Collaborating for Self-Reliance – Co-Creating IoT Connectivity Solutions Using NB.Fi

Satya N. Gupta[1] FIETE, **Dr. Alice Maltseva**[2] and **Keshav Sharma**[3]
[1,3]Bluetown (India) Pvt. Ltd, Salcon Rasvillas, District Centre, Saket, New Delhi 110017 India
[2]Moscow State Institute of International Relations (University) MFA, WAVIoT, Russia
[1]sg@bluetown.com, [2]amaltseva@waviot.com, [3]kes@bluetown.com

Abstract -- **An innovative connectivity technology, named NB-Fi enables data transmission over 10 km or even more featuring 10 years of expected battery life. NB-Fi standard supports up to 4.3 billion devices in a single network with a 32-bit ID for each device.**

Few years back, Low Power Wide Area (LPWA) innovations were not in focus, however, the Internet of Things was waking up and taking off in light of the fact that individuals were roused by the conceivable outcomes. Web of Things (IoT) changes essentially the prerequisites for the network, mostly with respect to long battery life, low gadget cost, low connectivity cost, expanded scope and support for countless. Driven from these necessities, a few diverse cells and non-cell low power wide area (LPWAN) arrangements are rising and viewed for IoT business and the general network advertise.

Roused by this, in this paper, we audit and analyze the outline determinations of various LPWAN solutions, and discuss their appropriateness for IoT applications. What's more, we examine the IoT related components of these LPWAN advancements, and we debate about various situations and map which innovation is the best fit for every one of these situations. In end, we conclude with the challenges, requirements, and customisation of LPWAN technology to facilitate the mass deployment of IoT in various domains.

Keywords: Internet of Things, Low power wide area network, Sub-GHz band, Fifth generation wireless network, WiFi, Narrow-band radio modulation based wireless data transmission protocol, Secure wireless transmission, Machine-to-machine communication, Unlicensed spectrum, LoRaWan, WAVIoT Platform.

I. INTRODUCTION

WIRELESS network architecture is ever evolving and creating more capacities with 4G/LTE densification and 5G wireless and Wi-Fi. More small cells as close to each other as 250 metres means that each access point (AP) creates more bandwidth per square metre while the promise of fixed wireless 5G in the sub 6-GHz range and sub-millimetre wave band (*e.g.* 28GHz) creates more bandwidth as well as additional usable spectrum. In tandem with this evolution, the converged network that IoT (Internet of Things) devices rely on, must be efficient as this is the feature that consumers expect of their IoT devices.

All developing countries across the world are increasingly engaged on a journey towards "Digital Transformation". Exactly what this journey entails, and its desired impact may vary from sector to sector, as will the speed of this transformation. But it is clear that IoT with evolving technologies like: LoRaWan, NB-Fi and other emerging wireless connectivities will underpin this wide-ranging transformation across all industries [1].

Harnessing the potential of IoT will be crucial for companies and the economy as a whole over the coming years. Different sectors will face their own specific challenges. For example, some organisations might need to control and connect multiple robots within a factory plant to improve processes, reduce production down time and increase productivity; others – such as utility networks – might rely on sensors collecting data across the electricity grid to manage their operations more effectively. Such a range of requirements will need a diverse mix of technology and business models to deliver connectivity.

Today, a range of wireless technologies, from Wi-Fi to IoT solutions, have already been deployed to meet connectivity requirements across many of these sectors. However, the requirements of some businesses are starting to go beyond the limits of existing solutions. The diversity and complexity of new connectivity requirements, with increased focus on security and resiliency mean that many businesses and industries need to review their strategy to improve efficiency, flexibility and scalability [2].

Businesses and organisations across different sectors of the economy are increasingly looking to new technologies and digital solutions to become more flexible, agile and responsive in the way they do things to achieve tangible benefits such as increased efficiency, productivity and lower costs.

