Specialty Grand Challenge: IoT Communication and Networking Protocols

Deze Zeng[1,2]*

[1]School of Computer Science, China University of Geosciences, Wuhan, China, [2]Hubei Key Laboratory of Intelligent Geo-Information Processing, Wuhan, China

Keywords: IoT—internet of things, communication protocol, networking protocol, IoT systems, the internet of things (IoT)

1 INTRODUCTION

In the last decade, various kinds of smart end devices and sensors have been widely deployed and applied, and become the necessities in modern society Chettri and Bera (2019). It is also widely recognized that these devices should well collaborate with each other. This also catalyses the birth of Internet-of-Things (IoT) Hassan. (2019). IoT allows various devices, such as sensors, actuators, smart phones, and any smart devices, to connect with each other *via* the network, and to work together for providing better services eventually. Thanks to the fast development in the last decades, IoT has been applied in various aspects successfully, i.e., smart home Yang et al. (2018), smart city Kim et al. (2017) and smart health Sun et al. (2020), greatly reshaping our society.

As communication is the core to realize collaboration, the communication and networking protocol plays a critical role in implementing an IoT system. As already widely discussed, due to the limitation of size, power and computation capability, traditional Internet oriented communication and networking protocols are not quite suitable to IoT. To this end, many protocols, such as Bluetooth Low Energy, ZigBee, Lora, NB-IoT, CoAP, 6LoWPAN, MQTT, have been proposed with different characteristics (e.g., power consumption, transmission rate, transmission range, etc.,) and application domains Dizdarević et al. (2019). In addition, the recent 5G, B5G, and 6G networks are also well known for their special support to IoT communications. Besides, Artificial Intelligence (AI) technology also become an essential part of IoT systems. Besides exploring AI technology to process the IoT data, the system could be also manipulated by AI for autonomous performance or resource efficiency optimization. Recognizing the fact that one protocol may not fit for all scenarios, the coordination and the compatibility between different protocols thus become critical issues. Besides, various IoT applications also urge us to optimize the communication and network protocols to satisfy diverse Quality-of-Experience (QoE). Therefore, in the past decades, many efforts has been devoted to optimizing the IoT communication and networking protocols from various aspects. Nonetheless, with the emergence of new technologies (e.g., Software Define Networking, backscatter communications, Blockchain), new trend (e.g., in-network computing), new applications (e.g., autonomous driving), the protocol design is still a hot topic as it still confronts many challenges. As a result, in this article, we will discuss the main challenges imposed by these new technologies, concept, and trends to the design of IoT communication and networking protocols.

The rest of the paper is organized as follows: **Section 2** discusses eight main challenges in the development of IoT communication and networking protocols. **Section 3** summarizes these challenges and concludes this article.

OPEN ACCESS

Edited and reviewed by:
Rajkumar Buyya,
The University of Melbourne, Australia

****Correspondence:***
Deze Zeng
deze@cug.edu.cn

Specialty section:
This article was submitted to IoT Communication and Networking Protocols,
a section of the journal Frontiers in the Internet of Things

Received: *20 May 2022*
Accepted: *09 June 2022*
Published: *12 July 2022*

Citation:
Zeng D (2022) Specialty Grand Challenge: IoT Communication and Networking Protocols. Front. Internet Things 1:948558. doi: 10.3389/friot.2022.948558

2 CHALLENGES

2.1 Software Definability

The potential of Software-Defined Networking (SDN) has been widely recognized in traditional Internet domain since its inception as a way to simplify the network management and configuration. By integrating the technology, or concept of SDN into Wireless Sensor Network (WSN), it realizes a new concept known as Software-Defined Sensor Network (SDSN) Zeng et al. (2013, 2015). In SDSNs, thanks to the decoupling of the control plane and the data plane, not only the networking behaviours can be manipulated in a software-define way, but also the sensing and computation behaviours can be defined in an on-site manner. Thus, the whole IoT infrastructure, from sensing, transmission, storage and computation, can be defined over the air, realizing comprehensive system management and orchestration. At the same time, it also introduces some new problems to be tackled.

