Data Link in IoT WSNs

Subjects: Computer Science, Information Systems

Contributor: Muhammad Zulkifl Hasan , Zurina Mohd Hanapi

The Internet of things (IoT) and wireless sensor networks (WSNs) have been rapidly and tremendously developing recently as computing technologies have brought about a significant revolution. Their applications and implementations can be found all around us, either individually or collaboratively. WSN plays a leading role in developing the general flexibility of industrial resources in terms of increasing productivity in the IoT. The critical principle of the IoT is to make existing businesses sufficiently intelligent to recognize the need for significant fault mitigation and short-cycle adaptation to improve effectiveness and financial profits.

wireless sensor networks (WSNs) Internet of things (IoT) computer network security

1. Introduction

The Internet of things (IoT) and wireless sensor network (WSNs) have seen a rapid and massive transformation in recent years, when all the computer science domains, operating independently or collaboratively, have seen unprecedented change, and their technologies and deployments can be observed all around us. A wireless sensor network (WSN) is a network that connects and collaborates. Its sensors are placed in different environments to collect the best data [1]. WSNs are made up of remote nodes that have a lot of promise for various businesses and are built on ad-libbed system architectures [2]. According to a report, a new network uprising has just recently begun, with approximately 50 billion items and smartphones expected to be connected to the Internet by 2020 [3]. The ever-increasing number of internet-related things is transforming the world we live in. Smart cities, network security management, e-health, traffic control, smart shopping, pollution control, radiation level detection, online education, cloud computing, intruder detection, smart parking, vehicle auto-fault diagnostics, and many other implementations of the IoT and WSN are only a few examples of this transformation [4]. The demographics of the WSN application spectrum palette are shown in **Figure 1** [5].

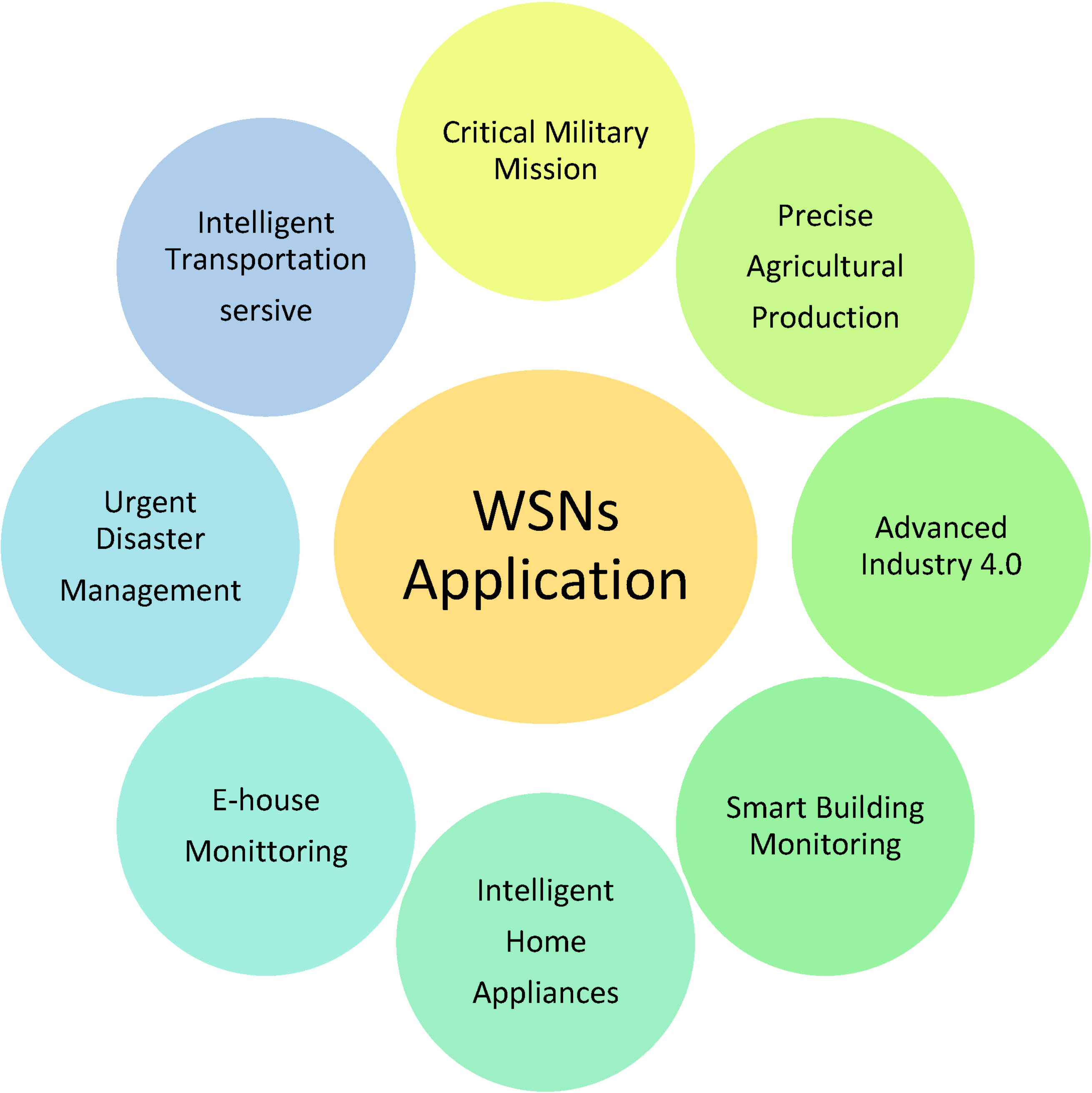
Critical Military Mission
Intelligent Transportation sersive
Precise Agricultural Production
Urgent Disaster Management
WSNs Application
Advanced Industry 4.0
E-house Monittoring
Smart Building Monitoring
Intelligent Home Appliances

