Requirements for Energy Efficient Edge Computing: A Survey

Olli Väänänen[1(✉)] and Timo Hämäläinen[2]

[1] Industrial Engineering, School of Technology, JAMK University of Applied Sciences, Jyväskylä, Finland
olli.vaananen@jamk.fi
[2] Department of Mathematical Information Technology, University of Jyväskylä, Jyväskylä, Finland
timo.t.hamalainen@jyu.fi

Abstract. Internet of Things is evolving heavily in these times. One of the major obstacle is energy consumption in the IoT devices (sensor nodes and wireless gateways). The IoT devices are often battery powered wireless devices and thus reducing the energy consumption in these devices is essential to lengthen the lifetime of the device without battery change. It is possible to lengthen battery lifetime by efficient but lightweight sensor data analysis in close proximity of the sensor. Performing part of the sensor data analysis in the end device can reduce the amount of data needed to transmit wirelessly. Transmitting data wirelessly is very energy consuming task. At the same time, the privacy and security should not be compromised. It requires effective but computationally lightweight encryption schemes. This survey goes thru many aspects to consider in edge and fog devices to minimize energy consumption and thus lengthen the device and the network lifetime.

Keywords: IoT, Edge Computing, Fog Computing, sensor data compression.

1 Introduction

The Internet of Things (IoT) has been in focus on recent years. There are already billions of devices connected to the Internet and the amount of the Internet connected things is estimated to grow exponentially in these years [1, 2]. There are forecasts that by 2020 there will be more than 50 billion devices connected to the Internet [3]. These connected devises and things are very heterogeneous and require very different and application specific solutions and approaches. [1] The IoT as a concept was first introduced in 1999 by Kevin Ashton and it was related to the devices connected to the Internet via RFID connection. [1] The term IoT was mainly forgotten for years after that but it was reinvented some years ago. The exact definition of the IoT is still not described clearly, [1] but the technologies, solutions and the use of the IoT is all the time emerging.

There are already solutions of the IoT in use but the real success of the IoT depends on the standardization, which allows the compatibility, interoperability, relia-

bility and effectiveness of the IoT solutions. The IoT devices and things should be able to autonomously communicate with other devices or things and connect data to the Cloud. The IoT describes the next generation of the Internet, where physical things are connected to the Internet and can be identified and accessed via Internet. [1]

There are presented and used many solutions and techniques to save energy in the IoT devices. These methods are mainly based on reducing wireless broadcasting because it is more energy consuming to broadcast data than pre-analyze it in close proximity of the source (sensor). [4] The IoT sensor data need to be compressed efficiently to reduce and minimize the cost of broadcast and storage [5]. At the same time, many IoT devices are battery powered wireless devices. Thus, these IoT devices can be located in places where changing the battery might be impossible or at least battery replacement cost is one of the most critical source of cost in this kind of devices. [2] These devices are often very limited in computing power. So often, it is the case that it is possible to perform only very light analysis of the collected data in locally. In addition, the IoT itself is very constrained in terms of bandwidth, energy and storage. [5, 6]

The IoT systems and the whole IoT sector is very heterogeneous. The things vary a lot and may move geographically and they need to interact with other things and Cloud systems in real-time mode. When designing the IoT systems it should be taken account scalability and interoperability of the heterogeneous devices. Design of the IoT applications and systems require involvement of many factors like networking, communication, business models and processes, and security. The IoT architecture should be very adaptive to make IoT devices to interact with other devices and with the Internet. [1]

2 Definition of Edge and Fog

The term Fog Computing was introduced by Flavio Bonomi in 2012. [7, 8] It refers to dispersed Cloud computing which is vital in several applications where the IoT devices collect data in the local network and the actions required from analyzed data take place in the same local network. [9] In that kind of case, it is not efficient to send all the data to centralized Cloud to be analyzed. It is not even possible to send data to the Cloud for analysis in many latency critical applications. The term Edge Computing means that computing happens in close proximity of data sources in the edge of the network. In many cases the terms Edge Computing and Fog Computing are interchangeable. But it can be defined that Edge refers more to the device side very close to data sources and Fog refers more infrastructure side like gateways and routers. [10]

