Inferring Packet Forwarding Priority, Network Tomography, Congestion Control Based On Packet Probing In Network

J.Benitha Christinal, V.Vivek

Department of Computer Science and Engineering, Karunya University

Coimbatore, Tamil Nadu, India

***Abstract*-Current Internet is a massive, distributed network which continues to grow in size as globalization takes major role in everyone's life like e-commerce, social networking and related activities grow. The heterogeneous and largely unregulated structure of the Internet renders tasks such as optimized service provision, rate limiting certain classes of applications (e.g. peer-to-peer), provide bandwidth guarantee for certain applications, avoiding shared congestion in flows are increasingly challenging tasks. The problem is complicated by the fact that one cannot rely on the cooperation of individual servers and routers to aid in the collection of network traffic measurements vital for these tasks. Hence we go for network monitoring and inference method based on packet probing in the network. This paper presents a hybrid inference method to deal with network characteristics such as shared congestion, packet forwarding priority, network tomography and evaluates each methodology based on packet loss rate.**

***Key words* - Inference, Packet forwarding priority, Packet loss, Congestion control, Network tomography.**

I. INTRODUCTION

The Internet was designed with no gatekeepers over new content or services. A lightweight but enforceable neutrality rule is needed to ensure that the internet continues to thrive--Vint Cerf.

Internet is a massive, distributed network which takes major role in our day-to-day life. As the network grows, the internet has evolved very rapidly in a largely unregulated and open environment. The lack of centralized control and the heterogeneous nature of the internet lead to a very important problem: mapping network connectivity, bandwidth, sharing resources and performance functions. Wide varieties of network characteristics and internet maps have been produced using existing networking tools such as ping and trace route. Information on these tools, along with a collection of interesting internet mapping projects are found in CAIDA [1] and Network tools[2]. The mapping techniques described in the reference above, usually provide only a partial picture of the internet and network characteristics.

In this paper we present a user-level Inference Method for shared congestion, packet forwarding priority, network tomography, measuring services based on Packet Probing in Network. This paper discusses the hybrid inference method to measure various network characteristics. Rest of the paper is organized as follows. Section II contains a literature survey of various techniques and brief description of few end to end inference methods for analysing Network Characteristics have been taken for study. Section III gives a comparative analysis of various inference based on certain parameters. Section IV explains our hybrid inference method. We conclude in Section V analysing the network characteristics using hybrid inference method.

II. LITERATURE SURVEY

Inference and prediction of network conditions is of fundamental importance to a range of network-aware applications. We classify and survey these research efforts.

One widely adopted strategy is to mine the data collected by network internal resources, such as Border Gateway Protocol routing tables, to generate performance reports [3]-[5]. This approach is best applied over long-time scales to produce aggregated analyses such as Internet data sources and analysis reports, but does not lend itself well to providing answers to the fine grained issues we propose here. Another approach is statistical inference of network internal characteristics based on end to end measurements of point to point traffic [6]-[9]. We adopt this general approach because information is gathered at the appropriate granularity. These approaches can be further classified as active approaches, which introduce additional probe traffic into the network, and passive approaches, which make inferences only from existing network traffic. The benefit of the former approach is flexibility: one can make measurements at those locations and times which are most valuable. While the benefit of the latter approach is that no additional bandwidth and network resources are consumed solely for the purpose of data collection [10]. On other dimensions, one can also classify approaches as either receiver-oriented or sender- oriented, depending on where inferences are made and multicast driven or unicast driven, depending on the model used to transmit probe traffic. These are the most common environment under which all inferences made are studied. The general survey gives the idea about various approaches and methods the analysis is made to infer the network characteristics, network conditions of the internet. In this section we have done an literature survey analysis network characteristics like congestion control inferring shared resources [11]-[13], [19], [20], network tomography inferring link level performance and topology information [14]-[16], [21], [22] and packet forwarding prioritization inferring network QoS and packet scheduling[17], [18], [23]. From the above end to end network inference methods; few are selectively analyzed in detail in this literature.

