

Received 2 September 2022, accepted 18 September 2022, date of publication 26 September 2022,  
date of current version 30 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3209376

TOPICAL REVIEW

# Data Exchange Techniques for Internet of Robotic Things: Recent Developments

NEHA KOUL<sup>1</sup>, NEERENDRA KUMAR<sup>1</sup>, AQSA SAYEED<sup>1</sup>, CHAMAN VERMA<sup>2</sup>,  
AND MARIA SIMONA RABOACA<sup>3,4,5</sup>

<sup>1</sup>Department of Computer Science and IT, Central University of Jammu, Jammu 181143, India

<sup>2</sup>Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, 1053 Budapest, Hungary

<sup>3</sup>University Politehnica of Bucharest, 060042 Bucharest, Romania

<sup>4</sup>Department of Civil Engineering and Management, Faculty of Civil Engineering, Technical University of Cluj-Napoca, 400020 Cluj-Napoca, Romania

<sup>5</sup>ICSI Energy Department, National Research and Development Institute for Cryogenics and Isotopic Technologies, 240050 Ramnicu Valcea, Romania

Corresponding authors: Chaman Verma (chaman@inf.elte.hu), Neerendra Kumar (neerendra.csit@cuammu.ac.in), and Maria Simona Raboaca (mariasimona1706@gmail.com)

The work of Chaman Verma was supported in part by the National Research, Development and Innovation (NRDI) funded by Hungarian Government under “ÚNKP, Ministry of Innovation and Technology (MIT); and in part by the Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University. This work was supported in part by UEFISCDI Romania and MCI through Eötvös Loránd University. This work was supported in part by UEFISCDI Romania and MCI through BEIA Projects CREATE, NGI-UAV-AGRO, PREVENTION, MULTI-AI, RECICLARM, and EITMIHA; and in part by the European Union’s Horizon 2020 Research and Innovation Program through (ADMATranS4MErs) under Grant 101037866.

**ABSTRACT** The world we live in is where a human-machine connection is a barometer, and this tendency is only growing to provide richer and universal human reminiscences. New technologies, as well as the fusion of different classes of current technologies, are used to create such unique solutions. The Internet of Robotic Things (IoRT) is the product of collaboration between robotics and the Internet of Things (IoT), which has opened up incredible potential for localized self-sufficient solutions. Robots can collect accurate data from the environment and provide a comprehensive service instantaneously. Being an amalgamation of two different concepts i.e. IoT and Robotics, the IoRT system is anticipated to benefit both by expanding their potential to innovative heights. This paper gives a concise introduction to the communication architecture of the IoRT system. The taxonomy of various data exchange protocols used in an IoRT system is proposed. The necessary improvements in protocols that are required to enhance communication in an IoRT system are presented. A Review of some data exchange methodologies based on Artificial Intelligence (AI) for secure and reliable communication is also given in this paper. The key motive of this paper is to understand the data exchange within an IoRT system using common communication protocols.

**INDEX TERMS** Artificial intelligence, communication architecture, Internet of Robotic Things, robotic communication.

## I. INTRODUCTION

The way we communicate has changed a lot because of the internet. As time went on, a mounting amount of devices were associated with the Internet, resulting in IoT, which relegates to a significant number of distinctively recognizable things which are associated via the Internet [1]. IoT is the expansion of Internet connection into substantial devices and familiar objects [2]. Because the Internet of Things pervades several application areas, disciplines, and scientific domains, it is worthwhile to investigate its interaction, effect, and purpose

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen<sup>1</sup>.

in robotics research [3]. Robotics is a cutting-edge, rapidly-unfolding technology [4] that is rapidly being employed in commercial, industrial, and household contexts, as well as for human-safety salvage missions. Robotics is an engineering area that deals with the idea, design, construction, and manoeuvring of robots. Robots are used because it is generally less expensive than people to use them, simpler for robots to perform certain activities, and often the only means to complete certain tasks. A mechanics (i.e. grippers, wheels, motors, pistons, and gears that allow the robots to grab, move, lift, and turn), controller (i.e. the robot’s brain), and sensors (i.e. to aid the robot’s perception of its environment) make up the majority of robotics [5].

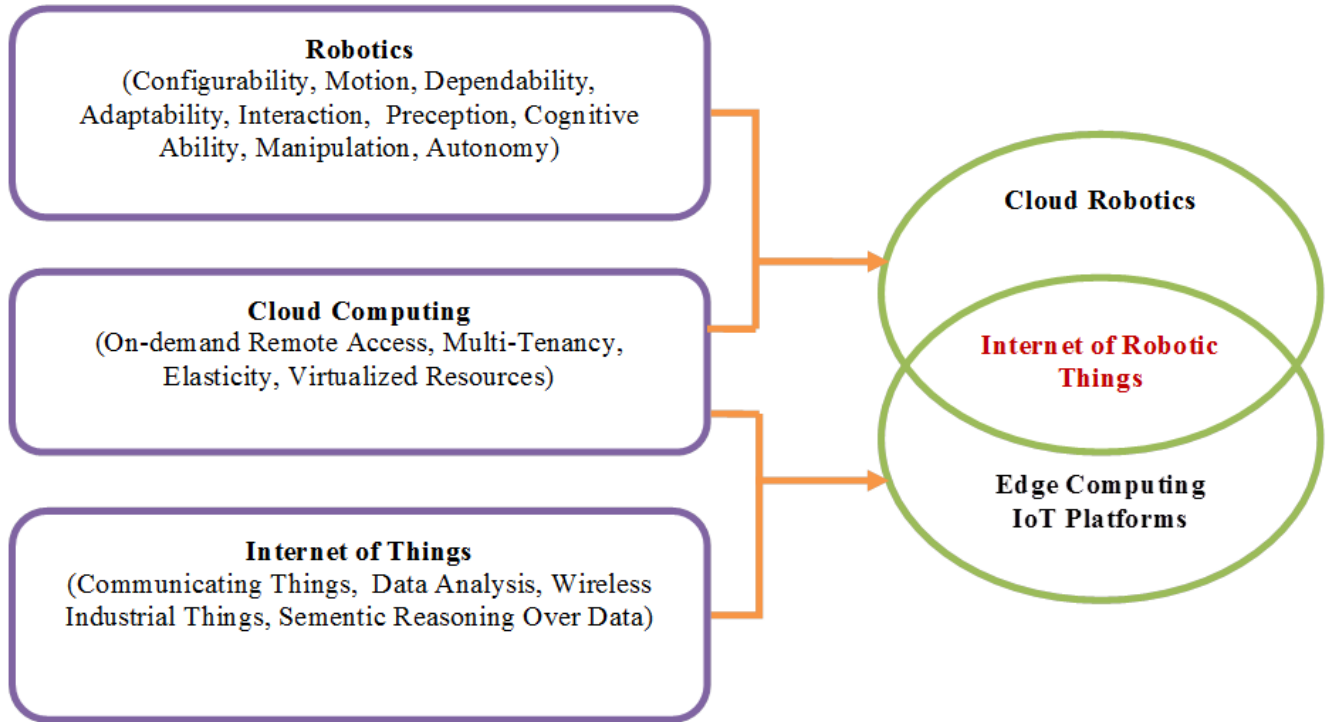


FIGURE 1. Concepts that merge to form IoRT [9].

IoRT is a term that describes the interconnection and link between cloud computing, robotics, and IoT [6], [7], [8]. IoRT is a worldwide infrastructure that connects robotic things using current and growing consistent information and data exchange methodologies such as cloud storage, cloud computing (CC), and other currently existing Network technologies to enable sophisticated robotic services. Figure 1 gives an overview of IoRT and its connected technologies.

The Internet of Things enables robots to interact using the protocol named IP, particularly its version IPv6, which is premeditated for billions of things linked by the internet [10]. Network connectivity allows for real-time updating of information or data (and maybe the firmware of Robots), cloud storage/processing of data, and use of Internet protocols for security, substantiation, data uprightness, message steering, and other functions [5]. In the development of IoRT systems, the integration of robots and networking is crucial.

Networked Robotics is the fusion of robot system designs (including hardware and software) with network-based applications like the Internet and cloud computing [11]. Networked robots have been essential in the amalgamation of robots, CC, databases, and even humans throughout the globe in topical years, thanks to the expansion of the Internet and robotics. They can be hinged on a Local Area Network (LAN) or disseminated across a Wide Area Network (WAN). The use of this technology is made by combining robots having smart sensors that can communicate, exchange data, and operate in a network. The variety of components of IoRT is shown below in Figure 2.

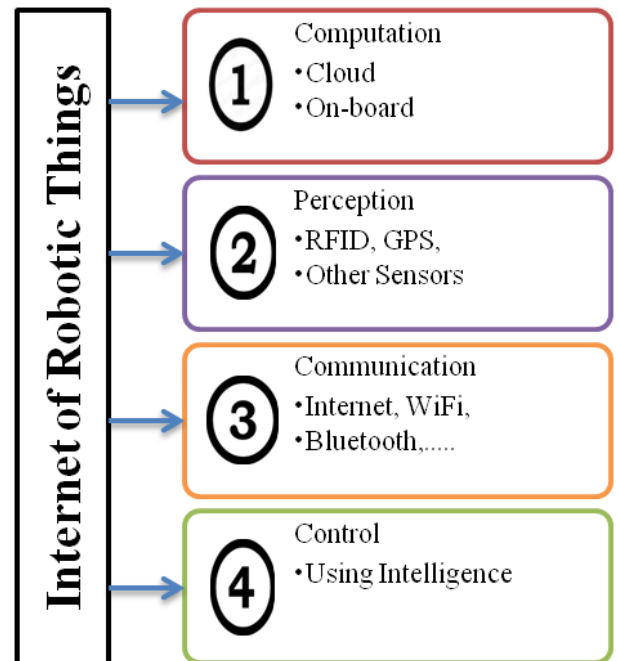


FIGURE 2. Components of the Internet of Robotic Things [12].

As robots grow more integrated into people’s daily lives, assisting them with chores and engaging with them, software, hardware platforms, sensory paraphernalia, and data exchange styles of robotic technology becomes extra complex and challenging.

TABLE 1. The list of abbreviations used in the survey.

Acronym	Description	Acronym	Description
IoT	Internet of Things	NR-U	New Radio Unlicensed
IoRT	Internet of Robotic Things	IETF	Internet engineering task force
IPv6	Internet protocol version 6	NFC	Near Field Communication
LAN	Local Area Network	RFID	Radiofrequency identification
WAN	Wide area Network	WPAN	Wireless Personal Area Network
R2R	Robot-To-Robot	WLAN	Wireless Local Area Network
R2H	Robot-To-Human	6LoPAN	IPv6 Over Low Power Wireless Personal Area Network
M2M	Machine-To-Machine	CSL	Coordinated Sampled Listening
WSN	Wireless Sensor Network	ANT+	Adaptive network Topology
NAT	Network Address Translation	WNAN	Wireless Neighborhood Area Network
AMQP	Advanced Message Queuing Protocol	WWAN	Wireless Wide Area Network
ROS	Robot Operating System	LTE-MTC	Long Term Evolution-Machine Type Communication
WOT	Web of Things	LPWAN	Low Power Wide Area Network
ML	Machine Learning	LoRA	Low Range
DL	Deep Learning	AP	Access Point
ANN	Artificial Neural Network	GSM	Global System For Mobile Communication
UWB	Ultra-Wideband	MAC	Medium Access Control
PSO	Particle Swarm Optimization	WCDMA	Wideband Code Division Multiple Access
AI	Artificial Intelligence	LTE	Long-Term Evolution
VFA	Virtual Force Algorithm	3GPP	3rd Generation Partnership Project
MQTT	Messaging queuing telemetry transport	NB-IoT	NarrowBand-Internet of Things
COBRA	Common Object Request Broker Architecture	LPWA	Low Power Wide Area
QoS	Quality of Service	GPRS	General Packet Radio Service
5g NR	Fifth Generation New Radio	BSS	Base Station Sub-system
PHY	Physical Layer	TSCH	Time slotted channel hopping
<b>Abbreviations used in Figures:</b>			
CoAP	Constrained Application Protocol	JSON	Javascript Object Notation
HTTP	Hypertext Transfer Protocol	WSDL	Web Services Description Language
LOADng	Lightweight On-Demand Ad hoc Distance Vector Routing Protocol	RPL	Routing Protocol for Low-Power and Lossy Networks
Protobuf	Protocol Buffers	gRPC	Google Remote Procedure call
BSON	Binary Javascript Object Notation	DDS	Data Distribution Service
XML	Extended Mark-up Language	REST	Representational state transfer
UDP	User Datagram Protocol	TCP	Transmission Control Protocol
DTLS	Datagram Transport Layer Security	ND	Neighbor Discovery
SDP	Session Description Protocol	ICMPv6	Internet Control Message Protocol Version 6

As previously said, robots must interact with their surroundings, including other robots, gadgets, and machines (R2R), as well as people (R2H). IoT comes into play to do this in an exceedingly interoperable fashion toward genuine machine-to-machine (M2M) communication with context awareness, taking into account the large diversity of protocols, communication frameworks,/ software,/ hardware, and available solutions [7]. IoT’s increased output (i.e., by reusing completely acknowledged and understandable protocols and software), lesser costs, improved client experiences owing to

simpler assimilation with presently subsisting gears of the surrounding medium and cloud computing, premium data in contexts of context understanding, semantics consciousness, and numerous other possible outcomes summed up in related work [5] could all benefit robotics. Furthermore, robotics can gain from low-power data exchange algorithms and protocols, IoT research, expansion in requisites of resource-constrained hardware and software, and optimized results for wireless sensor networks (WSN), including networking, network architecture construction, data transmission, mobility,

and operation, and so on [13]. The list of abbreviations used in the survey is listed in Table 1.

