symmetry

MDPI

Editorial

Advances in Future Internet and the Industrial Internet of Things

Jong Hyuk Park

Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul 01811, Korea; jhpark1@seoultech.ac.kr

Received: 31 January 2019; Accepted: 31 January 2019; Published: 16 February 2019

Abstract: After the emergence of the Internet and mobile communication networks, the IoT has been considered as the third wave of information technology. The Industrial Internet of Things (IIoT) is the use of Internet of Things (IoT) technologies in manufacturing. IIoT incorporates machine learning and big data technology, sensor data, and machine-to-machine (M2M) communications that have existed in industrial areas for years. In the future, people and objects will be connected at any time, any place, with anything and anyone and will utilize any network and services. IIoT is creating a new world in which people and businesses can manage their assets in more informed ways and can make more opportune and better-informed decisions. Many advanced IIoT and 5G technologies have been successfully applied in everyday life, but there are still many practical problems tackled by traditional methods which are generally difficult to experimentally solve in the advanced Industrial Internet of Things. Therefore, in this special issue, we accepted five articles in three different dimensions: communication networks, optimized resource provisioning and data forwarding, privacy and security.

Keywords: Industrial Internet of Things; security and privacy; smart city; smart home; machine-to-machine communications

1. Introduction

Currently, organizations are able to collect and analyze large amounts of data more quickly than before by adopting smart, connected devices. The integration of the Industrial Internet of Things (IIoT) improves performance, scalability and narrows the gap between users, giving industry companies a clearer view of how their operations are evolving and helping them to improve their business. The basic philosophy of the Internet of Things (IoT) is that intelligent machines are more efficient than humans in capturing and communicating data accurately and consistently. These data can give companies the means to identify inefficiencies and opportunities, and save time and money. Many manufacturers have made great strides in connecting their products and devices to IoT. However, to succeed at this stage requires much more than technological connectivity. In fact, the advent of IoT is a unique disruption of business which requires new capabilities and will offer incredible opportunities. For manufacturers, the IIoT holds considerable potential, especially in terms of the quality control and traceability of the supply chain.

The adoption of IIoT can revolutionize the way industries operate, but the challenge is to put strategies in place to strengthen digital transformation efforts while maintaining security through increased connectivity. The three major areas we need to focus on are scalability, security, and availability. The proliferation of smart devices has created vulnerabilities and security issues. IoT users have the de facto responsibility to secure the configuration and use of their connected devices, but device manufacturers have an obligation to protect their consumers when launching their products. Manufacturers should be able to guarantee the safety of users and provide for preventive or corrective

measures when safety concerns arise. Furthermore, the need for cybersecurity has been highlighted as larger security incidents have surfaced over the years. Hackers accessing connected systems not only expose a company to a major breach, but also potentially subject the operations to a shutdown. To some extent, industries and businesses that adopt IIoT must plan and operate as technology companies to safely manage physical and digital components.

This special issue covers pure research and applications within novel scopes related to IIoT, such as future Internet, 5G smart networks, cloud computing, and mobile technologies based on IIoT. In addition, it deals with hardware/software technologies, new frameworks and architectures, efficient data processing in IIoT, specific mathematical models, and designs for theories for the future Internet.

2. Advances in Future Internet and the Industrial Internet of Things

In this special issue, 'Advances in Future Internet and the Industrial Internet of Things' are presented in the five accepted articles [1–5]. All accepted articles are categorized into three different dimensions: communication networks, optimized resource provisioning and data forwarding, privacy and security.

In the communication network dimension, Cho S. [1] proposed an automatic modulation and coding scheme level adaptation algorithm using signal to interference plus noise ratios (SINRs) of acknowledgment (ACK) frames in carrier-sense multiple access with collision avoidance (CSMA/CA) wireless networks to accommodate the expected high density of IoT devices in CSMA/CA wireless networks. The proposed algorithm operates on the basis of information from normal ACK frames of institute of electrical and electronics engineers (IEEE) 802.11 standards without modification of the existing CSMA/CA mechanism. They also showed the effectiveness of the algorithm proposed in the simulation results. The results showed that the proposed algorithm uses the IEEE 802.11a wireless network resources almost as efficiently as the highest modulation and coding scheme (MCS) level of a given MCS scheme for various combinations of Poisson point processes densities of access points and wireless devices.

Two articles were accepted which aimed to optimize resource provisioning and data forwarding. Zhao et al. [2] presented the advantages of graph symmetry and extended it to the field of incorporation into the network. They conducted a theoretical analysis and a series of simulation studies on the advantages of the characteristics of intermediate structures, improving the computational efficiency of the virtual network embedding (VNE) process, and the static agency network modeled with such intermediate structures improved the quality of the VNE process. In future network architectures, in order to solve the problem of ossification, VNE will be a relatively important element of network virtualization technology and a promising approach. Recently, the uncertain quality of heuristic algorithms and the computational complexity of optimization-based approaches have led to a great deal of research. In their research, they found that the current algorithms of VNE lacked stability, which interested them in future work.

