



Energy Inefficiency in IoT Networks: Causes, Solutions and Enabling Techniques

Ziyad Almudayni¹(✉), Ben Soh², and Alice Li²

¹ Hail University, Hail, Saudi Arabia

20167676@students.latrobe.edu.au

² La Trobe University, Melbourne, Australia

{b.soh, a.li}@latrobe.edu.au

Abstract. The Internet of things (IoT) concept can be generally described as the ability of machines to communicate via the Internet to perform tasks. In addition to the communication between devices, humans can remotely control IoT devices via controllers such as smartphones. The main aim of introducing IoT technologies is to make our lives easier and more convenient. Due to the massive increase in both IoT devices and research on enhancing the security and the speed of these devices, there is a strong demand to work in parallel to promote IoT networks' energy efficiency to make IoT systems scalable. This paper outlines the causes of energy inefficiency in IoT systems and proposes some key tools to prolong the network lifetime of these devices.

Keywords: IoT · Routing · Clustering · Offloading · Scheduling

1 Introduction

The Internet of things (IoT) concept can generally be described as the ability of machines to communicate via the Internet to perform tasks. In addition to the communication between devices, humans can remotely control IoT devices via controllers such as smartphones [1]. The main aim of introducing IoT technologies is to make our lives easier and more convenient. In many various fields, the IoT systems can simplify work processes by building automatic systems that can operate without any human interaction, which saves time, money, effort [2]. Due to the massive rise in IoT devices, there is a strong demand to promote IoT networks' energy efficiency. In addition to the number of IoT devices, researchers have developed several complex algorithms to improve other parameters such as security, data rate, and bandwidth, which increase the workload and the consumption of power [3]. From an energy perspective, a study carried out in 2021 by Liu L et al., found that the number of connected IoT devices in use globally will reach 55.7 billion by 2025. Furthermore, these different IoT sensors and devices require various power costs to work normally; for example, a gas sensor requires 500–800 mW for operating normally [4]. From an economic perspective, several studies have shown the importance of IoT in the market and how this technology can lead to successful

investments. A recent study predicted that the total investment in IoT technology would increase from USD 130.33 billion in 2015 to USD 883.55 billion in 2022 [5]. Thus, engineering IoT systems to consume less power and cost will encourage providers and consumers to participate in the IoT markets and result in more successful investments in the IoT markets. From an environmental perspective, all energy sources have a negative impact on our air, water and land [6]. Thus, it is vital to be aware of the power emissions that IoT devices produce and to decrease their impacts as much as possible by reducing the power consumption of IoT systems while ensuring they continue to reaching their objectives, we will mitigate the impacts on the environment. From an industrial perspective, minimising the power consumption of IoT devices will encourage industries to integrate the IoT systems into their environment and to rely more on this technology. From a governmental perspective, introducing IoT systems with this advantage (low power requirements) will encourage organisations such as the Ministry of Health, the Ministry of Transportation to avail from this technology to simplify their work process.

2 The Causes and Solutions for Energy Inefficiency in the IoT Systems

Many technical issues in the IoT systems make the IoT devices consume more power in the IoT networks. Therefore, it is vital that researchers work more deeply on these technical issues to find and address gaps to reduce the amount of power consumed by IoT systems. In this section, thirteen common technical as shown in Fig. 1 for energy inefficiency with initial solutions will be discussed in detail.

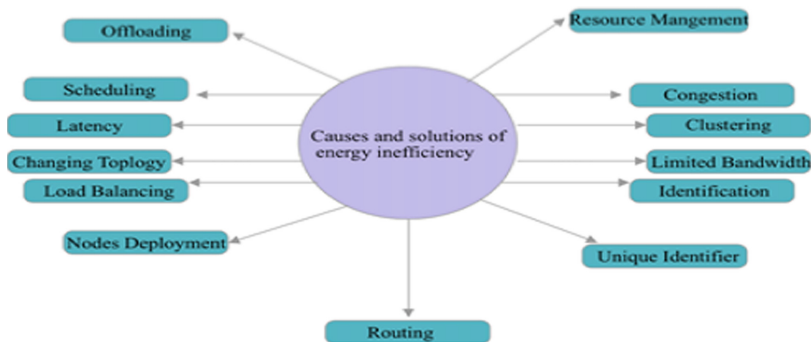


Fig. 1. Causes of energy inefficiency

2.1 Offloading

Offloading in general terms refers to moving things from one state to a different state. Offloading in IoT systems occurs when the tasks move from one fog node to another fog node or from a fog node to the cloud server. Efficient tasks offloading can be considered

