The Cellular Internet of Things (IoT): review

Hussain Alburki[1]* Mohammed A[2]

[a] *Alburki is with univiristy of atilim,ankarak, turky*

Abstract

Because of the dramatic expansion in the number of actuators, industrial devices, medical devices, and sensors, the Internet of Things (IoT), which enables objects to communicate with one another using information technology in a quick and adaptable manner, has been implemented. As a result, IoT communications have made it easier for things to be connected between applications, consumers, and connected devices in order to take additional advantage of the numerous services that are available via the Internet. LTE-M or NB-IoT are the two technologies that virtually all existing cellular Internet of Things applications utilize for connectivity. The important thing to note is that although there are significant, application-specific differences between the two types of cellular IoT, in general, you select either one depending as to whether LTE or GSM cellular connectivity is the standard in your area. The communication is different between LANs and WANs, where in WANs traditional cellular network most used such as GSM(2G), UMTS(3G), and LTE (4G). while radio technologies used in LANs such as ZigBee, Bluetooth, and Wi-Fi. The author of this paper has organized the content of the paper into several main sections. In the first of these, the author describes what cellular connectivity is and how it operates. Next, the author discusses the different types of IoT networks as well as the available alternatives. Finally, the author wraps up the paper by discussing cellular redundancy and IoT security.

1. Introduction

The purpose of this paper is to present the usage of cellular IoT that mostly relies on 2G, 3G, 4G, 5G and (LPWAN) technologies LTE-M and NB-IoT for transferring and collecting data. The usage of cellular and how the connectivity works will be illustrated as well as contemplating the different types of mobile network used

(1) *E-mail address:* Alburki.hthussain@student.atilim.edu.tr

by IoT, and the possible alternatives to cellular IoT. Moreover, why does redundancy play an important role for cellular IoT will be demonstrated in this paper, additionally, cellular IoT security will be covered.

Nomenclature	
IoT	Internet of Things.
LPWAN	Low Power Wide Area Networks.
RFID	Radio Frequency Identification.
NB-IoT	Narrowband IoT

1.1. What is Cellular IoT used for?

The Cellular Internet of Things (IoT) is essentially a newly designed connectivity system that links a variety of different devices (e.g. sensors) to the internet. Especially with the emergence of 5G networks, cellular IoT is starting to reach more significance and frequency of usage over time because it can be applied to a wide variety of fields. This is especially going to be the case over the next few years. Cellular networks carry our audio through the air, and also enables us to connect with the physical objects like electricity meters, healthcare facilities, boilers, streetlamps, and so on. Cellular networks can link smartphones to Google Maps, e-mail accounts, and more. It also has a wide range of applications in the industrial sector, including the manufacturing and agricultural industries, telematics and connected driving is an example. Telematics service based IoT provides a record of the data that is necessary to ensure the safety of drivers and their compliance. The measurement of driving data is the major responsibility of telematics service providers. This enables them to offer services such as the study of driver behavior, the integration of safety training, predictive analysis, and linked vehicle frameworks (Liberg et. Al, 2017).

1.2. How cellular IoT connectivity works

Cellular IoT connectivity which referred to as satellite connection. Connectivity with a range of 10-15 miles, such as the kind we use to connect our smartphones and tablets. Cellular connectivity is the number one WiFi alternative to be connected to the IoT devices. Cellular van be connected with a further range to anyone or anything globally unless you are out of range of the cellular tower.

Wi-Fi is not available everywhere and it cuts our most of time, while cellular is a reliable IoT connectivity and ubiquitous. Moreover, cellular is easy to use by everyone, and it does not require complicated connections or extra devices to connect it, since it can be connected just by SIM card.

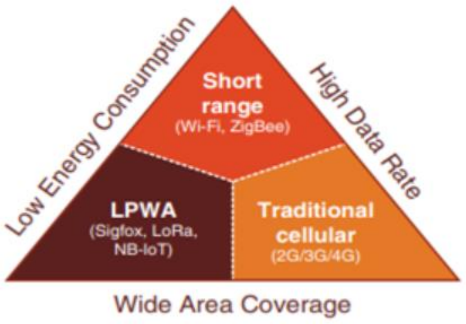

Figure 1: cellular IoT connectivity.