A. Robust identification of shared losses using end-to-end unicast probes [19]

Khaled Harf and Azer Bestavros in their paper titled Robust identification of shared losses using end-to-end unicast probes [19], explain method deals with current internet transport protocols make end-to-end measurements and maintain per-connection state to regulate the use of shared network resources. When two or more such connections share a common endpoint, there is an opportunity to correlate the end-to-end measurements made by these protocols to better diagnose and control the use of shared resources. This paper has developed packet-pair probing technique to determine whether a pair of connections experience shared congestion. It uses a packet pair probe to a pair of different receivers to introduce loss and delay correlation.
Estimation of Network Parameters Using End-to-End Measurements (Bayesian Approach) this paper proposes an analytical technique for the robust determination of both loss and bottleneck equivalence for pairs of unicast connections emanating from the same server. It is mainly based on end-to-end loss information available at the server as a result of passive monitoring or of active probing. The two connections sharing common end point is shown in Figure1 at node 2.

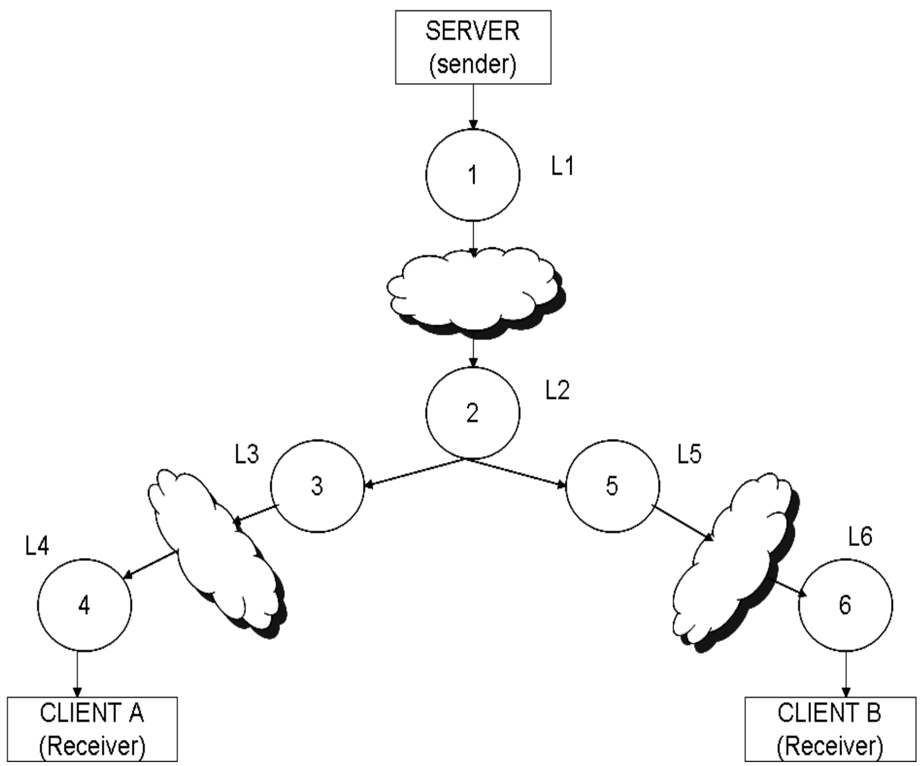

Fig1. Node 1 to Node 2 sharing connection [19]

The above scenario Fig1 with single server, which has active connections to two distinct clients, both experiencing steady-state packet loss rate €.the path from server to client form a tree, which from server's perspective consists of sequence of shared links followed by sequence of disjoint links, in which the shared portion of the sequence may be empty.

1. *Loss sharing:* for these two connections, determines if the incidence of packet loss on the shared portion of the tree is at least €/k, for a fixed constant k>1
2. *Bottleneck Equivalence:* for these two connections, determines if the incidence of shared loss is greater than the incidence of disjoint loss.

In this paper, a technique for determining whether a pair of connections emanating from the same node experience shared losses for unicast probes has been presented.

B. Detecting shared congestion of flows via end-to-end measurement [20]

Dan Rubenstein and Jim Kurose in their paper titled Detecting shared congestion of flows via end-to-end measurement [20], presents a technique based on loss or delay observations at end-hosts to infer using Poisson probing whether or not two flows experiencing congestion are congested at the same network resources. It validates these techniques via queuing analysis. Current Internet congestion control protocols operate independently on a per-flow basis. A key technical issue underlying both of these scenarios is the ability to detect whether two "flows" whether individual unicast sessions, or different senders within a single multicast session share a common resource bottleneck. In this paper, it addresses the fundamental issue of detecting shared points of congestion among flows. Informally, the point of congestion (POC) for two flows is the same when the same set of resources (e.g., routers) are dropping or excessively delaying packets from both flows due to backup and/or overflowing of queues.

