AN APPROACH ON NETWORK FAULT CORRECTION IN OVERLAY NETWORKS

Vikram Narayandas*

P.Ravinder Kumar**

M.Naveen Kumar***

S.Pradeep****

Abstract

We consider an end-to-end approach of inferring probabilistic data forwarding failures in an managed overlay network, where overlay nodes are independently operated by various administrative domains. Our optimization goal is to minimize the expected cost of correcting (i.e., diagnosing and repairing) all faulty overlay nodes that cannot properly deliver data. Instead of first checking the most likely faulty nodes as in conventional fault localization problems, we prove that an optimal strategy should start with checking one of the candidate nodes, which are identified based on a potential function that we develop. We propose several efficient heuristics for inferring the best node to be checked in large-scale networks.

Index Terms— network management, fault localization and repair, overlay network.

* Associate Professor, Department of CSE, Jayaprakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh.

** Associate Professor, Department of ECE, Jayaprakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh.

*** Associate Professor, Department of CSE, Vidya Jyothi Institute of Technology, R.R Dist, Andhra Pradesh.

**** Assistant Professor Department of IT, Jayaprakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh

1. INTRODUCTION

An overlay network is a computer network which is built on the top of another network. Nodes in the overlay can be thought of as being connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. For example, distributed systems such as cloud computing, peer-to-peer networks, and client-server applications are overlay networks because their nodes run on top of the Internet. The Internet was built as an overlay upon the telephone network.

Overlay networks are used in telecommunication because of the availability of digital circuit switching equipments and optical fiber. Telecommunication transport networks and IP networks (that combined make up the broader Internet) are all overlaid with at least an optical layer, a transport layer and an IP or circuit layers (in the case of the PSTN). Fault localization, a central aspect of network fault management, is a process of deducing the exact source of a failure from a set of observed failure indications. It has been a focus of research activity since the advent of modern communication systems, which produced numerous fault localization techniques. However, as communication systems evolved becoming more complex and offering new capabilities, the requirements imposed on fault localization techniques have changed as well. We consider an end-to-end approach of inferring probabilistic data forwarding failures in an externally managed overlay network, where overlay nodes are independently operated by various administrative domains. Our optimization goal is to minimize the expected cost of correcting (i.e., diagnosing and repairing) all faulty overlay nodes that cannot properly deliver data. Instead of first checking the most likely faulty nodes as in conventional fault localization problems, we prove that an optimal strategy should start with checking one of the candidate nodes, which are identified based on a potential function that we develop. We propose several efficient heuristics for inferring the best node to be checked in large-scale networks.

In proposed system we investigate the use of probing technology for the purpose of problem determination and fault localization in networks. We present a framework for addressing this issue and implement algorithms that exploit interactions between probe paths to find a small collection of probes that can be used to locate faults. Small probe sets are desirable in order to minimize the costs imposed by probing, such as additional network load and data management requirements and also show that although finding the optimal collection of probes

is expensive for large networks, efficient approximation algorithms can be used to find a nearly-optimal set. Utilizes specialized router primitives to directly isolate the location of failures that affect traffic. Generalize to localizing other end-to-end performance degradations such as delay and loss.

2. OVERLAY NETWORKS:

In this paper, we are interested in diagnosing and repairing faulty nodes in an overlay network, in which overlay nodes are independently operated by multiple administrative domains. By an administrative domain, we mean a single administrative authority that controls a collection of resources (e.g., routers and servers). Examples of externally managed overlay networks include Resilient Overlay Network which provides routing resilience toward Internet path outages, and Service Overlay Network which provides end-to-end quality-of-service guarantees. Both deploy overlay nodes over multiple administrative domains that cooperatively accomplish certain network services. To ensure the availability of these network services, an effective network fault mechanism. Secure Overlay Services defend against denial-of-service attacks. In both data is securely tunneled over an overlay network. Data may be re-routed to bypass failed nodes; robustness of data delivery will be degraded if the failed nodes are not immediately repaired because attackers can now devote resources to attacking the remaining non-failed nodes. Note that security-oriented overlay networks might be deployed over a number of end sites rather than a single ISP and can be viewed as externally managed networks since each end site is independently operated.

