Journal of Network and Computer Applications 32 (2009) 367–376

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

One-way queuing delay measurement and its application on detecting DDoS attack ☆

Wei-Zhou Lu *, Wei-Xuan Gu, Shun-Zheng Yu

Electronics and Communication Engineering Department, Sun Yat-Sen University, PR China

ARTICLE INFO

Article history:
Accepted 20 February 2008

Keywords:
One-way queuing delay measurement
Gerchberg-Saxton algorithm
DDoS attack

ABSTRACT

This paper presents a novel approach to measure and estimate end-to-end one-way queuing delay in a network, which carries information about traffic characteristics and congestion properties. The measurement results can be used to describe the normal behavior of the network and detect distributed denial-of-service attacks (DDoS attacks). The measurement does not require any synchronization between the two measurement ends. Pairs of probe packets are sent from the source to the destination and intra-gaps between the probes are separately measured at the two ends. By performing an iterative Fourier-to-time reconstruction algorithm on the measured intra-gaps, distribution of the end-to-end one-way queuing delay is estimated. The packet loss rate and delay jitter are simultaneously measured as well. The simulations and experiments are conducted to validate the approach.

1. Introduction

Distributed denial-of-service attack (DDoS attack) is a major threat to Internet. DDoS attack generates a large volume of traffic loads, exhausting service resources on the target nodes and consequently degrading the overall network performance, to deny service to legitimate users. DDoS attacks have drawn great interest of network researchers, and many detection and defense schemes are put forward. A few researchers (Long et al., 2005; Mirkovic et al., 2006) tried to evaluate the network performance under DDoS attacks, but none of them offered online measurement.

Accurately measuring network performance is very important in defending DDoS attacks. Firstly, detecting the severe change of network performance may help researcher to detect DDoS attack quickly. Secondly, measuring network performance during DDoS attack can help network operators to evaluate the severity of the attack and know about end-users' experience, therefore they can take some actions such as redirection and load balance. Thirdly, measuring the improving network performance can help researchers to evaluate the efficiency of defense schemes and make a tradeoff between defense schemes' efficiency and their price.

Network performance can be described by several metrics: packet loss rate, one-way delay (OWD), delay jitter, throughput, request/response delay. Among these metrics, we focus on the measurement of packet loss rate, OWD and delay jitter. Packet loss rate is defined as a ratio of the number of lost packets to the total number of transmitted packets. OWD is the time taken for a packet transmitting from the sender to the receiver. Delay jitter is the variation in delay over time from end-to-end.

Packet loss rate and delay jitter can be measured easily by sending probes from the source to the destination (Paxson, 1999). However, OWD is hard to measure because of the clock synchronization problem. Each node distributed in the network has its own time system, and clock offsets and skew ways exist among these nodes. If one simply uses the timestamps recorded at both ends, he will have a measurement that includes not only the actual OWD along the path, but also the corresponding clock difference between the two ends. For the worst case that the clock at the receiver lags a lot behind the clock at the sender, it will even lead to a negative one-way estimation result. Network Time Protocol (NTP) and Global Positioning Systems (GPS) have been used to solve the clock synchronization problem, but neither of them is suitable in measuring the impact of DDoS attack.

OWD contains deterministic delay and stochastic delay. Since deterministic delay does not change over time, it can be measured once and used repeatedly. The method measuring deterministic delay has been shown in Gurewitz et al. (2006). This paper focuses on measuring the stochastic delay, which means one-way queuing delay. One interesting but noticeable observation is that, contrary to the broad analyses of end-to-end OWD measurements, little

☆ This work was supported by the Key Program of NSFC-Guangdong Joint Funds (U0735002), The National High Technology Research and Development Program of China (2007AA01Z449).

* Corresponding author.
E-mail addresses: isp04lwz@mail2.sysu.edu.cn (W.-Z. Lu), willson11@21cn.com (W.-X. Gu), syu@mail.sysu.edu.cn (S.-Z. Yu).

1084-8045/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2008.02.018

attention has been paid to the inference of one-way queuing delay and its distribution. In fact, one-way queuing delay has the greatest significance because it is the variable delay component indicating the dynamics of network congestion along the path. As an example for the security problem when geo-locating Internet hosts based on delay measurements, an efficient estimation of queuing delay may greatly shrink the confidence region and improve the precision of identifying attackers or victims (Bamba et al., 2006).

This paper is organized as follows. In the next section we describe the probing process, the reconstruction of one-way queuing delay distribution and measurement of other metrics. Then in Section 3, we conduct simulation and experiments. Section 4 introduces some related studies on OWD estimation, and the final section concludes the paper.