as one of the main keys to enhancing the QoS and improving parameters such as energy efficiency, delay, data rate and more. From an energy perspective, inefficient offloading of the IoT tasks leads to an increase in processing time, resulting in a greater consumption of power. This might also lead to an increase in the load on fog nodes while other nodes remain empty if the tasks are not distributed equally. Therefore, it is necessary to take the offloading into account to reduce the power used by IoT devices [7]. Researchers have been working to develop the offloading strategies to achieve the best decision-making about whether the tasks are processed on the fog or the cloud; this decision could be counted as the key to improve the offloading [8].

2.2 Scheduling

Tasks in IoT systems can be allocated based on various scheduling criteria to handle the resources and functions in a specific amount of time. Constraints and objectives are the two main features that have to be fulfilled to solve most of the scheduling problems. The scheduling mechanism is another key to improving the QoS in IoT systems [9]. Due to the nature of heterogeneity and the number of IoT tasks and functions, efficient tasks scheduling makes IoT systems more organized and less heterogeneous, which leads to a decrease in the processing time, and as the processing time decreases the power consumption of the IoT systems will decrease accordingly. Inefficient tasks scheduling makes work in IoT systems more complicated and less efficient as well as consuming more power and processing time. Researchers need to be aware of this point to improve the QoS of IoT from an energy perspective as well as to improve other parameters, such as bandwidth and data rate.

2.3 Latency

Latency in general terms is when a system can not complete a process by the submission time. In other words, there is a delay. From an IoT perspective, as IoT applications require real-time processing to deliver services to the end-user, delays might lead to a large impact and affect the system's process negatively, so the response time has to be as short as possible to satisfy the QoS requirements [10]. Latency and power consumption in the IoT systems are related, so when the latency in systems is high, the IoT devices and network nodes will consume more power; the opposite is also true. The reason for this is the delays in the system will cause an increase in the processing time, which leads to more power consumption. As researchers, we must seek to minimise the response time for IoT communication as much as possible to save more power for the IoT systems.

2.4 Changing Topology

The wireless network is the fundamental method of communication that most IoT devices use. Due to the dynamic nature of the IoT environment, the wireless network topology updates its structure frequently, and the number of IoT nodes is updated from time to time. These changes affect the efficiency and reliability of data transmission [11]. A change in the network topology might affect the energy's performance in the IoT environment as

IoT devices and network nodes consume more power during these changes. The process of an IoT device joining and leaving a wireless network for the IoT devices consumes energy, researchers have to be aware of this and strive to make the IoT network as steady as possible to minimise the amount of joining and leaving. When there is a change in the IoT network topology, the number of the required network nodes for the IoT devices might change from time to time, for instance, a smart building might require 50 network nodes in winter while the same building might require 70 network nodes in summer. Prediction algorithms could play an important role in solving this problem by estimating the number of the required network nodes in all different scenarios.

2.5 Load Balancing

Load balancing in general terms can be defined as systems' ability to distribute the workload of things, humans, machines and nodes equally. From an IoT perspective, load balancing can be achieved when the workload is distributed equally between routes in the network routing and between nodes in computing services and between the IoT devices. As the traffic in the IoT networks increases accordingly with the rise in the number of processes in an IoT system, load balancing can play an essential role in minimising traffic in the network by distributing the workload over several IoT nodes and routes [12]. From an energy perspective, efficient load balancing can contribute to estimating the required nodes, routes, and devices. This estimation results in reducing the power consumption of the IoT devices, as there will be no extra nodes, routes and devices. Inefficient load balancing is one of the main reasons for losing power in IoT systems as there might be more active empty nodes where routes are not needed if the IoT system's workload is not balanced effectively. Also, there might be greater loads on nodes and routes, while others have less or zero loads, which leads to greater power consumption. There are two types of load balancing: static load balancing and dynamic load balancing. In the former, the load distribution and balancing are based on data that have been stored before the start of the system. In the latter, the system distributes the load equally during real-time [13].