3. Fault Localization:

Fault localization is the process of tracing back signals through an integrated circuit to locate the first failing node. This process can be performed using either mechanical probing or electron beam probing. The task of fault localization is heavily dependent on the design of the IC and usually requires individuals knowledgeable about the design of the IC and the test patterns needed to stimulate the IC. Although some tools, such as Schlumberger's Diagnostic Assistant, exist to help automate this process, fault localization is usually a manual task with highly

complex ICs.Proper design and test considerations up front can help reduce the complexity of this task. Techniques such as scan design, IDDQ testing and structured design and test principles can eliminate many hours of fault isolation later on during design validation and qualification.

Fault localization is necessary to determine the location of the defect. In most cases, the location of the defect is necessary to determine the root cause of failure. It is worth noting, however, that fault localization may not be necessary to give a satisfactory response to the requester. Many times, the requester is satisfied with a determination as to whether the defect is a wafer fabrication problem, a packaging problem, a testing problem, or an end use problem. Once the IC has been characterized electrically and the packaging material has been removed, the signal should be traced from the failing node back into the IC. At some point, gate causing the incorrect output can be found. While this sounds simple, with the complexity of modern ICs and the high fan outs found on many nodes, this process can get very tedious very quickly. Other non-contact methods, such as voltage contrast, are better suited to handle complicated ICs, but if they are not available, mechanical signal tracing is a very inexpensive alternative.

After the IC is placed in the failing electrical state and contact can be made to the metal or poly layer of interest, the rest is easy. Start from the failing output and trace the signals backward until a node is found in the wrong state. A common way to determine if a node is in the wrong state is to probe the same node on a comparison IC that is in the same electrical state. If possible, placing the two ICs side by side under the same probe station will help facilitate this process. Care must be taken at all times not to damage the IC with the probes. The most cumbersome part of this process is dealing with complicated branching that takes place on many circuits. Remember that these ICs were not laid out for ease of signal tracing for failure analysis.

Fault localization is performed usually after faster isolation techniques have been tried. You should first utilize techniques such as light emission, liquid crystal, fluorescent micro thermo graphic imaging, CIVA, and LIVA before performing fault localization. In addition, before setting up for a manual fault isolation effort, check to see if there are any scan or IDDQ based techniques you can first try. Fault localization using an e-beam probe should be performed before the top glass layer is removed. Fault localization using mechanical probes should be performed after the top glass layer is removed.

4. Related Work:

An overlay network is a layer of virtual network topology on top of the physical network, which directly interfaces to users. With the rapid advancement of Internet and computing technology, much more aggregate information and computing resources are available from clients or peers than from a limited number of centralized servers. Overlay networks provide us with the following advantages and opportunities to better utilize the increasingly growing Internet information and resources.

1) Overlay networks allow both networking developers and application users to easily design and implement their own communication environment and protocols on top of the Internet, such as data routing and file sharing management.

2) Data routing in overlay networks can be very flexible, quickly detecting and avoiding network congestions by adaptively selecting paths based on different metrics, such as probed latency.

3) The end-nodes in overlay networks are highly connected to each other due to flexible routing. As long as the physical network connections exist, one end-node can always communicate to another end-node via overlay networks. Thus, scalability and robustness in overlay networks are two attractive features.

4) The high connectivity of increasingly more end-nodes to join overlay networks enables effective sharing of a huge amount of information and resources available in the Internet.

Typical overlay networks include multicast overlays, peer-to-peer overlays, parallel file downloading overlays, routing overlays (e.g. skype for VoIP). Overlay networks also create several challenges and problems for us to do research. First, overlay networks not only have no controls of physical networks, but also lack critical physical network information. Second, because of the indirect or even miscommunications between overlay and underlay networks, in practice, inefficient usage network resources are quite often in many overlay applications, such as mismatch between overlay and underlay topology, inaccurate probing results among end-to-end nodes due to network dynamics, generating a large amount of redundant messages, and others. Third, since the overlay networks are open to all kinds of Internet users, security and

privacy issues can be quite serious. Fourth, overlay networks are highly decentralized, thus they are likely to have weak ability for resource coordination's. Finally, fairness of resource sharing and collaborations among end-nodes in overlay networks are two critical issues that have not been well addressed. We are conducting research to address several issues of performance, reliability, privacy, and coordination's in overlay networks. We focus on structured and unstructured P2P overlays, routing overlays for VoIP, and parallel file downloading overlays. Fig 2.1 below shows architecture of managed overlay networks.

