International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 1, Issue 1, August 2015

Efficient Heuristics to Network Fault correction

A.Angeline Priya[1], P.Eben Jasmin[2], R.Ida[3], V.Abinaya Catherin[4], T.Gowsalya[5], G.Jayaraman[6]

U.G. Scholars, Department of ECE, Francis Xavier Engineering College, Tirunelveli [1,2,3,4,5]

Assistant Professor, Department of ECE, Francis Xavier Engineering College, Tirunelveli[6]

***Abstract*— An end-to-end approach of inferring probabilistic data-forwarding failures is shown. 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. 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— *Probabilistic data-forwarding, Quality of sevice, Ovelay network*

I. INTRODUCTION

An overlay network is a virtual network of nodes and logical links that is built on top of an existing network with the purpose to implement a network service that is not available in the existing network.

- Expensive to develop entirely new networking hardware/software
- All networks after the telephone have begun as overlay networks
- Do not have to deploy at every node
  - Not every node needs/wants overlay network service all the time .e.g., QoS guarantees for best-effort traffic
- Overlay network may be too heavyweight for some nodes .e.g., consumes too much memory, cycles, or bandwidth
- Overlay network may have unclear security properties . e.g., may be used for service denial attack
- Overlay network may not scale (not exactly a benefit) . e.g. may require n2 state or communication

The central element of this system is the link between fault situations and their according causes based on a standard systematic. A fault-cause pair can be designated as a "case". The use of appropriate information engineering algorithms, for example case-based reasoning (CBR), allows database systems to very quickly find cases for newly occurring faults, which can be relevant for repairing the faults. This is a frequent use case, in particular for the customer service at an automobile workshop.

Another advantage is that the data basis "grows" with the experience gained by the users, a characteristic similar to an expert system. This "knowledge" expands continually during operation and usage of the system. The utilization of a common data basis over the various areas of the automotive value chain – development, production and service – also allows a consistent handling of electronic and mechanical faults for all steps.

We consider an end-to-end approach [1] of inferring network faults that manifest in multiple protocol layers, with an optimization goal of minimizing the expected cost of correcting all faulty nodes. 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%, and that checking first the candidate nodes rather than the most likely faulty nodes can decrease the checking cost of correcting all faulty nodes by up to 25%.

We show how end-to-end measurements of multicast traffic [2] can be used to infer the packet delay distribution and utilization on each link of a logical multicast tree. To exploit the inherent correlation between multicasts observations to infer performance of paths between branch points in a tree spanning a multicast source and its receivers. In real traffic simulations, we found rapid convergence, although some persistent differences from the actual distributions because of spatial correlation.We are extending our delay distribution analysis in several directions. First we plan to do more extensive simulations, exploring larger topologies, different node behavior, background traffic and probe characteristics.Moreover, we are exploring how probe delay is representative of the delay suffered by other applications and protocols, for example TCP.

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 1, Issue 1, August 2015

We apply Bayesian reasoning techniques [3] to perform fault localization complex communication systems while using dynamic, ambiguous, uncertain, or incorrect information about the system structure and state. We introduce adaptations of two Bayesian reasoning techniques for poly trees, iterative belief updating, and iterative most probable explanation. We show that fault localization through iterative belief updating is resilient to noise in the observed symptoms and prove that Bayesian reasoning can now be used in practice to provide effective fault localization. The approximate techniques proposed in this paper meet all or most of the objectives of our research.

One of the key reasons overlay networks are seen as an excellent platform for large scale distributed systems is their resilience in the presence of node failures. This resilience [4] rely on accurate and timely detection of node failures. In this paper, we study how the design of various keep-alive approaches affect their performance in node failure detection time, probability of false positive, control overhead, and packet loss rate via analysis, simulation, and implementation . The improvement in detection time between baseline and sharing algorithms becomes more pronounced as the size of neighbor set increases. Finally, sharing of information allows a network to tolerate a higher churn rate than baseline.

The problem of identifying topology and inferring link-level performance parameters such as packet drop rate or delay variance using only end-to-end measurements is commonly referred to as network tomography[5] . This paper describes a collaborative framework for performing network tomography on topologies with multiple sources and multiple destinations, without assuming the topology to be known. Using multiple sources potentially provides a more accurate and refined characterization of the internal network. A decision theoretic framework is developed enabling the joint characterization of topology and internal performance. This paper addressed the problem of determining internal characteristics of a network such as logical topology and link-level performance parameters using only end-to-end measurements made from multiple sources to multiple destinations. We reduced the general multiple-source, multiple destination problem to many smaller sub problems consisting of only two sources and two destinations , and we verified that the collection of 2-by-2 components suffices to describe the topology and link-level performance parameters for the multiple-source, multiple destination Network .

In [6], we explore the problem of inferring the internal structure of a multicast distribution tree using only observations made at the end hosts. By noting correlations of loss patterns across the receiver set and by measuring how the network perturbs the fine-grained timing structure of the packets sent from the source, we can determine both the underlying multicast tree structure as well as the bottleneck bandwidths.Our simulations show that the algorithm is robust and appears to converge to the correct tree with high probability. We presented algorithms that allow a receiver to infer the logical topology of the multicast tree, the bottleneck bandwidth of the path between the source and each receiver in the tree and the approximate location of the bottlenecks in the tree.

