Timestamp-resolution Problem of Traffic Analysis on High Speed Networks

Péter Orosz, oroszp@unideb.hu

Tamás Skopkó, skopkot@med.unideb.hu

University of Debrecen, Faculty of Informatics

Widely used traffic monitoring applications such as *tcpdump* and *Wireshark* use the same common 32-bit *libpcap* library for traffic capturing. Only packets that meets the user-defined filtering criterias will be processed and stored. *Libpcap* assigns a *pcap* format compatible timestamp to all processed frames. We could consider that the more physical bandwidth is available for the transmission, the shorter the *inter-frame gaps* between consecutive frames. Therefore requirements put up for timestamp resolution must be proportional to the link speed.
Original 32-bit version of *libpcap* provides a 10^{-6} sec native resolution, however *pcap* fileformat supports a larger 10^{-9} sec timestamp value for each stored packets. On gigabit or faster networks timestamp resolution that works in the microsecond domain does not enable us to precisely reproduce the time-domain relation between consecutive frames. Therefore cross-layer post-analysis of the overall data transmission could drive to a false result. Independently from one other four impact factors could directly manipulate the generation of timestamps: hardware architecture, NIC driver operation mode, kernel and the *libpcap* itself.

In an idealised case the generated timestamp is always converging and suitably close to the real arrival and transmission time of each frames so to conserve the original inter-frame time values. Rudimentary prerequisite of authoritative measurement data is that both traffic directions *(RX/TX)* must be processed and timestamped equally. This requirement is always violated by at least one of the four mentioned factors due to several known causes.

Timestamp resolution of network monitoring applications must be increased according to the requirements of novel high speed data transmission technologies. In our paper we are going to investigate those software *(64-bit libpcap, kernel jiffies, ndelay())* and hardware *(interrupt és polling mode NIC driver, Rx/Tx queue depths)* factors that could provide us a high resolution *(< 5 x 10^{-9} sec)* timestamp on high speed network connections.

Keywords: *32-bit/64-bit libpcap, timestamp, inter-frame gap, inter-frame time, NIC driver, kernel, monitoring, time-domain resolution*