IEEE Ottawa Section

The IEEE Ottawa Communications Society, Broadcast Technology Society, and Consumer Electronics Society (ComSoc / BTS / CES) Joint Chapter, IEEE Ottawa Signal Processing Society, Oceanic Engineering Society, and Geoscience and Remote Sensing Society (SP / OE / GRS) Joint Chapter, Antennas and Propagation Society and Microwave Theory & Techniques Society (AP / MTT) Joint Chapter, IEEE Photonics Society (PHO) Ottawa Chapter, IEEE Ottawa Computer Society (CS), and IEEE Ottawa Section (OS), are inviting all interested IEEE members and other engineers, technologists, and students to the following two technical seminars workshop:

1- Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks
2- Waveguide (Fiber)-based Ultrafast All-optical Signal Processors for Apps in Computing, Telecom & Measurement

DATE: Monday, September 12, 2011.
TIME: 12:00 pm – 2:00 pm Seminar: 12:00 pm – 1:30 pm Discussion, Refreshments and Networking: 1:30 pm – 2:00 pm
PLACE: University of Ottawa, School of Electrical Engineering and Computer Science, SITE Building, Room 5084 (Boarding Room), 800 King Edward Avenue, Ottawa, Ontario, Canada.
ADMISSION: Free. Registration required. To ensure a seat, please register by e-mail contacting: Qingsheng Zeng (qingsheng.zeng@crc.gc.ca) or Wahab Almuhtadi (almuhtadi@ieee.org).

1) Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks

by
Dr. Prof. Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada

Abstract

The A primary security challenge in mobile ad hoc networks (MANETs) is the likelihood of node compromises caused by weak physical protection and hostile environments. As a result, key revocation is essential. In this talk, I will present our recent results on key revocation problems in MANETs. I will introduce some novel methods for the design of fully self-organized key revocation schemes for MANETs, which can be directly used in any pairing-based identity based cryptography (IBC) scheme, are adaptable to certificate revocation schemes in public-key infrastructure (PKI) solutions, and secret key-based schemes in MANETs as well.
In the first scenario, the nodes monitor their neighbors, securely propagate their observations, and revoke keys once designed threshold accusations have been received. The solution is very efficient, completely thwart many attacks (including Sybil, impersonation and replay attacks as well as other attacks by insiders and outsiders) and is resilient to advanced attacks by colluding nodes and roaming adversaries.
In the second scenario, the statistical Dirichlet multinomial model is introduced to key revocation processes. Each node keeps track of three categories of behavior, i.e., good, suspicious and malicious behavior, which is defined and classified by an external trusted authority, and updates its knowledge about other nodes' behavior using 3-dimension Dirichlet distribution. It is worth to point it out that those methods have been extended to secure fully distribute peer-to-peer (P2P) network systems.

Speaker's Bio

Guang Gong received a B.S. degree in mathematics in 1981, a M.S. degree in applied mathematics in 1985, and a Ph.D. degree in electrical engineering in 1990, from universities in China. She received a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, Rome, Italy, and spent the following year there. After return from Italy, she was promoted to an Associate Professor at the University of Electrical Science and Technology of China. During 1995-1998, she had worked with several internationally recognized outstanding coding experts and cryptographers including Dr. Solomon W. Golomb at the University of Southern California, Los Angeles. She joined University of Waterloo, Ontario, Canada, in 1998, an Associate Professor at the Department of Electrical and Computer Engineering in September 2000. She is a full Professor since 2004. Her research interests are in the areas of signal processing for wireless communications, communication and network security, and lightweight cryptography. She has authored or co-authored more than 200 technical papers and one book, co-authored with Dr. Golomb, entitled as Signal Design for Good Correlation -- for Wireless Communication, Cryptography and Radar, published by Cambridge Press in 2005. She serves/served as Associate Editors for several journals including an Associate Editor for Sequences for IEEE Transactions on Information Theory, and served on a number of technical program committees of conferences. Dr. Gong has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, Outstanding Doctorate Faculty Award of Sichuan Province, China, in 1991 and the Premier's Research Excellence Award, Ontario, Canada, in 2001, and NSERC Discovery Accelerator Supplement Award, 2009, Canada.

2) Waveguide (Fiber)-based Ultrafast All-optical Signal Processors for Applications in Computing, Telecommunication and Measurement

by

Dr. Prof. José Azaña

Institut National de la Recherche Scientifique - Centre Energie, Matériaux et Télécommunications (INRS-EMT)

University of Québec, Montréal, Québec, Canada

Abstract

This talk will review recent work on the development of fundamental signal processors operating on ultrafast optical signals, in particular all-optical temporal differentiators and integrators, implemented in fiber-optics or integrated-waveguide technologies. Applications in computing (e.g. differential equation solving), telecommunication (e.g. pulse shaping, optical switching), and measurement (e.g. temporal phase reconstruction) will be also briefly discussed.

Speaker's Bio

José Azaña received the Telecommunication Engineer degree (six years engineering program) and Ph.D. degree in telecommunication engineering from the Universidad Politécnica de Madrid (UPM), Spain, in 1997 and 2001, respectively. He completed part of his PhD research at University of Toronto, ON, Canada (1999) and University of California, Davis, CA, USA (2000). Following some postdoctoral research at McGill University (2001-2003), he was appointed as an Assistant Professor at the Institut National de la Recherche Scientifique - Centre Energie, Matériaux et Télécommunications (INRS-EMT) in Montreal, where he is presently a Full Professor. His research interests cover a wide range of topics, including all-fiber grating technologies, ultrafast photonic signal processing, optical pulse shaping, fiber-optic telecommunications, all-optical computing, measurement of ultrafast events, light pulse interferometry and microwave waveform generation and manipulation. He has to his credit more than 260 publications in top scientific journals and leading technical conferences, including more than 130 publications in high-impact peer-review journals, and many invited review journal papers and invited presentations in international meetings. Some of his published works have been very highly cited by his peers. Prof. Azaña is a member of IEEE and OSA. He has served as a Guest Editor of two monographs devoted to the area of Optical Signal Processing, published by EURASIP J. Appl. Signal Proc. (2005) and J. of Lightwave Technol. (2006). He has been recognized with a number of prestigious research awards and distinctions, including the XXII national prize for the best doctoral thesis in data networks from the Association of Telecommunication Engineers of Spain (2002), the extraordinary prize for the best doctoral thesis from his former university, UPM (2003), the 2008 IEEE-Photonics Society (formerly LEOS) Young Investigator Award, and the 2009 IEEE-MTT Society Microwave Prize.

CONTACT: To ensure a seat, please register by e-mail contacting:
Qingsheng Zeng (qingsheng.zeng@crc.gc.ca) or Wahab Almuhtadi (almuhtadi@ieee.org).