For example, traditional network oriented SDN relies on a central controller. But when it comes to the IoT case, which is featured by its vast distribution, one controller may not be enough. In this case, multiple controllers should be introduced. How these controllers interact with each other horizontally, and how they interact with the IoT devices vertically (including not only the sensors, but also all the devices in the infrastructure) should be well defined. In addition, it is well known that traditional SDN is comparatively resource consuming due to the additional introduction of the control overhead, more resource efficient protocols are expected to realize lightweight software-definability of IoT. Another non-ignorable issue on software-definability is the security. Although the software-definability makes the infrastructure more elastic, flexible, and open, the infrastructure becomes more vulnerable at the same time. The protocols should be secure enough and robust enough to deal with the possible vulnerabilities and threats Mathebula et al. (2019).

2.2 Interoperability, Integration, and Compatibility

As mentioned before, there already have been lots of different communication protocols available. This raises the interoperability problem when the devices need to communicate with each other. To reach the full potential of the IoT, it is not sufficient for the things only to be connected to the Internet, they also need to be found, accessed, managed and semantically linked to each other Blackstock and Lea (2014). To enable this interaction, a higher degree of interoperability is necessary. An effective means to improve the interoperability is to use the Web technology, evolving from the IoT to the Web-of-Things (WoT) Zeng et al. (2011). Some protocols (e.g., 6LowPAN) have also been proposed toward such vision. However, we still have not yet achieve the consensus on many issues. For example, we still lack the standard on how to exposing physical objects on the Web. In addition, some low-power networking protocols (e.g., ZigBee, ZWave, and Bluetooth) are designed for domain-specific applications with unique capabilities. Addressing interoperability issues at this level requires standardization at the hardware level Desai et al. (2015). Therefore, a universal standard is highly demanded to address the whole IoT interoperability issue.

Besides the inter-device interoperability, it is also highly desired that the IoT can be seamlessly integrated with some other newly emerging technologies (e.g. cloud, Blockchain). This also raises some new challenges on the integration. For example, the IoT ecosystem's reliance on centralized cloud infrastructure and lack of security protocols may lead to many cybersecurity attacks Tawfik et al. (2017). For the integration of IoT and Blockchain, as discussed in Pieroni et al. (2020), it still faces many challenges such as data security, privacy protection, access control, and resource management.

With the evolution of IoT, many different IoT architectures and protocols arises, and this introduces the problem on compatibility. Just like the evolution from IPv4 to IPv6, we cannot suddenly change all the protocols on all the devices at the same time. Thus, from the consideration of interoperability, the newly introduced protocols would be better compact with the old protocols. However, most existing solutions restrict compatible devices to a certain type of protocol Bin Ahmadon et al. (2021). Thus, the compatibility is also another challenge to the development of IoT.

2.3 In-Network Computing

With the development of IoT, it is predicted that billions of IoT devices will be connected to the Internet. Bulk data will be produced and cannot be fully processed by the IoT devices on the premises. Although it is possible to shuffle these data to the cloud, simply transmitting the raw data may overwhelm the network and cause extremely high energy consumption at the same time. This is not friendly to the development of IoT. To this end, there comes a compromise proposal, i.e., In-Network Computing (INC) or COmputing In the Network (COIN) Zeng et al. (2021a), which unlocks all the networked devices' computing power to process the data along the transmission route.

Traditionally, the communication and networking protocols, such as TCP's congestion control, flow control, and various routing algorithms, are designed independent of the computing. Hence, after the introduction of INC, the whole protocol stack needs to be refactored. For example, the congestion control needs to take the packet processing semantics into consideration as even the same routine may have different end-to-end delays due to the different processing semantics. The routing protocols should further take the computation power into consideration as the routing devices (beyond router) are able to handle some data processing tasks. INC blurs the edge between networking and computing, and any device may participate in. An IoT device could also be a routing device, and the IoT data may be processed by some routers on its routing path. Thus, the protocols should be able to deal with the high heterogeneity in the infrastructure, and can well adapt to different devices with different capabilities.

2.4 By AI and for AI

The INC converges the networking and the computing. Such convergence enables, and also asks for, a high degree of intelligence and automation to enhance the productivity and efficiency Mai et al. (2021). Artificial Intelligence (AI) emerges as a key enabling technology toward such vision. It has been demonstrated that AI technology such as reinforcement learning is with high potential in the routing management and congestion control in traditional networks. Without doubt that it can be also applied in the IoT communication and networking management. However, it still faces many challenges. Firstly, AI technology faces severe adaptability problem. The agent well trained for one scenario may not perform well in another scenario. It is still hard to realize a general solution. Secondly, different service providers use different AI agents for different needs, and the asynchrony between these agents may also lead to performance degradation Sheth et al. (2020). Thirdly, the AI based solution could be are computationally intensive and it may take a long time to train, which requires a lot of time and resource costs, and may even be unaffordable to some IoT devices. Fourthly, the operation of an intelligent agent requires a large volume of data. The collection of these data also introduces some additional overhead, which even competes with the data transmission. While, latency requirements are especially critical when the data collected by IoT devices is used for automatic or semiautomatic control applications Kaminski et al. (2017). Therefore, applying AI technology to manage the IoT communication and networking seems a promising way but it still needs more efforts to tackle these challenges.