The increasing use of connected devices and sensors is extending the uses for IoT. While IoT solutions are not necessarily a new phenomenon, the increasing number of applications being developed have the potential to deliver significant benefits to consumers, such as improved healthcare and better energy and transport services. The vast amount of data generated by these devices, can provide significant insight and generate better targeted interactions, improve processes and increase quality of service.

Currently many different industrial applications are delivered using IoT Technologies via unlicensed spectrum or ISM band, including proprietary technologies, new connectivity platforms based on 5G and Wi-Fi evolutions that could enable more innovative IoT applications to increase flexibility, agility and responsiveness.

Some applications might require low power and long-range connectivity (over 20 km) using devices with long battery life in case of deployments in remote and hard-to-reach areas; common applications are: smart metering, smart lighting, asset monitoring and tracking, smart cities, livestock monitoring, energy management, manufacturing, and industrial IoT deployments. These solutions can be offered by Low Power Wide Area (LPWA) technologies.

II. WHY INTERNET OF THINGS?

Internet of Things makes our world as connected as possible together. Now-a-days, we have internet infrastructure almost everywhere and we can use it whenever. Embedded computing devices are being exposed to internet influence. Common instances for embedded computing devices are MP3 players, MRI, traffic lights, microwave ovens, washing machines and dishwashers, GPS even heart-monitoring implants or biochips etc.

IoT attempts to establish advanced connectivity (with the aid of internet) among these mentioned devices or systems or services to introduce automation in all areas. Imagine all things connected together, and all information would be interacting to each other over standard and different protocol domain and applications [3].

In a nutshell, IoT promises to connect all potential objects to interact with each other on the internet to provide secure, comfortable and pleasant life experience for humans.

Recent research shows by 2021 we will have over 20 billion devices which use IoT. IoT does that because of control on device and lower expense on media. But these huge fields make challenges such as depleting IP (V4) address, developing compatible and useful protocol and environment. Thus, the Non-IP Data Delivery (NIDD) is an important feature that are used in various appropriate technologies and even in narrowband-IoT to provide improved support of small data transfer.

III. APPLICATIONS OF IOT

Environmental Monitoring: Simple example is: You surely noticed by now that you surf the net and suddenly when open your Gmail, you see some interesting thing which are near to your favourite or in Facebook when you like page, on the right section similar content page will appear. These are common and tangible but imagine when we can monitor all embedded computing system to improve our life, such as –

a. with the aid of water or soil or air measurement device can say as how these are well for which plants.
b. with the aid of earthquake or tsunami warning systems, we can have less damages and victims.
c. we can monitor wild-life habitat and by such tracking provide them their propitious conditions to prevent their extinction.

Infrastructure Management: Infrastructure Management is needed for monitoring and tracking if there is any problem in urban or rural Infrastructure such as bridge, railway etc. to diminish and reduce risk of dangerous incidences and any failure in strength would be tested and alarms raised as soon as possible for repairs.

Industrial Applications: Industrial Applications investigate the quality of product for real-time optimizing to have good marketing such as who are most interested in which product and how this product can find marketing with tiny changes.

Energy Management

Energy Management are categorized with systems which are connected to Internet and with some sensor to reduce power consumption such as cloud based, remote control for oven, lamp etc.

Medical and Healthcare Systems: Healthcare Systems help to improve patient state better by monitoring and controlling their heartbeat or blood pressure or even their diet. Smart tablet which show us how much doughs with which gradient can help patient to get better.

Building and Home Automation: It is related to everything in home which have the potential to monitor and remote control such as air condition, security lock, lightening, heating, ventilation, telephony system, TV to make life comfortable, secure, with low energy consumption.

Transport Systems: To make regular city environment with less employees for police or automatic configuration in traffic lights, smart parking, traffic cameras to detect which road has heavy traffic to offer automatically less crowded road, or smart camera which can fine over-speeding drivers.

Large Scale Deployments: There are cities, which are almost smart cities with wide range of IoT deployments and wireless coverage.