### A. CONTRIBUTION OF THE STUDY

Being a novel concept, the surveys on the particular research area of IoRT is very limited. Most of the work has been done on just understanding and defining the term IoRT, its characteristic features, applications, architectures, enabling technologies, and open issues. Only a few surveys were tailored around the connectivity of the IoRT system and data exchange within it. The diverse data exchange methodologies used for communication have not been reviewed. We intend to review various techniques used for data exchange in IoRT and study the communication architecture of IoRT. So, the main benefactions of our study are given as follows (i–v):

- (i) The study presents a structured and systematic review of the various communication protocols that are used for data exchange in an IoRT system.
- (ii) The paper proposes a taxonomy of IoRT data exchange protocols based on the types of different wireless connectivity technologies.
- (iii) The study also reviewed some data sharing techniques for better and more secure data exchange in an IoRT system.
- (iv) The work is focused on the enhancements of a set of wireless protocols that would connect robotics and the internet of things. The original wireless standards have been adjusted to make device-to-device communication more suited to these upgraded wireless standards.
- (v) Finally, the paper summarized artificial intelligence techniques for robotic data communication.

### B. IMPORTANCE OF UNDERSTANDING THE DATA EXCHANGE TECHNIQUES

IoRT is focused on efficient, secure, and intelligent data exchange. With a lot going on in the field of robotics, IoT, and their convergence field IoRT, the need for an improved communication system is required to maximize the data exchange quality. There are articles available on IoRT, which explain the concept of IoRT and its related terms, but most of them are general and mention the future improvements needed in an IoRT system.

Many researchers are working very hard to understand the communication system of IoRT and to study the various methodologies by which the robots in an IoRT system can exchange data without any interference and with great efficiency. More and more researchers want to work in this emerging field and overcome the various limitations that affect the exchange of data between different Robots and also with their surroundings.

For fulfilling this motive it is necessary to have a good knowledge and understanding of the communication architecture of the IoRT system. It is also important to know about the various techniques that can be used to design an efficient

IoRT system so that it can be made possible to enhance the quality of data exchange between IoRT systems. By understanding and studying different data exchange techniques, the new researchers can improve the IoRT communication systems and can also reduce or minimize the various existing limitations.

Therefore, the study finds this issue very important and so, this paper gives an insight into different data exchange systems available for IoRT with their characteristics, advantages, disadvantages, and future difficulties.

## II. INTERNET OF ROBOTIC THINGS DATA EXCHANGE: AN OUTLINE

The Internet of Things focuses on enabling services for omnipresent monitoring, sensing, and tracking whereas robot communities are more concerned with bringing forth action, interaction, and self-governing behaviour. Collaborating the two and establishing an IoRT system would offer momentous value. The Internet of Robotic Things aims to increase Internet usage by allowing robots to access external resources over the Internet. IoRT systems are made up of several Internet-connected components such as robots, sensors, and clouds. Each component is linked together through communication protocols, forming a system of systems.

Depending on the mechanisms and technologies, there exists a variety of Robots. Generally, these Robots must possess the following three capabilities (i–iii):

- (i) Sensing
- (ii) Intelligence
- (iii) Motion

These capabilities called the “sense-think-act” formula enable Robots to accomplish a variety of jobs without any extrinsic stimuli, therefore, providing them autonomy. The abilities of Robots and their description are given in Table 2. IoRT is separated into five primary layers, as per the research of Ray [6], which is one of the layers accountable for creating Internet connections. He described many IoT protocols that facilitate it, a few of which use a messaging or notifying architecture having a broker to exchange messages.

The messaging protocol which has the broker eliminates the data exchange restriction placed by firewalls and Network Address Translation (NAT) mechanisms, allowing bi-directional information exchange between end devices on the Internet, making it a critical technology for achieving the IoT’s first proposition, “Connecting all things.” A robotic device may be viewed as an influential processing and actuation machine that can also navigate here and there, from the IoT viewpoint. IoT may be viewed as a tool for robots to improve their sensing capability and enhance their steering, manoeuvring, and maintenance operations [9], [14].

As a result, Robots join forces with objects and smartly collaborate toward a communal purpose, in an IoRT system. This became feasible with the advent of a variety of effective wireless data exchange technology that can connect the Internet of Things and Robots.

**TABLE 2. Abilities of robots and their description [15].**

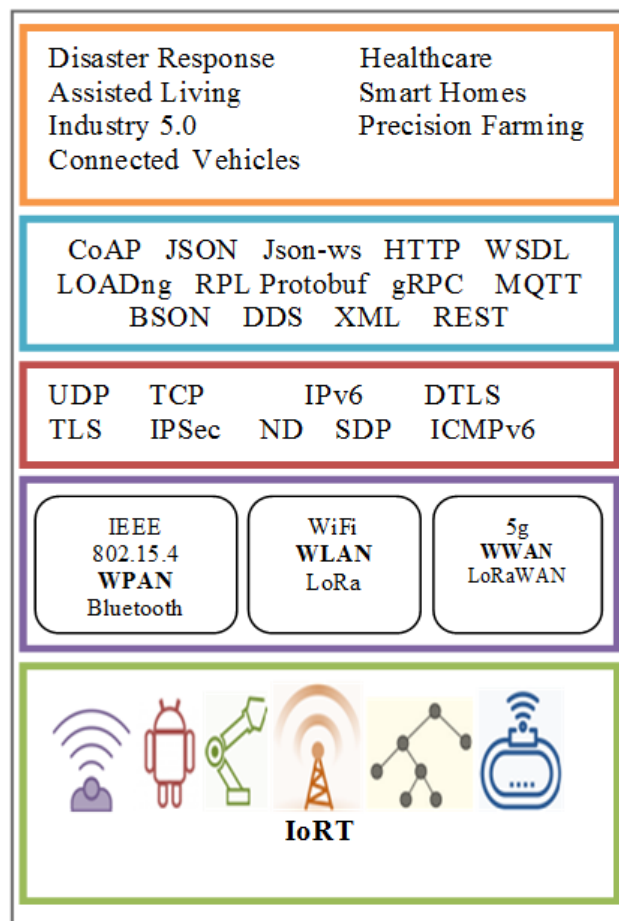
S.No.	Capability	Description
1	Sensing	The Robots use their ability to sense to know about their surroundings. They sense the environment by employing their sensing technology using sensors embedded within them.
2	Intelligence	The information captured by Robots is processed by using their sensing technology to produce outputs for control, decision making, and coordination.
3	Motion	The instructions produced in real-time or the pre-programmed instructions are followed by Robots automatically based on sensor input to carry out controlled, iterative, and premeditated mechatronic acts which include point-to-point mobility.

**A. COMMUNICATION ARCHITECTURE FOR IoRT**

The set of self-directed or semi-autonomous Robots and geographically distributed interconnected sensors and actuators are the central part of the IoRT communication system. The Robots as well as sensors/actuators are considered nodes in the IoRT Network. These nodes have to communicate with each other very unflinchingly and swiftly. To deliver autonomous robotic systems that measure the environment utilizing a variety of IoT devices, robust communication between the nodes is required. Numerous benchmark bodies, corporations, researchers, and educationists have worked hard throughout the years to develop communication technology. The architecture for communication of a general IoRT system is shown in Figure 3. The hardware layer contains a variety of embedded devices such as robots, various types of sensors, and actuators [16] All monitoring, local computation, and actuation capabilities will be provided by this bottom layer. The link layer, which provides wireless links between the multiple nodes, is the neighbouring layer. By the use of standards that specify modulation, channel hopping, the common radio frequency bands, and media access control procedures, all of the individual nodes may transmit signals to each other directly. Many protocols are used at the subsequent network connection layer to offer standard means to transport data, through routes between nodes [17]. The IPv6 protocol, which has been adjusted to suit low-power devices and ensures smooth Internet communication, is the most essential in this layer. Different IoRT systems may have different bottom layers. The communication layer is the most significant in the design since it connects Robots and heterogeneous IoT devices. It is made up of many data exchange protocols that give a universal platform for data exchange. The system’s uppermost layer contains software that is application-specific for interaction between people as well as ubiquitous domain-specific services. For big data analytics or cloud services, there might be a middleware layer underneath the application layer, depending on the specific domain. All of these layers work together to provide highly contained, profoundly intellectual, and omnipresent solutions in spheres such as automated manufacturing, smart homes, assisted living, smart buildings, and healthcare among others. Figure 3 depicts communication architecture of IoRT.

**B. ROBOT AS A CLIENT AND A NODE IN IoT**

Robotic nodes are sophisticated robots that can carry out tasks autonomously according to a set of instructions. They are



**FIGURE 3. IoRT’s communication architecture [18].**

getting incredibly capable of making appropriate judgements in the educational realm, or they might be self-subsistent and receive a small number of directives from a remote command center. They can be mobile robots with wheels or stationary nodes, as in industrial robotics. They have different functions and come in many sizes, including fixed arms, tiny bots, mobile ground robots, and even aerial robots.

Robots and objects might roam about while still being connected as a network, thanks to wireless communication technologies that are enhancing device mobility. Robotic and IoT devices might be connected to separate wireless networks. The communication layer would then be required to provide data exchange protocols. Figure 4 depicts the two functions

of a robotic device in an IoRT system. A robot can work as a client as well as a node in an IoRT system. For smooth interaction in the case of a mobile robot, both situations must have minimal terminal latency, high dependability, and a brace for mobility.

For less power and highly reliable data flow among IoRT nodes, novel communication protocols, and standards are being developed.

### III. LITERATURE REVIEW

Yoshino *et al.* [19], established AMQP, a pub/sub messaging protocol having a broker, as it can guarantee message delivery and order, as well as generate a wide range of message flows. They chose RT-Middleware for broadening the AMQP data exchange interface in their study because it permits networking apparatus to have several kinds of data exchange interfaces, which has previously proven difficult with other IoT systems, as well as robot middleware like ROS or ROS2. They build a more stable and vigorous IoRT system implementing only RT-Middleware by integrating the AMQP data exchange interface with the RabbitMQ server.

Kamilaris *et al.* [5], investigated the present application of the IoT in robotics using tangible examples discovered using a bibliographic-based research strategy. The principles, properties, and designs of IoT as they are employed in current robot systems, as well as common hardware, software, and data communication techniques, have been noted and catalogued. In addition, the application domains, sensors, and services or actions of robots used in IoT-based robotics are discussed. Their study also looks at the existing use of the Web of Things (WoT) in robotics and discusses the whole ability of the Web of (WoRT) Robotic Things.

Alsamhi *et al.* [20], investigated some of the current intelligence strategies like deep learning (DL), Fuzzy logic, artificial neural networks (ANN), machine learning (ML), Particle swarm optimization (PSO), etc. being utilized to improve robotic communication and make robots behave dynamically. The study focuses on artificial intelligence (AI) strategies for robotic data exchange to improve the data exchange capabilities of a multi-robot team. allowing them to do more complicated tasks, make better decisions, take concerted responses, and complete their jobs more effectively. They give a detailed overview of the intellectual robotic data exchange methods that have been established and improved in the latest years of the surveys of the literature.

