© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Tracing the Packet Loss between Different Nodes within Same Link at Particular Interval of Time

Dr. Rajdev Tiwari*, Parul Sirohi

Department of Computer Science and Engineering, Noida Institute of Engineering & Technology, Uttar Pradesh, India

ABSTRACT

Realistic and accurate packet loss measurement of production traffic has been challenging, since the frequently-used active monitoring approaches using probe packets cannot capture the packet loss experienced by the traffic of individual user applications. In this paper, we present a new approach for the accurate measurement of the packet loss rate faced by nodes at same link at particular instant of time. In contrast to previous work, our method is able to pinpoint the packet loss rate experienced by the individual traffic flows of concurrently running applications. Due to the exponential back-off scheme, one of these connections could gain an unfair advantage in channel access. If both the connections generate heavy loads, then the connection that began first will dominate the channel. If one of the connections is heavily loaded, while the other is lightly loaded, the heavily loaded connection dominates the channel.

Keywords: Advantage of longer Connection, Architecture Of packet Loss, Calculation Communication within Same Link, Metrics for pattern of Loss

I. INTRODUCTION

Packet loss is an important performance characteristic of network traffic, crucial for applications including long-range data transfers, video and audio transmission, as well as distributed and GRID computing. Unfortunately, most of the existing tools report only network link packet loss rate and cannot measure the actual packet loss experienced by the traffic of individual applications. Most of the existing techniques are based on active network monitoring, which involves the injection of probe packets into the network for measuring how many of them eventually reach their final destination [2, 10, 11]. Although these approaches approximate the overall packet loss of a link, they inherently cannot measure the packet loss faced by the traffic of individual applications. To make matters worse, for accurately approximating bursty and volatile packet loss events, active monitoring methods need to inject a large number of packets, increasing their intrusiveness in the network, and possibly perturbing the dynamics of the system. When using a small number of probe packets to avoid a high level of intrusiveness, such methods need to run for a long period, and then are only able to approximate packet loss rates that remain constant for a long duration a highly unlikely case in real networks.

II. METHODS AND MATERIAL

A. Unfair Advantage To Longer Connections

The longer the connection in terms of number of hops the more likely are the link failures due to mobility. Thus, longer connections are more likely to suffer from degraded throughput. Shorter connections will have an unfair advantage: improved throughput due to the ability to transmit more packets.[14]

- Packet Losses due to Mobility

When nodes move, links tend to break, and get formed again. When the SIR is below certain threshold, the MAC layer concludes that the link is broken.

This would create an interrupt at the routing layer. Now, the routing protocol has to deduce the new location of the destination. It keeps reducing the transmission window and trying to retransmit.

This leads to unnecessary retransmissions when there is no link beginning at slow start when the link comes up again. ICMP may be used to detect link failures etc.[8] (Notice at the IP layer) SNMP could be used for fault management. But these are slow.. If links fail often, but you know that recovery is possible, then aborting the connection each time may not be the right thing to do.

B. Architecture of Packet Loss

Over the past few years, we have been witnessing an increasing deployment of passive network monitoring sensors all over Europe [5].

In this paper, we propose to capitalize on the proliferation of passive monitoring sensors and use them to perform accurate per-application packet loss measurements. Our approach is quite simple: assuming a network path equipped with two passive monitoring sensors at its endpoints, as shown

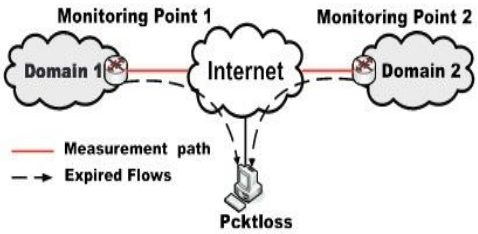

Fig. 1. Overall architecture of PcktLoss.

C. Related Work

Ping is one of the most popular tools for inferring basic network characteristics, such as round-trip time and packet loss. Ping sends ICMP probe packets to a target host at fixed intervals, and reports loss when the response packets are not received within a specified time period. Although ping has been used as a first-cut mechanism for link packet loss estimation, its applicability has recently started to get limited because several routers and firewalls drop or rate-limit ICMP packets, which introduces artificial packet loss that undermines the accuracy of the measurement. Instead of using ICMP packets, zing [2] and Badabing [11] estimate end-to-end packet loss in one direction between two cooperative end hosts by sending UDP packets at pre-specified time intervals.