Substantially in Wide Area Coverage, a technology that has long coverage such as 3G, 4G cellular networks are appropriate. While in High Data Rate, huge bandwidth is used with adaptive modulation which is supported mostly by Wi-Fi and cellular networks. On the other hand, a low data rate that is supported by LPWAN consumes less power than the others. Short-range technologies like Wi-Fi, ZigBee, and traditional cellular networks offer high data rates, as shown in the Figure1.2, while in Wide Are Coverage LPWANs such as NB-IoT and traditional cellular networks used. As a result, LPWANs provide wide area coverage while consuming low energy (Aagaard, 2022).

1.3. The types of mobile network IoT uses

The term "IoT Network" refers to the communication technologies that are utilized by Internet of Things (IoT) devices. These technologies allow IoT devices to share or spread data to other devices or interfaces that are within reachable distance. IoT devices are able to communicate with one another via a wide variety of different types of IoT networks. It is of the utmost importance to select the appropriate networking protocol for the tasks at hand.

The wireless network is not a new concept in the world of technology; yet, it has been exposed to development and innovation from time to time in order to face rising issues with growing products and systems in the domain of communication. The following is a list of important types of wireless networks that can make the adoption of IoT in industries easier (Types of IoT Networks | Reference Guide, 2022).

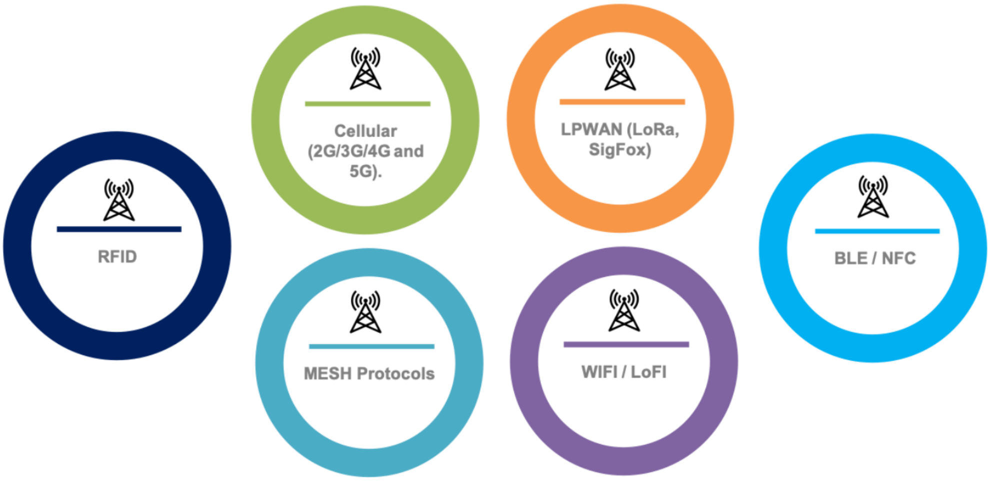

Figure 2: Types of mobiles network IoT uses. (Image reproduced from <https://www.fogwing.io/types-of-iot-networks/>)

From fig.1, The use of RFID scanning and communication, as well as Bluetooth (BLE/NFC) data transfer, are examples of how increasingly sophisticated standards are being adopted. Even while BLE and NFC are focused on the operation of mobile phones, there are other techniques commonly that can serve the goal of deploying IoT devices in a manner that is compliant with industry pre-requisites. IoT implementation is enabled by cellular network technologies (2G, 3G, 4G, and 5G), as well as WiFi and LoFi, which together provide effective local area communication between devices and online access.

MESH protocols, which are comprised of radio nodes grouped in a mesh topology, directly connect and terminals for the purpose of data transfer and communication. These protocols are an option for Internet of Things deployment and can be selected by customers according to their requirements. Low Power Wide Area Network (also known as LoRa or sigfox) is an innovative technology that will be used in the distant future. It is planned to make wireless communications over long distances possible while maintaining a low bit rate among the linked devices and systems.

1.4. Cellular IoT security

As it has been mentioned that (IoT) is used to connect everything with the internet providing the interaction with everyone which will increase the security issues. In OSI model, each layer may face an issue related to privacy and security (Jan et. Al, 2019).

- **Perception layer:** here the resemblance to the physical layer, it has several types of sensors and actuators (i.e.., QR code, RFID). The sensors, sense and process data related to the location, vibration, etc. The attacker usually finds the perception layer is the easiest to attack in IoT network, since the power consumptions capability of those sensors are low which makes them the favorite part to the attackers. Exploiting the confidentiality can be one of the most dangerous threat to IoT, where spoofing can be used here for that purpose which can rotate identity information of the IoT devices.

