DOI: 10.5958/0976-2469.2023.00002.7

LIBRARY HERALD
Vol 61 No 1
March 2023

Connectivity Technologies for Small Internet of Things (IoT) Devices and Challenges

Jitender Singh*
Gopal Singh**

The emergence of new technologies in the 21stcentury has redefined the way human beings have interacted in public and private spaces. Today, if we want to book a cab, we can easily book the same using our mobile phone within a few seconds if we exclude the human side of delay/error or if we are supposed to commute through other means of public transport such as the metro, we can use smart cards. In terms of performance do we notice any difference? The computing, processing, and operations are done within the blink of an eye. The time taken to complete such tasks is nearly the same but they use different underlying connectivity technologies and through these technologies, mobility and interactions are being redefined.Well, the convenient connectivity technologies for mobile devices with high battery and processing power in current trends of this era are cellular, simply put 3G, 4G, and 5G. However, small or microdevices that may only use sensors or may have limited power and processing cannot be categorized as other mobile devices like smartphones, laptops, PDAs, etc. In the past couple of decades, humans have become the minority as the generator and the receiver of traffic over the Internet. Much of the communication is done in a machine-to-machine manner and this communication has been reshaped by the Internet.If we are to define the Internet, simply put it is the network of computers. However, the Internet of Things on the other hand can be said as the network of "things" or devices or physical "objects", that may be connected over the Internet. At the same time, the scope of IoT is much broader than the Internet as it covers the dimension of connecting physical objects like fans, air

* Assistant Professor (Guest), Department of Computer Science, University of Delhi, Delhi; E-Mail: jitender100t@gmail.com

** Assistant Professor, Department of Computer Science and Applications, MDU, Rohtak, Haryana; E-Mail: gsbhoria@gmail.com

conditioners, lighting systems, surveillance cameras, etc. What has IoT to offer and why IoT is so popular in this era? The IoT offers an advanced level of services where we can connect embedded systems, computing platforms, nanotechnology, etc., all working as independent nodes. Unlike Computers, small sensor-based devices or "things" require a connectivity technology that consumes low power and energy and transmits limited data. Some examples are ZigBee, NFC, Bluetooth, 6LoWPAN, BLE, etc. This is what makes them different from smartphones which consume comparatively higher power and processing. No doubt, due to the increase in the number of connected devices the shortage of addressing also becoming a problem as currently, we use IPv4 and IPv6 addressing for the Internet Protocol and since the active devices are already over 10 billion in count we will soon or later run out of addresses. One example is how the current IPv4 infrastructure is used to transmit IPv6 data, as the internet backbone follows IPv4 addressing so one has to translate the IPv6 address into an IPv4 one. Likewise, discussion about the current solution to this problem and what are the limitations of current addressing methods and future scope.

Keywords: *Internet of Things, Internet, Connectivity technology, IP Addresses.*

1 INTRODUCTION

The emergence of new technologies in 21st century have redefined the way human beings have interacted in public and private spaces. In this digital era, dependence on technology is ever-increasing when it has to offer a lot of convenience over traditional workflow. How much an individual may depend on technology when it comes to finishing a basic task may vary from partial to complete. It is easier to order food from an app rather than cooking a meal on your own which requires some set of life skills and ingredients, it may cost money and health while ordering online but at the same time convenience is there. From selecting a food item to doorstep delivery, everything can be done with technology, one may be completely dependent on technology. However, this process can also partially depend, suppose you choose to pay via cash. Be it an organization, governance, or an individual person, the dependency on technology is only increasing over the years.

To get our basic work done, we have to rely on technology, and if we are more specific, we are relying on the network of computing devices that we usually call the Internet.