2.6 Node Deployment

The structure of network nodes is one of the first steps that a designer has to be aware of when establishing a network system. There are three main structures in IoT systems and fog services for the deployment of nodes: cluster, peer to peer, and master-slave [14]. Selecting the appropriate structure for an IoT system enhances the QoS and improves the performance in terms of data rate, bandwidth, security and energy consumption. From an energy perspective, the inefficient selection of a network node structure might affect the energy consumption performance and lead to consuming more power as there might be extra nodes more than needed and some nodes might have extra loads while others empty. To satisfy the QoS requirements and improve the performance of IoT communications, when selecting the structure of deployments designers need to consider certain things such as the amount and type of tasks, the number of IoT devices and sensors and the workloads [15].

2.7 Resource Management

Adequate resource management of IoT devices could be considered one of the key factors to enhance the IoT systems' performance and satisfying the QoS requirements. These resources are managed and powered by tiny operating systems such as TinyOS, FreeRTOS and Contiki. For each IoT device, there are five main components of resources management: process management, memory management, energy management, communication management and file management. For instance, when aiming to reduce power consumption and enhance energy efficiency of an IoT system, we can focus on energy resource management. This can be achieved by improving the network protocols and OS scheduling modes such as the CPU's sleep mode when the queue is empty. Researchers have to be aware of all the different layers of IoT architecture to save more power or any different parameters, and inefficient resource energy management might cause in losing more power and make the network lifetime shorter, so it is vital to be aware of this point [16].

2.8 Congestion Control IoT

IoT networks include various types of networks such as wireless sensors networks, ad-hoc networks and vehicular ad hoc networks. The complexity of these networks will cause traffic and increase the size of the network, which leads to congestion in the IoT network and delays in communication [17]. Congestion in the IoT network negatively affects the IoT system's performance, thus decreasing the level of QoS in the system. Effective routing protocols could be counted as one of the main keys to avoid congestion in the network by selecting the best and the shortest path and controlling these paths when sending and receiving data [18]. From an energy perspective, congestion in the IoT network node results in the use of more power due to the increase in the processing and transferring of data in the node. It is vital to handle the congestion problem in IoT networks by effectively controlling the routing paths and balancing the network nodes' workload to prolong the network lifetime of IoT networks [19].

2.9 Clustering

Clustering is a key to enhancing the overall performance of the IoT networks. Without clustering, all IoT nodes send data packets to the base station, leading to more power consumption. There are two types of nodes in clustering: cluster heads (CH) and cluster members. CHs work as a centre point to aggregate data from the cluster members (neighboring nodes) to the base station, leading to saving power. Machine learning, fuzzy logic and other approaches can be utilised to select the appropriate CH and the number of nodes in each cluster [20].

2.10 Routing

The route in the network is the path from the source (sender) to the destination (receiver), and routing is the process of following these paths when sending and receiving data packets in the network. As deployment of IoT devices is heterogeneous in nature, finding

the shortest path is one of the primary ways to satisfy the QoS requirements in IoT networks. From an energy perspective, the power consumed by a transmission when forwarding data packets from the source to the destination via long paths is higher than the forwarding through shorter paths. Therefore, it is vital to take advantage of using optimizing algorithms such as ant colony optimization algorithm to find the shortest path in order to save power and prolong the network lifetime [21].

2.11 Limited Bandwidth

Minimizing the bandwidth in IoT networks is essential. Limiting the bandwidth in IoT systems can play an essential role in enhancing the QoS of IoT technologies. Power consumption and the speed of real-time processing in IoT networks show significant improvements when the bandwidth is limited. The average range of the bandwidth in most of the IoT networks is about 200 kbit/s [22]. It is vital to minimize the bandwidth of the IoT network without affecting the delivered services for end-users, as all the requested services from end-users have to arrive on time.