[7] allows the determination of the logical multicast topology without assistance from the underlying network nodes .We provide five instances of the class, variously using loss or delay measurements. We compare their accuracy and computational cost, and recommend the best choice in each of the light and heavy traffic Load regimes. We have presented a general framework for the inference of the multicast tree topologies from end-to-end measurements. In contrast with tools such as mtrace, cooperation of intervening network nodes is not required. Finally, the algorithms described in this paper are each based on a different performance metric.

A Resilient Overlay Network (RON) [8] is an architecture that allows distributed Internet applications to detect and recover from path outages and periods of degraded performance within several seconds, improving over today's wide-area routing protocols that take at least several minutes to recover. A RON is an application-layer overlay on top of the existing Internet routing substrate. The RON nodes monitor the functioning and quality of the Internet paths among themselves, and use this information to decide whether to route packets directly over the Internet or by way of other RON nodes, optimizing application-specific routing metrics. These improvements, particularly in the area of fault detection and recovery, demonstrate the benefits of moving some of the control over routing into the hands of end-systems.

We propose an architecture called Secure Overlay Services (SOS) [9] that *proactively* prevents DoS attacks, geared toward supporting Emergency Services or similar types of communication. The architecture uses a combination of secure overlay tunneling, routing via consistent hashing, and filtering. Through simple analytical models we show that DoS attacks directed against any part of the SOS infrastructure have negligible probability of disrupting the communication between two parties: for instance, when only ten nodes act as beacons, ten nodes act as secret servlets , and ten nodes act as access points, for an attack to be successful in one out of ten thousand attempts, approximately forty percent of the nodes in the overlay must be attacked simultaneously.

Companies that rely on the Internet for their daily business are challenged by uncontrolled massive worm [10] spreading and the lurking threat of large-scale distributed denial of service attacks. We present a new model and methodology, which allows a company to qualitatively and quantitatively estimate possible financial losses due to partial or complete interruption of Internet connectivity. Our systems engineering approach is based on an in-depth analysis of the Internet dependence of different types of enterprises and on interviews with Swiss Telco's, backbone and Internet service Providers. A discussion of sample scenarios illustrates the flexibility and applicability of our model.

Existing monitoring link delays and faults in a service provider or enterprise IP network.Our two-phased approach attempts to minimize both the monitoring infrastructure costs as well as the additional traffic due to probe messages. In the first phase of our approach, we

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 1, Issue 1, August 2015

compute the locations of a minimal set of monitoring stations such that all network links are covered, even in the presence of several link failures. Subsequently, in the second phase, we compute a minimal set of probe messages that are transmitted by the stations to measure link delays and isolate network faults. We show that both the station selection problem as well as the probe assignment problem is NP-hard. We then propose greedy approximation algorithms that achieve a logarithmic approximation factor for the station selection problem and a constant factor for the probe assignment problem.

II. PROPOSED SYSTEM

The most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Network components are prone to a variety of faults such as packet loss, link cut, or node outage. To prevent the faulty components from hindering network applications, it is important to diagnose (i.e., detect and localize) the components that are the root cause of network faults. However, it is also desirable to repair the faulty components to enable them to return to their operational states. Therefore, we focus on network fault correction, by which we mean not only to diagnose, but also to repair all faulty components within a network. We want to devise a cost effective network fault correction mechanism that corrects all network faults at minimum cost in diagnosing and repairing faulty nodes in an externally managed overlay network, in which overlay nodes are independently operated by multiple administrative domains.

The transmitter sends a packet to the receiver and waits for its acknowledgment. Based on error-detection results, the receiver generates either a negative acknowledgment (NACK) or a positive acknowledgment (ACK) for each received packet and sends it over a feedback channel. If an ACK is received, the transmitter sends out a next packet; otherwise, if an NACK is received, retransmission of the same packet will be scheduled immediately, and this process continues until the packet is positively acknowledged.

