Proposal to Bucknell University's Undergraduate Research Program
Summer 2004

A Simulation Study of Denial of Service Attacks on Wireless Ad-hoc Networks

Samuel C. Nelson
Class of 2006
snelson@bucknell.edu

Luiz Felipe Perrone (Faculty Mentor)
perrone@bucknell.edu
Assistant Professor
Department of Computer Science

Proposal approved (funding from Accenture Undergraduate Research Fund Summer 2004).

Part A: Project description

Imagine the following scenario: A chemical plume quickly spreads over a metropolitan area as the result of an accident or a terrorist attack. Emergency response helicopters fly over the area dropping thousands of tiny battery-powered sensors, called *smart dust*. They are about a cubic millimeter in size and have the ability to form a massive *wireless ad-hoc network*; that is, a self-configurable web of sensors that collect and disseminate information about their environment. Each of these sensors collects data pertaining to its surroundings and, using the wireless network, forwards their measurements to collection points outside of the chemical plume. The response team on the ground now has, in real-time, information about the gas density at different sections of the city and can coordinate the movement of rescue personnel with minimal danger to their lives. Not only are such sensors helpful in situations of this nature, but they are also applicable in response to natural catastrophes, in warfare, in law enforcement, in scientific exploration, and in surveillance.

The backbone of this system is the wireless ad-hoc network that the sensors create without human intervention. Before a system like this can effectively be used, there must be measures of scientific and thorough testing to qualitatively assess the performance and effectiveness of each of its components. With potentially hundreds of thousands of network nodes and many different operation scenarios, it is impossible to test this system without the aid of computer simulations. The Simulator for Wireless Ad-hoc Networks (SWAN) is a tool created with this goal in mind. SWAN was started at the Institute for Security Technology Studies (ISTS), at Dartmouth College. It is a continuing project involving Professor Perrone at Bucknell University, and researchers at Dartmouth College and the University of Illinois Urbana-Champaign.

The focus of our research will be to use SWAN to evaluate and quantify how wireless ad-hoc networks can be affected by security attacks. The nature of the communication medium in these networks (radio waves) leaves them wide open to malicious adversaries, so before we can apply this technology in mission-critical scenarios, we need to understand its vulnerabilities. Without this understanding, in the event of an attack, time, money, and most importantly, lives could be lost.

Methods:
We will develop different models of attacks on wireless networks and use simulation to evaluate how they impact the operation of the network. Primarily, we will be dealing with attacks known as *denial of service* attacks. The main objective in these attacks is to slow down or to completely halt the flow of information in the network, effectively rendering it useless. When time is of the essence, this is a factor that must be acknowledged and dealt with. Therefore, our specific objective over the course of eight weeks is to use SWAN to understand how well the network holds up against these types of attacks. We will generate simulation data for a wide number of different scenarios and parameters in the attack models, evaluating metrics such as end-to-end delay (the time a packet of information takes to go from source to destination), packet delivery ratio (the percentage of packets sent that is actually delivered), and routing control traffic (internal information used to reconstruct or maintain the damaged network).

The specific types of denial of service attacks that we will be studying are attacks that do not require much technical expertise to perform, what makes them most dangerous. An example of this type of attack is disabling and re-enabling a small number of nodes, what could cause much control traffic and make the network unreliable. Prof. Perrone's has already designed a few of these attack models; our goal this summer is to create new models and use the simulator to experiment with them. This will involve programming these models, constructing and running experiments, and analyzing the results.

Outcomes:
The data that we will obtain from running simulations of these attack models will allow us to put together, by the end of the summer, what we anticipate to be a good conference paper. We will make this data available to the research community via the World Wide Web together with careful and thorough descriptions of our experiments, so that others may attempt to reproduce them. Our goals are feasible with the resources we already have at Bucknell as described in the next section, Research Environment. It is important to point out that the work we propose builds up on and complements preliminary, unpublished results from Prof. Perrone's work.

Part B: Research Environment

SWAN is a C++ open source computer simulation program three years in the making, which is readily available for use. SWAN will be the major resource we will use in this research. The simulations will be run on a state-of-the-art cluster computer with sixteen processors and over thirty gigabytes of memory, allowing for up to sixteen simulations to run at the same time. This will vastly accelerate the computation time in our explorations in the space of possible scenarios and parameter settings, allowing us to produce statistically solid results. We will also utilize Bucknell's internal network, computer labs, and personal laptops. This research will take place on Bucknell's campus, with a high level of interaction between Professor Perrone and I.

Communication between Professor Perrone and I will occur according to two mechanisms, one formal and another informal. Namely, we will schedule three one-hour long meetings per week and work with an open-door policy for interaction as often as necessary. Professor Perrone has dedicated this summer exclusively to doing research with SWAN at Bucknell, so we will be working in close proximity to discuss, plan, write, test, and analyze different attacks that can be brought onto a wireless ad-hoc network.

Wireless ad-hoc networks are a new and rapidly growing field that will have a strong effect on the world. We feel that this is a worthwhile, necessary research project that will have a positive impact on this developing technology. As evidence for the importance and relevance of this project, the development of SWAN and the computing power needed to perform the simulations are funded by a Dartmouth College - United States Department of Justice grant under Bucknell fund 228233, grant number GFE023.