International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 4, Issue 5 (October '2018)

NETWORK CAPABILITY IN LOCALIZING NODE FAILURES VIA END-TO-END PATH MEASUREMENTS

K.Vimala,
Assistant Professor,
Department of Computer Science,
Pavai Arts and Science College for Women,
Pachal, Namakkal,Tamilnadu.

R.Deepika,
Research Scholar,
Department of Computer Science,
Pavai Arts and Science College for Women,
Pachal, Namakkal,Tamilnadu.

Abstract: Our study 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.

***Keywords:* Computer Network ,Communication,Topology,LAN,WiFi**

I. INTRODUCTION

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered as a computer network. A **computer network** or **data network** is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other. Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology and organizational intent.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols.

The transmission media (often referred to in the literature as the *physical media*) used to link devices to form a computer network include electrical cable (Ethernet,HomePNA, power line communication, G.hn), optical fiber (fiber-optic communication), and radio waves (wireless networking). In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted *family* of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables. Wireless LAN standards (e.g. those defined by IEEE 802.11) use radio waves, or others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today.

A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. (Wi-fi.com)

An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface

card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software.

A wide variety of communication protocols exists. These protocols were defined by many different standard organizations throughout the world and by technology vendors over years of technology evolution and development. One of the most popular protocol suites is TCP/IP, which is the heart of Internetworking communications. The IP, the Internet Protocol, is responsible for exchanging information between routers so that the routers can select the proper path for network traffic, while TCP is responsible for ensuring the data packets are transmitted across the network reliably and error free. LAN and WAN protocols are also critical protocols in network communications. The LAN protocols suite is for the physical and data link layers of communications over various LAN media such as Ethernet wires and wireless radio waves. The WAN protocol suite is for the lowest three layers and defines communication over various wide-area media, such as fiber optic and copper cables.

The protocols for data communication cover all areas as defined in the OSI model. However, the OSI model is only loosely defined. A protocol may perform the functions of one or more of the OSI layers, which introduces complexity to understanding protocols relevant to the OSI 7 layer model. In real-world protocols, there is some argument as to where the distinctions between layers are drawn; there is no one black and white answer.

To develop a complete technology that is useful for the industry, very often a group of protocols is required in the same layer or across many different layers. Different protocols often describe different aspects of a single communication; taken together, these form a protocol suite. For example, Voice over IP (VOIP), a group of protocols developed by many vendors and standard organizations, has many protocols across the 4 top layers in the OSI model.

II. RELATED WORK

The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another.

The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.

Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved.
The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions. (Wi-fi.com)

On the other hand, many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed will be slowed.

III. PROBLEM STATEMENT

3.1 EXISTING MODEL

Existing approach, generally known as network tomography, 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

3.1.1 Drawbacks

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)Does not guarantee that nodes in this minimum set have failed or that nodes outside the set have not.There exists ambiguity in failure localization across the entire network.

3.2 PROPOSED SYSTEM

In this STUDY, we consider three closely related problems: (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

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, and (iii) Uncontrollable Probing (UP), where measurement paths are determined by the default routing protocol.

3.2.1 Advantages Of Proposed System

These probing mechanisms assume different levels of control over routing of probing packets and are feasible in different network scenarios.

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.

IV. METHODOLOGY

Network Topology

The network topology is known and models it as an undirected graph. The graph can represent a logical topology where each node in graph corresponds to a physical sub network. Without loss of generality, we assume graph is connected, as different connected components have to be monitored separately.

Monitors

A subset of nodes is monitors that can initiate and collect measurements. The rest of the nodes are non-monitors. We assume that monitors do not fail during the measurement process, as failed monitors can be directly detected and excluded (assuming centralized control within the monitoring system). Non-monitors, on the other hand, can fail, and a failure event may involve simultaneous failures of multiple non-monitors. Depending on the adopted probing mechanism, monitors measure the states of nodes by sending probes along certain paths.

Models and Assumptions

We assume that the network topology is known and model it as an undirected graph2 G = (V,L), where V and L are the sets of nodes and links. In G, the number of neighbors of node v is called the degree of v; $\xi := |L|$ denotes the number of links. Note that graph G can represent a logical topology where each node in G corresponds to a physical sub-network. Without loss of generality, we assume G is connected, as different connected components have to be monitored separately. A subset of nodes M ($M \subseteq V$) are monitors that can initiate and collect measurements. The rest of the nodes, denoted by $N := V \setminus M$, are non-monitors. Let $\mu := |M|$ and $\sigma := |N|$ denote the numbers of monitors and non-monitors.

Definitions

Let a failure set F be a set of non-monitors ($F \subseteq N$) that fail simultaneously. Note that the collection of all failure sets in a given network covers all possible failure scenarios (each corresponds to a failure set) that can occur in this network; the goal of failure localization is to infer the current failure set from the states of measurement paths. The challenge for this problem is that there may exist multiple failure sets leading to the same path states, causing ambiguity. Let PF denote the set of all measurement paths traversing at least one node in a failure set F. (i.e., PF contains all failed paths that are caused by node failures in F). To quantify the capability of uniquely determining the failure set, we introduce the following definitions.

