Analysis of packet traffic in a data network model under normal traffic conditions & under distributed denial-of-service attack.

A.T. Lawniczak1, S. Xie1, H. Wu1 and B. Di Stefano2
1Department of Mathematics & Statistics, University of Guelph, Canada.
2Nuptek Systems Ltd., Canada

The Packet Switching Network (PSN) is a dominant technology of data communication networks. Many factors, e.g. routing algorithms, traffic load and type, network connection topology type, influence performance of PSNs. To achieve the desired network performance, one needs to study quantitatively which of these factors and which of their interactions have more significant effect on various network performance metrics measuring service delivery of packets.

A denial of service (DoS) attack is an attempt to make a computer resource normally available in a PSN unavailable to its intended users. In a distributed DoS (DDoS) attack, the attacker carries on his/her actions by means of multiple computers, called “zombies”, located at various network nodes, almost always controlled in a covert and surreptitious way, without any knowledge of their legitimate owners. For example, by issuing a huge number of ping, ‘echo requests’, from a very large number of zombies spread all over the network, it is possible to cripple the target victim rendering it so overloaded that it will eventually come to a standstill.

We present a modification of our existing PSN model of the Network Layer of the 7-Layer OSI Reference Model and its C++ simulator, Netzwerk [1,2,3] to study DDoS attack [4,5]. This modification allows modeling a PSN containing one victim computer and a user defined number of zombies located at either specified nodes or located at random. Start and end of attack time can be specified separately for each zombie. As in most real life cases, zombies continue to carry on their normal jobs during the attack, i.e., they act also as source, destinations, and routers of legitimate data transfers. However, each zombie also sends a packet to the victim at each time step of the simulation.

Using statistical techniques of design of experiment (DoE) and functional fixed effect models based on ANOVA (Analysis of Variance) we study how the factors routing cost metric and source load, considered at various levels, and their interactions affect response metric network performance indicator “number of packets in transit” NPT.

For normal type of traffic our focus is on the study near phase transition point from free flow to congested states of our PSN model where the transmission efficiency is the highest. The aggregate measure of network performance indicator NPT provides important information about the packet traffic level and if the network is congested or not. We study the effects of DDoS attacks on NPT. Additionally, we use information entropy to detect the presence of a DDoS attack [4,5]. We consider different dynamic routing cost metrics and static routing cost metric. We present selected simulation results and outline our future work.