It presents the technique that operates on an end-to-end basis and use only end-system observations to detect whether or not a pair of flows experiences a common POC. It says it is *testing* two flows when it is trying to identify whether or not they have the same POC. For conciseness, it say that two flows *share congestion* if their POCs are identical, and that flows *do not share congestion* if the intersection of their POCs is empty. The insight is to construct a measure of correlation between flows and a measure of correlation within a flow with the following property: the measure within the flow is greater than the measure within a flow if and only if the flows share the same POC. We call this method of identifying whether or not two flows share a POC a *comparison test.* The techniques for detecting whether or not pair of flows share congestion is based on observations of internet congestion: Losses or delay experienced by two packets passing through the same POC exhibit some degree of correlation. However, in general, the degree of correlation decreases as the time between the packets' transmission is increased.

Thus in this paper a technique has been proposed that, via end-to-end measurement, we are able to accurately detect whether or not two flows share the same points of congestion within the network

C. Internet Tomography [21]

Mark Coates and Alfred Hero in their paper titled Internet Tomography [21], deals with 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. This inference is commonly referred to as network tomography.

It explores two approaches to service discovery: active probing and passive monitoring. Active probing finds all services currently on the network, except services temporarily unavailable or hidden by firewalls; however, it is often too invasive, especially if used across administrative boundaries. Passive monitoring can find transient services, but miss services that are idle. It compares the accuracy of passive and active approaches to service discovery and show that they are complimentary, highlighting the need for multiple active scans coupled with long-duration passive monitoring. It finds passive monitoring is well suited for quickly finding popular services, finding servers responsible for 99% of incoming connections within minutes. Active scanning is better suited to rapidly finding all servers, which is important for vulnerability detection--one scan finds 98% of services in two hours, missing only a handful.

This paper has provided an overview of the large scale inference and tomography in communication networks by using probing schemes and inference methods.

D. Multiple Sources, Multiple Destination Network Tomography [22]

Michael Rabbat and Robert Nowak in their paper titled multiple Source, multiple Destination Network Tomography[22], presents a study of the multiple source, multiple destination network tomography problem. Using multiple sources in the context of network tomography, it is possible to identify segments within a network shared by the paths connecting multiple sources and destinations. This information may be useful for identifying potential bottlenecks. Sharing statistics between sources may also be useful for optimizing the use of network resources when transferring large amounts of data.

Jointly solving for performance parameters and topology leverages on the close coupling between link-level characteristics, routes derived from the network topology on end-to-end measurement. This paper focuses on the multiple source, multiple destination network tomography problem of characterizing the topology and performance on links connecting a collection of sources and destinations. The contributions are as follows.

1) It is shown that the general network tomography problem can be decomposed into a set of smaller components, each involving just two sources and two destinations and easily extend the results to more general multiple source, multiple destination networks.

2) It identifies a dichotomy of possible two-source, two-destination topologies based on the model order of their representations.

3) A novel multiple-source probing algorithm is presented for determining the model order of an unknown two-source, two-destination topology.

Multiple source topologies can be decomposed in to 2-by-2 networks, thus by solving the 2-by-2 problem it can essentially solve the M-by-N problem.

This paper has provided a probing algorithm for multiple source, multiple destination tomography in networks by using multiple source probing schemes and inference methods.

E. POPI: A User-level Tool for Inferring Router Packet Forwarding Priority [23]

Guohan Lu, Yan Chen and Stefan Birrer in their paper titled A User-level Tool for Inferring Router Packet Forwarding Priority[23], In this paper, it presents an end-to-end approach for packet forwarding priority inference by measuring the loss rate difference of different packet types and its associated tool, POPI. This tool can be used by the enterprises or end-users to discover whether their traffic are treated differently by the ISPs, and whether the ISPs has fulfilled the contracts between them and the users.

