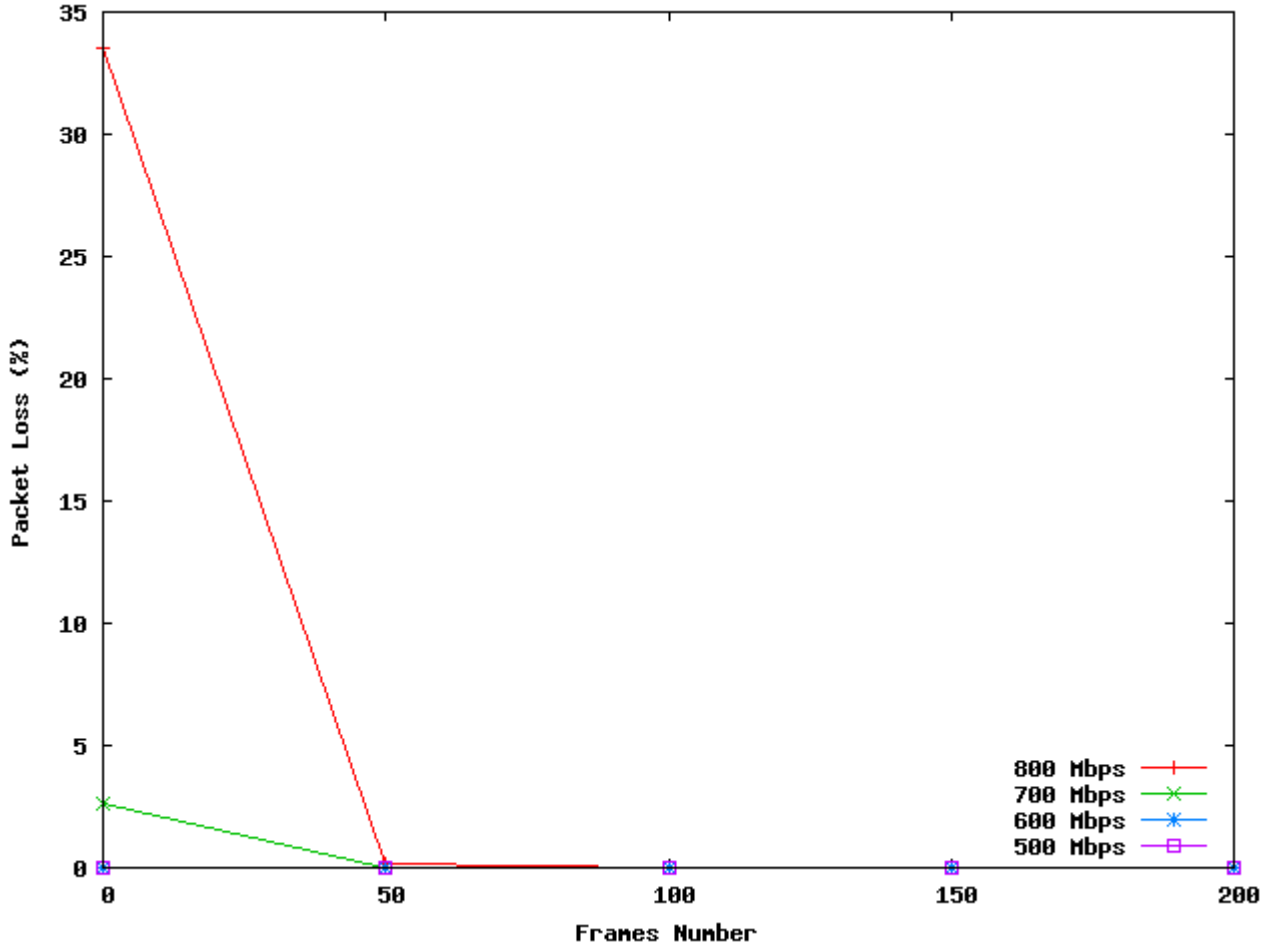
Evaluation of the mmap-pcap library

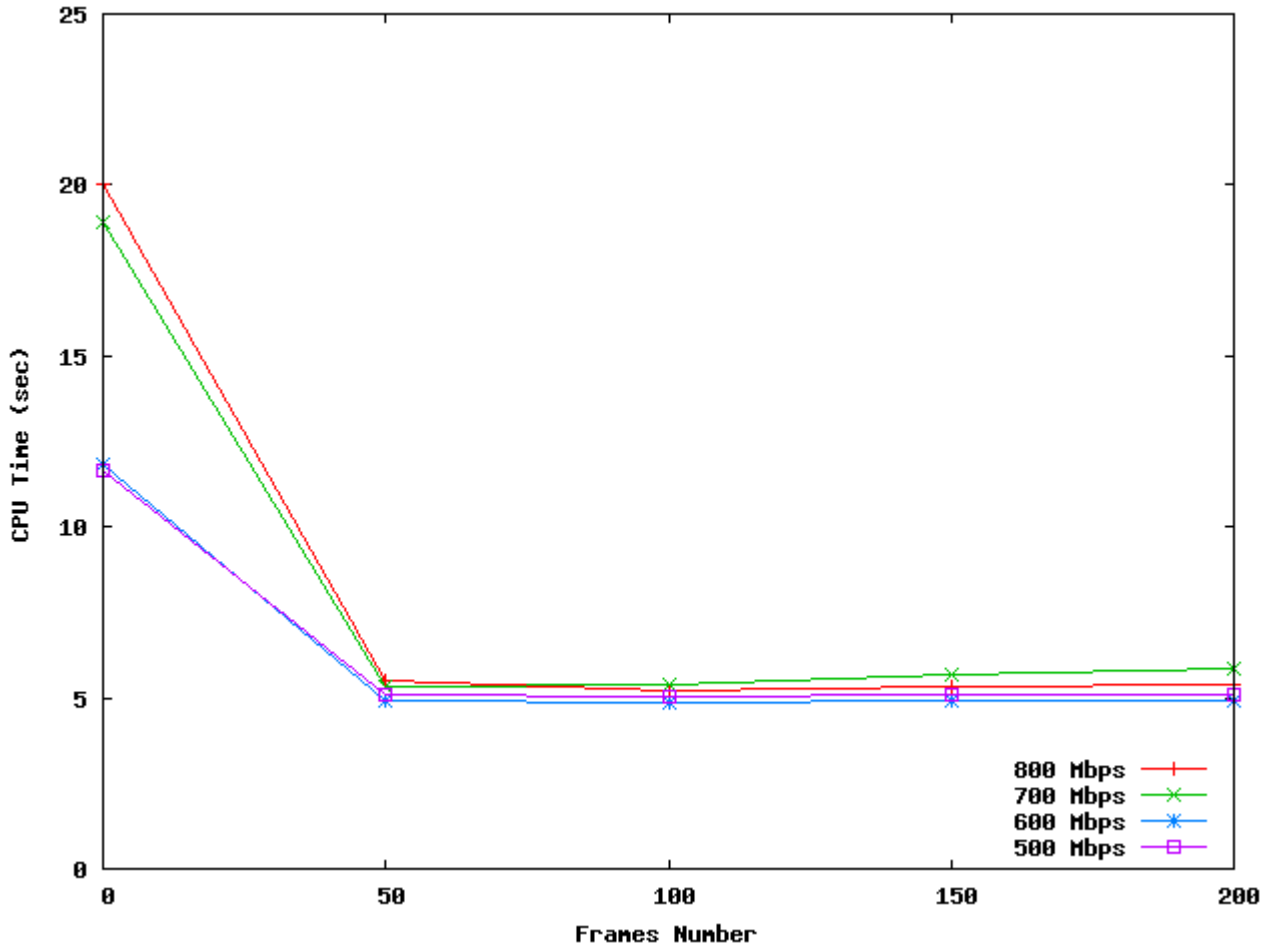
We used two different applications (tcpdump and snort) to measure the benefit of the mmap'ed version of the pcap library against the default one. The traffic was generated from another host with *nuttcp* utility at different speeds. The traffic sent constituted from 2 million packets for tcpdump application and 5 million packets for snort. Each packet was 1500 bytes (TCP protocol used).
The first application (tcpdump) simply captures the packets and ignores them by saving them to */dev/null*. No filters were used.
Snort was tested using with two different configurations: with and without preprocessors. The default rules were used both times.

