CMC

Center for Mobile Computing • Dartmouth College • September 2006 • cmc.cs.dartmouth.edu

CRAWDAD Supplies Researchers with Wireless Data

A Community Resource for Archiving Wireless Data at Dartmouth (CRAWDAD, funded by the National Science Foundation, continues to help researchers and educators worldwide who are interested in using wireless network data and associated tools for collecting and processing the data.

The CRAWDAD project stores large data sets collected from real wireless networks, and develops tools for collecting, sanitizing, and analyzing this data. Used at over 205 universities and research labs by more than 300 users, the CRAWDAD archive has contributed to the wireless research community in a broad range of areas including workload characterization, location-aware services, network management, and protocol development.

Professors David Kotz and Tristan Henderson were joined in November by staffer Jihwang Yeo, who is developing software and managing the CRAWDAD collection. They have been approaching wireless network operators and researchers to encourage them to contribute their data to the archive. They recently made major changes to the CRAWDAD website with several new features:

- several new tools and data sets, including data from Bluetooth networks, MANETs (Mobile Ad hoc Networks), DTNs (disruption tolerant networks), and location-aware data sets;
- a structured metadata description of each data set and tool;
- basic and advanced searches on CRAWDAD data, tools, authors, and papers; and
- a wiki for the community to share ideas and techniques with others.

They are also setting up special-interest "Areas" within the collection. Tracy Camp, an Associate Professor at the Colorado School of Mines, is the MANET Area Editor, and John McHugh, Professor at Dalhousie University, became the Education Area Editor.

The CRAWDAD team has started compiling "HOWTO" documents on various topics such as collecting data, sanitizing data, and writing an IRB proposal, to make it easy for other researchers to conduct measurement studies or to use measurement data. These documents are on the CRAWDAD wiki. They also plan to host the second CRAWDAD workshop, co-located with ACM Mobicom in September 2006, for those interested in measuring or analyzing wireless-network traffic, studying wireless-device mobility, or building models or simulators of wireless networks. Through these efforts, by working with the community to ensure that the archive meets community needs, the CRAWDAD team hopes to support innovative research.

For more information, visit http://CRAWDAD.cs.dartmouth.edu.

Securing Wireless Networks

Is your mobile phone secure? Imagine if someone:

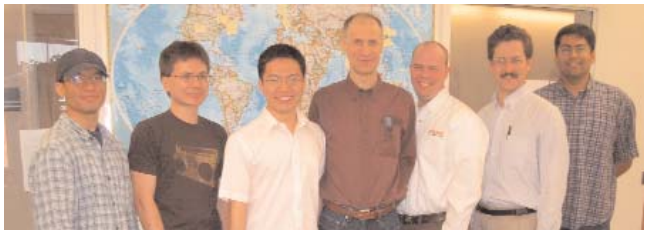
- Intercepted your voice traffic, and replaced it with their own; your business call that includes the phrase "no, the deal's off" becomes "yes, I agree to all your terms",
- Blocked your voice traffic; you attempt to make an E-911 call to report your burning house, and the call connects, but the fire station is unable to hear where you live, or
- Stole bandwidth from your mobile phone; so you are unable to make any calls.

These are some of the problems being examined in the MAP (Measure, Analyze, Protect) research project. IEEE 802.11 wireless networks are increasingly being used to carry voice (VoWLAN or Voice over Wireless Local Area Network) traffic, and new mobile phones feature technology for switching between traditional cellular and 802.11 networks. The shared medium and unlicensed nature of these 802.11 networks means that any complete wireless security solution must address denial of service (DoS) attacks against real-time voice traffic. Such attacks can be far more subtle than traditional DoS attacks, with one or two malicious frames being sufficient to disrupt a voice call.

The MAP project proposes a three-point approach to these problems. First, they are investigating scalable methods for measuring 802.11 wireless networks. Second, they are using novel statistical techniques for real-time analysis of this measured data. These techniques will allow them to detect the anomalies caused by subtle MAC-layer attacks, and feed into the third component of the project, whereby system administrators are notified of attacks and can take appropriate protection actions.

