

CSC2231 – Internet Systems and Services

Paper Review – Sting

Name: Alex Wun

Sting actively sends a specific sequence of TCP packets to measure the loss rate to and from an endpoint host. Sting purposely creates an initial sequence number “hole” in a series of transmitted TCP packets. By exploiting TCP’s fast retransmit behaviour (which dictates that an immediate ACK is sent for out-of-sequence packets), Sting can infer the number of packets that were dropped out of the transmitted series. The tool can also infer that a drop occurred on the reverse path if no ACK is received.

This active technique provides a portable approach with the unique ability to accurately distinguish between forward and reverse path loss rates. Additionally, the authors are able to make use of an existing protocol (TCP) for performance measurements – making the tool universally accessible.

However, the authors admit to encountering problems with Web Servers, operating systems, and firewalls that prevent their technique from working. In each case, they come up with ad hoc methods to circumvent these issues. It is interesting to note that Sting is essentially a misbehaving TCP client that abuses the protocol. The additional fact that the authors have needed to develop “workarounds” for some problems indicate that the type of measurement conducted by this tool is not welcome by most administrators. As such, widespread deployment of this tool is likely not a good idea.