Special Issue on Security and Privacy in Communication Systems and Networks

Guest Editorial

The rapid advancement of communications and networking technologies has revolutionized human's lifestyles by providing the best convenience and flexibility ever in accessing the Internet services and various types of personal communication applications. For instance, with the emerging wireless communication technologies, healthcare industry now is offering high-quality services to patients at low costs through a variety of applications. It can provide the right care to patients with different needs and patients can be treated in alternative, more cost-effective settings, for example, patients' homes or workplaces, instead of in traditional costly hospital settings. This is because these wireless-equipped healthcare systems enable remote and continuous monitoring of patients' health status in both residential settings and outdoor settings, where patients feel more comfortable and their activities are less restricted.

As always, while we experience tremendous benefits from adopting the new technologies, i.e., latest communication and networking technologies, and at the same time, we also face many challenges especially with respect to security and privacy issues. This is made worse by the fact that modern technology may have provided increased comfort and convenience in our daily lives but at the expense of privacy. This special issue consists of six papers addressing the security and privacy issues in communication systems and networks such as vehicular communication systems, delay tolerant networking and wireless mesh networks.

Recently, vehicular communication networking has emerged as a promising approach for facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. However, the attractive features of VANET inevitably incur higher risks for abuse if privacy and security have not yet been addressed before the widely deployment of such networks. It would jeopardize the public safety and become the main barrier to the acceptance of such a new technology. The first paper aims to address the important security and privacy issues in VANETs. In the first paper, "Prioritized WAVE-based Parking Assistance with Security and User Anonymity", an elliptic curve based secure application for parking assistance to WAVE-enabled vehicles is presented by S. Biswas and J. Misic. In this work, vehicles and infrastructure use separate access categories to exchange parking assistance application messages. The authentication mechanism uses a vehicle's current location information as the "identity" to generate the signature so that the user remains anonymous.

The second paper entitled "Designing P2P Networks Tolerant to Attacks and Faults based on Bimodal Degree Distribution" by K. Suto, H. Nishiyama, S. Shen, and N. Kato, addresses the stability and communication efficiency of P2P networks, and proposes a novel method to construct P2P networks based on the bimodal degree distribution, to achieve high stability and communication efficiency.

The third paper entitled "Mitigating Eavesdropping Attack Using Secure Key Management Scheme in Wireless Mesh Networks" by F. Kandah, Y. Singh and W. Zhang, presents an effective secure key management scheme (SKeMS) seeking an encryption key assignment, such that the induced network is securely key connected and well protected against potential malicious eavesdropping attacks. SKeMS, by assigning the available encryption keys among all nodes in the network considering the 2-hop eavesdropping ability, provides a more secured network against malicious eavesdropping attack compared to that using previous key assignment schemes.

In the fourth paper, "Privacy Support in People-centric Sensing", an approach to support privacy in people-centric sensing is proposed by L. Becchetti, L. Filipponi and A. Vitaletti. The technique allows user-assisted coverage of a given area of interest without disclosing user geographical information. The results of extensive experimental analysis on public data from real applications are presented, supporting the effectiveness and accuracy of the proposed technique.

The fifth paper entitled "A Secure Message Transaction Protocol for Delay Tolerant Networks" by Z. Jia, L. Li, Z. Yu, S. Li and Y. Yang, deals with the security and path recording of DTN message delivery and presents a payment mechanism, which makes the participants have no incentive to launch the collusion attacks in the path disclosure.

In the last paper, "Trust-based Mutual Authentication for Bootstrapping in 6LoWPAN", H. Yu and J. He aim at secure bootstrapping in 6LoWPAN by establishing pairwise keys between neighboring nodes as well as trust paths from nodes to the base station. Pairwise keys that are established using mutual authentication based on pairing requires the storage of only one key along with the exchange of IDs. A trust path is established based on trust evaluation that uses multiple criteria to balance the whole network. Quantitative analysis shows that although the proposed scheme is a little higher in energy consumption than protocols that are based on Elliptic curve cryptography (ECC), the storage requirement for each node is much lower than those protocols and that the trust evaluation mechanism can balance the whole network to prolong the life of the network.

