A Survey on IoT Protocol in Real-Time Applications and Its Architectures

M. L. Umashankar, S. Mallikarjunaswamy, N. Sharmila, D. Mahesh Kumar, and K. R. Nataraj

Abstract In recent days, activities are completely automated and are more flexible because of Internet of Things [IoT]. Due to IoT devices, effective integrated communication between all types of embedded devices is possible. The devices should have communication in stipulated range through the support of Internet. This significant functionality is built by the IoT protocols. In the digital world, internet-connected devices has enabled the IoT protocols to be one of the significant fields in computing, and it acts as a bridge between the physical and the cyber-world. This paper gives a brief overview of Internet of Things (IoT) and standards used to it. Important IoT protocols and their review are presented. The similarities and dissimilarities of Advanced Message Queuing Protocol (AMQP) and Message Queue Telemetry Transport (MQTT) protocols are also discussed. The main aim of this review papers is to provide a functional view of IoT architecture, standards and protocols.

Keywords Advanced message queuing protocol · Message queuing telemetry transport · Constrained application protocol · Internet of things

M. L. Umashankar
Department of Artificial Intelligence and Machine Learning, BMS Institute of Technology and Management, Bangalore, Karnataka 560064, India

S. Mallikarjunaswamy (✉) · K. R. Nataraj
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bangalore, Karnataka 560060, India
e-mail: pruthvi.malli@gmail.com

N. Sharmila
Department of Electrical and Electronics Engineering, JSS Science and Technology University, Mysore, Karnataka 570006, India

D. Mahesh Kumar
Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bangalore, Karnataka 560060, India

A. Kumar et al. (eds.), *ICDSMLA 2021*, Lecture Notes in Electrical Engineering 947,
https://doi.org/10.1007/978-981-19-5936-3_12

1 Introduction

The increase in the use of Internet on the everyday task and rapid growth in technology are revolutionizing and automatizing the world scenario to improve the quality of human lives as shown in Fig. 1. IoT enables the Internet-connected devices to connect together for different application. It is network of different combination of domain and heterogeneous devices. These devices act as an actuators to sense the inputs and respond immediately by quickly analyzed. The physical devices of the network are realized by using these sensing devices and can be used in several application such as communication, transportation, agriculture, home automation, healthcare, industrial automation and emergency services. Raspberry Pi and Arduino microcontrollers are enable the devices to measure sensor's data and send it over the Internet. Car, refrigerator and any other electronic devices are the example of such devices. Nowadays use of transmission, collection, consolidation and displaying of sensor's data are most common practice. In other words, data between physical devices each other are being controlled by IoT physical devices. In upcoming days, billions and trillions of devices will get involved in building a smarter world [1]. In addition to this, IoT application is extended to smart domain such as e-health, transportation, home and industry automation as described by Said and Albagory [2]. IoT is a model of large number of heterogeneous devices, so data interoperability is a challenge in data mining. To overcome this issue, most popular methods are presented in Madhu et al. [3]. In IoT, many researchers are contributing in design and development of protocols for different fields of IoT. The secure authentication is provided for different nodes or devices in a hierarchical network of IoT. Pooja et al. [4] presented protocol for secure communication among the nodes which is formulated using three way authentications. Sadiya Thazeen et al. [5] presented comparison of IoT and Cyber-Physical Systems (CPS). Several aspects of IoT and CPS are consider during comparison such as differences between CPS and IoT, overview of the CPS, security and privacy in IoT, challenges of each layer of architectures and various architectures of IoT.

Li et al. [6] presented a survey on security and privacy in IoT. In this paper, different attack on IoT device, limitation of the IoT device, IoT security at different layers, authentication and access to IoT device have been addressed. Hence, this helps in to understand various aspects of security. The rest of this paper is organized as follows; Internet of things functional overview is presented in Sect. 2, the protocol standards are discussed and highlighted in Sect. 3, comparative analysis of AMQP and MQTT is presented in Sect. 4 and Conclusion is presented in Sect. 5.