Hu *et al.* [21], in their study, provide a WiFi distribution network optimization technique and terminal data exchange method, as well as set a system test framework, centered on the MQTT protocol and the speculative underpinning of WiFi technology. The experiment they perform shows that the MQTT-based communication method for IoT terminal equipment presented in this research can unflinchingly and supply execute the equipment's data exchange function and fulfil the IoT system's data exchange demands. According to the WiFi access setup technique, their research evaluates the performance of sending data with lengths of 10 bytes,

30 bytes, 50 bytes, and 70 bytes, with average distribution network times of 0.6692s, 1.3546s, 2.8600s, and 4.7319s, respectively.

Jia *et al.* [22], in their research, presented an Internet-based robotic system that implements networking connections between a distant robotic system and a client using the Common Object Request Broker Architecture (CORBA). To deal with communication delays, the author created the robot control server, that permits the handler or user to handle the telerobotic system on a task-by-task basis. The subsist image feedback server, which delivers live picture responses to a distant user, has also been built.

Vermesan *et al.* [23], discuss the intelligent connectivity of IoRT applications. According to the author, mobile cellular and upgraded wireless technologies will enable communication across vertical domains of IoRT. As cellular connection and 5G are introduced to unlicensed spectrum, the new 5G NR in unlicensed spectrum (NR-U) is vital for upcoming IoRT approaches. NR-U can increase coverage capacity, accessibility, dependability, and precise timing by supporting both license-assisted and autonomous utilization of unlicensed spectrum.

Razafimandimby *et al.* [13], [24], used an ANN algorithm and scheme based on IoT to address the crucial technology for maintaining the global interconnection between devices in an IoRT system and providing the required Quality of Service (QoS). In [13], the author represented Multi-Robot systems by a graph  $G(E, V)$ , where,  $E$  represents the edge set and  $V$  is a vertex set representing an IoRT robot. Here,  $E$  is defined in (1).

$$E = \{(a, b) \in V^2 | a \neq b \wedge S(a, b) \leq R_n\}. \quad (1)$$

where,  $S(a, b)$  is the Euclidean distance between IoRT robots  $a$  and  $b$ .  $R_n$  is the data exchange range. Depending on the given definition, suppose  $H_a$  is the neighbourhood of IoRT robot  $a$ . Hence, the set of robots  $H_a$  can swap information with robot  $a$ .  $H_a$  can be defined as given in (2).

$$H_a = \{b \in V | S(a, b) \leq R_n\}. \quad (2)$$

Graph  $G$  in this article may change over time owing to the movements of the IoRT robots, but it must always be linked. In [24], the author introduced a customized version of the Virtual Force Algorithm (VFA), to control the robot's movement in an IoRT system. The  $j^{\text{th}}$  IoRT robot must move away from the IoRT robot  $k \in N_i$  (neighbourhood node) if  $S(j, k) < S_{th}$  and should move closer if  $S(j, k) > S_{th}$  to maintain the appropriate distance and consequently the requisite connection eminence with its neighbour. The intended remoteness between every pair of IoRT robots is denoted by  $S_{th}$ . This basic control elicits a vector position  $\vec{Q}_{jk}$  such that the robot  $j$  maintains the line of sight with robot  $k$  in an IoRT system. The formula  $\vec{Q}_{jk}$  is given in (3) as follows:

$$\vec{Q}_{jk} = \begin{cases} (0.1 \times l \times \Delta, \Theta_{jk}), & \text{if } S(j, k) > S_{th} \text{ and } \Delta > \epsilon \\ (l \times \Delta, \Theta_{kj}), & \text{if } S(j, k) < S_{th} \text{ and } \Delta > \epsilon. \end{cases} \quad (3)$$

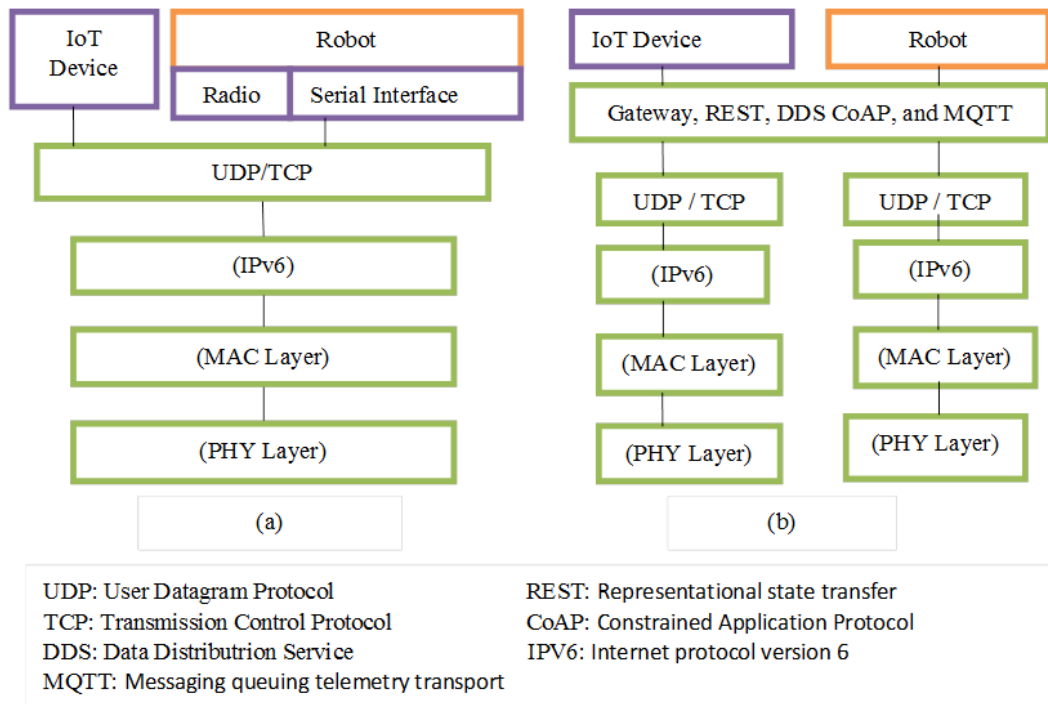


FIGURE 4. (a) Robot acting like a node and (b) Robot acting like a client in IoT.

where,

$$\Delta = |S(j, k) - S_{th}|$$

$\Theta_{jk}$  is the line segment orientation from robot  $j$  to  $k$ .

$l$  is the damping coefficient.

$\epsilon$  is lower-bound of  $\Delta$ .

The algorithms suggested by the author enable the entire IoRT robot network to drift to the specified distance and therefore to the befitting data exchange quality. Table 3 shows the comparative analysis of some data exchange methodologies.

#### IV. WIRELESS CONNECTIVITY TECHNOLOGIES

There are several sorts of wireless networking technologies that are useful for IoRT; these technologies encompass areas ranging from a few centimeters to several kilometers. Wireless Local and Personal Area Network (WPAN/LAN) technologies such as ZigBee, Bluetooth, Wi-Fi, and 6LowPAN is suggested for short to medium-scope data exchange [25].

Wireless Wide Area Network (WWAN) technologies are recommended for long-distance connectivity, and these may be separated into two types: unlicensed technologies (LPWA LoRa, SIGFOX, and others) or licensed (Cellular 2G/3G/4G and 5G). Figure 5 shows the taxonomy of different wireless technologies. Networking is the backbone of IoT, and the kind of access obligatory may vary depending on the type of a particular application. Table 5 presents comparison of some commonly used protocols for data exchange in IoRT system.

Numerous IoT appliances would be supplied by broadcasting technologies that function on unlicensed bands and are

geared for small-range communication with security measures and low QoS specifically characterized for a home or domestic scenario.

#### A. SHORT-RANGE WIRELESS TECHNOLOGIES

Despite its substantially greater power consumption, WiFi is an excellent contender for ensuring connectivity in IoRT systems due to its enormous rise in recent years. WiFi is now available almost anywhere there is anything to convey or there is some information to be transferred. Regrettably, due to the relatively high energy utilization of its standard protocols, WiFi has been out of scope for sensor communications. This changed after 2006 when the WiFi society began to use renowned technologies like putting chips in a state of snooze for the majority of the time or duty cycling and a minimum power WiFi components, like the Microchips RN171 component, which is a self-subsistent, entrenched 802.11 b/g Wireless Local Area Network (WLAN) component, are illuminated [26]. IEEE 802.15.4 technology is another viable option for short-range connections. The Internet Engineering Task Force (IETF) developed the 6LowPAN protocol, and the ZigBee Alliance developed the ZigBee protocol, which is based on the low-power IEEE802.15.4 standard. IPv6 over low-power personal area networks is abbreviated as 6LowPAN [27]. The 6LowPAN goal aims to integrate the IP natively into tiny, cheap sensors. Because there aren't adequate addresses in IPv4, 6LowPAN begins with IPv6, intending to assign an address to all the devices. Given the plethora of different data rates needed for IoT applications,

TABLE 3. Comparative analysis of different data exchange technologies.

Author Reference	Area of Study	Technology used	Security	Communication Quality	Intelligence
D.Yoshino et al. [19]	IoRT/ Communication systems	RT-Middleware with AMQP communication Interfaces	Yes	Better	No
Kamilaris et al. [5]	IoRT/ WoRT	TCP/IP Protocols	No	Good	No
Alsamhi et al. [20]	AI / Robotic Communication	ANN/ ANFIS/ PSO/ Fussy Logic	No	Good	Yes
N.Hu et al. [21]	IoT/ IoRT/ Network Communication	MQTT/ WiFi Technology	Yes	Good	No
S. JIA et al. [22]	Internet-based Robotic System/ Robotic communication	COBRA	No	Better	No
Vermesan et al. [23]	IoRT/ Connectivity and Platforms	TCP/ IP Protocols	No	Good	Yes
Razafimandimby et al. [13]	IoT/ IoRT/ Neural Networks	IoT-Based Algorithm/ NN Algorithm	No	Better	Yes
Razafimandimby et al. [24]	IoRT/ Robotic Communication	AI/ ANN	No	Better	Yes

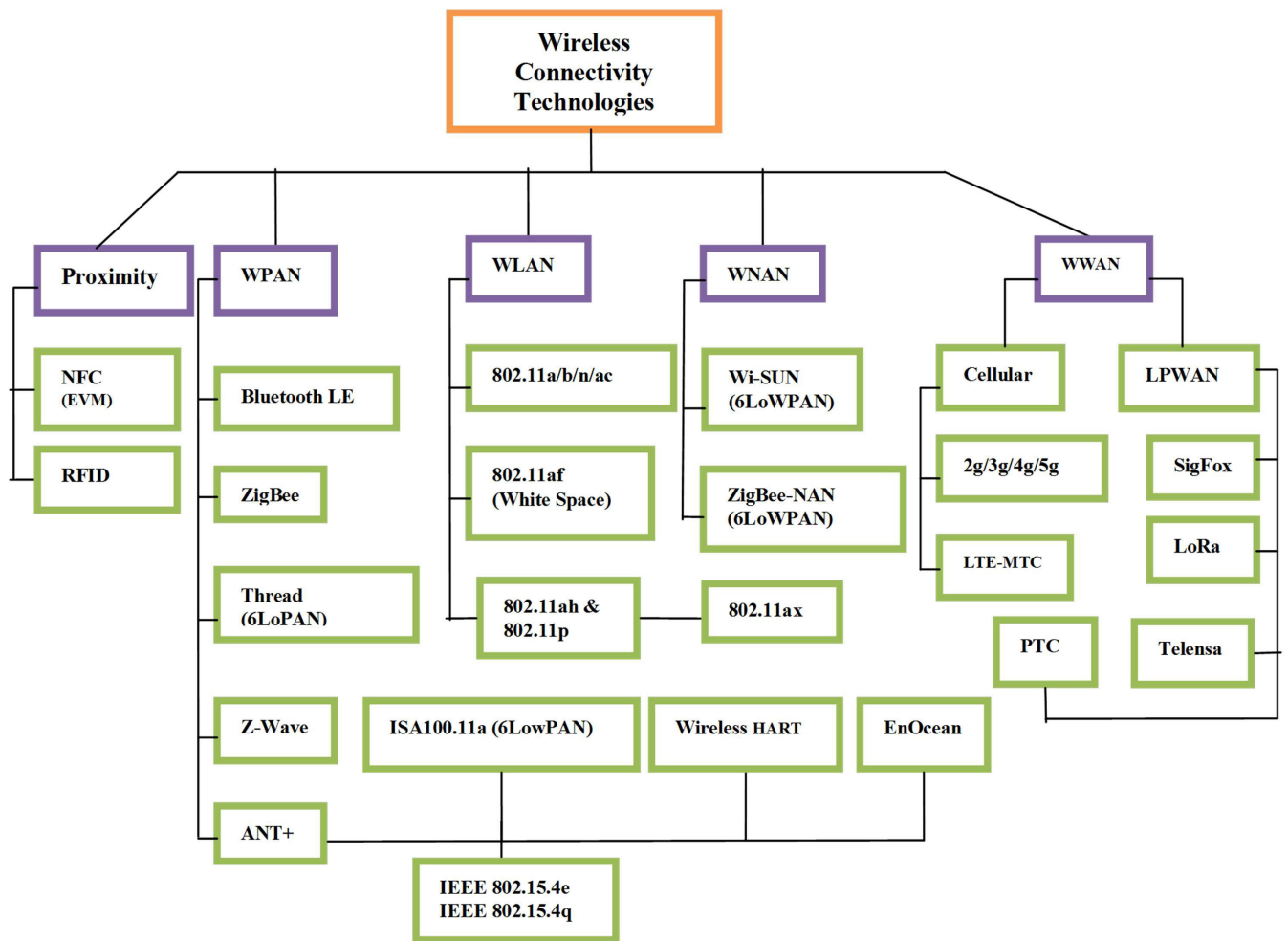


FIGURE 5. Proposed taxonomy of various wireless technologies used for data exchange in IoRT.

