Network Capability in Localizing Node Failures via End-to-End Path Measurements

T Jayasree #1, V Venkata Rakesh Reddy #2, L Mohan Reddy #3, M Nagarjuna Reddy #4
#1 Associate Professor, #2,3,4 B.Tech, Scholars
Department of Computer Science and Engineering, QIS College of Engineering and Technology

Abstract:

We investigate the capability of localizing node failures in communication networks from binary states (normal/ failed) of end-to-end paths. Given a set of nodes of interest, uniquely localizing failures within this set requires that different observable path states associate with different node failure events. However, this condition is difficult to test on large networks due to the need to enumerate all possible node failures. Our first contribution is a set of sufficient/necessary conditions for identifying a bounded number of failures within an arbitrary node set that can be tested in polynomial time. In addition to network topology and locations of monitors, our conditions also incorporate constraints imposed by the probing mechanism used. We consider three probing mechanisms that differ according to whether measurement paths are (i) arbitrarily controllable, (ii) controllable but cycle-free, or (iii) uncontrollable (determined by the default routing protocol). Our second contribution is to quantify the capability of failure localization through (1) the maximum number of failures (anywhere in the network) such that failures within a given node set can be uniquely localized, and (2) the largest node set within which failures can be uniquely localized under a given bound on the total number of failures. Both measures in (1–2) can be converted into functions of a per-node property, which can be computed efficiently based on the above sufficient/necessary conditions. We demonstrate how measures (1–2) proposed for quantifying failure localization capability can be used to evaluate the impact of various parameters, including topology, number of monitors, and probing mechanisms.

1. Introduction

Effective monitoring of network performance is essential for network operators in building reliable communication networks that are robust to service disruptions. In order to achieve this goal, the monitoring infrastructure must be able to detect network misbehaviors (e.g., unusually high loss/latency, un reachability) and localize the sources of the anomaly (e.g., malfunction of certain routers) in an accurate and timely manner. Knowledge of where problematic network elements reside in the network is particularly useful for fast service recovery, e.g., the network operator can migrate affected services and/or reroute traffic. However, localizing network elements that cause a service disruption can be challenging.

The straightforward approach of directly monitoring the health of individual elements (e.g., by collecting topology update reports) is not always feasible due to the lack of protocol interoperability (e.g., in hybrid networks such as cellular wireless ad hoc networks), or limited access to network internal nodes (e.g., in multi-domain networks). Moreover, built-in monitoring mechanism running on network elements

cannot detect problems caused by misconfigured/unanticipated interactions between network layers, where end-to-end communication is disrupted but individual network elements along the path remain functional (i.e., silent failures) [1]. These limitations call for a different approach that can diagnose the health of network elements from the health of end-to-end communications perceived between measurement points.

One such approach, generally known as network tomography [2], focuses on inferring internal network characteristics based on end-to-end performance measurements from a subset of nodes with monitoring capabilities, referred to as monitors. Unlike direct measurement, network tomography only relies on end-to-end performance (e.g., path connectivity) experienced by data packets, thus addressing issues such as overhead, lack of protocol support, and silent failures. In cases where the network characteristic of interest is binary (e.g., normal or failed), this approach is known as Boolean network tomography [3]. In this paper, we study an application of Boolean network tomography to localize node failures from measurements of path states.1 Under the assumption that a measurement path is normal if and only if all nodes on this path behave normally, we formulate the problem as a system of Boolean equations, where the unknown variables are the binary node states, and the known constants are the observed states of measurement paths. The goal of Boolean network tomography is essentially to solve this system of Boolean equations. Because the observations are coarse-grained (path normal/ failed), it is usually impossible to uniquely identify node states from path measurements. For example, if two nodes always appear together in measurement paths, then upon observing failures of all these paths, we can at most deduce that one of these nodes (or both) has failed but cannot determine which one. Because there are often multiple explanations for given path failures, existing work mostly focuses on finding the minimum set of failed nodes that most probably involves failed nodes. Such an approach, however, does not guarantee that nodes in this minimum set have failed or that nodes outside the set have not. Generally, to distinguish between two possible failure sets, there must exist a measurement path that traverses one and only one of these two sets. There is, however, a lack of understanding of what this requires in terms of observable network properties such as topology, monitor placement, and measurement routing. On the other hand, even if there exists ambiguity in failure localization across the entire network, it is still possible to uniquely localize node failures in a specific sub-network (e.g., sub-network with a large fraction of monitors). To determine such unique failure localization in sub-networks, we need to understand how it is related to network properties.

