

Reasons Why Narrowband IoT Offers Great Telecom Prospect

Due to an increase in connectivity demand, Narrowband IoT holds great potential for the upcoming market. IoT is therefore gradually shifting from wireless to narrowband

Dharmendra Kumar

The Internet of Things (IoT) collectively refers to an ecosystem of connected physical objects that are accessible through the Internet. Consisting of steps such as Collect, Communicate, Analyse, and Act, IoT interconnects three platforms: things, people, and cloud. In IoT, connectivity plays a major role. But since there are no defined rules for connectivity, we have to consider which kind of connectivity should be used: wired or wireless. Although wireless is convenient, it has a complex connectivity topology and protocols.

The four layers of IoT are:

1. **Integrated applications.** Any social media or GUI based app.
2. **Information processing.** Related to data gathering and interfacing with the integrated applications.
3. **Network infrastructure.** Related to how the network is going to be deployed for the end-user and what topology is exactly

available. For the network topology of wireless communication, we have Wide Area Range, Low Power Wide Area Network, and Local Area Network.

4. Sensing and identification. Comprises sensors, which interface with networks for data communication.

The IoT reference diagram in Fig. 1 tells us how data will travel from the physical device to the last mile. As per the interface with the last mile and data requirement, relevant connectivity is required. Connectivity decides how much data is to be sent to the end-user and what kind of data packet is required for sending on the edge.

Some available IoT connectivity options are:

- Satellite communication
- Unlicensed band
- LTE - GSM band
- Narrowband IoT
- LoRa

- Local connectivity
- Wide area connectivity
- Low power wide area network (LPWAN)

Technologies such as LoRa, NBIoT, and Sigfox come under LPWAN. They have different use cases.

IoT connectivity demand

IoT connectivity is related to the kind of connectivity available on the device side as well as on the server side. Such connectivity types are:

Multi-sensor fusion. Het-

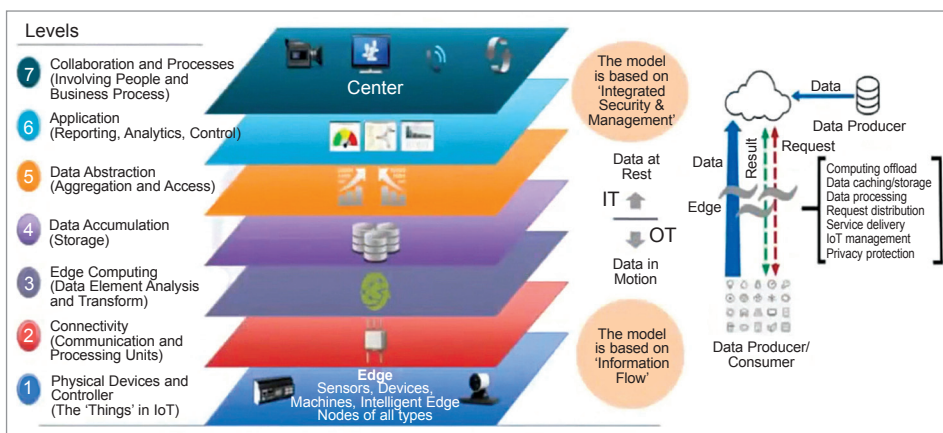


Fig. 1: IoT reference model

erogenous, multifaceted, and distributed sensors talk to each other to create a sensor mesh for solving complicated problems.

Sensor to cloud (S2C) integration. Cyber physical systems (CPS) emerge at the intersection of physical and virtual/cyber worlds.