2 Functional Overview of IOT

Sensing, analysis, communication and computation are the four functioning modules of Internet of Things. IoT implementation using different functional modules is

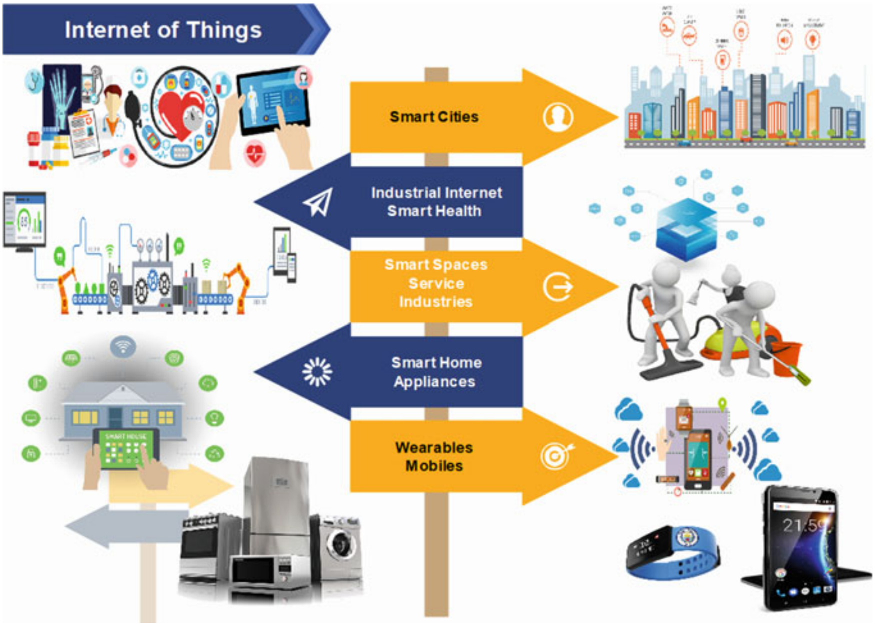

Fig. 1 IoT applications

shown in Fig. 2 [7]. These functional modules are used to establish the functional environment for different applications ranging from industries to healthcare.

2.1 Sensing

Different types of sensors are used to collect different types of data such as non-programmable peripheral interface devices, actuators, etc. [8]. The sensing devices collect the data in raw form and store it in temporary storage without processing. In the constrained environment such as the uses of deployment and low power, these devices are used.

2.2 Communication

Several protocols such as Wi-Fi, Bluetooth, LTE-Advanced, NFC, UWB, RFID and communication links are used to store the data in storage devices. To implement IoT standards such as MQTT, CoAP, AMQP, Data Distribution Service (DDS), Extensible Messaging and Presence Protocol (XMPP), etc. [9], above protocols are used since it support for the IoT platform. Device usability and their environment need to

