CENTER FOR MOBILE COMPUTING
http://CMC.cs.dartmouth.edu
DARTMOUTH COLLEGE
DECEMBER 2002 NUMBER 6

CMC

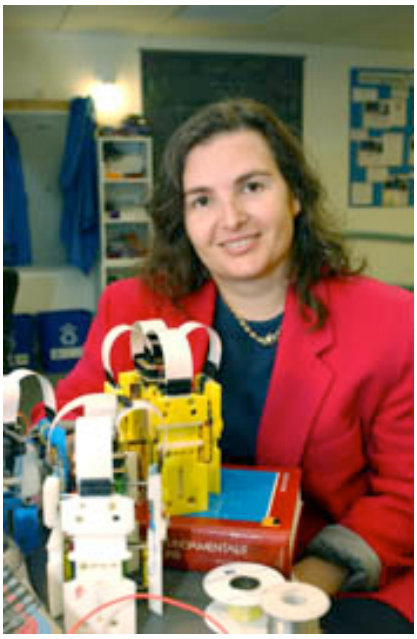
In this issue

Active Communication

In this issue we focus on the results of our five-year DoD-funded ActComm project. In this multi-university research initiative we set out to develop technologies to maximize the usability of complex, global computer and communications networks, focusing especially on wireless networks for modern command-and-control applications. The project was based on the concept of an active communications system: active software, active information, active hybrid networks, and active resource allocation. Most of the research effort focused on mobile agents and wireless networking.

Bob Gray also reports on our involvement in the Coalition Agents Experiment (CoAX). Our D'Agents mobile-agents software and Grid-based Mobile-Agents interoperability framework play a key role in this military simulation of a coalition forces operation.

Daniela Rus Wins MacArthur Fellowship



Prof. Daniela Rus was named a John D. and Catherine T. MacArthur Fellow in September. The MacArthur Fellows Program awards five-year unrestricted fellowships to individuals across all ages and fields who show exceptional merit and promise of continued and enhanced creative work.

Rus is the founder and director of the Dartmouth Robotics Laboratory. Her research interests include robotics, mobile computing, and information capture and access. She is known for her work on self-reconfiguring robots, shape-shifting machines have the ability to adapt to different environments by altering their internal geometric structure. They do this on their own, without remote control, for locomotion, manipulation, or sensing purposes. For example, this new breed of robot could first self-organize into a snake shape to squeeze through a narrow tunnel and then reorganize as a multi-legged walker to traverse rough terrain. (*Photo by Joseph Mehling*)

NEWS

New CMC Partner

NTT DoCoMo is best known for its introduction of the iMode mobile device that is used by millions of Japanese. They recently opened a research lab in Silicon Valley. We are proud to welcome them as a new CMC partner, as we begin to collaborate on a further exploration of usage patterns in the Dartmouth campus-wide wireless network.

Wired Magazine profiles the Dartmouth wireless network

"Founded in 1769, Dartmouth College is truly old school. But its precocious use of technology -- including a vast wireless network -- makes it a prototype for tomorrow's unwired society." In its October 2002 issue, Wired magazine included a fun feature article discussing our campus-wide wireless network, and the impact it is already having here on campus. The article mentions the CMC research highlighted in the previous CMC newsletter, which details patterns of usage on the wireless network. The wireless network is indeed a vast experimental test-bed for the CMC and its partners, literally a prototype for the future. See www.wired.com.

Discovery Channel profiles the Dartmouth wireless network

The Discovery Channel television network in Canada has a technology column called "Gadget Grrrls" in its "Daily Planet" news magazine. In November they broadcast a three-part series, filmed on campus, in which they explore the nature of the campus wireless network and its impact. These stories also interview CMC professor David Kotz and mention the CMC research investigating usage patterns in the wireless network. See www.exn.ca.

CMC begins new on-campus seminar series

The CMC is sponsoring a biweekly seminar to gather researchers and application developers, students and staff and faculty, from all across campus. There are so many cool projects underway; by meeting occasionally we can encourage the exchange of ideas, discuss technology trends, and learn about each other's projects.

CMC rolls out a new web site

http://cmc.cs.dartmouth.edu

Check out our new web site! It also integrates the web sites of our two major projects, both nearing completion: ActCOMM (featured in this issue) and D'Agents (our mobile-agent platform). The attractive new site gathers all related projects in one place and in one format.