11 INTERNET OF THINGS (IOT)

The Internet is generally defined as a network of connected computers and computing devices, in a global manner. But when we talk about the Internet of Things, the scope is beyond just computers and computing devices and includes devices and physical objects like lights, fans, cooling systems, etc. With the help of IoT, we are already moving fast towards smart homes, smart cities, etc. The first IoT device was developed by a group of graduate students of Computer Science at Carnegie Mellon University in 1982. Where a coke vending machine is connected to the ARPANET, which at that time was connected to less than 300 computers. The vending machine was able to report inventory and whether drinks were cold or hot. Which made it the first connected appliance in the history of the Internet of Things.(Teicher, J., 2018)

An alternate definition by Gartner research says "*The **Internet of Things (IoT)** is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.*" (Gartner," n.d.) The reason IoT is popular that is offers an advanced level of service. One can connect watches, embedded systems, computing platforms, etc. all working as an individual node of this network.

As per the Statista report, the number of active devices in 2019 was 8.6 billion, and this number is likely to triple by 2030. (Sujay,2022) With the evolving connections of small devices, it has been found that though the users on the internet are billions of humans may become a minority as the generator and receiver of the traffic, and most of the traffic data flow among the devices and different kinds of "things" (Spumail, n.d.). It underlines the challenges of regulations connections of small devices and brings into picture cyberspace.

12 CYBERSPACE

The word "Cyberspace" is derived from the Greek word "Cybernetics" which means controlling and regulating the mechanism of a machine, a human, or a computer. It was first used by the Science fiction American-Canadian writer William Gibson in a short story in 1982, later in 1984, he published a novel named Neuromancer where he officially used the word Cyberspace which is a combination of "Cybernetics" and "Space" as 'consensual hallucination' of data. *(Neuromancer,* 1984). As the technology evolved, over the years US Department of Defense aka Pentagon has released more than 12 definitions of Cyberspace including- a "*notional environment in which digitized information is communicated over computer networks.*"(Singer & Friedman, 2014) But the same got rejected as it focused on communication and was largely imaginary. The other definition said "*domain characterized by the use of electronics and electronic spectrum.*" (Singer & Friedman, 2014) This again got rejected as it encompassed computers.

In 2008, Pentagon assembled a team for the specific purpose to define Cyberspace and it took over a year for the team to define the term Cyberspace:

> "*A global domain within the information environment consisting of the interdependentnetwork of information technology infrastructures,*

> *including the Internet,telecommunications networks, computer systems, and embedded processors and controllers*." (Singer & Friedman, 2014)

The chief of Air Force's new Cyberspace command, Major General William T. Lord added "*we define the domain as the entire electromagnetic spectrum*."(Nast, 2008). It emphasizes changing role of the internet in cyberspace.

13 INTERNET

Over the computer network, the first word transmitted was "*Lo*". But wait before you guess the meaning of "*Lo*". In 1969, the researchers at UCLA were trying to connect and log into the Stanford Research Institute's computer but before the complete message could be transmitted the Sandford Research Institute's side computer network got crashed and they were not able to add "*g*". (Singer & Friedman, 2014)

ARPANET was introduced by the US Department of Defense in 1969 under the Advanced Research Projects Agency (ARPA) for reliable and efficient communication among computers and was the first wide area network based on TCP/IP suite. By that time most of the communications were circuit-switched including the old Electrical Telegraph introduced in 1838 by Samuel Morse. What makes the ARPANET so special is it was the first packet-switched network, which simply means that even if the current link breaks in the middle of the communication the data can be transmitted without any information loss which was a limitation of circuit-switched networks. Later, ARPA was renamed DARPA adding 'Defense' to the Advanced Research Projects Agency (DARPA). The ARPANET is now joined by more universities and research centres around the world to share information and computational resources or alternatively designed their own networks.

14 IOT TECHNOLOGIES

There are numerous technologies that can be labelled as enablers of IoT. Out of them, the major enabling technology for IoT is RFID and Sensors. Through the word, "enablers" one can guess what is the use of these technologies. Further discussions will clarify the details.

