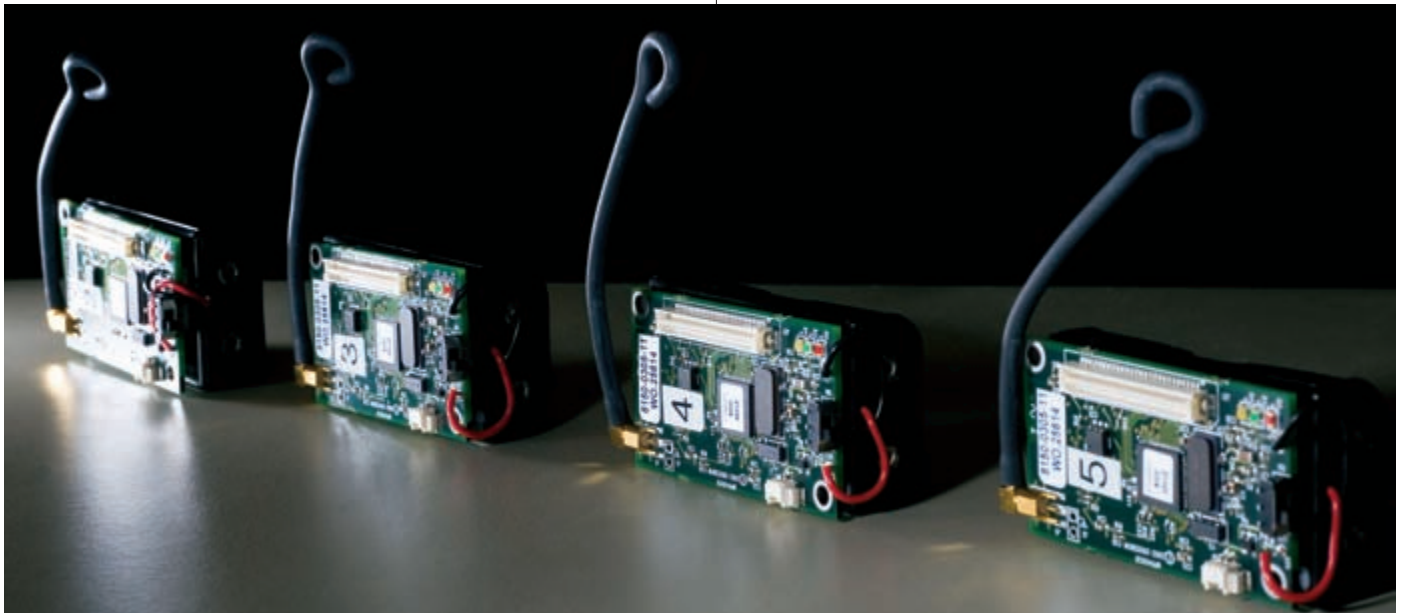


# NETWORKING

## FACULTY

Luiz DaSilva  
Mohamed Eltoweissy  
Thomas Hou  
Yao Liang  
Allen MacKenzie  
Scott Midkiff  
Amitabh Mishra  
Leyla Nazhandali

Jung-Min Park  
Binoy Ravindran  
Yaling Yang



Motes—test platforms for low-power, limited resource systems—in the Laboratory for Advanced Networking (LAN) are used to test network vulnerabilities.

## Wireless sensor nets vulnerable to denial-of-sleep

According to research in ECE's Laboratory for Advanced Networking (LAN), the medium access control (MAC) protocols of state-of-the-art wireless sensor networks (WSN) are susceptible to denial-of-sleep attacks that can reduce network lifetime from years to days.

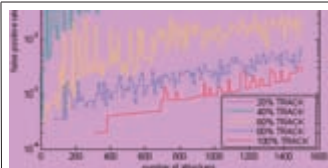
"Like other networks, sensor networks are vulnerable to malicious attacks," said Ph.D. candidate Lt. Col. David Raymond (U.S. Army), who conducted the study with his advisor, Scott Midkiff. "However, their limited resources make these devices particularly vulnerable to denial-of-sleep attacks."

The sensor platforms typically use 8-bit processors, less than 8 kb of RAM, and 100 kb of program memory. "Not only are they more sensitive, but because of their hardware simplicity, defense mechanisms designed for traditional networks are not feasible," he said. The team identified features of WSN MAC protocols that increase vulnerability to denial-of-sleep attacks, then ana-

lyzed the impact of attacks tailored to these vulnerabilities.