Wireless trace data now available

The CMC is making available all of the data collected as part of Professor Kotz's characterization of the campus-wide wireless network. Once the data is suitably anonymized, it will be freely available to academic researchers and to partners of the CMC. In November we released the syslog (nearly continuous since April 2001), which identifies each card as it associates and disassociates with the network (over 5,000 network cards are represented!) Soon, we hope to release the SNMP data (11-15 weeks of Fall 2001, and 11 weeks of Spring 2002). This data includes, for every access point for every five minutes, the MAC addresses of recently associated client stations, and the current value of two counters, one for inbound bytes and one for outbound bytes. Later, we will release the tcpdump data (11-15 weeks of Fall 2001, and 11 weeks of Spring 2002). In each of four locations (five, in Spring 2002) we attached a computer and the building's APs to a common hub, and attached the hub's uplink to a switch port on the campus network. With this “sniffer” in promiscuous mode, we used tcpdump to record the header of every packet passing by.

Two researchers join CMC

Ted Cooley and Susan McGrath have joined the other four faculty in the CMC. Ted is an Assistant Professor of Engineering and the Director of Information Technology at the Thayer School of Engineering. Sue is a Technical Program Coordinator at Dartmouth's Institute for Security Technology Studies, and a Lecturer in the Thayer School of Engineering.

Other Projects

There are several fascinating projects underway on campus. Although some of these projects are not explicitly connected to the CMC, we summarize them here because they are a great example of the environment for innovation in computing at Dartmouth.

The Tacos Wireless Device Tracking System

Tacos is a web site allowing users to register any wireless device by listing its MAC address, after authenticating through our campus authentication database. If a device is ever lost or stolen, they use the website to report it as missing. If the device is ever activated on the Dartmouth Campus, they receive an immediate email indicating the device location. The location is derived from the associated AP name. For more information see http://tacos.dartmouth.edu/

Greenwave Wireless

Two students are installing private APs in off-campus residences, and configuring them as repeaters. The goal is to expand the reach of the campus wireless network into private residences nearby. For more Information see www.greenwavewireless.com/

Sensor networks

Ron Peterson and Daniela Rus, and their students, are developing distributed algorithms for wireless sensor networks that respond by directing a target (robot or human) through a region. The sensor
network models the event levels sensed across a geographical area, adapts to changes, and guides a moving object incrementally across the network. We are also building a device we call a Flashlight for interacting with the sensor field. This interaction includes collecting navigation information from the sensors in the local neighborhood, activating and deactivating specified areas of the sensor network, and detecting events in the sensor network. Another current topic of study is the interaction of flying robots with a wireless sensor network.

New Research Papers

Arne Grimstrup, Robert Gray, David Kotz, Maggie Breedy. Marco Carvalho, Thomas Cowin, Daria Chacón, Joyce Barton, Chris Garrett and Martin Hofmann. **Toward Dynamic Interoperability of Mobile Agent Systems.** In Proceedings of the Sixth IEEE International Conference on Mobile Agents, pages 106-120, October, 2002.

David Kotz and Kobby Essien. **Analysis of a Campus-wide Wireless Network.** In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, pages 107-118, September, 2002. Revised and corrected as Dartmouth CS Technical Report TR2002-432.

David Kotz, Robert Gray and Daniela Rus. **Future Directions for Mobile-Agent Research.** IEEE Distributed Systems Online, 3(8), August, 2002. Based on a conversation with Jeff Bradshaw, Colin Harrison, Guenter Karjoth, Amy Murphy, Gian Pietro Picco, M. Ranganathan, Niranjan Suri, and Christian Tschudin.

Qun Li, Javed Aslam and Daniela Rus. **Distributed Energy-Conserving Routing Protocols for Sensor Network.** In Proceedings of the 37th Hawaii International Conference on System Science, January, 2003.

Qun Li and Daniela Rus. **Communication in Disconnected Ad-hoc Networks Using Message Relay.** Journal of Parallel and Distributed Computing, 2003. To appear.