Packet forwarding prioritization (PFP) Packet forwarding prioritization (PFP) in routers is one of the mechanisms commonly available to network operators. PFP can have a significant impact on the accuracy of network measurements, the performance of applications and the effectiveness of network troubleshooting procedures. Despite its potential impacts, no information on PFP settings is readily available to end users. In this paper, it uses packet loss as the inference metric because it is the most direct consequence of a priority configuration. PFP in routers are set in a per-interface basis. This observation defines the basis of the approach used in POPI: *In order to reveal packet-forwarding priorities, one needs to saturate the path available bandwidth for a given class to produce loss rates difference among different classes.* Assuming the existence of a PFP mechanism in routers such an approach will succeed at uncovering priority settings in routers along a path if the available bandwidth for the controlled class is lower than the bottleneck available bandwidth of the path.

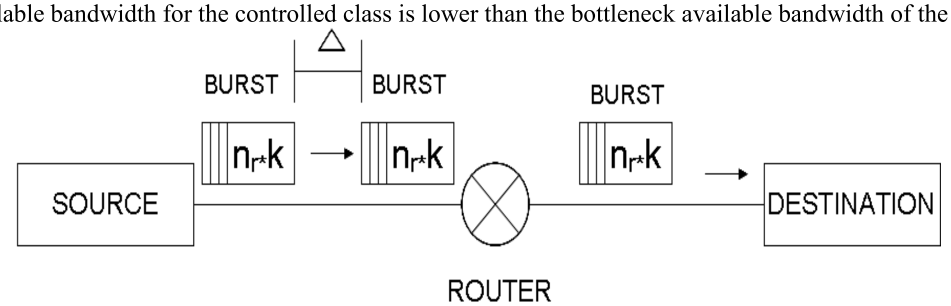

Fig 2. A burst consists of *nr* × *k* packets [22]

For every burst Fig2, loss rate ranks are computed by first sorting packet types in ascending order according to their packet loss rates in that burst and then assigning ranks in order. On observation, Identifying whether there is consistent difference among *k* ranks over *n* observations. Based on ranks packets are grouped. Grouped packets are assigned priority on loss basis and priority is inferred at user level.

In this paper, it has demonstrated that POPI, an end-to-end priority inference tool, is able to accurately infer the router's packet forwarding priority using loss statics.

III. ANALYSIS AND DESIGN ISSUES

Packet-level measurement is now critical to many aspects of broadband networking, for example for guaranteeing service level agreements, facilitating measurement-based admission control algorithms and performing network tomography. Because it is often impossible to measure the entire data passing across a network, the most widely used method of measurement works by injecting probe packets. The probes provide samples of the packet loss and delay, and from these samples the loss and delay performance of the traffic as a whole can be deduced. However, measuring performance like this is prone to errors. Using packet probing method we have analysed many network characteristics and comparison of inference methods is made.

Parameters used for Comparison

The main parameters we considered for the analysis on End-To-End Inference Methods Based on Packet Probing in Network are probing methods, Technique to Evaluate, Packet Loss Statistics, Packet Delay statistics, probing rate, Queuing Discipline and Topology.

Packet Probing: Packet probing is an important Internet measurement technique, supporting the investigation of packet delay, path, and loss. Current packet probing techniques use Internet Protocols such as the Internet Control Message Protocol (ICMP), the User Datagram Protocol (UDP), and the Transmission Control Protocol (TCP) to infer network Characteristics.

Technique to Evaluate: It is a procedure used to accomplish a specific activity or task. The network characteristics like shared congestion, Congestion control, Network tomography, Internet tomography,

tomography using multiple sources and multiple destinations, packet forwarding prioritization can be evaluated using mentioned techniques.

Packet Loss Statistics: Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. To understand packet loss, it is first necessary to know that information is sent over the Internet in packets. These packets contain all the information needed for the sending computer to communicate the desired information to the destination. In many cases, these packets arrive without any problems. When problems do occur, packet loss can take place. Here we specify where packet loss exactly occurs in network during congestion.

Packet Delay statistics: In computer networking, packet delay variation is the difference in end-to-end delay between selected packets in a flow with any lost packets being ignored. The effect is sometimes, incorrectly, referred to as jitter. The delay is specified from the start of the packet being transmitted at the source to the end of the packet being received at the destination.

Probing rate: we use probe packets to measure the packet level performance (e.g. loss, delay); for example whether it is best to probe at a uniform rate, high, or to send probes according to some renewal process, such as a Poisson process. This can be inferred using probe rate.