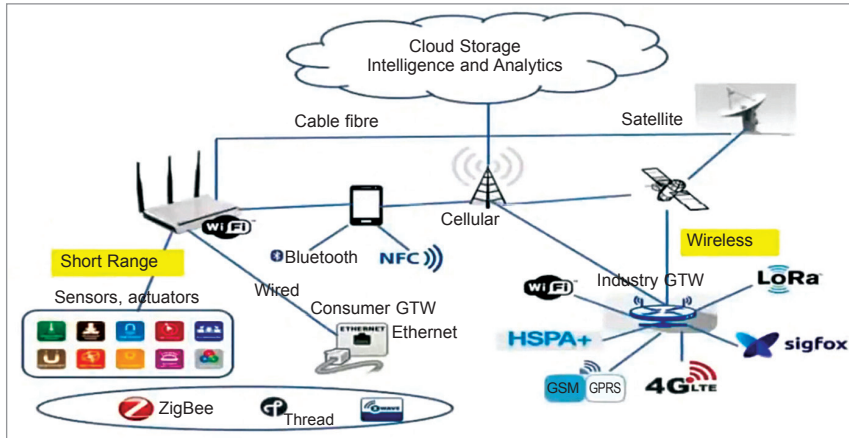


Fig. 2: Network architecture

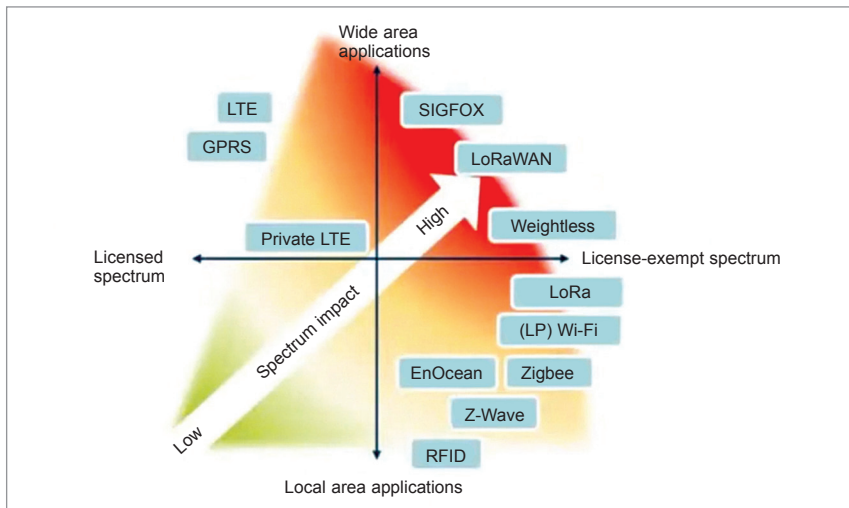


Fig. 3: Wireless network comparisons

Carrier frequency	Technology	Channel bandwidth	Representative data rate	Link budget target or max. range
Licensed cellular	LTE Cat. 0	20MHz	DL: 1Mb/s UL: 1Mb/s	140dB
	LTE Cat. M	1.4MHz	DL: 1Mb/s UL: 1Mb/s	155dB
	NB-IoT	200kHz	DL: 128kb/s UL: 64kb/s	164dB
	EC-GSM	200kHz	DL: 74kb/s UL: 74kb/s	164dB
Unlicensed	2.4GHz	Ingenu RPMA	UL: 624kb/s DL: 156kb/s	500km line of sight
	Sub-1 GHz	LoRa chirp spread spectrum	UL: 100kb/s DL: 100kb/s	15km rural 5km urban
	Sub-1 GHz	Weightless-N	UL: 100b/s	3km urban
	Sub-1 GHz	Sigfox	UL: 100b/s	50km rural 10km urban

Fig. 4: IoT Long Range technical solutions

Device to device (D2D) integration.

Device to enterprise (D2E) integration. In order to have remote and real-time monitoring, management, repair, and maintenance, and for enabling decision-support and expert systems, ground-level heterogeneous devices have to be synchronised with control-level enterprise packages such as ERP, SCM, CRM, and KM.

Device to cloud (D2C) integration.

Cloud to cloud (C2C) integration.

Mobile edge computing (MEC), cloudlets, and edge cloud formation through the clustering of heterogeneous edge/fog devices.

When we talk about IoT, we generally refer to connectivity among millions and billions of devices. However, it is difficult to interface them all.

As can be seen, networks such as short-range, wireless, cellular, satellite, and fibre optics are available. For IoT, we have to see how feasible the connectivity is for end devices. Generally, it has to be low-power and low-data type to connect to multilayer devices. GSM seems to fit into this requirement.