Figure 1. Application area spectrum of wireless sensor networks (WSNs) [5].

One of WSN's applications can be found in the clinical and medical sciences. Consequently, medical frameworks are being developed that collect health data from the human body using wearable sensors that can also be embedded within an individual's body. These sensors communicate the gathered information, which can be further monitored and processed to obtain various insights [6][7][8]. **Figure 2** shows 2020's top IoT applications and the enterprise share of IoT projects worldwide [9].

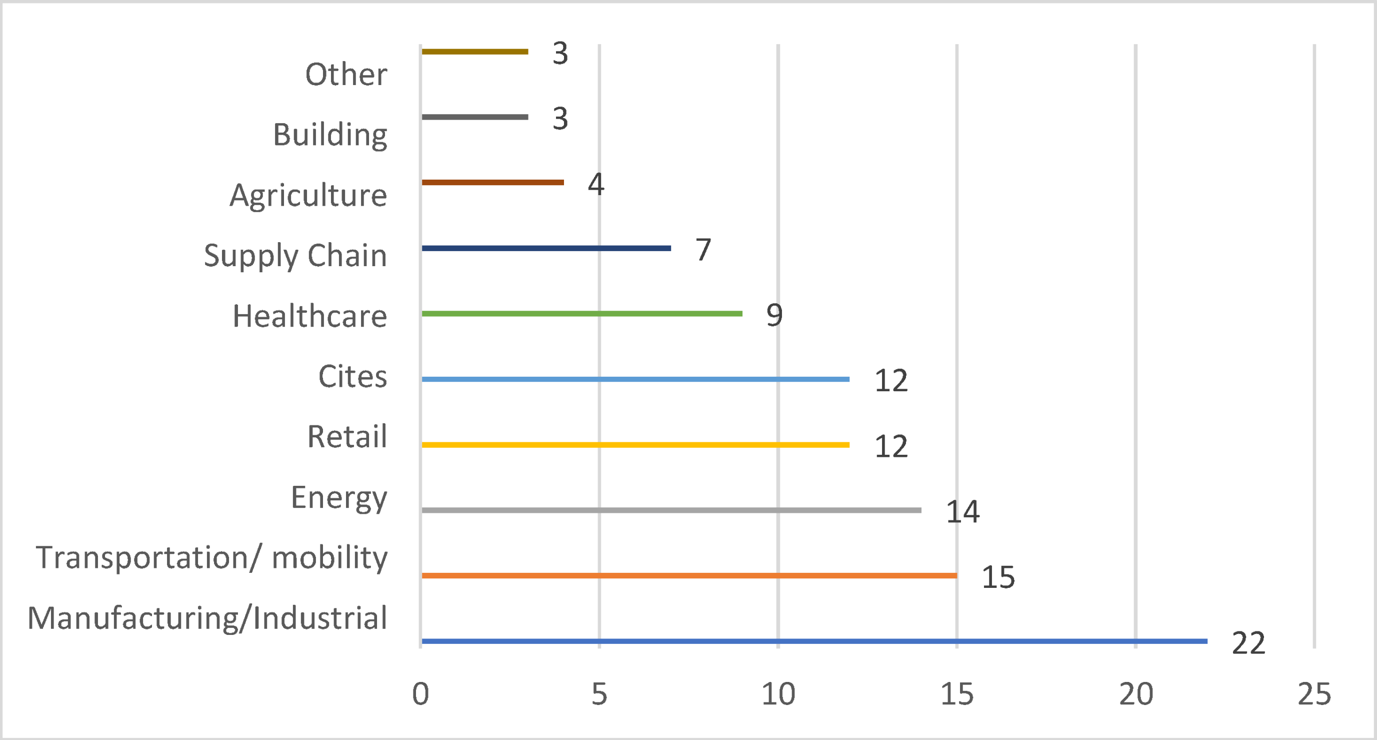

Figure 2. Top areas of IoT application in 2020 [10].

WSN makes use of a sensor network architecture. The Open Systems Interconnection (OSI) architectural model is the most common architecture for wireless sensor networks. WSN's structure comprises five primary and three cross layers. It is common practice in sensor n/w to use all five levels. In addition to hospitals and schools, roadways and buildings may also benefit from this design, which can be used for several purposes, including disaster and crisis management and security. The two types of WSN architecture are layered network architecture (LNA) and clustered architecture (CA).

2. Layered Network Architecture

A base station and a high number of sensor nodes are used in this network. Network nodes may be arranged in concentric circles. The structure consists of three cross layers and five interlocking layers. The five architectural layers are as follows:

- Application layer;
- Transport layer;
- Network layer;
- Data link layer;
- Physical layer.

The following are examples of the three cross layers:

- Power management plane;
- Mobility management plane;
- Task management plane.

Data Link Layer

The data connection layer is a program's protocol layer that regulates data transit through and out of the physical link of a network. The Open Systems Interconnection (OSI) model is used for telecommunication protocols [11]. Data bits are decoded, organized, and encoded at the data link layer until they are transferred as frames between two nearby nodes on the same LAN or WAN [12]. The data connection layer also manages the recovery of devices from collisions that occur when many nodes attempt to send frames simultaneously. The data link layer has two sub-layers: the logical connectivity control (LLC) sub-layer and the network access control (MAC) sub-layer [13]. The communication channel that links the adjacent nodes is known as the tie, and each datagram must be sent via a separate connection from the source to the destination [14].

Clustered Network Architecture

This architecture relies on the "LEACH protocol", since it uses clusters to group sensor nodes. "LEACH protocol" is an acronym for "low-energy adaptive clustering hierarchy". Clustering is implemented in a two-tier structure. Sensor nodes are organized into clusters using this distributed approach. The TDMA (time-division multiple access) plans are created by the cluster head nodes in each individually formed cluster. The energy consumption of a network is reduced because of the data fusion concept. The ability to combine data in this network design makes it incredibly popular. In any cluster, all nodes may access data by interacting with the cluster head.