The Homeland Security Advanced Research Projects Agency (HSARPA) is funding a group of researchers from Dartmouth, the University of Massachusetts Lowell, and Aruba Networks to implement and deploy the MAP system. An initial deployment throughout the Dartmouth Computer Science building using Aruba Networks hardware is planned for later this year, with a full campus-wide deployment possible next year.

See http://www.cs.dartmouth.edu/~map/ for more information.

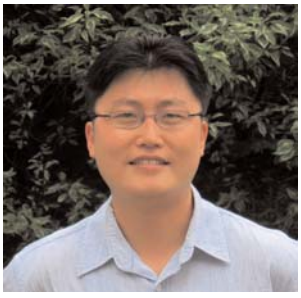


Jihwang Yeo Joins Staff of CRAWDAD Project

Jihwang Yeo is a programmer and administrator for the CRAWDAD project, working with Professors David Kotz and Tristan Henderson.

Prior to joining Dartmouth College, he was a research assistant in the MIND (Maryland Information and Network Dynamics) lab at University of Maryland, where his primary contribution was the development of a wireless monitoring technique for the analysis and modeling of wireless traffic. His professional career also includes developing an XML/SOAP-database gateway when he worked at the IBM Almaden Research Center in summer 2001.

He received a master's degree in Computer Science from University of Maryland, College Park MD. He also holds a bachelor's degree and another master's degree in Computer Engineering from Seoul National University, in Korea.



Graduates

Kazuhiro Minami recently completed his Ph.D. thesis "Secure Context-sensitive Authorization", in which he built and evaluated a distributed authorization system that protects confidential policies and context information in each administrative domain. Kazuhiro is now an I3P Fellow at the Information Trust Institute at University of Illinois at Urbana-Champaign for the 2006-2007 academic year.

Zhenhui Jiang completed his M.S. thesis on "A Combined Routing Method for Ad hoc Wireless Networks", in which he proposes a way for a MANET to switch routing protocols on the fly (while continuing to route packets). He recently began work as a programmer at SYSTRA Consulting in Lebanon, NH.

New Postdoc

Apu Kapadia received his PhD from the University of Illinois at Urbana-Champaign and was the recipient of a four-year High-Performance Computer Science Fellowship from the Department of Energy. His doctoral research focused on trustworthy communication and models for privacy in pervasive environments. In October 2005, Apu joined ISTS as a Post-Doctoral Research Fellow and is working with Profs. David Kotz and Sean Smith on topics related to location privacy, mobile computing, trustworthy platforms, and public-key infrastructures.

CMC News

CMC Updates by Email

You can now receive CMC news by email. Simply email a message to listserv@listserv.dartmouth.edu with a message whose body says only "SUB CMC-news", or visit the CMC web site and click on the link in the News section.

Aruba Networks Donates Hardware to CMC

Aruba Networks, a leading vendor of Wi-Fi networking equipment to enterprises around the world, donated several of their AP70-model access points to our wireless networking lab. These APs have immediately been useful for experimental work in security (MAP project) and for sensor-network experiments (PLACE project). These versatile APs have two radios and a USB port. We are grateful to Aruba Networks for their generous donation.

Palm Donates Treos and Tungstens to CMC

Palm Computing, the leading vendor of personal digital assistants and smart phones, has donated a collection of Treo 650 smart phones and Tungsten E2 PDAs for use in our research and education projects. So far these have been used by software-design students to develop a mobile user-survey application for a local science museum, by a research student to explore secure interactions between PDAs and public kiosk computers, and by the PLACE project. We are grateful to Palm Computing for their generous donation.

