J Supercomput (2011) 55: 123–125
DOI 10.1007/s11227-010-0514-z

EDITORIAL

# Special issue on "Theory and practice of high-performance computing, communications, and security"

**Tai-Hoon Kim · Omer F. Rana · Juan Tourino · Isaac Woungang**

Published online: 10 November 2010


With the rapid growth in computing and communication technology, the past decade has witnessed a proliferation of powerful parallel and distributed systems and an ever increasing demand for practical applications of high-performance computing, communications, and security (HPCCS). HPCC has moved into the mainstream of computing and has become a key technology in determining future research and development activities in many academic and industrial branches, especially when the solution of large and complex problems must cope with very tight timing schedules.

This special issue aims to foster the dissemination of high-quality research in any new HPCCS idea, method, theory, technique, and application. The objective of this special issue is to showcase the most recent developments and research in the HPCCS field, as well as to enhance its state-of-the-art. Original research articles have been solicited in all aspects of HPCCS including theoretical studies, practical applications, new communication technology, and experimental prototypes for HPCCS.

T.-H. Kim (✉)
Hannam University, Daejeon, South Korea
e-mail: thkim2005@gmail.com

O.F. Rana
Cardiff University, Cardiff, UK
e-mail: o.f.rana@cs.cardiff.ac.uk

J. Tourino
University of a Coruna, Coruna, Spain
e-mail: juan@udc.es

I. Woungang
Ryerson University, Toronto, Canada
e-mail: iwoungan@scs.ryerson.ca

In "Design of efficient Java message-passing collectives on multi-core clusters" G.L. Taboada et al. present a scalable and efficient Message-Passing in Java (MPJ) collective communication library for parallel computing on multi-core architectures. The library provides multi-core aware primitives, implements several algorithms per collective operation, and explores thread-based communications, obtaining significant performance benefits in communication-intensive MPJ applications.

In "Admissible Bilinear Map based Key Management Protocol for HPCCS in Heterogeneous Network", Jong Sik Moon et al. propose secure and efficient key management in a heterogeneous network environment. Therefore, it provides secure communication between heterogeneous network devices. In this paper, experiments have been conducted to develop secure and efficient technologies between heterogeneous networks using public key to fix and support related problems.

In "Efficient and short certificateless signatures secure against realistic adversaries", Raylin Tso et al. focus on the efficiency of a certificateless signature (CLS) scheme and introduce an efficient CLS scheme with short signature size. The scheme is proved secure in the random oracle model and can be applied to systems with low-bandwidth channels and/or low computation power.

In "A Novel Design of Variable-Rate RS Encoder for Ubiquitous High Performance Multimedia Service in Gbps Transmission System", Yang Sun Lee and Sang-Soo Yeo have first reviewed the state-of-the-art technologies related to DOCSIS 3.0 high-speed data transmission system and also looked at current trends in the next generation Gbps transmission technology, which is a key technology for ubiquitous high-performance multimedia service environments. In addition, they implemented the RS encoder which was designed using VHDL and verified its operation in order to confirm our design through the ModelSim simulation analysis tool.

In "An Approach on Introducing Locality in Remote Attestation using Near Field Communications", Toegl and Hutter introduce a compact radio interface to the Trusted Platform Module. Their modification allows one to include a proof of physical presence in the security protocol of Remote Attestation.

In "The Study on End to End Security for Ubiquitous Commerce", Hangbae Chang has carried out research for the purpose of securing keyboard input information at end to end area between the keyboard hardware and the computer main system. To secure derived vulnerabilities the author has designed a couple of detailed system components, such as debug interrupt exception processing, "JUMP" code insertion, keyboard input encryption and direct transmission. We expect that this research would be able to contribute to a follow-up study not only to prevent leaking keyboard input information but also to secure important information in ubiquitous commerce applications.

In "Pool-Based Anonymous Communication Framework for High Performance Computing", Minh-Triet Tran et al. propose and analyze XPROB, an infinite family of pool-based anonymous communication systems. Each instance of XPROB uses a pool mix as its core component to provide resistance against global active adversaries. In XPROB, any message can be delivered with high probability within a few rounds after its arrival into the system and users can choose their own preference balance between anonymity and delay.

In "A Portable UPnP-based High Performance Content Sharing System for Supporting Multimedia Devices", Chin-Feng Lai et al. propose a portable UPnP-based

high-performance content sharing system for supporting multimedia devices, which includes a content sharing server, and media players. The content sharing server can realize the share services and file control of the portable disk and other devices, so that users no longer need to carry out complex processes to install software and settings, as the media players can allow users to play the multimedia file on any media device.

In “Secure Mobile Communication via Identity-based Cryptography and Server-aided Computations”, Matthew Smith et al. propose an identity-based key agreement protocol for securing mobile telephony in GSM and UMTS networks. The approach allows two mobile phones to perform a session key agreement over an unsecured channel and between different providers using telephone numbers as public keys.

In “Efficient RNTS System for Privacy of Banking Off-line Customer,” Cheol Ho Jeong and Kwang Seon Ahn propose a system for when an off-line customer visiting a bank for banking service; the RNTS (RFID Number Ticket Service) system provides both anonymity in customer identification and efficiency of banking service. In addition, the RNTS system protects the off-line privacy of the user who visits a bank, and it is an efficient method that may offer service in arriving in the bank.

We wish to thank all the authors for their great work and for considering the Journal of Supercomputing for submitting their papers. Special thanks go to the anonymous reviewers for their help and dedication in reviewing the papers and providing useful comments to the authors for the improvement of their papers. Special thanks go to the EiC, Hamid Arabnia, for hosting this special issue, and for the excellent support.