2.12 Identification of IoT Devices

All devices and nodes in the IoT environment have to be identified in all layers of IoT. The IoT nodes are distinguished from one to another in terms of many aspects like performance, properties, functions and more. As IoT nodes are dissimilar in their methods, it is important to identify each node in the IoT environment to understand the behavior of the IoT network nodes. Identification in the IoT devices is one of the main challenges in IoT systems due to the high number of IoT devices [23]. Therefore, the process of identification has to be as simple as possible to reduce the work complexity in IoT networks.

2.13 Unique Identifier

IoT has contributed to increasing the number of connected devices via the Internet to reach to billions. Network identifiers (NIs) allow IoT nodes to communicate and transmit data by addressing each node in the network. NIs systems such as IPv4, IPv6, 16-bit and ZigBee are distinguished from each other in the way and size of addressing. IPv4 is widely considered as the most addressing system to define each node in IoT systems. However, this addressing system is not reliable when applied to a large number of IoT devices because it is 32 bits long and has limited addressing the devices, which is about 4.3 billion. IPv6 (128-bit) provides more spaces than IPv4, however, using a long identifier for small IoT networks is wasteful because 128-bits is too large to be utilised to define only 100 IoT nodes. It is vital to have a unique identifier as these distinguishes in addressing and protocols can lead to technical issues in compatibility and interoperability [24].

3 Enabling Technologies

Enabling technologies are the tools that can be used to solve any technical issues. This section focuses on the tools that can be used to solve technical issues in IoT systems and, especially, to improve the energy efficiency of these systems. Six of the most important tools are listed below in more detail; however, it is important to be aware that there are more than these six tools (see Fig. 2.).

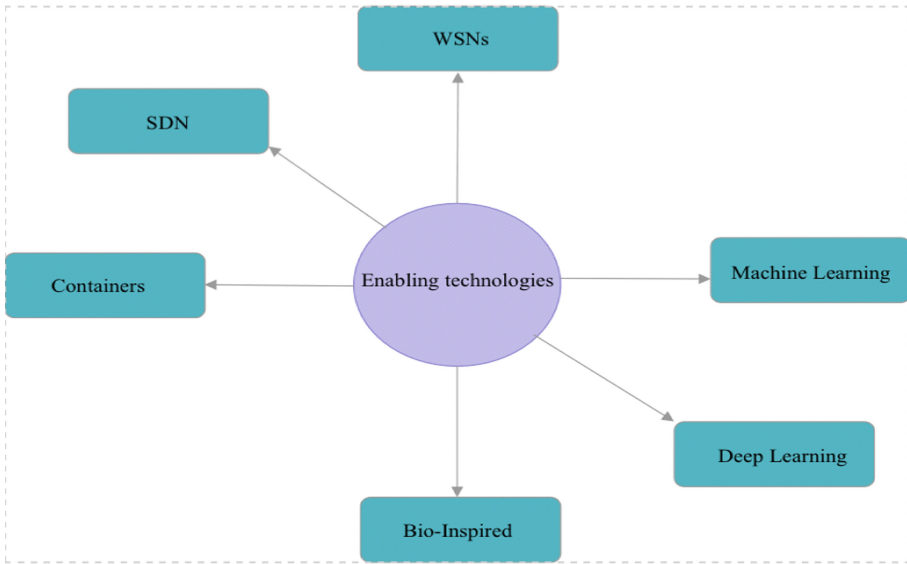


Fig. 2. Enabling tools

3.1 Software-Defined Networking

SDN is a software tool that is used to manage and control networks virtually. The control plane and the data plane, which work separately, are the main parts of SDN. The control plane manages the network routes, and the data plane is responsible only for forwarding the data. SDN has added value to the network management by reducing the cost and efforts as these managements can be done without any physical interactions [25]. SDN has the potential to simplify network management and programmability and this advantage might add value to the IoT network management and make the system less complex for example by scheduling and the work load of tasks and activities in the IoT networks. SDN can also improve the IoT network's energy efficiency by managing sensor nodes and IoT devices as well as by controlling the duty cycles and sleep-scheduling mechanisms for low rate WPAN [26].

