IEEE Transactions on Intelligent Transportation Systems

Call For Papers

Special Issue on Deep Learning Models for Safe and Secure Intelligent Transportation Systems

MOTIVATION AND SCOPE

Autonomous vehicular technology is approaching a level of maturity that gives confidence to the end users in many cities around the world for their usage so as to share the roads with manual vehicles. Autonomous and manual vehicles have different capabilities which may result in surprising safety, security and resilience impacts when mixed together as a part of Intelligent Transportation System (ITS). For example, autonomous vehicles are able to communicate electronically with one another, make fast decisions and associated actuation, and generally act deterministically. In contrast, manual vehicles cannot communicate electronically, are limited by the capabilities and slow reaction of human drivers, and may show some uncertainty and even irrationality in behavior due to the involvement of human. At the same time, humans can react properly to more complex situations than autonomous vehicles. Unlike manual vehicles, the security of computing and communications of autonomous vehicles can be compromised thereby precluding them from achieving individual or group goals. Given the expected mixture of autonomous and manual vehicles that is expected to persist for many decades, safety and security issues for a mixture of autonomous and manual vehicles are crucial to investigate before autonomous vehicles enter our roadways in numbers. To improve the safety and security of the transportation system, the artificial intelligence (AI) based techniques and deep learning models have extensively been applied to data-driven ITS model. Despite the pioneering works on the integration of ITS data with deep learning techniques, such techniques still require more accurate perception since the false positives generated during the execution of the algorithms can perturb the utility real-time data analytics particularly for safety applications in ITS. More importantly, the recent breakthrough in generative adversarial networks in machine learning better demonstrates the criticality of the safety problems in ITS in the presence of advanced persistent threats as that adversarial models can be generated at an accelerating pace. Therefore, it is crucial to understand how both types of vehicles will fare in terms of safety (avoidance of dangerous situations), performance (acceptable delays and throughput), and resilience (fast recovery from dangerous situations) under a variety of uncertain situations without and with attacks on autonomous vehicle communications in in the presence of hidden advertises who exploit machine learning security loop holes. Despite the existing research on cyber-attacks on the functions of individual vehicles, the focus on the interplay of different types of vehicles under the influence of cyber-adversaries is missing. To address the above-mentioned challenges, there is a need for new algorithmic developments beyond traditional topics in big data, deep neural networks, and cyber security. The aim of this special issue is to provide a multi-aspect up-to-date reference for theoretical development of deep learning models and techniques for improving security and safety in ITS.

LIST OF TOPICS: Topics of interest to this special issue include, but are not limited to:

1. Deep learning based security, integrity and privacy solutions for ITS.
2. Deep learning based energy-aware traffic management solutions
3. Deep learning based 5G communication for ITS
4. Deep learning based physical layer design techniques for autonomous vehicles
5. Deep learning based object detection for autonomous vehicles
6. Deep learning based SDN-enabled network management for ITS
7. Deep learning based intrusion detection/prevention techniques
8. Low power based deep learning techniques for autonomous vehicles
9. Trusted machine/deep learning for ITS
10. Security hardening of ITS
11. Artificial intelligence for the integration of communications and sensing in ITS
12. Deep learning models for trusted ITS
13. Artificial intelligence safety for ITS
14. Explainable artificial intelligence for ITS
15. Explainable decision making for autonomous vehicles operating in uncertain and evolving environments
16. Optimizing safety and security of ITS using Artificial intelligence
17. Deep learning models for resilient ITS
18. Innovative deep learning techniques for attacks detection, prevention, and mitigation in ITS
19. Nature-inspired artificial intelligence for ITS

PAPER SUBMISSION GUIDELINES

Paper submission should conform to the information for authors available at https://mc.manuscriptcentral.com/t-its.

IMPORTANT DATES

First submission deadline: May 30, 2020
Notification of first decision: August 30, 2020
First revision submission deadline: October 30, 2020
Notification of final decision: February 30, 2021
Final manuscript (camera ready) submission deadline: March 30, 2021
Issue of Publication: May 30, 2021

GUEST EDITORS

Alireza Jolfaei
Macquarie University, Sydney, Australia
alireza.jolfaei@mq.edu.au

Neeraj Kumar
Thapar Institute of Engineering and Technology, India
neeraj.kumar@thapar.edu

Min Chen
Huazhong University of Science and Technology, Wuhan, China
minchen@ieee.org

Krishna Kant
Temple University, Philadelphia, USA
kkant@temple.edu

Alireza Jolfaei received his Ph.D. degree in Applied Cryptography from Griffith University, Gold Coast, Australia. He is an Assistant Professor in Cyber Security at Macquarie University, Sydney, Australia. Prior to this appointment, he worked as an Assistant Professor at Federation University Australia and Temple University in Philadelphia, USA. His current research areas include cyber security of industrial automation and control systems and cyber physical systems. He has authored over 50 peer-reviewed articles on topics related to cyber security. He has received multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He received the prestigious IEEE Australian council award for his research paper published in the IEEE Transactions on Information Forensics and Security. He received a recognition diploma with cash award from the IEEE Industrial Electronics Society for his publication at the 2019 IEEE IES International Conference on Industrial Technology. He is a founding member of IEEE Northern Territory Section and Federation University IEEE Student Branch. He served as a Chairman of Computational Intelligence Society in IEEE Victoria Section and as a Chairman of Professional and Career Activities for IEEE Queensland Section. He has served as a guest associate editor in IEEE journals and transactions, including IEEE IoT Journal and IEEE Transactions on Industrial Applications. He has served over 10 conferences in leadership capacities including program co-Chair, track Chair, session Chair, and Technical Program Committee member, including IEEE TrustCom and DependSys. He is a Senior Member of the IEEE.