Cloud service providers locate their data centers often in rural areas to minimize costs. This lead to high latencies because customers are often located far from data centers. [11] Many IoT applications require very short response times, some create a large amount of data that can be heavy for network and some applications are involved with sensitive private data. Cloud computing cannot reply all these requirements so the Edge Computing is one answer for these challenges. [10] Latency criti-

cal applications are for example many intelligent transportation and traffic systems, autonomous vehicles, virtual reality (VR) and augmented reality (AR) applications. [7] Also many safety critical applications cannot rely on the connection to the Cloud. For example, vehicle-to-vehicle connection or data from vehicles can be used to avoid collision, but that analysis need to be done locally or in very close proximity located Cloudlet [7]. The Cloudlet means smaller size local datacenter. Safety critical systems are also very common in industrial automations systems. These kind of applications cannot tolerate possible Cloud outages and they often need low and predictable latency [7, 11]. This kind of new Fog Computing paradigm is not a replacement of the centralized Cloud. These concepts are more complementary to each other. [9, 11] In some applications the Cloud is not even possible to be used; this kind of situation happens for example in the modern aircraft. The modern aircraft can generate nearly half a terabyte of data from its sensors in one flight. [7] This amount of data cannot be sent to the Cloud for real time analysis from the middle of the ocean. Only possibility is to analyze the data locally and then perhaps download the raw data after flight for further analysis that can be executed in the Cloud. Even in ground level, the current wireless networks will be challenged with the amount of data that the huge amount of devices will produce in the near future [10]. Most of the data produced by the IoT devices will be analyzed locally in the Edge devices and will never be transmitted to the Cloud. [10]

In Fig. 1 is illustrated the basic architecture of the IoT infrastructure including Edge and Fog devices. The difference between the Edge and the Fog devices is not always as clear as presented in Fig 1.

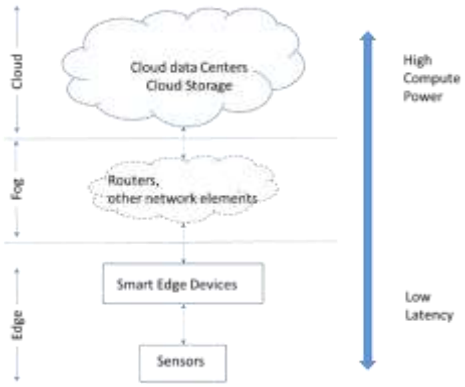

Fig. 1. Edge and Fog architecture in IoT. [12]

Fog and Edge devices can be efficient data servers, routers, gateways, any kind of embedded systems or even end node like vehicles or sensors with some computational capability. [11] The Edge devices can be small-embedded devices with very energy efficient and limited micro controller or more capable single board Linux-computer like Raspberry PI. In Fig 1. typically sensors are small wireless sensor tags and Smart Edge Devices are gateways for sensors. Smart Edge Device (gateway) is connected to

the Internet via wireless or wired connection. Edge and Fog devices are very heterogeneous in nature with different hardware architectures and they run various different Operating Systems (OS). There are also available numerous different wireless access technologies and sensor network topologies [11]. This heterogeneous nature of Edge and Fog devices and systems avoid developing generic and easily adaptable solutions for Edge and Fog analytics. It is predicted that the Edge Computing could have as big impact in society as Cloud Computing has [10].