RFID stands for "Radio-Frequency Identification" and is a chip-based system that communicates over radio frequency and is used for identification purposes like identifying objects, people or animals. Originally the technology was used for military purposes, Identify Friend or Foe (Foe) was used to identify and distinguish the friendly planes and friendly ships from the planes and ships of enemies during the second world war.(Franklin et.al 2009)

Over the years the technology has become common as one can easily buy an RFID tag and program it via a smartphone for day-to-day use.

Sensors as human beings we collect pieces of information about our surroundings based on our senses namely eyes, nose, skin, ears, and tongue. Once the information is collected it will be sent to the brain for processing and accordingly, action shall be taken. In the case of objects and robots, in order to make them intelligent we put sensors, the sensors collect information from the real world and pass it to the computation units for further processing. The sensors are transducers that collect the measurements of the physical variables from the surrounding.

The fundamentals of sensors are derived from humans, just like senses. Like a human body we can say if we have some internal pain, we can feel that while if we need to collect visible information, we collect that through our eyes. Same way, Sensors are major of two types Internal and External.

Internal sensors are used internally and used to operate the drive units while external sensors are simply used to collect information from the external environment. Some examples of Internal sensors are Position sensors, Velocity sensors, acceleration sensors, etc. while some examples of external sensors are Proximity sensors, Temperature sensors, Visual sensors, etc.

15 IOT APPLICATIONS IN THE MODERN DAY

Business, Healthcare, Retail, and Security hold the most market share when it comes to IoT. Some of the modern applications of IoT include:

- Smart Cities
- Smart Parking
- Robots
- Smartwatches
- Portable Health Monitoring Devices
- Inventory Tracking and Management
- Smart Home/Home Automation
- Surveillance Systems
- Authentication Systems
- Real-Time Analytics of Supply Chains
- Smart Vehicle
- Air Pollution Monitoring
- Intelligent Shopping
- Earthquake Early Detection, etc.

The applications of IoT have radically changed the life of human beings, particularly in urban areas where new challenges of urbanization require technology-based solutions. Delhi has already seen the installation of anti-pollution machines to minimize pollution in the winter seasons particularly. Further, the role of smartwatches has increased in the post-covid period where the unpredictability of health has already killed the human resource of India. The death of Indian comedian Raju Srivastava in Gym or TV personality Sardana shows that the human body is witnessing continuous changes and smartwatches can facilitate hourly based update body and accordingly appropriate solutions may be applied.

2 CONNECTIVITY TECHNOLOGIES IN IOT

It is a fact that depending on multiple factors like the transmission range, data rate, and power consumption the connectivity/communication technology and protocol may change for different applications. Currently, there are numerous connectivity technologies that are running in IoT devices for communication and handshaking techniques. The most widely used technologies are tried to cover in brief detail below.

21 BLUETOOTH CLASSIC

IEEE 802.15.1 standard Bluetooth was introduced in 1998 as an industrial standard by the Special Interest Group (SIG) Which was jointly formed by Ericsson, IBM, Nokia, Intel and Toshiba and was based on the Ericsson-developed mobile communication architecture.

Bluetooth is a wireless communication technology that offers a limited range for communication to low-powered devices like smartphones, PDAs, and embedded computational systems.The Bluetooth is named after the 10th Danish King, Harald Bluetooth Gormsson who ruled Denmark and Norway from c. 958 – c.986. The king was known to have united Denmark and Norway in 958 and also had a dead tooth having dark blue/grey colour and the same earned him the nickname Bluetooth. (“Origin of the name,” n.d.)