Network connectivity issues

- Sensors cannot be easily connected to the power source.
- Sensors deployed in secure or hostile operating conditions are difficult to change without impacting the system.
- Sensors have very different life-time expectancy rate.

- Resource-constrained endpoints.
- High sensitivity on reception.

Some possible options available to us are:

1. Direct connectivity

- Easiest to install and configure.
- Combines machine logic with IoT logic.

However, it is complex, not possible for legacy systems, and is less secure.

2. Cloud gateways

- Devices come with embedded connectivity to a proprietary cloud.
- Forwarding capabilities available to IoT platforms.

3. Field gateways

- Easy to start in the cloud.
- Enables legacy systems.
- More secure.

It requires extra hardware, machine logic is separated from IoT logic, and

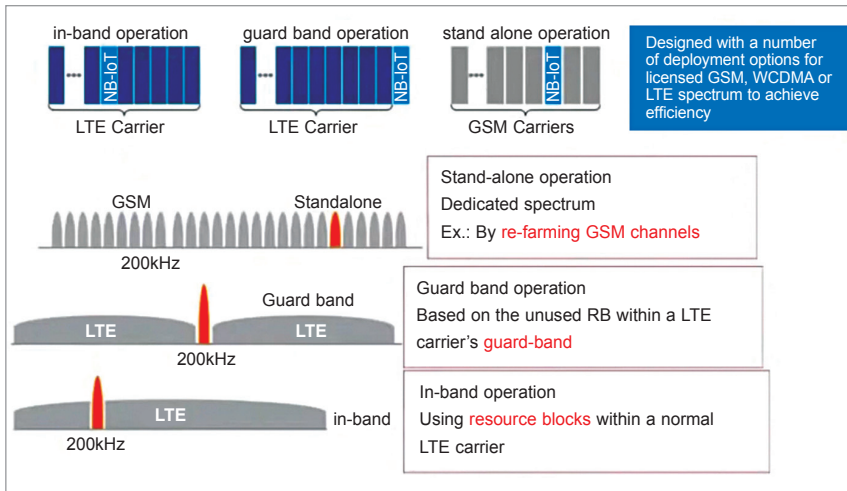


Fig. 5: NB-IoT spectrum and access

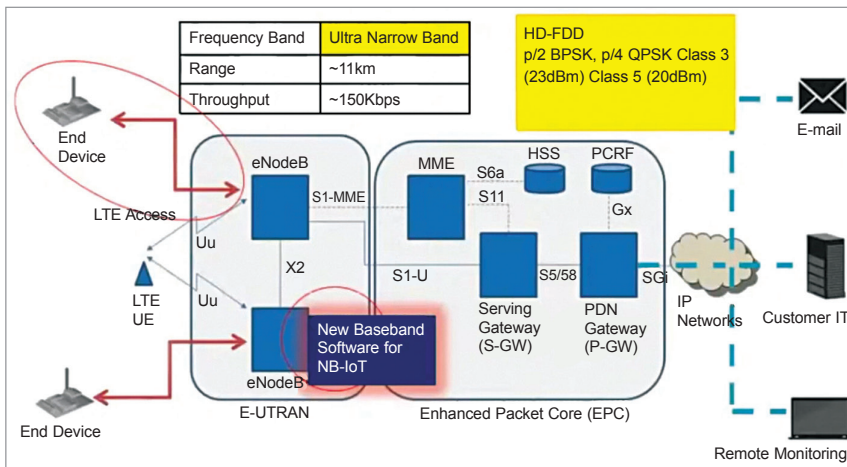


Fig. 6: NB-IoT architecture

3GPP Release	12 (Cat.0) LTE-M	13 (Cat.1.4MHz) LTE-M	13(Cat. 200KHz) NB-IoT
Downlink peak rate	1Mbps	1Mbps	300bps to 200kbps
Uplink peak rate	1Mbps	1Mbps	144kbps
Number of antennas	1	1	1
Duplex mode	Half	Half	Half
UE receive bandwidth	20MHz	1.4MHz	200kHz
UE transmit power (dBm)	23	20	23

Fig. 7: NB-IoT and LTM comparison

complexity of IoT is in one single place here.