With high popularity, many IoT applications adopt AI technologies to process the IoT data. The notorious thing of AI technologies is the extremely high computation power consumption. As mentioned above, the requirement may be beyond the capability of some IoT devices. There are two main approaches to deal with such problem. One approach is on the AI technologies themselves. For example, to some DNN models, we may apply pruning and compression to lower the computation power needs. Another approach is on the task scheduling. For example, we may split a large DNN models into a set of dependent tasks, which are then assigned to networked devices to process in a distributed manner. Actually, we may also try to combine the two approaches to find a more efficient solution to well match the computation power demands and supply, and eventually to the high Quality-of-Service (QoS) of AI based IoT applications. Nevertheless, this is still a grand challenge asking for more novel solutions.

2.5 Energy Efficiency

Energy efficiency has already been extensively studied in the IoT community as many IoT devices are powered by capacity limited batteries, and communicate with each other via wireless communications Hossein Motlagh et al. (2020). It is significant to apply appropriate communication technologies to ensure continuous connection links and support real-time transmission in an energy-efficient manner Ramamurthy and Jain (2017). As a result, low-power communication technologies suitable for IoT such as Bluetooth, Zigbee, and Long Range (LoRa) have been continuously developed. Meanwhile, the research community has also proposed many energy-efficient routing mechanisms to extend network lifetime Gopika and Panjanathan (2020) and reduce energy consumption. Low-power network encapsulation protocols such as 6LoWPAN, ZigBee IP, and Routing Protocol for Low Power and Lossy Networks (RPL) continue to emerge. However, the newly introduced ICN requires an IoT device not only able to sense and communicate but also to do some computation tasks. These things correlate with each other and solely relying on energy efficient communications seems not an end-all solution. New protocols that can well balance the energy consumption in sensing, transmission, and computation are highly expected.

Another development trend to deal with the energy efficiency issue is to exploit renewable energy from the environment to pursue the goal of zero-carbon IoT Zeng et al. (2021b). Energy harvesting technology also has experienced fast development in recent years. It is appealing to integrate these technologies to power the IoT devices with renewable energy. By now, although many algorithms on how to efficiently exploit the renewable green energy to extend the IoT device's lifetime or to lower the brown energy have been proposed. We are still in the early stage of such trend. The communication and networking protocols should also be designed in an energy-aware way, other than working independently. In addition, some new energy efficient communication technologies have also attracted lots of attention recently. For example, researchers recently have advocated backscatter communications for IoT Zhang et al. (2019). With the emergence and adoption of these new technologies, corresponding communication and networking protocols are also required.

2.6 Diverse Communication Mediums

Most IoT communication and networking protocols target at electromagnetic or optical communications. However, some special environments (e.g., underwater and underground) require some other medium oriented communication technologies and the corresponding protocols. For example, the underwater IoT is considered as one of the revolutionary technologies not only for ocean exploration but for its biodiversity maintenance as well Khalil et al. (2021). The performance of electromagnetic communication severely declines in the harsh underwater environment. To address such problem, acoustic communication is often advocated for underwater IoT Ghimire and Badi (2018). Similarly, the underground IoT devices are usually buried in the medium composed of asphalt and soil layer. The rate of electromagnetic wave, and hence the communication performance, will be greatly affected by soil texture (e.g., pore spaces, clay, sand, and silt particles) Vuran et al. (2018). Hence, it is important to understand the impact of these layers of communication medium over the propagating signal and design the communication and networking protocols in an environment-aware way Raza and Salam (2020) The ultimate goal of IoT development is to realize a global pervasive IoT system, and this requires that all the IoT devices can be seamlessly interconnected and freely communicate, no matter where the

TABLE 1 | Summary of the challenges and directions.