Qun Li and Daniela Rus. **Message Relay in Disconnected Ad-hoc Networks.** In IEEE MASCOTS Workshop on Mobility and Wireless Access, October, 2002.

Qun Li, Michael De Rosa and Daniela Rus. **Distributed Algorithms for Guiding Navigation across a Sensor Net.** Technical Report TR2002-435, Dept. of Computer Science, Dartmouth College, October, 2002.

Javed Aslam, Qun Li and Daniela Rus. **Three Power-aware Routing Algorithms for Sensor Networks.** Wireless Communications and Mobile Computing, 2003. To appear.

These papers are available on the web at
http://www.CMC.cs.dartmouth.edu/papers/

Soldiers, Agents and Wireless Networks: The ActComm Project

http://actcomm.thayer.dartmouth.edu/

Bob Gray

In current military operations, soldiers typically have voice communication only, which makes it difficult to access needed information and coordinate mission activities. Ideally each soldier would have a portable computing device through which they could query military databases, access maps of the surrounding terrain, view the positions of their fellow soldiers, and send complex observations to the mission planners at headquarters. Providing such computing capabilities to soldiers in the field involves many technical challenges at both the hardware and software levels.

The Active Communications (ActComm) project, which is a DoD Multi-University Research Initiative (MURI), focuses on two pieces of the software level: (1) ad-hoc routing systems that route traffic from one soldier to another (and back to headquarters), and (2) mobile-code systems that allow the soldiers to efficiently access databases in the main military network. The ActComm project began in 1998, and aside from some final experimental work, is finishing now in December 2002. The project participants are Dartmouth College, Harvard University, Rensselaer Polytechnic Institute, the University of Illinois, Lockheed Martin, and ALPHATECH.

The underlying assumption in the ActComm research is that all soldiers have short-range, high-bandwidth wireless hardware to communicate with each other, while a few soldiers also have long-range, low-bandwidth hardware to serve as gateways to the main network. Due to the short range of the soldier-to-soldier hardware, data going from one soldier to another might need to go through several intermediate soldiers. Moreover, soldiers continually move relative to each other, so available routes change from one moment to the next. In addition, the soldiers might move out of range of each other, requiring the routing system to queue messages until the network disconnection goes away. Together, the ActComm technologies allow applications to work effectively on such ad-hoc wireless networks, one of the most challenging network environments in existence, and one that arises not only in military operations, but also in civilian search-and-rescue, disaster relief, and refugee management. In this article, we first describe the ActComm test scenario and hardware testbed, and then some of the routing and mobile-code research.

Scenario and Testbed

The current test scenario for the ActComm project is shown in *Figure 1*. An intelligence team at headquarters has intercepted one or more phone calls and determined that a terrorist faction is likely to meet in a particular building. [We adopted this scenario before the events of September 11, 2001. Those events, and the nature of the resulting United States military missions, make the scenario even more relevant, however.] Headquarters dispatches a team of soldiers, who take up observation posts (probably hidden) around the building. If the terrorists come to the building, the soldiers will secure the building and arrest the terrorists.

This scenario has been run several times on the Dartmouth campus with students playing the role of soldiers. Since the ActComm project does not consider hardware issues, each soldier has a standard laptop computer. Each laptop has a GPS unit to determine the soldier's position and a wireless card to communicate with other soldiers.

Each gateway soldier simply has a second wireless card set to a different transmission frequency. We use fifty laptops for experimental evaluation of individual components, but we typically have only twenty students for outside experiments.

Each soldier has a map of the urban area where the building is located, and the current positions of other soldiers are displayed on the map. The soldiers enter descriptions of the people that they observe entering the building, and each observation is sent to headquarters so that mission planners can (attempt to) determine whether the person is one of the suspects. As the planners make their determination, they might send a series of pictures to the soldiers, and ask them to identify whether the person is in one of the pictures. The soldiers also can query military databases that live in the main network. The testbed has three available databases: (1) news articles arriving on a military news feed, (2) transcripts of intercepted phone calls, and (3) descriptions of people relevant to the mission at hand and the operational area. The database containing the descriptions is called a black-gray-white (BGW) database, since each person is marked as bad, neutral or good. The soldiers in the field primarily search the BGW database, while the team at headquarters searches all three databases.