The Bluetooth technology is based on piconets. **Piconets** are ad hoc wireless networks that work in a self-organized and self-configured manner.The formation of piconets is dynamic, new devices may join or leave on their own. Piconets may allow up to 8 active devices that may use exactly the same channel simultaneously.The devices in the piconets can communicate with one another directly, called peers. One of the nodes acts as a master for synchronisation purposes and the rest of the nodes would be called slave nodes.(Wang & Kissel, 2015)

A Bluetooth device can be in both park state and standby, the standby devices may take longer to be active as compared to the parked state, which can quickly become active. In a piconet, there can be up to 255 parked devices.When a Bluetooth device wants to create a piconet it sends out a special packet and becomes a master node if any Bluetooth device wants to join the piconet in this range sends a request-to-join packet to the master node and upon joining the piconet becomes a Slave node. Multiple piconets may overlap with one another to form a scatternet but a Bluetooth device can only be a part of one piconet at a time.

22 BLUETOOTH LOW ENERGY (BLE)

The original Bluetooth is called Bluetooth Classic. The BLE is not an upgrade to the Bluetooth classic but a different and new technology that offers transmission of lower data speeds for smaller amounts of data. The latest Bluetooth 5.2 is an example of BLE that was released in January 2020.The BLE focuses on the applications for IoT objects and devices. In terms of specifications, the difference between Bluetooth Classic and BLE is huge really was introduced in 2010.

Some of the applications of Bluetooth classic can be seen as audio streaming and file transfer while the applications for BLE specifically include sensor data control of devices, etc. Bluetooth Low Energy is therefore optimized for low power and low data rate.

The advantage of BLE is the lower cost of chips and modules even compared with similar types of technologies. While we BLE for its advantages and application it does have its own limitations like short-range, data throughput, and an internet gateway shall be required for internet connectivity. The BLE operates over 40 Radio Frequency channels while the Classic operates over 79 Radio Frequency channels.

23 ZIGBEE

Based on IEEE 802.15.4 the ZigBee communication is a product of the ZigBee alliance and is specifically introduced for IEEE 802.15.4 standard-based control and sensor networks for Wireless Personal Area Networks (WPANs).In 1990 the self-organising digital radio ad hoc networks have developed a part of ZigBee specification IEEE 802.15.4-2003 was approved in 2004. Further, in 2005 specification 1.0 was announced by ZigBee Alliance.(Agarwal, 2022)

ZigBee offers low data rates and medium-range communication between IoT objects or devices by defining changes in Media Access Control (MAC) and Physical layer (PHY). For ZigBee networking topologies may include peer-to-peer, star, mesh, and cluster-tree (hybrid).

ZigBee operates at three frequencies:

Frequency Band	**Channel(s)**	**Rate of communication**
868 MHz	1	<20 kbps
902 – 928 MHz	10	<40 kbps
2.4 GHz	16	<250 kbps

The transmission nature is the Line of Sight (LOS) and can be transmitted up to 70 m. Usually, the packet size is 128 bytes for data transmission. For the 2.4 GHz band Offset Quadrature Phase Shift Keying (OQPSK) is used while for other lower frequency bands Binary Phase Shift Keying (BPSK) modulation scheme is used.

24 6LOWPAN

6LoWPAN stands for IPv6 over Low-Power Wireless Personal Area Networks. 6LoWPAN made connecting low-powered and IP-driven nodes to the cloud possible. It is an open standard defined by Internet Engineering Task Force (IETF), a network technology that enables IPv6 packets to be transmitted efficiently in small frames as defined by IEEE 802.15.4 standard. The 6LoWPAN works at two frequencies, the 902-929 MHz (North America) and 2400-2083.5 MHz (Worldwide). (CIC IPN - Inicio, n.d.)

The Maximum Transmission Unit (MTU) of IPv6 is 1280 bytes in length while on the other hand, the packet size can be 127 bytes in IEEE 802.15.4, that's why an additional adaptation Link Layer is placed between the network and MAC layer that provides multiple functionalities including header compression, packet fragmentation, and reassembly of packets. The fragmentation is mandatory as the IPv6 packet is supposed to fit into a different frame of about 106 bytes. In every fragmentation, a header is included.

