Internet of Things Protocols (IoTp) Literature Review

Ali Alamery
Balad Al-hadeth group company.
Baghdad, Iraq
alamery.ali.mohamed@gmail.com

Yousif I. Hammadi
Department of Medical Instruments Engineering Techniques, Bilad Alrafidain University College, Diyala, Iraq
yousif.ibrahim.hammadi@gmail.com

Mohanad Abd Shehab
Electrical Engineering Department College of Engineering, Mustansiriyah University, Baghdad, Iraq
mohanadshehab@uomustansiriyah.edu.iq

Ahmed Aziz
Department of computer science, Faculty of computer and Artificial intelligence, Benha university, Egypt.Department of international business Management, Tashkent state university of Economics, Tashkent, Uzbekistan
ahmed.aziz@fci.bu.edu.eg

Omar Abdulkareem Mahmood
Department of Communications Engineering, College of Engineering, University of Diyala, Diyala, Iraq
omar_abdulkareem@uodiyala.edu.iq

Mohammed Saleh Ali Muthanna
Institute of Computer Technologies and Information Security, Southern Federal University, 347922 Ta-ganrog, Russia
muthanna@sfedu.ru

ABSTRACT

Considering today's variety of technologies and devices connected to the network, a huge number of manufacturers, there are many problems of their interaction and the need to create and adopt specialized communication standards and protocols. This article is devoted to the description of various protocols proposed by the IEEE, IETF and ITU for use in the framework of the concept of the Internet of Things. The article includes a description of the protocols of the application, transport, network and data link layers of the TCP / IP model. It also discusses protocols designed specifically to meet IoT requirements. A brief description of the protocols and the principle of operation of each of them are given. This review article contributes to a more correct choice of protocols when building a network, detecting and managing devices, and establishing interaction between objects of the Internet of Things.

CCS CONCEPTS

• **Internet of things, protocols, TCP/IP, standards.**;

ACM Reference Format:
Ali Alamery, Yousif I. Hammadi, Mohanad Abd Shehab, Ahmed Aziz, Omar Abdulkareem Mahmood, and Mohammed Saleh Ali Muthanna. 2023. Internet of Things Protocols (IoTp) Literature Review. In *The International Conference on Future Networks and Distributed Systems (ICFNDS '23), December 21, 22, 2023, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3644713.3644835

ICFNDS '23, December 21, 22, 2023, Dubai, United Arab Emirates

ACM ISBN 979-8-4007-0903-6/23/12
https://doi.org/10.1145/3644713.3644835

1 INTRODUCTION

An increasing number of physical objects are linked to the Internet at an unparalleled pace, realizing the Internet of Things (IoT) concept. Thermostats and HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems that allow smart homes are a fundamental examples of such objects. There are also other areas and conditions where the IoT can play a significant role and enhance the quality of our life. Transportation, healthcare, factory automation, and emergency response are among these applications .

Such apps include travel, healthcare, industrial automation, and emergency response to natural and man-made disasters where it is difficult to make human decisions. The IoT helps physical objects, by making them "talk" together, exchange information and organize decisions, to see, hear, think and perform jobs. By leveraging its underlying technologies, such as ubiquitous and widespread computing, embedded devices, networking technologies, sensor networks, Internet protocols and applications, the IoT transforms these objects from conventional to smart.

Today, IoT technologies are applied aggressively in all aspects of society, enabling the use of different, not necessarily physical, devices to deliver real, life enhancing solutions to humans. Devices may hear, see, think and act in some cases[1]. For proper and efficient operation, devices must communicate and coordinate correctly with others in order to make decisions that can be as critical as saving lives or buildings. Distributed computing technologies, built-in sensors, and modern wireless technologies allow the Internet of Things to do its job.

However, taking into account the current diversity of these technologies and devices, a huge number of manufacturers, there are many problems of their interaction and the need to create and adopt specialized standards and communication protocols[2]. The development of successful IoT applications includes the tasks of ensuring mobility: when the IoT device moves, the IP address changes, therefore, it is necessary to streamline the routing protocols; reliability (the system must be very reliable and fast in terms of collecting and

transmitting data and making decisions), scalability, i.e. expandability of network users.