Neeraj Kumar (SM'17) received his Ph.D. in CSE from Shri Mata Vaishno Devi University, Katra (Jammu and Kashmir), India in 2009, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala (Pb.), India. He has published more than 300 technical research papers in top-cited journals such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS, IEEE SG, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE SJ, Computer Networks, Information sciences, FGCS, JNCA, JPDC and ComCom. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. His research is supported by funding from UGC, DST, CSIR, and TCS. He is an Associate Technical Editor of IEEE Communication Magazine, IEEE Network Magazine. He is an Associate Editor of IJCS, Wiley, JNCA, Elsevier, Elsevier Computer Communications, and Security and Communication, Wiley. He has been a guest editor of various International Journals of repute such as - IEEE Access, IEEE Communication Magazine, IEEE Network Magazine, Computer Networks, Elsevier, Future Generation Computer Systems, Elsevier, Journal of Medical Systems. Springer, Computer and Electrical Engineering, Elsevier, Mobile Information Systems, International Journal of Ad hoc and Ubiquitous Computing, Telecommunication Systems, Springer and Journal of Supercomputing, Springer. He has been a workshop chair at IEEE Globecom 2018 and IEEE ICC 2019 and TPC Chair and member for various International conferences. He is senior member of the IEEE. He has more than 6200 citations to his credit with current h-index of 42. He has won the best papers award from IEEE Systems Journal and ICC 2018, Kansas city in 2018. He has edited more than 10 journals special issues of repute and published four books from CRC, Springer, IET UK, and BPB publications. He is visiting research fellow at Coventry University, Newcastle University, UK.

Min Chen (SM'09) is a full professor in School of Computer Science and Technology at Huazhong University of Science and Technology (HUST) since Feb. 2012. He is the director of Embedded and Pervasive Computing (EPIC) Lab at HUST. He is Chair of IEEE Computer Society (CS) Special Technical Communities (STC) on Big Data. He was an assistant professor in School of Computer Science and Engineering at Seoul National University (SNU). He worked as a Post-Doctoral Fellow in Department of Electrical and Computer Engineering at University of British Columbia (UBC) for three years. Before joining UBC, he was a Post-Doctoral Fellow at SNU for one and half years. He received

Best Paper Award from QShine 2008, IEEE ICC 2012, ICST IndustrialIoT 2016, and IEEE IWCMC 2016. He serves as editor or associate editor for Information Sciences, Information Fusion, and IEEE Access, etc. He is a Guest Editor for IEEE Network, IEEE Wireless Communications, and IEEE Trans. Service Computing, etc. He is Co-Chair of IEEE ICC 2012-Communications Theory Symposium, and Co-Chair of IEEE ICC 2013-Wireless Networks Symposium. He is General Co-Chair for IEEE CIT-2012, Tridentcom 2014, Mobimedia 2015, and Tridentcom 2017. He is Keynote Speaker for CyberC 2012, Mobiquitous 2012, Cloudcomp 2015, IndustrialIoT 2016, Tridentcom 2017 and The 7th Brainstorming Workshop on 5G Wireless. He has more than 300 paper publications, including 200+ SCI papers, 80+ IEEE Trans./Journal papers, 18 ISI highly cited papers and 8 hot papers. He has published eight books: OPNET IoT Simulation (2015), Big Data Inspiration (2015), 5G Software Defined Networks (2016) and Introduction to Cognitive Computing (2017) with HUST Presss, Big Data: Related Technologies, Challenges and Future Prospects (2014) and Cloud Based 5G Wireless Networks (2016) with Springer, Cognitive Computing and Deep Learning (2018) with China Machine Press, and Big Data Analytics for Cloud/IoT and Cognitive Computing (2017) with Wiley. His Google Scholars Citations reached 17,500+ with an h-index of 65. His top paper was cited 2000+ times. He is an IEEE Senior Member since 2009. He got IEEE Communications Society Fred W. Ellersick Prize in 2017. He was selected as Highly Cited Researcher at 2018. His research focuses on Cyber Physical Systems, IoT Sensing, 5G Networks, Mobile Cloud Computing, SDN, Healthcare Big Data, Media Cloud Privacy and Security, Body Area Networks, Emotion Communications and Robotics, etc.

Krishna Kant received his Ph.D. degree in Mathematical Sciences from University of Texas at Dallas in 1981. He is currently a professor in the Computer and Information Science Department at Temple University in Philadelphia, PA where he directs the IUCRC center on Intelligent Storage. Earlier he was a research professor in the Center for Secure Information Systems (CSIS) at George Mason University. From 2008-2013 he served as a program director at NSF where he managed the computer systems research (CSR) program and was instrumental in the development and running of NSF-wide sustainability initiative called SEES (science, engineering and education for sustainability). Prior to NSF, he served in industry for 18 years (at Intel, Bellcore, and Bell Labs) and 10 years in academia (at Penn State and Northwestern Univ.). He carries a combined 40 years of experience in academia, industry, and government. He has published in a wide variety of areas in computer science, authored a graduate textbook on performance modeling of computer systems. His research interests span a wide range including security, privacy preserving, energy efficiency, and robustness in cyber and cyber physical systems. He is a Fellow of IEEE.

SUBMISSION AND REVIEW OF PAPERS

Submitted papers should be original and not be under consideration elsewhere for publication. The authors should follow the journal guidelines, regarding the manuscript content and its format when preparing their manuscripts. All papers will be reviewed by at least three independent reviewers for their suitability in terms of technical novelty, scientific rigor, scope, and relevance to this special issue