Journal of
Sensor and Actuator Networks

MDPI

Editorial

Machine Learning in IoT Networking and Communications

Mona Jaber

School of Electronic Engineering and Computer Science, Queen Mary University of London, Mile End Rd, London E1 4NS, UK; m.jaber@qmul.ac.uk

check for updates

Citation: Jaber, M. Machine Learning in IoT Networking and Communications. *J. Sens. Actuator Netw.* **2022**, *11*, 37. https://doi.org/10.3390/jsan11030037

Received: 15 July 2022
Accepted: 21 July 2022
Published: 29 July 2022

Introduction

The fast and wide spread of Internet of Things (IoT) applications offers new opportunities in multiple domains but also presents new challenges. A skyrocketing number of IoT devices (sensors, actuators, etc.) is deployed to collect critical data and to control environments such as manufacturing, healthcare, urban/built areas, and public safety. At the same time, machine learning (ML) has shown significant success in transforming heterogeneous and complex datasets into coherent output and actionable insights. Thus, the marriage of ML and IoT has a pivotal role in enabling smart environments with precision in decision-making and adaptive automation. However, leveraging ML and IoT still faces significant challenges, obstructing the full realisation of foreseen opportunities. Direct challenges relate to scalability, security, accessibility, resilience, and latency, all of which have resulted in a growing corpus of research addressing one or more of these issues. This Special Issue has attracted leading scholars in this area and offers a view of cutting-edge research centred on the intersection of networks, IoT, and ML.

The role of IoT in enabling a smart environment has become indisputable in key verticals that include *Energy*, *Transportation*, *Industrial application*, and *Supply Chain*. The authors of [1] examine the problem of residential energy demand management and the avoidance of collective peak demand. To this end, they use IoT, namely smart meters and appliances, and propose a reinforcement learning method based on a time-of-use tariff that reschedules electric appliances to avoid peak energy demands and, therefore, reduce energy cost. In [2], the problem of road maintenance is investigated, and a solution that leverages IoT (camera-based in this case) to detect and prioritise road damage is proposed. The authors use deep learning (DL) computer vision to segment images and classify the types of damages detected as single cracks, crocodile cracks, and potholes. This information, together with the number of reported damages, is used to prioritise the road maintenance work to improve road safety and reduce emissions by addressing the most damaging road faults. Industrial applications, particularly the supply chain, are addressed in [3], where an IoT-based (in this case, Radio Frequency Identification (RFID)) solution is proposed to detect food or beverage contamination that may take place at the production phase or during the transportation of goods. An ensemble ML approach, XGBoost, is proposed to mine the RFID's received signal strength indicator (RSSI) and detect the presence and level of contamination. Jointly, these studies demonstrate the disruptive potential of merging IoT and ML to solve real-life problems. However, there are major challenges in the design and implementations of ML-based IoT solutions; these include *connectivity*, *security*, and *privacy*.

A dominant challenge in this area stems from the exponential increase in IoT devices and the resulting massive number of data generated. In this context, the connectivity of the IoT devices is not a trivial problem when combined with the already crowded wireless and connected networks. This problem is examined from different angles in this Special Issue. The authors of [4] investigate indoor private networks that cater, among other usage, to the continuous monitoring of IoT devices, which causes network overload. In this regard, they propose an ML method for predicting the position of IoT devices and, therefore, reducing the need for continuous monitoring. Different ML methods are employed, including Random Forest and Artificial Neural Networks, which succeed in predicting the intermediate coordinates of the trajectories on the server-side without relevant data loss. On the other hand, the authors of [5] focus their study on the emerging narrow band NB-IoT radio access technology and propose a multi-objective dynamic configuration for the user equipment to achieve a combination of connectivity metrics including energy efficiency, reduced delay, and throughput. Towards this end, reinforcement learning utilising gradient descent and a genetic algorithm is adopted synchronously with ML and DL algorithms to predict the environmental states and suggest an optimal configuration. A review of intelligent communication systems that is centered on the role of ML is presented in [6] to address the challenge of IoT connectivity. In this work, the authors give an overview of the progress in standardisation including Open Radio Access Networks (O-RAN) and 3rd-Generation Partnership Project (3GPP). In this context, the role of the radio intelligent controller (RIC) in the operation and configuration of the O-RAN is discussed, as is the use of ML in its automation for enabling IoT connectivity. On the other hand, the NetWork Data Analytic Function (NWDAF) is examined in the context of 3GPP and the new related interfaces that allow for the implementation of ML and interoperability with the O-RAN. Leading pilot projects in the implementation of intelligent communication systems are surveyed and lessons learnt for IoT connectivity are highlighted.

