On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks.

**Contributors: Vivek Datla and Charles E Ellis II**

**Abstract**

The area of cyberspace defense mechanism design is receiving attention from the research community for more than two decades. However, the cyberspace security problem is far from being solved. In this research we explore the applicability of game theoretic approaches to address some of the network security issues. We focus on active attack scenarios where the attacker launches Denial-of- Service (DoS) by flooding one or more links in the network. We model the interaction between the attacker and the defender as a two-player non-zero-sum game in two cases with one single attacking node and multiple attacking nodes, the latter of which arises in Distributed DoS (DDoS) attacks. The defender’s challenge is to determine the best firewall settings to block rogue traffics while allowing legitimate ones. In our analysis, we consider the worst case scenario where the attacker is also interested in finding the most effective packet sending rate or the scale of the botnet. In either case, we build a static and a dynamic game model to find the Nash Equilibrium which represents the best strategy of the system administrator. We validate the effectiveness of our game theoretic defense mechanism via extensive simulation experiments using NS-3.