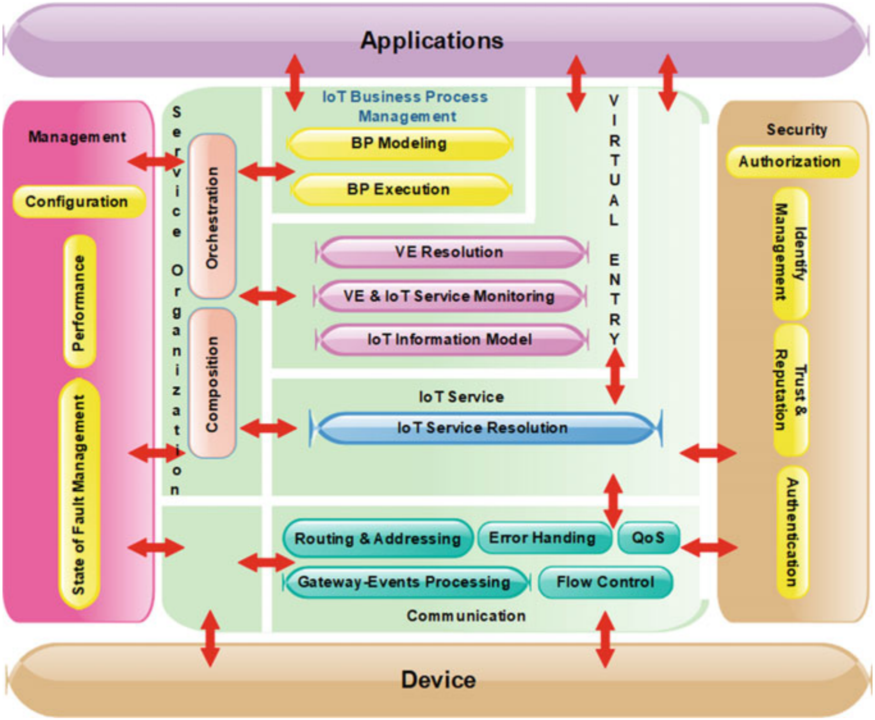

Fig. 2 IoT functional view

be keeping in the mind when developing these protocols. As the growth of Internet of Things is increased rapidly, the network will be connected with large number of heterogeneous devices. In IoT communication due to this various issues communication between the devices is challenging such as memory usage, Quality of Service (QoS), addressing and identification.

2.3 Computation

Structures of data verification make them available for processing which is done by protocols during computation. The separate hardware and software level of processing is done. Cloud computing and Fog or Edge are used on software level. Embedded devices such as sensors, actuators and other devices are connected in IoT. The above devices generates large amount of data, and to extract knowledge from this, a complex computations is required. In Lenka et al. [10] presented various IoT platforms for hardware utilization such as the, Raspberry Pi, Intel Galileo, BeagleBone, Cubieboard, Arduino and WiSense. Authors also highlighted use of smart devices such as laptop and mobile. Different software and operating systems are used by these smart devices such as C, C++, JAVA and TinyOS, LiteOS, RiotOS, Android, Contiki etc. The Fog or Edge computing and cloud computing which provide smart computing ability to IoT [11]. A cloud is a platform which stores the data and managed the data in real time, and it can be processed further for intelligent analysis.

2.4 Analysis

Analysis is extracting the vision from information for further processing in IoT. Through sensors data are collected in the form of batches during analysis. These data are in large amount, and it is called Big Data. Analysis of data helps in understanding disposal of the data, with interest toward avoiding failures minimizing maintenance and improving operations.

- **Analysis of Intelligent**: Cognitive technologies driven the analysis of data. The data analysis process varies in the form of voice, information, vision and usability with the ability of technological advancement. For real-time data streams, analysis is very much required. Within an IoT managing, the real-time data and ability to analyze unstructured data in data model are the open challenging issues in data analytics.
- **Intelligent Actions**: Machine to Human (M2H) and Machine to Machine (M2M) interfaces can be expressed for intelligent actions. In improving machine functionality and minimizing the machine prices, an intelligent agent will play a vital role in IoT [12]. In unpredictable situations, machine actions will become more challenging to privacy, security, machine interoperability and mean-reverting human behaviors which slow adoption of new technologies in IoT as described by Shin et al. [13], Taher et al. [14] IoT functions, elements and levels are illustrated in Table1.

3 Standards

Internet of Things has covered scope of different areas and fields. To provide the features of IoT and to support in various distinct fields, protocols and standards are used by many groups. Many organizations such as Internet Engineering Task Force (IETF), Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE) are proposed several standards to support of Internet of Things. Protocols standardization is process is fully done by the Internet Engineering Task Force Ghahramani [12]. Different level of standards is highlighted in Fig. 3. Different domains such as infrastructures, influential and application above standards are utilized [15].

Table 1 IoT levels, functions and elements

Level	Function	Elements
Sensing	Raw data sense and measure	Actuators, smart sensors, RFID tags and embedded sensors
Communication	At application and infrastructure level, a gateway protocols are used for linking and providing	**Application level** HTTP-REST, CoAP, MQTT, AMQP, DDS and XMPP **Infrastructure level** IEEE 802.15.4, LTE-A, Z-wave, RPL, EPC-global and IPV4/IPV6 6LowPAN
Computational	Processing and storage ability provided by software and hardware level	**Software:** LiteOS, TinyOS, Android, RiotOS, Cloud Computing and Contiki **Hardware:** Microprocessors, Microcontrollers, Arduino and Raspberry Pi
Analysis	For specific purpose normalize and concluding the data	For services related identity purpose, ubiquitous services, collaborative aware services and information aggregation