3 Benefits of the Edge Computing

While the Cloud Computing is very efficient method for data processing having a huge amount of computing power, [10] the Cloud Computing cannot meet and ensure the Quality of Service (QoS) in the IoT due to unstable latency and possible outages in the network connection and the Cloud servers. Fog or Edge Computing is an answer for the problem. In the Edge Computing the majority of the computing is carried out in close proximity of the data source. There are researches done that proof the Edge Computing reduction in response times and in energy consumption. By doing part of computation and analysis in the Edge reduce the needed wireless connection bandwidth. For example, photos can be compressed in the Edge before transmitting to the cloud. [10] Even if most of the data analysis is done in the Cloud, it is recommended to do some preprocessing for sensor data in the Edge before uploading it to the Cloud. In minimum this kind of preprocessing can be only filtering erroneous sensor data. More advanced preprocessing can mean different compression methods like sending only the information of the variation/alteration of the sensor values and not absolute values. This kind of preprocessing can reduce significantly the amount of data needed for upload data in the Cloud [10].

Security and privacy critical application can also benefit from the Edge/Fog Computing approach where the original raw and sensitive data is not sent to the centralized Cloud thru public Internet. [7] Data sent to the Cloud can be denatured data; for example, in images the faces can be blurred. [7] Applications producing very sensitive and private data are for example different healthcare applications.

Also home automation systems sending information to the Cloud could include some private sensitive data. For example, information of the water and electricity usage could easily tell if the house is vacant or not. If the computation is kept in close proximity of this data (in the Edge), it could be decent solution to keep sensitive data in private. [10] But if this home automation application is connected to the Internet, this sensitive data could be reachable for inappropriate quarters. So the cybersecurity is vital for all IoT applications whether the sensitive data is transferred to the Cloud or not.

4 Edge and Fog Computing Challenges

Fog and Edge devices are very heterogeneous. [11] It is difficult to design easily adaptable and generic solutions for the Edge Computing. Most applications are indi-

vidual and cannot utilize generic computational, data aggregation and data analysis methods. There are different hardware platforms and different operational systems. Hardware platforms can vary from very simple micro-controller based platform with very limited memory to single board Linux-computer like Raspberry PI that is rather powerful platform. Virtualization is one way to handle multiplatform and multi-OS challenge.

One possibility towards generic solutions to be used in different and computationally restricted platforms is a container-based approach. Container-based virtualization can be considered as a lightweight virtualization solution. Because of lightweight nature, the containers can run in computationally limited IoT-platform like Raspberry PI. [13, 14] Containers could be used in the different platforms to perform same tasks. Anyway, these platforms could not be very limited basic embedded micro-controller based platforms, but require more computational power and generic operating system (OS) like Linux.

In [15], has been tested the ARM-based Single Board Computers with Docker containers and compared the overall efficiency in power consumption to the native executions. The performance evaluation showed almost negligible impact with container virtualization compared to native executions.

4.1 Methods for Reducing Energy Consumption in Wireless Sensor Networks

Several energy-efficient routing algorithms have been proposed for wireless sensor networks (WSN) but they are mostly not suitable for the IoT. Current IoT devices are mostly static and follow tree-based structure. [16] Dynamic routings developed for WSN architectures are not suitable for the IoT. The IoT network is often a complex large scale network and dynamic routing is difficult to be used effectively in this kind of network. [17]

The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol utilizes several methods and techniques to reduce energy consumption in WSN. [18] LEACH is the most popular routing algorithms used in WSNs [19]. There are several variations and further developments of LEACH protocol like LEACH-C and ENHANCED LEACH for example [16, 20]. Weight energy efficient clustering (WEEC) is an extended version of LEACH. In WEEC the energy efficiency optimization is done by cluster head (CH) selection procedure. Every node in the sensor network can be elected as a cluster head. WEEC is a single-hop routing protocol. [19]

In [16], the authors have presented a cluster head selection for energy optimization (CHSEO) algorithm to reduce the overall energy consumption in the IoT network. The CHSEO algorithm is based on selecting the optimal cluster head of the sensor nodes to reduce overall energy consumption. Hierarchical IoT sensor node framework is composed of different node types. Sensor node is sensing, aggregating and forwarding data, Relay node is receiving the data from sensor nodes and transmit it to the cluster head. Cluster head collects, aggregates and transmit the data to the base station. Base station collects, aggregates, analyses and process the data. The CHSEO algorithm was proved to have better performance than traditional WSN mechanism in energy consumption and network lifetime.