In this paper, we consider three closely related problems: Let S denote a set of nodes of interest (i.e., there can be ambiguity in determining the states of nodes outside S; however, the states of nodes in S must be uniquely determinable). (1) If the number of simultaneous node failures is bounded by k, then under what conditions can one uniquely localize failed nodes in S from path measurements available in the entire network? (2) What is the maximum number of simultaneous node failures (i.e., the largest value of k) such that any failures within S can be uniquely localized? (3) What is the largest node set within which failures can be uniquely localized, if the total number of failures is bounded by k? Answers to questions (2) and (3) together quantify a network's capability to localize failures from end-to-end measurements: question (2) characterizes the scale of failures and question (3) the scope of localization. Clearly, answers to the above questions depend on which paths are measurable, which in turn depends on network topology, placement of monitors, and the routing mechanism of probes. We will study all these problems in the context of the following classes of probing mechanisms:

(i) Controllable Arbitrary-path Probing (CAP), where any measurement path can be set up by monitors

(ii) Controllable Simple-path Probing (CSP), where any measurement path can be set up, provided it is cycle-free

(iii) Uncontrollable Probing (UP), where measurement paths are determined by the default routing protocol. These probing mechanisms assume different levels of control over routing of probing packets and are feasible in different network scenarios (see Section II-C); answers to the above three problems under these probing mechanisms thus provide insights on how the level of control bestowed on the monitoring system affects its capability in failure localization.

2. Literature Survey

Node Failure Localization via Network Tomography

We investigate the problem of localizing node failures in a communication network from end-to-end path measurements, under the assumption that a path behaves normally if and only if it does not contain any failed nodes. To uniquely localize node failures, the measurement paths must show different symptoms under different failure events, i.e., for any two distinct sets of failed nodes, there must be a measurement path traversing one and only one of them. This condition is, however, impractical to test for large networks. Our first contribution is a characterization of this condition in terms of easily verifiable conditions on the network topology with given monitor placements under three families of probing mechanisms, which differ in whether measurement paths are (i) arbitrarily controllable, (ii) controllable but cycle-free, or (iii) uncontrollable (i.e., determined by the default routing protocol). Our second contribution is a characterization of the maximum identifiability of node failures, measured by the maximum number of simultaneous failures that can always be uniquely localized. Specifically, we bound the maximal identifiability from both the upper and the lower bounds which differ by at most one, and show that these bounds can be evaluated in polynomial time. Finally, we quantify the impact of the probing mechanism on the capability of node failure localization under different probing mechanisms on both random and real network topologies. We observe that despite a higher implementation cost, probing along controllable paths can significantly improve a network’s capability to localize simultaneous node failures.

Node failure localization via network tomography

We investigate the problem of localizing node failures in a communication network from end-to-end path measurements, under the assumption that a path behaves normally if and only if it does not contain any failed nodes. To uniquely localize node failures, the measurement paths must show different symptoms under different failure events, i.e., for any two distinct sets of failed nodes, there must be a measurement path traversing one and only one of them. This condition is, however, impractical to test for large networks. Our first contribution is a characterization of this condition in terms of easily verifiable conditions on the network topology with given monitor placements under three families of probing mechanisms, which differ in whether measurement paths are (i) arbitrarily controllable, (ii) controllable but cycle-free, or (iii) uncontrollable (i.e., determined by the default routing protocol). Our second contribution is a characterization of the maximum identifiability of node failures, measured by the maximum number of simultaneous failures that can always be uniquely localized. Specifically, we bound the maximal identifiability from both the upper and the lower bounds which differ by at most one, and show that these bounds can be evaluated in polynomial time. Finally, we quantify the impact of the probing mechanism on the capability of node failure localization under different probing mechanisms on both random and real network topologies. We observe that despite a higher implementation cost, probing along controllable paths can significantly improve a network's capability to localize simultaneous node failures.