Ad-Hoc Routing

The APRL algorithm (Karp, 1998) from Harvard University provides the basic routing functionality for the soldiers. Each laptop continually broadcasts "ping" packets. A laptop that receives a "ping" packet knows that it is in transmission range of the sender and marks the sender as an immediate neighbor. The ping packet includes the complete routing table of the sender, so the receiving laptop

also adds routes for those laptops that are reachable via the sending laptop. As the laptops move relative to each other, they receive ping packets from different sets of neighbor laptops and update their routing tables accordingly.

The APRL algorithm has the benefit of simplicity, but it generates more control traffic than desired in some situations. In the ActComm project we developed several other routing algorithms. Under the GPSR algorithm from Harvard, the sending laptop looks up the physical location of the target laptop, and then sends the message to the neighboring laptop that is physically closest to the target's location and closer to the target than the sending laptop. Due to variations in laptop distribution, there might be times when there is no neighbor closer to the target. To handle these cases, GPSR uses a computational geometry approach to route packets around the boundaries of void regions, empty regions that contain no laptops. GPSR does require a robust position lookup service; in our military scenario, soldiers continuously exchange position information anyway. Every soldier's machine has the position information that GPSR needs, making GPSR particularly attractive for our environment.

GPSR generates less control traffic than APRL, but like APRL, does not take hop count or link delays into account. The STARA algorithm from the University of Illinois includes timestamps with each data packet, and estimates the delay along each path from source to target. STARA prefers paths with shorter delays, but the algorithm can detect if a long-delay path becomes a short-delay path due to changes in network topology or load.

Individual results demonstrate that APRL, GPSR and STARA outperform other ad-hoc routing algorithms in terms of the amount of control traffic or end-to-end packet latencies, but a team of Dartmouth staff and student programmers is comparing these three algorithms (as well as two popular alternative algorithms, AODV and ODMRP) on top of our fifty laptop testbed. These experiments are one of the first efforts to examine routing performance on top of this many real, rather than simulated, laptops. Currently, we have completed indoor baseline tests, and once the New England weather turns more clement in the spring, we will conduct a series of outdoor experiments with all fifty laptops.

Mobile Code and Agents

A mobile agent is simply the most general form of mobile code, namely, an executing program that can move at times of its own choosing from one machine to another. A mobile agent often, but not always, displays some of the other characteristics associated with agents, such as autonomy and adaptivity. Mobile agents are used to move computation to more attractive network locations, often to avoid the use of unreliable or low-bandwidth network links. In the ActComm testbed, mobile agents are used for two purposes.

First, mobile agents move from the soldiers' machines into the main network to perform all multi-step queries. [Mobile agents also perform the queries entered by the mission planners at headquarters, since headquarters itself often has an unreliable connection to the main network.] The agents interact with the needed databases without using the unreliable, low-bandwidth link that connects the soldiers to the main network. The agent completes the query faster, and does not waste bandwidth by sending intermediate results back to the soldiers. Of course, with sufficient a priori knowledge of a multi-step query, database or proxy developers could implement a single high-level operation that performs the query. Developers can never have a priori knowledge of all queries, however. Mobile agents allow the queries to be performed efficiently even when developers have not provided query-specific support.

Second, after a soldier sends an observation to headquarters, headquarters might send back a set of pictures. The soldier confirms whether the person she saw is in one of the pictures. In the testbed, headquarters sends not only the pictures, but also the code that displays the pictures and allows the soldier to browse them. The code and pictures are sent as a single mobile agent. As before, the picture-browsing code could be installed on the soldier's machine before the mission begins. The mobile agent, however, eliminates the need for the pre-installation step, something that is important if the mission is planned rapidly, and the soldier has never been involved in a "picture" mission before.

The mobile agents used in the ActComm testbed are implemented with Dartmouth's mobile-agent system, D'Agents, which supports Tcl, Scheme and Java agents. *Figure 2* compares the performance of D'Agents with traditional client/server techniques for a simplified version of one of the query tasks in our military scenario. In this version of the query task, a database provides a keyword-query interface to a corpus of documents. An application performs a keyword query to get a set of candidate documents, and then performs its own filtering to decide which of the candidate documents actually should be presented to the user. Either 5% or 20% of the candidate documents pass the application-specific filter. With mobile agents, the filtering is done at the document location, and only the filtered document set is sent across the network. In the client/server approach, all candidate documents are sent across the network for filtering on the client machine. As can be seen in the figure, mobile agents significantly outperform the client/server solution in terms of query completion

time, particularly as the number of clients increases. Although these results do not hold for all bandwidths or document sizes, mobile agents can provide significant performance benefits, and should be part of any distributed programmer's toolbox.