Other example of hierarchical network architecture to reduce IoT network energy consumption is presented in [17]. It is based on hierarchical relay node placement with energy efficient routing mechanism. Ad Hoc On-Demand Distance Vector (AODV) routing protocol has been used. This proposed network architecture gives balanced energy consumption and thus better network lifetime. [17]

Modern long-range low-power IoT networks (NB-IoT, LoRa, SigFox) have star topology, so intelligent routing algorithms are out of the question. [21] In these technologies, the ultra-low energy consumption has been achieved by using very limited bandwidth and/or intelligent modulation.

4.2 Data Compression Methods in Edge Device: Lossy and Lossless Methods

In the IoT, huge amount of sensors are generating data and that data should be stored and processed with minimal loss of information. Sensor data compression is not a new discipline and several different compression algorithms are presented. [5] There are also very energy efficient contemporary compression methods for resource constrained IoT-nodes presented [6]. Data aggregation is also related to the data compression. Data aggregation here means for example to combine multiple sensor data and filter the redundant data. Data aggregation in wireless sensor network reduce the amount of data needed to transmit to the base station and thus reduce energy consumption. [18] Most of the compression methods presented for the IoT sensor data compression are lossy compression methods. Lossy methods are more efficient in compression compared to lossless methods. Lossy methods try to identify meaningful data points and discard redundant data. Different compression algorithms perform differently with different types of data sets. Also their computational complexity differs. [5]

Lossy compression methods can be divided in two groups: Time domain and Transform domain. Time domain compression algorithms compress time series data directly without any transformation. Transform domain compression methods transform data into a different domain. Well-known transform domain methods are for example Discrete Fourier Transform (DFT) and Fast Fourier Transform (FFT). [5] Different lossy compression algorithms are listed in Table 1.

Table 1. Lossy Compression Algorithms. [5, 6]

Name of the Algorithm	**Type**
Box-Car	Time Domain
Backward Slope	Time Domain
OSIsoft PI software	Time Domain
Compression extracting major extrema	Time Domain
PLA, PCA	Time Domain
Critical Aperture (CA)	Time Domain
Fractal Resampling (FR)	Time Domain
Lightweight Temporal Compression (LTC)	Time Domain
Fast Fourier Transform (FFT)	Transform Domain
Discrete Cosine Transform (DCT)	Transform Domain
Chebyshev Transform (CH)	Transform Domain

Wavelet Transform (CWT, DWT, WPT)	Transform Domain

In ref. [5] the authors have selected four different lossy compression methods and compared their applicability to different signal characteristics. Compared methods were Critical Aperture (CA), Fractal Resampling (FR), Chebyshev Transform (CH) and Wavelet Packet Decomposition (WPD). Data used for comparison has been diverse publicly available sensor datasets. Comparison has been made by comparing the compression ratio with same Percentage Root mean square deviation (PRD). PRD level used in comparison has been 5 %. Used datasets were different in composition. Some were quasi-periodic (QP), some non-stationary (NS) with sudden transient spikes and some non-stationary (NS) with periodic seasonal components. [5]

As a result, the CH was the most effective method for QP data in terms of compression ratio. For NS with transient spikes data, the CA, FR and WPD were remarkably more effective than CH method. For NS with periodic seasonal data the WPD is the most effective method. [5]

In [5], it is also shown that WPD requires considerably more computational time compared to the other methods. This means a higher energy consumption. In ref. [6] has been introduced lightweight compression algorithm for spatial data which is more energy efficient than wavelet compression. This lightweight compression algorithm can reduce energy consumption to half of the original consumption. This lightweight and energy-efficient compression algorithm is based on a lightweight temporal compression method named LTC [22]. LTC is tunable in accuracy and suitable for the datasets that are largely continuous and slowly changing. LTC is widely used method due to its good compression performance and low computational complexity. [6] LTC also requires very little storage compared to many other compression techniques. LTC is very effective for many environmental type data (temperature, humidity) which are approximately linear in small enough time window. Thus, LTC leverages temporal linearity of environmental data to compress that data. [22]