3.2 Containers

Containers can be defined as light virtual operating systems that can be run on various systems such as IoT, fog computing and more. The main objective of establishing containers is to manage each single point in the system, including IoT nodes and fog nodes. The management of resources such as CPUs, power, and memory and more in IoT nodes or fog nodes can be easily done through containers when they are established in the fog or IoT system. In addition to the management of resources, containers can control, monitor, and schedule the tasks. The containers can play an important role in enhancing the performance of IoT or fog system and making the system more scalable to increase the number of devices in the network [27]. There is a potential to improve the energy efficiency of both the fog nodes and the IoT nodes to satisfy the QoS requirements by effectively managing resources such as power, CPUs, I/O and memory through containers.

3.3 Wireless Sensor Networks (WSNs)

A WSN consists of a group of sensor nodes that can process, communicate and store data. The main purpose of sensor nodes is to detect and sense the changes in the surrounding areas in the environments such as temperature, humidity etc., and transfer data between IoT nodes. The end-user is updated frequently about the current state of the environment from the data collected by sensor nodes and can take actions accordingly. Lack of energy resources, lack of memory and a limited physical range are the main things that the WSNs suffer from [28]. It is vital to improve the performance of the WSNs to satisfy the QoS requirements by significantly improving the energy efficiency of networks and other parameters such as security. This can be achieved by working deeply in the network such as improving the clustering and distribution of WSNs, and selecting the shortest path between the nodes to send and receive data.

3.4 Machine Learning

Machine learning analyses historical data to predict future events and make intelligent decisions. In IoT systems, ML and AI can act as the brain of the IoT network to handle and control the system and perform tasks [29]. There are three main categories of machine learning: supervised learning, unsupervised learning, and reinforcement learning: each has its own features that benefit the IoT system and improve the overall performance of the system. The main objective of supervised learning is to classify things such as tasks in the IoT networks or any other system, which can be done by using labeled data. The IoT networks can benefit from supervised learning by classifying the tasks into categories to enhance the performance of scheduling in IoT nodes, fog nodes and resources management. Unsupervised learning obtains to cluster things by using unlabeled data where a machine figures out the output. It can add value to the IoT networks by, for example by clustering in the WSNs to reduce the power consumption and improve the network's performance. Reinforcement learning can be defined as the ability of agents to interact in the environment to take actions; it can be used to design the routing protocols in IoT systems to satisfy the QoS requirements [30].

3.5 Deep Learning

Deep learning (DL) aims to analyse a large volume of data to predict events and perform tasks in a complex environment. Due to its multilayer structure, DL can be considered as advanced type of machine learning. As IoT systems deal with a large value of data, DL can perform better performance than ML, and it can also solve different problems automatically by extracting new features [31]. DL uses artificial neural networks (ANNs) to process and analyse data, which has inputs, hidden layers and outputs. The neural network's hidden layers act as the brain of the network to analyse and process the inputs data to generate the outputs as solutions, tasks, and events. DL can add advantages to most IoT applications; including those in healthcare, agriculture and educations. This DL technology has numerous features, such as image recognition, voice recognition and indoor localization. As IoT systems have limited energy, developers have to be aware that DL techniques demand a large amount of resources such as battery energy, memory and processors [32]. Therefore, the DL algorithms have to be as simple as possible to limit power consumption and take the advantage of finding solutions for energy inefficiency.

3.6 Bio-Inspired Algorithm

Bio-inspired optimization algorithms are a promising tool for solving and developing computing techniques by using biological principles such as genetic bee colony (GBC) algorithm, fish swarm algorithm (FSA). Biology optimization algorithms are capable of solving complex machine learning problems in science and engineering [33]. From a network perspective, these biology algorithms have played a vital role in enhancing and providing solutions for communication protocols between devices. For example, most of the routing and clustering problems in the wireless sensor network have been solved using these algorithms. These bio-inspired optimization algorithms have added values to IoT systems and contributed to enhancing the IoT system's overall performance [34]. Therefore, we as researchers have to take advantage and benefit from these biology algorithms to solve and develop our energy efficiency problems by employing these algorithms.