Queuing Discipline: Queuing Discipline represents the way the queue is organised (rules of inserting and removing customers to/from the queue). Queues are identified by a handle <major number: minor number>, where the minor number is zero for queues. Handles are used to associate classes to queuing disciplines. Queuing disciplines and classes are tied to one another. The presence of classes and their semantics are fundamental properties of the queuing disciplines. There are many queues like FIFO, CBQ, RED, Drop Tail etc., which are used for Queuing is analysed.

Topology: Network topology is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer network. Topology can be considered as a virtual shape or structure of a network. This shape does not correspond to the actual physical design of the devices on the computer network. Any particular network topology is determined only by the graphical mapping of the configuration of physical and/or logical connections between nodes.

Thus we have compared papers based on shared congestion in unicast environment, shared congestion and congestion control on multicast environment, network tomography to infer topology information and loss statistics, internet tomography, tomography with multiple sources and multiple destinations. The comparisons of the characteristics of all these inference methods are given in Table1. We have analysed and studied many papers on End-User level inference to study network characteristics. Then we selected five papers which have similar approach, techniques or network statistics which is used to analysis the network and internal parameters and proposed a hybrid inference method.

IV. PROPOSED SYSTEM-HYBRID INFERENCE METHOD

In this paper we have proposed a hybrid inference method for detecting shared congestion, network tomography and packet forwarding priority. This method is proposed from the analysis of various inference techniques.

Table 1 Comparison of End-User Level Inference Methods

Techniques	**Shared congestion using unicasting**	**Shared congestion using multicasting**	**Internet Tomography**	**Network Tomography**	**Packet Forwarding Prioritization**
probing	Packet pair probing	Poisson probing	Multicast probing	Semi-Randomized probing	Link level probing
Topology	Multicast tree topology	Y topology and inverted Y topology	Tree topology	Cluster topology	Dumbbell topology
Packet Loss Statistics	Sharing Common link	Point of congestion (router)	When cross traffic is more	Link level loss	Forcing packets to drop
Packet Delay Statistics	Packet reorder	Packet reorder	Due to cross traffic	Path delay, link delay	No cross traffic so there is no variability in delay
Probing Rate	High	High	Normal	Low	Faster
Queuing Discipline	Drop Tail	RED	Drop Tail/RED	Drop Tail/FIFO	CBQ/ Priority Queuing

A. Probing the path

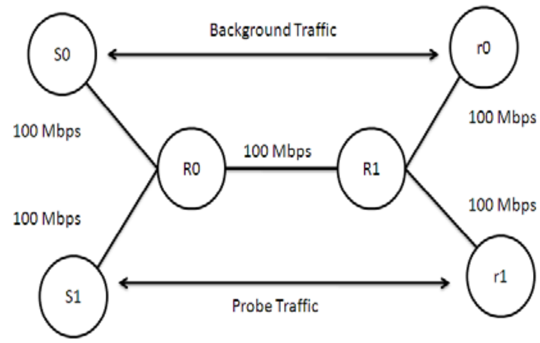

Fig3. Dumbbell Topology of Hybrid Inference Method

Fig 3 shows the dumbbell topology of proposed system where s0, s1 are senders. r0, r1 are receivers and Let R0, R1 be the routers. We test k packet types from sender to receiver. The Link R0 to R1 is the place where it shares the resource of bandwidth 100 Mbps. We use link probe method. It sends several bursts (Nb) from source to a destination. The interval between bursts is Δ. Each burst consists of Nr rounds, in which k packets, one for each packet type is studied, are interleaved in random order.

Fig 4 shows the architecture of the hybrid inference method where the client sent probe packets which are analysed to identify congestion, network tomography and packet forwarding priority. This inference is reported to client at end-user level.