The concept of the Internet of Things assumes that millions of devices will be connected to the network. Also among the tasks it is necessary to note the provision of control and availability: tracking failures, configuration and performance of such a large number of devices, for which the corresponding management protocols are responsible. In addition, interoperability in the network must be ensured: heterogeneous devices and protocols must be able to work with each other while maintaining security and confidentiality. In general, the following model of interaction between devices in the Internet of Things is adopted. Terminal devices, sensors, sensors communicate with each other (the so-called D2D interaction - Device to Device).

The data collected by the devices is sent to the server for further processing analysis (D2S - Device to Server interaction). This server can include several computers or objects that also need to communicate with each other (S2S - Server to Server interaction). Different protocols need to be used to accomplish different tasks. The following are the most common and promising protocols to date, with a brief description of each. Figure 1 shows the growth of IoT during the last three decades[3].

2 UTILIZATION OF IOT

Wearable IoT devices are an important part of the healthcare domain. Device that supports efficient data synchronization between multiple devices, Fit Pieces, Heart Rate Monitors, and Glucose Monitors are examples of wearable devices. those devices help to diagnose diabetes disease, and monitoring could be used to view the glucose level[4]. For remote control and management of home appliances such as air conditioners, TV sets, locks, surveillance cameras and electrical appliances such as lights, fans, electronic meters and so on, a home-based IoT application uses devices linked through the Internet[5]. . IoT devices also used for monitoring climate conditions, green house automation, crop management, cattle rearing and management, agriculture is supported. The data status of the fields can be accessed remotely via smart phones, laptops or desktops[6]. In industrial applications, the fundamental improvements in the way IoT is remotely combined with control, monitoring and manufacturing produce a groundbreaking improvement in automation[7].

The IoT is used by Smart Grid apps to enhance the energy consumption of houses and buildings and to help power providers monitor and manage resources. These can be used for energy use collection, analysis, control, tracking, and management. The IoT helps energy suppliers to develop their services to meet the needs of customers.

The smart grid also eliminates future faults, increases reliability and improves the quality of services (QoS). Usage of IoT and convergence between computing and communication in industrial transportation to track and manage the energy network. Its goal is to enhance the reliability, performance, availability and protection of the smart grid infrastructure. Sensors will gather data in the event of a natural disaster, and repetitive signals from emergency areas will come into play.

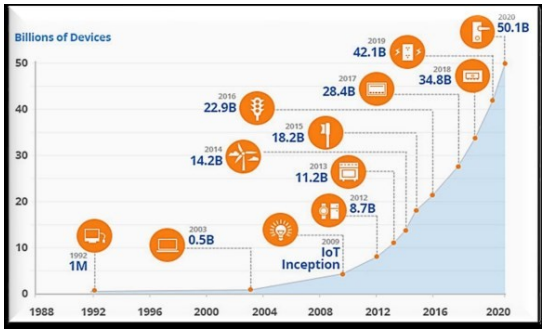

Figure 1: IoT growth rate.

These sensors will directly relay information to government officials and emergency teams about their surroundings IoT applications therefore need effective security protocols for the safety of network data.[8]. For any layer of IoT architecture from the research front, security is the most important function based on. With security issues, the efficient implementation of the IoT framework would be possible while designing it. Safety must therefore be discussed at the stage of developing the application to control and maintain IoT networks[9]. In this paper the most important IoT protocols discussed depending on the field of application and protocol nature.

Currently, IoT applications are the significant domain that requires security of data and information. There are more chances that the hackers will launch attacks on the data used by the applications. IoT protection is therefore the most necessary and paramount prerequisite for IoT developers. Current authentication mechanisms such as Regular Message Digest (MD5), Hash-based Message Authentication Code (HMAC) and hashing algorithms and encryption mechanisms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest, Shamir, and Adelman are of little concern (RSA)[10]. IoT has formerly dealt with bytes and bytes of data to be shared over the network every second. Secondly, when exchanging information between users, the IoT devices are memory and space limited, which are more vulnerable to security challenges.

