Editorial

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2017, Vol. 13(9)

DOI: 10.1177/1550147717732446
journals.sagepub.com/home/ijdsn
SAGE

Edge computing in the Internet of Things

The Internet of Things (IoT) is envisioned to significantly enhance the quality of life and socio-economic efficiency and effectiveness by supporting numerous applications, such as smart home, smart city, smart grids, mobile health, connected cars, and smart transportation that leverage deeply embedded IoT devices (called things). However, IoT devices often lack enough resources to perform compute-intensive tasks such as big sensor data analytics for detecting important events, for example, traffic congestion and anomalous state of power grids. A naive approach is for each IoT device to upload all sensor data to cloud to perform compute-intensive tasks and data analytics. However, this approach is not applicable to IoT applications with real-time constraints, such as smart transportation, electric grid management, or surveillance for public safety. Even if an IoT application does not have stringent timing constraints, uploading all big sensor data to cloud imposes huge burden on the Internet with the limited upload bandwidth. A promising emerging technology that can address this challenge is edge computing (also called fog computing), where compute resources are pushed to and made available at the edge of the Internet. For instance, a cloudlet (a datacenter in a box) at the network edge may perform extensive data analytics and only uploads the value-added information derived from sensor data to the cloud. By supporting compute-intensive services (e.g. big sensor data analytics, computer vision/image processing, or data security/privacy measures) near sensors, edge computing can significantly alleviate the latency and bandwidth concerns, while enhancing the quality and availability of service.

This issue of the journal is devoted to recent research advances in IoT and edge computing. The papers accepted through the rigorous review process provide a broad perspective on IoT, namely, visual sensor networks, power storage, situation awareness, routing based on data priorities, lightweight cipher for radio-frequency identification (RFID) systems, and malware detection in IoT. Fanhuai Shi, Jian Gao, and Xixia Huang in "An affine invariant approach for dense wide baseline image matching" present an affine invariant method to perform dense wide baseline image matching in visual sensor networks that enables distributed intelligent applications, such as three-dimensional (3D) reconstruction, camera calibration, motion prediction, and image stitching. The major contribution is a sparse-to-dense framework for image matching, which (1) produces reliable sparse matches with feature points extracted by Hessian-based detector, (2) incorporates region growing for match propagation in dense matching, and (3) reconstructs complete dense matching results with low-rank matrix recovery techniques on unmatched points.

Jianwen Xu, Ping Yi, Wei Wang, and Ting Zhu in "A power storage station placement algorithm for power distribution based on electric vehicle" propose a novel algorithm to assist in the placement of power stations for electric vehicles. The problem tackled in this paper is key in smart cities wherein electric vehicles tend to become more prominent. The authors raise important questions which are left as subjects for future work. Could we use buses to replace the power distribution system of a city? According to the authors, in the near future, the answer is negative, as their feasibility study indicates that thousands of buses would be needed to cope with the demand of small cities. For this reason, the authors conclude that a static grid system between power plants and power stations will still be needed in the foreseen future, and buses equipped with batteries will help to distribute energy from power stations to end users.

Johannes Ehala, Jaanus Kaugerand, Raido Pahtma, Sergei Astapov, Andri Riid, Timo Tomson, Jürgo-Sören Preden, and Leo Mõtus in "Situation awareness via Internet of things and in-network data processing" propose a new design of a wireless sensor network (WSN) that combines data-to-decision (D2D) and mist computing. The proposed WSN is more flexible than traditional ones since the data flow is more flexible. The data are identified and sent to the nodes that are interested in the data. Also, the computation could take place at the server or the edge nodes depending on the situation. This decentralized WSN is more robust since it can still work if the cloud server is attacked.

Furthermore, the nodes in this WSN can get the required data more rapidly. With the above advantages, the proposed WSN is suitable for intelligence, surveillance, and reconnaissance (ISR).

Liansheng Lu, Haifeng Jiang, Guangzhi Han, Shanshan Ma, and Renke Sun in "Multi-criteria routing metric for supporting data-differentiated service in hybrid wireless mesh networks in coal mines" present a routing metric for hybrid wireless mesh networks in coal mines by considering the priorities of end-to-end data. The key contribution has three parts: (1) the data labeled as urgent is optimized to low end-to-end delay, (2) the non-urgent data is optimized to reduce the mesh clients utilization, and (3) this metric satisfies the differentiated service requirements and prolongs the network lifetime in coal mines.

Shiyong Zhang, Gongliang Chen in "Micro-Trivium: A lightweight algorithm designed for radio frequency identification systems" propose an extension to the classical trivium security algorithm to guarantee the feasibility of its deployment in RFID systems. The authors show that the proposed solution consumes less power and has a smaller chip size compared to the classical trivium solution. As the trivium cipher is designed to provide a flexible trade-off between speed and hardware footprint, this paper is a fundamental contribution in the realm of lightweight ciphers.

Futai Zou, Siyu Zhang, Linsen Li, Li Pan, Jianhua Li in "Detecting malware based on expired command-and-control traffic" study heartbeat traffic generated by command-and-control malware. They observe that such traffic tends to be very periodic and can be easily detected using simple filters. In particular, the authors indicate that the presence of period requests targeting non-existing (expired) domains is a strong evidence of security holes. Although by the time of the submission of this paper, the HeartBleed Bug has not been reported yet, it is worth pointing out that expired domains played an important role in such an incident, indicating the wide applicability of the results presented in this paper.

We hope readers will enjoy the papers in this issue, which provides timely, interesting research outcomes. Moreover, we hope the papers will help readers find directions for research in the exiting area of IoT and edge computing.

Kyoung-Don Kang[1], Daniel Sadoc Menasche[2], Gürhan Küçük[3], Ting Zhu[4] and Ping Yi[5]
[1]Binghamton University, Binghamton, NY, USA
[2]Federal University of Rio de Janeiro, Brazil
[3]Yeditepe University, Istanbul, Turkey
[4]University of Maryland, Baltimore County, USA
[5]Shanghai Jiaotong University, China