Challenge	Core	Future directions
Software Definability	The whole IoT infrastructure can be defined over the air	- Distributed control plane - Low control overhead - Security enforcement
Interoperability, Integration, and Compatibility	The IoT devices should be freely inter-operable with each other, and can be seamlessly integrated with newly emerging technologies	- Interoperability between different protocols - Integration with new technology (e.g., Blockchain) - Compatibility between different generations
In-Network Computing	All the networked devices' computing power (including the router) should be explored to process the data along the transmission route	- Redesign of in-network computing aware protocols (e.g., routing, congestion control) - Adaptability to the high heterogeneity in both the networking and the computing
By AI and For AI	The AI technology should be able to adapt to the diverse computing capability of various devices and the IoT infrastructure could be manipulated by AI.	- Adaptability of AI technology for diverse devices (e.g., pruning, compression, knowledge distillation, etc.) - Low latency communication for high performance AI based control - Interoperability between different intelligent agents - Application of AI technology (e.g., reinforcement learning) to mange the IoT infrastructure
Energy Efficiency	Appropriate communication technologies are demanded to ensure continuous connection links and support real-time transmission in an energy-efficient manner	- Zero-carbon IoT (e.g., energy harvesting, backscatter communications) - Collaboration between communication and networking for low energy consumption
Diverse Communication Mediums	Some special communication medium ask for corresponding communication and networking protocols	- Analysis of the influence from the environment (e.g., underwater, underground) - Seamless interconnection across diverse communication medium - Medium aware cross-layer protocol design
Security and Privacy	The capacity-constrained IoT device and the sensitive IoT data should be well protected	- Balance the openness and the security/privacy - Pervasive security and privacy enhancement
Mobility	The infrastructure should be able to well deal with the mobility of any sensing, networking and computing devices	- Mobility management with massive connections - Space-air-ground-sea integration with well mobility support - Three-dimensional mobility management

device is and what kind of communication medium it uses. This raises another interconnection challenge on how to adapt to these different communication mediums and technologies. Thus, the protocols should be designed in a cross-layer design way to strengthen their adaptability.

2.7 Security and Privacy

This is also an topic always under discussion. Malicious hackers may easily compromises the capacity-constrained IoT devices to launch network-wide attacks. Meanwhile, the integrity and authentication of the IoT data may also be damaged by malicious operations. For example, Denial-of-Service (DoS) attacks may saturate the network and shut down the network between the devices and their source Lyu et al. (2019). A false overflow indication may be injected to an IoT device to kill a normal processes. The data may be overheard by malicious attackers and the private data may be exposed. The attackers can also inject false data to pollute the system and make it react inappropriately or even dangerously. These attacks severely jeopardize the functionality of many IoT devices or IoT systems, e.g., auto-driving system, smart cities Kanuparthi et al. (2013). Although many solutions have already proposed, many threats are still continuously emerging. Beside pervasiveness, another development of IoT is on the openness, which is with high potential to excavate the power of IoT. However, openness always implies security hazards. Specially, with the introduction of software-definability, an IoT device's could be manipulated over the air. Although this makes the IoT become flexible and open, it also introduce more security threats as either the controller or a device could be compromised by malicious attackers. Such new trend also asks for more security solutions.

2.8 Mobility

An IoT system may contain a large number of heterogeneous communication devices, which are usually resource-constrained and require efficient routing protocols to realize data transmission from source to destination. In recent years, other than deploying dedicated IoT devices at some fix locations, mobile IoT devices are advocated to expand the coverage or to increase the flexibility. For example, Unmanned Aerial Vehicles (UAVs) and Unmanned Ground Vehicles (UGVs) equipped with various sensors (e.g., cameras) could be regarded as an IoT device and crowdsensing applications could be built by recruiting a number of mobile smartphones. Obviously, different from traditional IoT infrastructure, another challenges introduced in such scenario is on the mobility. Some recent effort have been devoted to the mobility management. For example, Santos et al. (2018) propose Mobility Matrix (μMatrix) as a complementary solution to standard routing protocols for IoT by using hierarchical IPv6 address allocation to manage mobile devices.

During movement, sometimes it is hard to guarantee the QoS of the network connections. While, some IoT applications ask for low-latency and reliable data communication. The movement may incurs long delay and high packet loss. In the past decades, many novel solutions have been proposed to address the mobility issue. For example, Hossein et al. Fotouhi et al. (2015) integrate an active handover mechanism (called smart-HOP) in RPL to achieve simple and effective backward compatibility with standard protocols. Nonetheless, the mobility still imposes a grand challenge on the IoT management and orchestration, especially with the emergence of new telecommunication technology like 5G, B5G and 6G. These technologies are all characterized with massive connections and even integrate with space-air-ground-sea networking. Besides the inter-connectivity challenge as discussed above, the mobility in the three-dimension environment also imposes a grand challenge to the IoT communication and networking.

