# ABSTRACT

Sellke, Sarah H. Ph.D., Purdue University, May 2010. Analytical Characterization of Internet Security Attacks. Major Professors: Saurabh Bagchi and Ness B. Shroff.

Internet security attacks have drawn significant attention due to their enormously adverse impact. These attacks includes Malware (Viruses, Worms, Trojan Horse), Denial of Service, Packet Sniffer, and Password Attacks. There is an increasing need to provide adequate defense mechanisms against these attacks. My thesis proposal deals with analytical aspects of the Internet security attacks, as well as practical solutions based on our analysis.

First, We focus on modeling and containment of internet worms. We present a branching process model for the propagation of worms. Our model leads to the development of automatic worm containment strategies, which effectively contain both uniform scanning worms and local preference scanning worms. Incremental deployment of our scheme provides worm containment for local networks when combined with traditional firewalls.

Next, we study the capacity of Bounded Service Timing Channels. We derive an upper bound and two lower bounds on the capacity of such timing channels. We show that when the length of the support interval is small, the uniform BSTC has the smallest capacity among all BSTCs. Based on our analysis, we design and implement a covert timing channel over TCP/IP networks. We are able to quantify the achievable data rate (or leak rate) of such a covert channel. Moreover, by sacrificing data rate, we are able to mimic normal traffic patterns, which makes detecting such communication virtually impossible.