Statement of Research Interests

Luiz Felipe Perrone
Institute for Security Technology Studies, Dartmouth College
perrone@ists.dartmouth.edu

The pervasiveness of computer technology in our society has been in steady increase in the last decade and current advances will lead to a further acceleration of this trend. Wireless networking is the enabling technology behind this new revolution that will lead to the widespread deployment of communicating computing platforms. This push for ubiquity, which will lead to very large and complex wireless networks, has resulted in many interesting research challenges in network architecture and protocol design which are permeated by a need for strong security and privacy.

My primary research interests are the development of computer simulation technology and its applications in the analysis of computer networks. In my recent work, I have addressed the use of computer simulation for the analyses of wireless networks architecture, protocol design, scalability and security. The pursuit of these interests reflects my intention to participate in the development of large-scale wireless networks that are suitable for the applications of today and of the future.

Development of Modeling and Simulation Techniques
In over 30 years of research, attempts to produce a general purpose high-performance simulator through parallel and distributed computing have failed to produce a *silver bullet*. The fastest and most efficient simulators are still those that exploit the particular characteristics of a problem class. I am interested in researching new simulation technologies that can be applied to models of communication systems, especially wireless networks. In more concrete terms, my interest lies in the development of high-performance models and simulation algorithms that yield fast execution.

My Ph.D. research was focused on studying the characteristics of cellular wireless phone system models and on developing acceleration techniques for that specific problem. This research resulted in a new simulation algorithm called *interval jumping* that can substantially speed up the simulation of hybrid models (time-stepped/discrete-event) for which state updates are based on fixed-point computations. Interval jumping works by identifying large numbers of consecutive time-steps in which the state of the system would change little, and allows the simulation to skip over the end of that sequence of steps. My work on this problem involved both the theoretical aspects of the development and the performance analysis of interval jumping, and its implementation in a simulator for wireless cellular networks.

Research on high-performance simulation technology is particularly relevant today, when the developments in computer networking require special attention to scalability, reliability and security. At the Institute for Security Technology Studies (ISTS), my current research has been focused on the development of algorithms and software for high-performance simulation with applications to security, counter-cyber-terrorism and emergency-response. My activities in this area have produced a simulation testbed for the design and the evaluation of security features of large-scale wireless networks dubbed the Dartmouth Simulator for Wireless Ad-hoc Networks (SWAN).

To achieve its goals of high-performance and scalability, SWAN builds upon the strengths of the Dartmouth Scalable Simulation Framework (DaSSF) allowing for parallel or distributed execution. SWAN offers various models of protocols used in wireless networks (802.11b PHY and MAC, ARP, IP, AODV and DSR) and also provides models of applications that carry out denial-of-service attacks on lower protocol layers. The framework integrates models of network protocols with models of radio propagation, terrain profile, host mobility and environmental processes that provide

stimulus for sensors on mobile nodes. A first beta-version of SWAN is currently in preparation for public release.

The significance of a simulator rests on whether its models have been validated against real systems. Those who have built and operated wireless networks which have been studied in prominent simulators have remarked that the observed behavior of the real system has been substantially different from what was predicted. Much of these differences can be attributed to the inadequacies of the radio propagation models used in the simulators. There exists today a pressing need for the development of radio propagation models which reflect more accurately the behavior of specific technologies such as 802.11, for instance. Experience has shown that propagation models such as free-space, two-ray ground reflection, and even the Irregular Terrain Model (ITM) fail to describe accurately what happens in reality. This observation casts serious doubts on the faithfulness and the relevance of simulations of wireless protocols using such models, since it has been shown that physical layer effects strong influence higher layer protocol metrics. The continued development of SWAN or enhancements to other simulation platforms should carefully address this problem.

Further advances in high-performance simulation for wireless networks should seek to understand particular characteristics of protocols so that their essence can be captured by simple mathematical models which result in fast computations. The development of one such model for a medium access control protocol resulted in the article *Towards High Performance Modeling of the 802.11 Wireless Protocol*, which I presented at the Winter Simulation Conference (WSC) 2001. This work captures the behavior of the 802.11b protocol in a stochastic model that estimates packet delays and packet losses as a function of the number of neighbors within the radio range of a network node. I intend to carry out further explorations in this line of research, which can substantially accelerate the simulation of network protocols when one is willing to sacrifice a small measure of accuracy in favor of faster results.