3. WSN in IOT

Heterogeneous WSNs that connect a diverse set of intelligent sensors have formed the foundation for IOT-based systems all around us, promising significant advancements shortly. With the rapid expansion of these technologies, there has been an increase in the temptation to reduce their energy use. Tremendous advances in communication and information flow have contributed to unsustainable increases in energy consumption and carbon emissions. However, sensor nodes must operate successfully for extended periods (even years) in most applications because of various application criteria (e.g., environmental management, agriculture, border surveillance or protection, etc.). Dead nodes may affect data reliability, precision, and device compatibility, which are essential for an application's long-term sustainability. A sensor node is typically composed of four primary units: the processing unit, the sensing/identification unit, the communication unit, and the power supply unit, as shown in **Figure 5**. Filters, amplifiers, transducers, comparators, and other secondary components are combined with the core above. Data from the workplace are collected and detected by the sensor device. All the other devices require power, which is supplied by the power unit (usually a battery-limited one) and delivered to the BS (base stations) through the communication unit, which performs data processing functions, including data collection, as well as data manipulation duties, such as data gathering. The quantity of energy that a sensor node utilizes is based on its present state, which may be one of three states: sleeping, idle, or active. In active mode, the node uses the most significant energy. Due to the transmission and reception of information, the sensing device can release as much energy as is feasible while absorbing as little as possible. Though the energy the processing unit uses is far less than that required by the radio subsystem, it is more significant than that required by the sensor subsystem. There is a relationship between factors such as communication distance, monitoring cases, operational criteria, and the activities taken by each unit. When the node is idle, it waits for data packets to arrive from another node. Data transfer may waste 50% to 100% more energy if more power is required to run the CPU, radio, and other components. When the node is resting, substantially less energy is lost since no processing is undertaken and the communication unit is switched off. However, other energy dissipation problems exist, such as packet losses, packet collisions, physical channel challenges, frame overhearing, overhead protocols, and overhead processing. As a result, IoT researchers have been driven to develop energy-efficient and renewable IoT solutions [15]. **Figure 3** shows the typical IoT architecture for WSN.

