Editorial
Special Issue on Application of Advanced Intelligent Methods in Vehicle to Smart Grid Communications: Security, Reliability, and Resiliency

THIS Special Issue was organized on the application of advanced intelligent methods in vehicle-to-smart grid communications considering the security, reliability, and resiliency perspectives. We tried to bring together the ideas from researchers and experts on both transportation and smart grid areas to tackle the technological challenges in future power systems with more electric vehicles and intelligent systems. Theoretically, vehicles consist of different electrical and electronic hardware devices, which are connected with each other through the so-called ECUs being controlled by different software tools. As a well-perceived technology, all sensing instruments located at different points in an electric vehicle will direct their data to the ECU, wherein these data are analyzed and processed, and the demanding orders are sent to the pertinent actuators. With the advance of automobile technology, the electric vehicles are not only an electric load consumer anymore, but are appearing at different parts of human life, ranging from the smart homes and smart buildings to smart grid and smart cities. Owing to the complex and interconnected cyber-physical nature of electric vehicles, they can are getting a more appealing and accessible target for cyber hackers to penetrate the entire system through car hacking. This can result in long-term effects on the security and privacy of the electric vehicle owners, smart buildings, smart grids, and smart cities of the future. Be on that, this Special Issue scope includes methods, tools, applications, and solutions for analyzing, processing, and improving the electric vehicles as a complex cyber-physical system considering its direct or indirect effects on the modern human life factors. Among the high number of submissions received, 13 articles were finally chosen to be published in this Special Issue. The core ideas and concepts of the works are summarized in the rest.

In [A1], Yamany et al. introduced a new optimal Quantum-based Federated Learning (OQFL) model to regulate the hyperparameters in the federated learning deploying different adversarial penetrations. The model performance is compared with MINST and Fashion-MINST, in Autonomous Vehicles.

In [A2], Diao et al. suggested a novel prediction model of spatial–temporal neural network to enhance the cyber security. The new attention tool resolves the cycle offset concerns by mining data before and after the predicted time period and effectively aligning the data.

In [A3], Zhang et al. introduced a secure management structure for the optimal management of energy systems within the smart cities. Different technologies including the vehicle-to-subway (V2S) and vehicle-to-grid (V2G) concepts are simulated for managing the energy system.

In [A4], Alyami et al. develop two flexibility indices to examine the performance of controllable loads in smart houses. The first index measures the capability of controllable loads to help the EV charging intervals throughout the process. The other one measures the capability of controllable load to use the PV power throughout its working.

In [A5], Yang et al. have focused on the minimization of AoI within the smart vehicular systems to mitigate the possible cyber attacks. It is suggested that the Stackelberg game can provide a suitable perspective to analyze and solve this problem.

In [A6], a novel penalty-based encryption approach is devised by Wang et al. to preserve the security of each message launched by a vehicle or station. The proposed method is cryptosystem mixing belief propagation and vibrational message process.

In [A7], Ahmed et al. suggest a strategic co-balancing dynamic solution to map sensor data and vehicles within the data centers performance. Moreover, a packet-level hacking detection approach is proposed based on entropy active learning which helps to detect and avoid any malicious activity.

In [A8], Abbasi et al. devise a 3-D could-based processing and learning focusing on progress, enhancement, and performance for the autonomous vehicle system. They have tried to make a survey on the current technologies on detection sensors and suggest the options which would make them safer and more optimal in autonomous vehicles.

In [A9], Kumar et al. present an agreement-induced data verification approach for making vehicular communication safe against any intrusion. Their model reveals around 10%

Digital Object Identifier 10.1109/TITS.2022.3230580

1558-0016 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

success ratio to make the inter communications among the vehicles secured.

In [A10], Li et al. introduce a new cooperation-based graph solution for traffic signal control to mitigate the delay and high energy usage in the system. The k-th order neighborhood idea is borrowed to help the intersection traffic management and thus optimal performance of the transportation system.

In [A11], Oseni et al. suggest an explainable deep-learning model for detecting the cyber hacking in the IoT-based environments. Also, a so-called SHapley Additive exPlanations is deployed to clarify and take decision on the final outcomes.