Privacy in Location-Aware Computing Environments (PLACE)

Digital technology plays an increasing role in everyday life, and this trend is only accelerating. Consider daily life five years from now, in 2010: we will each be surrounded by far more digital devices, mediating far more activities in our work, home, and play; the boundary between cyberspace and physical space will fade as sensors and actuators allow computers to be aware of, and control, the physical environment; and the devices in our life become increasingly (and often invisibly) interconnected with each other and with the Internet. Today, typical home users struggle to maintain the security of their home computer and have difficulty managing their privacy online. Tomorrow, these challenges may become unimaginably complex. This 18-month project studies, and begins to address, the security and privacy challenges involved in developing this world of Digital Living in 2010.

Specifically, this project focuses on the advent of sensor networks, their applications in the home and work environment. Although sensor networks have been an active area of academic research, and are becoming commercially available for deployment in industrial settings, sensor networks will soon have many uses in enterprise and residential settings. People will live in spaces, or work with devices, that have embedded sensing capability. For people to accept this new technology into their lives, they must be able to have confidence that the systems work as expected, and do not pose unreasonable threats to personal privacy.

This confidence results from a variety of technical and organizational mechanisms. This project delves into the sociological underpinnings of privacy and trust in digital living, into the technological foundations for secure and robust sensor networks, and into mechanisms for users to express control over information about their activity. The PLACE project chose to focus on location, and location privacy, because location is fundamental to many pervasive-computing applications and is likely to be one of the first types of sensor data to be incorporated into working systems and applications.

This research program is a part of the Institute for Security Technology Studies at Dartmouth College, supported by Grant number 2005-DD-BX-1091 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this article are those of the authors and do not represent the official position or policies of the United States Department of Justice.

Bennet Vance Joins Staff

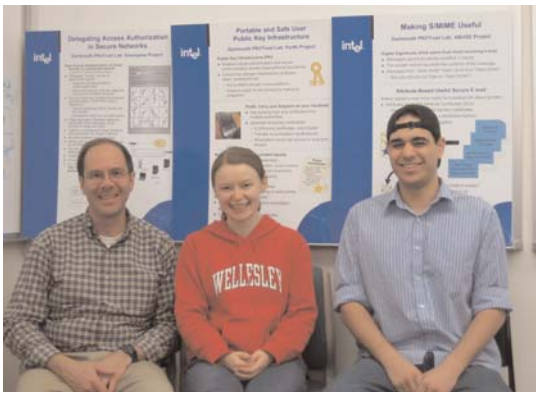
Bennet Vance was a public school student in Hanover when computing arrived at Dartmouth in the 1960s. Bennet soon acquired the habit of heading over to the computation center after school to try out his latest BASIC programs. His subsequent career as a software developer has included stints at AT&T Bell Laboratories in New Jersey; at True BASIC, the compiler company co-founded by Dartmouth computing pioneers John Kemeny and Thomas Kurtz; and at the IBM Almaden Research Center in Silicon Valley, where he helped extend IBM's DB2 database system. Returning to Hanover in 2001, Bennet worked in Dartmouth's Department of Psychological and Brain Sciences before taking his current position with the MAP project. He holds a bachelor's degree in math from Yale and graduate degrees in computer science from Stanford and from the OGI School of Science & Engineering.

Greenpass Demonstration a Success

In December, the Dartmouth PKI Lab, funded in part by ISTS, showed off their Greenpass project and described other current research at the Intel IT Innovation and Research Open House, held in Folsom, California. This event for key Intel technical experts and researchers, university partners, and invited press and analysts highlighted current technology trends and challenges and showcased Intel's enterprise and information technology R&D activities.

Bob Brentrup, then Dartmouth's Associate Director of Technical Services, installed a working demo of Greenpass, which provides delegated guest access to a secure wireless or wired network using the 802.1x and EAP/TLS protocols. Visitors to the Greenpass exhibit were able to connect their laptops to the Greenpass web application, obtain a guest delegation certificate, and then reconnect their system to the secure network. The installation consisted of a wireless access point, network switch and router, and a laptop running the Greenpass servers. A Greenpass system installation integrated on a bootable Linux CD was used to create the server computer's disk image on site.

