Analysis on Optimal Network Fault Correction in Externally Managed Overlay Networks

[1] E.Srivani, [2] D.Jamuna [3] M. Venkata Krishna Reddy [4] L.Haritha

[1] MTECH(CSE), Jaya Prakash Narayan College of Engineering,Mahabubnagar, Andrapradesh.

[2] Professor and HOD, Jayaprakash narayan college of Engineering ,Mahabubnagar, Andrapradesh

[3] Associate Professor, Jaya Prakash Narayan College of Engineering, Mahabubnagar, Andrapradesh.

[4] Associate Professor, Jaya Prakash Narayan College of Engineering, Mahabubnagar, Andrapradesh.

ABSTRACT

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 variousadministrative 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. By extensive simulation, we show that we can infer the best node in at least 95% of time, and that first checking the candidate nodes rather than the most likely faulty nodes can decrease the checking cost of correcting all faulty nodes.

Index terms: potential function, network failures, simulation, candidate node, probe

1. INTRODUCTION

Overlay networks not only have no controls of physical networks, but also lack critical physical network information. Overlay networks create virtual topologies on top of the existing networking infrastructure and come as a middle layer between end-user applications and the basic network services To diagnose (but not repair) network faults, recent approaches like use all network nodes to collaboratively achieve this. For instance, in hop-by-hop authentication each hop inspects packets received from its previous hop and reports errors when packets are found to be corrupted. While such a distributed infrastructure can accurately pinpoint network faults, overlay networks that scales with the number of participants and groups.

A service may be replicated across multiple servers for redundancy. We often use site or Web site synonymously with service. This examines the paths taken by and processing performed on packets involved in a simple Internet service. Collect failure signatures from two different fault detection systems deployed in a tier-1 ISP and construct a topology-dependent risk model for each system. Distributed Denial of Service (DDoS) attacks and other malicious traffic are responsible for an Increasing number of outages.

Deployment Challenges and Overlay Networks:

Once the system has access to multiple paths, it must address two subsequent issues:

1. What are the right metrics for path selection? Applications may have widely differing needs.

2. How can such a system be deployed? Making rapid change to the core Internet architecture is a slow and difficult process.

This dissertation argues that overlay networks meet the needs of both of these requirements. An overlay network is a network that runs on top of another network. In the case of an overlay network built over the Internet, the overlay network treats a host-to-host path provided by the Internet as a *"link."* The hosts in the overlay participate in an overlay routing protocol and cooperatively forward data for each other. Overlay networks have become a popular field of research in the last few years.

2. PROBLEM FORMULATION

In existing paper, we are interested in diagnosing and repairing faulty nodes in an externally managed overlay network, in which overlay nodes are independently operated by multiple administrative domains.

a)Hop-by-hop reliable communication in overlay networks

The easiest way to achieve reliability in Overlay Networks is to use a reliable protocol, usually TCP, between the end points of a connection. This mechanism has the simplicity in implementation and deployment, but pays a high price upon recovery from a loss. As overlay paths have higher delays, it takes a relatively long time to detect a loss, and data packets and acknowledgments are sent on multiple overlay hops in order to recover the missed packet**.** In large networks,The lack of detailed failure models makes an accurate analytical evaluation difficult and there is no proper hop by hop node checking is impossible.

3. PROBLEM SOLUTION

In this paper, proposed one contributes heuristics in large scale networks. in diagnosing and repairing faulty nodes in an externally managed overlay network, in which overlay nodes are independently operated by multiple administrative domains .A single authority person will control resources.

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. Our results 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. Each node in a logical tree T is classified as faulty or non-faulty, depending on how we first define whether a (root-to-leaf) path exhibits any *"anomalous behavior".*

a)Anomalous path:

The path which fails to deliver a number of correct packets within a time window, and that some node on the path is faulty.

b) Selection of candidate node:

Select a subset of nodes termed candidate nodes, one of which should be first checked in order to minimize the expected cost of correcting all faulty nodes. Evaluate the performance of three candidate-based heuristics that approximate the best node selection of the inference algorithm. These heuristics are:

a) Cand-Prob: which selects the candidate node with the highest conditional failure probability given a bad tree,
b) Cand-Cost: which selects the candidate node with the least checking cost,
c) Cand-Pot: which selects the candidate node with the highest potential.

Interference approach:

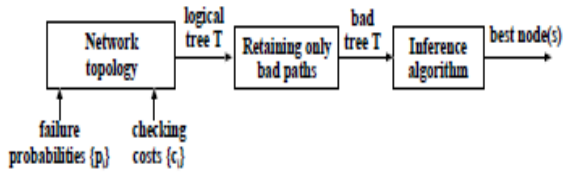

Fig: End to End interference approach for network faults.

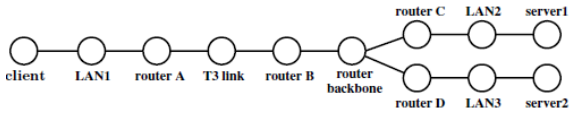

Fig :logical topology of networks.