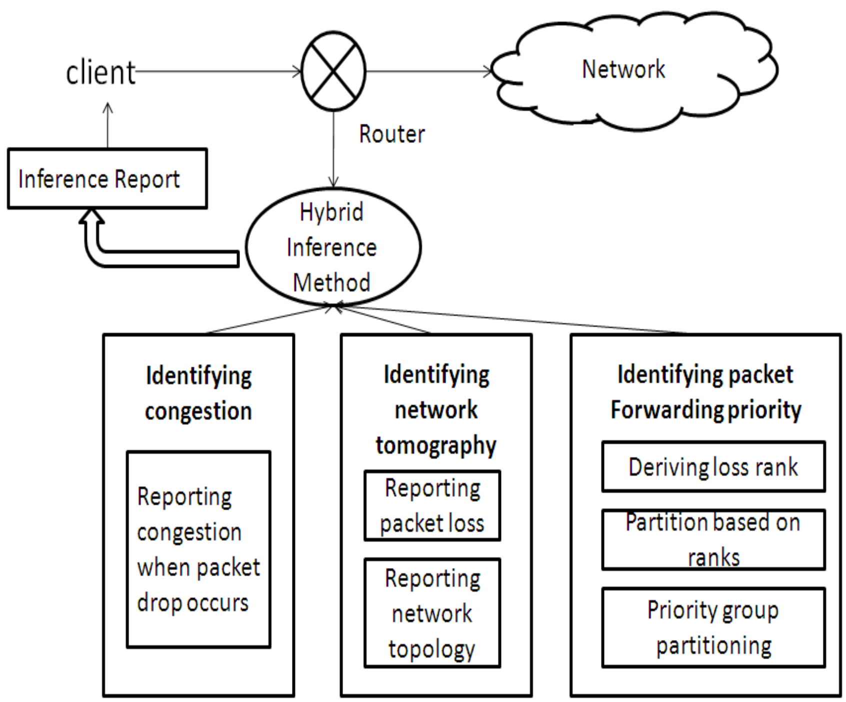

Fig4. A hybrid inference method for network characteristics

B. Identifying congestion and network tomography

Congestion: In network, current internet transport protocols make end-to-end measurements and maintain per-connection state to regulate the use of shared network resources. When two or more such connections share a common endpoint, there is an opportunity to correlate the end-to-end measurements made by these protocols to better diagnose and control the use of shared resources. Hence we go for probing technique to determine whether a pair of connections experience shared congestion. When packets are dropped at certain node, we identify that congestion occurs at that node. We identify the point of congestion when the path is overloaded and packets are dropped. Once we have identified congestion, we have few choices to deal with congestion. We can add more bandwidth, perform quality of service (QoS) on the traffic or compress the traffic. It depends on the user.

Network tomography: The problem of identifying topology and inferring link-level performance parameters such as packet loss, packet drop rate or delay variance using only end-to-end measurements is commonly referred to as network tomography. Active measurement technique has been designed using both unicast and multicast measurement to estimate link-level performance parameters such as loss rate and delay variance, in addition to identifying topology.

C. *Identifying packet forwarding priority*

It takes the following three steps to infer packet forwarding priority inference. First, it sends a relatively large amount of traffic to temporarily saturate the bottleneck traffic class capacity, which gives hybrid inference method a better resistance against background traffic fluctuations. Secondly, we apply a robust non-parametric method based on the ranks instead of pure loss rates. Thirdly, we assign a rank-based metric to each packet type and use a hierarchical clustering method to group them when there are more than two packet types. Hence we can identify packet forwarding priority at end-user level.

D. Analysis and Inference report

We validated our approach via statistical analysis and NS2 simulation. Here we have used dumbbell topology for NS2 simulation which is shown in Fig 5. The graph is generated to infer packet loss rate and packet drop rate is shown in Fig 6, 7.