5 Wireless Technologies for Energy Efficient IoT

For years the main wireless technology for transmitting sensor data with low energy consumption was IEEE 802.15.4 (mostly used protocol is called ZigBee). ZigBee was designed for ultra-low energy consumption and it has been popular in WSNs. [21] IEEE 802.11 (WiFi) has also been available for years but traditionally it has been used for high data rates and it has had rather high energy consumption. To address this energy consumption problem, there is available Power Saving Mode (PSM) in IEEE 802.11. [18] This Power Saving Mode is developed for battery powered mobile devices. IEEE 802.11 was not designed for sensor applications but with PSM it has proofed to be potential alternative for other technologies used for WSNs. In some cases, the IEEE 802.11 PSM can outperform the IEEE 802.15.4 in energy consumption. [23] Bluetooth Low Energy (BLE) is very popular and widely used due to its availability. It is already available in most modern smartphones and it is widely used in wearable devices like heart rate monitors and other monitoring applications.

ZigBee, BLE and WiFi uses the 2.4 GHz ISM frequency band while ZigBee is available also in sub-1 GHz band (868 and 915 MHz). IEEE 802.11ah version address for requirements of the IoT, like increased range, increased reliability and low energy consumption. IEEE 802.11ah is operated in sub-1 GHz range. [21]

Using sub-1 GHz band increases the range and penetration thru obstacles (buildings, constructions). Sub-1 GHz band is also less crowded compared to popular 2.4 GHz band and thus these technologies are less vulnerable for interference. [24]

ZigBee, BLE and WiFi all have rather short range, even if sub-1 GHz band is used (ZigBee and WiFi). As an answer for this limitation there are recent developments in long-range technologies like SigFox and LoRa. These are so called low-power wide-area-networks (LPWAN) [25]. SigFox is an ulta-narrow-band technology and it uses sub-1 GHz band (868 MHz in Europe). Its range is announced to be even up to 40 km. Direct competitor for SigFox is the LoRa. It uses the same frequency band as SigFox but its modulation is based on Chirp Spread Spectrum (CSS). [21] CSS modulation was developed in the 1940's and it is very robust for interference and multipath fading. In CSS modulation the information in spread to different frequency channels and it has noise like properties. [26]

Novel cellular based wireless technology for IoT solutions is Narrow Band-IoT (NB-IoT) which uses narrow bandwidth for lower power consumption. [27] The Third Generation Partnership Project (3GPP) introduced the NB-IoT in LTE Release 13. NB-IoT bandwidth for both uplink and downlink is set to 180 kHz. It is exactly size of one physical resource block (PRB) in LTE standard. [28]

In Table 2 has been combined the main characteristics of the main WSN technologies used in the IoT. LPWAN technologies have long range and very limited data rate. ZigBee, BLE and WiFi have much higher data rate but the range is very limited.

Table 2. Wireless technologies summary for IoT. [1, 23, 24, 26]

Technology	**Band**	**Topology**	**Announced range**	**Data rate**
802.15.4	2.4 GHz / 0.9 GHz	Meshed	50 m	0.25 Mb/s
BLE	2.4 GHz	Scatternet	10 m	0.125 – 2 Mb/s
802.11 PSM	2.4 GHz	Star	100 m	11 Mb/s
802.11ah	0.9 GHz	Star	100m – 1 km	0.15 – 78 Mb/s
SigFox	0.9 GHz	Star	Up to 40-50 km	100 b/s or 1000 b/s
LoRa	0.9 GHz	Star	Up to 15 km (suburban), 45 km (rural)	0.25 – 50 kb/s
NB-IoT	700-900 MHz	Star	Up to 35 km	20-65 kb/s

