IEEE INTERNET OF THINGS JOURNAL
A joint publication of
IEEE Sensors Council, IEEE Communications Society, IEEE Computer Society, and IEEE Signal Processing Society

**CALL FOR PAPERS**

**IEEE Internet of Things Journal Special Issue on**

# Towards Securing Internet of Connected Vehicles from Virtual Vehicle Hijacking

Today's vehicles are no longer stand-alone transportation means, due to the advancements on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enabled to access the Internet via technologies including WiFi, Bluetooth, 4G, and even 5G networks. The sensor enabled intelligent automation of vehicle's mechanical operations enhance safety for on-road travelling, while cooperative traffic information sharing in vehicular network improves travelling efficiency. However, safety and efficiency oriented sustainability in transportation via Internet of connected Vehicles (IoV) came with a greater risk of virtual vehicle hijacking. Ranging from unauthorized accessing of wheels, disabling brakes, locking doors, engine disruption to path forging, location and identity manipulation, denial of traffic service, tracking, are the few examples virtual vehicle hijacking. Therefore, there has been the emerging trend to prepare for virtual vehicle hijacking in IoV.

The concern on ensuring the service quality in IoV is due to the challenges in technical migration of protocols, techniques and standards, from static wireless communication to highly mobile vehicular communication environments. However, in existing IoV scenarios where virtual hijacking of connected vehicles is possible, the modelling and practice for securing connected vehicles has not witnessed enough attentions from academia and industries. There are a number of questions remain for open investigation. For example, how to guarantee unauthorized tracking while using GPS for navigation? Who will assure the quality of accumulated traffic information from neighboring vehicles? How to avoid identity theft while using phone on vehicular on-board unit? What are the non-cryptographic security mechanisms suitable for ad-hoc vehicular network environments?

The aim of this special issue is to answer some of the questions on securing connected vehicular networks, for effectively realizing safety and efficiency oriented sustainability in transportation via IoV. Potential topics include, but are not limited to, the following:

- Privacy ensuring communication architecture for GPS enabled navigation use case in IoV
- Location verification for geo-location centric communication in IoV
- Light-weight security framework for Vehicle-to-Everything (V2X) communication
- Quality of traffic information modelling for guarantying cooperative communication
- Optimization of cryptography based security implementation for resource constrained ad-hoc networks
- Reputation calculation frameworks for identifying Denial of Traffic Service (DoTS) in IoV
- Puzzle-based security implementations for time constrained communication in IoV
- Beaconing traffic information without identity theft in IoV
- Hijacking solution- From autonomous connected vehicle to disconnected machine

**Important Dates**

Submissions Deadline: **July 1, 2018**
First Reviews Due: September 15, 2018
Revision Due: October 15, 2018
Second Reviews Notification: November 15, 2018
Final Manuscript Due: December 15, 2018
Publication Date: 2019

**Submission**

IEEE INTERNET OF THINGS JOURNAL
A joint publication of
IEEE Sensors Council, IEEE Communications Society, IEEE Computer Society, and IEEE Signal Processing Society

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Solicited original submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at http://iot.ieee.org/journal.

**Guest Editors**

Yue Cao (Lead Guest Editor)
Northumbria University, UK
yue.cao@northumbria.ac.uk

Houbing Song
Embry-Riddle Aeronautical University, USA
Houbing.Song@erau.edu

Omprakash Kaiwartya
Universiti Teknologi Malaysia, Malaysia
omprakash@utm.my

Naveed Ahmad
University of Peshawar, Pakistan
n.ahmad@uop.edu.pk

Sinem Coleri Ergen
Koc University, Turkey
sergen@ku.edu.tr