For each application, the packet loss and cpu time were measured regarding the size of the ring buffer and the bandwidth rate. The size of the ring buffer used by the mmap-pcap is equal to Frames Number multiplied with the size of an Ethernet Frame plus 16 bytes (usually this is equal to 1516 bytes). When Frames Number are equal to zero (no ring buffer used), the behaviour of the mmap-pcap is the same with the default pcap library. Each experiment was repeated several times and the mean values were taken. The results are shown in the following figures.

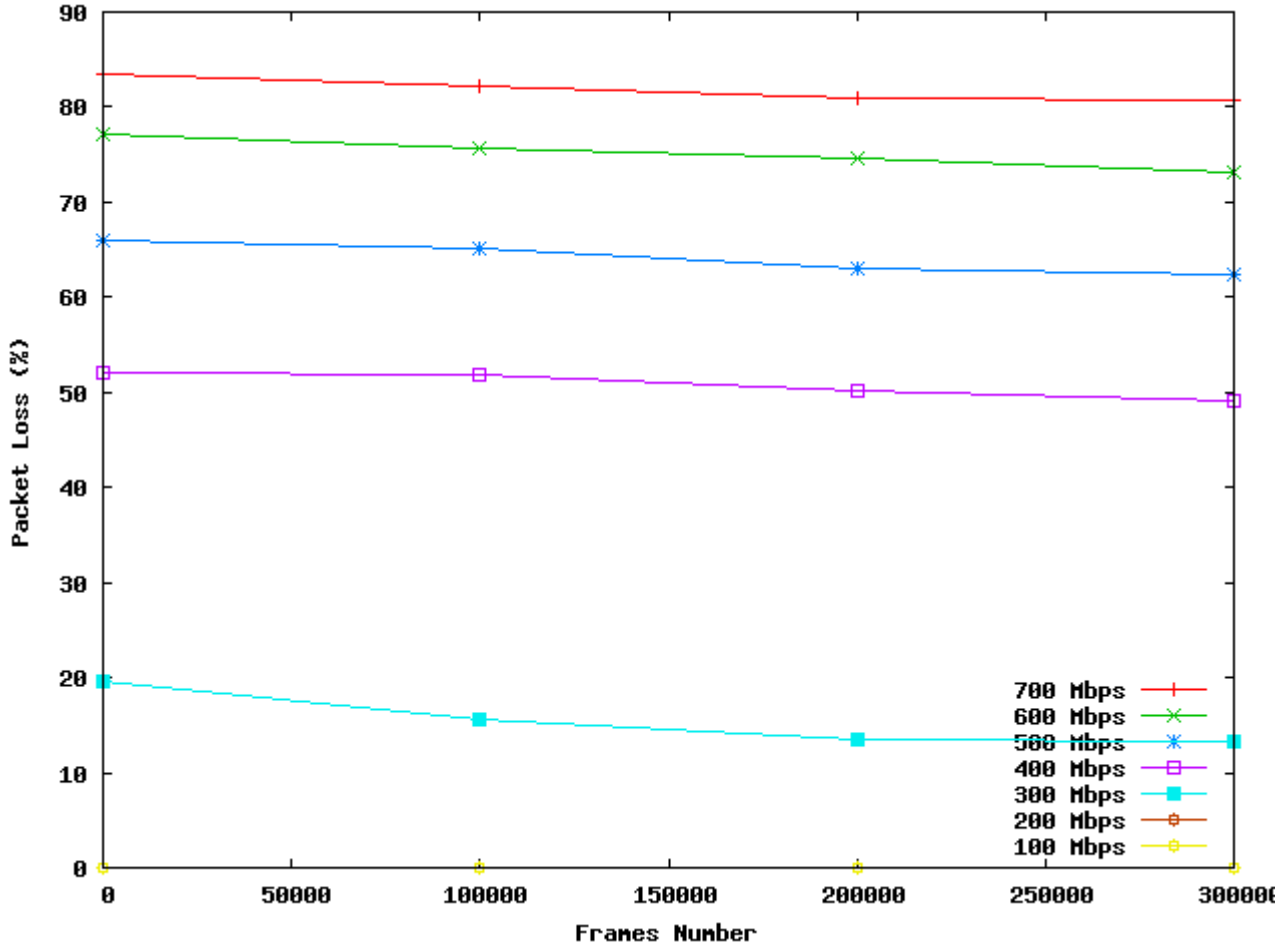
We observe that mmap-pcap improves packet capture performance under high traffic load.