2. End-to-end measurement without clock synchronization

As with most studies, we actively send probing packets to conduct our measurement. Active measurements capture probing packets instead of background traffic packets. Different with traditional methods, our measurement approach presented in this section simply relies on the intervals that are separately measured at the sender and the receiver, so it need not consider any synchronization problems. In this section, we mainly describe the one-way queuing delay measurement, among which packet loss rate and delay jitter can also be measured.

2.1. One-way queuing delay

When a packet is transmitted throughout a multi-link path, it encounters two delay components that compose the overall end-to-end OWD. One is deterministic and the other is stochastic.

The deterministic delay is the sum of propagation delay and transmission delay on each link along the path. Propagation delay is the time to transmit a signal from one node to another. It is solely dependent on the physical medium and the distance between the nodes, and generally signals going through a wire or fiber travel at two-thirds the speed of light. Transmission delay is the time required to transmit all of the packet's bits onto a link, and is determined by the link capacity and the packet size. Because link conditions along the path do not change during a measurement, and probe packets we will send are of the same size, this deterministic delay is a constant component of the end-to-end OWD. Here we do not assume the deterministic delays are identical in forward and return directions, since the links' distances and capacities may be totally different.

The stochastic delay is the sum of queuing delays. Because of the existence of background traffic and cross traffic on the links, each packet arriving at a node would be queued in the output interface and could not be processed until the currently transmitted and the previously waiting packets finish all their transitions. The queuing time changes from packet to packet and also from node to node, subject to the congestion level along the path. Hereby it is a variable delay component.

In our study, we use $d^{(j)}$ to denote end-to-end OWD for the jth probing packet going through the path, and $c^{(j)}$ and $v^{(j)}$ the constant and variable delay, respectively. Obviously $d^{(j)} = c^{(j)}+v^{(j)}$ and we have $c^{(j)} = c^{(l)}$ for any arbitrary probe packets j and l in the measurement. Estimation for $c^{(j)}$ could be based on some existing methods (Gurewitz et al., 2006), and our approach to be discussed in the following is to effectively measure the stochastic delay $v^{(j)}$ regardless of $c^{(j)}$.

2.2. Non-synchronization measurement

In our scheme, pairs of UDP probing packets are sent from the sender to the receiver to measure network performance. The format of probe packets is shown in Fig. 1. The pattern index field and two parameter fields indicate the probing pattern and the probing parameters. We only present one probing pattern in this article. In this probing pattern, the sending intervals between adjacent pairs are identical, and the sending intervals between two packets in the same pair are also identical, as shown in Fig. 2. The parameter 1 field records the sending interval between adjacent pairs, while the parameter 2 field records the sending interval between two packets in the same pair. The parameter fields help the receiver to reconstruct the distribution of queuing delay. The total number field records the total number of probing pairs in the measurement. The pair index is the sequence number of the probing pair which the probing packet belongs to. The packet index field identifies the position of the probing packet in probing pair. These fields help the receiver to identify each probing packet, terminate the receiving process and measure packet loss rate or delay jitter. The last field, the padding field, is an optional field, which is used to change the size of probing packet. Note that the probing packet does not contain any information of the exact sending time because we do not need the information to solve the clock synchronization problem.

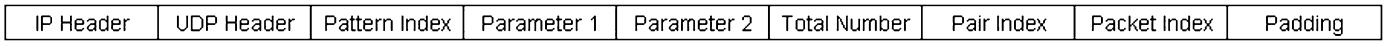

Fig. 1. Format of probing packet.

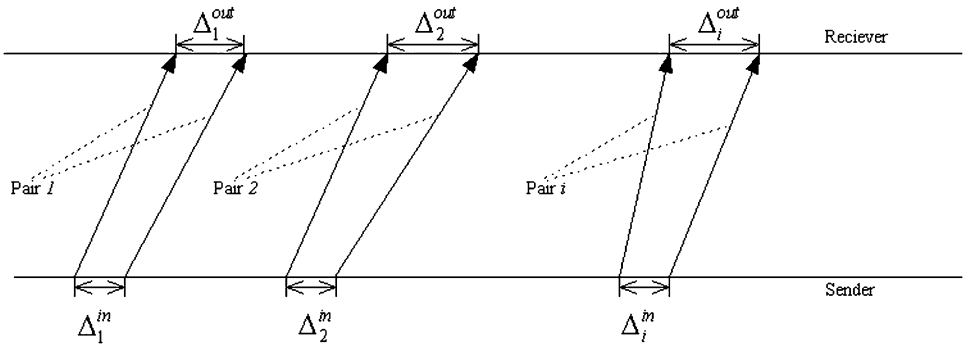

Fig. 2. Probing packet sending pattern.