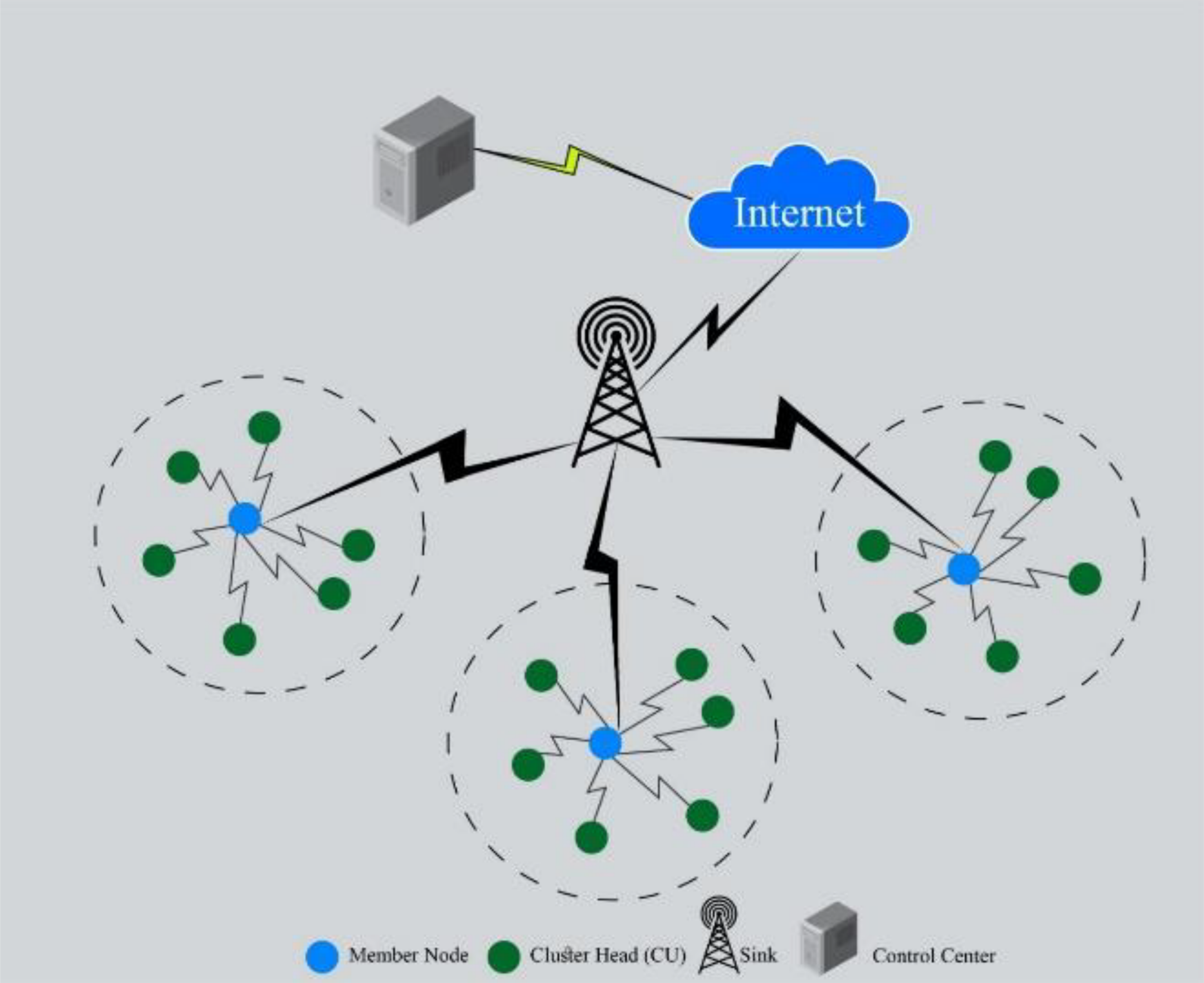

Figure 3. Typical IoT architecture for WSN.

Smart technology is becoming an increasingly important part of human life. WSNs are becoming more critical to the Internet of things every day. Consequently, the obstacles intensify, and the demand for reform becomes even more imperative. WSNs and the Internet of things may benefit from machine learning. A new operational framework for next-generation wireless sensor networks based on the IoT has been proposed. Using a three-layer transmission method, the nodes can communicate efficiently concerning energy.

4. Research Issues of WSN in IOT

The first difficulty for all uses of the WSNs is security. Protecting one's private and confidential information has become a top priority for modern consumers. Data regarding "personal health" and corporate operations, for example, should not be made public. To preserve their privacy and security, they must be transmitted above WSNs. Authentication and encryption are critical stages in safeguarding WSNs, but they alone are not adequate.

Despite recent developments in this sector, WSNs require substantial power from energy-restricted batteries to analyze and send data. Because of their limited size and computer capacity, wireless sensor nodes cannot perform to a great extent. WSNs have long been utilized in harsh, difficult-to-reach environments. Wireless sensor node resource limitations represent another issue for WSN-based systems.

Apps' potential to interact with sensors, other users, and the cloud is called "coverage and connectivity".

- Data aggregation methodologies;
- How to use sensors in a distributed environment;
- Clustering algorithms;
- Localization techniques;
- Rerouting protocols.

The differences between IoT devices raise the question of interoperability. The WSN or IoT environment must be able to interface with the many heterogeneous devices that generate various types of data. With the increasing variety of IoT applications and linked devices, a continued effort is needed to achieve this.

The reuse of IoT devices is necessary because of the rising need for essential information (such as heart rate, temperature, blood pressure, etc.) in different WSN or IoT applications. The ability to use gadgets in a variety of ways saves money. It is therefore always a goal to design a device for an application that can be reused in future applications. Things and sensor nodes already communicate regularly using current IoT and WSN systems. Battery life is quickly depleted by these exchanges, limiting non-stop operation to a few hours or days. As a result, improving processing and communication energy efficiency should be considered a significant open problem [16]. Many remedies have been presented in the literature to rectify this issue. To manage gathered data or events through different current solutions and services, the Internet of things (IoT) requires effective tactics. For IoT systems, the scalability criteria of WSNs cannot be met because of the higher number of IoT devices or other items linked to create an IoT system compared with conventional WSNs. Thus, the challenge of IoT scalability and flexibility must be addressed. An outstanding question rests in how flexible subscription and event monitoring systems may be provided while ensuring scalability for both objects and users.