early optimization attempts indicate that Wi-Fi might be ten times extra power-saving compared to ZigBee [28], [29]. Work has been in full swing on a low-power WiFi version standardized in IEEE 802.11ah, by IEEE.

**B. LONG-RANGE WIRELESS TECHNOLOGIES**

There are currently the following two potential associated options for the various IoT-based applications that require wider reach:



**TABLE 4. Characteristics, advantages, and disadvantages of different data exchange methodologies.**

References	Data Exchange Method	Characteristics	Advantages	Disadvantages	Future difficulty
[13]	A neural network control scheme	It maintains the desired wireless communication coverage among neighboring robots.	Efficiently maintain the global connectivity among multiple mobile robots to the desired quality-of-service (QoS) level.	This approach only focuses on global connectivity.	Considering other issues like security, reliability, etc. except for global connectivity, this approach may not provide quality data exchange.
[19]	AMQP on RT-Middleware	It is a pub/sub messaging protocol with a broker. Bidirectional communication between multiple machines.	Emphasizes reliability and high functionality in the data exchange. Provides relatively stable communication.	It causes a small amount of latency when compared to other data exchange interfaces.	Maintaining realtime performance is difficult, especially in a wired LAN environment.
[20]	AI in Robotic Communication	It enhances the communication capability of the multi-robot team. Takes an appreciated decision and coordinated action while performing their tasks.	Provides intelligent solutions for robotic data exchange. Automatically generate desired actions for multiple robots in an environment with moving obstacles.	Data exchange between robots in a large coverage area are a challenge that AI should address	A lot of research efforts are still required regarding connectivity issues between heterogeneous robots. The betterment of Quality of Service (QoS) and Quality of Control (QoC) for intelligent robotic communication.
[21]	MQTT protocol based on WiFi Distribution Network	It is a messaging protocol based on publish/subscribe method and works on TCP/IP. It is a lightweight information transmission protocol that is designed for low bandwidth, high latency, or unreliable networks.	It makes the network access of Robots more convenient, fast, effective, and low-cost. It ensures reliability and a certain degree of delivery guarantee that is suitable for IoRT devices.	It is efficient in network distribution but it does not provide stable communication. Also the quality of data exchange is not so high.	Work needs to be done on latency issues and message service quality upgradation, Especially for unstable networks.
[22]	Common object request broker architecture (COBRA)	A basic platform to implement networking connections between a client and a robotic system. It uses an Object Request Broker (ORB) as the middleware to establish a client/server relationship between robots.	Using CORBA to implement the Internet robotic system is flexible and robust. It gives the users the ability to operate the remote robotic system to retrieve and manipulate the desired tableware or other things	It lacks intelligence and is less secure. It is less reliable and provides unstable communication. Data may be lost during communication.	The messaging quality of COBRA is very poor, working on that would not be an easy task.
[24]	IoT-based and Neural-network based methods	Uses the graph connectivity metric to maintain the global connectivity of the IoRT robots' team.	Effective and efficient convergence time, connectivity and energy consumption. Maintains global connectivity.	Not focuses on the security of data exchange. A trade-off between network coverage and communication quality.	Maintaining both network coverage and data exchange quality, and minimizing the trade-off between them.

1) CELLULAR TECHNOLOGIES

GSM, WCDMA, LTE, and eventual 5G are all 3<sup>rd</sup> Generation Partnership Project (3GPP) technology. These WANs use authorized spectrum and have typically focused on high-quality mobile phone and data applications. They are now fast evolving with new capabilities and the latest technology of radio access, narrowband IoT (NB-IoT), which is especially geared to provide an appealing solution for upcoming applications of Low Power Wide Area (LPWA) [30]. Table 4 shows the comparison of commonly protocols [31], [32].

2) UNLICENSED LPWA

The benefit of cellular connection is that it allows you to connect to the internet anywhere on the planet but there

are some limitations also. LPWA, on the other hand, solves the limits of cellular connectivity. These limits are mostly due to two factors: high power usage, which limits battery operation, and the cost of maintenance, which comprises the device's cost as well as the associated infrastructure, which affects the service provider's return on investment. In essence, LPWA technologies operate in tandem with currently existing cellular mobile networks and short-range technologies to enable wide-area networking at lower costs and with improved power efficiency [33]. Low-power wide-area (LPWA) refers to a collection of technologies that have the following characteristics (i–iv):

- (i) Extended battery life, less power consumption.
- (ii) Characteristics of wide-area connection, enabling out-of-the-box connected systems.

TABLE 5. Comparison of some commonly used protocols for data exchange in IoRT system.

Protocols ⇒ ↓Characteristics	WiFi	LoRa	ZigBee	Cellular	Z-Wave	SigFox	NFC	6LoWPAN	Bluetooth LE	RFID
Standard	IEEE 802.11n	LoRaWAN	IEEE 802.15.4	GSMA, GSM/GPRS/EDGE (2G), HSPA/ UMTS (3G),LTE (4G)	Z-Wave Alliance ZAD12837 / ITU-T G.995	SigFox	ISO/IEC 18000-3	IEEE 802.15.4	IEEE 802.15.1	RFID
Type of Network	LAN WPAN/P2P	LAN	WPAN	WNAN	WPAN	LPWAN	P2P Network	WPAN	WPAN	Proximity
Power	Low-high	Very Low	30 mA Low power	High power consumption	2.5 mA Low power Consumption	10 mW - 100 mW low power	50 mA Very Low power	(1-2 years Battery lifetime) Low power consumption	30 mA Low Power	Ultra-low-power
Data Rate	Up to 1.3Gbps	0.3Gbps to 100 kbps	250 kbps	Up to 1Gbps	40kbps	10-1000bps	424 kbps	200 kbps	1Mbps	4 Mbps
Range	Up to 100m	3-5km urban area	Short Range 10-100 m	Several km	30m (indoors) 100 (outdoors)	Long Range 10km(URBAN) 50km (RURAL)	Short Range 0-10cm 0-1m 10cm-1m	Short Range 10-100 m	Short Range 15-30 m	Short Range Up to 200 m
Security	WPA and WPA2	Per-device AES128 keys, AES128 secret key	AES	RC4	AES-128	Partially addressed	RSA AES	AES	E0 Stream AES-128	RC4
Features	High capacity load balancing, Scalability	Long-range, secure, low cost	Mesh Network	Longer Range	Simple Protocol	Long Battery life (up to 20 years) Low Cost	Security	Commonly Used Internal Access	Low power version available	Low Cost
Applications	Any device with cellular connectivity	Smart city, sensor networks, industrial automation application	Monitoring and controlling of home industry	Use in WiFi, ADSL ,broadband ,digital TV & Radio, M2M	Residential lighting & automation	Smart Grid / Street Lighting Energy meters	Payment Access, Business Transactions	Senor networks Industrial automation	Wireless headsets, Audio Applications	Inventory, Access & Tracking
Network Size	Medium	Medium/large	Very Large	Very Large	Large	Medium	Small	Very large	Small-Medium	Medium

- (iii) Networks and chipsets at a minimal cost.
- (iv) Data transmission throughput power is limited.

C. FEATURES OF WIRELESS DATA EXCHANGE PROTOCOLS

For efficient data exchange, the different wireless communication protocols must perform well. Therefore to measure the performance of wireless data exchange protocols, the following matrices are used:

1) SIZE OF NETWORK

The network size can be aligned depending on the amount of interference, transmission protocols used, the size of packets of data throughout traffic, and the number of end users hooked up to GSM voice services. This has an impact on the number of open sessions of GPRS, which can touch 1000 per cell. The ZigBee star network takes first place with a total of 65000 nodes, followed by the Wi-Fi network having a total of 2007 nodes in the configuration of BSS, the Wi-Max network

with 1600 nodes, UWB in the piconet structure with 236 nodes, and finally Bluetooth with 8 nodes. The network size can be expanded by utilizing the protocols that allow for the creation of more complicated network topologies from basic ones [34].

2) TIME OF TRANSMISSION

The factors on which time of transmission depends are the size of the message, data rate, and the remoteness between two nodes [35]. The time of transmission ( $P$ ) can be given by the (4).

$$P = P_b P_{pt} \left\{ Q_{ds} + \left( Q_{os} \frac{Q_{ds}}{Q_{mp}} \right) \right\} \tag{4}$$

where,  
 $Q_{ds}$  is the size of the data.  
 $Q_{mp}$  is the size of the maximum payload.

$Q_{os}$  is the overhead size.  
 $P_b$  is bit-time.  
 $P_{pt}$  is the time of propagation between two nodes.

### 3) TRANSMISSION RANGE AND POWER

The Friis equation, given in (5), presents the relation between transmission range and transmission power for wireless data transmissions [36].

$$\frac{Q_r}{Q_t} = L_r L_t \left( \frac{\lambda}{4\pi X} \right)^2. \quad (5)$$

where,

$X$  is the distance between two antennas. The formula of coverage range can be given in (6).

$Q_r$  is the power of receiving the data module.  
 $Q_t$  is the power when transmitting data.  
 $L_t$  is the gain by Omni basic antenna transmitting.  
 $L_r$  is the gain received by an antenna.  
 $\lambda$  is the wavelength.

$$X = \frac{1}{\frac{4\pi}{\lambda} \sqrt{\frac{Q_r}{Q_t L_r L_t}}}. \quad (6)$$

### 4) CONSUMPTION OF ENERGY

The consumption of energy for smart sensors consists of three steps (i–iii):

- (i) acquisition
- (ii) communication
- (iii) computation and data aggregation

Depending on the type of application, the energy consumption may vary in the acquisition operation [37]. In transmission, data traffic generally requires more energy as compared to other operations [38]. Depending upon the data exchange range ( $C_s$ ), the modal of the energy consumption  $K_s$  of a smart sensor  $s$  is given as in (7).

$$K_s = gC_s^\beta + K_c, \text{ for } \beta \geq 2. \quad (7)$$

where,

$g$  is the size of the packet.  
 $\beta$  is the coefficient of signal attenuation.  
 $K_c$  is the cost of energy transmission.

Using the modal of radio energy [39], [40], [41], [42], the transmission energy to a distance  $s$  of a  $g$  bit message is given by (8)–(9).

$$K_{x,y}(g, s) = \begin{cases} (g\gamma_f s^2 + gK_e), & \text{for } S < S_0 \\ (g\gamma_a s^4 + gK_e), & \text{for } S \geq S_0. \end{cases} \quad (8)$$

$$S_0 = \sqrt{\frac{\gamma_f}{\gamma_a}}. \quad (9)$$

where,

$K_e$  is the electrical energy.  
 $\gamma_f, \gamma_a$  are the amplification energies.