Brentrup developed the demonstration and staffed the Greenpass exhibit at Intel along with Ph.D. students Chris Masone and Sara Sinclair. Brentrup reports, "The visitors we talked to were impressed with the Greenpass concept and its implementation. They felt that the system would be a useful ongoing addition to a secure wireless network. They could see applications of it within Intel.



Intel and Cisco Systems sponsored the graduate student research by Nick Goffee and Sung Kim, who developed the Greenpass prototype under the direction of Professor Sean Smith and William Taylor. Intel and Dartmouth's ISTS have committed to provide additional support to refine the prototype and develop an open source distribution. Dartmouth's PKI Lab continues to work with Intel and plans to explore an ongoing deployment of Greenpass and related projects.

For more information, visit http://www.dartmouth.edu/~pkilab/greenpass

Yong Sheng, New MAP Postdoc

In September, Yong Sheng joined the MAP project as a postdoctoral researcher, where he will focus on wireless-network intrusion detection and analysis. He received the B.S. degree in Computer Engineering in 1992 from the Beijing University of Posts and Telecommunications (BUPT), and the M.S. degree in Computer Engineering (1996, also from BUPT). He just finished his Ph.D. Program in Computer Engineering in August 2006, from Dartmouth College, Hanover, NH, with the dissertation entitled "The Theory of Trackability and Robustness from Process Detection".

Yong's research interests include stochastic modeling, detection and estimation theory, time series pattern analysis, computer and network security, autonomic computing, and collaborative signal processing for distributed sensor networks and data fusion.

PorKI Enhances Portability, Security of Cryptographic Infrastructures

With their Portable Key Infrastructure (PorKI) project, Sarah Sinclair and Sean Smith of the PKI/Trust Laboratory are working to integrate human needs-- particularly, portability-- into existing Public Key Infrastructures (PKIs).

Secure web connections via SSL and encrypted or signed email through S/MIME depend on PKI and its use of public key cryptography to enable secure communication among parties who do not share secrets a priori.

Security in a PKI depends on the protection of a user's private key. PorKI stores a user's keys on a PDA or other handheld device, and allows the user to generate temporary keys for use on different individual computers. This allows users to bring their keys with them, and decreases the chance that a malicious workstation can compromise them. This work is funded in part by the Intel Corporation.

Mesh Networks for Emergency Response

In a project funded by Dartmouth's Institute for Security Technology Studies (ISTS), Ph.D. student Soumendra Nanda is exploring ways to deploy and manage Wi-Fi mesh networks in support of emergency responders at large-scale disaster scenes. "We imagine a mesh router on every fire truck, ambulance, and police car, as well as portable nodes that can be deployed throughout a disaster scene." A mesh network can quickly self-organize and provide Wi-Fi coverage for portable devices, such as the triage PDAs and environmental sensors developed in a companion ISTS project. Soumendra and his advisor David Kotz have deployed an experimental multi-radio mesh network in the Department of Computer Science, and are developing scalable protocols in order to monitor the dynamic state of the mobile network and diagnose its network failures in real-time.

This research program is a part of the ISTS and is supported by Grant number 2005-DD-BX-1091 awarded by the Bureau of Justice Assistance. For more information, see page 2. We are also grateful to the Intel Corporation for their donation of mesh routers, and to Aruba Netwrks for their donation of AP70 wireless access points.

New Research Papers

Complete Text at http://cmc.cs.dartmouth.edu/papers

Minkyong Kim and David Kotz. Periodic properties of user mobility and access-point popularity. Journal of Personal and Ubiquitous Computing, 2006. Special Issue of papers from LoCA 2005; Accepted for publication.