4 Conclusion and Future Work

Developing any layers from the four architecture layers can enhance the IoT system's energy efficiency and all other parameters. Thus, from a computing perspective, it is vital to know that saving power in IoT systems can be achieved without working directly on watts, voltage and joules. Instead, working on and developing other parameters that are more related to computing and networking, such as latency and capacity, can achieve the aim of saving energy. Also, improving these parameters can be accomplished without working on them directly. The conclusion of this paper is to suggest that researchers who are aiming to improve the IoT systems' power consumption should work more deeply in such areas as scheduling, offloading, node deployment, resource management, routing, and clustering. Future studies will review previous studies related to improving the energy efficiency of IoT networks from different aspects to help researchers target research areas to address gaps.

References

1. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **82**, 395–411 (2018)
2. Nižetić, S., Šolić, P., González-de, D.L.-D.-I., Patrono, L.: Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future. *J. Cleaner Prod.* **274**, 122877 (2020)
3. Sen, S., Koo, J., Bagchi, S.: TRIFECTA: security, energy efficiency, and communication capacity comparison for wireless IoT devices. *IEEE Internet Comput.* **22**, 74–81 (2018)
4. Liu, L., Guo, X., Lee, C.: Promoting smart cities into the 5G era with multi-field Internet of Things (IoT) applications powered with advanced mechanical energy harvesters. *Nano Energy*, 106304 (2021)
5. Tsai, C.-W.: SEIRA: an effective algorithm for IoT resource allocation problem. *Comput. Commun.* **119**, 156–166 (2018)
6. Bilgen, S.: Structure and environmental impact of global energy consumption. *Renew. Sustain. Energy Rev.* **38**, 890–902 (2014)
7. Yousefpour, A., Ishigaki, G., Gour, R., Jue, J.P.: On reducing IoT service delay via fog offloading. *IEEE Internet Things J.* **5**, 998–1010 (2018)
8. Jiang, J., Li, Z., Tian, Y., Al-Nabhan, N.: A review of techniques and methods for IoT applications in collaborative cloud-fog environment. *Secur. Commun. Networks* **2020** (2020)
9. Aburukba, R.O., AliKarrar, M., Landolsi, T., El-Fakih, K.: Scheduling Internet of Things requests to minimize latency in hybrid Fog–Cloud computing. *Future Gener. Comput. Syst.* **111**, 539–551 (2020)
10. Ma, Z., Xiao, M., Xiao, Y., Pang, Z., Poor, H.V., Vucetic, B.: High-reliability and low-latency wireless communication for internet of things: challenges, fundamentals, and enabling technologies. *IEEE Internet Things J.* **6**, 7946–7970 (2019)
11. Marietta, J., Mohan, B.C.: A review on routing in internet of things. *Wireless Pers. Commun.* **111**, 209–233 (2020)
12. Tseng, C.H.: Multipath load balancing routing for Internet of things. *J. Sens.* **2016** (2016)
13. Kaur, M., Aron, R.: A systematic study of load balancing approaches in the fog computing environment. *J. Supercomput.*, 1–46 (2021)
14. Mahmud, R., Kotagiri, R., Buyya, R.: Fog computing: a taxonomy, survey and future directions. In: Di Martino, B., Li, K.-C., Yang, L.T., Esposito, A. (eds.) *Internet of everything*. IT, pp. 103–130. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-5861-5_5
15. Zahmatkesh, H., Al-Turjman, F.: Fog computing for sustainable smart cities in the IoT era: caching techniques and enabling technologies-an overview. *Sustain. Cities Soc.* **59**, 102139 (2020)
16. Musaddiq, A., Zikria, Y.B., Hahm, O., Yu, H., Bashir, A.K., Kim, S.W.: A survey on resource management in IoT operating systems. *IEEE Access* **6**, 8459–8482 (2018)
17. Bhandari, K.S., Hosen, A., Cho, G.H.: CoAR: congestion-aware routing protocol for low power and lossy networks for IoT applications. *Sensors* **18**(11), 3838 (2018)
18. Verma, L.P., Kumar, M.: An IoT based congestion control algorithm. *Internet Things* **9**, 100157 (2020)
19. Bhandari, K.S., Hosen, A., Cho, G.H.: CoAR: congestion-aware routing protocol for low power and lossy networks for IoT applications. *Sensors* **18**, 3838 (2018)
20. Srivastava, V., Tripathi, S., Singh, K., Son, L.H.: Energy efficient optimized rate based congestion control routing in wireless sensor network. *J. Ambient Intell. Humanized Comput.* **11**, 1325–1338 (2020)
21. Radhika, S., Rangarajan, P.: On improving the lifespan of wireless sensor networks with fuzzy based clustering and machine learning based data reduction. *Appl. Soft Comput.* **83**, 105610 (2019)