In closing, we would like to thank all the authors who have submitted their research work to this special issue. We would also like to acknowledge the contribution of many experts in the field who have participated in the review process and provided helpful suggestions to the authors on improving the content and presentation of the papers. We would also like to express our gratitude to the Editor-in-Chief, Dr. Haohong Wang, and Associate Editor-in-Chief, Prof. Song Ci, for their support and help in bringing forward this special issue. We hope you will enjoy the papers in the special issue.

Guest Editors

Xiaodong Lin, University of Ontario Institute of Technology, Canada
E-mail: xiaodong.lin@uoit.ca

Joel José P. C. Rodrigues, Institute of Telecommunications, University of Beira Interior, Portugal
E-mail: joeljr@ieee.org

Xu Li, INRIA Lille – Nord Europe, France
E-mail: xu.li@inria.fr

Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology (UOIT), Oshawa, ON, Canada. His research interests include wireless network security, computer forensics, software security, and applied cryptography. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), the 3rd International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2010), and IEEE International Conference on communications (ICC 2007). He is a senior member of IEEE.

Joel José P. C. Rodrigues is a professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in informatics engineering, an MSc degree from the University of Beira Interior, and a five-year BSc degree (licentiate) in informatics engineering from the University of Coimbra, Portugal. His main research interests include sensor networks, e-health, e-learning, vehicular delay-tolerant networks, and mobile and ubiquitous computing. He is the leader of NetGNA Research Group (http://netgna.it.ubi.pt), the Vice-chair of the IEEE ComSoc Technical Committee on Communications Software, the Vice-Chair of the IEEE ComSoc Technical Committee on eHealth, and Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the editor-in-chief of the International Journal on E-Health and Medical Communications, the editor-in-chief of the Recent Patents on Telecommunications, and editorial board member of several journals. He has been general chair and TPC Chair of many international conferences. He is a member of many international TPCs and participated in several international conferences organization. He has authored or coauthored over 200 papers in refereed international journals and conferences, a book, and 2 patents. He had been awarded the Outstanding Leadership Award of IEEE GLOBECOM 2010 as CSSMA Symposium Co-Chair and several best papers awards. Prof. Rodrigues is a licensed professional engineer (as senior member), member of the Internet Society, an IARIA fellow, and a senior member of ACM and IEEE.
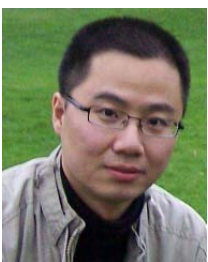
Xu Li is a research scientist (with tenure) at the French National Institute for Research in Computer Science and Control (Inria). He received a PhD (2008) degree from Carleton University, Canada, an MSc (2005) degree from the University of Ottawa, Canada, and a BSc (1998) degree from Jilin University, China, all in computer science. During 2004.1-8, he held a visiting researcher position at the National Research Council Canada (NRC). From 1998 to 2002, he spent four years in industry developing network security products as R&D team leader. He has published more than 60 refereed papers in the areas of machine-to-machine communications and mobile social networks. He is on the editorial boards of the European Transactions on Telecommunications, Ad Hoc & Sensor Wireless Networks, and Parallel and Distributed computing and Networks. He regularly organizes journal special issues as guest editor, for example, recently at International Journal of Parallel, Emergent, and Distributed Systems, Computer Communications, Peer-to-Peer Networking and Applications, and Ad Hoc & Sensor Wireless Networks. He is/was among the TPC and/or organizing committees of many major international conferences, for example, recently, IEEE MASS, DCOSS, IPCCC, LCN, etc. He was a recipient of the NSERC PDF awards and a number of other awards.