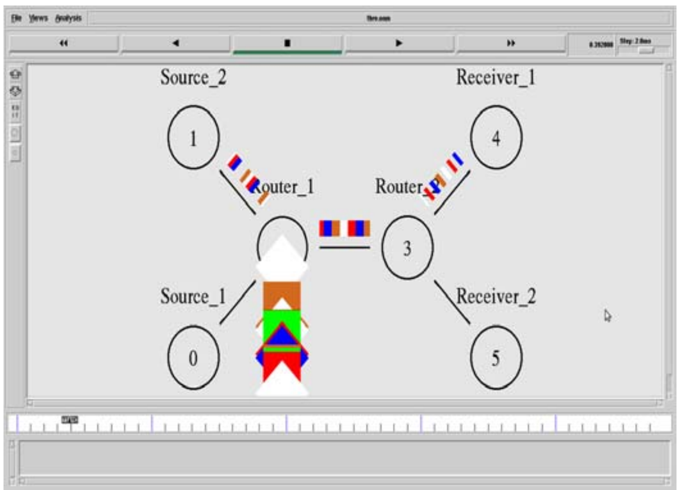

Fig5. Dumbbell topology using NAM Animator in NS2

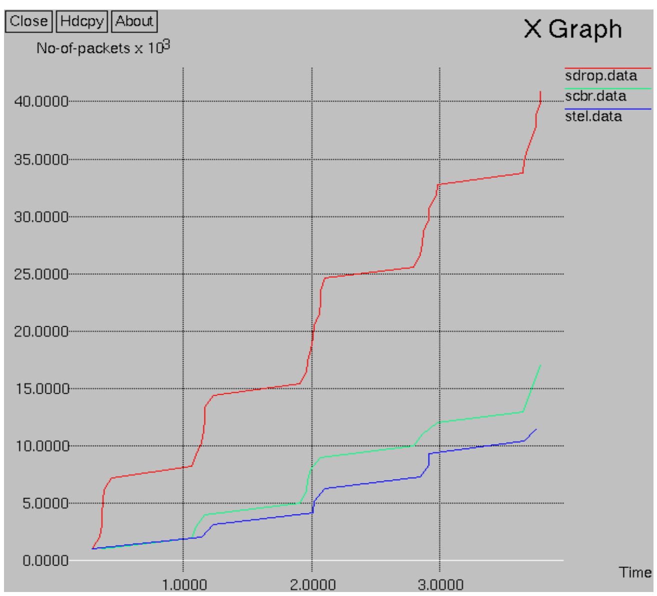

Fig6. Drop rate of CBR, Telnet packet in SFQ queue

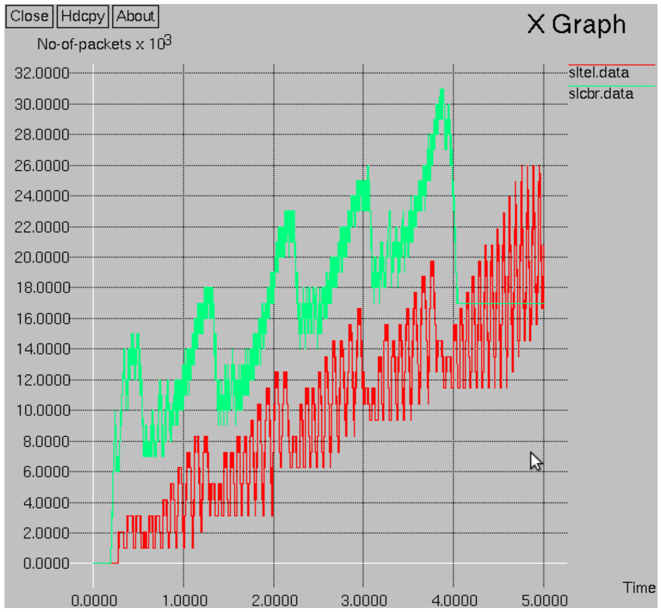

Fig7. Loss rate of CBR, Telnet packet in SFQ queue

Table 2 Drop rate, Loss, Loss rate of Telnet and CBR packet in different queuing discipline

	DROP RATE			LOSS			LOSS RATE		
Queuing Discipline	Drop Tail	RED	SFQ	Drop Tail	RED	SFQ	Drop Tail	RED	SFQ
TELNET	8320	15000	17000	20800	22880	20800	1.01765	1.01838	1.01722
CBR	2000	15000	17000	20000	15000	17000	1.00756	1.00666	1.00088

We have formulated the packet loss, packet loss rate, packet drop rate in Table 2 for two different packet types (CBR, Telnet). We analyzed this in three different queuing disciplines (Drop tail, RED, SFQ). Drop rate is the number of packets dropped due to congestion. Loss is calculated by difference between number of packets sent and number of packets received. Loss is calculated by finding the ratio between number of packets sent by number of packets received. Based on these values we will calculate loss ranks for packet forwarding priority and cluster then accordingly. Congestion is identified by node which drops packet (point of congestion). Network tomography is inferred by packet loss rate and packet drop rate.

V. CONCLUSION

In this paper, we studied an analysis of different inference methods for network characteristics to deal with shared congestion, packet forwarding priority, network tomography and evaluate each methodology based on packet loss rate. We have proposed a hybrid inference method based on the packet loss statistics. This hybrid inference will act as the end-user network analysis tool to know shared congestion, packet forwarding priority, and network tomography. Our evaluation shows the hybrid inference methods at End-user level will help the users and network administrators in better way to know network characteristics which are private at router level through various approaches.

REFERENCES

[1] CAIDA: Cooperative Association for Internet Data Analysis. http://www.caida.org/Tools/.