IoT systems are often heterogeneous in design, requiring the implementation of standard protection mechanisms. IoT systems therefore need effective security measures for the safety of network data[11]. For any layer of IoT architecture from the research front, security is the most important function based on. With security issues, the efficient implementation of the IoT framework would be possible while designing it. Safety must therefore be discussed at the stage of developing the application to control and maintain IoT networks.

3 EXISTING PROTOCOLS OVERVIEW

The proper descriptions of transmission, design, and rules of any digital message are communication protocols. These protocols form the backbone of IoT networks as they enable smart services and applications to be linked and connected to them. Furthermore, they allow intelligent things and devices via these networks to exchange their sensed data. The following features are specified by the key

functions of communication protocols: various smart device addressing systems, transmitted data formats, data encoding, flow control, retransmission of lost packet paths, and IoT packet routing processes from source nodes to destination nodes[12]. The IoT sector is widespread and rapidly expanding, comprising a vast number of heterogeneous smart objects and power-restricted devices that have limited storage and computing resources linked to the IoT network[13]. IoT communication protocols, on the basis of that, face several difficulties that should be taken into account when developing an IoT application, which are as follows[14]:

Identification and addressing: Since millions of smart devices are connected to internet, a single address must be used to identify each device that enables it to communicate with other objects. A broad addressing space is needed based on that.

Reduced power communication: the data exchange process via devices, particularly in a wireless medium, is a power consuming activity. A solution is therefore needed to facilitate communication between smart devices with low power consumption.

Routing protocol with minimal memory requirements and effective communication patterns.

High speed robust communication among IoT devices.

Smart devices mobility requirements insurance.

To address the aforementioned difficulties of IoT protocols, several classifications have been suggested. We follow the well-known classification in this article that refers to the OSI model to define the initial, recent and future changes to each IoT layer protocol as follows:

4 IOT PROTOCOLS FOR APPLICATION LAYER

The IoT application layer is responsible for deciding acceptable protocols and providing services that are needed at the application level for message passing. Many considerations, such as power consumption, necessary bandwidth, transmission and link time, delivery guarantee, data protection, and packet size, should be taken into account when choosing the appropriate communication protocol for a particular application. The main protocols are:

Message Queue Telemetry Transport: It is a lightweight protocol developed by Andy Stanford-Clark and Arlen Nipper in 1990. In several ways, such as M2M, server to server and machine to server, it allows the communication process between IoT devices and the middleware and applications network, and it operates above the Transmission Control Protocol/Internet Protocol (TCP/IP) top[15].

Hypertext Transfer Protocol: It is a web message and text-based protocol that was developed by Tim Berners-Lee in 1997 and also supports the request/response feature of the Representational State Transfer Protocol (RESTful) where the client sends an HTTP request message to the server[16].

Extensible Messaging and Presence.

Protocol: It was proposed by the Homonym open source group in 1999 and has been standardized by the Internet Engineering Task Force (IETF). XMPP facilitates lowlatency communication and small-message delivery, making it ideal for many services such as video and voice calls, instant messaging, chat, publish-subscribe systems, gaming, and IoT applications. This protocol allows communication between heterogeneous applications due to its simplicity and versatility. However, it consumes network bandwidth, requires high CPU capabilities, only allows basic data type transmission, and there is no QoS guarantee[17].

Representational State Transfer Protocol: The REST Protocol has been developed by Roy Fielding to provide web services that facility data exchange and communication between different devices, and construct and offer desirable features such as modifiability, and scalability, of distributed hypermedia systems. RESTful is based on the HTTP protocol to support request-response and client-server models, which will allow the client to access IoT server resources. However, RESTful Application Programming Interfaces (APIs) are considered a reasonable option for multiple IoT applications because they are lightweight and simple protocols[18].

