Peer-to-Peer Netw. Appl. (2015) 8:1023–1024
DOI 10.1007/s12083-015-0393-4

Guest editorial: Security and privacy of P2P networks in emerging smart city

Hongwei Li[1] · Haojin Zhu[2] · Bong Jun (David) Choi[3,4]

Published online: 22 July 2015

Recently, the smart city has been introduced as a promising concept due to its potential benefits including low-carbon economy, intelligent traffic management, ubiquitous information sharing, and etc. In the smart city, there are many key components, such as smart grid, smart vehicle, smart cloud, and mobile social network. Thanks to the good salability and low processing cost on content delivery and distributed search engine in these components, P2P technologies are expected to play an essential role in accelerating the implementation of the smart city. Although we have witnessed the major and remarkable development in the field of smart city in the recent years, the security and privacy issues of the smart city have not been well studied. Thus, there is a crucial need for security and privacy research to achieve secure and privacy-preserving smart city.

This special issue has gained overwhelming attention and received 32 submissions from researchers and practitioners working on security and privacy of P2P Networks in emerging smart city, including: full lifecycle privacy protection, effective trust model for the P2P system, privacy in wireless healthcare system, user authentication with unlinkability, location privacy in vehicular ad hoc network, and etc. After initial examination of all submissions, 32 papers are selected to go under a rigorous review process where each submission has been reviewed by at least two reviewers. After 2 round reviews, eventually 10 quality papers are recommended to be included into this special issue, which are summarized as follows.

"A full lifecycle privacy protection scheme for sensitive data in cloud computing'' by Jinbo Xiong, Fenghua Li, Jianfeng Ma, Ximeng Liu, Zhiqiang Yao, and Patrick S. Chen, presents a full lifecycle privacy protection scheme for sensitive data. Security analysis of this paper indicates that the proposed scheme is able to resist against Sybil attacks on the DHT network.

"A lightweight identity authentication method by exploiting network covert channel" by Haijiang Xie, and Jizhong Zhao, exploits the reverse usage of the Network Covert Channel (NCC) which is originally designed by attackers to create stealth communication and provides a more secure authentication method compared with many existing approaches.

"A topological potential weighted community-based recommendation trust model for P2P networks" by Qiyi Han, Hong Wen, Mengyin Ren, Bin Wu, and Shengqiang Li, studies effective strategies to establish trust model for the P2P system and designs a novel topological potential weighted community-based recommendation trust model architecture.

"An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system" by Haomiao Yang, Hyunsung Kim, and Kambombo Mtonga, investigates the security and privacy issues

✉ Hongwei Li
hongweili@uestc.edu.cn

Haojin Zhu
zhu-hj@cs.sjtu.edu.cn

Bong Jun (David) Choi
bjchoi@sunykorea.ac.kr

[1] University of Electronic Science and Technology of China, Chengdu, China

[2] Shanghai Jiao Tong University, Shanghai, China

[3] The State University of New York Korea, Incheon, Korea

[4] Stony Brook University, Stony Brook, NY, USA

of the remote health monitoring system and presents an efficient privacy-preserving authentication scheme with adaptive key evolution in wireless healthcare.

"An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks" by Qi Jiang, Jianfeng Ma, Xiang Lu, and Youliang Tian, studies user authentication with unlinkability in wireless sensor networks. The proposed scheme not only remedies some security flaws but also improves the performance compared with existing work.

"EAPA: An efficient authentication protocol against pollution attack for smart grid" by Mi Wen, Jingsheng Lei, Zhongqin Bi, and Jing Li, focuses on the pollution attacks in smart grid communication network. By verifying the integrity and origin of the packets received without having to decode, the proposed protocol can detect and discard the malicious packets in transit.

"Fault-aware flow control and multi-path routing in VANETs" by Xiaomei Zhang, Xiaolei Dong, Naixue Xiong, Jie Wu, and Xiuqi Li, investigates the optimization problem via the joint design of rate control and multi-path routing for fault-aware vehicular ad hoc netwok (VANET) and develop a leaky-path model based on statistical information and estimation.

"Mix-zones optimal deployment for protecting location privacy in VANET" by Yipin Sun, Bofeng Zhang, Baokang Zhao, Xiangyu Su, and Jinshu Su, deploys mix-zones to protect location privacy in VANET.

"PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications" by Le Chen, Rongxing Lu, and Zhenfu Cao, investigates the security problem of smart grid and design a data aggregation scheme based on the homomorphic Paillier Encryption technique.

"Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement" by Jun Wu, Mianxiong Dong, Kaoru Ota, Lin Liang, and Zhenyu Zhou, identifies the requirements for storage in Social Internet of Things (SIoT) scenarios, and uses the regenerating codes and symmetric-key encryption with a Blom based key management to realize the secure sensor distributed storage for SioT with repairing capability.

Finally, we would like to appreciate all authors who submitted manuscripts for consideration, and over 60 anonymous dedicated reviewers for their expert comments and time to help us making the final decisions. Without their valuable and strong supports, we could not have made this special issue successful. We would like also to express our sincere gratitude to the PPNA EiC, Prof. Xuemin (Sherman) Shen, as well as Ms. Melissa Fearon, Ms. Ethel Dionela and Mr. Hector Nazario from the Springer Journal Editorial Office for helping us to publish this special issue to readers.