- **Network Layer:** here the collected data from the various (IoT) devices and sensors are transmitted in this layer. Moreover, several technologies such as (3G, Wi-Fi, Bluetooth, etc.) are used for the network devices here. Therefore, DoS attacks can be carried out here in this layer, network sniffing and passive monitoring also likely to happen here. To secure the communication between IoT devices through the network, network protection and object protection are equally important in order to the IoT devices to be fully secured, the objects must be capable of detecting and defending themselves against any network attack

- **Application layer:** This layer oversees the confidentiality, authenticity, and integrity of the data. Several applications available and each one has a different method of authentication, for that reason it is not possible to countermeasure the authenticity and privacy without any difficulties. In the development of the applications there must be (Access control) where users and roles of the applications are set which shows who will be able to access to which data and when the data can be used (Jan et. Al, 2019).

The chief major for the success of the IoT framework, to have a secure system and people who are aware of the security measures. Therefore, in order to make IoT environment useful and not harmful, the IoT environment should have policy for the those whom part of the IoT environment to practice more on security awareness and not using default security parameters which can be harmful.

1.5. Alternatives to cellular IoT

When evaluating the quality of an Internet of Things network, there are typically three aspects that we focus on:

• **Power consumption:** battery power is used by many Internets of Things devices rather than direct electrical connection. When selecting a network, bear that in mind, since you will not want something that requires an excessive amount of power if you want it to last for a long time.

• **Coverage range:** When selecting an Internet of Things network, you should give coverage range some thought if your devices are spread out over a big area.

• **Bandwidth**: There are some Internet of Things devices that can go through a lot of data. In order to meet your requirements, you will need to select a wireless IoT network that is able to both receive and process the necessary quantity of data.

There are a number of technologies that can replaces the cellular IoT such as:

a- LPWAN

Low Power Wide Area Network, also known as LPWAN (Misran et.al, 2019), is a relatively new competitor in the Internet of Things (IoT) network arena; yet, it brings a wealth in terms of range of coverage while still retaining low power consumption. LPWAN achieves this by powering its connectivity with relatively inexpensive and compact battery packs. Different forms of low-power wide-area network connections, or LPWANs, have been developed for various applications, including the following:

• LTE-M (designed for small power consumption)

• NB-IoT (Narrowband IoT)

• LoRa

A general overview Low-power wide-area networks (LPWANs) are useful for a variety of applications, but they are best suited for people who do not require a particularly high bandwidth. This is because LPWANs are only intended to work with very short data packets at a relatively low cost.

b- Zigbee

Zigbee is yet another well-liked option in contrast to cellular for Internet of Things networks and communication (Danbatta, et. al, 2019). It functions by utilizing a structure known as a mesh network, which involves linking a multiple sensors or devices to one another in such a way that they may distribute data to whatever device is selected. All of the Internet of Things devices that are part of the system have the capability, when connected to a mesh network, to send and receive signals and information throughout the network. Zigbee was developed specifically for the Internet of Things, and it is already supported by popular IoT devices such as Amazon Echo. It is capable of connecting up to 65,000 units in its mesh network.

c- Bluetooth

Since most of us have been using Bluetooth on our mobile phones for the past ten years, we are all well familiar with the technology behind it. Users are able to communicate data across small distances via wireless technology thanks to Bluetooth's capabilities (Li et. Al, 2018). In recent times, Bluetooth has seen significant improvements in terms of the amount of power it consumes. In the past, Bluetooth connections ran on a model that consumed a very high amount of power. However, modern Bluetooth connections use a model that consumes a relatively low amount of power. Although it had a comparable bandwidth of 2 Mbps, Bluetooth only had a low range capability of less than 30 feet (10m). In summary, the connectivity provided by Bluetooth IoT networks is an excellent choice to consider when seeking for a means to transmit data over a short distance and with a medium to low data transfer rate.

d- Z-Wave

Z-Wave, much like Zigbee, is driven by a link that is based on radio frequency (RF). However, in contrast to Zigbee, Z-Wave typically requires the use of a central hub in order to function properly. This requirement might result in connection disruptions, issues with lag, and a restricted range of operation.

In summary, when it comes to connecting your Internet of Things product, the majority of the time, the best experience can be had through the use of cellular IoT wireless networks and connectivity. Cellular technology provides not just extensive coverage but also the possibility of expansion. And all of this may be accomplished with a comparatively small financial investment.

