Editorial

Honghao Gao

School of Computer Engineering and Science,
Shanghai University,
Shanghai 200444, China
Email: gaohonghao@shu.edu.cn

Yuyu Yin

School of Computer Science,
Hangzhou Dianzi University,
Hangzhou 310000, China
Email: yinyuyu@hdu.edu.cn

Wenbing Zhao

Department of Electrical Engineering and Computer Science,
Cleveland State University,
Ohio 44115-2214, USA
Email: w.zhao1@csuohio.edu

Biographical notes: Honghao Gao is a Fellow of IET, BCS, and EAI, and a Senior Member of IEEE, CCF, and CAAI. His research interests include software formal verification, industrial IoT/wireless networks, service collaborative computing, and intelligent medical image processing.

Yuyu Yin is currently a Professor with the College of Computer Science and Technology at Hangzhou Dianzi University. His research interests include service computing, cloud computing, and business process management.

Wenbing Zhao is a Professor with the Department of Electrical Engineering and Computer Science at Cleveland State University. His current research interests include distributed systems, blockchain, machine learning, smart and connected health.

The guest editors would like to express their deep gratitude to all the authors who have submitted their valuable contributions. In this special issue, we have accepted high-quality papers from open calls and invitations. A summary of these papers is outlined below.

In the paper, 'An attribute-based cross-domain trustworthy model for internet of vehicles', Ou et al., propose a multi-attributes-based cross-domain trustworthy model. They divide the security domain into three layers which are the cross-domain application layer, cross-domain network layer, and cross-domain perception layer.

In the paper, 'The cross-layer oriented security performance to wireless network fibre communication router: the optimisation perspective', Zhou et al., analyse the characteristics of traditional optimised link state routing (OLSR) routing protocols, apply cross-layer design theory, and combine the characteristics of the link layer in a wireless mesh network (WMN) network. They propose a point-to-point lightweight encryption algorithm, which realises secure wireless mesh network transmission through the key exchange and fast encryption and decryption methods of the receiving and sending nodes.

In the paper, 'SIP network secure communication model based on improved SIP protocol', Min, focuses the chaotic sequence generated by chaotic equations, and makes hypertext transfer protocol (HTTP) digest for session initiation protocol (SIP). They optimise the dynamic password generation during the authentication process, propose a SIP security authentication mechanism based on chaotic equations, and extend the header field of the SIP protocol.

In the paper, 'A security protocol of RFID communication system based on password authenticated with provable security', Li and Liu, propose security architecture for radio frequency identification (RFID) systems based on a chain of trust. They construct a security trust chain from the perception layer, the transmission layer to the application layer. And they propose a privacy protection model of label ownership transfer aiming at the problem of privacy disclosure of label ownership transfer.

In the paper, 'Security model and design of network communication system based on data encryption algorithm', Ma and Liu, build a unified clustering framework based on secure multi-party computing that can be used in practice. Their framework can reduce the difficulty of deploying clustering algorithms on privacy data sets, and can quickly expand and support clustering algorithms.

In the paper, 'Connection-oriented computer network secure communication and encryption algorithm', Wu studies the data encryption model and encryption method for connection-oriented computer network communication systems. It includes comprehensive communication security strategy, and data encryption. The method can simplify the deployment of the cryptosystem and improve the efficiency of the cryptosystem.

In the paper, 'A hybrid chemical reaction optimisation algorithm for solving 3D packing problem', Su et al., combine the chemical reaction optimisation algorithm with the greedy algorithm to solve the three-dimensional bin packing problem (3D-BPP). They adjust parameters to the chemical reaction optimisation algorithm and carry out experiments on classic 320 examples.

In the paper, 'A channel estimation algorithm for large-scale MIMO system using block sparsity adaptive matching pursuit', Chen, proposes a new adaptive channel estimation algorithm for large-scale multiple-input multiple-output (MIMO) systems by combining the block sparsity adaptive matching pursuit technique with adaptive beamforming. They optimise the sparse matrix and enhance channel sparsity. The atoms of the support set can be selected quickly and preliminarily. And they also consider the energy dispersion caused by the non-orthogonality of the observation matrix.

In the paper, 'Identifying natural images and computer-generated graphics based on convolutional neural network', Long et al., propose an image source pipeline forensics method based on convolutional neural network (CNN), aiming at the identification of natural images and computer-generated graphics. They use Inception-v3 as the basic

network and adopt the pre-trained model parameters in ImageNet. Then, they construct a new network model with transfer learning.

In the paper, 'A HDFS dynamic load balancing strategy using improved niche PSO algorithm in cloud storage', Jian and Jian, propose an HDFS NameNode dynamic load balancing strategy (NDLBT) using improved niche particle swarm optimisation (PSO). First, they analyse the relationship between bandwidth consumption and the bit rate of video files, the size of data blocks, and access hotspots of online video files. Then, they realise adaptive backup by dynamic multiple copies of heterogeneous nodes. Finally, they propose a new improved niche PSO algorithm to achieve load balance schedule.

In the paper, 'End-to-end encrypted communication security technology for mobile terminals', Zhang, adopts the end-to-end encryption technology to study the communication security technology in mobile terminals. First, he uses a smart card for encryption and decryption operation and secure storage of keys. Second, he introduces a multi-level key management mechanism to update the key regularly. At last, he shows the bidirectional authentication and authentication.

In the paper, 'A new signcryption algorithm for secure communication in ad hoc networks', Li, studies a new signcryption algorithm for secure communication in ad-hoc networks. The key management scheme using the algorithm can have lower operation cost and communication cost, which is suitable for the security requirements of ad-hoc networks.

In the paper, 'Research on the application of data encryption technology in communication security', Li et al., propose a lightweight data encryption algorithm based on the dynamic key. And then they construct a data authentication scheme combining with the characteristics of communication system aiming at the security problems of data monitoring, and forgery and tampering in the process of the wireless communication network.