8-4-2019

Guest Editorial Special Issue on Toward Securing Internet of Connected Vehicles (IoV) From Virtual Vehicle Hijacking

Yue Cao
Lancaster University

Houbing Song
Embry-Riddle Aeronautical University, songh4@erau.edu

Omprakash Kaiwartya
Nottingham Trent University

Sinem Coleri Ergen
Koç University

Jaime Lloret
Polytechnic University of Valencia

See next page for additional authors

Scholarly Commons Citation

Cao, Y., Song, H., Kaiwartya, O., Ergen, S. C., Lloret, J., & Ahmad, N. (2019). Guest Editorial Special Issue on Toward Securing Internet of Connected Vehicles (IoV) From Virtual Vehicle Hijacking. *IEEE Internet of Things Journal, 6*(4). https://doi.org/10.1109/JIOT.2019.2926608

Authors

Yue Cao, Houbing Song, Omprakash Kaiwartya, Sinem Coleri Ergen, Jaime Lloret, and Naveed Ahmad

Guest Editorial
Special Issue on Toward Securing Internet of Connected Vehicles (IoV) 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 recent technologies in mobile communications, including WiFi, Bluetooth, 4G, and even 5G networks. The Internet of vehicles was aimed toward sustainable developments in transportation by enhancing safety and efficiency. The sensor-enabled intelligent automation of vehicles' mechanical operations enhances safety in on-road traveling, and cooperative traffic information sharing in vehicular networks improves traveling efficiency.

However, safety and efficiency oriented sustainability in transportation via Internet of Connected Vehicles (IoV) comes with greater risk of virtual vehicle hijacking, with examples ranging from unauthorized accessing of wheels, disabling brakes, locking doors, and engine disruption to path forging, location and identity manipulation, denial of traffic service, and tracking. We have witnessed security threats in computer networks in terms of unauthorized system and application hijacking on a greater scale targeting particular individuals, specific organizations, or even entire systems of a country. So there is also a necessity to prepare for a virtual vehicle hijacking in IoV, concerning the reliable, ubiquitous, and seamless IoV communication.

The literature on V2V and V2I-centric connected vehicles has vastly contributed toward efficient communication and analysis of accumulated traffic information leading toward optimization of fuel and time in traveling, and enabling on-time smart mechanical decisions on roads, respectively. The need for communication-centric study on 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 the current IoV scenario, where virtual hijacking of connected vehicles is possible, the modeling and practice for securing connected vehicles has not gained enough attention from academia and industries focusing on smart technologies for greener transportation.

The aim of this special issue is to fill this gap, and create a forum for researchers and developers from academia and industries to publish their recent outcomes. The response to our Call for Papers on this special issue was satisfactory, with 20 submissions from around the globe. During the review process, each paper was assigned to and reviewed by at least three experts in the relevant areas, and with a rigorous two-round review process, we were able to accept seven excellent articles covering the scope of this special issue.

The paper "Novel Beamforming Approach for Secure Communication in UDN to Maximize Secrecy Rate and Fairness Security Assessment" by Chopra *et al.* examines the security challenges of high-speed users for ultradense network (UDN) under dense picocells deployment. By considering a dense condition where users are randomly distributed within the picocell for vehicular users, the paper proposes beam broadening (BB) and beam merging (BM) techniques that ensure reliable transmission between source and destination, and proves the effectiveness of the proposed approach through mathematical and simulation analysis that guarantees high QoS and secure communication.

The paper "Dynamic Scalable Elliptic Curve Cryptographic Scheme and Its Application to In-Vehicle Security" by Wang *et al.* suggests a dynamic scalable elliptic curve cryptosystem. To synchronize the curve in use, a curve list of different security levels is generated and preserved on both parties. Since both parties randomly choose the curve and the prime number, an extra security level is provided, so that the security level can still remain the same even using smaller key sizes, while the computation efficiency will be enhanced and the power consumption will be reduced, which is especially suitable for application in on-board embedded devices.

The paper "On Location Privacy-Preserving Online Double Auction for Electric Vehicles in Microgrids" by Li *et al.* addresses the issue of demand response in microgrids via V2V technology in the smart grid with consideration for location privacy protection supported by Internet of Vehicles (IoV). The paper presents a new truthful online double auction scheme, which features multiunit energy trading among electric vehicles (EVs), routing optimization for EV charging, and location privacy protection. A theoretical analysis demonstrates that the online double auction scheme is capable of achieving several important economic properties as well as the privacy guarantee (i.e., *k*-anonymity).

The paper "TrustVote: Privacy-Preserving Node Ranking in Vehicular Networks" by Azad *et al.* presents TrustVote, a collaborative crowdsourcing-based vehicle reputation system that

Digital Object Identifier 10.1109/JIOT.2019.2926608

enables vehicles to evaluate the credibility of other vehicles in a connected vehicular network. The TrustVote system allows participating vehicles to hide their rating/feedback scores and the list of interacted vehicles under a homomorphic cryptographic layer, which can only be unfolded as an aggregate. The proposed approach also considers the trust weight of a vehicle providing the rating scores while computing the aggregate reputation of the vehicles. A prototype of TrustVote is developed and its performance is evaluated in terms of the computational and communication overheads.