Sting [10] overcomes the limitation of requiring two cooperative hosts by measuring the link loss rate from a client to any TCP-based server on the Internet based on the loss recovery algorithms of the TCP protocol. Benko and Veres have proposed a TCP packet loss measurement approach based on monitoring sequence numbers in TCP packets [4]. Our approach uses a completely different estimation approach, independent from the L4 protocol specification, and thus can be universally applied to both TCP and UDP connections. Ohta and Miyazaki [8] have explored a passive monitoring technique for packet loss estimation relying on hash-based packet identification. Their work is similar to our approach, but ours differs in that it matches packets to flows and compares flows with each other for computing the packet loss, while theirs hashes the packet's payload and correlates them. Our approach is more lightweight and thus can be performed on-line, while Ohta and Miyazaki's technique needs to stop monitoring for computing the packet loss.

D. Approach For Calculating Communication Between Samelink

802.11 wireless devices have become commonplace in today's computing environment. In both the home and in business, the easy deployment of wireless is leveraged in order to provide Internet connectivity to users. The potential applications for wireless communication are extensive ranging from Internet connectivity to games to military-based applications as well as numerous other applications. Considering the ubiquity of 802.11 devices, it is important to correctly understand the characteristics of the wireless medium in order to improve wireless performance [1]–[5]. Chief among the characteristics is an understanding of the underlying loss dynamics of the medium due to the significant implications for reliability and interaction with higher level network layers. Traditionally, errors in the physical medium have been viewed as the dominant factor in patterns of packet loss. In contrast to previous work, this paper points to a significant alternative source of error, the wireless device itself. We justify our findings through two key observations from our experiments:

- Lack of Packet Loss Correlation:

It is expected that nodes in immediate proximity would exhibit highly correlated loss if loss is primarily determined by the physical medium. In our experiments, we show that the packet loss correlation between closely located nodes is low, indicating that a substantial portion of loss is due to localized errors at the receiving device. Moreover, the results occur consistently despite observations across different days, different positions, and different close proximities.[16]

- Varying Loss Burstiness:

It would be expected that different but closely located wireless devices should display similar patterns of loss burstiness if physical medium errors are the dominant source of packet loss. Conversely, we show how several popular wireless cards have significantly different loss patterns despite possessing a similar overall loss rate. While other works have attempted to understand the underlying sources of packet loss by dispersing numerous monitoring nodes throughout an environment [3], [6], the works make implicit assumptions regarding the accuracy of the devices. In contrast, our experiments took a skeptical view of the accuracy of a single device with regards to physical medium loss by placing multiple devices in close proximity. To that end, we investigated a variety of scenarios and configurations by validating our results over multiple monitoring periods, monitoring environments, device placement, and device orientations. [17]

E. Metrics for Patterns of Loss

A common method, also known memory-based loss, as presented in [1], [2] is defined as: P(li+k|li) where the above is read: the probability of dropping the (i+k)th packet given that the Ith packet is lost. For small values of k, if Eq. 1 is greater than the overall loss (P(li)), than the loss can be said to be bursty. For larger values of k, if the P(li+k|li)> P(li) , then that likely indicates a periodic source of interference (ex. beacon interval), not an inherent property of the wireless medium.

Conversely, the works in [3], [4] propose using a modified Allen Deviation to capture burstiness. The modified Allen Deviation measures the average change in loss between adjacent, fixed time intervals as defined by:

$$\Sigma n = sPNi = 2(yi - yi-1)^2 / 2(N-1)$$

Where yi is the loss at time interval i, and N is the number of time intervals. It is important to note, that unlike the original Allen Deviation, the modified Allen Deviation is not dimensionless and provides an exact measurement of the average variation in loss. In order to determine if loss is bursty, results are graphed against data generated from a uniform pseudo-random number generator. If the two plots overlap significantly, the loss is not bursty. If the two plots are distinct, then the loss shows a trend towards burstiness.[18]

F. Four Sources of Packet Delay

1. Nodal processing:
– check bit errors
– determine output link

2. Queueing
– time waking at output link for transmission
– depends on congestion level of router

3. Transmission delay:
– aka store & forward delay
– R=link bandwidth (bps)
– L=packet length (bits)
– time to send bits into link =L/R

4. Propagation delay:
– d = length of physical link
– s = propagation speed in medium (~2x108 m/sec)
– propagation delay = d/s