5. SAMPLE SCREENSHOT

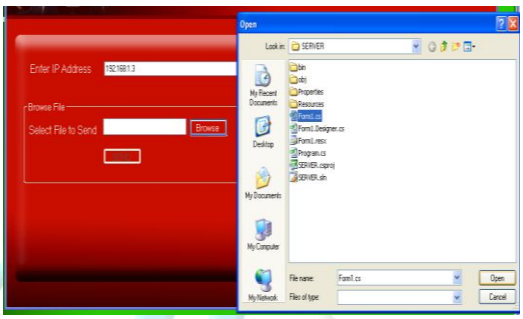

Fig 5.1 Source select file

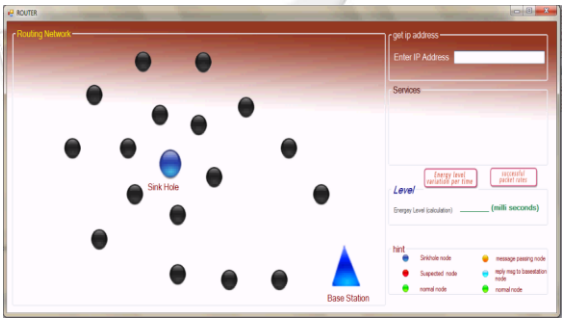

Fig 5.2 Routing Network

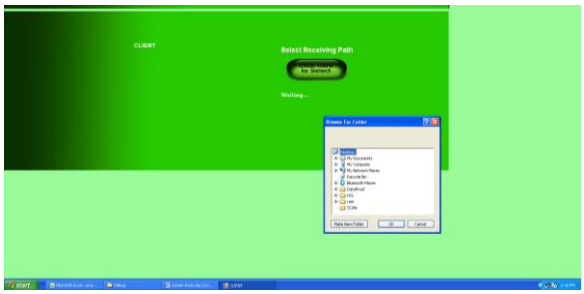

Fig 5.3 Client Node

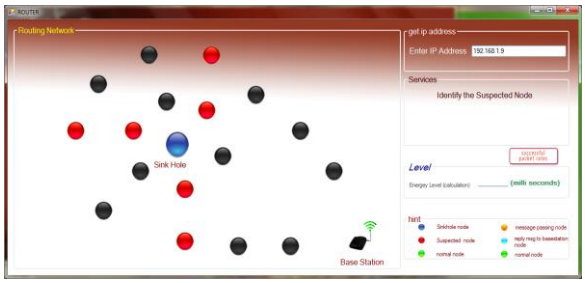

Fig 5.4 Identified Failure Nodes End to End Path.

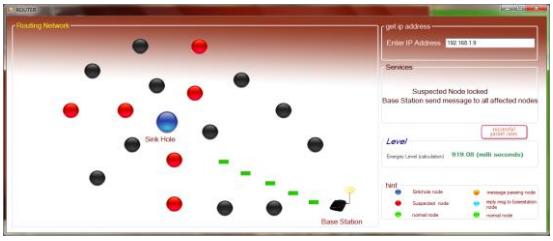

Fig 5.5 Identified signal from Base Station

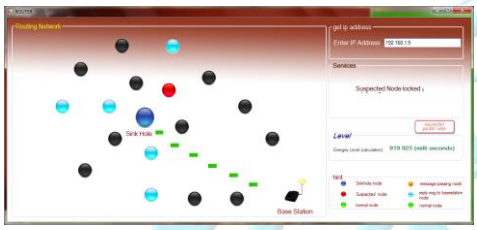

Fig 5.6 Reply Message to Base Station node

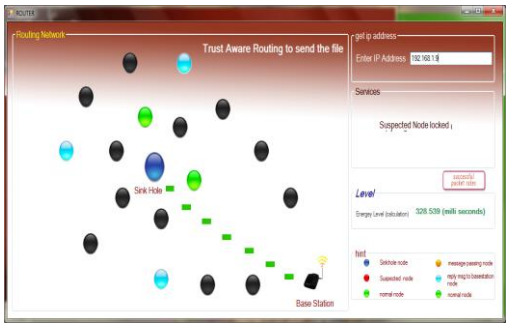

Fig 5.7 Failure Node Locked

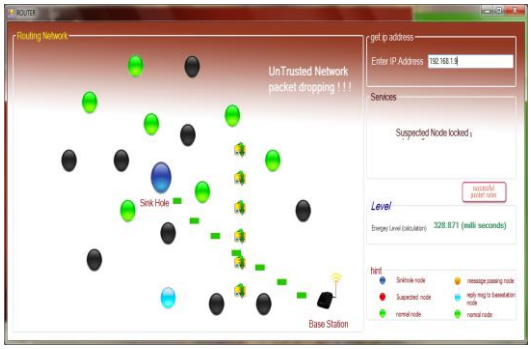

Fig 5.8 Detect Rectification of Failure Node

VI. 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 wrt 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.

VII. REFERENCE

[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.