Journal of Reliable Intelligent Environments (2018) 4:187
https://doi.org/10.1007/s40860-018-0071-4

EDITORIAL

Editorial

Antonio Coronato[2] · Juan Carlos Augusto[1]

Published online: 24 October 2018

This issue of the Journal of Reliable Intelligent Environments includes four papers, of which two are survey papers.

In particular, *A Survey on Verification Strategies for Intelligent Transportation Systems*, by Hedda R. Schmidtke reports an overview and classification of techniques for handling Intelligent Sensor Actuator Systems (ISAS) in terms of cyber-physical systems, intelligent autonomous robots, or intelligent agents. The study emphasizes that each of the three classical perspectives misses one important characteristic of ISAS and proposes to combine the three for a full solution. The study also argues that in particular, two mechanisms are promising: an intelligent environments perspective that verifies local safety and techniques for context-aware monitoring that allow a mobile system to leverage context awareness to reduce complexity for self-monitoring tasks.

User expectations in intelligent environments, by Fulvio Corno surveys and analyzes the recent literature of the IEs research community, aiming at highlighting to which extent users are taken into account, or are involved, into the reported research works. The paper shows that, while most articles refer to users in their description, only a small minority actually involve them in the design, testing, or experimentation phases.

A Novel Digital Twin-centric Approach for Driver-intention Prediction and Traffic Congestion-Avoidance, by Madhumathi Ramasamy presents a technological solution to reduce traffic congestions and related issues (e.g., the increasing number of incidents) by adopting accurate prediction methods. The technological framework includes a variety of tools and technologies such as software-defined cloud environments, digital twin, artificial intelligence algorithms (machine and deep learning algorithms), etc.

Experimenting and Assessing Machine Learning Tools for Detecting and Analyzing Malicious Behaviors in Complex Environments, by Alfredo Cuzzocrea, Fabio Martinelli, Francesco Mercaldo and Giorgio Mario Grasso reports on machine-learning technologies to face security issues in complex environments, specifically identifying and analyzing malicious behaviors. Authors refer to real-world case studies. To evaluate the effectiveness of algorithms to detect anomalies and demonstrate the effectiveness of machine learning in supporting security of complex environments.

We hope these articles stimulate the community to further improvements in this area and perhaps to collaborations between the participating teams, so that complementary solutions can be used in a combined way to tackle more complex problems.

✉ Antonio Coronato
antonio.coronato@icar.cnr.it

Juan Carlos Augusto
j.augusto@mdx.ac.uk

[1] Department of Computer Science, Research Group on Development of Intelligent Environments, Middlesex University, London, UK

[2] Institute for High Performance Computing and Networking, National Research Council, Naples, Italy