Editorial

Daojing He*

College of Computer Science,
Zhejiang University,
China
E-mail: hedaojing@zju.edu.cn

Maode Ma

School of Electrical and Electronic Engineering,
Nanyang Technological University,
Singapore
E-mail: Maode_Ma@pmail.ntu.edu.sg

Sammy Chan

Department of Electronic Engineering,
City University of Hong Kong, SAR,
Hong Kong
E-mail: eeschan@cityu.edu.hk

Biographical notes: Daojing He is currently a PhD candidate in Zhejiang University, China. He received his BEng and MEng degrees in Computer Science from Harbin Institute of Technology in 2007 and 2009, respectively. His research interests include wireless networking, network security and privacy. As the first author, he has published more than ten research papers in prestigious journals and conferences such as *IEEE Transactions on Wireless Communications (IEEE TWC)*, *IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS)* and *Elsevier Computer Communications Journal*. He has served on the technical programs for some flagship conferences including IEEE Globecom 2011 and IEEE PIMRC 2011.

Maode Ma received his PhD in Computer Science from Hong Kong University of Science and Technology in 1999. He is an Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has published about 200 international academic research papers on wireless networks. He has been a member of the technical programme committee for more than 100 international conferences. He has been a technical track chair, tutorial chair, publication chair and session chair for more than 50 international conferences. Currently, he serves as an Associate Editor for *IEEE Communications Letters*, an Editor for *IEEE Communications Surveys and Tutorials*, an Associate Editor for *Int. J. Wireless Communications and Mobile Computing* and an Associate Editor for *Int. J. Security and Communication Networks*.

Sammy Chan received his BE and MEng Sci degrees in Electrical Engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a PhD degree in Communication Engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994, he was with Telecom Australia Research Laboratories, first as a Research Engineer, and then between 1992 and 1994 as a Senior Research Engineer and a Project Leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an Associate Professor.

Recent advances in electronics and wireless communication technologies have enabled the extensive deployment of wireless sensor networks (WSNs). These networks have applications in many important areas, such as military, healthcare, environment monitoring and manufacturing. Security and privacy are critical issues to many sensor network applications including military target tracking and healthcare monitoring. To provide security and privacy to the sensor networks with these applications is challenging, due to the open nature of wireless communications and the limited capabilities of sensor nodes in terms of processing power, storage, bandwidth and energy. Additionally, widespread and unrestricted deployment of WSNs makes them exposed to a number of security vulnerabilities. Moreover, a number of trust and reputation issues arise in WSNs since trust communication is a fundamental consideration for the operation and the stability of WSNs. An example is that a trust management frame in WSNs can be utilised to prevent nodes from performing malicious or selfish behaviours.

This special issue brings together three papers on diverse topics in the area of trust, reputation, security and privacy of WSNs.

- The contribution ‘An efficient reputation-based system for wireless ad hoc networks’ by Gang Peng et al., copes with malicious behaviours using a decentralised reputation system. Each source node actively triggers the detection process to collect evidence towards malicious behaviours. Based on available evidences, each node relies on Bayesian inference to internally update its reputation beliefs about how reliable each other node is. Moreover, a flocking algorithm is proposed to allow careful dissemination of reputation information and thus shorten the misbehaviour detection time.
- The contribution by Kavitha Ammayappan et al. titled ‘New route discovery design for routing misbehaviour prevention in multi-hop wireless sensor networks’ presents a new route discovery design for multi-hop WSNs which prevents routing misbehaviours and establishes non-plausible route. It uses the proposed limited broadcasting communication to mitigate network wide flooding and incorporates end-to-end mutual authentication and key agreement to secure the route establishment process. The feasibility of the proposed routing approach and its resilience to various attacks are presented through simulations.
- The contribution by Jacques M. Bahi et al. proposes two layers for secure data aggregation in sensor networks. Firstly, an end-to-end encryption scheme is studied which is based on elliptic curve cryptography and supports operations over cypher-text. Secondly, to enhance the security a new watermarking-based authentication is proposed, which enables sensor nodes to ensure the identity of other nodes they are communicating with. The experimental results show that this

hybrid approach guarantees high security level for data aggregation in sensor networks and significantly reduces computation and communication overhead.

While concluding, we thank the Editor-in-Chief, Prof. Thanos Vasilakos, for his guidance, the reviewers for their insightful comments that help to enhance the quality of the papers, and the authors for their academic contributions and the great work they have done.