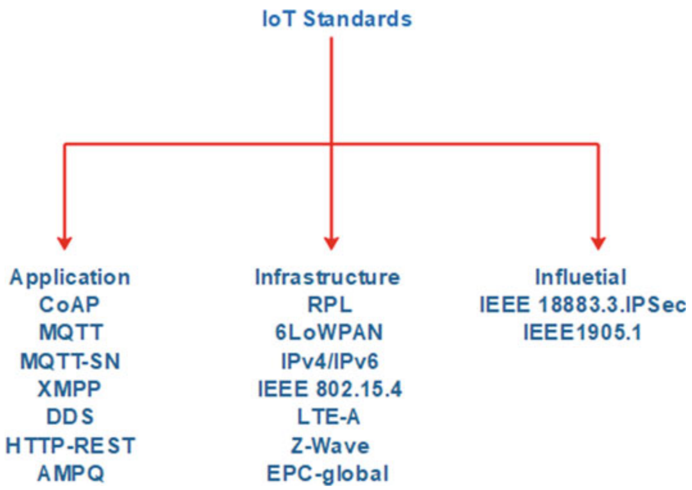

Fig. 3 IoT standards

3.1 Application Protocols

The data presentation and formatting is the responsibility of the application layer. HTTP protocol has been considered as reference protocol form long time in communication as shown in Fig. 4. HTTP especially supported for Internet applications

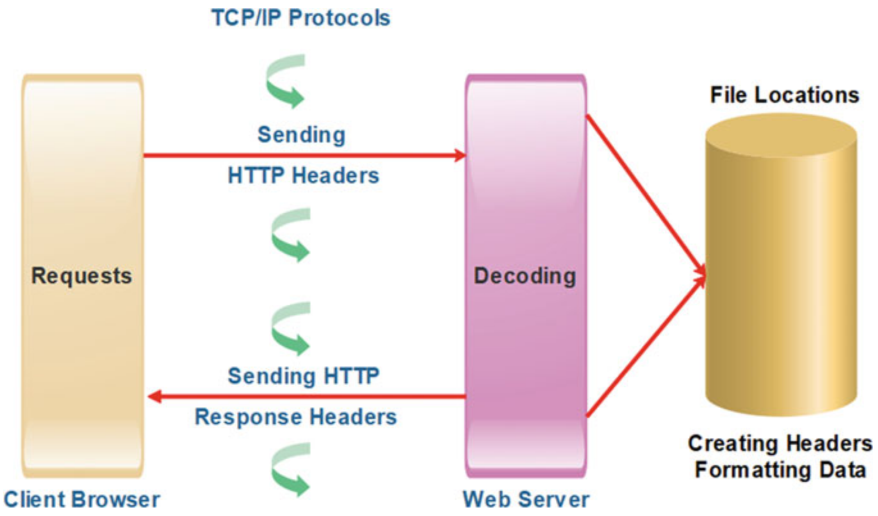

Fig. 4 HTTP protocol formation

but HTTP is not suitable for some of the constrained environment. Hence to find solution, several other protocols are developed such as MQTT, CoAP, MQTT-SN, XMPP, DDS, AMQP etc. The protocols MQTT and AMQP are most popular and widely used protocols [13]. Some of the popular protocols discussed in this section are Shin et al., Taher et al.

3.2 *Constrained Application Protocol (CoAP)*

IETF is proposed the CoAP for managing and retrieving information for devices and sensors. For IoT, application layer protocol and literature with functionalities are presented of CoAP), Municio et al. [16]. Fulfilling the needs of resource-constrained devices which is the primary aim of CoAP protocol. Two-layered approach is used by CoAP; request–response models and processing the features of messaging. In general, the messaging model deals with interchanging the messages asynchronously through the user datagram protocol Stute et al. [17]. For IoT applications, CoAP is bound to UDP to make it more suitable Moosavi [18]. Hence, it is not limited to TCP and DTLS implementation if required. It uses protocols such as Representational State Transfer (REST) protocol to share the communication model with HTTP Mahendra et al. [19]. Confirmable, Non-confirmable, Acknowledge and Reset are four types of messages which are represented by two bits such as 00, 01, 10 and11, respectively. It is well suited for constrained oriented environments, and it uses four methods supported by HTTP Get, Post, Put and Delete Mallikarjunaswamy et al. [20].

