# ABSTRACT

Internet scanning worms are widely regarded to be a major security threat faced by the Internet community today. Active worms spread in an automated fashion flooding the Internet in a very short time. Slammer worm infected more than 90% of vulnerable machines within 10 minutes on January 25th, 2003. Hence it is necessary to monitor and detect the worms as soon as they are introduced to minimize the damage caused by them. This project concentrates on developing an anti-scanning worm detection system that can automatically detect and control the spread of internet scanning worms without any manual intervention. The Intelligent Failure Connection Algorithm (IFCA) developed in this project can detect both stealth and normal worms within a short time. Experiments conducted as part of the evaluation shows that IFCA detects a worm within two scanning cycles of the worm. This is faster than any of the currently available algorithms or mechanisms reported in the literature. The IFCA uses Artificial Immune System (AIS) for the purpose of monitoring and detecting the worms. The Traffic Signature Algorithm (TSA) developed in the project captures the traffic signature of the worm from the infector when it sends the traffic to the victim. The Intelligent DNA Signature Detection Algorithm (IDNASDA) algorithm works by breaking an infection session into different infection phases, each phase containing a number of different traffic such as Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), or User Datagram Protocol (UDP). Finally it converts the traffic signature to DNA signature. The tests carried out show that the IDNASD could detect DNA signature for MSBlaster worm.