Preface

Al-Sakib Khan Pathan*

International Islamic University Malaysia,
Kuala Lumpur 53100, Malaysia
Email: sakib@iium.edu.my
Email: sakib.pathan@gmail.com
*Corresponding author

Xianglin Wei

Nanjing Telecommunication Technology Research Institute,
Nanjing 210007, China
Email: wei_xianglin@163.com

Homero Toral Cruz

University of Quintana Roo,
77019 Chetumal, Quintana Roo, Mexico
Email: homerotoralcruz@gmail.com

Luca Caviglione

Area della Ricerca di Genova (CNR-ISSIA),
Via de Marini 6, Genova16149, Italy
Email: luca.caviglione@ge.issia.cnr.it

Biographical notes: Al-Sakib Khan Pathan received his PhD in Computer Engineering in 2009 from Kyung Hee University, South Korea. He received his BSc in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. He is currently an Assistant Professor at Computer Science department in International Islamic University Malaysia, Malaysia. His research interest includes wireless sensor networks, network security, and e-services technologies. He has served as a Chair, organising committee member, and TPC member in numerous international conferences/workshops. He is also serving as an Editor of several renowned journals. He is a senior member of IEEE.

Xianglin Wei received his Bachelor's degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China in 2007, and PhD from PLA University of Science and Technology, Nanjing, China. He is currently working as a researcher at the Nanjing Telecommunication Technology Research Institute, China. His research interests include cloud computing, peer-to-peer networks, network anomaly detection, network measurement, and distributed system design and optimisation. He has served as editorial member of many international journals and TPC member of international conferences.

Homero Toral Cruz received his PhD and MS in Electrical Engineering, Telecommunication option, from CINVESTAV, Jalisco, Mexico in 2006 and 2010, respectively. He received his BSc in Electronic Engineering from Instituto Tecnológico de la Laguna, Coahuila, Mexico, in 2002. He is currently an Assistant Professor at Sciences and Engineering Department in University of Quintana Roo, Mexico. His research interest includes VoIP technologies, traffic modelling, and wireless sensor networks. He has served as the Guest Editor of some international journals and TPC member of several international conferences. He has been awarded a national recognition (SNI member) as a researcher by CONACYT.

Luca Caviglione is a researcher at the Institute of Intelligent Systems for Automation of the National Research Council of Italy. He holds a PhD in Electronic and Computer Engineering from the University of Genoa, Italy. His research interests include P2P systems, wireless communications, and network security. He is author/co-author of more than 90 academic publications, and several patents. He has been involved in research projects funded by the ESA, and the EU. Also, he is a Work Group Leader of the Italian IPv6 Task. From 2011, he is an Associate Editor for the *Transactions on Emerging Telecommunications Technologies*.

Owing to their popularity, file-sharing applications relying upon peer-to-peer (P2P) are still responsible for a vast amount of internet traffic. Besides, the diffusion of services for streaming multimedia has increased the impact of this paradigm. Therefore, applications such as BitTorrent and PPstream are being daily used to exchange a wide variety of digital resources, for instance, audio, video, games, music, and e-books. Unfortunately, mechanisms underlying P2P architectures could also make the system vulnerable to various kinds of security attacks and threats. Possible examples are:

1 malicious peers, which could refuse to contribute hence disrupting the cooperative flavour at the basis of P2P systems

2 distributed denial-of-service (DDoS) attack, or injection of useless data (commonly termed poisoning) taking advantage of the diffuse nature of the architecture

3 identity theft, collusion attack, and Sybil attack causing leak of sensitive data or transforming a service into a botnet.

As a consequence of hacking attempts (especially from high-profile attackers) that happen on a daily basis, unmonitored P2P file-sharing systems are threatened today with unparalleled magnitude. Sensitive information could easily be exposed, harvested, and distributed across multiple P2P networks, often with information of government or critical military facilities.

Researchers have already offered many techniques to mitigate security issues of P2P architecture. A common idea is to use reputation schemes or architectures using mutual certificates so as to isolate malicious nodes. Another idea, which has been probably inspired by the dramatic diffusion of online social networks, is called friend of friend. The key idea is that a friend could certify and support another friend (i.e., a peer, or a node in this case). However, this solution leaves many issues unanswered such as privacy issues, scalability of the network, handling of non-participating nodes, resource scarcity among the socially networked nodes, and so on. Besides these aforementioned examples, the existing literature is full of techniques based on intelligent and adaptive methods (i.e., artificial intelligence-based methods), fuzzy logic, and game theory, just to mention some.

In this perspective, the goal of this special issue is to provide a platform for the researchers and students to share their thoughts and findings on various security issues in P2P networks and systems. Nevertheless, we required works covering unexplored areas, or dealing with novel services or emerging trends (an archetypal example could be Bitcoin).

After rigorous review process, based on timeliness, merit, originality, and quality of presentation, we could accept only six papers for this issue. The titles are:

1 *Detection and mitigation of the eclipse attack in chord overlays*

2 *Traversing Bitcoin's P2P network: insights into the structure of a decentralised currency*

3 *Neighbourhood failures in covert communication network topologies*

4 *Distributed reputation management for service-oriented P2P enterprise communities*

5 *A traffic identification based on PSO-RBF neural network in P2P network*

6 *A fuzzy logic-based sustainable and trusted routing for P2P-enabled smart grid.*

As the review process ensured the appropriate quality of all these accepted papers, we hope that this issue will be very helpful for the researchers who are working on the relevant research areas.

We would like to give our sincere thanks to all the authors who submitted their papers (including those whose papers could not be accepted after the review process), to all the reviewers who volunteered in reviewing the papers, and last but not the least, to the Editor-in-Chief, Professor Kuan-Ching Li, for giving us the opportunity to organise this special issue for this journal.