IV. LOW POWER WIDE AREA NETWORKS

Low-power Wide-area Network (LPWAN) is a class of wireless technologies for transmission of small amounts of data over long distances used in distributed telemetry networks, inter-machine interaction and IoT. LPWAN can collect data from different equipment, for example meters, sensors or gauges.

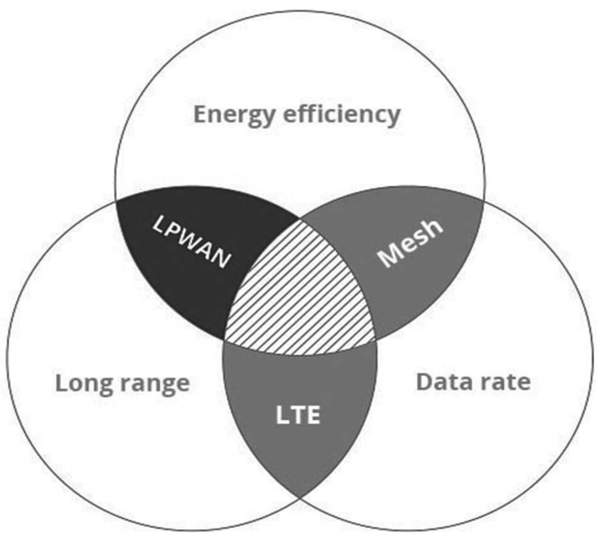

Figure 1. Existing wireless data transmission technologies achieve high performance only in two out of three communication characteristics at a time: energy efficiency, range and data rate.

Existing wireless data transmission technologies achieve high performance only in two out of three communication characteristics at a time: range, data rate and energy efficiency.

LPWAN technologies enable long-distance and energy-efficient data transmission. WAVIoT, a technology company developed an innovative connectivity technology, named NB-Fi and interfaced IoT devices with NB-Fi modules which could transmit data over a range of 10 kilometres or even more with up to 10 years of expected battery life. This development is described later.

LPWAN focuses on applications that require transfers of small data packages over long ranges, where network autonomy and independent power supply are important. Main areas of application of LPWAN are wireless sensor networks, automatic collection of meter readings, industrial monitoring and control systems [4].

NB-Fi is one of the leading technologies for IoT and M2M communications because of its high energy efficiency (battery life of devices reaches over 10 years), large network capacity (thousands of devices may be connected to a few NB-Fi base stations), high link budget and long signal transmission range. Geared for low-bandwidth, low computing end nodes, the newer LPWAN offer highly power-efficient and affordable IoT connectivity in vast, structurally dense environments. No current wireless classes can beat LPWAN when it comes to battery life, device and connectivity costs, and ease of implementation. As the name implies, LPWAN nodes are designed to operate on independent batteries for years, rather than days as with other wireless solutions. They can also transmit over many kilometres while providing deep penetration capability to connect devices at hard-to-reach indoor and underground locations.

Due to this unique combination of features, LPWAN has established itself as a prime driver of massive, latency-tolerant sensors network in industrial IoT, smart building and smart city sectors. While there is a plethora of LPWAN protocols available today, it is important to look at the distinct advantages of standard-based technologies. Given the explosive growth of IoT connected devices, Quality-of-Service, scalability and interoperability will be cardinal criteria in a wireless decision.

3GPP-based technologies like NB-IoT and LTE-M, along with MYTHINGS – a connectivity solution based on the latest ETSI open standard for low-throughput networks, are emerging together with proprietary technologies (*e.g.* NB-Fi, LoRa, Sigfox, etc.) and specifically address these requirements.

In terms of applications, NB-IoT and other carrier-based LPWAN standards will be a core pillar of future smart city networks. Leveraging existing cellular infrastructure, these managed networks provide extensive coverage in urban areas, while removing infrastructure expenses. On the other hand, for industrial deployments where data security and ownership are supreme, privately deployed solutions will rise as a preferred option. As an aside, industrial facilities are often located in remote regions that are poorly serviced by network operators.