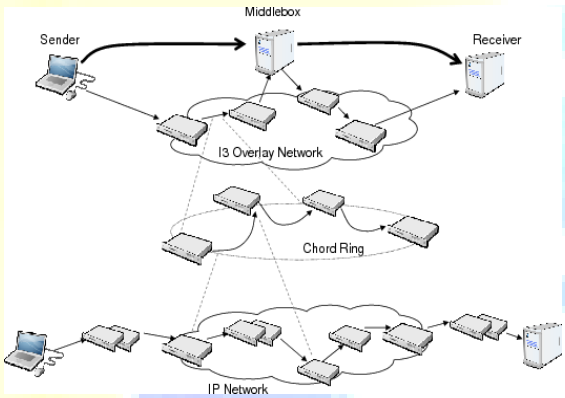

Fig2.1 Architecture of Overlay Network

The peer-to-peer (P2P) model, being widely adopted in today's Internet computing, suffers from the problem of topology mismatch between the overlay networks and the underlying physical network. Traditional topology optimization techniques identify physically closer nodes to connect as overlay neighbors, but could significantly shrink the search scope. Efforts have been made to address the mismatch problem without sacrificing the search scope, but they either need time synchronization among peers or have a low convergent speed. In this paper, we propose a scalable bipartite overlay (SBO) scheme to optimize the overlay topology by identifying and replacing the mismatched connections. In SBO, we employ an efficient strategy for distributing optimization tasks in peers with different colors. We conducted comprehensive simulations to evaluate this design. The results show that SBO achieves approximately 85 percent of reduction on traffic cost and about 60 percent of reduction on query response time.

Our comparisons with previous approaches to address the topology mismatch problem have shown that SBO can achieve a fast convergent speed, without the need of time synchronization among peers.

Overlay networks consist of a series of virtual or physical computers layered on top of an existing network. The purpose of the overlay network is to add missing functionality without a complete network redesign. Typically, these networks link to the existing network through virtual or physical nodes. Common examples of overlay networks are found in cloud computing structures and peer-to-peer networks. The most widely used overlay network is the Internet. Prior to its commercialization in the 1980s, the Internet was a government-based research network built on top of the physical infrastructure of the Public Switched Telecommunications Network, or PTSN. The Internet started as a series of linked computers connected via the country's phone lines to share stored files and information between governmental offices and research agencies. Adding to the underlying voice-based telecommunications network, the Internet layer allowed the distribution of data packets across the same network infrastructure without changing the public telephone system

Just as the Internet used phone lines as a backbone, peer-to-peer networks use standard Internet protocols to prioritize data transmission between two or more remote computers. Peer-to-peer is a type of overlay network, as it uses specific software-based applications, such as the background downloader from "World of War craft" or the music-sharing service Spotify, to create direct connections to remote computers for the sharing of files. Peer-to-peer networks use the physical network's topology, but outsource data prioritization and workload to software settings and memory allocation, which are all established within the application's settings.

Cloud computing is considered an overlay network, as it's a virtual extension for the storage of additional files, programs and network resources. This extended processing environment isn't physically linked to the home network, but is instead accessed on demand and separate from the main network. It acts as a virtual layer within the network, but linked via an application that allows connection to the remote environment. All files and applications use the virtual resources of the cloud, not the local, physical network.

5. Methodology:

5.1. Network configuration:

An Internet service provider (ISP) is an organization that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit. Access ISPs directly connect clients to the Internet using copper wires, wireless or fiber-optic connections. Hosting ISPs lease server space for smaller businesses and other people (collocation). Transit ISPs provide large amounts of bandwidth for connecting hosting ISPs to access ISPs. ISPs may engage in peering, where multiple ISPs interconnect at peering points or Internet exchange points (IXs), allowing routing of data between each network, without charging one another for the data transmitted—data that would otherwise have passed through a third upstream ISP, incurring charges from the upstream ISP.

