
Editorial

Ming-Hour Yang

Department of Information and Computer Engineering,
Chung Yuan Christian University, Taiwan
E-mail: mhyang@cycu.edu.tw

Jonathan C.L. Liu

Department of Computer and Information Science and Engineering,
University of Florida, USA
E-mail: jclius@cise.ufl.edu

Yu-Chee Tseng

Department of Computer Science,
National Chiao Tung University, Taiwan
E-mail: yctseng@cs.nctu.edu.tw

Biographical notes: Ming-Hour Yang received his MS Degree in Electronic Engineering from the Chung-Hua University, Taiwan, in 1996, and his PhD Degree in Computer Science and Information Engineering from the National Central University, Taiwan, in 2001. He was a Research Fellow of National Strategic Studies Institute at National Defence University. Now, he is currently an Assistant Professor at the Department of Information and Computer Engineering, Chung Yuan Christian University. His interests include video on demand, parallel and distributed computing, fault tolerance, mobile computing, security, and wireless network.

Jonathan C.L. Liu received his MS and PhD Degrees in Computer Science from the University of Alabama and the University of Minnesota respectively. Since 1999, he has joined the CISE Faculty at the University of Florida and now is a tenured Associate Professor. His research interests include high-speed wired and wireless networks, multimedia communications, parallel processing and artificial intelligence. He has published over 80 technical papers including 32 journal papers in the above areas. He was awarded the National Science Foundation CAREER Award and is now a senior member of IEEE and a professional member of ACM.

Yu-Chee Tseng received his PhD in Computer and Information Science from the Ohio State University. He joined National Chiao-Tung University, Taiwan, as Professor since 2000 and is now Associate Dean since 2007. He received Best Paper Award, International; Conference on Parallel Processing, 2003, Elite I.T. Award, and Distinguished Alumnus Award by the Ohio State University, 2005. His research interests include mobile computing, wireless communication, and parallel and distributed computing. He served/serves on the editorial boards of *IEEE Trans. on Vehicular Technology*, *IEEE Trans. on Mobile Computing*, and *IEEE Trans. on Parallel and Distributed Systems*.

Sensors and sensor networks have got a lot of research interest because of their potentials in providing diverse services to pervasive computing applications, not only on science and engineering, but also equally important on issues related to critical infrastructure protection, security, health care, environment protection, energy, etc. The ad-hoc networking technology has also enabled sensor nodes to connect with each other via wireless communications in a much easier way. The flexibility of installing and configuring a sensor network is thus greatly improved.

Communications in wireless sensor networks are resource-constrained, in terms of sensor nodes' processing power, bandwidth communication, storage space and energy. This gives rise to new challenges in system

and network security in wireless sensor networks. The underlying communication medium for wireless networks provides serious exposure to attacks against wireless networks. Wireless sensor networks usually cannot depend on traditional infrastructure found in enterprise environments such as dependable power sources, high bandwidth, and continuous connectivity. Without adequate security, enterprises will not be able to profit from the use of wireless sensor networks, defence organisations might be unable to guarantee the safety of their personnel, and wireless sensor networks will remain on the drawing board even if the other problems associated with them are solved. Security-related issues still remain challenging issues for wireless sensor networks.

This special issue includes seven accepted papers. These papers can be divided into two categories: system security and network security. In the system security category, Malliga and Tamilarasi proposes a backpressure technique to push DDoS attack traffics back to the attacker. Huang and Shieh develop a secret search mechanism to search cipher data in wireless sensor networks. In the network security category, Hsiao and Hwang propose an efficient data dissemination scheme to allow the sink node to collect data in a wireless sensor network correctly. Based on the Bloom filter, Xu et al. develop a secure DSR protocol. Tsai et al. propose a secure peer-to-peer transmission protocol for wireless networks to guarantee

the integrity of data during transmission. Yang proposes a lightweight authentication protocol for mobile RFID networks that complies with EPC Class-1 Gen-2 norms, which effectively achieves forward security. Wang and Smith develop a secure video transportation scheme incorporating with a watermark method to protect video contents.

These papers represent an exciting, insightful observation into the state of the art, as well as emerging future topics, for future wireless sensor networks. We thank reviewers who spent time and efforts reviewing manuscripts for this special issue and the Editor-in-Chief for great support to make this special issue possible.