3 SUMMARY AND CONCLUSION

In this article, with the consideration of newly emerging technologies, concepts, and trends on IoT communication, networking, and computing, we shed light on the challenges that may encounter during the design and implementation of IoT communication and networking. For the convenience of the readers, we summarize the main challenges and future directions in **Table 1**. It is worth noting that these challenges do not exist independently. Some of them are correlated with each other to shape the future IoT systems. More efforts from the researchers and engineers are expected to devote to these fields to advance the development of IoT.

AUTHOR CONTRIBUTIONS

DZ completed the whole work.

REFERENCES

Bin Ahmadon, M. A., Yamaguchi, S., Mahamad, A. K., and Saon, S. (2021). Physical Device Compatibility Support for Implementation of Iot Services with Design once, Provide Anywhere Concept. *Information* 12, 30. doi:10.3390/info12010030

Blackstock, M., and Lea, R. (2014). Iot Interoperability: A Hub-Based Approach. In *2014 International Conference on the Internet of Things*. IEEE, 79–84. doi:10.1109/iot.2014.7030119

Chettri, L., and Bera, R. (2019). A Comprehensive Survey on Internet of Things (Iot) toward 5g Wireless Systems. *IEEE Internet Things J.* 7, 16–32.

Desai, P., Sheth, A., and Anantharam, P. (2015). Semantic Gateway as a Service Architecture for Iot Interoperability. *IEEE Int. Conf. Mob. Serv. (IEEE)*, 313–319. doi:10.1109/mobserv.2015.51

Dizdarević, J., Carpio, F., Jukan, A., and Masip-Bruin, X. (2019). A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *ACM Comput. Surv. (CSUR)* 51, 1–29.

Fotouhi, H., Moreira, D., and Alves, M. (2015). Mrpl: Boosting Mobility in the Internet of Things. *Ad Hoc Netw.* 26, 17–35. doi:10.1016/j.adhoc.2014.10.009

Ghimire, A., and Badi, A. (20182018). Underwater Acoustic Channel Propagation Module for Simulation of Large-Scale Sub-aquatic Internet of Things (Iot) Networks in Jist/swans. *SoutheastCon*, 1–4. doi:10.1109/SECON.2018.8479242

Gopika, D., and Panjanathan, R. (2020). “Energy Efficient Routing Protocols for WSN Based IoT Applications: A Review,” in *Proceedings of the Materials Today: Proceedings*. doi:10.1016/j.matpr.2020.10.137

Hassan, W. H. (2019). Current Research on Internet of Things (Iot) Security: A Survey. *Comput. Netw.* 148, 283–294.

Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., and Zakeri, B. (2020). Internet of Things (IoT) and the Energy Sector. *Energies* 13, 494. doi:10.3390/en13020494

Kaminski, N., Macaluso, I., Di Pascale, E., Nag, A., Brady, J., Kelly, M., et al. (2017). “A Neural-Network-Based Realization of In-Network Computation for the Internet of Things,” in *2017 IEEE International Conference on Communications*, 1–6. doi:10.1109/ICC.2017.7996821

Kanuparthi, A., Karri, R., and Addepalli, S. (2013). “Hardware and Embedded Security in the Context of Internet of Things,” in *Proceedings of the 2013 ACM Workshop on Security, Privacy Dependability for Cyber Vehicles* (New York, NY, USA: Association for Computing Machinery), 61–64. doi:10.1145/2517968.2517976

Khalil, R. A., Saeed, N., Babar, M. I., and Jan, T. (2021). Toward the Internet of Underwater Things: Recent Developments and Future Challenges. *IEEE Consum. Electron. Mag.* 10, 32–37. doi:10.1109/MCE.2020.2988441

Kim, T.-h., Ramos, C., and Mohammed, S. (2017). *Smart City and Iot*.

