Editorial

Ciprian Dobre*

University Politehnica of Bucharest,
Splaiul Independenţei 313,
Bucureşti 060042, Romania
E-mail: ciprian.dobre@cs.pub.ro
*Corresponding author

Xiaofeng Chen

School of Telecommunications Engineering,
Xidian University,
266 Xinglong Section of Xifeng Road,
Xi'an, Shaanxi 710126, China
E-mail: xfchen@xidian.edu.cn

Biographical notes: Ciprian Dobre received his PhD in Computer Science at the University Politehnica of Bucharest in 2008. His main research interests are grid computing, monitoring and control of distributed systems, modelling and simulation, advanced networking architectures, and parallel and distributed algorithms. He is a member of the RoGrid consortium and is involved in a number of national projects and international projects. His research activities were awarded with the Innovations in Networking Award for Experimental Applications in 2008 by the Corporation for Education Network Initiatives (CENIC). He has published in leading international journals and conferences and has served in the organising committees of many conferences and workshops.

Xiaofeng Chen received his BSc and MSc in Mathematics from Northwest University, China. He received his PhD in Cryptography from Xidian University in 2003. Currently, he works at Xidian University as a Professor. His research interests include applied cryptography and cloud computing security. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 1,500 times at Google Scholar. He has served as the programme/general chair or programme committee member in over 30 international conferences.

The tremendous advances in wireless communication and mobile computing technologies have created a new computing and communication environment that provides services anytime and anywhere for everyone. In order to accelerate this trend, further progresses of the researches on wireless and pervasive computing are necessary. This is especially true because future information networks will integrate, most likely, existing and upcoming technologies into a heterogeneous and highly dynamic resource pool. To alleviate the capacity crunch in mobile networks, for example, emerging wireless technologies are being actively studied and developed in both wireless academia and industry. With the ever-increasing demand for bandwidth, connection quality, and end-to-end interactivity, computer networks and mobile devices are requiring more and more sophisticated and power-hungry technologies. In order to minimise energy consumption as much as possible while maintaining extreme adaptability to environmental challenges and resources, it is necessary to develop highly autonomous systems with the capability to adapt dynamically to energy availability and usage. Emergent behaviour, such as self-organisation, is another concern in seeking to model and reason about the control structures of such information network systems. Self-organisation means that structures appear within the system without the use of explicit programming or environmental constraints. Thus, green communication and computing research is concerned with the best practice support, in all manner of highly distributed computing systems.

Such issues are nowadays real challenges to the development of large distributed systems and applications. This special issue covered the latest advances in intelligent networks and collaborative technologies that lead to competitive advantages in business and academia scenarios. Its aim was to stimulate research leading to the creation of responsive environments for networking and, in the longer term, the development of adaptive, secure, mobile, and intuitive intelligent systems for future network systems. Industry and academic researchers, professionals and practitioners were invited to exchange their experiences and present their ideas in the field. Examples of subjects covered include technological advances in devices equipped with greater embedded intelligence capable to communicate with others for the full user benefits to be realised, intelligent networks incorporating smart algorithms that can realise autonomy and self-management, and smart power and energy technologies for future network systems. The Special Issue received much attention from the scientific community, and following a thorough review, six papers were carefully selected based on their originality, significance, technical soundness, and clarity of exposition. The papers in this special issue are organised as follows.

In the first paper, Tan and Jiang present two identity authentication schemes that use identification confirmation and decoy states to check outside eavesdropping. Controlled quantum teleportation (CQT) is today widely used to realise communication between two entities, when they need to cooperate with a third controller. The idea is to send quantum states successfully by a quantum communication system. However, the drawback of this quantum schema is that an entity cannot easily confirm the identities. Thus, the authors propose a solution where the identity is confirmed by using two Bell states' entanglement swapping. The scheme can effectively prevent forgery identity attack to ensure the security of quantum teleportation. The authors also present their improved controlled quantum teleportation (ICQT) scheme with decoy states to make sure the security of quantum channel.

In the second paper, Chilipirea et al. present novel contributions to opportunistic mobile networks. In such particular intelligent ad hoc networks, node connectivity is transient, thus traditional routing mechanisms are infeasible. New approaches use social relations between mobile users as a criterion for the routing process. The authors argue that such an approach could quickly deploy energy resources for nodes with high social popularity, and, therefore, popular nodes might be unwilling to participate in the routing process. Next, the authors introduce energy awareness as an important criterion in the routing decision, and propose an approach that experimentally delivers performances similar to BUBBLE Rap, whilst balancing the energy consumption between nodes in the network.

In the third paper, Sang et al. introduce the notion of security associated with modern mobile devices. With the development of the communication industry, the smartphone plays a more important role in people's lives, and provides rich functionality with a variety of smartphone operating system platforms. But, with the internet becoming increasingly more complex and changeable, more and more manufacturers focus on the security evaluation of smartphone operating system to make their product more secure. The paper analyses security mechanisms, and highlights risk factors associated with different smartphone operating systems. Next, the paper presents security requirements used for the common smartphone operating system. Finally, the authors propose a protection profile in EAL4+ (evaluation assurance level 4 including the extended security assurance requirements).

In the fourth paper, Ma extends an identity-based group signature scheme previously proposed, and gives a construction of identity-based group signatures. The identity-based public key cryptosystem allows, in fact, a user to use his identity as the public key, which can be a good alternative for certificate-based public key setting. Group signature allows any member of a group to sign on behalf of the group without revealing his identity. The author constructs, as well, an efficient identity-based group signature scheme, and shows that the group signature scheme is provably secure in the random oracle model.

In the fifth paper, Feng and Li present a certificate-based signature scheme derived from bilinear pairings and prove its security in the random oracle model. Certificate-based signature preserves advantages of implicit certification. The authors present, as such, a scheme that is secure and follows on the traditional difficult problem defined in bilinear pairings. Compared with earlier signatures with these properties, the authors demonstrate that their scheme is highly efficient. Many other constructions could be derived from this, using the certificate-based signature in practical applications.

In the last paper, Deng and Chang follow up on multicast approaches for delay-tolerant networks (DTNs). The authors present a multicast routing scheme based on social difference (SDMR). SDMR considers the social differences between nodes (including both the similarity and the centrality differences), and chooses the nodes with greater social differences to forward data. Considering the critical role of the recent contact history, the authors propose a time-considered multicast routing scheme based on SDMRT, which can improve the transmission efficiency further. Through extensive trace-driven simulation, the scheme can not only ensure high data delivery ratio and low delay, but also reduce the transmission cost greatly compared with other existing protocols. Moreover, SDMRT can further reduce the transmission cost of SDMR without comprising data delivery ratio and delay.

Acknowledgements

The guest editors wish to thank the referees who carefully reviewed the papers and gave useful suggestions and feedback to the authors. We hope that the readers will find this special issue useful in their research. Finally, we would like to thank all editors and staff members of the *International Journal of Embedded Systems* (IJES) for the opportunity to edit this special issue.