

(MITACS)
Security Research
in Canada



Canada France Meeting on Security, Dec 06-08

New/Old MITACS Projects

- Continuous change within MITACS:
- New projects considered twice a year

Summary

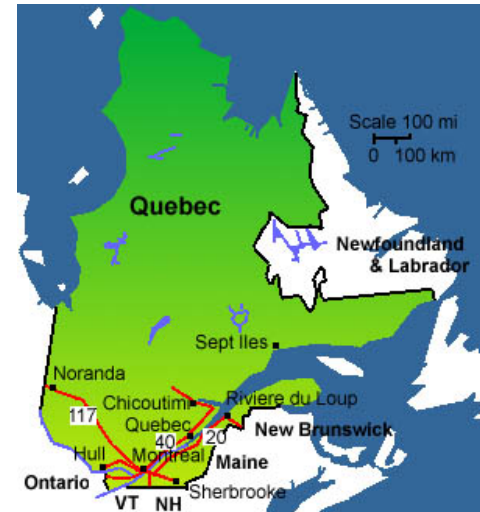
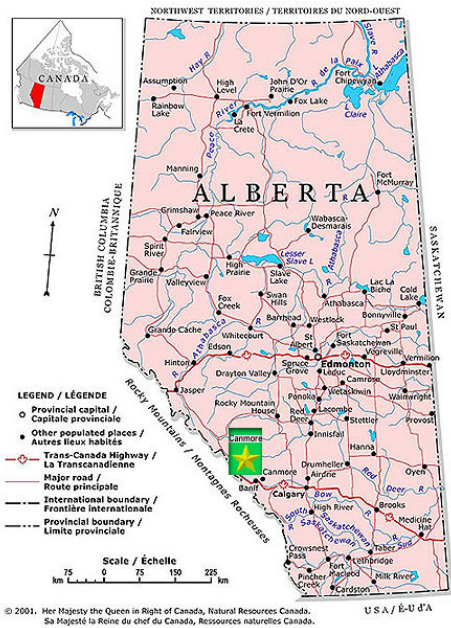
Goals of Security Research

- Strengthen emerging areas
- Amplify strengths within Canada
- Incorporate security research within existing projects
- Study and research (all) mathematical aspects of security



Canada France Meeting on Security, Dec 06-08

Analog Wideband Communications Based on Nonlinear Dynamics



Analog Wideband Communications Based on Nonlinear Dynamics

- **Project Leader:** Henry Leung, University of Calgary
- **Co-investigators:**
Guarong Chen, City University of Hong Kong, Robert Elliott, University of Calgary, Michael C. Mackey, McGill University, John G. Milton, Claremont College, Jianhong Wu, York University
- **Non-NCE partners:**
AUG Signals Ltd., Alberta Ingenuity, Canadian Microelectronics Corp., Communication Research Center, DRDC Valcartier, National Research Council Canada

Research

- Analog wideband communications have the potential to eliminate the drawbacks of power-hungry digital wideband systems.
- Develop an analog system along with a working plan for its implementation.
- Research focused on transmitter, the channel, and the receiver.
- Techniques from areas such as artificial intelligence are being used to develop mathematical models that describe phenomena such as signal propagation and noise distortion in home networks.

Complex Adaptive Networks for Computing and Communication



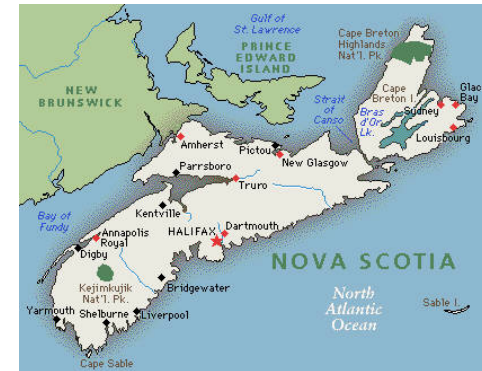
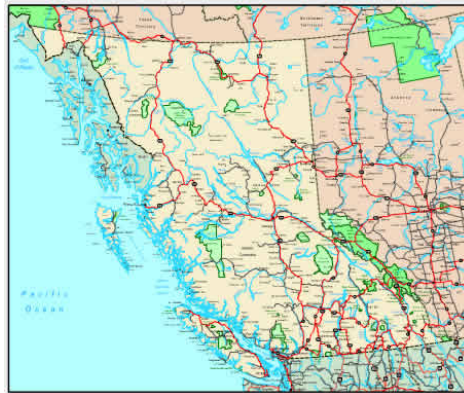
Complex Adaptive Networks for Computing and Communication

- **Project Leader:** Michel Barbeau, Carleton University
- **Co-investigators:**
Evangelos Kranakis, Carleton University, Ioannis Lambadaris,
Carleton University, Raj Srinivasan, University of
Saskatchewan, Yiqiang Zhao, Carleton University
- **Non-NCE partners:**
Alcatel-Lucent, Cistel Technology Corp., Nortel Networks,
Solana Networks Inc.