1.6. Why redundancy is critical for cellular IoT

The concept of network redundancy refers to the utilization of backup network resources for the purpose of minimizing or preventing downtime in the event of a power failure, malfunction in the hardware, error on the part of a person, failure of the system, or a cyber-attack. This requires running multiple instances of fundamental network services and constructing additional network infrastructure (EMnify, 2022).

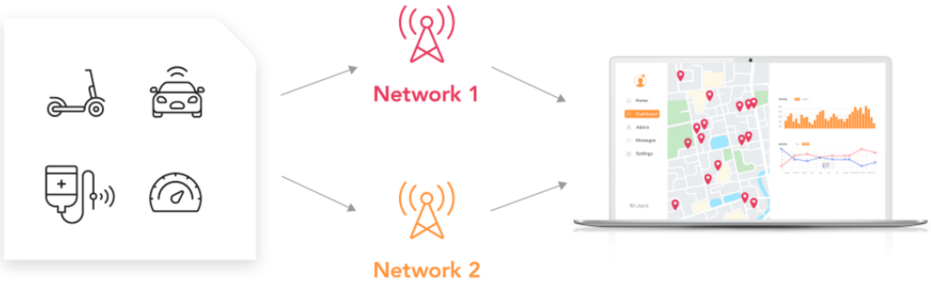

Figure 3: The concept of cellular IoT redundancy. Image reproduced from <https://www.emnify.com>

When discussing cellular networks, network redundancy refers to the capability of connecting to various Mobile Network Operators inside the same region. This redundancy, which makes use of the appropriate technologies, allows your networks to interact to the strongest signal regardless of where you deploy them.

The far more redundancy your net possesses, the lower the risk that your company and your services are exposed to in the event of a failure in the network. Because there are additional resources on standby, your network is not dependent on a single component or function in particular at any given time. Instead of pulling the entire system down with it if a single component fails, it is simply replaced when that happens.

A single hour of network disruption costs more than $300,000 for the majority of enterprise organizations. (According to the findings of a research that was conducted in 2016, even one minute of unscheduled downtime might cost as much as $17,000.) When your services are down for even one minute, you run the risk of losing thousands of dollars, hurting the reputation of your business, and irritating your clients. Because of the nature of business-to-business apps, disruptions on your end can have a negative impact not only on your own income but also on the revenue and reputation of your clients. Because of this, redundancy is one of the most critical aspects of the Internet of Things. You will be able to maximize service availability and limit the effect of problems that are caused by the network if you have a backup plan for each and every possible failure.

2. Conclusion

This paper describes the several usages of cellular IoT networks, and how the usage of it has been significantly increasing over time. Moreover, it has been pointed out that mostly cellular IoT connectivity provide better experience than its alternatives when it comes to connecting IoT to the internet. To ensure a backup plan in case of any disaster, redundancy is essential for cellular IoT. Lastly, as the usage of IoT increases, there might be plenty of security issues now and in the future. Security countermeasures should be followed to provide authenticity, confidentiality, and integrity of data transmitted over IoT networks

References

Liberg, O., Sundberg, M., Wang, E., Bergman, J. and Sachs, J., 2017. Cellular Internet of things: technologies, standards, and performance. Academic Press.

Fogwing.io. 2022. Types of IoT Networks | Reference Guide. [online] Available at: <https://www.fogwing.io/types-of-iot-networks/> [Accessed 22 May 2022].

Aagaard, H., 2022. How do cellular IoT networks work? – Onomondo. [online] Blog.onomondo.com. Available at: <https://blog.onomondo.com/cellular-iot-networks-explained> [Accessed 22 May 2022].

Misran, N., Islam, M.S., Beng, G.K., Amin, N. and Islam, M.T., 2019, July. IoT based health monitoring system with LoRa communication technology. In 2019 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 514-517). IEEE.

Li, Y., Chi, Z., Liu, X. and Zhu, T., 2018, November. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems (pp. 159-171).

Collotta, M., Pau, G., Talty, T. and Tonguz, O.K., 2018. Bluetooth 5: A concrete step forward toward the IoT. IEEE Communications Magazine, 56(7), pp.125-131.

Danbatta, S.J. and Varol, A., 2019, June. Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

Jan, M., Khan, F. and Alam, M., 2019. Recent Trends and Advances in Wireless and IoT-enabled Networks.

EMnify, 2022. What Is Network Redundancy? [online] Available at: <https://www.emnify.com/blog/network-redundancy#:~:text=%20Why%20network%20redundancy%20is%20critical%20for%20the,with%20NB-IoT%20networks%20or%205G%20networks%2C...%20More%20> [Accessed 22 May 2022].