3.3 Message Queuing Telemetry Transport (MQTT)

MQTT is designed based on binary lightweight protocol as bandwidth efficient and consumes very low power. It is called as reliable protocol since it uses acknowledgment scheme in all formats as shown in Fig. 5. It uses the concept of asynchronous message queuing, hence it is referred as open protocol. For machine-to-machine communication, it uses subscribe architecture or publish in an environment of low bandwidth and works on transmission control protocol. Connection semantics, routing and endpoint are the three elements specification provided by MQTT Shivaji et al. [21]. Publisher, subscriber and broker are the three component consists in the protocol. To enable the messages be pushed to the clients, the publish and subscribe are event-driven. MQTT broker is with the central control. Between the sender and right receivers, the broker is responsible for dispatching all messages is given in Eq. 1.

$$\begin{aligned}\text{MQTT packet length} &= \text{control header} + \text{length} + \text{protocol level}\\ &\quad + \text{connect flags} + \text{payload}\end{aligned} \tag{1}$$

QoS level of delivery assurance is defined by protocol level. Maximum 4 bytes is the packet length and control header is fixed 1 byte. MQTT protocols are developed in two versions, for TCP/IP protocol, MQTT is designed and for UDP and ZigBee protocols, MQTT-SN is designed.

3.4 Advanced Message Queuing Protocol (AMQP)

For the message-oriented environment, AMQP is an open standard application layer protocol is addressed in Mallikarjunaswamy [22]. AMQP is an open standard application layer protocol for the message-oriented environment which is presented in Chaitra et al. [23]. Its main objective is to enhance interoperability by making to operate in different systems and applications to work together. It is also open source and asynchronous protocol. AMQP has a same architectural scheme as MQTT like publishing, broker and subscriber, but it includes message exchange mechanism like separate queues for the respective subscriber as shown in Fig. 6.

According to the predefined criteria as shown in Fig. 6, the exchange model receives the messages from the publisher and route them to queues. To examine the message and route, it uses a routine and instances in proper queue by using key, which is called as a virtual address.

