future internet

MDPI

Editorial

The Internet of Things for Smart Environments

Giuseppe Ruggeri [1], Valeria Loscrí [2], Marica Amadeo [1,*] and Carlos T. Calafate [3]

1 DIIES Department, University Mediterranea of Reggio Calabria, Via Graziella, Loc. Feo di Vito, 89100 Reggio Calabria, Italy; giuseppe.ruggeri@unirc.it
2 Inria Lille-Nord Europe/FUN, 59650 Villeneuve D'Ascq, France; valeria.loscri@inria.fr
3 Department of Computer Engineering (DISCA), Universitat Politècnica de València, 46022 València, Spain; calafate@disca.upv.es
* Correspondence: marica.amadeo@unirc.it; Tel.: +39-0965-1693276

Received: 5 March 2020; Accepted: 5 March 2020; Published: 14 March 2020

By leveraging the global interconnection of billions of tiny smart objects, the Internet of Things (IoT) paradigm is the main enabler of smart environments, ranging from smart cities to building automation, smart transportation, smart grids, and healthcare. However, despite the research advancements in recent years, many open issues still prevent the full realization of such a vision.

Today's communication systems hardly suit the connection of a huge number of (usually battery-powered and resources-constrained) IoT devices, including low-power sensors, actuators, smartphones, tablets and robots. When massively distributed into the environment, those devices may generate huge amounts of data, offer computational resources, and cooperate to perform some tasks locally, as well as delegate their execution to more powerful nodes. Such a complex ecosystem requires proper scalable management platforms able to dynamically discover, integrate and orchestrate the new IoT devices that might be introduced in the smart environment. New lightweight protocols that support security services such as authentication and data integrity must be devised. In addition to designs based on the IP protocol, such as CoAP/6LoWPAN, it is expected that novel future Internet networking paradigms, such as Information Centric Networking (ICN), will also play a key role in the deployment of IoT smart environments. Last but not least, middleware architectures, together with the cloud and the edge computing paradigms, will be crucial to deal with device heterogeneity, and to manage the huge amount of data generated by IoT sources.

In response to the call for papers, we received 11 submissions, and only six manuscripts have been accepted for publication.

The first paper, titled "RFID Based Embedded System for Sustainable Food Management in an IoT Network Paradigm", presents a RFID (radio frequency identification) food management system that prevents food waste. It consists of two main components: *(i)* RFID readers placed on the user's kitchen furniture, which automatically read food information, and *(ii)* a multi-platform web application, which allows its users to check food information, including the date of expiration. The application notifies the user when a product is about to expire, and offers recipes that might be prepared with available foods.

The second paper, titled "Fog Computing in IoT Smart Environments via Named Data Networking: A Study on Service Orchestration Mechanisms", shows how the novel Information-Centric architecture called Named Data Networking (NDN) is an effective enabler of edge computing services. With focus on a smart campus scenario, an NDN-based fog computing framework is designed, where the execution of IoT services is dynamically orchestrated and performed by nodes in a distributed fashion.

The third paper, titled "Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment", studies the security requirements in IoT device-to-device (D2D) communication. A novel authentication approach called Secure Key Exchange with QR Code (SeKeQ) is proposed that verifies user identity by ensuring an automatic key comparison, and providing a shared secret key using Diffie-Hellman key agreement with an SHA-256 hash.

The next paper, titled "WLAN Aware Cognitive Medium Access Control Protocol for IoT Applications" focuses on energy issues in the presence of IEEE 802.15.4-compliant Wireless Sensor Networks (WSN), which are subject to interference caused by high-powered IEEE 802.11-compliant Wireless Local Area Network (WLAN) users. A WLAN Aware Cognitive Medium Access Control (WAC-MAC) protocol is proposed that reduces interference by leveraging energy detection based sensing, adaptive wake-up scheduling, and adaptive backoff.

The next paper, titled "MCCM: An Approach for Connectivity and Coverage Maximization" considers the problem of maximizing connectivity and coverage in the presence of movable IoT devices. A low complexity algorithm is proposed that keeps the movement of devices as minimal as possible to save energy, and reduces the overlapping areas covered by different devices to increase the coverage while maintaining connectivity.

The last paper, titled "EAOA: Energy-Aware Grid-Based 3D-Obstacle Avoidance in Coverage Path Planning for UAVs", focuses on the problem of avoiding obstacles in the presence of Unmanned Aerial Vehicle (UAV) flight missions. An energy-aware grid based solution for obstacle avoidance is proposed, which first generates a trajectory path offline using the area top-view. Then, based on the frontal view from the camera on board of the drone, the algorithm determines the new position where the drone has to move to, in order to bypass the obstacle.

Acknowledgments: We thank all the authors for submitting their work to this special issue. We also thank all the reviewers, who contributed to improve the quality of the papers through their valuable comments and suggestions. We are extremely grateful to Dino Giuli, Editor-in-Chief of Future Internet, for giving us the possibility of serving the community with this special issue, and to Jingjing Lu, the managing Editor of this special issue.

Conflicts of Interest: The authors declare no conflict of interest.