Locating node failures via end-to-end path measurements in wireless sensor networks

We investigate the capability of localizing node failures in communication networks from binary states (normal/ failed) of end-to-end paths. Here we try to identify the nodes which are failed during data transmission by applying network monitoring technique and those nodes which are failed will be automatically identified by the group manager and they will be send from an alternate path to the destination Here we try to find out the end to end path measurements on the network once the data transfer is completed.

Efficient identification of node failure and recovery through end to end Probing techniques

Identification of Node failure detection and a localization is a very important challenge in a network community to get a quick recovery and avoid useless traffic in network. But it is very difficult to check the failure nodes or locations because of the large number of Screw ups in dense network. As finding the main source for failure of network is always challenging our proposed work will achieve that, it identifies the node failure by using probing measurement of binary state to end to end paths. Apart from identifying the network failure, it also quantifies the total failure nodes and the ip address or vicinity of failure nodes, Identification of node failure is done by monitoring nodes which are deployed in the netwok. Our Proposed word is divided majorly in two phases one is identifying the node failures by using Probing Packets and other is finding of the failure and its recovery.

3. System Study

Existing work can be broadly classified into single failure localization and multiple failure localization. Single failure localization assumes that multiple simultaneous failures happen with negligible probability. Under this assumption, [4], [5] propose efficient algorithms for monitor placement such that any single failure can be detected and localized. To improve the resolution in characterizing failures, range tomography in [6] not only localizes the failure, but also estimates its severity (e.g., congestion level). These works, however, ignore the fact that multiple failures occur more frequently than one may imagine [7]. In this paper, we consider the general case of localizing multiple failures.

Multiple failure localization faces inherent uncertainty. Most existing works address this uncertainty by attempting to find the minimum set of network elements whose failures explain the observed path states. Under the assumption that failures are low-probability events, this approach generates the most probable failure set among all possibilities. Using this approach, [8], [9] propose solutions for networks with tree topologies, which are later extended to general topologies in [1]. Similarly, [10] proposes to localize link failures by minimizing false positives; however, it cannot guarantee unique failure localization. In a Bayesian formulation, [11] proposes a two-stage solution which first estimates the failure (loss rate above threshold) probabilities of different links and then infers the most likely failure set for subsequent measurements. By augmenting path measurements with (partially) available control plane information (e.g., routing messages), [12], [13] propose a greedy heuristic for troubleshooting network unreachability in multi- AS (Autonomous System) networks that has better accuracy than benchmarks using only path measurements.

Proposed System:

In the proposed system, the system studies an application of Boolean network tomography to localize node failures from measurements of path states1. Under the assumption that a measurement path is normal if and only if all nodes on this path behave normally, we formulate the problem as a system of Boolean equations, where the unknown variables are the binary node states, and the known constants are the observed states of measurement paths. The goal of Boolean network tomography is essentially to solve this system of Boolean equations.

4. Implementation

Source

In this module, Source browse the file, select the destination and sends to the router. In Source while uploading the file, encrypt and then uploads the file. File content will be initialized to all the nodes.

Router

In this module, router consists of four Networks, each Network contains specific nodes. When Source sends the file initially it comes to the Network1 and passes through the Network1 nodes, if any congestion found in the Network1 node, It automatically selects the another node an moves to Network2 and Network 3 and Network4 and reaches the destination. The energy size also be modified, view the Network details. In router the routing path and time delay can be viewed.

Router Manager

In this module, ROUTER MANAGER views the attacker details by checking the energy details and find attackers.

Destination

In this module, Receiver request for file name and secret key and receives the content from the router. Time delay will be calculated by sending the file from source to destination and time taken to reach the destination.

Attacker

In this module, attacker selects the Network and node, gets the original energy size and modifies the energy size for the node.

