CISC 499: 4th Year Undergraduate Project

Supervisor: Dr. Mohammad Zulkernine, P.Eng.
School of Computing, Queen's University
mzulker at cs.queensu.ca

Project 1: Combining the Pushback Technique and the Distance-Based Defense Framework (Group Members: 2/3)

Distributed Denial of Service (DDoS) attacks are widely regarded as a major threat to the Internet. A flooding-based DDoS attack is a very common way to attack a victim machine by sending a large amount of malicious traffic. Existing network-level congestion control mechanisms are inadequate in preventing service quality from deteriorating because of these attacks. Although a number of techniques have been proposed to defeat DDoS attacks, it is still hard to detect and respond to flooding-based DDoS attacks due to a large number of attacking machines, the use of source-address spoofng, and the similarities between legitimate and attack traffic. This project will combine the pushback technique [1, 3] with the distance-based defense framework [2] for detecting and controlling attack traffic due to flooding-based DDoS attacks. The pushback technique mitigates a DDoS attack by identifying aggregated traffic responsible for congestion, and preferably dropping that traffc at the routers. The defense framework defends against attacks by coordinating between the distance-based DDoS defense systems of the source and victim ends. The combination of these two techniques will help to improve the quality of service of internet service providers for legitimate traffic under DDoS attacks. The combined system should be capable of detecting flooding-based DDoS attacks and controlling attack traffic in order to sustain the quality of service for legitimate traffic.

[1] Y. Ioannidis and S. Bellovin, "Implementing pushback: router-based defense against DDoS attacks," *Proc. of the Network and Distributed System Security Symposium*, February 2002.
[2] Y. You, *A defense framework for flooding-based DDoS attacks,* MSc thesis, Queen's University, Kingston, Canada, August 2007.
[3] Y. Fan, *Defeating denial of service attacks with source router preferential dropping,* MSc thesis, Queen's University, Kingston, Canada, June 2003.

Project Title: A Soft Computing Technique for Automatic Intrusion Detection (Group Members: 2/3)

Different soft-computing based methods have been proposed in recent years for the development of intrusion detection systems. Soft computing is a general term for describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty. The principal constituents of soft computing techniques are Fuzzy Logic (FL), Artificial Neural Networks (ANNs), Probabilistic Reasoning (PR), and Genetic Algorithms (GAs). This project will first compare and contrast the current soft computing tools used for automatic intrusion detection as well as network security in general. Then a soft computing approach will be developed for intrusion detection. The implemented technique will be based on one or more of the above mentioned constituents of soft computing. The technique will be experimented for automatic intrusion detection using some benchmark data sets.