"With full protocol knowledge and an ability to penetrate link-layer encryption, all WSN MAC protocols examined are susceptible to a full domination attack, which reduces network lifetime to the minimum possible by maximizing the power consumption of the nodes' radio subsystem," he said. "Even without the ability to penetrate encryption, subtle attacks can be launched that reduce network lifetime by orders of magnitude."

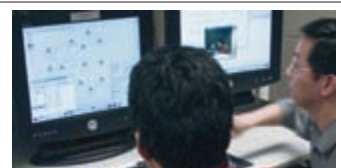
The team is working to design and implement mechanisms to prevent or mitigate the impact of these attacks. As WSNs grow less expensive, the potential for widespread use in applications from health monitoring to military sensing continues to rise, he said.



**Advanced Research in Information Assurance and Security**  
Director: Jung-Min Park  
[www.arias.ece.vt.edu](http://www.arias.ece.vt.edu)



**Complex Network and System Research Group**  
Director: Thomas Hou  
[www.ece.vt.edu/thou/CNSR](http://www.ece.vt.edu/thou/CNSR)



**Laboratory for Advanced Networking**  
Director: Luiz A. DaSilva  
[www.irean.vt.edu/lan](http://www.irean.vt.edu/lan)

# 1st-ever ad hoc networking contest set

In November, Virginia Tech is launching a first-of-its kind competition for students and researchers in mobile ad hoc networking. Called the MANIAC Challenge (Mobile Ad Hoc Networking Interoperability and Cooperation), the competition will be held in conjunction with IEEE's Globecom 2007, November 25-26 in Washington, D.C.

Competing teams will come together to form a large (estimated 30-50 node) ad hoc network. The organizers will create and send traffic to each team. Teams will be judged based on how much of the traffic destined to them makes it through the network, how

little energy they consume in forwarding traffic, and a subjective evaluation of the quality of their solution's design. To get their traffic across the network, each team must rely on other teams' willingness to forward traffic for them, according to Luiz DaSilva, who with Allen MacKenzie is organizing the project with funding from the NSF.

The two-in-one effort is aimed at meeting educational and research goals of improving network throughput, deepening understanding of overall network behavior, and motivating students in the field. For more information, see [www.maniacchallenge.org](http://www.maniacchallenge.org).

## Battery-sensing intrusion system for mobile computers

Using a dynamic threshold calculation algorithm, a CpE team has developed an attack-detection system for mobile computers, which alerts users when battery power changes are detected on handheld wireless devices, such as PDAs and smart phones.

Hosts enabled with the battery-sensing intrusion protection systems (B-SIPS) are employed as sensors in a wireless network and form the basis of the intrusion-detection system (IDS). "When a small mobile device is kept in a high activity state for extended periods of time, the battery resources are depleted faster than normal, decreasing its charge life," explained Timothy Buennemeyer, a Ph.D. candidate on the project. "Our system not only alerts the user, but

it also provides security administrators with a nontraditional detection capability that is scalable and complementary in a network environment with existing commercial and open system IDSs." Irregular and attack activity is detected and reported to the intrusion detection engine for correlation with existing signatures and further investigation.

An analytic model was developed to examine the smart battery characteristics to support the theoretical intrusion-detection limits and capabilities of

B-SIPS. The dynamic polling rate algorithm allowed the smart battery to gauge the network's illicit attack density and adjust its polling rate to more efficiently detect attacks and conserve battery charge.

The team is currently developing a device-profiling and attack matching capability, and a usability study is being conducted. Buennemeyer is working on the project with fellow graduate student Theresa Nelson, Professor Joe Tront, and Randy Marchany, director of Virginia Tech's IT Security Laboratory.



## AIRBORNE NETWORKS Creating a mesh in the sky

Researchers in electrical and computer engineering are designing routing protocols for airborne networks, a technology that provides reliable communication between aircraft, unmanned aerial vehicles (UAVs), and other airborne assets.

Airborne networks arise naturally in military scenarios, search-and-rescue operations, and even potentially in civil aviation. Ensuring that airborne platforms can communicate effectively without necessarily relying on ground relays is a major objective in this area.

Luiz DaSilva and graduate student Bo Fu are working with a team from SCA Technica, Inc. as part of an Air Force Research Lab SBIR project. The team is developing mechanisms that will overcome routing challenges in networks of high-speed nodes through the use of location awareness and disruption tolerant network techniques. Inspired by the idea of mesh networks, wireless networks of ground nodes that sometimes cover an entire city. They are proposing to opportunistically create a mesh in the sky, with underlying robust mechanisms that address the particular challenges of airborne platforms.

TIM BUENNEMEYER