The paper "Security in Vehicles With IoT by Prioritization Rules, Vehicle Certificates, and Trust Management" by García-Magariño *et al.* develops a novel agent-based simulator about security in IoT for V2V communications (ABS-SecIoTV2V). The experiments focus on the scenario of avoidance of collisions with hijacked vehicles misinforming other vehicles. The simulation results show that in the current approach, vehicles properly distinguished hijacked vehicles from others, by managing trust and reputation based on the information directly observed and that received from other vehicles. The simulation results also show that the current approach improved traffic flow performance as reflected in the increase of average speed of vehicles.

The paper "TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles" by Kerrache *et al.* proposes a trust-aware communication architecture for social IoV (TACASHI) to connect SIoVs and online social networks (OSNs) for the purpose of estimating the honesty of the drivers and passengers based on their OSN profiles. The authors compare the current location of the vehicles with their estimated path based on their historical mobility profile, then combine SIoV, path-based and OSN-based trusts to compute the overall trust for different vehicles and their current users. TACASHI offers a trust-aware social in-vehicle and intervehicle communication architecture for SIoVs considering also the drivers, honesty factor based on OSN.

The paper "Cybersecurity Measures for Geocasting in Vehicular Cyber Physical System Environments" by Kumar *et al.* presents cybersecurity measures for geocasting in vehicular traffic environments (CMGV) focusing on security-oriented vehicular connectivity. Specifically, a vehicular intrusion prevention technique is developed to measure the connectivity between the cache agent and cache user vehicles. The connectivity between static transport vehicles and cache agent/cache user is measured via vehicular intrusion detection approach. The performance of the proposed vehicular cybersecurity measure is evaluated in realistic traffic environments.

To conclude, the Guest Editors would like to thank all the authors for their contributions to this special issue, and all the reviewers for their excellent reviews. We also would like to give special thanks to Dr. Sherman Shen, the Editor-in-Chief of the IEEE INTERNET OF THINGS JOURNAL, and all the Journal's staff for their help in the publication process. We hope you will enjoy this special issue!

YUE CAO
School of Computing and Communications
Lancaster University
Lancaster, U.K.

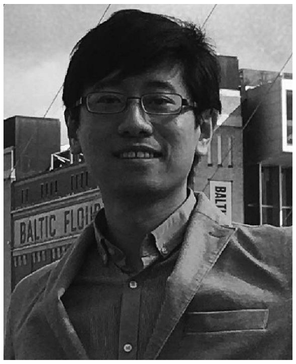
OMPRAKASH KAIWARTYA
School of Science and Technology
Nottingham Trent University
Nottingham, U.K.

SINEM COLERI ERGEN
Department of Electrical and Electronics Engineering
Koç University
Istanbul, Turkey

HOUBING SONG
Department of Electrical, Computer, Software, and Systems Engineering
Embry–Riddle Aeronautical University
Daytona Beach, FL, USA

JAIME LLORET
Department of Communications
Polytechnic University of Valencia,
Valencia, Spain

NAVEED AHMAD
Department of Computer Science
University of Peshawar
Peshawar, Pakistan



Yue Cao received the Ph.D. degree from the Institute for Communication Systems (ICS) (formerly, Centre for Communication Systems Research), University of Surrey, Guildford, U.K., in 2013.

He was a Research Fellow with ICS. Since 2017, he has been with the Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, U.K., and the School of Computing and Communications, Lancaster University, Lancashire, U.K. His current research interests include delay/disruption tolerant networks, electric vehicle charging management, autonomous driverless vehicle parking, and information centric networking.

Omprakash Kaiwartya (M'15) received the Ph.D. degree from the School of Computer and Systems Sciences, Jawaharlal Nehru University (JNU), New Delhi, India, in 2015.

He is currently a Post-Doctoral Research Fellow with the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia. He has been involved in funded projects related to communication protocols for vehicular ad-hoc networks (VANETs) and wireless sensor networks (WSNs), as a Key Researcher with UTM and JNU. His current research interests include Internet of Vehicles, electronic vehicles, VANETs, and WSNs.

Dr. Kaiwartya is serving as the Program Chair of ICACCT-2017 (Springer, New Delhi), the Session Chair of ICTUS-2017 (IEEE, UAE) and ICSNCS-2016 (Springer, India), and the Technical Program Committee Member in recent conferences, including CPSCom-2017 (IEEE, U.K.) and ICT-SPCS-2017 (IEEE, Malaysia). He has served as a Reviewer for a number of journals, including the IEEE INTERNET OF THINGS JOURNAL, IEEE SENSORS JOURNAL, IEEE ACCESS, the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, *Ad-Hoc Networks* (Elsevier), *Computer Communications*, and *Vehicular Communications*.

Sinem Coleri Ergen (S'98–M'05–SM'16) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2000, and the M.S. and Ph.D. degrees in electrical engineering and computer sciences from the University of California at Berkeley, Berkeley, CA, USA, in 2002 and 2005, respectively.