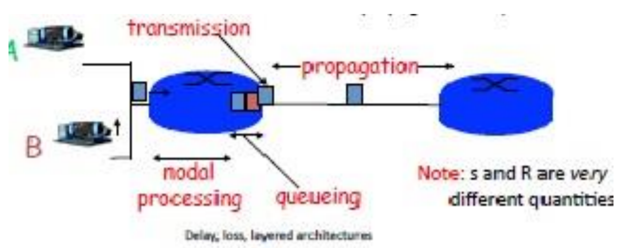

Figure 2: Four Sources of packet Delay

III. CONCLUSION

We have concluded that under many conditions, instantaneous packet loss within same link between particular interval of time are not highly correlated as would be expected. However, the two identical nodes do exhibit similar patterns of loss (both memory-based and modified Allen Deviation measurements) indicating that the observed patterns of loss by an individual node may be a property of the wired device itself. Importantly, we show that while one device may display large amounts of burstiness in loss, when the results are combined from the receivers, the burstiness of loss is significantly reduced. This paper demonstrates the importance of not assuming that the pattern of loss received at a single node indicates the true performance of the wired medium. We presented the design and implementation of Packet Loss, a novel method for the accurate measurement of the packet loss faced by user traffic. Based on passive network monitoring, Packet Loss can measure the packet loss ratio of individual traffic flows, allowing pinning point loss events for specific classes of traffic. Our experimental evaluation and real-world deployment have shown that Packet Loss can precisely measure the packet loss rate even when monitoring multi-Gigabit traffic speeds.

IV. REFERENCES

[1] Hades active delay evaluation systemhttp://www-win.rrze.uni-erlangende/ippm/hades.html.en.

[2] Andrew Adamns, Jamshid Mahdavi, Matthew Mathis, and Vern PaxsonCreating a scalable architecture for internet measurementIn Proceedings of INET, 1998.

[3] BAdamson The MGEN Toolset http://pf.itd.nrl.navy.mil/mgen.

[4] Peter Benko and Andreas VeresA Passive Method for Estimating End-to-End TCP Packet LossIn Proceedings of IEEE Globecom, pages 2609–2613, 2002.

[5] SBradner and JMcQuaidBenchmarking Methodology for Network Interconnect Devices RFC 2544 (Informational), March 1999 http://www.ietf.org/rfc/rfc2544.txt.

[6] SHemmingerNetwork Emulation with NetEmIn Proceedings of Linux Conf Au, 2005.

[7] THolleczeckStatistical analysis of IP performance metric in international research and educational networks (diploma thesis), 2008.

[8] SOhta and TMiyazakiPassive packet loss monitoring that employs the hash-based identification techniqueIn Ninth IFIP/IEEE International Symposium on Integrated Network Management (IM), 2005.

[9] APapadogiannakis, AKapravelos, M Polychronakis, EPMarkatos, and ACiuffolettiPassive end-to-end packet loss estimation for grid traffic monitoringIn Proceedings of the CoreGRID Integration Workshop, pages 79–93, 2006.

[10] Stefan SavageSting: A TCP-based network measurement toolIn USENIX Symposium on Internet Technologies and Systems (USITS), 1999.

[11] Joel Sommers, Paul Barford, Nick Duffield, and Amos RonImproving accuracy in end-toend packet loss measurementIn Proceedings of the ACM SIGCOMM '05, pages 157–168.

[12] SUbik, VSmotlacha, STrocha, SLeinen, VJeliazkov, AFriedl, and GKramerReport on passive monitoring pilot, September 2008Deliverable MS.3.7.5 GN2 Project.

[13] Sven Ubik, Aleˇs Friedl, and Stanislav HotmarQuantification of traffic burstiness with mapi middlewareSeptember 2008.

[14] QLv, PCao, ECohen, KLi, and SShenkerSearchand replication in unstructured peer-to-peer networks In ICS'02, New York, USA, June 2012

[15] Christos Gkantsidis, Milena Mihail, and Amin Saberi, Random Walks in Peer-to-Peer Networks, to appear in IEEE Infocom 2014

[16] Yatin Chawathe, Sylvia Ratnasamy, Lee Breslau, Nick Lanham, and Scott Shenker, Making Gnutella-like P2P Systems Scalable, In ProcACM SIGCOMM 2003, Karlsruhe, Germany, Aug 2013.

[17] CLaw and K.-YSiu, Distributed construction of random expander networks, In ProcIEEE Infocom 2013

[18] Gopal Pandurangan, Prabhakar Raghavan, and Eli Upfal, Building low-diameter p2p networks, In STOC 2011, Crete, Greece, 2011

AUTHOR'S PROFILE

Dr.Rajdev Tiwari having work experience of more than 16yr. Completed phd from Computer Science in 2012 from Dr. B.R ambedkar University AGRA. Completed Master of Computer Application in 2005 from Indra Gandhi National Open University. Also completed Master of Science in 1997 from Dr. Rammanohar Lohia Awadh University Faizabad

Parul Sirohi persuing M.tech from Computer Science in 2013 from Noida Institute of engg. & Technology, Greater noida. Completed B.tech in Information Technology in 2012 from Gyan Bharti Institute Of Technology Meerut. My area of interest are Computer Network and Operating System.