Foreword

Computational Intelligence for Network Control and Security

Computational intelligence for network control and security has been an important application field as it has the property of intelligence countermeasure. Now computational intelligence for network control and security has been envisioned as an important topic in researches, where many emerging open problems still be solicited to answer. This special issue aims to provide the network control community in general and the network security community in particular, with the state of the art on the study of Computational Intelligence. After peer review, the guest editors accepted 12 final accepted papers from 96 online submissions for the special issue to reflect the current development of computational intelligence for network control and security.

The first paper by Lingxi Peng, Dongqing Xie, Ying Gao, Wen-bin Chen, Fu-fang Li, Wu Wen and Jue Wu is entitled “An Immune-inspired Adaptive Automated Intrusion Response System Model”. The authors give an immune-inspired adaptive automated intrusion response system model (MAIM), which not only solves the problem that the current automated response system models could not accurately evaluate the network attacks, but also greatly reduces the response times and response costs. The theory analysis and experimental results prove that MAIM provides a positive and active network security method, which will help to overcome the limitations of traditional passive network security systems.

The second paper by Hong Peng, Shiyuan Fu, Limin Meng and Xia Liu is entitled “A Novel Location-aided Routing Algorithm for Mobile Ad Hoc Network with a Small Expenditure on Route-Discovery”. The authors propose a novel routing algorithm based on Grover searching theory to reduce the expenditure in route discovery. In the proposed algorithm, the density of the nodes’ distribution in the request-zone determines the adopted mechanism for packet transmission. Simulation results show that the proposed algorithm can reduce the number of nodes to be influenced and save the expenditure on route discovery.

The third paper by Yali Liu, Xiaolin Qin, Bohan Li and Liang Liu is entitled “A Forward-secure Grouping-proof Protocol for Multiple RFID Tags”. The authors propose a forward-secure grouping-proof protocol (FSGP) for multiple RFID tags based on Shamir’s (n, n) secret sharing. In comparison with the previous grouping-proof protocols, FSGP has the characteristics of forward-secure and order-independent addressing the scalability issue by avoiding relaying message. The proposed protocol provides security enhancement, performance improvement and controls the computation and communication cost at the same time.

The fourth paper by Min Lei, Haipeng Peng, chunyu Yang and Lixiang Li is entitled “Synchronization of Time-Delay Chaotic Systems in Presence of Noise”. The authors propose a nonlinear synchronization scheme for the time-delay chaotic system in the presence of noise. In

the proposed scheme, the integrator is introduced to suppress the influence of channel noise in the synchronization process. The numerical simulations prove the effectiveness and feasibility of the proposed scheme. The proposed scheme can obtain strong characteristic of robustness in presence of noise, especially in presence of high frequency noise.

The fifth paper by Haiyang Hu, Zhongjin Li, Liguo Huang and Hua Hu is entitled “Statistical Mechanisms for Detecting Malicious Behaviors in Resource Allocation from Non-cooperative P2P Environments”. The authors present a bidding based approach for resource allocation to address these issues. In designing an efficient and security resource allocation algorithm for resisting the damage to the P2P system brought by malicious peers, the authors explore different types of malicious behavior and present several statistical mechanisms to detect the malicious peers. The experiments show that the proposed mechanism is effective.

The sixth paper by Jinxin Zhang, Mangui Liang and Shujuan Wang is entitled “A Credibility-based Congestion Control Scheme and its Performance Evaluation”. The authors propose a novel congestion control method in the network layer, which is credibility-based and under supervision. The effectiveness of this scheme is analyzed. The authors provide extensive simulation results to demonstrate that the proposed scheme can process congestion and provide better performance gains.

The seventh paper by Jianfeng Lu, Jianmin Han, Wei Chen, Jinwei Hu is entitled “Safety and Availability Checking for User Authorization Queries in RBAC”. The authors propose a recursive algorithm using the ideas from backtracking-based search techniques to search for the optimal solution. For the availability checking, the authors introduce the notion of max activatable set (MAS), and show formally how MAS can be determined in a hybrid role hierarchy. For the safety checking, the authors give a formal definition of DSoD policies, and show how to reduce the safety checking for DSoD to a SAT instance.

The eighth paper by Ming Wan, Ying Liu, Jianqiang Tang, Hongke Zhang and Siyu Lin is entitled “Locator/Identifier Separation: Comparison and Analysis on the Mitigation of Worm Propagation”. The authors systematically analyze the mitigation of worm propagation in the three aspects: address semantics, address space and mapping delay. By applying the classical AAWP and SIR worm propagation models, the paper give a quantitative comparison between today’s Internet and networks with locator/identifier separation. The characteristics of locator/identifier separation can help to markedly mitigate worm propagation, and networks with locator/identifier separation are more resistive to worm propagation than today’s Internet.

The ninth paper by Liangyu Luan, Yingfang Fu, Peng Xiao and Lingxi Peng is entitled “Watch-Nodes-Based Wormhole Attacks Detection in Wireless Mesh Networks”. The authors present a type of wormhole attack model and its corresponding wormhole attack detection schemes, i.e., the watch node based detection scheme that is based on the combination of a number of techniques, such as distributed voting, watch node based detection and identity-based cryptosystem. The proposed wormhole attack detection schemes are more advantageous over the some of the previous schemes in terms of performance and cost.

The tenth paper by Qian Xiao, Kangfeng Zheng, Shoushan Luo and Xu Cui is entitled “A Secure Network Coding-based Data Gathering Model and Its Protocol in Wireless Sensor Networks”. The authors propose a formalized model SNCDG, and design a SNC protocol used in this model, called DPP&PP. This protocol achieves the security objective and the requirements of environment adaptability of our model. DPP&PP not only preserves private source data, but also prevents external pollution attacks. One the other hand, DPP&PP needs low overhead on computation and communication, so it is suitable for WSNs with limited energy.

The eleventh paper by Wei Li, Dawu Gu, Xiaoling Xia, Chen Zhao, Zhiqiang Liu, Ya Liu and Qingju Wang is entitled “Single Byte Differential Fault Analysis on the LED Lightweight Cipher in the Wireless Sensor Network”. The authors propose a differential fault analysis on the LED cipher by inducing faults based on the single byte-oriented fault model. Mathematical analysis and simulating experiment show that the attack could recover its 64-bit secret key by introducing 4 faulty ciphertexts, and recover 128-bit secret key by introducing 8 faulty ciphertexts, respectively.

The twelfth paper by Yu Yang, Shangbao Gong, Yucui Guo, Min Lei and Yan Yang is entitled “A Complex Estimation Function Based on Community Reputation for On-line Transaction Systems”. The authors propose a generalized set-theoretic reputation function in this paper, which can be configured to meet various assessment requirements of a wide range of reputation scenarios encountered in online transaction nowadays. Simulating experiment shows tolerance of this reputation function against various socio- communal reputation attacks. And the authors find the function to be dynamic, customizable and tolerant against different attacks. As such it can serve well in many online transaction systems such as e-commerce websites, online group activities, and P2P systems.

Yixian Yang
Beijing University of Posts and Telecommunications
Beijing, 100876, P. R. China

Fuji Ren,
Tokushima University,
Tokushima, Japan