### 5) BIT ERROR RATE

To access the effectiveness of a communication system's modulation, calculating the bit error rate  $B$  is very useful [34]. It also enhances the robustness of the system. Formula in (10) is used to compute  $B$ .

$$B = \frac{E}{T}. \quad (10)$$

where,

$E$  is the number of errors.  
 $T$  is the number of bits transmitted.

### 6) THE EFFICIENCY OF DATA CODING

The formula for computing the efficiency of data coding is given in (11) as follows:

$$D_e = \frac{100Q_{ds}}{\left( Q_{ds} + Q_{os} \left( \frac{Q_{ds}}{Q_{mp}} \right) \right)}. \quad (11)$$

### 7) INDEX OF ENERGY

To conclude the lifetime of a sensor network and to compute the cost of transmitted energy of a sensor node, the energy index  $I_e$  is used [43]. The  $I_e$  is given in (12).

$$I_e = \frac{L_p - P_o}{(1 + r_n)(t_e + m_e + c_e)}. \quad (12)$$

where,

$L_p$  is the length of the packet.  
 $P_o$  is packet overhead.  
 $r_n$  is the number of re-transmissions.  
 $t_e$  is the energy of the transceiver.  
 $m_e$  is overhearing and idle energy.  
 $c_e$  is a collision.

### 8) REAL-TIME THROUGHPUT

It is used to define the octets transmitted per second on a particular link in relevance with real-time throughput [43]. The analytical formula for real-time throughput  $T_p$  is given as follows in (13).

$$T_p = \frac{n}{T_f + T_b}. \quad (13)$$

where,

$n$  is the total data transmitted.  
 $T_f$  is the time taken to transmit a data frame.  
 $T_b$  is the backoff time needed.

## V. ARTIFICIAL INTELLIGENCE-BASED METHODS FOR DATA EXCHANGE IN IORT

Artificial intelligence is difficult to characterize accurately. The founder of AI, John McCarthy, described AI as “the engineering and science of constructing intelligent machines.” As a result, AI alludes to the capacity of robots to respond to data and information and create results in an approach comparable to how people learn, make decisions, and solve problems. Furthermore, AI is always improving, allowing robots to get smarter and smarter. Machine intellect means

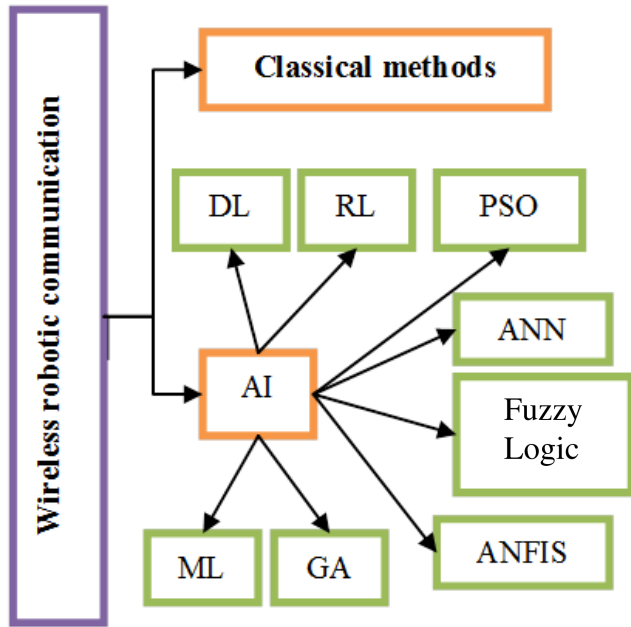


FIGURE 6. Wireless communication for robots using AI.

the capability of a machine to execute the highbrowed work in any situation that an individual would perform. AI is used to create more intelligent machines. Robots serving or working with humans are supposed to understand human requirements with minimum human communication. Because of its incredible capacity to deal with complexity, high precision, enormous data, and quick processing, Artificial Intelligence (AI) is being used to improve technological applications and development.

The familiar AI technologies include pattern recognition, ANN, ML, fuzzy logic, neuro-fuzzy interference system (ANFIS), DL, genetic algorithm, PSO, clustering, and so on. Figure 6 shows various AI approaches for wireless communication for robots [44]. Engineering, science, health, computers, finance, economics, and other fields have all benefited from AI. It's also being used to improve the intelligence of robots. Smart machines are capable of doing tasks with great intelligence in a turbulent environment, like or identical to that of a person. As a result, AI is a component of computer science, as well as the cognitive and supervisory component of a robotic system. When robotics and AI are combined, a machine can do certain human-like jobs. Robots will be omnipresent in the future, and they will assist humans at any time and in any location. To attain this aim, future robots will need to be able to communicate effectively both among themselves and with people. The authors of [45] have examined the principles of many communication methods as well as wireless communication for robotics networks.

In both study and application, robotics technologies have frequently been coupled with communication network technology. Both technologies together will aid robots in moving independently and extending robot functions to do any given work successfully and proficiently.

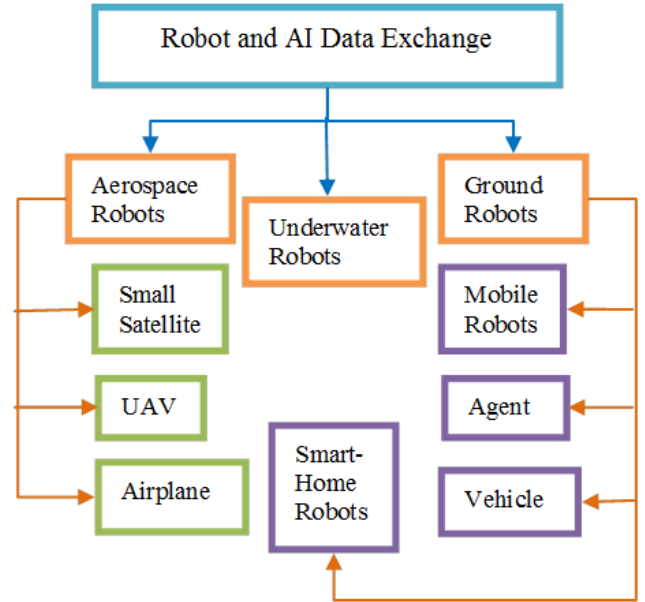


FIGURE 7. Robot and AI Data Exchange in different areas.

Teleoperation or independent communication is also possible [6]. Robots that are entirely controlled by human operators via communication networks are referred to as teleoperated robots. Autonomous robots, on the other hand, are capable of doing tasks or acting alone. In [46], the authors have discussed effective communication in cooperating robot teamwork. Information sharing between robots must also provide collision avoidance and preserve the communication link's quality. Energy and power metrics, quality-of-service (QoS) metrics, dependability, movability, collision avoidance, connection, and robot cooperation are the most often utilized metrics for robot communication systems. A great deal of study has been done on robot-team communication [47], [48].

When the robots engaged are on the ground, in the sky, in water, or other surroundings, as depicted in Figure 7, intelligent robotic communication is necessary. AI improves the robot's capabilities as well. For several years, AI approaches have improved robot abilities in areas such as sensor data fusion, processing information, contextual identification, and decision-making. DL and ML algorithms are enhancing the potential of robotic systems. The evolution of AI algorithms promotes (a–c):

- (a) autonomous robot intelligence
- (b) enhanced robotic component intelligence (enhancing robot or helped human capabilities)
- (c) overall assistive robot intelligence

The intellectual ability of autonomous robots is focused on intelligent machines that have a wide range of operating skills and high redundancy while completing tasks in groups. The system's scalability, adaptability, and fault tolerance must all be guaranteed. Augmented robotics intelligence focuses on improving robotics devices' sensing, acting, and

cognitive capacities. This concept is applied to people by the enhancement of their capacities, such as increasing human force. Human-assisting robots' intelligence draws on and incorporates principles from a variety of domains, including AI, cognitive science, psychology, and sociology. Humans anticipate assistant robots to communicate with them in a friendly manner. They should be predictable while providing human help [49].

To do their duties successfully and consistently, robots must communicate with one another. Several types of research on AI in applications of robotics and complicated tasks have surfaced subsequently, including works of [50], [51], [52]. Despite their focus, these surveys encompass a wide range of topics. They are mostly limited in dimension to AI for robotic tasks and controls [50], allocation and navigation and prosecution of portable robots in multifaceted surroundings [51], and robotic visualization [52], and thus are of superior value but lack quantitative descriptions on the wide assortment of AI techniques appropriate for robotic transmission of information. Moreover, considerable research on AI for Robotic data exchange has occurred [13], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62]. These studies are fascinating, but they only apply to a few aspects of robot communication. The research [53], [59] largely focused on ML for WSN and M2M connections [60], therefore they don't address the applications that ML can use to improve future robot connections and networks.

The authors of [58] gave a complete overview of ML methods in the context of IoRT devices. They have proposed a distributed ML algorithm based on Liquid State Machine (LSM) framework. The cloud can predict users' content distribution requests, using this proposed algorithm, if there is limited information on the network and user states. This increases the efficiency of a network for UAVs. In addition, DL for UAV application domains was covered in brief. In supplement to the study of authors [53], [55], [57], [58], and [59] used machine learning to introduce UAV connectedness and anticipate the number of users linked to the UAV. The complexity of logarithms, on the other hand, may be lowered in the future. For example, in [54], the authors devised a machine learning approach for echo state networks that can vigorously change the speed of the network and allow UAVs to observe their surroundings.

The suggested approach significantly improves the quality of experience (QoE) utilities of users. In [56], the authors have presented ML strategies for predicting every user and determining the UAV cached contents. The suggested approach was created to allow cached UAVs to provide limited service to ground users over licensed and unlicensed bands. Utilizing a liquid state machine allows UAVs to allocate resources autonomously with minimal information. The liquid state machine improves the number of persistent queue users significantly. The authors of [62] presented an echo state network for interference-aware route control of cellular-connected UAVs based on RL. The UAVs' objectives were to strike a balance between low delay, high power efficiency,

and low interference levels during network transmission. As a result, the RL allowed every UAV to choose its data exchange power, next position, and cell association. The data demonstrate that higher wifi delay per UAV and higher UAV elevation both help to reduce interference levels.

The authors, on the other hand, neglected to account for latency and drone interference. The research [56], [62] focuses on using machine learning to optimize UAV sites and forecast user actions. Additionally, robotic data communication entails not only determining signal intensity between robots, but also establishing some criteria to examine, such as context, kind of information, and where the signal originates. As a result, robot data exchange must be fully realized. The authors of [61] concentrated on the Recurrent Neural Network (RNN) approach for useful and proficient end-to-end widespread interaction to enable robots to interact with one another and achieve the aim. The suggested works were separated into three elements to accomplish this: negotiations, defuzzification, and end-to-end data exchange. RNN assists robots in making appreciative decisions based on received signals and after discussion to prevent robot disputes.

Additionally, it enables receiving robots to progressively receive signals from dispatcher robots and then shift to the correspondent position following the RNN output. As a result, the receiver robot may reach a specific destination from anywhere. In [13], the authors have addressed the issue of combining AI, IoT, and robotics, and came up with the notion of the IoRT. The research focuses on robot aggregate exposure and connection preservation. The neural network approach was utilized to make a middle course between the robots' connection and the required QoS. The results revealed that the ANN approach had benefits in terms of connectivity, energy usage, and convergence time. The authors, on the other hand, have not offered a determinable account of the AI diversity that existed.

Arsénio *et al.* [54] emphasized the internet of intelligent things (IoIT), which integrated AI into networking technologies and objects. For achieving the operational needs and "the cost efficiency of the vehicle networks".

AI methods like machine learning (ML) are employed as proficient tools to handle challenges encountered in 5G wireless data exchanges [63] (e.g., caching, processing, and data exchange processes). To allow new connections, cellular and wireless communication networks must provide conventional/assured latency, which has become the facilitator for the next coming generation of IoRT intelligent services. Broadcast systems and/or peer-to-peer can be used by IoRT devices for information exchange and direct communication.

Khan *et al.* [64] propose an AI-based algorithm named Artificial Bee Colony (ABC) so that devices within an IIoT system can act intelligently and safeguard the confidentiality and authenticity of data and devices. They proposed this algorithm for secure communication and better network connectivity of an IIoT ecosystem.

Xia *et al.* [65] scrutinized the power control strategy of secure intelligent data exchange with Statistic Channel State

Information (CSI) for IoT networks. They propose a reinforced learning algorithm named Q-Learning for secure and intelligent communication for IoT networks.