Constrained Application Protocol: The IETF proposed this protocol to adapt to communicate between resource-controlled and non-sync devices, ensure flow management, efficient distribution and easy control of congestion to IoT applications. It also supports a contact model for publishing/subscribing based on multi-cast and unicast requests. Because of the simplicity, small message size and low code footprint, CoAP runs over User Datagram Protocol (UDP) in order to handle resources, reduce the requirements for bandwidth and avoid TCP handshake overloads until transmission begins[19].

Advanced Message Queuing Protocol: In 2003, John O'Hara developed the architecture for publishing/subscribing based on an accurate and stable message queue. It supports efficient and safe communication between heterogeneous devices and is widely used in both business and commercial areas. AMQP The TCP protocol also provides greater reliability. The data transmission process through AMQP involves two steps: message queue and exchange queue. The messages are saved in the message queue model before they are forwarded to the recipient, while the message will be routed in proper order in the message queue type[20].

Data Distribution Service: The Object Management Group (OMG) works on high performance, real time, interoperable, scalable, and secure data communication based on the publish/subscribe model via TCP/UDP transportation protocols. DSS is founded on Peer-to-Peer (P2P) and Decentralized communication through a data bus that enables the transmission of asynchronous data, making it an effective solution for IoT applications.

5 IOT PROTOCOLS FOR TRANSPORT LAYER

This layer is known as a routing layer because it runs data packets in the network region where its protocols are responsible for ordering packets, detecting errors and correcting. The following parts define the key transport protocols that are used with their developments and potential works in IoT environments.

Transmission Control Protocol (TCP): This is a heavy-weight protocol, which means that the link needs to be formed before all necessary data is exchanged. TCP is suitable for secure communications because it requires a message of acknowledgement to ensure that each transmission and receipt phase is assured, supports transmission of missing or corrupted packets and a flux control mechanism. The overhead packet in this protocol would therefore be extremely wide, resulting in higher power consumption on devices and therefore in an unsuitable operation on power-controlled

systems. TCP splits the data packet into several packets, of which each packet has a source and destination IP order number[21].

User Datagram Protocol (UDP): It is a protocol that provides unreliable, minimum message queueing, message passing and optimum transport to IP-operated protocols and applications. No link between communicating entities must be formed between the ends, so that certain applications that require real time performance at low latency such as video and voice communication is very efficient. In addition, the ordering, duplicate, distribution or security of data packets are not guaranteed. On the other hand, UDP includes a port number attribute to address source and destination functions as well as a data integrity management description[22].

DCCP (Datagram Congestion Control

Protocol): It provides unicast bidirectional datagram-controlled insecure dynamic congestion links. DCCP is thus suitable for applications with large quantities of data and applications that sacrifice reliability and timeliness, for example Voice over Internet Protocol (VoIP) and media streaming. The DCCP flow rate can be changed progressively as it is unstable and does not have a receiving window[23].

Stream Control Transmission

Protocol(SCTP): It is a protocol with a connectionless, message-oriented and IP transport layer like UDP that Stewart developed and released in 2007. On the other hand, SCTP provides secure P2P connection-oriented transmission for applications that communicate over an IP. Thus, most TCP features are inherited, including the recovery of missing packets and congestion management[24].

Resource Reservation Protocol (RSVP): It is a multicast and unicast transmission control protocol designed to provide a versatile, stable, scalable and heterogeneous reserve resource setup for data stream transmission at each router. RSVP organizes the formats of messages, hosts and routers, and can also run over IPv4 or IPv6 (Baker et al., 1997). It also supports several features, such as resource reservations along the data path in each node, multipoint to multipoint communication paradigms, cache (state) management routers and reservation initiated by the recipient[25].

Aeron: It is an open-source connection oriented communication protocol that Martin Thompson proposed to run over insecure media such as InfiniBand and UDP, as well as to provide optional redundancy for transmission by retransmitting dropped packets in order. Aeron aims to provide the lowest latency with the highest efficiency, which makes it suitable for real-time device communication, VoIP, fast-paced networked multiplayer gaming, video streaming, and high-frequency financial trading. However, Java language implementation of this protocol would focus on decreasing resource requirements such as memory and CPU[11].