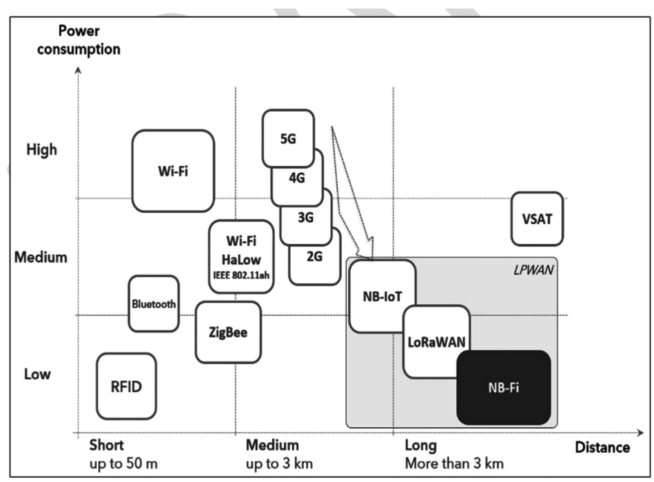

Figure 2. Wireless IoT technologies ecosystem: Niche position for NB-Fi.

IV. KEY ATTRIBUTES OF LPWAN

Long Range: Radio range is often measured in terms of receiver sensitivity – the lowest signal power for which a message can be detected and demodulated. In LPWANs, receiver sensitivity can reach -148 dBm, as compared to a moderate -70 dBm sensitivity in Bluetooth. This high receiver sensitivity is typically achieved by reducing the signal bandwidth and thus experienced noise levels (*i.e.* ultra-narrow band) or adding processing gain (*i.e.* Spread Spectrum); both come at the cost of lower data rates.

In addition to special modulation techniques, the use of sub-GHz frequency bands in most LPWAN solutions, instead of the popular 2.4 GHz band, further improves range and penetration capability. As the wavelength is inversely proportional to free space path loss, the long radio waves in sub-GHz systems can travel over long distances. Compared to 2.4 GHz signals, they can also penetrate through walls, trees and other structures along the propagation path much better, while bending around solid obstacles.

Low Power: LPWAN systems adopt multiple approaches to optimize power efficiency, giving many years of battery life on end nodes. First, when not actively transmitting, the transceivers are put into "deep sleep" mode whereby very minimal power is consumed. In bi-directional communications, a listening schedule is defined so that the device is "awake" only at predefined times or shortly after an uplink is sent to receive the downlink message [5].

Secondly, many LPWAN technologies employ a lightweight asynchronous protocol at the Medium Access Control layer to minimize data overhead.

Low Cost: LPWAN's simplified, lightweight protocols reduce complexity in hardware design and lower device costs. Its long range combined with a star topology reduce expensive infrastructure requirements, and the use of license-free or already owned licensed bands, reduce network costs [6].

Key IoT Verticals	LPWAN	Cellular	Mesh	BLE	Wi-Fi
Industrial IoT	●	○	○		
Smart Metering	●				
Smart City	●				
Smart Building	●		○	○	
Smart Home			●	●	●
Wearables	○			●	
Connected Car		●			○
Connected Health		●		●	
Smart Retail		○		●	●
Asset Tracking	●	●			
Smart Agriculture	●				

● Highly applicable ○ Moderately applicable

Figure 3. An overview of technology application compatibility.

V. LPWAN: CHALLENGES AND REQUIREMENTS

The importance of industrial-grade reliability cannot be overstated. Because of mission-critical applications like environmental monitoring, predictive maintenance and worker safety, the Industrial IoT sector demands a packet-error rate of less than one percent. High reception rate and minimal packet loss ensures important data is accessible; providing the business intelligence needed to improve operational efficiency across an entire campus at the lowest total cost of ownership.