Why prioritise wireless?

The key considerations for preferring wireless are:

- Radio range
- Power consumption
- Interference
- Data rate
- Antenna size
- Standard versus proprietary

So, the wireless module is interfaced via SPI or I2C with the microcontroller, which in turn will decide the kind of data to be transmitted.

If we go for the licensed spectrum, then it means to go for a wide area range network. On the connectivity side, there is no requirement for gateways. That is why people prefer GSM protocols and network. But the GSM network is designed for voice communications. In fact, all mobile

network operators (MNOs) do not want to support GSM network from an IoT point of view because once IoT devices increase in number, GSM network and voice communications will get interrupted and suffer. Also, the GSM network is very power-hungry. For IoT, we cannot select any such mode. Therefore, NB-IoT is needed.

We can go with the unlicensed band also. But for unlicensed bands, the priority of the data and data interface (methodology of interface) is different. From a security point of view, the unlicensed band needs to have more securities. We need to take care of the hardware and network side. The GSM network topology, however, has already taken care of security.

The end device can work over WAN, GSM, and 2G/3G/4G/5G. And this end device interfaces with the cloud. Therefore, we need to write protocols for the APIs. These protocols have to be decided by following the standards available. The GSM already has 3GPP standards and AT command, which makes it very easy to interface with the device as well as the cloud. However, GSM is power-hungry, and for IoT we require low power. So, LPWAN and NB-IoT are found suitable as they offer low-power data.

Narrowband IoT

Narrowband (NB) standards are based on low power wide area network (LPWAN) technology. It enables a wide range of new IoT devices and services using the GSM platform.

Its features include:

Uses LTE design extensively. These include single carrier frequency division multiple access (SC-FDMA) and frequency division multiple access (FDMA). 3G and 4G are also used on the same spectrum and same bandwidth.

Low cost. Narrowband supports both low-packet and low-power. So, the GSM 2G and 4G networks come together in 3GPP for Narrowband.

Extended coverage. 164dB maximum coupling loss or link budget in comparison to GPRS link budget of 144dB and LTE of 142.7dB.

Low receiver sensitivity. The sensitivity completely depends on the network. As for NB, 2G, and 3G, the sensitivity is high.