Network layer IoT protocols

It is the duty of this layer to form, address and route data packets, as it receives datagram packets from the transport layer and converts them into the form of data packets, which are then transmitted to the destination side. The following sections address the common routing protocols, together with their potential improvements, that are commonly used in the transmission of data packets.

Routing Protocol for Low-Power and Lossy Network (RPL): It is a tree-based, IPv6 constructive, distance vector routing protocol designed in 2012 by the routing over-low-power-and-lossy-networks working group to operate over networks of commercial appliances that are lossy and low-power, where their interconnections are characterized by instability, low data rates and high loss rates[26].

Cognitive Routing Protocol for Low-Power and Lossy Network (CORPL): It is an extension of the RPL protocol, which has been developed to suit the cognitive network and is based on DODAG topology with new modifications in routing generation. CORPL uses an opportunistic forwarding mechanism which allows the next hop for data transmission to select the optimal forwarder from a collection of qualified neighbors. Each node maintains a collection of forwarders rather than one parent in this approach and updates its set based on the receiving DIO messages[27].

Channel-Aware Routing Protocol (CARP): It is a distributed protocol which, because of its lightweight data packet, was designed for underwater and IoT applications. Based on the efficient data transfer that occurred by neighboring sensors, CARP considers connection quality to opt for the forwarder nodes. CARP's routing operation consists of an initialization step for the network and a forwarding step for data. The sink node transmits hello messages containing its ID along with the hop count in the first step, enabling the receiving node to update its distance to the sink node. In the data transmission process, the sender transmits a ping message to its neighbors in order to select the optimal relaying node based on the quality of the connection and the information it receives from the pong messages, in order to transmit the data through the optimal node. [28].

Collection Tree Protocol (CTP): It is a tree based routing protocol that was developed to provide the best effort in networks with low energy demands for any communication. Some nodes initially advertise themselves as root nodes (sink nodes), where data is supplied to the root at a minimal cost. Other nodes will connect via beacon advertising to the root tree, then send their collected data to the next hop towards the sink node based on their neighbors' minimum estimated transmission count (ETX) cost. CTP does not, however, allow reverse routing to sensors from the sink node[29].

An Efficient Routing Protocol for Emergency Response Internet (ERGID): It attempts to provide IoT applications with reliable data transmission and effective emergency response. Considering global latency estimation and the residual energy of the candidate route nodes, ERGID selects the optimal route towards the destination. The first technique is called the iterative delay process, which aims to mitigate the issue of disregarding valid routes, constantly updating routing tables and maintaining real-time coordination for emergency response applications. Whereas, the second procedure is called the option of residual energy likelihood[30].

Parent Aware Objective Function (PAOF): It is a constructive objective feature protocol that aims to achieve load balancing by using parent count and ETX metrics for data transmission in route selection. PAOF first calculates the difference between the ETX of the candidate nodes in order to choose the desired path, in the event that if it is smaller than the predefined value called MinHopRank-Increase, 4 it will compare the number of parents and ultimately choose the least value as the preferred route[31].

Ad-Hoc On-Demand Multipath Distance Vector for IoT (AOMDV-IoT): It aims to discover and establish a link between the Internet and nodes. For each node, AOMDV-IoT establishes two routing tables: the Internet Connecting Table (ICT) and the routing table. It also converts IP addresses to Internet Connecting Addresses (ILA).

Once a node requests to be linked to the internet, to allow searching via ICT, the requisite IP will be converted to ILA, which provides the source node with an acceptable internet node. In the event that there is no ICT internet node, the source node broadcasts a requested packet to update both tables before the optimal route to the internet node is identified[32].

6 CONCLUSIONS

The emerging notion of technology for IoTs has quickly spread Throughout our contemporary lives, it seeks to maximize the quality of our lives by incorporating intelligent objects, software, and technology in order to automate all things in the surrounding setting. What separates our survey paper from other works is that it covers the IoT paradigm's most important sides, concentrating on what has been done and what has needed further study. In particular, this paper provides an overview of IoT protocols. IoT protocols divided into three groups depending on the field of application : application layer protocols, transport layer protocols and network layer protocols to give the reader clear view about one of the most important part in IoT field.

