Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 6812816, 2 pages
http://dx.doi.org/10.1155/2016/6812816

Hindawi

Editorial

Security and Privacy Challenges in Vehicular Cloud Computing

Rongxing Lu,[1] Yogachandran Rahulamathavan,[2] Hui Zhu,[3] Chang Xu,[4] and Miao Wang[5]

[1]*University of New Brunswick, Fredericton, NB, Canada*
[2]*Loughborough University in London, London, UK*
[3]*Xidian University, Xi'an, China*
[4]*Beijing Institute of Technology, Beijing, China*
[5]*McMaster University, Hamilton, ON, Canada*

Correspondence should be addressed to Rongxing Lu; rxlu@ieee.org

Received 24 November 2016; Accepted 24 November 2016

The recent developments and deployments of connected and autonomous vehicular network or the so-called vehicular ad hoc networks (VANETs) offer the promise of significant benefits to the society and environment including robust road safety and intelligent traffic management. When a swarm of vehicles with sophisticated sensing and connectivity capabilities travel together, aggregating the resources such as sensors, sensor results, and onboard computing infrastructure in vehicles creates a platform equivalent to cloud computing. As a special cloud computing platform, Vehicular Cloud Computing (VCC), which seamlessly combines cloud computing and VANETs, has been recently proposed to accelerate the adoption of VANETs. VCC is a mobile computing paradigm, which consists of in-motion vehicles cooperating with each other to achieve a bunch of practical applications, such as collaborative package delivery and information dissemination. Essentially, VCC coordinates the computing, communication, sensing, and storage resources of the vehicles on the road to balance the service requirements and the hardware limitation. Nevertheless, different from the traditional cloud infrastructure, VCC requires sophisticated security and privacy protection mechanisms as the legitimate users and attackers have the same privileges in mobile VCC. Therefore, in order to enhance the security and scalability of VCC, a number of crucial issues must be addressed such as trust model, data security, connection fault, and query tracking attacks. In this special issue on security and privacy challenges in VCC, we have invited a few papers that address such issues.

The paper "On Preventing Location Attacks for Urban Vehicular Networks" focuses on preventing potential attacks from a perspective of location prediction, which proposes a sophisticated prediction model to predict driver's next location, analyzes the restriction of the proposed advanced predication model, and presents a schema to decrease the risks of location prediction attacks. Experimental results obtained from the real-world vehicular network data have demonstrated the effectiveness of preventing location attacks in urban vehicular networks.

The paper "Conditional Ciphertext-Policy Attribute-Based Encryption Scheme in Vehicular Cloud Computing" presents an expressive and fine-grained conditional ciphertext-policy attribute based encryption (C-CP-ABE) scheme in vehicle cloud computing, which can maintain both data security and system efficiency. Compared with traditional CP-ABE, the scheme brings a trivial amount of storage overhead and a lower amount of computations but can associate one ciphertext with different access trees under different conditions.

The paper "A Safety Resource Allocation Mechanism against Connection Fault for Vehicular Cloud Computing" discusses the vehicle connection fault issue and proposes a safety resource allocation mechanism against connection fault in VCC by using a modified workflow with prediction capability. In the mechanism, the connection fault probability model of the moving vehicles is proposed firstly. And then a safety resource allocation algorithm is proposed to realize the safety resource allocation for VCC. Extensive evaluations

demonstrate that the proposal can improve both reliability and real-time performance of VCC.

The paper "LSOT: A Lightweight Self-Organized Trust Model in VANETs" addresses the trust management in VANETs and proposes a novel lightweight self-organized trust model in VANETs. The model combines both trust certificate-based and recommendation-based trust evaluations, and the evaluation in it can be made quickly and reaches an excellent performance in a lightweight manner.

The paper "A Trust-Based Model for Security Cooperating in Vehicular Cloud Computing" describes a trust-based model for security cooperating to promote the secure cooperation in VCC, in which a double board based trust estimation and correction scheme is proposed to predict the reliability of vehicles and guide the selection of trustworthy cooperative vehicles in a more effective manner.

The paper "A Privacy-Preserving Location-Based System for Continuous Spatial Queries" proposes a novel location cloaking method to resist query tracking attacks. Compared with previous location cloaking methods, this proposed method can generate minimized cloaked regions while protecting the location and trajectory privacy of the query issuer in VCC.

Rongxing Lu
Yogachandran Rahulamathavan
Hui Zhu
Chang Xu
Miao Wang