Editorial

K. Chandra Sekaran

Department of Computer Engineering,
National Institute of Technology,
Surathkal, Srinivasnagar, Karnataka, 575 025, India
E-mail: kchnitk@ieee.org
E-mail: kch@nitk.ac.in
E-mail: kchnitk@gmail.com

Biographical notes: K. Chandra Sekaran is currently working as Professor in the Department of Computer Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India. He has 22 years of experience in academic teaching and research. His PhD work was in the area of formal methods in communication protocols using object oriented approach and he has been an active researcher in the areas of distributed computing, network protocols and cyber security. He was the Organising Chair of ADCOM 2006, ISAHUC'06, ADCOM 2008 and associated with many international events and journals at various capacities.

In recent years cyber security has been at the forefront of the research world. The distributed nature of modern computing that involves interconnected heterogeneous environments poses newer security challenges. This concern, in the area of security, is due to the tremendous increase in the deployment of networks and distributed platforms now in place across the globe. Due to this, newer security threats are inadvertently created in these domains. Although research in communication networks and distributed systems security has been constantly growing with significant contributions and presented in various events, it is felt that modern security threats seem to demand additional research efforts and results. In this context, *IJCNDS*' special issue is an opportunity for the researchers to contribute their results.

This special issue encapsulates eight best papers from the potential submissions. In the first paper, entitled 'A mesh checksum ABFT scheme for stream ciphers', Chang N. Zhang and Xiao Wei Liu address the issue of fault tolerance and reliability in stream ciphers and demonstrate their work known as – algorithm based mesh check-sum fault tolerant scheme. The second paper, 'LoBA128, a Lorenz-based PRNG for wireless sensor networks' by Rui M.S. Silva et al., presents a pseudo random number generator that is useful in symmetrical encryption system, particularly in the domain of wireless sensor networks. The third paper titled 'High-speed string matching for network intrusion detection' by Ning Weng et al., proposes solutions to the daunting challenge in designing effective IDS with high-speed string matching technique experimented on FPGA platforms. In the paper 'A new hardware efficient stream cipher based on hash functions', the authors P.P. Deepthi et al., propose a solution that uses stream ciphers that is based on hashing technique in the domain of cryptography as it requires less complex hardware requirement in the implementation level and demonstrate the effectiveness of it. In the fifth paper titled 'Free-roaming mobile agent (FRoMA) protection against multiple attacks' by S. Venkatesan and C. Chellappan, it is proposed to make use of the mobile

agents towards protecting systems from multiple attacks. The sixth paper titled 'Knapsack based ECC for digital signature authentication' by R. Rajaram et al., illustrates the implementation of knapsack algorithm on elliptic curve cryptography for encryption and decryption. In the seventh paper entitled 'Password-based authenticated key distribution in the three-party setting with forward security' by Shuhua Wu and Yuefei Zhu attempt to provide solutions to some of the drawbacks of 3PKD protocol by revising the protocol with a proving towards 'forward security'. The last (eighth) paper titled 'Protection of LAN-wide, P2P interactions: a holistic approach' by André Zúquete, proposes a security oriented LAN architecture which uses a holistic view in terms of building systems/applications.

Finally, as guest editor of this special issue, I thank the Editor-in-Chief Dr. Sudip Misra for providing me an opportunity to edit this issue with his constant trigger and help. Also, I thank the referees for their outstanding cooperation and interesting comments and suggestions that have helped to improve the presentations of the papers and, all the authors for their quality contributions. I believe that the contributions in this special issue will stimulate further research in the important areas of security in communication networks and distributed systems.