Security is another overarching challenge that is amplified due to the massive number of IoT devices. The security risk is higher in the case of IoT devices, as these are often limited in computational power, memory, and access to energy sources. It follows that IoT devices are vulnerable to security threats, a challenge that is more pronounced in the case of devices installed in unprotected and/or remote locations and, hence, exposed to tampering. The authors of [7] propose an intrusion detection algorithm that detects malicious behaviour within low-power, low-rate, and short-range IoT networks. A support vector machine (SVM) method is designed that successfully monitors and detects abnormal activity within the smart IoT device. On the other hand, the authors of [8] propose detecting malware attacks in IoT networks using methods inspired by the human immune system. To this end, they present a survey of artificial immune systems (AIS) and draw a parallel between the advantages of AIS and the limitations of IoT devices and systems. Furthermore, a quantitative performance analysis of leading AIS methods in IoT malware detection is discussed in which the negative and positive detector system (NPS) is shown to outperform the state of the art.

IoT data privacy is a common concern that affects IoT applications in multiple verticals. Indeed, IoT devices are used for remote sensing and actuating in critical solutions including health, security, and autonomous things (e.g., vehicles, factories). Tampering with data measured and communicated through the IoT puts at risk the privacy of the owner of the data, such as the identity of people using e-health solutions, private information of people captured by security cameras, or enabling targeted tampering using remote actuators. This Special Issue addresses concerns for data privacy in two leading works. The first [9] proposes a countermeasure to the risk of statistical traffic analysis that allows attackers to infer users' online activities. The paper puts forward a data obfuscation mechanism supported by a heuristic algorithm that selects the applications to mutate to and therefore reduces the accuracy of user activity classification to 1.42%. In the second work [1], the authors present a multi-layer digital twin system that allows for privacy-preserving coordination between the central energy provider and edge residential energy consumers. The design employs a smart home IoT gateway that receives dynamic time-of-use energy tariffs from the central server and, accordingly, orchestrates the usage of electric appliances at home. The orchestration aims at reducing the cost of energy whilst respecting preferences set by residents. On the other hand, the local transformer collects the collective energy consumption data of all households in the area and reports them to the central server, who then adjusts the time-of-use tariffs to nudge collective usage away from peak demand. The presented digital twin system succeeds in flattening the collective energy demand and reducing the cost of energy of households without exposing detailed household-specific energy consumption data.

In summary, this Special Issue presents cutting edge research that sits at the intersection of IoT and ML and addresses real-life problems. The articles presented jointly cover leading applications of IoT and ML methods that address dominant challenges, including connectivity, security, and privacy.

Funding: This editorial received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Fathy, Y.; Jaber, M.; Nadeem, Z. Digital Twin-Driven Decision Making and Planning for Energy Consumption. *J. Sens. Actuator Netw.* **2021**, *10*, 37. [CrossRef]
2. Salcedo, E.; Jaber, M.; Requena Carrión, J. A Novel Road Maintenance Prioritisation System Based on Computer Vision and Crowdsourced Reporting. *J. Sens. Actuator Netw.* **2022**, *11*, 15. [CrossRef]
3. Sharif, A.; Abbasi, Q.H.; Arshad, K.; Ansari, S.; Ali, M.Z.; Kaur, J.; Abbas, H.T.; Imran, M.A. Machine Learning Enabled Food Contamination Detection Using RFID and Internet of Things System. *J. Sens. Actuator Netw.* **2021**, *10*, 63. [CrossRef]
4. Carvalho, D.; Sullivan, D.; Almeida, R.; Caminha, C. A Machine Learning Approach to Solve the Network Overload Problem Caused by IoT Devices Spatially Tracked Indoors. *J. Sens. Actuator Netw.* **2022**, *11*, 29. [CrossRef]
5. Nassef, O.; Mahmoodi, T.; Michelinakis, F.; Mahmood, K.; Elmokashfi, A. Optimising Performance for NB-IoT UE Devices through Data Driven Models. *J. Sens. Actuator Netw.* **2021**, *10*, 21. [CrossRef]
6. Koufos, K.; EI Haloui, K.; Dianati, M.; Higgins, M.; Elmirghani, J.; Imran, M.A.; Tafazolli, R. Trends in Intelligent Communication Systems: Review of Standards, Major Research Projects, and Identification of Research Gaps. *J. Sens. Actuator Netw.* **2021**, *10*, 60. [CrossRef]
7. Ioannou, C.; Vassiliou, V. Network Attack Classification in IoT Using Support Vector Machines. *J. Sens. Actuator Netw.* **2021**, *10*, 58. [CrossRef]
8. Alrubayyi, H.; Goteng, G.; Jaber, M.; Kelly, J. Challenges of Malware Detection in the IoT and a Review of Artificial Immune System Approaches. *J. Sens. Actuator Netw.* **2021**, *10*, 61. [CrossRef]
9. Chaddad, L.; Chehab, A.; Kayssi, A. OPriv: Optimizing Privacy Protection for Network Traffic. *J. Sens. Actuator Netw.* **2021**, *10*, 38. [CrossRef]