Simulation in the Development of Emergent Security Technology

Large-scale self-configurable sensor networks are an important emergent technology which can benefit much from the use of computer simulation at development and analysis stages. The applications of this technology to security and emergency-response are numerous, emphasizing the need for its maturity. My work in this area has been to modify the SWAN framework to produce a platform for the simulation of smart-dust devices running TinyOS. Smart-dust systems will consist of a *very* large number of communicating devices capable of sensing and perhaps even actuating on the environment. The simulation of these systems, which is particularly difficult given the scale of the problem, is relevant to the development of new distributed algorithms and software. The prototype of simulator I developed can directly execute the same source-code written for TinyOS devices using more accurate models for radio propagation than its predecessors. Future work will need to address issues on environment models and parallelization, in addition to catching up with the latest TinyOS developments in application description language.

While sensor networks are themselves tools that can aid the enforcement and the evaluation of security, being a sub-class of general purpose wireless ad-hoc networks, their protocols suffer from many of the same vulnerabilities, which are not few or unimportant. Wireless ad-hoc networks have volatile topologies, in which nodes are constrained by their battery power, and are subject to limited physical security. In addition, the implicit mutual trust between network nodes would leave their protocols open to malicious interventions by adversaries. The widespread use of these technologies hinges on further advances to mitigate or eliminate these vulnerabilities.

In order to evaluate the effects of security exposures in protocols for wireless ad-hoc networks, I am currently using simulation to investigate how different attacks affect operating metrics such as latency, packet delivery ratio and packet delay, among others. At this stage, the focus

is on simple attacks which can be carried out by enemies with minimal technological sophistication seeking maximal disruption to network operation. This scope should be broadened to include studies that quantify the effects of attacks on different layers of the protocol stack described by Wood and Stankovic's recent article "Denial of Service in Sensor Networks", in IEEE Computer Oct. 2002.

From Simulation to Practice in Wireless Networks

At present, several different proposals have been made to secure wireless networks. Some of these attempts use cryptographic techniques that rely on infrastructures for key distribution similar to PKI. The use of these infrastructures applies directly to guaranteeing properties like confidentiality, non-repudiation, and authenticity to data traffic. This "protection" to traffic can be used to secure routing protocol messages in ad hoc wireless networks. What is particularly exciting about research in these infrastructures is that in order to make them scalable, one will have to resort to hierarchical architectures to establish trust chains. It is likely that these hierarchies can also be used to create novel scalable routing algorithms. Clearly, simulation will play a part in the development of authentication infrastructures, but I'm also interested in investigating how to efficiently unify authentication hierarchies with scalable routing.

My experience with simulation has required that I develop an intimate knowledge of the systems under study. In the coming years, I see myself making a transition from research in simulation to more directly working on the problems to which I have been applying simulation. The continued need for progress in wireless network protocols presents a problem-rich research area in which my skill set will allow me to contribute. In the future, I envision working in topics such as medium access control (MAC) algorithms for new radio technologies, such as UWB, and synchronization.

Research Philosophy

My formal education has taken me around different fields. I started out with an interest in health sciences, which I pursued in a few classes in high-school. In college, I went through an engineering program that led me to studies concentrated in control systems, signal processing, communication systems and computer technology. Finally, in graduate school, I arrived at computer science, where I've been interested in systems, networks, simulation and security. This amalgamation of knowledge from diverse areas has allowed insights in my research that would have been hard to achieve otherwise. Even my strong interest for foreign languages and cultures has played an important part in my work by allowing me on occasion to get information directly at the source.

I believe that breadth of knowledge can be one of the greatest blessings for someone engaged in cutting-edge research. There's evidence that interdisciplinary knowledge can facilitate new developments in a specific area through the application of insights obtained from different fields. I expect to establish scholarly relationships with researchers in other areas, as well as in my own, in the attempt to pursue solutions to problems I will be working on and also to identify topics for future investigations.

In what regards the participation of undergraduate and graduate students in my research activities, I believe that one cannot get students involved too early. I've been successful in bringing undergraduates from my classroom into my research projects. These students have been successful both in learning new skills and in making contributions of their own. I view the relationship with my students as that of trade master and apprentice and make every effort to show them, through practice, how science is done. I look forward to establishing a strong research program and to getting students involved in my activities.