Research

- New methods for detecting malicious access in wireless networks
- Communications mechanisms between smart toys
- RFF
- RFID
- Security Risk Analysis
- Methods for detecting faults in networks and making them fault tolerant.

Modeling and Mining of Networked Information Spaces



Modeling and Mining of Networked Information Spaces

- **Project Leader:** Jeannette Janssen & Evangelos Milios, Dalhousie University
- **Co-investigators:**
Bill Aiello, University of British Columbia, Anthony Bonato, Wilfrid Laurier University, Allan Borodin, University of Toronto, Malcolm Heywood, Dalhousie University, Nauzer Kalyaniwalla, Dalhousie University, Nur Zincir-Heywood, Dalhousie University
- **Non-NCE partners:**
Brandimensions Inc., Communications Security Establishment, RCMP, Telecom Applications Research Alliance

Research

- Studies on the Internet
- Methods to detect unusual email patterns without looking at the messages themselves; using methods that mimic evolution.
- Internet traffic models have been developed that can help detect attacks before their consequences become catastrophic.
- Algorithms to analyze online discussion groups such as blogs and wikis to help companies optimize their marketing efforts.

Privacy and Number-Theoretic Cryptography



Privacy and Number-Theoretic Cryptography

- **Project Leader:** Alfred Menezes, University of Waterloo & Hugh Williams, University of Calgary
- **Co-investigators:**
Mark Bauer, University of Calgary, Guang Gong, University of Waterloo, Michael Jacobsen, University of Calgary, Renate Scheidler, University of Calgary, Edlyn Teske, University of Waterloo, Scott Vanstone, University of Waterloo
- **Non-NCE partners:**
Certicom Corp., Communications Security Establishment, iCore, Microsoft Canada

Research

- Mechanisms for providing privacy that do not interfere with the legitimate duties of law enforcement agencies.
- Foster the research of privacy-enhancing policy and technologies and to study fundamental mathematical tools used in cryptography.
- Efficient methods were also developed for implementing cryptographic protocols based on sophisticated mathematical methods.

Quantum Information Processing



Quantum Information Processing

- **Project Leader:** Barry Sanders, University of Calgary
- **Co-investigators:**
Andris Ambainis, U of Waterloo, Richard Cleve, U of Waterloo, Claude Crpeau, McGill University, Joseph Emerson, U of Waterloo, Patrick Hayden, McGill University, Peter Hoyer, U of Calgary, Raymond Laflamme, U of Waterloo, Debbie Leung, U of Waterloo, Hoi-Kwong Lo, U of Toronto, Michele Mosca, U of Waterloo, Ashwin Nayak, U of Waterloo, Alain Tapp, U de Montreal, John Watrous, U of Calgary
- **Non-NCE partners:**
Alberta Informatics Circle of Research Excellence, Canadian Institute for Advanced Research, CSE, General Dynamics Canada, U.S. Army Research Office

Research

- **Quantum Cryptography:** Develop novel systems and techniques for information processing, transmission and security by exploiting the properties of quantum mechanical operations.
- **Zero-knowledge:** A zero-knowledge proof system is an interactive method for one party to prove to another that some mathematical statement is true, without revealing anything other than the veracity of the statement.
- An application of this system, for example, is to implement a cryptographic system in which two people can interact, and one comes away convinced of the other person's identity, but nothing more and therefore cannot steal their identity.

Understanding and Mitigating Malicious Activity in Networked Computer Systems



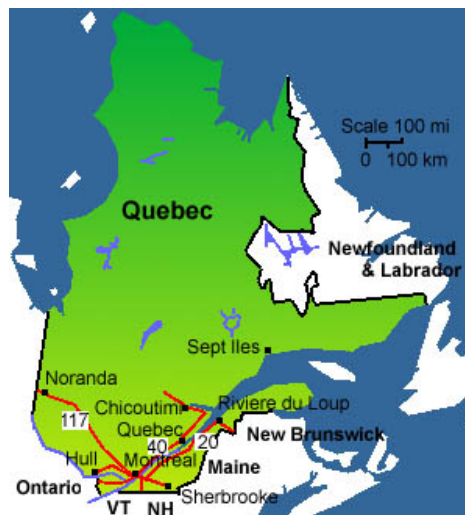
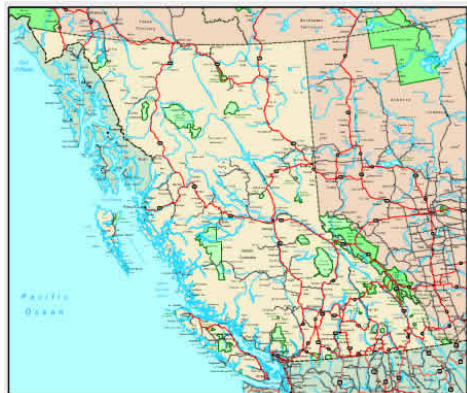
Understanding and Mitigating Malicious Activity in Networked Computer Systems