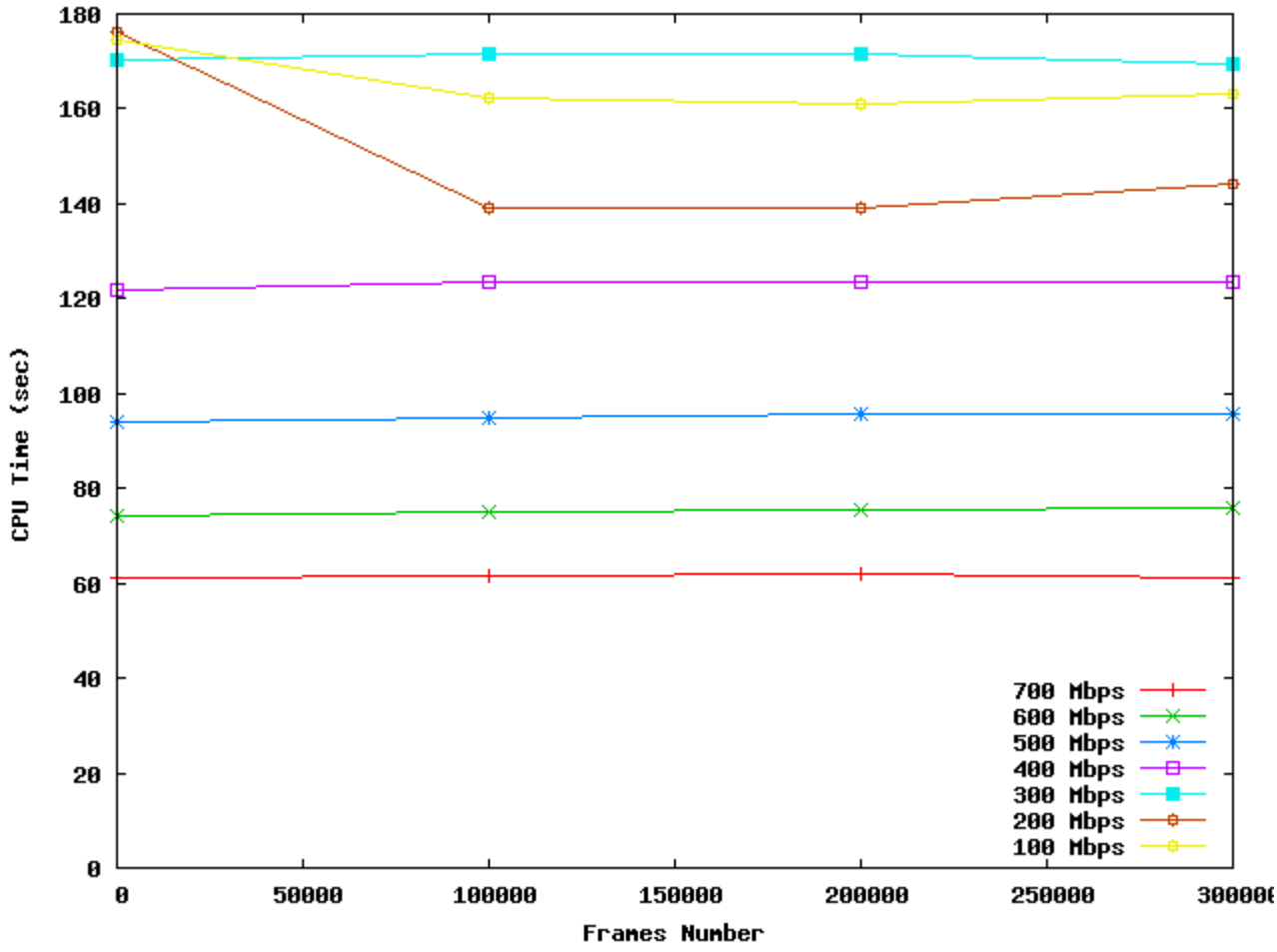
TCPDUMP Application





SNORT (with Default Rules and Preprocessors)





SNORT (Default Rules, Without Preprocessors)