**Title:** Detection Of Anomalous Traffic In Packet Switching Networks

**Abstract:**
We study application of information entropy for detection of anomalous traffic in packet switching network (PSNs), in particular distributed denial-of-service (DDoS) attacks. The attack is “distributed” because the attacker carries on his/her actions by means of multiple computers, located at various network nodes, and called “zombies”. We focus on the type of DDoS attacks directing a huge number of “ping” requests to the target victim of the attack. In this type of attack, the target (victim) machine becomes saturated with external communications requests, being pounded by spurious packets, so that it becomes effectively unavailable to legitimate traffic. Using a modified PSN model of the Network Layer of the 7-Layer OSI Reference Model and its C++ simulator, Netzwerk developed by us, we study the applicability of information entropy to detect DDoS attacks by monitoring changes in packet traffic at selected observation points in a network. Additionally, we study how DDoS attacks affect network performance indicators and spatio-temporal packet traffic dynamics.

This is a joint work with H. Wu and B.N. Di Stefano. The authors acknowledge the prior work of A.T. Lawniczak (A.T.L.) with A. Gerisch and X. Tang and the use of Sharcnet computational resources. A.T.L. acknowledges partial financial support from NSERC of Canada and H. Wu from the Univ. of Guelph.