25 NFC

NFC stands for Near Field Communication. NFC is designed for the devices to communicate within proximity to each other. NFC devices are of two types active and passive devices the passive devices contain information but are unable to read even their own information. The active NFC device can transmit and collect information as well. An example of passive NFC devices is the NFC tags we see in supermarket products while active NFC devices, the smartphones are a good example.

The NFC mechanism is based on the principle of magnetic induction. The NFC reader creates a magnetic field by emitting a small electric current and this magnetic field works as a bridge between the devices.The frequency of transmission in NFC is 13.56 MHz and the NFC tags generally store data between 96 to 512 bytes. The communication range is up to 20 cm and the data can be transmitted at rates of either 106, 212, or 424 kilobits per second.(Egan, 2015)

The NFC has three different modes of operation namely peer-to-peer, read/write, and card emulation. Peer-to-peer enables a pair of smartphones (active devices) to swap their data. Read/Write mode of operation is the most widely used application where the active NFC device picks up the information from a passive device. In card emulation, the functioning NFC can be used as a contactless credit card to enable payments electronic.

3 CHALLENGES IN IOT

The advantages of the IoT in general have already been reached to a regular household. Like any other innovation and technology, the IoT brings numerous challenges. Some of the challenges are discussed in this section.

31 ADDRESSING ISSUE

With the growing number of connected devices and the integration of the Internet with IoTs, Machine-to-machine interactions are increasing exponentially as every day millions of new objects/devices/things are adding up. The current communication technology used TCP/IP protocol for data transmission. Therefore, in the current scenario, the major addressing modes are used is either IPv4 or IPv6. Now, if we look closely at the architecture of these IP addresses then we may observe that IPv4 used 32 bits of address which means 2^{32}= 4294967296 (around 4 billion) addresses can be made possible at a specific time for IPv4. For IPv6, it uses the IP address of 64 bits which means 2^{64}= 18,446,744,073,709,551,616 (around 18.5 quintillion).

The current internet architecture is majorly based on IPv4 IP addressing. The backbone network that is connecting different nations and cities is following IPv4 addressing. Since in this article we already have discussed the number of active devices, alone IPv4 cannot fulfil all the needs. Hence, modern IoT devices are using IPv6 addressing. Now, in order to communicate the IPv6 IP addresses with IPv4 addresses, certain solutions are used. Two of them are IPv6 to IPv4 address translation and Tunnelling. In the IPv6 to IPv4 address translation, handshaking, and translation of IPv6 addresses are done. Another one is IPv6 tunnelling over IPv4, in this technique we use the current IPv4 routing infrastructure to carry the traffic of IPv6.

In a nutshell, currently, two different addressing modes are used and their interconnection is not optimised. In the future, we may expect a uniform addressing mode that works efficiently and takes care of future scope.

32 SECURITY AND PRIVACY

The IoT has its weaknesses when it comes to security and privacy. The foundation of IoT is based upon the already existing Wireless Sensor Network (WSN) and hence architecturally acquire the security and privacy issues that are possessed by WSN. Multiple attacks on IoT devices over same weakness urges researchers to explore this area.

Further, the principals of CIA triad and cryptographic algorithms can be applied to make the IoT devices and networks more secure.

33 INTEGRATION OF DIFFERENT IOT CONNECTIVITY TECHNOLOGIES

Another challenge in terms of IoT connectivity technologies, there are different technologies that may be used in order to transmit data for physical objects. Some of the discussed ones are Bluetooth Classic, BLE, ZigBee, 6LoWPAN, NFC, etc. All these technologies have isolated standards. If we want a better-optimised interconnection we need a uniform handshaking mechanism for all these isolating standards.