REFERENCES

[1] Ateya, Abdelhamied A., Ammar Muthanna, Irina Gudkova, Anastasia Vybornova, and Andrey Koucheryavy. "Intelligent core network for Tactile Internet system." In Proceedings of the international conference on future networks and distributed systems, pp. 1-6. 2017.

[2] Muthanna, Mohammed Saleh Ali, Ammar Muthanna, Ahsan Rafiq, Mohammad Hammoudeh, Reem Alkanhel, Stephen Lynch, and Ahmed A. Abd El-Latif. "Deep reinforcement learning based transmission policy enforcement and multi-hop routing in QoS aware LoRa IoT networks." Computer Communications 183 (2022): 33-50

[3] K. A. M. Zeinab and S. A. A. Elmustafa, "Internet of things applications, challenges and related future technologies," World Sci. News, vol. 2, no. 67, pp. 126–148, 2017.

[4] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," IEEE access, vol. 3, pp. 678–708, 2015.

[5] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," in 2016 international conference on computing, communication and automation (ICCCA), 2016, pp. 1286–1289.

[6] I. Mohanraj, K. Ashokumar, and J. Naren, "Field monitoring and automation using IOT in agriculture domain," Procedia Comput. Sci., vol. 93, pp. 931–939, 2016.

[7] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A lightweight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," Futur. Gener. Comput. Syst., vol. 78, pp. 1005–1019, 2018.

[8] K. Yang, D. Forte, and M. M. Tehranipoor, "Cdta: A comprehensive solution for counterfeit detection, traceability, and authentication in the iot supply chain," ACM Trans. Des. Autom. Electron. Syst., vol. 22, no. 3, pp. 1–31, 2017.

[9] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digit. Commun. Networks, vol. 4, no. 2, pp. 118–137, 2018.

[10] S. Turner and L. Chen, "Updated security considerations for the MD5 message-digest and the HMAC-MD5 algorithms," RFC 6151, March, 2011.

[11] A. B. M. Adam, M. S. A. Muthanna, A. Muthanna, T. N. Nguyen and A. A. A. El-Latif, "Toward Smart Traffic Management With 3D Placement Optimization in UAV-Assisted NOMA IIoT Networks," in IEEE Transactions on Intelligent Transportation Systems, 2022, doi: 10.1109/TITS.2022.3182651.

[12] M. S. Mahmoud and A. A. H. Mohamad, "A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications," 2016.

[13] I. J. Timmins and G. T. Hazelton Jr, "Self-monitoring cable system." Google Patents, 11-Apr-2017.

[14] Muthanna, M.S.A.; Wang, P.; Wei, M.; Abuarqoub, A.; Alzu'bi, A.; Gull, H. Cognitive control models of multiple access IoT networks using LoRa technology. Cogn. Syst. Res. 2021, 65, 62–73.

[15] A. A. O. Bahashwan and S. Manickam, "A brief review of messaging protocol standards for internet of things (IoT)," J. Cyber Secur. Mobil., vol. 8, no. 1, pp. 1–14, 2019.

[16] N. S. Han, "Semantic service provisioning for 6LoWPAN: powering internet of things applications on Web." 2015.

[17] M. B. Yassein and M. Q. Shatnawi, "Application layer protocols for the Internet of Things: A survey," in 2016 International Conference on Engineering & MIS (ICEMIS), 2016, pp. 1–4.

[18] H. V Nguyen and L. Lo Iacono, "RESTful IoT authentication protocols," in Mobile Security and Privacy, Elsevier, 2017, pp. 217–234.

[19] [19] Rafiq, A.; Ali Muthanna, M.S.; Muthanna, A.; Alkanhel, R.; Abdullah, W.A.M.; Abd El-Latif, A.A. Intelligent edge computing enabled reliable emergency data transmission and energy efficient offloading in TiSCH-based IIoT networks. Sustain. Energy Technol. Assess. 2022, 53, 102492.