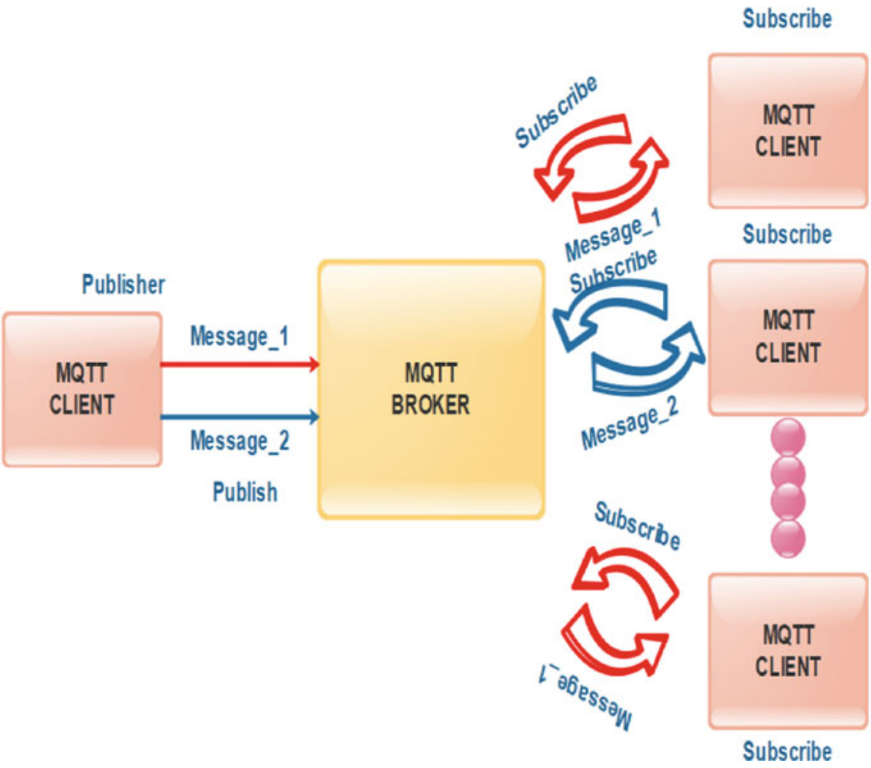

Fig. 5 MQTT communication protocol

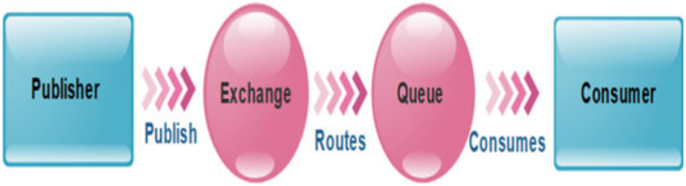

Fig. 6 Mechanism of AMQP protocol

4 AMQP and MQTT Comparative Analysis

In the literature, most popular protocols used are AMQP and MQTT. Different parameters are consider to make comparison between MQTT and AMQT such as frame structure as in Table 2, use of the protocol, response and transaction. The similarities and dissimilarities are highlighted in Tables 3 and 4 of MQTT, CoAP and AMQT protocols [24–27].

Table 2 CoAP and MQTT protocol comparison

CoAP	MQTT
Works over UDP	Works over UDP
4-bytes size of packet header	2-bytes size of packet header
Avoid duplication of messages	Using message-ID and DUP flag duplication of messages are avoided
Messages on the original device and convention named topics are used to manage their sources	On the device itself, resources are managed

Table 3 AMQP and MQTT protocol similarities

AMQP	MQTT
Similarities	(1) Queuing scheme of message
	(2) Nature of asynchronous
	(3) Cloud computing supports
	(4) Minimal set of configuration
	(5) TCP/IP developed

Table 4 AMQP and MQTT protocol dissimilarities

	AMQP	MQTT
Protocol use	For any bandwidth network and for any device, AMQP protocol can be used	In low bandwidth, networks intended to design for small and dump devices MQTT protocol is preferred
Optimization of frame	Fragmentation use buffered oriented approach is used by AMQP protocol	• Writing of frames is easy for low memory devices using stream oriented approach of MQTT protocol • No fragmentation
Transaction	Across message queues, it supports transactions	Not support for transaction
Response	Different acknowledgment is supported with use cases	Basic acknowledgments are supported

The comparison results MQTT and AMQP helps in selection of protocols in different IoT application in a real-life scenario.

5 Conclusion

Internet of Things has a huge contribution for the development of technology and application design along with the artificial intelligence and machine learning. Data is a major component in all the applications. Secure data transfer is of utmost importance via networking interfaces which has to be authenticated. Protocols and computational algorithms are necessary for processing the senses data through various IoT devices to predict results. In this paper, we present the overview and characteristics of IoT protocols. Apart from this, an extensive analysis has been carried out on the IoT application layer protocol such as CoAP, AMQP and MQTT used in different IoT applications. Furthermore, we have highlighted similarities, dissimilarities and comparison of application layer protocol. However, this review helps the several researchers to identify and utilize in appropriate protocol for different real-time IoT applications.

Acknowledgements The authors would like to thank BMS Institute of Technology and Management, Bengaluru, JSS Academy of Technical Education, Bengaluru, Don Bosco Institution of Technology, JSS Science and Technology, Mysore, SJB Institute of Technology, Bengaluru, Visvesvaraya Technological University (VTU), Belagavi , Vision Group on Science and Technology (VGST) Karnataka Fund for Infrastructure strengthening in Science and Technology Level—2 and Center For Interdisciplinary Research (CIR) JSSATEB for all the support and encouragement provided by them to take up this research work and publish this paper.