As both SigFox and LoRa uses unlicenced ISM band, there is no guarantee for latency. For latency critical applications, the NB-IoT is better choice while SigFox and LoRa are suitable for low-cost projects with wide area coverage [26]. NB-IoT latency is maximum 10 seconds according to the standard, while SigFox and Lora can have latency of 10s of seconds. [27, 28] Lora and SigFox are both very energy efficient technologies with very large range. BLE is also very energy efficient in its range. [21]

6 Energy Efficient IoT Protocols

The most common IoT application protocols are MQTT, CoAP, XMPP and AMQP. MQTT (message queue telemetry transport) and CoAP (constrained application protocol) are designed especially for resource constrained devices like IoT end nodes and gateways. [29, 30]

MQTT protocol is a publish-subscribe messaging protocol with minimal bandwidth requirements. It uses TCP (transmission control protocol) for transport. It is designed to be used in devices with restricted computational power and limited memory. MQTT is considered as a perfect messaging protocol for M2M and IoT applications because of its ability to function within low power, low memory and cheap devices with low bandwidth networks. [29]

CoAP protocol is a request-response protocol but it can function as a publish-subscribe mode too. CoAP uses UDP (user datagram protocol) for transport but it can be used for TCP too. CoAP has a wide acceptance for constrained devices. [30]

In ref. [30] the authors have made comparison and experimental analysis between MQTT and CoAP. As a result they have found that MQTT consumes more bandwidth for transferring same payload than CoAP. But both protocols are efficient in terms of energy consumption.

In ref. [31] have been evaluated the performance, energy efficiency and resource usage of several IoT protocols (MQTT, CoAP, MQTT-SN, WebSocket and TCP). As a result, the authors found that MQTT and CoAP protocols are largely affected by the packet size. In generally CoAP is the most efficient in terms of energy consumption and bandwidth usage. But MQTT protocol is more reliable.

XMPP (extensible messaging and presence protocol) and AMQP (advanced message queuing protocol) are other popular protocols but they require more resources and they are not so suitable for resource constrained devices.

7 Security and Privacy Issues in the Edge

Privacy and security is a very big issue and concern in the IoT systems and applications. In the IoT systems, the end nodes (IoT devices) are connected to the Internet and thus these devices are reachable from all over the Internet. This kind of devices can be for example IP-cameras, health monitors and wearable devices or even WiFi connected toys. These devices can be connected by others if not protected properly.

Ownership of the collected data is other issue to take account. If the data is left on edge device for storage and analysis, then there are no ownership problems as the owner of the device can have all the rights for that data. [10]

Battery powered IoT devices have very limited computational power, so complex encryption techniques require significant amount of computing and thus increase energy consumption. Lightweight encryption algorithms for the IoT devices have been developed.

Encryption scheme can be symmetric or asymmetric and both can be used in the IoT devices. In symmetric encryption scheme only one key is used to encrypt and

decrypt the data. Both sender and receiver need to know the same key. In asymmetric encryption scheme two distinct keys are used. One for encrypting and other for decrypting. The advantage here is that the encrypting key can be public key and available to anyone. For asymmetric scheme the key need to be longer than in symmetric scheme to be secure. Thus calculations needed are longer than in symmetric scheme. Famous asymmetric encryption schemes are Rivest, Shamir, Adleman (RSA) scheme and Elliptic Curve Cryptography (ECC). [32]

Several researches have been done to compare ECC and RSA schemes to each other in regarding to encryption/decryption time and key length. The ECC has proved to be more efficient with shorten encryption/decryption time, smaller storage and in generally more energy efficient than RSA. [33]

In ref. [34] the authors have presented lightweight asymmetric encryption scheme called AAβ and in ref. [35] the authors have made comparison in energy consumption between AAβ and RSA. The AAβ outperforms the RSA significantly in encryption and decryption.