Lyu, C., Zhang, X., Liu, Z., and Chi, C.-H. (2019). Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things against Dos Attacks. *IEEE Access* 7, 31068–31082. doi:10.1109/ACCESS.2019.2902843

Mai, T., Yao, H., Guo, S., and Liu, Y. (2021). In-network Computing Powered Mobile Edge: Toward High Performance Industrial Iot. *IEEE Netw.* 35, 289–295. doi:10.1109/MNET.021.2000318

Mathebula, I., Isong, B., Gasela, N., and Abu-Mahfouz, A. M. (2019). “Analysis of SDN-Based Security Challenges and Solution Approaches for SDWSN Usage,” in *Proceedings of the IEEE International Symposium on Industrial Electronics*, 1288–1293. doi:10.1109/isie.2019.8781268

Pieroni, A., Scarpato, N., and Felli, L. (2020). Blockchain and IoT Convergence-A Systematic Survey on Technologies, Protocols and Security. *Appl. Sci.* 10, 6749. doi:10.3390/app10196749

Ramamurthy, A., and Jain, P. (2017). *The Internet of Things in the Power Sector Opportunities in Asia and the Pacific*.

Raza, U., and Salam, A. (2020). Wireless Underground Communications in Sewer and Stormwater Overflow Monitoring: Radio Waves through Soil and Asphalt Medium. *Information* 11, 98. doi:10.3390/info11020098

Santos, B. P., Goussevskaia, O., Vieira, L. F. M., Vieira, M. A. M., and Loureiro, A. A. F. (2018). Mobile Matrix: Routing under Mobility in Iot, Iomt, and Social Iot. *Ad Hoc Netw.* 78, 84–98. doi:10.1016/j.adhoc.2018.05.012

Sheth, K., Patel, K., Shah, H., Tanwar, S., Gupta, R., and Kumar, N. (2020). A Taxonomy of Ai Techniques for 6g Communication Networks. *Comput. Commun.* 161, 279–303. doi:10.1016/j.comcom.2020.07.035

Sun, J., Xiong, H., Liu, X., Zhang, Y., Nie, X., and Deng, R. H. (2020). Lightweight and Privacy-Aware Fine-Grained Access Control for Iot-Oriented Smart Health. *IEEE Internet Things J.* 7, 6566–6575. doi:10.1109/jiot.2020.2974257

Tawfik, M., Almadani, A., and Alharbi, A. A. (2017). A Review: the Risks and Weakness Security on the Iot. *IOSR J. Comput. Eng. (IOSR-JCE)*.

Vuran, M. C., Salam, A., Wong, R., and Irmak, S. (2018). Internet of Underground Things in Precision Agriculture: Architecture and Technology Aspects. *Ad Hoc Netw.* 81, 160–173. doi:10.1016/j.adhoc.2018.07.017

Yang, H., Lee, W., and Lee, H. (2018). Iot Smart Home Adoption: The Importance of Proper Level Automation. *J. Sensors*, 2018. doi:10.1155/2018/6464036

Zeng, D., Ansari, N., Montpetit, M.-J., Schooler, E. M., and Tarchi, D. (2021a). Guest Editorial: In-Network Computing: Emerging Trends for the Edge-Cloud Continuum. *IEEE Netw.* 35, 12–13. doi:10.1109/MNET.2021.9606835

Zeng, D., Guo, S., and Cheng, Z. (2011). The Web of Things: A Survey (Invited Paper). *Jcm* 6, 424–438. doi:10.4304/jcm.6.6.424-438

Zeng, D., Li, P., Guo, S., Miyazaki, T., Hu, J., and Xiang, Y. (2015). Energy Minimization in Multi-Task Software-Defined Sensor Networks. *IEEE Trans. Comput.* 64, 3128–3139. doi:10.1109/TC.2015.2389802

Zeng, D., Li, Y., Chen, L., Gu, L., and Hu, C. (2022b). Sensing or Transmission? Stochastic Scheduling of Energy-Harvesting Sensors toward Zero-Carbon IoT. *IEEE Trans. Green Commun. Netw.* 6, 1132–1140. doi:10.1109/TGCN.2021.3133936

Zeng, D., Miyazaki, T., Guo, S., Tsukahara, T., Kitamichi, J., and Hayashi, T. (2013). "Evolution of Software-Defined Sensor Networks," in *Proceedings - IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks* (New York: MSN), 2013410–2013413. doi:10.1109/MSN.2013.60

Zhang, W., Qin, Y., Zhao, W., Jia, M., Liu, Q., He, R., et al. (2019). A Green Paradigm for Internet of Things: Ambient Backscatter Communications. *China Commun.* 16, 109–119. doi:10.23919/jcc.2019.07.009

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.