## VI. CHALLENGES IN DATA COMMUNICATION (NETWORKING) IN IoRT

Considering the global IoRT market size, large device manufacturing, IoRT technology investment, academic interest in IoRT, and the possible return on investment of IoRT businesses, the future of IoRT technology seems extremely bright and promising [66]. However, because of the immense scope of the IoRT infrastructure and the large number of devices involved, security issues will become much more prevalent. Security procurement is required to disarm malevolent actors that pose a danger to the IoRT, and it has yet to be satisfied effectively, as seen in the preceding section's protocol comparison. The security concerns posed by IoRT will serve as a crucial research topic [66].

The open networking problems in the IoRT area are summarised in Table 6. Aside from security provisioning, compatibility between network protocols is another major difficulty in IoRT development. Leading firms throughout the world are designing smart devices with complete interoperability in mind. These features are critical because they will allow for seamless interaction with the present Internet [67]. The expense of an IoRT protocol with numerous sophisticated capabilities rises as the convenience of use decreases. Building an attractive protocol is not an easy undertaking, and it is usually a trade-off between system cost and performance. IPv6 introduces beneficial and adaptable networking technologies, bringing IoRT features one step closer to desired interoperability. The Internet of Things will connect a variety of things to create revolutionary services.

As a result, an effective name and identity, and access management system are necessary, one that maintains the distinct traits of a huge number of objects. Using RFIDs to physically tag one thing is one approach to constructing such a system. Another option is to provide each item with its characterization, allowing it to immediately broadcast its identification and associated data. Because of the huge number of smart objects, stronger scalability management techniques are required. Current organizational protocols, as indicated in [68], cannot be expanded effectively enough to fulfil the requirements of IoRT devices due to their inadequate potential.

Moreover, IoRT data is characterized by heterogeneity, which implies that information is created in large quantities, arrives in real-time, has a changing structure, and may have an unknown source. Because total performance is in a straight line proportional to the characteristics of the data managing service [69], the problem of managing massive data is crucial. Whenever the data integrity component is examined, the problem becomes much more problematic, not only because it impacts service quality, but also because it raises privacy and security concerns, especially with outsourced data [70].

Another important aspect of the IoRT paradigm is mobility management. Because of the hard processing and power limits, conventional mobility-supporting protocols for Vehicular Ad Hoc Networks (VANETs), sensor networks, Mobile Ad Hoc Networks (MANETs) and are unable to effectively cope with common IoRT devices. To keep track of the device's location and response to topological changes, movement tracking is required.

Furthermore, the energy needs of IoRT are yet unmet. A few routing protocols, as previously mentioned, offer low-power data exchange, however, they are still in the early stages of development. As a result, green technologies must be used to make IoRT devices as power-efficient as feasible.

## VII. CYBER-SECURITY FOR ROBOTIC DATA EXCHANGE

In the context of data exchange in robotic systems, the purpose of cyber security is to minimize the impact of vulnerabilities and protect robotic systems from cyber attacks. This task is often challenging and necessitates the introduction of some specific requirements. These requirements are commonly named as CIA-Triad, referring to the following three (i-iii) pillars of cyber-security,

- (i) Confidentiality,
- (ii) Integrity
- (iii) Availability

Although these three principles are the keystone of the security infrastructure of any organization, there are some additional requirements such as accuracy and safety, that a robotic system needs to meet. Figure 8 shows the security scenario of a robotic system.

### A. ROBOTIC SECURITY ATTACKS

After the integration of robotic systems in IoT domains, the various attacks targeting robotic systems are increasing. These attacks target both robotic data and the security of the system including confidentiality, integrity, availability, privacy, and authentication. There are certain levels of attack in a robotic system which are as follows (a-c):

- (a) Attack on the hardware of robots.
- (b) Attack on the firmware of robots.
- (c) Attack on robotic communication.

**Attack on Robotic Communication:** If there will be insecure data exchange between users and robots, it may increase a variety of cyber security risks. A hacker can hack into insecure communication links, particularly if robots are connected to public internet services. Most of the robots are connected to the Internet through networks, so the attackers could exploit communication vulnerabilities and gain full control of the robots. The data exchange in robotics is prone to different attacks that may affect many security services. These attacks are stated below (i-xii):

- (i) Jamming Attacks
- (ii) De-authentication Attacks
- (iii) Traffic Analysis Attack
- (iv) Denial of service attack

TABLE 6. Data communication problems in IoRT.

Challenges in Data Communication in IoRT	Characteristics
Intercommunication	(a) Necessity of standardization (b) IPv6 addressing must be used to lead the way (c) The current Internet should be easily integrated (d) Components designed with predetermined parameters (e) Cross-layer intercommunication required
Inpregnability	(a) Confidentiality of data (b) Management of identity of privacy (c) Access control (d) Substantiation (e) Trusted platforms (f) Encryption
Extensibility	To enable a higher number of smart objects, an extensible management protocol is being developed
Identification	Developing a name and identity management system that works
Movability	(a) Detection of movement required (b) Energy and processing restrictions should not exist in VANETs and MANETs
BigData	(a) The qualities of the data management service have a direct correlation with performance (b) The data integrity attribute should be considered
Management of Energy	(a) Green technologies are required for energy-efficient systems (b) Still not fulfilled completely

- (v) Replay Attacks
- (vi) Man-in-the-middle Attack
- (vii) Masquerading Attacks
- (viii) Meet-in-the-middle Attack
- (ix) Identity Attack
- (x) Network Impersonation attack
- (xi) Message fabrication and alteration Attacks
- (xii) Illusion Attacks

These are some of the attacks that hinder secure data exchange in IoRT systems. These attacks can be extremely dangerous as they can hurt the robotic systems as well as humans.

**B. SOURCE OF ATTACKS**

There are several sources from where these attacks can originate. These sources include cyber crimes, cyber warfare, and even cyber terrorism. The common sources of attacks are as follows (a-i):

- (a) Insiders or whistle-blowers
- (b) Outsiders
- (c) Competitors
- (d) Incompetent developers
- (e) Cyber-criminals
- (f) Organized criminals
- (g) Malicious manufacturers
- (h) State-sponsored hackers
- (i) Terrorists and spies.

All these sources of attacks generate a great deal of threat to the robotic system and its data exchange methodologies.

**C. SOLUTIONS AND COUNTERMEASURES FOR SECURING ROBOTS**

To secure Robotic communication and robotic systems it is very important to maintain and implement effective security measures. There is a need for a strong multi-authentication procedure, along with the verification and identification process. Securing robotic systems, and their communication is not an easy task, however, it is neither impossible. Hence, a variety of cryptographic, non-cryptographic, and AI-based solutions are available there to countermeasure the various cyber security attacks.

**VIII. IMPROVED PROTOCOLS FOR COMMUNICATION IN IoRT**

Before proceeding to know about the various enhancements made to some wireless communication protocols, it is necessary to understand why these enhancements are done. Why there is a need to improve the existing wireless protocols? This question is very important and has relevance because it serves as the base of these very improvements done to wireless communication protocols. This question can be simply answered by saying that “IoT systems that are supported by these protocols +v are slightly different from IoRT systems with Robots as end devices.”

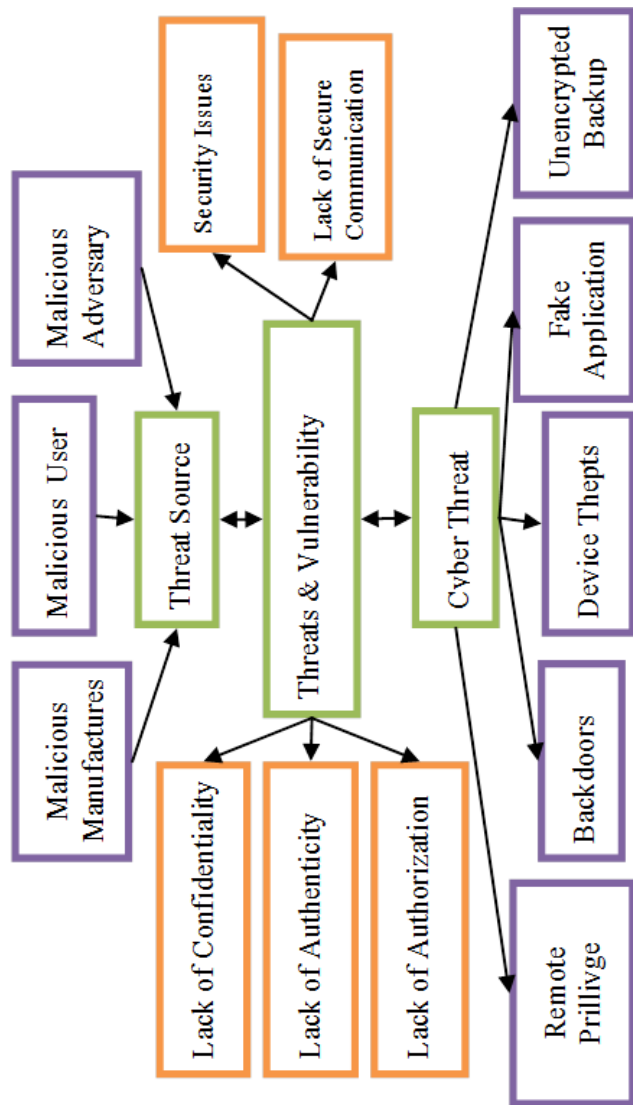


FIGURE 8. Security scenario of a robotic system.

These protocols are not efficient enough to support the communication between Robots within an IoRT system as they are for the IoT systems. Also, with the rapid evolution of the Internet Industry, the need for fast, interoperable, powerful, more secure, and reliable communication technologies are growing. Hence these protocols are required to enhance and change with the growing needs and improving technologies used for data exchange between Robots within an IoRT system.

**A. DIFFERENCE BETWEEN IOT AND IORT**

Both IoT and IoRT include cloud services as their infrastructure and group of devices across the Internet are concerned. The important distinctions between IoRT and IoT may be summed down (i–ii) into two aspects.

- (i) The Robots on the field side receive instructions from the cloud or some other devices to interact with the

physical world. Depending upon these instructions they operate and drive the system.

- (ii) On the working ground, or via the network (multi-robot system), robots can exchange data with one another in real-time.

Now, as per i, the distinction between IoT and IoRT is the position of sensors and actuators, whether they are at the center of the system or on the edge. In IoT, the sensors are located centrally but the actuators in some situations can directly affect the objects in physical space.

In contrast, IoRT systems have Robots at the center, which includes drive systems. There is communication between Robots and physical entities, which is essential, so the physical security and safety of Robots must be ensured. Sensors are used by both robots and IoT devices to perceive their surroundings, analyze data fast, and decide how to react. Most IoT solutions can only perform well-defined tasks, whereas robots can anticipate circumstances. The primary distinction between the IoT and the robotics society is that robots perform real-world tasks and are physically present. They take action. The focus of IoT has shifted from cyberspace to the physical side, and this is where the efforts are coming together [71].

Therefore, it becomes significant to make sure the uprightness of extrinsic commands is given to the Robots. If there will be any inconsistency or deficiency in the instruction given to the Robots, it will make them go out of control.

So, if the Robots in an IoRT system need to act in control properly after receiving instruction from an external source or remote location, the consistency, and integrity of the system must be enhanced. The driving force behind the enhanced system is the improvements that are done to some of the wireless communication protocols.

These improvements will enhance the entire communication system within an IoRT system and will uplift the quality of Data Exchange between different Robots, humans, and Robots, and also between the Robots and other devices.

**B. IMPROVEMENTS IN WPAN HAVING LESS POWER**

The IEEE 802.15.4 standard, which is built on radio transmissions, allows small devices that run on batteries or solar power to connect wirelessly across short distances.

To maintain operations at low power and moderate access control mechanisms were developed so that the radio may be kept off the majority of the occasion. It offers modest data rates, although they are suitable for these sensor devices with payloads that are projected to be below. To guarantee excellent dependability and energy savings at the same time as minimizing end-to-end latency latest wireless standards have been created.

**1) IMPROVEMENTS IN IEEE 802.15.4**

To maximize the efficacy of radio-frequency (RF) communications in low-power devices, modifications are made to the MAC and physical (PHY) layers [72], [73] of this standard.