Furthermore, inefficient data transmission can cause significant personal and property loss, which is a major challenge in IIoT. Even though there is some related research on end-to-end tracking, when tracking a constantly moving mobile target, sensing data should be delivered to sinks continuously and quickly. A system for transmitting detection data through a fast-reacted routing trajectory that can effectively reduce delays is proposed by Zhou et al. [3]. To reduce tracking delay and maintain a long lifetime of sensor networks, a fast and efficient data forwarding scheme for mobile tracking targets is essential. The proposed scheme transmits sensing data via a fast-reaction routing path, which effectively reduces delays. In addition, they also proposed a technique to be able to quickly and efficiently optimize their routing to make the path work more efficiently. The proposed scheme reduced communication delay by 87.4%, improved network energy utilization by 2.65% over the traditional routing scheme, and provided an extended network life.

Finally, two articles were accepted in the privacy and security dimension. To provide customers with convenience and improve their quality of life, many gadgets and services include innovative IoT technologies. Smart TVs are one of the classic IoT devices that offer broadcast services, but are prone to security intrusions via email, media players, cameras, and Internet connectivity. Appropriate

countermeasures are needed because of the increased hacking frequency via malicious apps installed in smart TVs. In addition, because of the proximity of smart TVs to users, security and reliability have become critical factors. When hacking a smart TV, sensitive user information may be disclosed and an invasion of privacy may occur because smart TVs are connected to the Internet and have cameras. To solve these problems, Kang et al. [4] presented the world's first common criteria evaluation assurance level 2 certification for smart TVs. They discussed their experience with the certification process and examined several aspects of smart TV security and reliability. In future work, they will work to provide a single integrated security platform that can be applied to other home appliances.

On the other hand, smart homes have been studied and developed by various companies and organizations that can collect and analyze the information of those who reside there using various sensors and emerging technologies. Emerging technologies have been combined with IoT to provide a smart home environment service, and most of the sensors in this service have low power and computing capabilities. Therefore, it is very important to provide sensing information without burdening the sensor. A technique to secure communication and consume low computing and storage resources with physical unclonable function (PUF) while effectively utilizing sensor capabilities is presented by Kim et al. [5]. The technique has been evaluated as being secure against various security threats by performing a security analysis. They believe their solution could provide secure communication by using fewer resources in a smart home environment in the future. However, the proposed schema has some limitations, such as cross-platform compatibility and security policies that are based on the importance of information, which they will improve upon in future work.

3. Conclusions

The IoT is one of the branches of a growing global network which will reach about 50 billion connected devices by 2020. It is not just an Internet of Things; it is becoming an Internet of everything, including IIoT, smart homes, smart cities, smart healthcare and so on, where everything is connected everywhere. Connected devices and equipment are not a new manufacturing concept, but the proliferation of IoT is changing everything. This "smart" feature is now integrated with almost all devices and machines, allowing us to extract data at virtually any point in the supply chain. One of the main concerns around IoT is technological fragmentation and the IIoT, by extension, is not exempt from the coexistence of different standards, protocols and architectures that we will need to put in place in the future.

Special thanks go to Symmetry's Editor-in-Chief, as well as to all editorial teams for their invaluable support throughout the preparation and publication of this special issue. In addition, we thank the external reviewers for their invaluable help in reviewing the papers.

Funding: This research received no external funding.

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

Biographies

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park was a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, he was a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has served as chair and as program committee or organizing committee chair for many international conferences

and workshops. He is a steering chair of international conferences, such asMUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of Human-Centric Computing and Information Sciences (HCIS) by Springer, the Journal of Information Processing Systems (JIPS) by KIPS, and the Journal of Convergence (JoC) by KIPS CSWRG. He is Associate Editor/Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has served as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He received best paper awards from the ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he received outstanding research awards from the SeoulTech, 2014. His research interests include IoT, human-centric ubiquitous computing, information security, digital forensics, vehicular cloud computing, multimedia computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.

References

1. Cho, S. SINR-Based MCS Level Adaptation in CSMA/CA Wireless Networks to Embrace IoT Devices. *Symmetry* **2017**, *9*, 236. [CrossRef]
2. Zhao, C.; Parhami, B. Symmetric Agency Graphs Facilitate and Improve the Quality of Virtual Network Embedding. *Symmetry* **2018**, *10*, 63. [CrossRef]
3. Zhou, M.; Zhao, M.; Liu, A.; Ma, M.; Wang, T.; Huang, C. Fast and Efficient Data Forwarding Scheme for Tracking Mobile Targets in Sensor Networks. *Symmetry* **2017**, *9*, 269. [CrossRef]
4. Kang, S.; Kim, S. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. *Symmetry* **2017**, *9*, 233. [CrossRef]
5. Kim, M.; Lim, K.-S.; Song, J.; Jun, M.-S. An Efficient Secure Scheme Based on Hierarchical Topology in the Smart Home Environment. *Symmetry* **2017**, *9*, 143. [CrossRef]