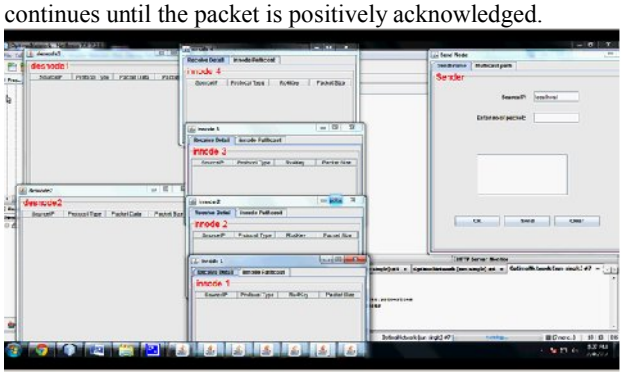

Fig.1.Transmitter module

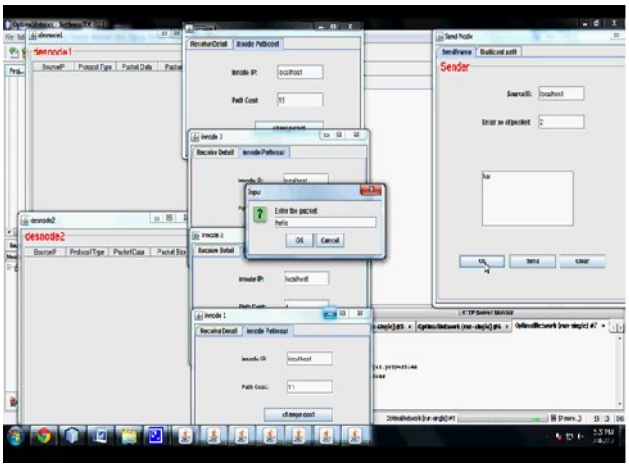

Fig.2.Receiver Operation

The receiver generates either a negative acknowledgment (NACK) or a positive acknowledgment (ACK) for each received packet.

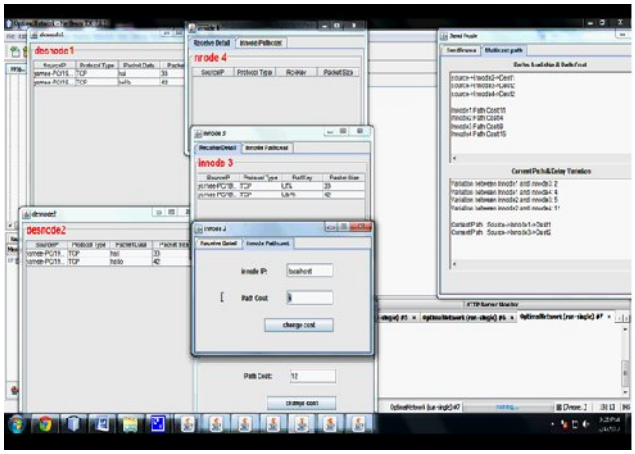

Fig.3.Fault Node diagnosis and correction

Packet node waiting for transmission or retransmission is stored. In a similar manner,all nodes are checked with low cost using end-to-end method.

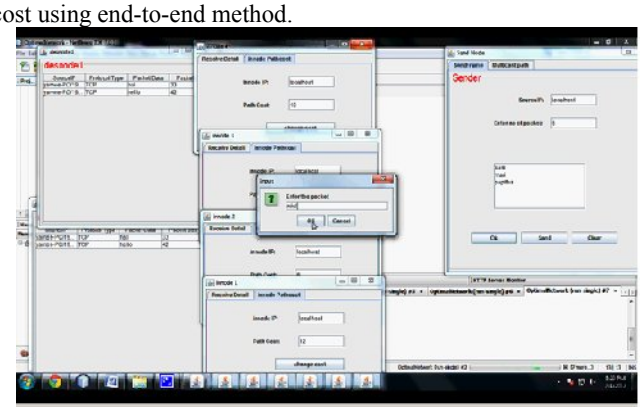

Fig.3.Cost Reduction

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 1, Issue 1, August 2015

III. CONCLUSION

An end-to-end approach of inferring probabilistic data-forwarding failures is shown. 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. 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.

REFERENCES

[1] F. LoPresti, N. Duffield, J. Horowitz, and D. Towsley-(2002), Multicast-based Inference of Network-Internal Delay Distributions. IEEE/ACM Trans. on Networking, 10(6):761–775, Dec.

[2] Avramopoulos, H. Kobayashi, R.Wang, and A. Krishnamurthy-(2004),"Highly Secure and Efficient Routing". In Proc. of IEEE INFOCOM, March

[3] M. Coates, A. O. Hero, R. Nowak, and B. Yu-(2002),Internet Tomography IEEE Signal Processing Magazine, pages 47–65, May.

[4] M. Rabbat, R. Nowak, and M. Coates-(2004),Multiple Sources, Multiple Destination Network Topomography. In Proc. of IEEE INFOCOM

[5] M. Steinder and A. S. Sethi-(2004),Probabilistic Fault Localization in Communication Systems Using Belief Networks. IEEE/ACM Trans. On Networking, 12(5):809–822, Oct.

[6] N. Duffield, J. Horowitz, F. L. Presti, and D.Towsley-(2002),Multicast Topology Inference from Measured End-to-End Loss. IEEE Trans. on Information Theory, 48:26–45, January.

[7] N.G. Duffield and F. Lo Presti-(2000),"Multicast Inference of Packet Delay Variance at Interior Network Links", in Proc. IEEE Infocom 2000, Tel Aviv, March.

[8] P. Papadimitratos and Z. Haas-(2002),"Securing the internet routing infrastructure," IEEE Communications Magazine, pp. 60–68, Oct.

[9] S. Q. Zhuang, D. Geels, I. Stoica, and R. H. Katz-(2005),"On Failure Detection Algorithms in Overlay Networks". In Proc. of IEEE INFOCOM, March.

[10] S. Jamin, C. Jin, Y. Jin, Y. Raz, Y. Shavitt, and L. Zhang-(2000),"The Placement of Internet Instrumentation", In Proceedings of IEEE INFOCOM'2000, Tel Aviv, Israel, March.