5. Conclusion

We studied the fundamental capability of a network in localizing failed nodes from binary measurements (normal/failed) of paths between monitors. We proposed two novel measures: maximum identifiability index that quantifies the scale of uniquely localizable failures writ a given node set, and maximum identifiable set that quantifies the scope of unique localization under a given scale of failures. We showed that both measures are functions of the maximum identifiability index per node. We studied these measures for three types of probing mechanisms that offer different controllability of probes and complexity of implementation. For each probing mechanism, we established necessary/sufficient conditions for unique failure localization based on network topology, placement of monitors, constraints on measurement paths, and scale of failures. We further showed that these conditions lead to tight upper/lower bounds on the maximum identifiability index, as well as inner/outer bounds on the maximum identifiable set. We showed that both the conditions and the bounds can be evaluated efficiently using polynomial time algorithms. Our evaluations on random and real network topologies showed that probing mechanisms that allow monitors to control the routing of probes have significantly better capability to uniquely localize failures.

References

[1] R. R. Kompella, J. Yates, A. Greenberg, and A. C. Snoeren, “Detection and localization of network black holes,” in Proc. 26th IEEE INFOCOM, May 2007, pp. 2180–2188.

[2] A. Coates, A. O. Hero, III, R. Nowak, and B. Yu, “Internet tomography,” IEEE Signal Process. Mag., vol. 19, no. 3, pp. 47–65, May 2002.

[3] D. Ghita, C. Karakus, K. Argyraki, and P. Thiran, “Shifting network tomography toward a practical goal,” in Proc. ACM CoNEXT, 2011, Art. no. 24.

[4] Y. Bejerano and R. Rastogi, “Robust monitoring of link delays and faults in IP networks,” in Proc. 22nd IEEE INFOCOM, Mar./Apr. 2003, pp. 134–144.

[5] J. D. Horton and A. López-Ortiz, “On the number of distributed measurement points for network tomography,” in Proc. 3rd ACM IMC, 2003, pp. 204–209.

[6] S. Zarifzadeh, M. Gowdagere, and C. Dovrolis, “Range tomography: Combining the practicality of Boolean tomography with the resolution of analog tomography,” in Proc. ACM IMC, 2012, pp. 385–398.

[7] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, “Characterization of failures in an IP backbone,” in Proc. 23rd IEEE INFOCOM, Mar. 2004, pp. 2307–2317.

[8] N. Duffield, “Simple network performance tomography,” in Proc. 3rd ACM IMC, 2003, pp. 210–215.

[9] N. Duffield, “Network tomography of binary network performance characteristics,” IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5373–5388, Dec. 2006.

[10] H. Zeng, P. Kazemian, G. Varghese, and N. McKeown, “Automatic test packet generation,” in Proc. ACM CoNEXT, 2012, pp. 241–252.

[11] H. X. Nguyen and P. Thiran, “The Boolean solution to the congested IP link location problem: Theory and practice,” in Proc. 26th IEEE INFOCOM, May 2007, pp. 2117–2125.

[12] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot, “Netdiagnoser: Troubleshooting network unreachabilities using end-to-end probes and routing data,” in Proc. ACM CoNEXT, 2007, Art. no. 18.

[13] Y. Huang, N. Feamster, and R. Teixeira, “Practical issues with using network tomography for fault diagnosis,” ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 5, pp. 53–58, 2008.

[14] H. X. Nguyen and P. Thiran, “Active measurement for multiple link failures diagnosis in IP networks,” in Proc. 5th PAM, 2004, pp. 185–194.

[15] S. S. Ahuja, S. Ramasubramanian, and M. Krunz, “SRLG failure localization in all-optical networks using monitoring cycles and paths,” in Proc. 27th IEEE INFOCOM, Apr. 2008.

[16] S. Cho and S. Ramasubramanian, “Localizing link failures in all-optical networks using monitoring tours,” Comput. Netw., vol. 58, pp. 2–12, Jan. 2014.

[17] L. Ma, T. He, A. Swami, D. Towsley, K. K. Leung, and J. Lowe, “Node failure localization via network tomography,” in Proc. ACM IMC, 2014, pp. 195–208.

[18] M. Cheraghchi, A. Karbasi, S. Mohajer, and V. Saligrama, “Graphconstrained group testing,” IEEE Trans. Inf. Theory, vol. 58, no. 1, pp. 248–262, Jan. 2012.

[19] Internet Protocol DARPA Internet Program Protocol Specification, accessed on Sep. 1981. [Online]. Available: http://www.ietf.org/rfc/rfc0791.txt

[20] Open Networking Foundation, accessed on 2016. [Online]. Available: http://www.opennetworkingfoundation.org