Empirical Study on RTT Measurement for the Authentication Scheme in a DRM System

Arjulie John P. Berena, *Graduate School of Electronics Engineering, N ihon University*
Yusuke Kojima, *Graduate School of Electronics Engineering, Nihon University*
Takahiro Tsuchiya, *College of Science and Technology, Nihon University*
Masami Kihara, *Faculty of the Graduate School of Electronics Engineering, Nihon University*

ABSTRACT

Packet delay is one of the most important metrics in network management and monitoring in the Internet. Recently, it has also been considered as a tool in distance estimation used for location-based services. In the Internet, packet delay is basically due to the link bandwidth, the propagation path distance, the number links, and the system resources at the end hosts. Quantitatively, the aggregate sum of the packet delay between the end hosts is practically equated to the constant and variable delay. The constant delay component is the minimum delay of the packet traversing the network and is usually associated with the packet transit time at an ideal condition, while the variable delay component is usually due to the queuing delay and the cross traffic effect that is represented by a long tail in the delay distribution.

There are several probe packet types being used in Internet measurement such as the single packet, packet pair and packet train. These probes packets have been described and used in many applications for the purpose of monitoring the condition and characteristics of the network path. Each of these probe packet types serve a specific purpose they are designed for. For example, *ping* and *traceroute*, uses single packet to measure RTT between the two hosts, while packet pair and packet trains are used to specifically estimate the available and bottleneck bandwidth of the given link.

In this paper, we will present an analysis of the various probe packet types for the purpose of measuring a stable round-trip time (RTT). We used the term “stable RTT” that means that every time we measure RTT, we can get the same value with minimal error, i.e., it possess a reproducibility characteristic. In initial experiment, we directly linked two computer running Linux OS and measured RTT using different probe packet types and in different parameters like packet size, inter-packet interval, and inter-packet train gap. Results show that varying the inter-packet interval affects the deviation of the delay distribution. This finding was attributed to the processing of probe packets at the network interface. Linux OS employs New Application Process Interface (NAPI) which operates in polling and interrupt modes; the rate of the incoming packets determines which mode NAPI operates. Without modification and tuning of the Linux OS, and just by carefully configuring the parameters of the probe packets, a highly stable RTT can be obtained.

Furthermore, we present an experimental analysis on the RTT measured in a real network environment. Our laboratory hosts the server machine wherein several client computers located around Kanto area access the server. The server sends the probe packets to the client and the client returns the packet back to the server, thus RTT is measured. As the RTT distribution exhibits long-tail which is caused by cross traffic, a packet filtering mechanism that is based on packet arrival times was employed in order to get a stable RTT.

The motivation behind achieving a stable RTT emerged after finding ways to enhance the authentication scheme for the New Digital Rights Management (DRM). The conventional authentication method uses username and password combination. However, this method pose a great deal of vulnerabilities especially that username and password can be guessed, forgotten, shared, or written down and subsequently lost or stolen. Moreover, it has also been reported that phishing attack is widely growing targeting service providers and financial institutions. Fraudulently acquired user information could then be used for spoofing. In our DRM system, we propose to enhance the authentication scheme by introducing a location-enforcement policy that is based on network location based on RTT. This policy ensures that access outside the permitted area is prohibited, thus spoofing could be prevented.