- **Project Leader:** Paul C. Van Oorschot, Carleton University
- **Co-investigators:**
Marsha Chechik, University of Toronto, Scott Knight, Royal Military College of Canada, David Lie, University of Toronto, Anil Somayaji, Carleton University, Mohammad Zulkernine, Queen's University
- **Non-NCE partners:**
Bell University Labs, Alcatel-Lucent, Cloakware, Communications Security Establishment, IBM Centres for Advanced Studies

Research

- Spyware, viruses, worms, denial-of-service attacks and phishing are some of the problems facing individuals, government and businesses.
- Developed techniques to improve the security of instant messaging networks to prevent the spread of malicious software via these popular on-line chat tools.
- Advancements in improving techniques for detecting attacks on web servers and general applications: methods, based upon both application-level (HTTP request) and operating system-level monitoring, have broader attack detection capabilities and fewer false positives than other proposed methods.

Decentralized Processing in Camera Networks



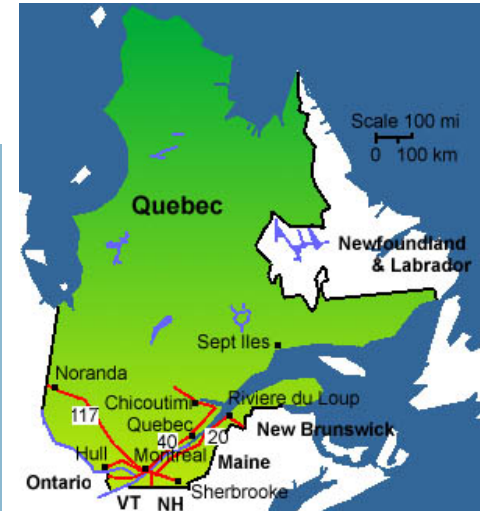
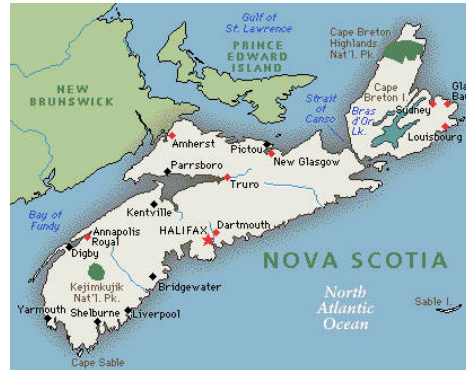
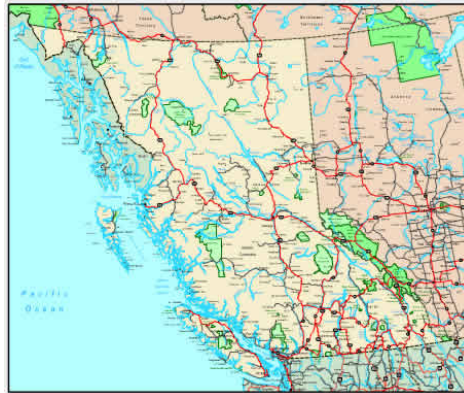
Decentralized Processing in Camera Networks

- **Project Leader:** Mark Coates, McGill University
- **Co-investigators:**
Nando de Freitas, University of British Columbia, Arnaud Doucet, University of British Columbia, Frank Ferrie, McGill University
- **Non-NCE partners:**
CAE, MacDonald Dettwiler & Associates Ltd.

Research

- Securing critical infrastructure and ensuring safety in public areas has motivated the recent widespread deployment of networks of cameras.
- In a network with hundreds of cameras, which camera views should be presented to the sole human operator?
- The decision of what camera views (or sequence of camera views) to present to the operator should be automatic, optimal and take into consideration all of the involved risks.
- Develop mathematical models and algorithms to attack this complex problem.

Gondwana: Towards Quantitative Security Metrics



Gondwana: Towards Quantitative Security Metrics

- **Project Leader:** John McHugh, Dalhousie University
- **Co-investigators:**
William A. Aiello, University of British Columbia, Jos Fernandez, Simon Fraser University, Sudhakar Ganti, University of Victoria, Michael McAllister, Dalhousie University, Michael L. McGuire, University of Victoria, Stephen Neville, University of Victoria, Alejandro Quintero, Ecole Polytechnique de Montreal, Jean-Marc Robert, Ecole de technologie superieure, Nur Zincir-Heywood, Dalhousie University
- **Non-NCE partners:**
Bell University Labs, Communications Security Establishment, ESET

Research

- IT networks and systems are at the core of modern societies whether this is from either the direct economic reliance or social safety perspectives.
- Defending against malicious activities targeted against these systems is the main thrust of computer security research and practice.
- Provide a basis for measuring how well these defensive measures work and to develop measurement techniques that can be validated in practice.

More

- CSE (Communication Security Establishment)
- NRC (National Research Council)
- CRC (Communication Research Council)
- DND (Department of National Defense)
- NSERC (Natural Sciences and Engineering Research Council)
- Other Universities