5. The Architecture of WSN Nodes

Wireless sensor network is a broad term that consists of several nodes; the more significant the WSN, the bigger the number of nodes. Each node acts as an individual unit consisting of a sensing unit, a communication unit, a processing unit, and a storage unit; these units make up a particular node [17]. The sensing unit exists to detect events and gather required data, such as temperature, humidity, sounds, light, etc., or the specific data it uses. The communication unit allows the collected data to be transferred; it makes the sensor communicate with other nodes for sending and receiving data. The storage unit is used to save the assembled data in a specific format for later use [18][19]. **Figure 4** shows the architecture of an individual WSN node [20]. A WSN is made up of hundreds of thousands of sensor nodes. These nodes can communicate with one another using multi-hop communication. WSNs have a lot of potential as a platform for various uses, including data collection and event prediction.

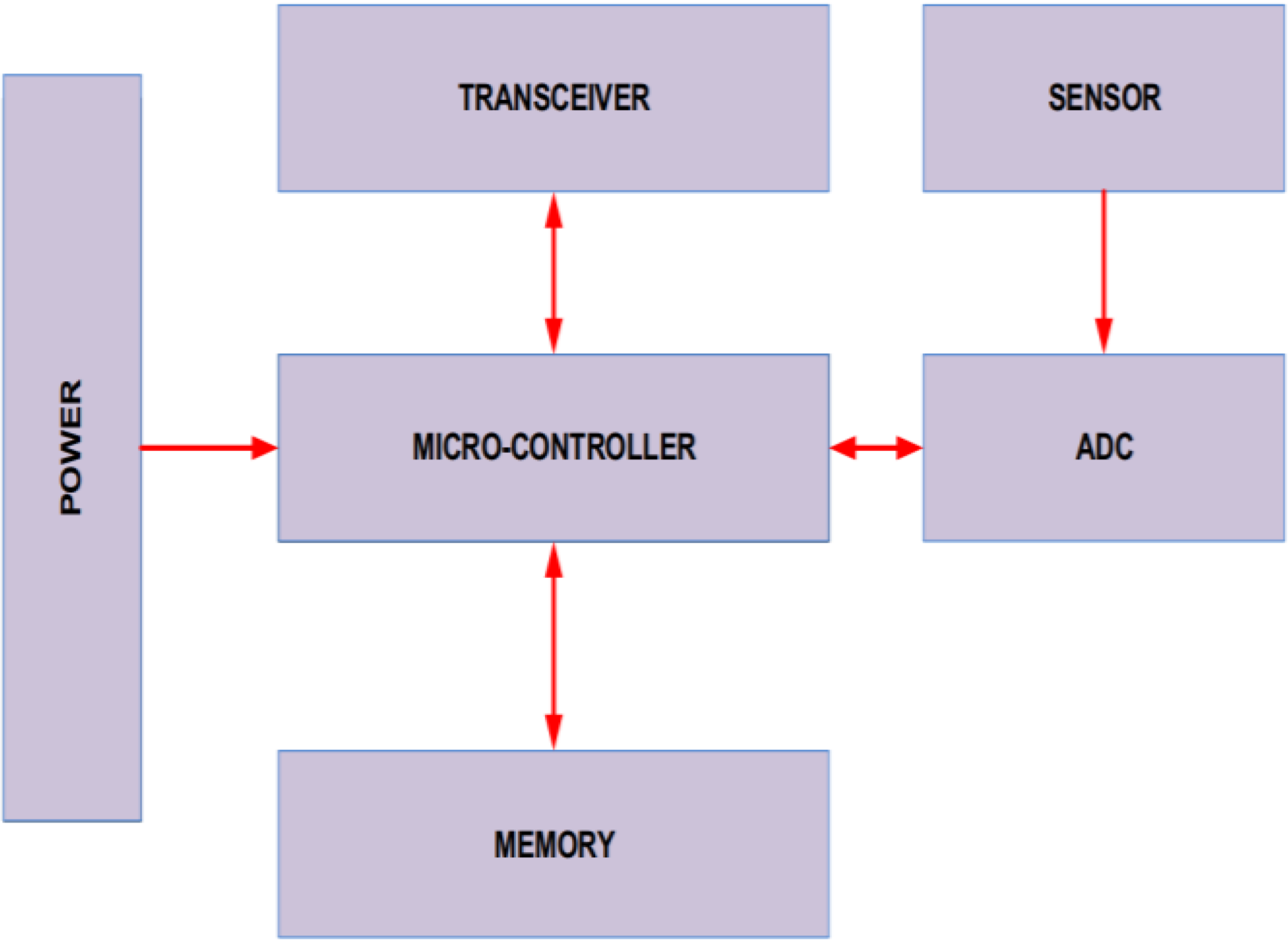

Figure 4. Architecture of an individual node [21].