References

1. Umashankar ML et al (2020) Design of high speed reconfigurable distributed life time efficient routing algorithm in wireless sensor network. J Comput Theor Nanosci 17:3860–3866
2. Said O, Albagory Y, Nofal M, Al Raddady F (2017) IoT-RTP and IoT-RTCP: adaptive protocols for multimedia transmission over internet of things environments. IEEE Access 5:16757–16773
3. Madhu TA et al (2020) Design of fuzzy logic controlled hybrid model for the control of voltage and frequency in microgrid. Indian J Sci Technol 13(35):3612–3629
4. Pooja S et al (2021) Adaptive sparsity through hybrid regularization for effective image deblurring. Indian J Sci Technol 14(24):2051–2068
5. Thazeen S et al (2021) Conventional and subspace algorithms for mobile source detection and radiation formation. Traitement Signal 38:135–145
6. Li P, Su J, Wang X (2020) iTLS: lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy. IEEE Internet Things J 7(8):6828–6841
7. Swamy SN, Kota SR (2020) An empirical study on system level aspects of internet of things (IoT). IEEE Access 8:188082–188134
8. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M (2018) Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet Things J 5(1):269–282
9. Liu A, Alqazzaz A, Ming H, Dharmalingam B (2021) Iotverif: automatic verification of SSL/TLS certificate for IoT applications. IEEE Access 9:27038–27050
10. Lenka RK, Rath AK, Sharma S (2019) Building reliable routing infrastructure for Green IoT network. IEEE Access 7:129892–129909

11. Ma Y, Yan L, Huang X, Ma M, Li D (2020) DTLShps: SDN-based DTLS handshake protocol simplification for IoT. IEEE Internet Things J 7(4):3349–3362
12. Ghahramani M, Javidan R, Shojafar M, Taheri R, Alazab M, Tafazolli R (2021) RSS: an energy-efficient approach for securing IoT service protocols against the DoS attack. IEEE Internet Things J 8(5):3619–3635
13. Shin D, Yun K, Kim J, Astillo PV, Kim J, You I (2019) A security protocol for route optimization in DMM-based smart home IoT networks. IEEE Access 7:142531–142550
14. Taher BH, Jiang S, Yassin AA, Lu H (2019) Low-overhead remote user authentication protocol for IoT based on a fuzzy extractor and feature extraction. IEEE Access 7:148950–148966
15. Al-Janabi TA, Al-Raweshidy HS (2018) A centralized routing protocol with a scheduled mobile sink-based AI for large scale I-IoT. IEEE Sensors J 18(24):10248–10261
16. Municio E, Latré S, Marquez-Barja JM (2021) Extending network programmability to the things overlay using distributed industrial IoT protocols. IEEE Trans Ind Inf 17(1):251–259
17. Stute M, Agarwal P, Kumar A, Asadi A, Hollick M (2020) LIDOR: a lightweight DoS-resilient communication protocol for safety-critical IoT systems. IEEE Internet Things J 7(8):6802–6816
18. Moosavi SR (2015) SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Comput Sci 52:452–459
19. Mahendra HN et al (2019) Evolution of real-time onboard processing and classification of remotely sensed data. Int J Eng Adv Technol 9:7153–7158
20. Mallikarjunaswamy S et al (2020) Implementation of an effective hybrid model for islanded microgrid energy management. Indian J Sci Technol 13:2733–2746
21. Shivaji R et al (2020) Design and implementation of reconfigurable DCT based adaptive PST techniques in OFDM communication system using interleaver encoder. Indian J Sci Technol 13:2108–2120
22. Mallikarjunaswamy S et al (2014) Design of high-speed reconfigurable coprocessor for next-generation communication platform. Emerg Res Electron Comput Sci Technol 57–67
23. Chaitra S et al (2021) A comprehensive review of parallel concatenation of LDPC code techniques. Indian J Sci Technol 14:527–539
24. Satish P et al (2020) A comprehensive review of blind deconvolution techniques for image deblurring. Traitement Signal 37:135–145
25. Manjunath TN, Mallikarjunaswamy S, Komala M, Sharmila N, Manu KS (2021) An efficient hybrid reconfigurable wind gas turbine power management system using MPPT algorithm. Int J Power Electron Drive Syst (IJPEDS) 12(4):2501–2501
26. Mallikarjunaswamy S, Sharmila N (2021) A novel architecture for cluster based false data injection attack detection and location identification in smart grid. Adv Thermofluids Renew Energy 599–611
27. Shivaji R, Nataraj KR (2021) Implementation of an effective hybrid partial transmit sequence model for peak to average power ratio in MIMO OFDM system. In: 2nd international conference on data science, machine learning and applications, pp 1343–1353