5.2. Analyze bad path and good path:

Network path or Shared path is a location where you can store files and other resources like your local path. One benefit of network share is that the files can be shared among multiple users.

5.3. Analyze cost:

Intuitively, the cost of network resources, such as buffers in routers, should go up as the resource is depleted. When the resource is not utilized at all, its cost should be zero. When the resource is fully utilized, its cost should be prohibitively expensive.

5.4. Graph representation:

The overlay network model used is a graph with nodes and overlay links. Each node on the graph represents a host running a daemon program. Each overlay link is a unicast link between two nodes, which may be along path traversing multiple routers and physical links in the Internet.

6. CONCLUSION

In this paper we have consider an end-to-end approach of inferring probabilistic data forwarding failures in an externally managed overlay network, where overlay nodes are independently operated by various administrative domains. Our optimization goal is to minimize the expected cost of correcting (i.e., diagnosing and repairing) all faulty overlay nodes that cannot properly deliver data.

REFERENCES:

[1].L. Jiang and J. Walrand, "A distributed CSMA algorithm for throughput and utility maximization in wireless networks," in Proc. 46th Annu. Allerton Conf. Commun., Control, Comput. Sep. 23–26, 2008, pp. 1511–1519.

[2] A. Eryilmaz, A. Ozdaglar, and E. Modiano, "Polynomial complexity algorithms for full utilization of multi-hop wireless networks," in Proc. IEEE INFOCOM, Anchorage, AK, May 2007, pp. 499–507.

[3].X. Lin, N. B. Shroff, and R. Srikant, "A tutorial on cross-layer optimization in wireless networks," IEEE J. Sel. Areas Commun., vol. 24, no. 8, pp. 1452–1463, Aug. 2006.

[4].J. W. Lee, M. Chiang, and R. A. Calder bank, "Utility-optimal random-access control," IEEE Trans. Wireless Commun., vol. 6, no. 7, pp. 2741–2751, Jul. 2007.

[5] P. Gupta and A. L. Stolyar, "Optimal throughput allocation in general random access networks," in Proc. Conf. Inf. Sci. Syst., Princeton, NJ, Mar. 2006, pp. 1254–1259.

[6] X. Wu and R. Srikant, "Scheduling efficiency of distributed greedy scheduling algorithms in wireless networks," in Proc. IEEE INFOCOM, Barcelona, Spain, Apr. 2006, pp. 1–12.

Author's Information:

1. Vikram Narayandas M.Tech (CN) from Shadan College of Engineering, R.R Dist, B.Tech (CSIT) from Sree Datta college of Engineering, Hyderabad and. Currently he is working as Associate Professor at Jayaprakash Narayan College of Engineering, Mahabubnagar. And he has 6 years of experience in Teaching. His areas of interest include Computer networks, wire less networks, Data mining, Network Security, Software Engineering, Sensor Networks, and Cloud Computing. He is the membership of IJMRA, IACSIT, ISTE, IAENG, and CSTA. He is Peer reviewer on honorary basis of GJCST.He is Associate Editor for IJMRA. He has Published 13 papers in International Journals.

2.P.Ravinder Kumar M.Tech(WMC) from vardhaman college of engineering ,B.Tech(ECE) from JayaPrakash Narayana College of Engineering Currently he is working as Associate Professor at Jayaprakash narayan college of engineering And has 9 years of Experience in teaching . His areas of interest include computer networks and communications, wireless networks, signal processing.

3. M.Naveen Kumar M.Tech (CSE) from Holy Mary Institute of Technology Hyderabad, B.Tech (IT) from Aditya Engineering College, East Godavari, Currently he is working as Associate Professor at Vidya Jyothi Institute of Technology, R.R Dist .And he has 6 years of Experience in teaching. His areas of interest include computer networks and communications, wireless networks.

4.S.Pradeep M.Tech CSE from Jaya prakash Narayana College of Engineering & Technology B.Tech from Jaya prakash narayana College of Engineering. Currently he is working as Assistant Professor at Jaya prakash Narayana College of Engineering. His areas of interest include Data mining, Network Security, Software Engineering and Sensor Network.