Interference approach considers of network topology for retaining good path and bad path. Below figure is tree topology which represents good path and bad path.

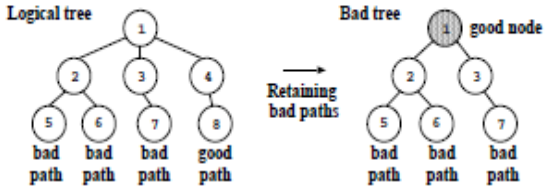

Fig: Logical tree for retain good and bad path

ALGORITHMS

1. Brute force interference algorithm:

S*=ϕ, c*=∞
For all diagnosis sequence S do
Compute c=the expected cost of S
If c < c* then
S*=S, c*=c
Return the first node is S*

2. Heuristics for theInterference algorithm:

While the brute-force inference algorithm returns the best node, its factorial complexity prohibits its use in large-scale networks. Thus, we propose three classes of efficient heuristics for the inference algorithm that are suitable for large-scale networks. Each class of heuristics consists of two approaches: one that considers the most likely faulty nodes and one that considers the candidate nodes.

By using these algorithms we calculate potential function. The potential function is derived based on the optimality results.

4. CONTRIBUTIONS

An end-to-end basis by layering routing and probing protocols atop the existing network substrate. We present several key findings that we believe are applicable to the design of a variety of Internet service provider based systems:

a) Overlay routing can improve upon the underlying network.RON is the first wide-area network overlay system that can detect and recover from path outages and periods of degraded performance within several seconds.

b) End-to-end measurements can guide path selection, end-to-end indications of path usability form a strong basis for choosing between different paths. By having end hosts decide whether or not a path is suitable, a failure making system can detect and avoid problems.

C) In is possible to provide higher availability between actively communicating hosts than between potentially communicating hosts. In line with the previous observation about end to-end probes, the systems described in this dissertation attempt to detect and mask failures between *actively* communicating end-points. RON restricts its probing and routing to a small group of cooperating nodes recovery, potential node-pairs on the Internet can concurrently communicate.

d) Waypoint selection can quickly locate working paths formulation of the waypoint selection problem, a generalization of the server selection problem that benefits from the knowledge of past accesses using particular paths. By attempting to use different Internet paths in a good order, a failure masking system improves its ability to find a working path

without spending excess time attempting non-working paths.

e)**Real-world failures are frequent and often avoidable**. Failures occur at a variety of locations in the network. Fortunately, these failures can often be masked through the use of simple techniques such as an overlay network

5. FUTURE ENHANCEMENT

We are in search of the mechanism responsible for the relative robustness of networks. It may stem from the evolutionary process producing thorough check that set up error correction patterns methods create more robust sorting networks than traditional design. Introducing of design patterns for analyzing of good path and bad paths and making usage of several algorithm for finding of probability function. Introducing of control graphs for fault nodes.

6. CONCLUSION

We present the optimality results for an end-to-end inference approach to correct probabilistic network faults at minimum expected cost. One motivating application of using this end-to-end inference approach is an externally managed overlay network, The optimization goal to minimize the expected cost of correcting all faulty nodes. In view of this, we construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy, difficulty of finding the best node so several approaches are used for correcting of faulty nodes.

7. REFERENCES

1.A. Eryilmaz, A. Ozdaglar, and E. Modiano, “Polynomial complexity algorithms for full utilization of multi-hop wireless networks,”.

2. A. Eryilmaz, A. Ozdaglar, and E. Modiano, “Polynomial complexity algorithms for full utilization of multi-hop wireless networks,”.

3. P. P. C. Lee, V. Misra, and D. Rubenstein. Toward Optimal Network Fault Correction via End-to-End Inference.

4. M. Steinder and A. Sethi. A Survey of Fault Localization Techniques in Computer Networks.

E.Srivani, Pursuing M.Tech from Jaya Prakash

Narayan college of engineering Mahabubnagar, Andhra Pradesh . Btech from Sri Sai Jyothi college of engineering .Vattinagulapally, Hyderabad, Andrapradesh. Her areas of interest include in networks finding of failures in overlay networks.

Prof.D.Jamuna ,M.Tech, (,Ph.D).

Professor & HOD. At Jaya Prakash Narayan College of Engineer ing, mahabub nagar, Andra pradesh. M.Tech. degree in SE from School of Information Technology, JNTU, Hyd and Pursuing Ph.D from Rayalaseema University, Kurnool. Her areas of interest include Wireless networks, Information Security currently focusing on IP Networks

M.Venkata Krishna Reddy, working as Associate professor in Jaya Prakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh. M.Tech(CSE) from Vidya vikas Institute of Technology, hyderabad. His areas of interest include Wireless networks, Information Security currently focusing on IP Networks .

KL.Haritha, MTECH(CSE) working as Associate professor in Jaya Prakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh Her areas of interest include Information Security currently focusing on IP Networks .