The IEEE 802.15.4e Standard is pointed out as follows (i–iv):

- (i) There are five distinct MAC options available to meet the needs of various applications.
- (ii) Time-slotted channel hopping (TSCH) is provided to handle a high quantity of concurrent connections while reducing interference and increasing dependability.
- (iii) Enhancements to the MAC layer to support industrial IoT.
- (iv) Coordinated sampled listening (CSL) reduces latency by synchronizing the transmitter and receiver by agreeing on the same transmission schedule.

The IEEE 802.15.4q standard can be summarized as follows (i–iii):

- (i) Use of a reduced preamble to promote low energy consumption.
- (ii) Adding two PHY layers that give extremely low power utilization and functions.
- (iii) As a result, these new enhancements are aimed at reducing interference and improving the dependability of lossy wireless signals.

## 2) IMPROVEMENTS IN BLUETOOTH

Bluetooth has been created to provide a small-range wireless connection with minimal formation for devices that have one transmitter and several receivers. To make it interference-tolerant, it employs radio communications using a frequency hopping spread spectrum. This standard has recently been updated to facilitate device-to-device interaction for IoRT applications.

The Bluetooth LE is pointed out as follows (i–iii):

- (i) Advertisement channels are used to convey broadcast messages.
- (ii) Uses smaller packet transfer to keep power consumption low.
- (iii) All communications must go through the central node.

IPv6 over Bluetooth LE [74] can be summarized in the following points (i–ii):

- (i) 6LoWPAN sits atop the logical connection control and adaptation layer.
- (ii) The innermost node takes on the role of a perimeter router, connecting slave nodes through an IPv6 connection.

## C. IMPROVEMENTS IN WLANS HAVING LESS POWER

A WLAN delivers wireless communication used for a group of nodes located within a few hundred meters of each other. The wireless feature lets devices move freely and increase mobility without affecting connection reliability. The networks use a permanent access point (AP) to connect numerous mobile nodes in one-to-one mode. The access point remains the core node, via which additional nodes interact with one another. Without the need for a central AP, ad-hoc

peer-to-peer connections are possible. WLAN is extensively accustomed to expanding Internet access for several devices inside a medium-range, even though isolated networks can be set up.

## 1) IMPROVEMENTS IN IEEE 802.11

The IEEE 802.11 wireless protocol, sometimes known as WiFi, is used to link devices within a wireless local area network. Multiple devices are interconnected across a small distance of a few 10's meters to 100 meters, but the range may be broadened by forming a mesh. The movability assistance and wide exposure limits provided by WiFi networks would help an IoRT system.

The IEEE 802.11ah is as follows (i–iv):

- (i) Less power is used and has a range of almost a kilometer.
- (ii) Because it operates in the megahertz spectrum, it has high incursion around obstructions.
- (iii) For low-power operations, it has pre-programmed sleep and waking cycles.
- (iv) Supports a communication range that is twice as far as standard WiFi.

The IEEE 802.11ax is pointed out below (i–ii):

- (i) To increase power efficiency, various groupings of devices are given varying waking-up times.
- (ii) The end-to-end data transmission latency may be kept consistent and stable across all nodes.

## IX. FUTURE WORK

In this paper, we have given an insight into various methodologies used for data exchange in IoRT systems. We have mainly focused on wireless connectivity technologies, their comparison, and their improvements. Some AI techniques used for robotic data exchange are also presented. We have presented a brief introduction to cyber security in robotic systems, the levels of attacks, and their sources. The data communication problems in IoRT systems are also listed.

The problems that presently exist in the IoRT data exchange techniques are not impossible to solve. These problems can be solved by the great effort of researchers by using new fast, reliable, and evolving techniques and by modifying the existing network technologies, some of which are mentioned above in Section VIII. We can perform a comparative analysis of available data exchange techniques and choose the most efficient one. Also, we can design a new IoRT system based on the existing ones. For example, for security issues, we can use blockchain technology or some lightweight cryptographic algorithms. For quality message service, AMQP over RT-Middleware can be used. For intelligent communication, various AI techniques like ANN, PSO, Fuzzy logic, ML, and DL can be used as mentioned in Section V.

In the future, we intend to work on solving the problems that presently exist for data exchange in IoRT. We will work on cyber security for IoRT in depth in the future and intend to develop a threat model for it. Also, we will discuss in detail

the various solutions and countermeasures to eliminate the threats and attacks on communication links used for IoRT data exchange. We will work on designing a novel IoRT system with secure and intelligent data exchange.

## X. CONCLUSION

The Internet of Things (IoRT) has a good deal of promise integrating a range of robotic conclusions and findings into regular life. Whether it is a smart home, private vehicle assistant, disaster response, assisted living, working in emergencies, surveillance, smart production, or outbreak management, ingenious IoRT solutions can assist us to make the globe more technologically intelligent. IoRT solutions rely heavily on wireless communication technology to provide a rich and pervasive experience. Corporations and digital technology firms are banding together to create open standards, incorporate them into their commodities, and license multi-vendor machines and robots for effortless cooperation.

Moreover, many researchers and owners of big firms are trying to make machines more and more intelligent and smart to compete with human intelligence and reasoning power. The use of AI and its various sub-fields is increasing with each passing day. Several AI algorithms are being used to incorporate intelligence in Robots in an IoRT system and also for data exchange in multi-robotic systems. This paper discusses the architecture of IoRT in relevance to data exchange, proposes a taxonomy of communication protocols based on wireless technologies, and also gives a comparison of some commonly used protocols.

This uncovers a new frontier in the field of networked robots, which we hope will lead to exciting future advances. It does enable adaptation into a linked ecosystem in which diverse technologies, such as communications networks, different types of devices, processing units, and cloud services, are used to leverage resource-constrained deployment of affordable robots. simultaneous localization and mapping (SLAM), grasping, navigation, and many more technologies that are outside the scope of this paper might all benefit from the IoRT methodology.

This paper looked at some of the current intelligence strategies being utilized to improve robotic data exchange and make robots behave dynamically. PSO, ANN, fuzzy logic, ANFIS, genetic fuzzy, big data, and machine learning are examples of AI techniques. The benefits of utilizing AI in robot data communication include assisting robots in learning about each other and the dynamic environment, coordinating individual robots' roles, preventing probable collisions, optimizing the performance of the team, and achieving faster processes and easier labor. Robots become smarter when intelligence is added to their communication, allowing them to do jobs more successfully and efficiently. This article also highlighted the improvements made to wireless standards to make them pertinent to the IoRT data exchange system. For aficionados to get part in this innovative concept shortly, open networking challenges are addressed in a detailed manner.

## CONFLICT OF INTEREST

The authors declared that they have no conflict of interest with this manuscript.

## REFERENCES

- [1] F. Xhafa and N. Bessis, *Preface*. Ormskirk, U.K. Edge Hill Univ., 2014.
- [2] R. H. Weber and R. Weber, *Internet of Things*. Germany: Springer, 2010.
- [3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1570870512000674>
- [4] B. Siciliano, L. Sciacivico, L. Villani, and G. Oriolo, *Robotics: Modelling, Planning and Control*. London, U.K.: Springer, 2009, vol. 1.
- [5] A. Kamilaris and N. Botteghi, "The penetration of Internet of Things in robotics: Towards a web of robotic things," *J. Ambient Intell. Smart Environ.*, vol. 12, no. 6, pp. 491–512, Nov. 2020.
- [6] P. P. Ray, "Internet of Robotic Things: Concept, technologies, and challenges," *IEEE Access*, vol. 4, pp. 9489–9500, 2016.
- [7] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, C. Gallicchio, A. Micheli, M. Dragone, A. Saffiotti, P. Simoons, F. Cavallo, and R. Bahr, *Internet of Robotic Things—Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence and IoT Platforms*. Belgium: River Publishers, 2017, pp. 97–155.
- [8] I. Afanasyev, M. Mazzara, S. Chakraborty, N. Zhuchkov, A. Maksatbek, A. Yesildirek, M. Kassab, and S. Distefano, "Towards the Internet of Robotic Things: Analysis, architecture, components and challenges," in *Proc. 12th Int. Conf. Develop. eSyst. Eng. (DeSE)*, Oct. 2019, pp. 3–8.
- [9] P. Simoons, M. Dragone, and A. Saffiotti, "The Internet of Robotic Things: A review of concept, added value and applications," *Int. J. Adv. Robot. Syst.*, vol. 15, no. 1, Jan. 2018, Art. no. 172988141875942.
- [10] A. J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things," *Mobile Inf. Syst.*, vol. 8, no. 3, pp. 177–197, 2012.
- [11] D. Song, K. Goldberg, and N.-Y. Chong, *Networked Robots*. Cham, Switzerland: Springer, 2016, pp. 1109–1134, doi: [10.1007/978-3-319-32552-1\\_44](https://doi.org/10.1007/978-3-319-32552-1_44).
- [12] L. Romeo, A. Petitti, R. Marani, and A. Milella, "Internet of Robotic Things in smart domains: Applications and challenges," *Sensors*, vol. 20, no. 12, p. 3355, Jun. 2020. [Online]. Available: <https://www.mdpi.com/1424-8220/20/12/3355>
- [13] C. Razafimandimby, V. Loscri, and A. M. Vegni, "A neural network and IoT based scheme for performance assessment in Internet of Robotic Things," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2016, pp. 241–246.
- [14] (Sep. 2021). *The Internet of Robotic Things*. [Online]. Available: <https://www.abiresearch.com/market-research/product/1019712-the-internet-of-robotic-things/>
- [15] L. D. Wall and T. W. Koch, "Bank loan-loss accounting: A review of theoretical and empirical evidence," *Econ. Rev.*, vol. 85, pp. 1–20, Jan. 2000.
- [16] (Feb. 2017). *Human Communication Technology: Internet-of-Robotic-Things and Ubiquitous*. [Online]. Available: [https://books.google.co.in/books/about/Human\\_Communication\\_Technology.html?idJLFJEAQAQBAJ&redir\\_esc=y](https://books.google.co.in/books/about/Human_Communication_Technology.html?idJLFJEAQAQBAJ&redir_esc=y)
- [17] M. Paavola, "Wireless technologies in process automation—Review and an application example," *Tech. Rep.*, 33, 2007.
- [18] T. Anusha and M. Pushpalatha, *Enhancements in Communication Protocols That Powered IoRT*. Hoboken, NJ, USA: Wiley, 2021, ch. 8, pp. 193–217, doi: [10.1002/9781119752165.ch8](https://doi.org/10.1002/9781119752165.ch8).
- [19] D. Yoshino, Y. Watanobe, and K. Naruse, "A highly reliable communication system for Internet of Robotic Things and implementation in RT-middleware with AMQP communication interfaces," *IEEE Access*, vol. 9, pp. 167229–167241, 2021.
- [20] S. H. Alsamhi, O. Ma, and M. S. Ansari, "Artificial intelligence-based techniques for emerging robotics communication: A survey and future perspectives," 2018, *arXiv:1804.09671*.
- [21] L. Liu, T. Zhang, N. Hu, P. Zhang, and Y. Zhang, "The method of Internet of Things access and network communication based on MQTT," *Comput. Commun.*, vol. 153, pp. 169–176, Jan. 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0140366419320171>
- [22] S. Jia and K. Takase, "Internet-based robotic system using CORBA as communication architecture," *J. Intell. Robot. Syst.*, vol. 34, pp. 121–134, Jun. 2002.