6. IOT Architecture and Its Layers

- **Application Layer**

The application layer characterizes all the applications where it is implemented. It serves as the link or medium between user-end devices and the IoT network. There are numerous IoT applications, and the application layer can aid the applications. Because of administrations based on sensor data, the administrations may be unique for each application. It is implemented by a dedicated program at the device end. The software uses the application layer on a computer [22] and supports application-layer protocols such as HTTPS, HTTP, FTP, and SMTP. The application layer uses a variety of protocols, including the restricted application protocol (CoAP), message queue telemetry transport (MQTT), the advanced message queuing protocol (AMQP), and an extensible messaging and presence protocol (XMPP) [23].

- **Data Processing Layer**

The service layer comprises functionalities that manage gathered data and link it to the component layer's data. This layer serves as a conduit between different IoT devices and provides advanced techniques for communicating between them [24]. The sensors are also connected to the application layer through the service layer, which sits on top of the network layer. It has two responsibilities: First, it verifies that information is submitted by legitimate clients while preventing all dangers and threats. Second, it demonstrates that information is sent by legitimate clients while avoiding all risks and threats [25].

- **Network Layer**

The Internet of things necessitates adaptability in operating a vast range of computers. Over a billion smartphones will be added to the framework every year. As a result, IPv6 will play a critical role in preserving network layer flexibility. This layer comprises network interchange programming as well as actual segments. Its fundamental object is to send information among gadgets and devices to the recipients [26][27]. The data is transmitted via the network layer, whether wired or wirelessly, using existing advanced methods.

- **Sensing Layer**

The sensing layer comprises the essential equipment, the gadget layer, hubs, and sensors, such as RFID, standardized tag names, actuators, and insightful identification gadgets [28]. Gadgets assemble and pass data to the network layer either directly or by implication. To discern the nodes, sensors are used to transport the gathered information into the next layer. It is predicted that all devices will be IPv6-competent in a few years' time [29][30].

References

1. Wang, H.; Wen, Y.; Lu, Y.; Zhao, D.; Ji, C. Secure localization algorithms in wireless sensor networks: A review. In Advances in Computer Communication and Computational Sciences; Springer: Singapore, 2019; pp. 543–553.
2. Prakash, S.; Saroj, V. A review of wireless charging nodes in wireless sensor networks. In Data Science and Big Data Analytics; Springer: Singapore, 2019; pp. 177–188.
3. Libelium. 50 Sensor Applications for a Smarter World; Libelium: Zaragoza, Spain, 2020.
4. Bushra, R.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. J. Netw. Comput. Appl. 2016, 60, 192–219.