We recently added two resource-scheduling algorithms to D'Agents, one based on an (economic) market analogy, and one based on a new dynamic-programming approach to traditional task scheduling. As seen in *Figure 3*, the dynamic-programming approach allows a mobile agent to complete its task significantly faster than if the agent selects resource copies randomly. In the experiment behind this figure, the machines continuously launched mobile agents, each of which performed five sequential subtasks and could choose any of the machines for each subtask. Each machine had a random (and changing) background CPU load that affected how quickly the agents could complete their subtasks. Although these initial results are promising, further experiments are needed to examine different subtask structures, different network environments, and different mechanisms for collecting the environmental information (CPU load and current bandwidth) that the scheduling algorithms need. Fortunately, simulation results indicate that both algorithms are tolerant to errors in the measured information, allowing us to collect the information without excessive network traffic.

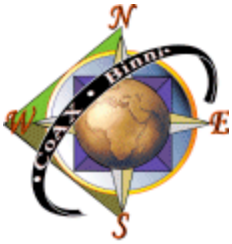
Conclusion

The routing algorithms and the mobile-code system are not the only critical components of the ActComm testbed. Other components include an active-messaging system, which queues messages during period of network disconnection, and a system to predict impending network disconnections based on observed error rates in received packets. Together, all of the ActComm components provide a robust, efficient and flexible infrastructure to support applications in ad-hoc wireless networks. With the current proliferation of such networks, the components and infrastructure will be applicable far beyond the military domain.

Acknowledgements

The ActComm project involves many people. Sue McGrath at Lockheed Martin, Eileen Entin at ALPHATECH, and Major Lisa Shay at RPI were instrumental in developing the counter-terrorism scenario. Brad Karp developed both the APRL and GPSR routing algorithms. The other lead researchers are George Cybenko, David Kotz and Daniela Rus at Dartmouth College, H. T. Kung at Harvard Univesity, Ken Vastola at RPI, P. R. Kumar, Tamer Basar and Gul Agha at the University of Illinois, and Ken Whitebread at Lockheed Martin. Arne Grimstrup and Ron Peterson, two staff members at Dartmouth, provided significant programming support. In addition, numerous students at each academic institution helped to integrate the components into the testbed. Finally, many thanks to the Department of Defense and AFOSR, who fund the project under AFOSR contract F49620-97-1-03821.

Coalition Agents experiment CoAX)



Part of the CMC's funding comes from the DARPA Control of Agent-Based Systems (CoABS) program,[1,2] which is concerned with the application of multi-agent systems to military command-and-control problems. A multi-agent system can be defined loosely as a collection of autonomous, goal-oriented programs (agents), interacting and cooperating with each other to accomplish some overall task. To demonstrate the benefits of these multi-agent systems, the CoABS program has conducted several Technology Integration Experiments (TIEs), most recently and notably the Coalition Agents eXperiment (CoAX).[3] The CoAX experiment demonstrated how multi-agent systems allow rapid and dynamic creation of appropriate command-and-control software infrastructures, even when the individual software components are under the control of multiple coalition partners. Dr. Austin Tate of the University of Edinburgh led the CoAX experiment, which involved software and personnel from twenty-nine universities and other organizations in the United States, England, and Australia. As a CoAX participant, Dartmouth College and the CMC explored the use of mobile agents, agents that can move under their own control from one machine to another within a heterogeneous network. Mobile agents are particularly attractive in a coalition setting, since they allow coalition partners to send processing functionality onto each other's machines, conserving network bandwidth and reducing latency when one coalition partner needs to access another's low-level data. Of course, such use of mobile agents involves numerous trust and security issues, but CoAX participants have developed sufficient resource-control and authentication systems for coalition partners to securely exchange mobile agents (after military commanders have given permission for the exchange of the underlying data).

