou, Iannaccone, Bhattacharya, Chuah and Diot analyze the updates of IS-IS routing from IP network of Sprint. This is done to distinguish failures that influence that connectivity in IP. First they categorize the failures on the basis of possible causes which may include activities of maintenance, problems related to routers and optical layers. It is indicated by the results that because of planned activities of maintenance 20% of failures occur, and 30% failures among the unplanned are by multiple links, a single link is affected by the 70% of failures at a time. The failures are classified based on the different causes. These classifications unveil the character and level of failures in backbones of today's IP. Overall, the formal case of locating the multiple failures is considered in this paper.

Locating the multiple failures faces innate unpredictability. Most of the existing systems use the approach of finding the least network elements set which addresses this unpredictability. By making use of this approach, Zeng, Kazemian, Varghese and McKeown in [8] propose Automatic Test Packet Generation approach. This approach is a process for testing and debugging networks. ATPG is utilized to produce the least test packets sets to employ every link present in the network or to employ each rule present in the network. But, it cannot detect the faults in performance or liveness of the packets. Also there is no guarantee of locating the failures uniquely.

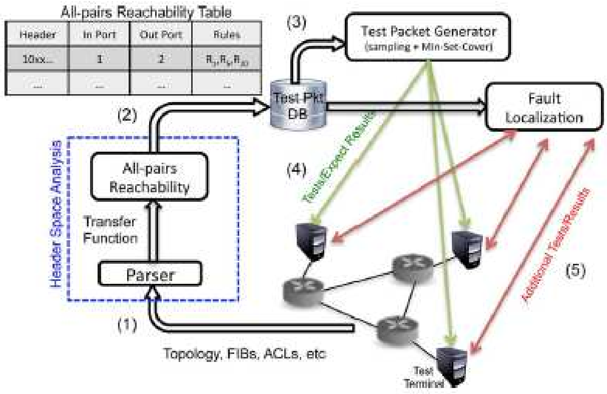

Figure 3: Block diagram of the ATPG System

In [9], a two-step explication is proposed by Nguyen and Thiran. In 1st step, the probability of failure of disparate links is estimated. Deducing the distinctively possible failure set for succeeding measurements will be the 2nd step. The authors of [10], A. Dhamdhere, R. Tiexeira, Dovrolis and Diot propose a troubleshooting algorithm. This is done to find out the failure locations in the environment of the internetworking. This algorithm makes use of the paths that are rerouted, the collected messages of route and LGs. The advantage of this is that small link sets can also be prosperously found out. The failed or misconfigured links are the one which are included in it.

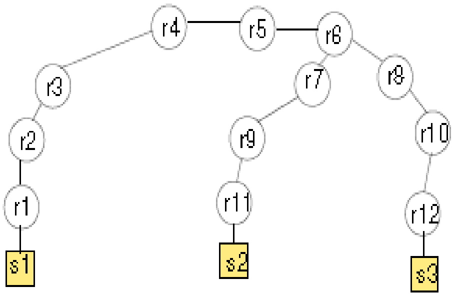

Figure 4: The Boolean Network Tomography

In [11], a concept of m-tours is introduced by Cho and Ramasubramaniam, to individually locate the failures possible in all the optical networks. Cycles and paths are established such that same link can be negotiated not more than two times. An ILP and greedy technique is introduced to find out the locations of the monitors. This is done to locate the failures uniquely. M-tours in a network are calculated using the heuristic scheme provided. The main focus of authors of this paper is, on the placement of monitors and the construction of measurement paths.

Arbitrary subset grouping of n-items into different pools is involved in uncharacterized group testing. A test is conducted on each pools and identification of the defective items occur. The least number of measuring paths are studied here, which are required to locate the node failures or the link failures uniquely under the CAP probing technique. But, in addition to this, our paper pursues in characterizing the failure type which can be located uniquely by the use of different probing techniques.

There are certain drawbacks in the existing works, such as the effortless proposal to directly monitor the network element's health is not practical everytime because of the absence of the protocol's ability to exchange and make use of information. Also, the problems induced due to the incorrect configuration or unexpected interactions within the elements of the network. Here, even though the communication between the end points is disturbed, the elements of the network will be working. There is no guarantee of determining which parts of the nodes have failed. Also, the confusion arises in locating the failures across the complete network.

To overcome these in the proposed work, the network's basic capacity with the monitors placed randomly are studied to locate the failures in the nodes uniquely. The proposed work contributes to the advancement in the form of four stages:

1) Two evaluations are proposed, (i) *maximum identifiability index* of the set of nodes, and (ii) *maximum identifiability set* for the upper bound stated on the no. of failures occurring concurrently. This is done to librate the capacity to locate the failures. These evaluations can be conveyed in the form of methods of maximum identifiablility index of every node.
2) Some required conditions are entrenched to uniquely locate the failures, which can be applied to all the probing techniques. Then, under three disparate probing techniques, these states are converted into more solid specifications regarding the topology of the network and monitor placement. This can be examined in polynomial time.
3) It is shown that a special bond that exists between the above constraints causing the tight bounds on the maximum identifiability index of a given set. Under the probing techniques of CAP and CSP, then bounds can be computed in polynomial time and they are NP-hard to be calculated in UP technique. Hence, a greedy method is presented to calculate the relaxed bound pair which habitually clash with the actual bounds.
4) The proposed estimations are evaluated using the different techniques to probe on both real as well as random topologies. Evaluation of the proposed work exhibits that controllable probing; particularly CAP technique of probing enhances the capacity of locating the node failure when compared to probing technique which cannot be controlled.

The advantage of using the probing techniques is that it believes in different control levels on the packets routing and are viable in variety of contexts in the network. It also delivers visions on the controlling level on the monitoring system influences the capacity of locating the failures.

3. CONCLUSIONS

The basic capacity of a network in locating the nodes that have failed from the normal/failed paths evaluation within the monitors is studied. All the existing works done in this field are studied and having a look on their disadvantages and making use of some of their advantages, they are compared to the newly derived work.

REFERENCES

[1] R. R Kompella, et.al., Detection and localization of network black holes," in *Proc. 26th IEEE INFOCOM*.

[2] A. Coates, Hero, Nowak, Yu, "Internet tomography", *IEEE Signal Process.*

[3] D. Ghita, et.al., "Shifting network tomography toward a practical goal," in *Proc. ACM*, 2011.

[4] Bejerano and Rastogi, "Robust monitoring of link delays and faults in IP networks," in *Proc. IEEE INFOCOM*,

[5] J. Horton and López-Ortiz, "On the number of distributed measurement points for network tomography," in *Proc. 3rd ACM IMC*.

[6] S. Zarifzadeh, et.al., "Range tomography: Combining the practicality of Boolean tomography" in *Proc. ACM IMC*.

[7] A. Markopoulou, Iannaccone, Bhattacharyya, Chuah, and C. Diot, "Characterization of failures in an IP backbone," in *Proc. IEEE INFOCOM*.

[8] H. Zeng, et.al., "ATPG," in *Proc. ACM.*

[9] Nguyen and P. Thiran, "The Boolean solution to the congested IP link location problem," in *Proc. IEEE INFOCOM*.

[10] A. Dhamdhere, et.al., "Netdiagnoser" in *Proc. ACM CoNEXT*

[11] S. Cho and Ramasubramanian, "Localizing link failures in optical networks using m-tours," *Comput. Netw.*, vol. 58.

[12] M. Cheraghchi, et.al., "Graph constrained group testing," *IEEE Trans*, vol. 58.