Proposal to Bucknell University's Undergraduate Research Program

Automated Optimization Study of Attack Models for Wireless Ad Hoc Networks

Summer 2008

Bryan C. Ward
bryan.ward@bucknell.edu

Class of 2011
Box C3733
(703) 615-5692
BU ID: 10750481

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

Part A: Project description

In this age of information, we rely on wireless networks to get us the information we demand, whether it be streaming video from the internet, or the audio of a cell phone conversation. One particular emerging wireless technology known as *ad-hoc* networking, has the potential to power many new applications, and spawn entirely new technologies.

Ad-hoc wireless networks create themselves without human intervention and don't rely on any existing infrastructure. The devices (or *nodes*) execute computer programs (or *protocols*) to discover one another and to establish information routes from any source to any destination. These protocols dynamically adjust the network to account for the mobility of nodes and/or to changes in the conditions for the communication between nodes.

An example application of this technology could be on the battlefield where wounded soldiers have historically relied upon their buddies or their cries for help to get medical assistance. If each soldier carried a sensor which monitored and transmitted his vital signs over a wireless ad-hoc network of similar nodes wounded soldiers could get medical attention without needing to cry for help. Not only could medics help men who might have otherwise been left for dead, but they could have some knowledge of the soldier's condition before they even arrived on the scene. Furthermore, strategists could have real time data on their army to know when to pull out and when to surge forth. Sensors such as these could provide invaluable information not only on the battlefield, but also in scientific applications, law enforcement, disaster relief and countless other applications.

The wireless ad-hoc network connecting the sensors in this example is the fundamental technology that allows applications such as these to be possible. Before any emerging technology can be fully implemented though, it must undergo thorough testing to evaluate performance and reliability in a number of different stress conditions. This kind of exhaustive testing is best done with the aid of computer simulations. Professor Perrone's project, the Simulator for Wireless Ad-hoc Networks (SWAN), is the tool that we will use to conduct this research.

Previous publications have used simulation to show how simple physical attacks have the potential to cause substantial damage to the performance of the network. (Perrone and Nelson 2006, Perrone 2007) These attacks are based on the idea of an *on-off process* in which the attacker alternates periods of activity and rest. The attacker performs some evil action for a period of time and then stops, leaving the network alone for another period of time. The continuous repetition of this cycle is damaging to network performance because each transition of the attack cycles causes the network protocols to spend time in computation and in communication to reevaluate how traffic should be routed around compromised nodes or communication channels. The papers cited above define a model with several parameters, such as attack length, that can be set to reflect a variety of scenarios.

Prof. Perrone's investigations so far have considered only fixed-length (deterministic) on-off cycles. In this research project we will be extending the experiments with attack models to also

include variable length (stochastic) on-off cycles. Our ultimate goal is to discover what combination of parameter settings in the attack models produce maximal damage on the performance of the network. We propose to integrate a search algorithm with the simulations to do an automated exploration of the space of parameter combinations and to identify the worst-case scenarios of different attack models.

Methods:

To better analyze the parameter space of the possible attack scenarios, we will be using a search algorithm to help find more damaging scenarios for the network. Simulations are very computationally intensive, so the search algorithm will allow us to more quickly find the set of parameters that induce the most damage on the network, instead of spending time investigating relatively harmless scenarios.

The basic premise of the search algorithm is that it uses past simulation results to select new scenarios to test. In order to better select new simulations to run, the program must analyze previous results to learn how sensitive the simulation is to different sets of parameters. It accomplishes this through different performance metrics, which are quantitative measurements of the damage to the network. In our research we will experiment with different performance metrics to find which run more efficiently, and which produce more damaging results.

Also, the results from the simulations will be stored in a database for easy access at a later date. This will further enhance performance because previous results from past experiments can be read in from the database instead of taking the time to re-compute the simulation. This will also enable us to access results more easily upon completion of the experiments.

Outcomes:

The project builds upon the work that Prof. Perrone and I have been doing in two independent studies, this semester and last. We hope that the work we will do this summer will provide results that we can publish in a conference paper. We expect these goals to be realistic given the work we have already done and the technology we have available as described in the Research Environment section.

Milestones:

In order to meet our goal of producing research worthy of sharing with the scientific community through a published article, we have laid out an approximate schedule of how the time over the summer will be utilized. First I will be doing research on my own to try and find effective and efficient search algorithms for this project. I will then implement those algorithms and incorporate them into the SWAN. Next I will put the processors to work running simulations while I work on coding and evaluating different performance metrics. I will then spend the rest of my summer further analyzing data and writing what I paper to be submitted to a conference.

Weeks 1-2: Investigate literature on search algorithms for the study of parameter sensitivity.

Weeks 3-4: Implement search algorithms and incorporate them into SWAN's framework.

Weeks 5-6: Execute simulations and analyze the performance of the attacks based on different metrics that can quantify the effect of the attacks.

Week 7-8: Draft a paper on our results for a conference submission.

Part B: Research Environment

The most important resource for our project is the simulator itself, SWAN, which is an open source C++ program readily available for our use. The simulations will be run on a cluster computer with 16 processors and 32 gigabytes of memory. This computer will allow us to run many simulations simultaneously and help us reach our goals in a reasonable amount of time. Furthermore, with this much processing power readily available, we can run more replications of simulations to get better statistical results. In addition to this cluster, we will be using Bucknell's network, workstations, and personal laptops for development and research.

Communication between Prof. Perrone and I will be crucial to the success of this project. For this reason, we have planned a minimum of three one-hour meetings each week. We will also work on an "open door policy" in which I can consult with Prof. Perrone whenever I have any questions or have important results to share. Prof. Perrone will be working with SWAN on a related research project over the summer as well, which means that we will both be immersed in similar work and will have a natural environment for our collaboration.

Wireless ad-hoc networks can enhance and even save the lives of many throughout the world through applications that may or may not have yet been realized. This research promotes the emerging technology by demonstrating possible weaknesses that need to be addressed. We hope that our results prove to be valuable to the research community, and that their implications are taken into consideration by engineers in real world, mission-critical applications.

References

Perrone, L. Felipe. "Could a Caveman Do It? The Surprising Potential of Simple Attacks." *IEEE Security and Privacy*. Vol. 5, Issue 6, pp.74-77. November/December 2007.

Perrone, L. Felipe, and Samuel C. Nelson. "A Study of On-Off Attack Models for Wireless Ad Hoc Networks." In *Proceedings of the First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks* (OpComm 2006). August 2006.