22. Raj, J.S., Basar, A.: QoS optimization of energy efficient routing in IoT wireless sensor networks. *J. ISMAC* **1**, 12–23 (2019)
23. Zikria, Y.B., Yu, H., Afzal, M.K., Rehmani, M.H., Hahm, O.: *Internet of Things (IoT): operating system, applications and protocols design, and validation techniques*. Elsevier (2018)
24. Aswale, P., Shukla, A., Bharati, P., Bharambe, S., Palve, S.: An overview of Internet of Things: architecture, protocols and challenges. In: Satapathy, S.C., Joshi, A. (eds.) *Information and Communication Technology for Intelligent Systems*. SIST, vol. 106, pp. 299–308. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1742-2_29
25. Liu, G., Quan, W., Cheng, N., Zhang, H., Shen, X.: VLI: variable-length identifier for interconnecting heterogeneous IoT networks. *IEEE Wireless Commun. Lett.* **9**, 1146–1149 (2020)
26. Qafzezi, E., Bylykbashi, K., Ikeda, M., Matsuo, K., Barolli, L.: Coordination and management of cloud, fog and edge resources in SDN-VANETs using fuzzy logic: a comparison study for two fuzzy-based systems. *Internet Things* **11**, 100169 (2020)
27. Li, Y., et al.: Enhancing the internet of things with knowledge-driven software-defined networking technology: future perspectives. *Sensors* **20**, 3459 (2020)
28. Aruna, K., Pradeep, G.: Performance and scalability improvement using IoT-based edge computing container technologies. *SN Comput. Sci.* **1**, 1–7 (2020)
29. Singh, H., Bala, M., Bamber, S.S.: Augmenting network lifetime for heterogenous WSN assisted IoT using mobile agent. *Wireless Netw.* **26**, 5965–5979 (2020)
30. Younan, M., Houssein, E.H., Elhoseny, M., Ali, A.A.: Challenges and recommended technologies for the industrial internet of things: a comprehensive review. *Measurement* **151**, 107198 (2020)
31. Khattab, A., Youssry, N.: Machine learning for IoT systems. *Internet Things (IoT)*, 105–127 (2020)
32. Li, H., Ota, K., Dong, M.: Learning IoT in edge: deep learning for the Internet of Things with edge computing. *IEEE Network* **32**, 96–101 (2018)
33. Mohammadi, M., Al-Fuqaha, A., Sorour, S., Guizani, M.: Deep learning for IoT big data and streaming analytics: a survey. *IEEE Commun. Surv. Tutorials* **20**, 2923–2960 (2018)
34. Darwish, A.: Bio-inspired computing: algorithms review, deep analysis, and the scope of applications. *Future Comput. Inf. J.* **3**, 231–246 (2018)
35. Hamidouche, R., Aliouat, Z., Gueroui, A.M., Ari, A.A.A., Louail, L.: Classical and bio-inspired mobility in sensor networks for IoT applications. *J. Network Comput. Appl.* **121**, 70–88 (2018)