8 Conclusions

In this study, a comprehensive study of the energy efficient Edge Computing has been carried out. There are a lot of research published from the different phases and aspects to reduce energy consumption in wireless end devices, but only few of them encompass the subject broadly. Minimizing energy consumption is one of the key aspects to carry out in the IoT device and system development. IoT end devices are often battery powered devices with wireless connection. Thus the computational resources are constrained but at the same time these devices should be able to do pre-processing and analysis for sensor data to reduce transferred data via wireless connection.

Most methods for reducing energy consumption in the IoT devices are concentrated to reduce wireless data transfer. Wireless data transfer is often the most energy consuming operation in the IoT device. In addition, many latency critical applications are pushing the development towards Edge Computing.

At the same time when more and more data analysis is carried out in close proximity of the sensors (in Edge and Fog); there are available several novel wireless technologies to transfer sensor data with low energy consumption. Considering energy consumption in every phase from the sensor to the Internet, it is possible to reduce energy consumption significantly. Many of these techniques are studied in this survey.

References

1. Li, S., Xu, L.D. & Zhao, S.: The internet of things: a survey. In: Springer Information Systems Frontiers, Volume 17, Issue 2, pp 243-259, April 2015.
2. Montori, F., Contigiani, R., Bedogni, L.: Is WiFi suitable for energy efficient IoT deployments? A performance study. In: 2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI), Modena, 2017, pp. 1-5.

3. Jayakumar, H., Raha, A., Kim, Y., Sutar, S., Lee, W.S., Raghunathan, V.: Energy-efficient system design for IoT devices. In: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, 2016, pp. 298-301.
4. Stojkoska, B.R., Nikolovski, Z.: Data compression for energy efficient IoT solutions. In: 2017 25th Telecommunication Forum (TELFOR), Belgrade, 2017, pp. 1-4.
5. Bose, T., Bandyopadhyay, S., Kumar, S., Bhattacharyya, A., Pal, A.: Signal Characteristics on Sensor Data Compression in IoT - An Investigation. In: 2016 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops), London, 2016, pp. 1-6.
6. Ying, B.: An Energy-Efficient Compression Algorithm for Spatial Data in Wireless Sensor Networks. ICACT 2016.
7. Satyanarayanan, M.: The Emergence of Edge Computing. Computer, vol. 50, no. 1, pp. 30-39, Jan. 2017.
8. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing-MCC '12, Helsinki, Finland, 17 August 2012; pp. 13–15.
9. Jalali, F., Khodadustan, S., Gray, C., Hinton, K., Suits, F.: Greening IoT with Fog: A Survey. In: 2017 IEEE International Conference on Edge Computing (EDGE), Honolulu, HI, 2017, pp. 25-31.
10. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.
11. Venkat Narayana Rao, T., Amer Khan, M.D., Maschendra, M., Kiran Kumar, M.: A Paradigm Shift from Cloud to Fog Computing. IJCSET (www.ijcset.net) Vol 5, Issue 11, pp 385-389. November 2015.
12. Yigitoglu, E., Mohamed, M., Liu, L., Ludwig, H.: Foggy: A Framework for Continuous Automated IoT Application Deployment in Fog Computing. In: 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, 2017, pp. 38-45.
13. Morabito, R.: A performance evaluation of container technologies on Internet of Things devices. In: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), San Francisco, CA, 2016, pp. 999-1000.
14. Pahl, C., Helmer, S., Miori, L., Sanin, J., Lee, B.: A Container-Based Edge Cloud PaaS Architecture Based on Raspberry Pi Clusters. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, 2016, pp. 117-124.
15. Morabito, R.: Virtualization on Internet of Things Edge Devices With Container Technologies: A Performance Evaluation. IEEE Access, vol. 5, pp. 8835-8850, 2017.
16. Krishna, P.V., Obaidat, M.S., Nagaraju, D., Saritha, V.: CHSEO: An Energy Optimization Approach for Communication in the Internet of Things. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.
17. Cho, Y., Kim, M., Woo, S.: Energy efficient IoT based on wireless sensor networks. In: 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 294-299.
18. Dargie, W., Poellabauer, C.: Fundamentals of Wireless Sensor Networks, Theory and Practise. Wiley (2010).
19. Bhushan, B., Sahoo, G.: A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In: 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, 2017, pp. 294-299.