Understanding user mobility and its effect on access points (APs) is important in designing location-aware systems and wireless networks. Although various studies of wireless networks have provided useful insights, it is hard to apply them to other situations. Here we present a general methodology for extracting mobility information from wireless network traces, and for classifying mobile users and APs. We used the Fourier transform to reveal important periods and chose the two strongest to serve as parameters to a classification system based on Bayes' theory. Analysis of one-month traces shows that while a daily pattern is common among both users and APs, a weekly pattern is common only for APs. Analysis of one-year traces revealed that both user mobility and AP popularity depend on the academic calendar. By plotting the classes of APs on our campus map, we discovered that their periodic behavior depends on their proximity to other APs.

Minkyong Kim, David Kotz, and Songkuk Kim. Extracting a mobility model from real user traces. In Proceedings of the 25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Barcelona, Spain, April 2006. IEEE Computer Society Press.

Understanding user mobility is critical for simulations of mobile devices in a wireless network, but current mobility models often do not reflect real user movements. In this paper, we provide a foundation for such work by exploring mobility characteristics in traces of mobile users. We present a method to estimate the physical location of users from a large trace of mobile devices associating with access points in a wireless network. Using this method, we extracted tracks of always-on Wi-Fi devices from a 13-month trace. We discovered that the speed and pause time each follow a log-normal distribution and that the direction of movements closely reflects the direction of roads and walkways. Based on the extracted mobility characteristics, we developed a mobility model, focusing on movements among popular regions. Our validation shows that synthetic tracks match real tracks with a median relative error of 17%.

Minkyong Kim, Jeffrey J. Fielding, and David Kotz. Risks of using AP locations discovered through war driving. In Proceedings of the Fourth International Conference on Pervasive Computing (Pervasive), volume 3968 of Lecture Notes in Computer Science, pages 67-82, Dublin, Ireland, May 2006. Springer-Verlag.

Many pervasive-computing applications depend on knowledge of user location. Because most current location-sensing techniques work only either indoors or outdoors, researchers have started using 802.11 beacon frames from access points (APs) to provide broader coverage. To use 802.11 beacons, they need to know AP locations. Because the actual locations are often unavailable, they use estimated locations from \emphwar driving. But these estimated locations may be different from actual locations. In this paper, we analyzed the errors in these estimates and the effect of these errors on other applications that depend on them. We found that the estimated AP locations have a median error of 32 meters. We considered the error in tracking user positions both indoors and outdoors. Using actual AP locations, we could improve the accuracy as much as 70% for indoors and 59% for outdoors. We also analyzed the effect of using estimated AP locations in computing AP coverage range and estimating interference among APs. The coverage range appeared to be shorter and the interference appeared to be more severe than in reality.

Guanling Chen, Heng Huang, and Minkyong Kim. Mining Frequent and Periodic Association Patterns. Technical Report TR2005-550, Dept. of Computer Science, Dartmouth College, Hanover, NH, July 2005.

Profiling the clients' movement behaviors is useful for mobility modeling, anomaly detection, and location prediction. In this paper, we study clients' frequent and periodic movement patterns in a campus wireless network. We use offline data-mining algorithms to discover patterns from clients' association history, and analyze the reported patterns using statistical methods. Many of our results reflect the common characteristics of a typical academic campus, though we also observed some unusual association patterns. There are two challenges: one is to remove noise from data for efficient pattern discovery, and the other is to interpret discovered patterns. We address the first challenge using a heuristic-based approach applying domain knowledge. The second issue is harder to address because we do not have the knowledge of people's activities, but nonetheless we could make reasonable interpretation of the common patterns.

Guanling Chen and David Kotz. Structural analysis of social networks with wireless users. Technical Report TR2005-549, Dept. of Computer Science, Dartmouth College, July 2005.

Online interactions between computer users form Internet-based social networks. In this paper we present a structural analysis of two such networks with wireless users. In one network the wireless users participate in a global file-sharing system, and in the other they interact with each other through a local music-streaming application.

Udayan Deshpande, Tristan Henderson, and David Kotz. Channel sampling strategies for monitoring wireless networks. In Proceedings of the Second International Workshop On Wireless Network Measurement (WiNMee). IEEE Computer Society Press, April 2006.