[2] Networking tools and monitoring devices. http://network-tools.com/.

[3] Felix: Independent Monitoring for Network Survivability. http://belore.Com/pub/mwg/felix/index.html.

[4] IPMA: Internet Performance Measurement and Analysis. http://www.Merit.edu/ipma.

[5] Mtrace: Tracing multicast path between a source and a receiver. http://Xerox.com/pub/netsearch/ipmulticast.

[6] R.Caceres, N. G. Duffield, S. B. Moon, and D. Towsley. Inference of Internal Loss Rates in the MBone. In IEEE *Global Internet (Globecom),* Rio de Janeiro, Brazil, 1999.

[7] V. Padmanabhan. Optimizing Data Dissemination and Transport in the Internet. Presented at the BU/NSF Workshop on Internet Measurement, Instrumentation and Characterization, September 1999.

[8] S. Ratnasamy and S.McCanne. Inference of multicast routing trees and Bottleneck bandwidths using end-to-end measurements. In *Proceedings* Of IEEE INFOCOM'99, pages 353-60, March 1999.

[9] M. Yajnik, S. Moon, J. Kurose, and D. Towsley. Measurement and Modelling of the temporal dependence in packet Loss. In Proceedings *Of IEEE INFOCOM '99,* pages 345-52, March 1999.

[10] H. Balakrishnan, H. Rahul, and S. Seshan. An Integrated Congestion Management Architecture for Internet Hosts. In *Proceedings of SIGCOMM'99*, Cambridge, MA, September 1999.

[11] V. Padmanabhan. Coordinated Congestion Management and Bandwidth Sharing for Heterogeneous Data Streams. In *Proceedings of NOSSDAV'99*, Basking Ridge, NJ, June 1999.

[12] L. Gautier, C. Diot, and J. Kurose. End-to-end Transmission Control for Multiparty Interactive Applications in the Internet. In *Proceedings of IEEE INFOCOM'99*, New York, NY, March 1999.

[13] J. Byers, M. Luby, and M. Mitzenmacher. Accessing Multiple Mirror Sites in Parallel: Using Tornado Codes to Speed Up Downloads. In *Proceedings of IEEE INFOCOM'99*, New York, NY, March 1999.

[14] A. Adams, T. Bu, R. Caceres, N.G. Duffield, T. Friedman, J. borowitz, F. Lo Presti, S.B. Moon, V. Paxson, and D. Towsley. "The Use of End-to-End Multicast Measurements for Characterizing Internal Network Behavior", *IEEE Communications Magazine*, May 2000.

[15] T. Bu, N.G. Duffield, F. Lo Presti, and D. Towsley. "Network Tomography on General Topologies". *UMass CMPSCI Technique Report*.

[16] M.J. Coates and R. Nowak. "Network Delay Distribution Inference from End-to-end Unicast Measurement," Proc. Of the IEEE International Conference on Acoustics, Speech, and Signal Processing, May 2001.

[17] M. Aron, P. Druschel, andW. Zwaenepoel. Cluster reserves: A Mechanism for resource management in cluster-based network servers. In *Proceedings of ACM SIGMETRICS 2000*, June 2000.

[18] J. Bennett and H. Zhang. WFwQ:Worst-case FairWeighted Fair Queueing. In *Proceedings of IEEE INFOCOM '96*, San Francisco, CA, March 1996.

[19] K. Harfoush, A. Bestavros, and J. Byers, "Robust identification of Shared losses using end-to-end unicast probes," in *Proc. IEEE ICNP*, 2000.

[20] D. Rubenstein, J. Kurose, and D. Towsley, "Detecting shared Congestion of flows via end-to-end measurement," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, pp. 381–395, 2002.

[21] A. Coates, A. Hero III, R. Nowak, and B. Yu, "Internet tomography," *IEEE Signal Processing Magazine*, vol. 19, no. 3, pp. 47–65, 2002.

[22] M. Rabbat, R. Nowak, and M. Coates, "Multiple source, multiple destination network tomography," in *Proc. IEEE INFOCOM*, 2004.

[23] G. Lu, Y. Chen, S. Birrer, F. E. Bustamante, C. Y. Cheung, and X. Li, "POPI: A User-level Tool for Inferring Router Packet Forwarding Priority," in *Proc. IEEE INFOCOM*, 2010.