CALL FOR PAPERS
Wiley’s Security and Communication Networks Journal Special Issue on Security and Privacy Preservation in Vehicular Communications

Aims & Goals
The advancement and wide deployment of wireless communication technologies have revolutionized human's lifestyles by providing the best convenience and flexibility ever in accessing the Internet services and various types of personal communication applications. Recently, car manufacturers and telecommunication industries gear up to equip each car with the latest technologies. The main vision is safety and commercial applications, enabled by short to medium range communication systems and/or networks (vehicle-vehicle or vehicle-roadside). In spite of the numerous value-added application scenarios, the VANETs (Vehicular Ad-hoc NETworks) come with their own set of challenges, especially in the aspects of security and privacy preservation. It is obvious that any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to the other users. In addition, the issues on VANET security become more challenging due to the unique features of such network scenarios, including the high-speed mobility/large amount of network entities (i.e., the vehicles). Furthermore, conditional privacy preservation must be achieved in the sense that the user related privacy information, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in the event of a traffic dispute, such as a crime/car accident scene investigation. Therefore, it is critical to develop a suite of elaborated and carefully designed security mechanisms for achieving security, conditional privacy preservation, and efficient IVC authentication in a VANET before it can be practically launched.

Scope of Contributions
Motivated by the above observations, this special issue is organized to accommodate the most state-of-the-art proposals and research studies on achieving secure and privacy-preserving vehicular communications. In particular, the research papers of the following topics (but not limited to) are highly solicited:

- Security features in Intelligent Transportation Systems (ITS)
- New/existing communication protocol/technology architecture for VANETs
- Location privacy preservation/ secure positioning
- Security in Vehicular Sensor Networks (VSNs)
- Power adjustment and topology control in VANETs
- Authentication and key management for Inter-Vehicle Communications (IVCs)
- Security trust model and threat models for VANETs
- Secure network middleware and protocol design for VANETs
- Commercial and industrial security services in VANETs
- VANETs on Electronic Toll Collection (ETC) systems
- Anomaly detection and compromised node revocation in VANETs
Submission
Only original and unpublished research papers will be considered in this special issue. All submissions will be reviewed based on technical merit and relevance. Guidelines for prospective authors can be found on-line at http://www.interscience.wiley.com/journal/security. Prospective authors should submit their paper online at http://mc.manuscriptcentral.com/scn. When submitting the papers, the authors should make sure to choose the Manuscript type as “Special Issue”, enter the “Running Head” and the “Special Issue title” as “SCN-SI-004” and “VANET Security”, respectively.

Important Dates
Manuscript Due January 1, 2008
Acceptance Notification March 1, 2008
Final Manuscript Due April 1, 2008
Publication June 2008

Guest Editors
Dr. Pin-Han Ho (pinhan@bcr.uwaterloo.ca)
Department of Electrical and Computer Engineering
University of Waterloo
Canada

Dr. Zonghua Zhang (zonghua.zhang@inria.fr)
IRCICA/LIFL - CNRS UMR 8022 - INRIA Futurs
France

Dr. Rongxing Lu (rxlu@bcr.uwaterloo.ca)
Department of Electrical and Computer Engineering
University of Waterloo
Canada