Monitoring the activity on an IEEE 802.11 network is useful for many applications, such as network management, optimizing deployment, or detecting network attacks. Deploying wireless sniffers to monitor every access point in an enterprise network, however, may be expensive or impractical. Moreover, some applications may require the deployment of multiple sniffers to monitor the numerous channels in an 802.11 network. In this paper, we explore sampling strategies for monitoring multiple channels in 802.11b/g networks. We describe a simple sampling strategy, where each channel is observed for an equal, predetermined length of time, and consider applications where such a strategy might be appropriate. We then introduce a sampling strategy that weights the time spent on each channel according to the number of frames observed on that channel, and compare the two strategies under experimental conditions.

Zhenhui Jiang. A combined routing method for ad hoc wireless networks. Master's thesis, Dept. of Computer Science, Dartmouth College, December 2005. Available as Dartmouth Computer Science Technical Report TR2005-566.

To make ad hoc wireless networks adaptive to different mobility and traffic patterns, we studied in this thesis an approach to swap from one protocol to another protocol dynamically, while routing continues. By the insertion of a new layer, we were able to make each node in the ad hoc wireless network notify each other about the protocol swap. To ensure that routing works efficiently after the protocol swap, we initialized the destination routing protocol's data structures and reused the previous routing information to build the new routing table. We also tested our approach under different network topologies and traffic patterns in static networks to learn whether the swap is fast and whether the swap incurs too much overload . We found that the swap latency is related to the destination protocol and the topology of the network. We also found that the control packet ratio after swap is close to the protocol running without swap, which means our method does not incur too many control packets for swap.

Zack Butler, Peter Corke, Ron Peterson, and Daniela Rus. From Robots to Animals: Virtual Fences for Controlling Cattle. International Journal of Robotics Research 25 (5/6), May/June 2006, pages 485-508.

We consider the problem of monitoring and controlling the position of herd animals, and view animals as networked agents with natural mobility but not strictly controllable. By exploiting knowledge of individual and herd behavior we would like to apply a vast body of theory in robotics and motion planning to achieving the constrained motion of a herd. In this paper we describe the concept of a virtual fence which applies a stimulus to an animal as a function of its pose with respect to the fenceline. Multiple fence lines can define a region, and the fences can be static or dynamic. The fence algorithm is implemented by a small position-aware computer device worn by the

New Research Papers (Continued)

animal, which we refer to as a Smart Collar. We describe a herd-animal simulator, the Smart Collar hardware and algorithms for tracking and controlling animals as well as the results of on-farm experiments with up to ten Smart Collars.

Kazuhiro Minami and David Kotz. Scalability in a secure distributed proof system. In Proceedings of the Fourth International Conference on Pervasive Computing (Pervasive), volume 3968 of Lecture Notes in Computer Science, pages 220-237, Dublin, Ireland, May 2006. Springer-Verlag.

A logic-based language is often adopted in systems for pervasive computing, because it provides a convenient way to define rules that change the behavior of the systems dynamically. Those systems might define rules that refer to the users' context information to provide context-aware services. For example, a smart-home application could define rules referring to the location of a user to control the light of a house automatically. In general, the context information is maintained in different administrative domains, and it is, therefore, desirable to construct a proof in a distributed way while preserving each domain's confidentiality policies. In this paper, we introduce such a system, a secure distributed proof system for context-sensitive authorization and show that our novel caching and revocation mechanism improves the performance of the system, which depends on public key cryptographic operations to protect confidential information in rules and facts. Our revocation mechanism maintains dependencies among facts and recursively revokes across multiple hosts all the cached facts that depend on a fact that has become invalid. Our initial experimental results show that our caching mechanism, which maintains both positive and negative facts, significantly reduces the latency for handling a logical query.

Kazuhiro Minami. Secure Context-sensitive Authorization. PhD thesis, Dartmouth College, Computer Science, Hanover, NH, February 2006. Available as Dartmouth College Computer Science Technical Report TR2006-571.

