Control and Cybernetics

vol. **42** (2012) No. 2

Guest Editorial: Special Section on Security for Intelligent Networking and Collaborative Systems

by

Xiaofeng Chen[1], **Fatos Xhafa**[2]

[1]The State Key Laboratory of Integrated Service Networks (ISN),
Xidian University, Xi'an, P.R. China
e-mail: xfchen@xidian.edu.cn
[2]Department de Llenguatges i Sistemes Informatics,
Universitat Politćcnica de Catalunya Barcelona, Spain
e-mail: fatos@lsi.upc.edu

With the fast development of the Internet, companies, communities and organizations of practice strongly leverage intelligent networking and collaborative systems by a great variety of formal and informal electronic relations, such as business-to-business, peer-to-peer and many types of online collaborative learning interactions. This has resulted in entangled systems that need to be managed efficiently and in an autonomous way. In addition, latest and powerful technologies based on Grid and Wireless infrastructure as well as Cloud computing are currently enhancing collaborative and networking applications a great deal but also entailing new issues and challenges. For example, well-known social networks lack knowledge management and adaptive solutions and the information shared among peers is rather static. Virtual communities of practice also provide poorly interactive solutions and lack full support for organization, management, mobility and security.

Security is an important research topic in networking and systems. With provable security, we are confident in using the schemes and protocols in various real-world applications. This special section on "Security for Intelligent Networking and Collaborative Systems" attempts to highlight some of the latest research addressing those challenges. It consists of six papers selected from the contributions to the 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS 2011). More specifically:

- The paper by Qin, Wu, Domingo-Ferrer and Susilo, "Robust Distributed Privacy-Preserving Secure Aggregation in Vehicular Communication", proposes a robust protocol with a set of new mechanisms for efficiently managing identities and securely compressing cryptographic witnesses, which are among the major obstacles to the deployment of strong security mechanisms in VANETs;

- Tian and Liu's paper on "A new strong multiple designated verifiers signature for broadcast propagation" presents a novel signature scheme featured by single verifier simulation, private verification, and one signature for multiple verifiers. It is the first multiple designated verifiers signature scheme for broadcast propagation model, and can be applied to a privacy-friendly service provided by multiple servers;
- The paper of Gao, Li, and Wei, "Improved Linear Complexities of the Frequency Hopping Sequences in Two Optimal Sets", determines the linear complexities of the frequency hopping sequences in two sets transformed by the power permutation or binomial permutation. The two transformed sets are also optimal and the sequences in two sets have larger linear complexity than the original ones;
- The paper of Liu and Chen, "Homomorphic Linear Authentication Schemes from epsilon-ASU2", proposes new constructions of epsilon-almost strong universal hashing functions (epsilon-ASU2), and employs these epsilon-ASU2 to build homomorphic linear authenticator schemes in Proofs of Retrievability to provide unforgeability. The homomorphic linear authenticator schemes enjoy shortest responses from storage server, due to the homomorphic property;
- Shen, Pei, Xu, Xi and Ma's paper on "HGRP: Hybrid Grid Routing Protocol for Heterogeneous Hierarchical Wireless Networks" presents a novel routing protocol for heterogeneous hierarchical wireless networks, called "Hybrid Grid Routing Protocol" (HGRP). Compared to the available routing protocols, HGRP enjoys the advantages of lower routing cost, lower energy consumption, smaller delay and higher throughput;
- The paper of Xiong, Wu and Chen, "An Efficient Provably Secure Certificateless Aggregate Signature Applicable to Mobile Computation", presents a new efficient certificateless aggregate signature scheme. The construction is proved secure against the super Type I/II adversary (the strongest attacker model) under the standard CDH assumption. Besides, the scheme is efficient due to constant pairing operations and signature size.

Finally, we would like to express our appreciation to all authors, reviewers and editorial staff for their invaluable contribution, without which this special section could not become reality.