Table 2: Specifications of IoT Connectivity Technologies

	BLE	Bluetooth Classic	ZigBee	NFC	6LoWPAN
Security/Encryption	128-bit AES	58/128 bit, SAFER+	128-bit symmetric encryption	-	128-bit AES
Frequency Band(s)	2.4 GHz	2.4 GHz	868 MHz, 902-928 MHz, 2.4 Ghz	13.56 MHz	902-929 MHz, 2.4GHz
Maximum Speed of Transmission	2Mbit/s	3Mbit/s	250 kbits/s	424 kbits/sec	200 kbits/s
Maximum Range	<100 m	100 m	<100 m	<20 cm	<200 m
Power Required	1W	0.01-0.05W	10-100mW	~5mW [15]	-
Peak Current Consumption	<15mA	<30mA	~6.60mW [14]	<15mA	<35mA

4 CONCLUSION

It may be argued that the functioning of human beings as an individual as well as part of groups has been reshaped by the emergence of IoT connectivity technologies. No doubt, these technologies have encroached on the spaces of human interdependence, and societies across the world have witnessed its repercussions in terms of changingnature and context of relationships. At the same time, these technologies have also expanded horizons for better improving spaces of human life and ensuring the best possible mobilityand interaction of human beings. The state and non-state actors must intervene to address the emerging challenges in the domain of these technologies and their applications may be used to address challenges faced in the process of development in any country such as unpredictable challenges of earthquake or terrorism etc. and a better may be created through IoT.

REFERENCES

1. 6LoWPAN demystified (n.d.). CIC IPN Inicio. https://www.cic.ipn.mx/~pescamilla/IoT/papers / 6LoWPAN%20demystified_ti_swry013.pdf
2. AGARWAL (T) (2022, March 20). *ZigBee technology: Architecture, working and its applications*. ElProCus - Electronic Projects for Engineering Students. https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/
3. AT03663: Power Consumption of ZigBee End Device (2022). Retrieved fromhttps://ww1.microchip.com/downloads/en/AppNotes/Atmel-

42321-Power-Consumption-of-ZigBee-End-Device_ApplicationNote_AT03663.pdf?ICID=I-CT-TECH-RES-CLA-SEP_21-0

4. CLOUGH (J) *Principles of Cybercrime*. Cambridge, UK: Cambridge University Press, 2014.
5. DEHOUSSE (F)and TANIA (Z). "What Is RFID?" *RFID: New "Killer Application" in the ICT World, New Big Brother, or Both?* Egmont Institute, 2009
6. Egan (M) (2015, May 12). *How to use NFC on your smartphone to do useful things*. Tech Advisor. https://www.techadvisor.com/article/726110/what-is-nfc-uses-of-nfc-how-to-use-nfc-on-your-smartphone.html
7. GIBSON (WILLIAM). *Neuromancer*. New York: Penguin Group, 1984.
8. *Information technology (IT) glossary - Essential information technology (IT) terms & definitions | Gartner*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary
9. *IoT-connected devices worldwide 2019-2030*. (2022, May 30). Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide
10. *ORIGIN OF THE NAME*.(n.d.). Bluetooth® Technology Website. https://www.bluetooth.com/about-us/bluetooth-origin/
11. SHACHTMAN (N) (2008). 26 Years After Gibson, Pentagon Defines 'Cyberspace'. *wired. com, 23*.
12. SINGER (P W), and ALLAN (Friedman). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014. [p. 13, p. 16-17].
13. SPUMAIL(n.d.). *ITU internet reports 2005: The Internet of things*. https://www.itu.int/osg/spu/publications/internetofthings/
14. TEICHER (J) (2018). The little-known story of the first IoT device. *IBM Industries Blog, 7*.
15. WANG (J) and KISSEL (Z A) (2015). Introduction to network security. https://doi.org/10.1002/9781119113102
16. ZHAO (Y), SMITH (JR) and SAMPLE (A) (2015).NFC-WISP: A sensing and computationally enhanced near-field RFID platform. In *2015 IEEE International Conference on RFID (RFID)* (pp. 174-181). IEEE.