Pervasive computing leads to an increased integration between the real world and the computational world, and many applications in pervasive computing adapt to the user's context, such as the location of the user and relevant devices, the presence of other people, light or sound conditions, or available network bandwidth, to meet a user's continuously changing requirements without taking explicit input from the users.
We consider a class of applications that wish to consider a user's context when deciding whether to authorize a user's access to important physical or information resources. Such a context-sensitive authorization scheme is necessary when a mobile user moves across multiple administrative domains where they are not registered in advance. Also, users interacting with their environment need a non-intrusive way to access resources, and clues about their context may be useful input into authorization policies for these resources. Existing systems for context-sensitive authorization take a logic-based approach, because a logical language makes it possible to define a context model where a contextual fact is expressed with a boolean predicate and to derive higher-level context information and authorization decisions from contextual facts.
However, those existing context-sensitive authorization systems have a central server that collects context information, and evaluates policies to make authorization decisions on behalf of a resource owner. A centralized solution assumes that all resource owners trust the server to make correct decisions, and all users trust the server not to disclose private context information. In many realistic applications of pervasive computing, however, the resources, users, and sources of context information are inherently distributed among many organizations that do not necessarily trust each other. Resource owners may not trust the integrity of context information produced by another domain, and context sensors may not trust others with the confidentiality of data they provide about users.
In this thesis, we present a secure distributed proof system for context-sensitive authorization. Our system enables multiple hosts to evaluate an authorization query in a peer-to-peer way, while preserving the confidentiality and integrity policies of mutually untrusted principals running those hosts. We also develop a novel caching and revocation mechanism to support context-sensitive policies that refer to information in dozens of different administrative domains. Contributions of this thesis include the definition of fine-grained security policies that specify trust relations among principals in terms of information confidentiality and integrity, the design and implementation of a secure distributed proof system, a proof for the correctness of our algorithm, and a performance evaluation showing that the amortized performance of our system scales to dozens of servers in different domains.

Libo Song, David Kotz, Ravi Jain, and Xiaoning He. Evaluating next cell predictors with extensive Wi-Fi mobility data. IEEE Transactions on Mobile Computing, January 2006. Accepted for publication.

Location is an important feature for many applications, and wireless networks can better serve their clients by anticipating client mobility. As a result, many location predictors have been proposed in the literature, though few have been evaluated with empirical evidence. This paper reports on the results of the first extensive empirical evaluation of location predictors, using a two-year trace of the mobility patterns of over 6,000 users on Dartmouth's campus-wide Wi-Fi wireless network. The surprising results provide critical evidence for anyone designing or using mobility predictors.
We implemented and compared the prediction accuracy of several location predictors drawn from four major families of domain-independent predictors, namely Markov-based, compression-based, PPM, and SPM predictors. We found that low-order Markov predictors performed as well or better than the more complex and more space-consuming compression-based predictors.

Libo Song, Udayan Deshpande, Ula\cs C. Kozat, David Kotz, and Ravi Jain. Predictability of WLAN mobility and its effects on bandwidth provisioning. In Proceedings of the 25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Barcelona, Spain, April 2006. IEEE Computer Society Press.

Wireless local area networks (WLANs) are emerging as a popular technology for access to the Internet and enterprise networks. In the long term, the success of WLANs depends on services that support mobile network clients. Although other researchers have explored mobility prediction in hypothetical scenarios, evaluating their predictors analytically or with synthetic data, few studies have been able to evaluate their predictors with real user mobility data. As a first step towards filling this fundamental gap, we work with a large data set collected from the Dartmouth College campus-wide wireless network that hosts more than 500 access points and 6,000 users. Extending our earlier work that focuses on predicting the next-visited access point (i.e., location), in this work we explore the predictability of the time of user mobility. Indeed, our contributions are two-fold. First, we evaluate a series of predictors that reflect possible dependencies across time and space while benefiting from either individual or group mobility behaviors. Second, as a case study we examine voice applications and the use of handoff prediction for advance bandwidth reservation. Using application-specific performance metrics such as call drop and call block rates, we provide a picture of the potential gains of prediction.
Our results indicate that it is difficult to predict handoff time accurately, when applied to real campus WLAN data. However, the findings of our case study also suggest that application performance can be improved significantly even with predictors that are only moderately accurate. The gains depend on the applications' ability to use predictions and tolerate inaccurate predictions. In the case study, we combine the real mobility data with synthesized traffic data. The results show that intelligent prediction can lead to significant reductions in the rate at which active calls are dropped due to handoffs with marginal increments in the rate at which new calls are blocked.