In [A12], Kumar et al. devise a reasoning structure to monitor and manage the road-based ITS utilizing a spatio-temporal event and deep learning model. Any malicious behavior would be detected based on the domain knowledge and the data gathered by the cameras.

In [A13], Wang et al. deployed blockchain concept to make data transactions secure within a smart grid in the presence of renewable energy sources and electric vehicles. Moreover, the feeder reconfiguration effect is assessed on the energy management of the system and charging and discharging process of the electric vehicles.

ABDOLLAH KAVOUSIFARD, *Guest Editor*
Electrical and Electronic Engineering Department
Shiraz University of Technology
7194684334 Shiraz, Iran
e-mail: kavousi@sutech.ac.ir

APPENDIX: RELATED ARTICLES

[A1] W. Yamany, N. Moustafa, and B. Turnbull, "OQFL: An optimized quantum-based federated learning framework for defending against adversarial attacks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 7, 2021, doi: 10.1109/TITS.2021.3130906.

[A2] C. Diao, D. Zhang, W. Liang, K.-C. Li, Y. Hong, and J.-L. Gaudiot, "A novel spatial–temporal multi-scale alignment graph neural network security model for vehicles prediction," *IEEE Trans. Intell. Transp. Syst.*, early access, Jan. 19, 2022, doi: 10.1109/TITS.2022.3140229.

[A3] L. Zhang, L. Cheng, F. Alsokhiry, and M. A. Mohamed, "A novel stochastic blockchain-based energy management in smart cities using V2S and V2G," *IEEE Trans. Intell. Transp. Syst.*, early access, Jan. 22, 2022, doi: 10.1109/TITS.2022.3143146.

[A4] S. Alyami, A. Almutairi, and O. Alrumayh, "Novel flexibility indices of controllable loads in relation to EV and rooftop PV," *IEEE Trans. Intell. Transp. Syst.*, early access, Feb. 8, 2022, doi: 10.1109/TITS.2022.3146237.

[A5] Y. Yang, W. Wang, L. Liu, K. Dev, and N. M. F. Qureshi, "AoI optimization in the UAV-aided traffic monitoring network under attack: A Stackelberg game viewpoint," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 22, 2022, doi: 10.1109/TITS.2022.3157394.

[A6] Z. Wang, S. Wang, M. Z. A. Bhuiyan, J. Xu, and Y. Hu, "Cooperative location-sensing network based on vehicular communication security against attacks," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 28, 2022, doi: 10.1109/TITS.2022.3160453.

[A7] U. Ahmed, J. C.-W. Lin, G. Srivastava, U. Yun, and A. K. Singh, "Deep active learning intrusion detection and load balancing in software-defined vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Apr. 27, 2022, doi: 10.1109/TITS.2022.3166864.

[A8] R. Abbasi, A. K. Bashir, H. J. Alyamani, F. Amin, J. Doh, and J. Chen, "Lidar point cloud compression, processing and learning for autonomous driving," *IEEE Trans. Intell. Transp. Syst.*, early access, May 2, 2022, doi: 10.1109/TITS.2022.3167957.

[A9] P. M. Kumar, C. Konstantinou, S. Basheer, G. Manogaran, B. S. Rawal, and G. C. Babu, "Agreement-induced data verification model for securing vehicular communication in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 29, 2022, doi: 10.1109/TITS.2022.3191757.

[A10] W. Li, B. Wang, Z. H. Khattak, and X. Deng, "Network-level traffic signal cooperation: A higher-order conflict graph approach," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 1, 2022, doi: 10.1109/TITS.2022.3191290.

[A11] A. Oseni et al., "An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 14, 2022, doi: 10.1109/TITS.2022.3188671.

[A12] P. P. Kumar, K. Kant, and A. Pal, "C-FAR: A compositional framework for anomaly resolution in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 22, 2022, doi: 10.1109/TITS.2022.3196548.

[A13] B. Wang et al., "An IoT-enabled stochastic operation management framework for smart grids," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 21, 2022, doi: 10.1109/TITS.2022.3183327.