5. Hashem, I.A.T.; Chang, V.; Anuar, N.B.; Adewole, K.; Yaqoob, I.; Gani, A.; Ahmed, E.; Chiroma, H. The role of big data in smart city. Int. J. Inf. Manag. 2016, 36, 748–758.
6. Bennett, C.C. Artificial intelligence for diabetes case management: The intersection of physical and mental health. arXiv 2018, arXiv:1810.03044.
7. Schick, L.; de Souza, W.L.; do Prado, A.F. Wireless body sensor network for monitoring and evaluating physical activity. In Information Technology-New Generations; Springer: Cham, Switzerland, 2018; pp. 81–86.
8. Gravina, R.; Alinia, P.; Ghasemzadeh, H.; Fortino, G. Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges. Inf. Fusion 2017, 35, pp. 68–80.
9. Lueth, K.L. Top 10 IoT Applications in 2020; IoT Analytics: Hamburg, Germany, 2020.
10. Oliff, H.; Liu, Y. Towards industry 4.0 utilizing data-mining techniques: A case study on quality improvement. Procedia CIRP 2017, 63, 167–172.
11. Tramarin, F.; Mok, A.K.; Han, S. Real-time and reliable industrial control over wireless lans: Algorithms, protocols, and future directions. In Proceedings of the IEEE; IEEE: Piscataway, NJ, USA, 2019; Volume 107, pp. 1027–1052.
12. AlMheiri, S.M.; AlQamzi, H.S. Data link layer security protocols in wireless sensor networks: A survey. In Proceedings of the 2013 10th IEEE International Conference on Networking, Sensing, and Control (ICNSC), Evry, France, 10–12 April 2013; pp. 312–317.
13. Li, X.; Liu, Y. Efficient implementation of the data link layer at the receiver of JESD204B. In Proceedings of the 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS), Chongqing, China, 6–8 December 2019; pp. 918–922.
14. Dahlberg, A.; Skrzypczyk, M.; Coopmans, T.; Wubben, L.; Rozpędek, F.; Pompili, M.; Stolk, A.; Pawełczak, P.; Knegjens, R.; de Oliveira Filho, J.; et al. A link layer protocol for quantum networks. In Proceedings of the ACM Special Interest Group on Data Communication, Beijing, China, 19–23 August 2019; pp. 159–173.
15. Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in the Internet of Things (IoT). Mater. Today Proc. 2021, 51, 161–165.
16. Swessi, D.; Idoudi, H. A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures. Wirel. Pers. Commun. 2022, 124, 1557–1592.
17. Wang, Y.; Zhang, Y.; Liu, J.; Bhandari, R. Coverage, connectivity, and deployment in wireless sensor networks. In Recent Development in Wireless Sensor and Ad-Hoc Networks; Springer: New Delhi, India, 2015; pp. 25–44.

18. Tan, Q.; An, W.; Han, Y.; Liu, Y.; Ci, S.; Shao, F.-M.; Tang, H. Energy harvesting aware topology control with power adaptation in wireless sensor networks. Ad Hoc Netw. 2015, 27, 44–56.

19. Priyadarshi, R.; Gupta, B.; Anurag, A. Deployment techniques in wireless sensor networks: A survey, classification, challenges, and future research issues. J. Supercomput. 2020, 76, 7333–7373.

20. Sharma, V.; Patel, R.; Bhadauria, H.; Prasad, D. Deployment schemes in a wireless sensor network to achieve blanket coverage in large-scale open area: A review. Egypt. Inform. J. 2016, 17, 45–56.

21. Mounir, T.A.; Mohamed, P.S.; Cherif, B.; Amar, B. Positioning system for the emergency based on RSSI measurements for WSN. In Proceedings of the 2017 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), Paris, France, 28–30 November 2017; pp. 1–6.

22. Chen, L.; Erfani, S. A note on security management of the internet of things. In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 30 April–3 May 2017; pp. 1–4.

23. HIOTRON. Iot Architecture Layers|HIOTRON; HIOTRON: Pune, India, 2019.

24. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in the internet of things: Challenges, solutions, and future directions. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781.

25. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.-L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat Analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the 2016 International Symposium on Networks, Computers, and Communications (ISNCC), Yasmine Hammamet, Tunisia, 11–13 May 2016; pp. 1–6.

26. Pacheco, J.; Benitez, V.; Félix, L. Anomaly behavior analysis for IoT network nodes. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems, Paris, France, 1–2 July 2019; pp. 1–6.

27. Li, J.; Zhao, Z.; Li, R.; Zhang, H. Ai-based two-stage intrusion detection for software-defined iot networks. IEEE Internet Things J. 2018, 6, 2093–2102.

28. Subasi, A.; Al-Marwani, K.; Alghamdi, R.; Kwairanga, A.; Qaisar, S.M.; Al-Nory, M.; Rambo, K.A. Intrusion detection in smart grid using data mining techniques. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6.

29. Matheu, S.N.; Hernandez-Ramos, J.L.; Skarmeta, A.F. Toward a cybersecurity certification framework for the Internet of Things. IEEE Secur. Priv. 2019, 17, 66–76.

30. Elsadig, M.A.; Altigani, A.; Baraka, M. Security Issues and Challenges on Wireless Sensor Networks. Int. J. Adv. Trends Comput. Sci. Eng. 2019, 8, 1551–1559.

Retrieved from https://encyclopedia.pub/entry/history/show/91976