20. Kumar, S., Verma, U.K., Sinha, D.: Performance analysis of LEACH and ENHANCED LEACH in WSN. In: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, 2016, pp. 1-7.
21. Morin, É., Maman, M., Guizzetti R., Duda, A.: Comparison of the Device Lifetime in Wireless Networks for the Internet of Things. IEEE Access, vol. 5, pp. 7097-7114, 2017.
22. Schoellhammer, T., Osterwein, E., Greenstein, B., et al.: Lightweight temporal compression of microclimate datasets. In: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks IEEE Computer Society, 2004, pp. 516-524.
23. Tozlu, S.: Feasibility of Wi-Fi enabled sensors for Internet of Things. In: 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, 2011, pp. 291-296.
24. de Carvalho Silva, J., Rodrigues, J.J.P.C., Alberti, A.M., Solic, P., Aquino, A.L.L.: LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities. In: 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, 2017, pp. 1-6.
25. Ayele, E.D., Hakkenberg, C., Meijers, J.P., Zhang, K., Meratnia, N., Havinga, P.J.M.: Performance analysis of LoRa radio for an indoor IoT applications. In: 2017 International Conference on Internet of Things for the Global Community (IoTGC), Funchal, 2017, pp. 1-8.
26. Poursafar, N., Alahi, M.E.E., Mukhopadhyay, S.: Long-range wireless technologies for IoT applications: A review. In: 2017 Eleventh International Conference on Sensing Technology (ICST), Sydney, NSW, 2017, pp. 1-6.
27. Wang, H., Fapojuwo, A.O.: A Survey of Enabling Technologies of Low Power and Long Range Machine-to-Machine Communications. IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2621-2639, Fourthquarter 2017.
28. Xu, J., Yao, J., Wang, L., Ming, Z., Wu, K., Chen, L.: Narrowband Internet of Things: Evolutions, Technologies and Open Issues. IEEE Internet of Things Journal, 2017.
29. Yassein, M.B., Shatnawi, M.Q., Aljwarneh, S., Al-Hatmi, R.: Internet of Things: Survey and open issues of MQTT protocol. In: 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, 2017, pp. 1-6.
30. Bandyopadhyay, S., Bhattacharyya, A.: Lightweight Internet protocols for web enablement of sensors using constrained gateway devices. In: 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, 2013, pp. 334-340.
31. Mun, D.H., Dinh, M.L., Kwon, Y.W.: An Assessment of Internet of Things Protocols for Resource-Constrained Applications. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, 2016, pp. 555-560.
32. Adnan, S.F.S., Isa, M.A.M., Hashim, H.: Analysis of asymmetric encryption scheme, AAβ Performance on Arm Microcontroller. In: 2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Langkawi, 2017, pp. 146-151.
33. Diro, A.A., Chilamkurti, N., Nam, Y.: Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication. IEEE Access.
34. Ariffin, M.R.K., Asbullah, M.A., Abu, N.A., Mahad, Z.: A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of N=P^2 .q. In: Malaysian J. Math. Sci. 7(S) 19-37 Spec. Issue 3rd Int. Conf. Cryptol. Comput. Secur. 2012, vol. 7, pp. 1– 6, 2012.
35. Adnan, S.F.S., Isa, M.A.M., Hashim, H.: Energy analysis of the AAβ lightweight asymmetric encryption scheme on an embedded device. In: 2016 IEEE Industrial Electronics and Applications Conference (IEACon), Kota Kinabalu, 2016, pp. 116-122.