SIMULATION OF CYBER ATTACKS ON COMPUTER NETWORKS.

Jason Kistner, *Michael Kuhl*, Department of Industrial and Systems Engineering, jpk7781@rit.edu, mekeie@rit.edu*

As the use of computer networks grows, cyber security is becoming increasingly important. To enable systems administrators better protect their networks, cyber security tools such as intrusion detection systems are employed to warn of suspicious network activity. In some situations, systems administrators have to deal with millions of such warnings each day. Consequently, situational awareness and threat assessment tools that employ information fusion techniques are being developed to aid in fighting cyber attacks. As these systems are being developed, data is needed to test and evaluate their performance. As an alternative to a physical computer network, a simulation modeling methodology is presented. The simulation method allows the user to construct a virtual computer network that produces cyber attack warnings representative of those produced by intrusion detection systems for both malicious and nonmalicious network activity. Consequently, this flexible simulation modeling framework will enable the efficient generation of data to test and evaluate situational awareness and treat assessment tools for cyber security.