To hear about new CMC papers as soon as they're posted, subscribe to the CMC-Papers mailing list. Simply send email to listserv@listserv.dartmouth.edu with a message whose body says only "SUB CMC-papers", or visit the CMC web site and click on the link in the Papers section.

About the CMC

The goal of the Center for Mobile Computing at Dartmouth College is to realize the potential for ubiquitous mobile devices and wireless communications to improve the way we live, the way we work, and the way we learn.

We have the opportunity to leverage Dartmouth's campus-wide wireless network, its group of experienced researchers, its residential campus with an innovative and creative student culture, its long tradition of pervasive deployment of cutting-edge technology and of technology in the classroom, and its local institutes for Security Technology (ISTS) and Information Infrastructure Protection (I3P). This combination makes Dartmouth College a unique environment for understanding the future, in which mobile computing becomes ubiquitous on university campuses, corporate campuses, and the consumer world.

The CMC is comprised of researchers from the Departments of Computer Science and Sociology and from the Thayer School of Engineering, including faculty, post-doctoral researchers, M.E. and Ph.D. students, and undergraduate students. Participating faculty members have extensive experience in wireless networks, sensor networks, mobile agents, parallel and distributed computing, operating systems, information retrieval, robotics, signal processing, and sociology.

The Center's projects receive support from industry donors Aruba, Cisco, Intel, and Palm, and federal funding from the Departments of Homeland Security and Department of Justice (through ISTS), the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research, and the National Science Foundation.

Center research facilities include campus-wide wired and wireless networks, a heterogeneous collection of mobile computing systems, and a growing lab supporting wireless-network research and sensor-network research. In effect, Dartmouth College is an extensive testbed with several thousand networked computers and active users.

Partnership

We invite corporations to become Partners of the CMC. Partners have early access to advanced research that can lead to next-generation products and services. At the same time, the CMC benefits from a better understanding of the needs and direction of industry, helping to keep research relevant and driven by application needs.

Contact us if you are interested in being a partner at cmc@cs.dartmouth.edu

Benefits:

- Access to CMC students, making connections that may lead to future employment
- Access to CMC faculty
- Early access to prototypes
- Access to CMC labs and facilities, when appropriate.

Ultimately, each partnership leads to a host of benefits and to a relationship that can be customized to the needs and interests of the partner.

Current Supporters

CMC Faculty and Staff

http://cmc.cs.dartmouth.edu/people/

Professor Denise Anthony, Department of Sociology

Professor Andrew Campbell, Department of Computer Science

Professor Ted Cooley, Thayer School of Engineering

Professor George Cybenko, Thayer School of Engineering

Research Professor Tristan Henderson, Department of Computer Science

Professor David Kotz, Department of Computer Science

Research Professor Sue McGrath, Thayer School of Engineering

Adjunct Professor Daniela Rus, Department of Computer Science

Professor Sean Smith, Department of Computer Science

Ron Peterson, Senior Programmer, Department of Computer Science

Bennet Vance, MAP Programmer, Department of Computer Science

Jihwang Yeo, CRAWDAD Programmer, Department of Computer Science

CONTACTS

General information, partnership inquiries, and subscription changes: cmc@cs.dartmouth.edu

All Dartmouth people mentioned in this newsletter can be reached at: firstname.lastname@dartmouth.edu