Guest editorial

K. Chandra Sekaran*

Department of Management Studies,
Indian Institute of Technology Madras,
Chennai 600 036, India
E-mail: kchnitk@ieee.org
*Corresponding author

Sabu M. Thampi

Indian Institute of Information Technology and Management-Kerala,
Technopark Campus, Trivandrum-695581, Kerala, India
E-mail: smthampi@ieee.org

Biographical notes: K. Chandra Sekaran is currently serving as Professor of Computer Science and Engineering in the National Institute of Technology Karnataka, Mangalore, India. He has 24 years of teaching and research experience. He specialises in distributed computing, computer networks and software systems. He has authored two books and published more than 100 papers in reputed journals and conferences. He has organised several international and Indian national events such as ADCOM 2006, ADCOM 2007, BioAdcom 2010, and ICRATEMS 2011. He is serving in the editorial board of many international journals and is a senior member of many academic bodies such as IEEE, ACM, ACS, and CSI.

Sabu M. Thampi is an Associate Professor in the School of Computer Science and Information Technology, Indian Institute of Information Technology and Management-Kerala (IIITM-K), India. He has completed his PhD in Computer Engineering from National Institute of Technology Karnataka. He has more than 17 years of teaching and research experience in various institutions. His research interests include mobile agents, network security, bio-inspired computing, collaborative learning, semantic web and P2P networks. He has authored one book and published several papers in academic journals and international and national proceedings. He has served as a technical committee member for several international conferences and workshops. He is serving as reviewer and editorial board member of few journals. He is also serving as Editor-in-Chief of *International Journal of Trust Management in Computing and Communications* (*IJTMCC*), Inderscience Publishers. He is a member of IEEE, ACM, ACS etc...

Peer-to-peer (P2P) systems are decentralised, self-organising distributed systems that cooperate mainly to exchange data. A P2P network offers a scalable and fault-tolerant means of locating nodes anywhere on a network without maintaining a huge amount of routing state. This permits for a variety of applications beyond simple file sharing. Millions of users now participate in these systems and the user bases are diffusing broadly. P2P computing is perhaps the most significant development in computing since the emergence of the web. So far, the success of P2P paradigms has been primarily in traditional wired network environments. With the advance of modern wireless and mobile communications, there is a growing interest for mobile users to participate in P2P services anywhere, anytime through their mobile handheld devices. However, the open and anonymous nature of P2P network makes it an ideal medium for attackers to spread malicious content. As a result, widespread and unrestricted deployment of P2P systems exposed a number of security vulnerabilities. Furthermore, a number of trust and reputation issues occur in P2P networks as trust is a fundamental consideration for growth and stability of systems. Hence, making P2P systems more 'secure' is an important challenge. Innovations of P2P systems proffer many interesting avenues of research in a variety of areas in computing.

This special issue invited authors to submit their original work that addresses recent developments in P2P systems with special focus on trust, reputation and security issues. It includes eight regular papers and one invited paper.

The invited paper by Joseph Idziorek and Mark Tannian, 'Security analysis of public cloud computing', presents an initial checkpoint of the current state of cloud computing security research by providing a systematic analysis and survey of relevant literature. The authors conclude that without standards with respects to terms, functionality, protocols and interfaces, meaningful security research in cloud computing that is comprehensive will be difficult to conduct.

The paper by Naeem Al-Oudat and Govindarasu Manimaran, 'Task scheduling in heterogeneous distributed systems with security and QoS requirements', deals with the feasible allocation of precedence constrained-tasks to heterogeneous sites in a distributed security-sensitive system to maximise the objective value.

The paper by G. Khataniar and D. Goswami, 'A hierarchical approach to improve performance of unstructured peer-to-peer system', proposes a hierarchical overlay network architecture for unstructured P2P systems. Because of the way the nodes are organised improves the connectivity, reduces the number of unnecessary messages and increases the success rate. The query is forwarded to the higher capability nodes which regulates the new nodes coming to the system.

The paper by Bridge Q. Zhao and John C.S. Lui, 'Using contracts to induce cooperation in large scale P2P communication networks: algorithms, stability and applications', proposes a new paradigm of using contracts to promote cooperation in large scale networks. The paper also proposes both centralised and distributed algorithms to find and implement a stable and balanced contract with fairness and security constraints. The authors argue that contract-based mechanisms are robust against collusion.

The paper by Brent Lagesse, 'Analytical evaluation of P2P reputation systems', introduces several analytical metrics and a utility-based method for evaluating reputation mechanisms for P2P systems. Further, the paper provides a case study of an evaluation of the EigenTrust reputation mechanism to demonstrate the use of these metrics and methods.

The paper by Abdullatif Shikfa, Melek Önen and Refik Molva, 'Local key management in opportunistic networks', first analyses the security challenges regarding key management in the context of opportunistic networks and extract important requirements for key management in this context. Subsequently, the paper proposes a key management scheme that enables the bootstrapping of local, topology-dependent security associations between a node and its neighbours along with the discovery of the neighbourhood topology.

The paper by D. Doreen Hephzibah Miriam and K.S. Easwarakumar, ‘SPA-based task scheduling for hypercubic P2P grid systems’, proposes the set pair analysis (SPA)-based task scheduling methodology to enhance system performance in hypercubic P2P grid. The authors claim that the SPA-based scheduling minimises the makespan along with load balancing and guarantees the high system availability in system performance.

The paper by Manish Chaturvedi and Sanjay Srivastava, ‘On effectiveness of cooperation enforcement mechanisms in wireless ad hoc networks’, analyses routing overhead of dynamic source routing (DSR) and a representative set of cooperation enforcement mechanisms. The authors show that routing overhead of cooperation enforcement mechanisms is higher than that of DSR.

The paper by Sandeep K. Sood, Anil K. Sarje and Kuldip Singh, ‘SSO password-based multi-server authentication protocol’, presents single sign-on (SSO) password-based multi-server authentication protocol that issues the ticket to the user for a specific time period. The proposed protocol bridges the gap between single server and multi-server password-based authentication protocols and eliminates the main point of vulnerability as existing in most of the single-server password-based authentication protocols.

In closing, we would like to thank the authors for submitting their work to this special issue as well as the reviewers who, through their expert and insightful comments, helped improve significantly the quality of the submitted material. We would also like to thank the Editors-in-Chief Dr. Sudip Misra and Dr. Isaac Woungang for providing the opportunity to edit this special issue. We hope you find the materials in this special issue interesting and useful.