In the most recent CoAX experiment, a regional conflict between fictional countries Gao and Agadez (over a disputed territory called Binni) led the United Nations to send a peacekeeping force to the area. During the peacekeeping mission, a Gao submarine attacked and damaged an Australian ship, the HMAS Coonawarra, and the United States was tasked with evacuating the wounded Australian sailors. Dartmouth provided a medical-monitoring system, based on mobile agents, that medics from the United States could use to monitor the condition of the wounded Australian sailors while those sailors were still on the ship. Essentially, we assumed that the Australian ship has some basic capability for monitoring the condition of the wounded sailors (oxygen saturation, heart rate, respiration rate, etc.), and can provide a raw stream of medical data to authorized software applications. This assumption is actually quite safe, since Dartmouth has a functional prototype system that uses a pulse oximeter (and some backend signal processing) to obtain this medical data. The wounded sailors in the CoAX demonstration were fictional, of course, so we used simulated medical data, rather than data from real pulse oximeters. The rest of the real software system was used as is, however. Essentially, the United States medics, who held ultimate responsible for the treatment of the wounded sailors, used the system to launch a mobile agent onto a machine on the Australian ship. This mobile agent monitored the raw data stream, using various medical models to quantify the sailors' current condition and to identify any changes in that condition. The agent sent only critical information and alerts back to the medics, rather than the raw data streams. The mobile agent, therefore, allowed the United States medics to monitor the sailors' condition using their own familiar algorithms, while still conserving significant network bandwidth. Of course, Australia could pre-install the United States monitoring routines on their ships, but such pre-installation is difficult even in the best of circumstances, let alone in the middle of a rapidly established coalition operation.

Although mobile agents are not effective for all applications, they should be a prominent part of a distributed-programmer's toolkit. Whenever pre-installation is difficult, and data volumes are large or networks unreliable, mobile agents can lead to significantly more efficient data access than traditional client/server techniques. In the case of the CoAX experiment, the raw streams of medical data were immense, and the network connection from a real ship to other military entities would be both low-bandwidth and high latency, and potentially be quite unreliable over short periods of time. Mobile agents allowed the medical-monitoring system to make minimal use of this network connection, while still providing the needed alerts to the United States medics. Although the CoAX experiment is over, many other military and civilian applications for mobile agents exist, and the CMC will continue to explore the application space.

---

[1] DARPA contract F30602-98-2-0107
[2] http://coabs.globalinfotek.com/
[3] http://www.aiai.ed.ac.uk/project/coax/

PARTNERS

Apple

Cisco Systems

Informix Software

MERL

Microsoft

Microsoft Research

Nortel Networks

NTT DoCoMo

DoCoMo USA Labs

Nuance

Versus Technology, Inc.

CMC Partnership

Our goal is to conduct advanced research in topics that are relevant to future commercial, government, and educational applications and products. We currently focus on pervasive and mobile computing, wireless networks, and sensor networks.

There are clear benefits for partnerships with Dartmouth's Center for Mobile Computing. Partners have early access to advanced research that can lead to next-generation products and services. Other benefits include:

- Subscription to this newsletter;
- Access to CMC students, making connections that may lead to future employment and other relationships;
- Early access to prototype systems;
- Access to CMC labs and facilities, when appropriate, and
- **[NEW]** access to wireless trace data.

Key People

Assistant Professor Edmond Cooley
Thayer School of Engineering
http://engineering.dartmouth.edu/~tedc

Professor George Cybenko
Thayer School of Engineering
http://www.dartmouth.edu/~gvc/

Chief Research Engineer Bob Gray
Thayer School of Engineering
http://actcomm.dartmouth.edu/~rgray/

Associate Professor David Kotz
Department of Computer Science
http://www.cs.dartmouth.edu/~dfk/

Chief Research Engineer and Lecturer Susan McGrath
Thayer School of Engineering
http://www.ists.dartmouth.edu/IRIA/bios.htm#mcgrath

Associate Professor Daniela Rus
Department of Computer Science
http://www.cs.dartmouth.edu/~rus/

As of December 2002 the group also includes 3 staff, 6 graduate and 6 undergraduate students.

Contact: cmc@cs.dartmouth.edu
Individuals: First.Last@dartmouth.edu