Hindawi
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 2057965, 2 pages
https://doi.org/10.1155/2017/2057965

Editorial

Security and Privacy in Internet of Things with Crowd-Sensing

Liangmin Wang,[1] Zhuo Lu,[2] Hongjian Sun,[3] Yantian Hou,[4] and Mengxing Huang[5]

[1]*Department of Cyber Security, Jiangsu University, Zhenjiang 212013, China*
[2]*Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA*
[3]*School of Engineering and Computing Sciences, University of Durham, Durham DH1 3HP, UK*
[4]*Department of Computer Science, Boise State University, Boise, ID 83706, USA*
[5]*College of Information Science and Technology, Hainan University, Haikou 570100, China*

Correspondence should be addressed to Liangmin Wang; wanglm.ujs@gmail.com

Received 28 November 2017; Accepted 28 November 2017; Published 21 December 2017

The rapid proliferation of mobile sensing devices, such as smartphones, wearable devices, and mobile vehicles, has promoted the emergence of a novel sensing paradigm for Internet of Things (IoTs). Crowd-sensing, known as a promising data collection method, is becoming increasingly popular in IoTs due to its low deployment cost and large-scale spatial coverage. Crowd-sensing-based IoTs interconnects various physical objects, including human, sensors, and smart devices, to collect data through the enhanced communication technology and process and share information with the assistance of cloud servers. Currently, a wide range of crowd-sensing applications are fostered in various domains such as environmental monitoring, assistive healthcare, social network, business, and intelligent transportation.

Numerous research challenges arise in the crowd-sensing-based IoTs, among which security and privacy are two critical issues that hinder the ubiquitous deployment of relevant applications. For data sensing in the front-end IoTs, sensed data may contain some sensitive information of mobile users. Moreover, data can be falsified and tampered with by external attackers or even be polluted by internal attackers (i.e., malicious users). For data storage and processing in the back-end IoTs, cloud servers may be curious to infer private information of data owners and query users or even maliciously modify some query results. In these circumstances, many factors, including user privacy, data confidentiality, integrity, reliability, and access control, should be taken into consideration in a holistic perspective.

This special issue provides the opportunity for researchers, practitioners, and application developers to discuss the recent technical advances and future challenges in security and privacy protection for crowd-sensing-based IoTs. The topic of accepted papers pertains to security and privacy issues from different aspects, ranging from secure network architecture, secure and privacy-preserving data sensing, and data transmission to data processing in IoTs with crowd-sensing.

Over the numerous submissions, six papers have been accepted after the rigorous review process. We now list and give a brief summary of these papers as below.

The paper "A Student Information Management System Based on Fingerprint Identification and Data Security Transmission" by P. Yang et al. studies the secure and reliable data transmission in the student information management system. Based on an improved AES algorithm, the authors propose a novel data encryption method and design a new S-box, which significantly reduces the encryption time. Experimental results also validate the efficiency of their algorithm.

The paper "Vulnerability Analysis of Interdependent Scale-Free Networks with Complex Coupling" by C. Cao et al. mainly analyzes the vulnerability of interdependent scale-free networks with complex coupling based on the BA model. The results indicate that these networks have the same vulnerability against the maximum node attack, the load of the maximum node attack, and the random node attack, indicating that the coupling relationship between network nodes is an important factor in network design.

The paper "The Anonymization Protection Algorithm Based on Fuzzy Clustering for the Ego of Data in the Internet of Things" by M. Xie et al. introduces the concept of ego of data and implements two steps of data clustering for the IoTs, which obscures the specific location information and achieves the anonymization protection. Experimental results show that their proposed algorithm can protect the data more efficiently, without sacrificing the anonymization quality.

The paper "A Variable Weight Privacy-Preserving Algorithm for the Mobile Crowd Sensing Network" by J. Zhong et al. addresses the problem of user privacy leakage in mobile crowd-sensing scenarios. The authors propose a variable weight privacy-preserving algorithm of secure multiparty computation. Its effectiveness and feasibility are demonstrated through experiments.

The paper "Abnormal Event Detection in Wireless Sensor Networks Based on Multiattribute Correlation" by M. Wang et al. focuses on the issue of abnormal event detection in wireless sensor networks. A novel approach is proposed to improve the quality of detection results, which considers both spatiotemporal and attributes correlations. Experiments prove the effectiveness and high detection accuracy of their scheme.

The paper "Health Monitoring System for Nursing Homes with Lightweight Security and Privacy Protection" by Y. Jiang et al. mainly designs a secure and effective monitoring system for nursing homes. A mobile authentication protocol based on hash function is proposed to realize secure access and privacy protection. Compared with the traditional protocols, lower computation and communication cost is induced, which satisfies the high real time and stronger security requirements.

Acknowledgments

We would like to thank all the authors for submitting their manuscripts to this issue and all the reviewers for every effort in the professional review process.

Liangmin Wang
Zhuo Lu
Hongjian Sun
Yantian Hou
Mengxing Huang