[20] [20] Ateya, Abdelhamied A., Ammar Muthanna, Anastasia Vybornova, Pyatkina Darya, and Andrey Koucheryavy. "Energy-aware offloading algorithm for multi-level cloud based 5G system." In Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 18th International Conference, NEW2AN 2018, and 11th Conference, ruSMART 2018, St. Petersburg, Russia, August 27–29, 2018, Proceedings 18, pp. 355-370. Springer International Publishing, 2018

[21] Y. Hasegawa and J. Katto, "A Transmission Control Protocol for Long Distance High-Speed Wireless Communications," IEICE Trans. Commun., 2017.

[22] U. D. P. Lightweight, "Internet Engineering Task Force (IETF) G. Fairhurst Request for Comments: 8304 T. Jones Category: Informational University of Aberdeen," 2018.

[23] HAMMADI, Yousif I. Fiber Bragg grating-based monitoring system for fiber to the home (FTTH) passive optical network. Journal of Optical Communications, 2022, 43.4: 573-583.

[24] "SCTP Overview - TechLibrary - Juniper Networks." [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-gprssctp.html. [Accessed: 08-Jan-2021].

[25] A. B. M. Adam, X. Wan, M. A. M. Elhassan, M. S. A. Muthanna, A. Muthanna, N. Kumar, *et al.*, "Intelligent and Robust UAV-Aided Multiuser RIS Communication Technique With Jittering UAV and Imperfect Hardware Constraints", IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 10737-10753, 2023.

[26] T. Winter *et al.*, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.," rfc, vol. 6550, pp. 1–157, 2012.

[27] HAMMADI, YOUSIF I.; MAHMOOD, OMAR ABDULKAREEM. Transmission performance analysis of 5.76 Tbps MC-WDM system incorporating optical wireless communication. Optoelectron Adv Mater Rapid Commun, 2022, 16: 130-6.

[28] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: A channel-aware routing protocol for underwater acoustic wireless networks," Ad Hoc Networks, vol. 34, pp. 92–104, 2015.

[29] Masek, Pavel, Radek Fujdiak, Krystof Zeman, Jiri Hosek, and Ammar Muthanna. "Remote networking technology for iot: Cloud-based access for alljoyn-enabled devices." In 2016 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT), pp. 200-205. IEEE, 2016.

[30] J. V. V Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," Sensors, vol. 19, no. 9, p. 2144, 2019.

[31] ALWAN, Mohammed Hasan, *et al.* A Novel Technique for Creating Optical Multi-carrier Generation Using Nested Electro-Absorption Modulators. In: International Conference on Distributed Computer and Communication Networks. Cham: Springer Nature Switzerland, 2022. p. 17-28.

[32] Y. Tian and R. Hou, "An improved AOMDV routing protocol for internet of things," in 2010 International Conference on Computational Intelligence and Software Engineering, 2010, pp. 1–4.

[33] Osamy, Walid, Ahmed Aziz, and Ahmed M. Khedr. "Deterministic clustering based compressive sensing scheme for fog-supported heterogeneous wireless sensor networks." PeerJ Computer Science 7 (2021): e463.

[34] Salim, Ahmed, *et al.* "Somaca: A new swarm optimization-based and mobility-aware clustering approach for the internet of vehicles." IEEE access (2023).

[35] Aziz, Ahmed, *et al.* "Optimising compressive sensing matrix using Chicken Swarm Optimisation algorithm." IET Wireless Sensor Systems 9.5 (2019): 306-312.

[36] Aziz, Ahmed, *et al.* "Iterative selection and correction based adaptive greedy algorithm for compressive sensing reconstruction." Journal of King Saud University-Computer and Information Sciences 34.3 (2022): 892-900.

[37] Aziz, Ahmed, *et al.* "Compressive sensing based routing and data reconstruction scheme for IoT based WSNs." Journal of Intelligent & Fuzzy Systems 41.1 (2021): 19-35.