Editorial

Abhishek Parakh

Nebraska University Center for Information Assurance,
University of Nebraska at Omaha,
Omaha, NE 68182, USA
Email: aparakh@unomaha.edu

Kewei Sha

School of Science and Computer Engineering,
University of Houston – Clear Lake,
2700 Bay Area Blvd,
Houston, TX 77058, USA
Email: comersha@gmail.com

Biographical notes: Abhishek Parakh is an Assistant Professor of Information Assurance at the College of Information Science and Technology at University of Nebraska, Omaha. He received his PhD in Computer Science from Oklahoma State University. He is also a member of Nebraska University Center for Information Assurance, a National Security Agency (NSA) designated Center for Academic Excellence in Information Assurance Education – Cyber Defense (CAE-CD). His research interests include cryptographic engineering, distributed systems security, resource constrained encryption systems, protocol development, quantum cryptography and SCADA systems security. He has over 40 publications and has been funded by NSF and NASA.

Kewei Sha is an Assistant Professor in Computer Science at University of Houston, Clear Lake (UHCL). Before he moved to UHCL, he was the Department Chair and Associate Professor in the Department of Software Engineering at Oklahoma City University. He received PhD in Computer Science from Wayne State University in 2008. His research interests include sensor networks, cyber-physical systems and mobile computing, and network security and privacy. He has served as the Secretary of Technical Committee on the Internet of the IEEE Computer Society (IEEE-CS TCI), a guest Editor at Wireless Personal Communications and International Journal of Security and Networks, a conference technical program committee chair for ICCCN 2015, a workshop general chair for ICCCN 2013, a workshop co-chair of MobiPST 2011, 2012 and 2014, a session chair in ICCCN and CollaborateCom, a member of editorial board in several journals, and a program committee member in numerous conferences. He is also a reviewer for numerous journals including *IEEE TPDS*, *IEEE TC*, *ACM TAAS*, *IEEE TDSC*, *IEEE TITS*, *Elsevier JPDC* and so on.

The pervasive nature of mobile and wireless systems in the form of wireless sensors, smart tags, RFIDs, tablets, smart phones and other wearable computing devices has led to significant and renewed interest in the issues of privacy, security and trust of data stored on these devices. Further the integration of cloud technology is only making the access to this data easier and more prevalent across various platforms thereby increasing the attack surface. At the same time the development of mobile applications (or apps as they are called) has significantly changed the way people manage their daily lives through mobile payment technology, social networking applications and keep informed about everyday events.

This special issue on *Privacy, Security and Trust for Mobile and Wireless Systems* includes eight high quality papers ranging in topics from quantum cryptography to group-key distribution techniques in social networks and intrusion detection systems in wireless body area networks. Some of the papers are extended versions of selected papers presented at the *4th International Workshop on Privacy, Security and Trust in Mobile and Wireless Systems (MobiPST 2014)* which was held in conjunction with the *23rd International Conference on Computer Communications and Networks (ICCCN 2014)*, Shanghai, China. Other papers, however, were received through an open call for papers for the special issue. Short synopses of papers included in this special issue are discussed below.

Subudhi and Panigrahi address the problem of detecting fraudulent phone calls in mobile phones by analysing the user calling behaviour. Their detection algorithm uses support vector machine (SVM) along with fuzzy clustering for detecting fraudulent usage of mobile phone. Their experiments show promising results in terms of finding fraudulent calls without raising excessive false alarms. Further comparative studies are carried out on the proposed system by applying different types of SVMs along with

various fuzzy clustering techniques for analysing the performance of the system.

Liu et al. discuss a solution to group-key distribution in online social networks for secure communication. Their proposed algorithm allows for newly added members to recover the historical session keys and when compared with other conventional public-key approaches the proposed algorithm only uses polynomial interpolation which makes it lighter in weight, more efficient, scalable and practical. Experimental performance data is presented.

Two papers focus on quantum cryptographic approach to key distribution. Nomula et al. discuss the issues behind integrating conventional quantum key distribution protocols in wireless networks and standards. Specifically they discuss the multi-photon tolerant quantum key distribution and its integration into IEEE 802.11, WiMAX and LTE wireless networks. In addition, their paper also proposes a multi-agent software approach for this implementation. In the second paper on quantum cryptography, Parakh et al. discuss a new probabilistic technique to increase the efficiency of entanglement based key exchange. Furthermore, the increase in efficiency is achieved simply by changing the ratio of qubits that are measured in random bases and requires no adjustments to the quantum mechanical equipment.

In another interesting paper Dadhich et al. talk about detecting slanders in peer-to-peer decentralised electronic communities. The proposed model derives final reputation by combining direct and indirect trust for destination host with which agent wants to do a transaction. The paper detects recommenders called slanders who give an unfair recommendation for the destination host in a peer-to-peer system. Their model obtains 80% accuracy in final reputation score of destination host before slandering and 50% accuracy after slandering of recommenders showing that existence of slanders lowers the performance of the model than that actually obtained before slandering.

Chen et al. presents a threat monitoring system to monitor and detect threats in enterprise networks with mobile devices. The proposed system was implemented and the experimental data shows that the developed system can accurately and effectively detect malware on the Android platform with low system overhead in terms of energy and CPU usage.

Thamilasaru discusses the challenges of intrusion detection in wireless body area networks. Since information transmitted in these wireless body area networks (WBAN) often consists of critical and sensitive patient health and personal information, securing these networks is central to their practical deployment in healthcare applications. The objective of this research was to design and develop intelligent intrusion detection techniques to improve security in WBAN. In their work the authors proposed iDetect, a multi-objective genetic algorithm based intrusion detection system to provide optimal attack detection in these networks. The proposed algorithm guaranteed that only the features necessary for detecting a specific attack are used in the intrusion detection process, thereby decreasing the computational complexity.

Last but not least Annadurai and Yazhini talk about optimising trust value-based clustering using trust evaluation scheme for ad hoc network. Their proposed algorithm elects trustworthy cluster heads that can provide secure communication via cooperative nodes and takes the trust value of the node dynamically into consideration. In addition they factor nodes energy, mobility, distance to neighbours and have connectivity to elect that are trustworthy, stable and high-energy. Simulation results are presented as well.

With the above collection of papers we believe that the special issue brings together a number of very interesting research topics addressing many different facets of security, trust and privacy issues in mobile and wireless networks.