Identifying TCP Congestion Control Algorithms

Using Active Probing

SeyedShams Feyzabadi(student) and Jürgen Schönwälder

{s.fezyabadi and j.schoenwaelder}@jacobs-university.de

Computer Science Department, Jacobs University Bremen, Germany

The Transmission Control Protocol (TCP) is widely used on the Internet and most of today's Internet traffic is carried over TCP. As a consequence, the performance of the Internet depends significantly on TCP's performance. One important aspect of TCP is the algorithm for controlling network congestion. On high bandwidth-delay product networks, the classic TCP congestion control algorithms do not work effectively since it takes a long time to open the congestion window to utilize the capacity of the network. This observation stimulated the design of several new congestion control algorithms. Meanwhile, some operating systems provide interfaces to choose at runtime from a set of congestion control algorithms or to even hotplug new customized congestion control algorithms into running operating system kernels. While several non-standard TCP congestion control algorithms are meanwhile available, so far no data is known to what extend they are deployed and used on the Internet. Dealing with traffic, using different congestion control algorithms will of course impact traffic shapes. With several TCP connections sharing the same link, performance of each connection has a significant effect on other connections. While it is a common assumption in many research papers and new protocol engineering efforts that the Internet traffic follows TCP's standardized congestion control behavior, it is not clear whether this assumption holds in today's deployed Internet. It might even be TCP traffic that does not behave "TCP friendly" at all. The goal of our work is to develop a technique to identify the congestion control algorithms used by remote TCP engines. Since direct access to this information via network management interfaces is generally not available due to access control restrictions and the lack of suitable managed objects, we choose an active probing approach. We have implemented a special test program capable of distinguishing and recognizing different TCP congestion avoidance algorithms. In practice, it is not possible to probe arbitrary TCP endpoints since our test tool needs to engage into a meaningful application layer protocol exchange. Furthermore, firewall policies and network address translators often block access to arbitrary TCP endpoints and only some well known ports are generally accessible. As a consequence, we chose web servers supporting the Hypertext Transfer Protocol (HTTP) as the main targets. Our tool sends a HTTP GET request to a web server, and based on the response, it tries to determine the congestion window size of the remote host. Having a series of window sizes, it computes a formula which represents the congestion window growth function. Then matching the obtained formula with standard TCP growth function, it identifies the running algorithm. At the moment this tool successfully detects Reno and Cubic TCPs. We believe that it is extendable to more complicated TCP algorithms as well.

Ps: No demo will be provided at the day of presentation.