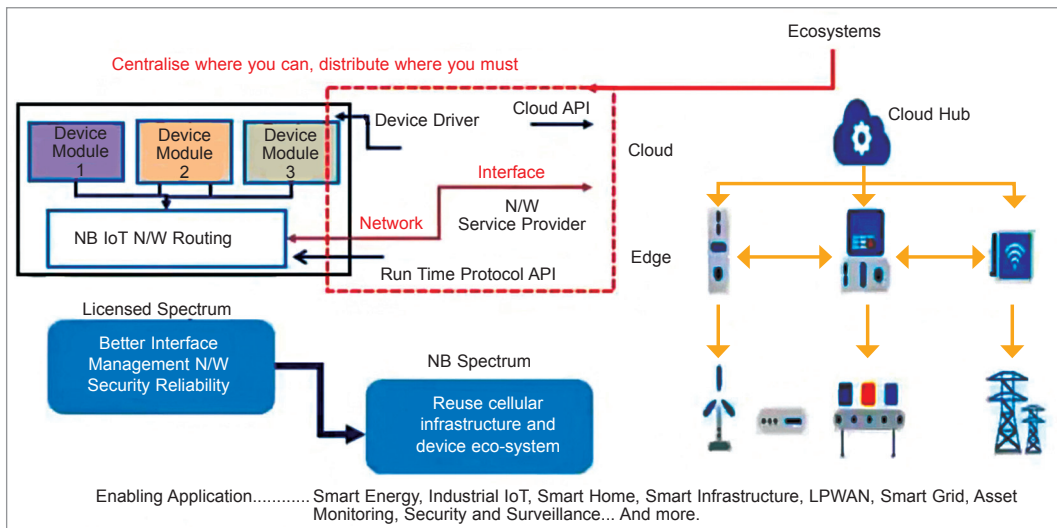


Fig. 8: NBIoT deployment

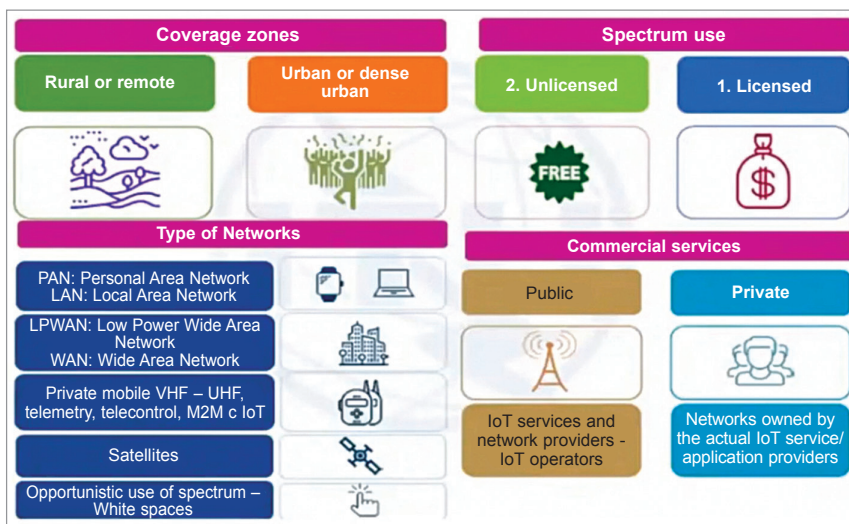


Fig. 9: Use cases

Long battery life. Up to ten years of operational lifetime with a 5-watt-hour battery (depending on traffic and coverage needs).

Supports high number of devices. At least 150k per cell.

Three modes of operation. These are:

1. **Stand-alone.** Spectrum currently used by GERA N (GSM Edge Radio Access Network) systems as a replacement of one or more GSM carriers.

2. **Guard band.** Unused resource blocks within an LTE carrier's guard band.

3. **In-band.** Resource blocks within a normal LTE carrier

In LTE carrier, we can use 3G or 4G. We have to use different modulations on the same band. And for that modu-

lation technique we require standalone operation, as well as we are sampling a frequency modulation that is either guardband or sideband. The difference between them is that the edge of a signal (for any spectrum) is always the sideband. And the amplitude of the middle of the signal is the guardband. The modulation is 200kHz.

The architecture of NBLoT is similar to the GSM architecture. But there is a difference in PDN gateways, serving gateways, and even the end devices. Take for instance LTE. We are targeting end devices that will go for NBA as well as for PDN gateways. But here on the LTE network, all the transmitters and receivers are on the side of the network. We need to make a change on the gateway (that is similar to the PDN gateway

and server gateway). And the network service provider is providing maximum signal availability to the infrastructure.

The challenge of Narrowband is that the network is not available in the market. Mobile network operators (MNOs) are working on this. So, on the design side, we are working with Narrowband Fall-back 2G since 2G is available everywhere in the market.

Wherever Narrowband is not available, the module will work on 2G. This altogether depends on standards, infrastructure, and mobile data rules.

Challenges and solutions

Some challenges being faced, and the solutions suggested for them are listed below.

Effect of resources. Maintenance of networks from threats. MNOs are going to change the network on the transmitter and receiver side for 2G, 3G, and LTE network as per the Narrowband.

Security. Hardware-level security needs to be defined when changing from 2G, 3G, or 4G. Cryptography is solving security and privacy issues.

Control access. Policies need to be defined for device control and user access.

Interoperability. Integration flexibility with device driver IP protocol.

Legality and rights. Data protection laws to be followed.

Economy and deployment. Investment incentives and technical skill required.

Considering the growing number of IoT devices and the requirement for low power, Narrowband IoT is the way forward as it meets this demand and offers fast connectivity along with robust and secure deployment. **EFY**

The article is based on the talk 'Telecom Narrowband IoT: The Next Big Thing' by Dharmendra Kumar, Head of IoT at Arihant Group, presented at February edition of Tech World Congress 2021. Vinay Prabhakar Minji is a technical journalist at EFY.