- [23] O. Vermesan, R. Bahr, M. Ottella, M. Serrano, T. Karlsen, T. Wahlstrøm, H. E. Sand, M. Ashwathnarayan, and M. T. Gamba, "Internet of Robotic Things intelligent connectivity and platforms," *Frontiers Robot. AI*, vol. 7, p. 104, Sep. 2020, doi: 10.3389/frobot.2020.00104.
- [24] C. Razafimandimby, V. Loscri, and A. M. Vegni, *Towards Efficient Deployment in Internet of Robotic Things*. Cham, Switzerland: Springer, 2018, pp. 21–37, doi: 10.1007/978-3-319-61300-0\_2.
- [25] M. S. Mahmoud and A. A. H. Mohamad, "A study of efficient power consumption wireless communication techniques/modules for Internet of Things (IoT) applications," *Adv. Internet Things*, vol. 6, no. 2, pp. 19–29, 2016.
- [26] (Apr. 2022). *Features*. [Online]. Available: <https://www.microchip.com/>
- [27] C.-Y. Yum, Y. Beun, S. Kang, Y. Lee, and J. Song, "Methods to use 6LoWPAN in IPv4 network," in *Proc. 9th Int. Conf. Adv. Commun. Technol.*, Feb. 2007, pp. 969–972.
- [28] W. Colitti. (2011). *State-of-the-Art: Communication, Technology, Interoperability. Version: 0.3, ISN—Interoperable Sensor Network*. Accessed: Apr. 10, 2022. [Online]. Available: [https://www.scrip.org/\(S\(i43dyn45teexjx455qlt3d2q\)\)/reference/referencespapers.aspx?referenceid1739336](https://www.scrip.org/(S(i43dyn45teexjx455qlt3d2q))/reference/referencespapers.aspx?referenceid1739336)
- [29] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, no. 7, pp. 1655–1695, 2007. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0140366406004749>
- [30] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–24, Sep. 2018.
- [31] U. Mehboob, Q. Zaib, and C. Usama, *Survey of IoT Communication Protocols Techniques, Applications, and Issues*. Islamabad, Pakistan: xFlow Research Inc, 2016.
- [32] S. Merzouk, A. Cherkaoui, A. Marzak, and S. Nawal, "IoT methodologies: Comparative study," *Proc. Comput. Sci.*, vol. 175, pp. 585–590, Jan. 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050920317841>
- [33] S. Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, May 2017, pp. 685–690.
- [34] C. Saad, B. Mostafa, E. Ahmadi, and H. Abderrahmane, "Comparative performance analysis of wireless communication protocols for intelligent sensors and their applications," *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 4, pp. 1–10, 2014, doi: 10.14569/2Fijacsa.2014.050413.
- [35] T. S. Rappaport, *Wireless Communications: Principles and Practice*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.
- [36] S. Haykin. (May 2006). *Communication Systems 4th Edition With Solutions Manual*. Accessed: May 10, 2022. [Online]. Available: <https://www.pdfdrive.com/communication-systems-4th-edition-with-solutions-manual-e33428536.html>
- [37] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "CoolSpots: Reducing the power consumption of wireless mobile devices with multiple radio interfaces," in *Proc. 4th Int. Conf. Mobile Syst., Appl. Services*, New York, NY, USA, 2006, pp. 220–232, doi: 10.1145/1134680.1134704.
- [38] C. E. Jones, K. M. Sivalingam, P. Agrawal, and J. C. Chen, "A survey of energy efficient network protocols for wireless networks," *Wireless Netw.*, vol. 7, no. 4, pp. 343–358, 2001.
- [39] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.
- [40] S. S. Nilange, A. S. Kolhe, S. U. Kulkarni, S. S. Sawai, S. M. Lambor, and M. S. Josh, "E-LEACH: An enhanced leach protocol for minimal data loss," *Int. J. Sci. Eng. Res.*, vol. 5, pp. 140–144, May 2014.
- [41] P. C. Gupta, *Data Communications and Computer Networks*. Upper Saddle River, NJ, USA: Prentice-Hall, 2006.
- [42] A. F. Molisch, *Wireless Communications*. Hoboken, NJ, USA: Wiley, 2011.
- [43] G. Gamba, L. Seno, and S. Vitturi, "Performance indicators for wireless industrial communication networks," in *Proc. IEEE Int. Workshop Factory Commun. Syst.*, May 2010, pp. 3–12.
- [44] S. H. Alsamhi, O. Ma, and M. S. Ansari, "Survey on artificial intelligence based techniques for emerging robotic communication," *Telecommun. Syst.*, vol. 72, pp. 483–503, Mar. 2019.
- [45] C. H. Barriquello, F. E. S. E. Silva, D. P. Bernardon, L. N. Canha, M. J. D. S. Ramos, and D. S. Porto, "Fundamentals of wireless communication link design for networked robotics," in *Service Robots*, A. J. R. Neves, Ed. Rijeka, Croatia: IntechOpen, 2017, ch. 7, doi: 10.5772/intechopen.69873.
- [46] G. S. Martins, D. Portugal, and R. P. Rocha, "A comparison of general-purpose FOSS compression techniques for efficient communication in cooperative multi-robot tasks," in *Proc. 11th Int. Conf. Inform. Control, Automat. Robot. (ICINCO)*, vol. 2, Sep. 2014, pp. 136–147.
- [47] E. Sandry, "Re-evaluating the form and communication of social robots," *Int. J. Social Robot.*, vol. 7, no. 3, pp. 335–346, Jun. 2015.
- [48] J. Fink. (2011). *Communication for Teams of Networked Robots*. [Online]. Available: <https://repository.upenn.edu/edissertations/395>
- [49] V. Dutta and T. Zielińska, "Cybersecurity of robotic systems: Leading challenges and robotic system design methodology," *Electronics*, vol. 10, no. 22, p. 2850, 2021. [Online]. Available: <https://www.mdpi.com/2079-9292/10/22/2850>
- [50] L. Tai, J. Zhang, M. Liu, J. Boedecker, and W. Burgard, "A survey of deep network solutions for learning control in robotics: From reinforcement to imitation," 2016, *arXiv:1612.07139*.
- [51] X.-B. Jin, T.-L. Su, J.-L. Kong, Y.-T. Bai, B.-B. Miao, and C. Dou, "State-of-the-art mobile intelligence: Enabling robots to move like humans by estimating mobility with artificial intelligence," *Appl. Sci.*, vol. 8, no. 3, p. 379, Mar. 2018. [Online]. Available: <https://www.mdpi.com/2076-3417/8/3/379>
- [52] Y. F. Chen, M. Liu, M. Everett, and J. P. How, "Decentralized non-communicating multiagent collision avoidance with deep reinforcement learning," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2017, pp. 285–292.
- [53] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.
- [54] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano, *Internet of Intelligent Things: Bringing Artificial Intelligence into Things and Communication Networks*. Berlin, Germany: Springer, 2014, pp. 1–37, doi: 10.1007/978-3-642-35016-0\_1.
- [55] U. Challita, W. Saad, and C. Bettstetter, "Interference management for cellular-connected UAVs: A deep reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2125–2140, Apr. 2019, doi: 10.1109/WFTWC.2019.2900035.
- [56] M. Chen, M. Mozaffari, W. Saad, C. Yin, M. Debbah, and C. S. Hong, "Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1046–1061, May 2017.
- [57] M. Chen, W. Saad, and C. Yin, "Echo state learning for wireless virtual reality resource allocation in UAV-enabled LTE-U networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
- [58] M. Chen, W. Saad, and C. Yin, "Liquid state machine learning for resource and cache management in LTE-U unmanned aerial vehicle (UAV) networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1504–1517, Mar. 2019.
- [59] Z. A. Khan and A. Samad, "A study of machine learning in wireless sensor network," *Int. J. Comput. Netw. Appl.*, vol. 4, no. 4, pp. 1–8, Aug. 2017.
- [60] T. Park, N. Abuzainab, and W. Saad, "Learning how to communicate in the Internet of Things: Finite resources and heterogeneity," *IEEE Access*, vol. 4, pp. 7063–7073, 2016.
- [61] K. Shibata, "Communications that emerge through reinforcement learning using a (recurrent) neural network," 2017, *arXiv:1703.03543*.
- [62] B. Soni and A. Sowmya, "Victim detection and localisation in an urban disaster site," in *Proc. IEEE Int. Conf. Robot. Biomimetics (ROBIO)*, Dec. 2013, pp. 2142–2147.
- [63] J. Hvizdos, I. Vojtko, M. Koscelansky, J. Pavlov, J. Vascak, and P. Sincak, "Applications of remote controlled robotics in the intelligent space," in *Proc. IEEE 15th Int. Symp. Appl. Mach. Intell. Informat. (SAMII)*, Jan. 2017, pp. 117–122.
- [64] F. Khan, M. A. Jan, A. U. Rehman, S. Mastorakis, M. Alazab, and P. Watters, "A secured and intelligent communication scheme for IIoT-enabled pervasive edge computing," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5128–5137, Jul. 2021.
- [65] J. Xia, Y. Xu, D. Deng, Q. Zhou, and L. Fan, "Intelligent secure communication for Internet of Things with statistical channel state information of attacker," *IEEE Access*, vol. 7, pp. 144481–144488, 2019.

- [66] B. Javed, M. W. Iqbal, and H. Abbas, "Internet of Things (IoT) design considerations for developers and manufacturers," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 834–839.
- [67] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, no. 3, pp. 1454–1464, 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S095965261631589X>
- [68] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017.
- [69] C. Dobre and F. Khafa, "Intelligent services for big data science," *Future Gener. Comput. Syst.*, vol. 37, pp. 267–281, Jul. 2014. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167739X13001593>
- [70] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Future Gener. Comput. Syst.*, vol. 49, pp. 58–67, Aug. 2015. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167739X14001551>
- [71] K. Matthews. (Jun. 2019). *The Internet of Robotic Things: How IoT and Robotics Tech are Evolving Together*. Accessed: May 4, 2022. [Online]. Available: <https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/>
- [72] A. G. Ramonet and T. Noguchi, "IEEE 802.15.4 now and then: Evolution of the LR-WPAN standard," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2020, pp. 1198–1210.
- [73] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Extension in the 2.4 GHz Band, Standard 802.11b-1999*, 2022. Accessed: May 10, 2022. [Online]. Available: [https://standards.ieee.org/standard/802\\_11b-1999.html](https://standards.ieee.org/standard/802_11b-1999.html)
- [74] (2015). *RFC 7668: IPv6 Over BLUETOOTH(R) Low Energy*. Accessed: May 10, 2022. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc7668.html>



**NEHA KOUL** received the master's degree in computer science and IT from Baderwah Campus, University of Jammu, Jammu and Kashmir, India, in 2014. She is currently pursuing the Ph.D. degree in computer science with the Central University of Jammu, India. Her Ph.D. topic is "intelligent and secure data exchange for Internet of Robotic Things." Her current research interests include the Internet of Robotic Things (IoRT), robotics, the Internet of Things (IoT), machine learning, and computer vision.



**NEERENDRA KUMAR** received the Ph.D. degree from Óbuda University, Budapest, Hungary. He is currently working as a Senior Assistant Professor at the Department of Computer Science and IT, Central University of Jammu. He has received the Stipendium Hungaricum Scholarship for his Ph.D. studies. His Ph.D. topic is "robot navigation in an unknown and dynamic environment." His current research interests include mobile robot navigation, the IoRT, machine learning, and programming languages.



**AQSA SAYEED** received the B.Tech. degree in information technology from Baba Gulam Shah Badshah University, Rajouri, Jammu and Kashmir, India, in 2020, and the M.Tech. degree in computer science and technology from the Central University of Jammu, India, in 2022. Her research interests include the Internet of Robotic Things, the Internet of Thing, cyber security, and machine learning.



**CHAMAN VERMA** is working as an Assistant Professor and the Ph.D. Candidate with the Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, Hungary. He has been awarded a Research Scholarship "ÚNKP, Ministry of Innovation and Technology (MIT), and National Research, Development and Innovation (NRDI) Fund, Hungarian Government," for the years 2021–2022, and 2022–2023. From 2018 to April 2022, he worked

as a Professional Assistant in the EFOP Project, which was co-funded by the European Union and the Hungarian Government. His current research interests include optimization and feature engineering, statistical analysis, machine learning, real-time systems, deep learning, computer vision, health care, educational informatics, and sickness prediction. He is a guest editor of reputed journals. He is also an editorial board member and a reviewer of several scientific conferences and international publications. He has Scopus citations 495 with H-index 14. He has Web of Science citations 78 with H-index 8.



**MARIA SIMONA RABOACA** is currently a Researcher at the Hydrogen, and Fuel Cell Department, National Research and Development Institute for Cryogenics and Isotopic Technologies (ICSI Rm. Valcea). Her Ph.D. topic is "theoretical and practical contribution regarding sustaining with hybrid energy a passive house" with the Faculty of Building Services Engineering, Technical University of Cluj—Napoca, Romania. She is also responsible at ICSI for the project "smart conductive charging station, fixed and mobile, for electric propulsion transportation (SMiLE-EV)." Her scientific activity materialized in 12 book chapters published abroad, and more than 50 scientific papers published in international/national conference proceedings and journals indexed in WoS/other international databases. Also, she is a Team Member in another research contract with Suceava University and has one patent application.

...