She was a Research Scientist with Wireless Sensor Networks Berkeley Laboratory under the sponsorship of Pirelli and Telecom Italia from 2006 to 2009. Since 2009, she has been a Faculty Member with the Department of Electrical and Electronics Engineering, Koç University, Istanbul, Turkey, where she is currently an Associate Professor. Her current research interests include wireless communications and networking with applications in machine-to-machine communication, sensor networks, and intelligent transportation systems.

Dr. Ergen was a recipient of the IEEE COMMUNICATIONS LETTERS Exemplary Editor Award, the Scientist of the Year Award in 2016 from Science Heroes Association, the Turkish Academy of Sciences Distinguished Young Scientist (TUBA-GEBIP) and Turkish Academic Fellowship Network—Outstanding Young Scientist Awards in 2015, the Science Academy Young Scientist (BAGEP) Award in 2014, the Turk Telekom Collaborative Research Award in 2011 and 2012, the Marie Curie Reintegration Grant in 2010, the Regents Fellowship from the University of California at Berkeley in 2000, and the Bilkent University Full Scholarship from Bilkent University in 1995. She has been an Editor of IEEE COMMUNICATIONS LETTERS since 2015, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY since 2016, and the IEEE TRANSACTIONS ON COMMUNICATIONS since 2017.

Houbing Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012.

In 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (www.SONGLab.us). He served on the faculty of West Virginia University, Morgantown, WV, USA, from 2012 to 2017. In 2007, he was an Engineering Research Associate with Texas A&M Transportation Institute, College Station, TX, USA. He has edited four books, including *Smart Cities: Foundations, Principles and Applications* (Hoboken, NJ, USA: Wiley, 2017), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications* (Chichester, U.K.: Wiley-IEEE Press, 2017), *Cyber-Physical Systems: Foundations, Principles and Applications* (Boston, MA, USA: Academic Press, 2016), and *Industrial Internet of Things: Cyber Manufacturing Systems* (Cham, Switzerland: Springer, 2016). He has authored over 100 articles. His current research interests include cyber-physical systems, Internet of Things, cloud computing, big data analytics, and wireless communications and networking.

Dr. Song serves as an Associate Technical Editor for *IEEE Communications Magazine*. He has served as a Guest Editor for over ten special issues within leading journals, including the IEEE INTERNET OF THINGS JOURNAL and the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He is a Senior Member of ACM.

Jaime Lloret (M'07–SM'10) received the B.Sc. + M.Sc. degree in physics and the B.Sc. + M.Sc. degree in electronic engineering from the University of Valencia, Valencia, Spain, in 1997 and 2003, respectively, and the Ph.D. degree in telecommunication engineering (Dr.Ing.) from the Polytechnic University of Valencia, Valencia, in 2006.

He is currently an Associate Professor with the Polytechnic University of Valencia, Valencia, Spain. He is the Chair of the Integrated Management Coastal Research Institute and the Head of the Active and Collaborative Techniques and Use of Technologic Resources in the Education (EITACURTE) Innovation Group. He is the Director of the University Diploma Redes y Comunicaciones de Ordenadores and the University Master Digital Post Production. He has authored 22 book chapters and has had over 360 research papers published in national and international conferences and international journals (over 140 with ISI Thomson JCR).

Dr. Lloret was the Internet Technical Committee Chair (the IEEE Communications Society and Internet Society) for the term 2013–2015. He has been the Co-Editor of 40 conference proceedings and the Guest Editor of several international books and journals. He is the Editor-in-Chief of *Ad Hoc and Sensor Wireless Networks* (with ISI Thomson Impact Factor), the international journal *Networks Protocols and Algorithms*, and the *International Journal of Multimedia Communications*, the IARIA Journals Board Chair (eight journals), and he is (or has been) an Associate Editor of 46 international journals (16 with ISI Thomson Impact Factor). He has been involved in over 320 program committees of international conferences, and over 130 organization and steering committees. He leads many national and international projects. He is currently the Chair of the Working Group of the Standard IEEE 1907.1. He has been the General Chair (or Co-Chair) of 39 international workshops and conferences. System to Recommend the Best Place to Live Based on Wellness State of the User Employing the Heart Rate Variability. He is an IARIA Fellow.

Naveed Ahmad received the Ph.D. degree from the Institute for Communication Systems (formerly, Centre for Communication Systems Research), University of Surrey, Guildford, U.K., in 2013.

He also served as a Research Assistant during his last year of Ph.D. tenure. He has been with the Department of Computer Science, University of Peshawar, Peshawar, Pakistan, as an Assistant Professor since 2013. He is supervising postgraduate students in addition to teaching Data Communication Network, Wireless Communication, and Network Security courses at the graduate and postgraduate level. He has coauthored over 15 academic papers. His current research interests include security and privacy issues in delay/disruption tolerant networks, vehicular ad hoc networks, and the Internet of Things enabled networks. Blockchain technologies and its applicability to IoT enabled networks is his recent research focus. He is part of the IoT hub at U.K. and closely working with the University of Surrey in IoT-related research topics.

Dr. Ahmad served as a Reviewer for a number of journals, including *IEEE Communication Magazine*, IEEE COMMUNICATIONS LETTERS, and the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.