For LPWAN technologies operating in the increasingly congested, license-free spectrum, interference resilience is a prerequisite to ensure high reliability. An LPWAN's technical design determines its ability to avoid interferers or packet collisions when the traffic is high, thereby improving overall reception rate.

LPWAN innovations are described by their emphasis on vitality effectiveness, adaptability, and scope. LPWAN systems are planned for IoT arrangements that need low power utilization, expanded battery life, and great entrance in structures and underground. A few unique innovations are being produced and sent to help such IoT necessities [7]. A vital classification of LPWAN is a versatile administrator oversaw IoT arrange in light of 3GPP guidelines for IoT systems. The two most usually recognized innovations as characterized inside the 3GPP models for these intentions are LTE-M (additionally alluded to as LTE Cat-M1) and NB-IoT (Narrow-Band IoT). Because of its key qualities, LPWAN is probably going to significantly affect the development rate of future IoT advancement and achieve higher volume gadget arrangements than that are available today [8].

Clearly, large numbers of LPWAN nodes are required for smart city applications, and hence the network should have large capacity and scalability. Applications like smart city may not be too concerned about monetary implications in an urban environment. Many of these nodes can be powered through a power line and, even if they are battery operated, in most of the cases, replacement of batteries is possible, and hence low power consumption requirement is at a moderate level. Enhanced characteristics required for smart city applications could be important in several ways such as heterogeneity of devices and software platforms, varied radio coverage requirement, co-existence and interference mitigation.

A significant segment of low-power wide-area solutions typically sends small-sized messages infrequently, are delay-tolerant, do not need high data rates, and require low-power consumption and low cost. The characteristics from above can be mapped into a set of requirements [9]. The key requirements relate to handling of M2M traffic, massive capacity, energy-efficiency, low power operations, extended coverage, security, and interworking. Some examples from real life scenario are analysed below:

Traffic Requirements: The inherent communication mechanism of LPWAN networks entails traffic generated by distributed sensors. In addition to the possible presence of traffic created by smartphones or other devices, the LPWAN traffic itself can vary in a wide range of attributes like the number of messages, message size, and reliability requirements. LPWAN technologies have diverse categories of applications with varying requirements. Some of the applications are delay-tolerant (*e.g.* smart metering), while applications like fire detection, nuclear radiation detection, and home security require prioritized and immediate transmission. In some applications, a priority message scheduling may be required for event-triggered transmissions. With the massive number of active devices, there is a possibility of a service level agreement (SLA) requirement of each application that might not be satisfied. Mechanisms need to be supported for the co-existence of different traffic types, the required quality of service (QoS), and SLA. In LPWAN applications, provision may need to be made for handling multiple classes of end devices based on their communication needs in uplink or downlink. In some applications, device mobility support is needed and is required to be able to be connected anywhere and ensure seamless service on the move.

Capacity and Densification: One of the essential requirements for LPWAN is to support a massive number of simultaneously connected devices with low data rates. Many applications require support for 100,000+ devices in a scalable manner. Scalability refers to the ability to seamlessly grow from a network of a small number of heterogeneous devices to massive numbers of devices, new devices, applications, and functions without compromising the quality and provisioning of existing services. As LPWAN end devices have low computational and power capabilities, network devices such as gateways and access stations can also play a vital role in enhancing scalability. Employing multi-channel and multi-antenna based on different diversity techniques can also significantly improve the scalability of LPWAN networks. However, it is to be ensured that such features do not compromise other performance metrics. A large number of devices also results in high densification. The network needs to mitigate the issues of bottlenecks in media access and interference, and avoid degradation of performance of the network.

Energy Efficient Operations and Low Power Sources: In several applications of LPWANs, the environment and the constraints do not allow the recharging of batteries. The battery is expected to last over ten years without charging. Typically, AA or coin cell batteries are used. If the battery loses power, replacement of the battery may not be possible within short periods. The cost of battery needs to be low. The LPWAN should be operated with a strict and very low duty cycle limit so that node lifetime can be enhanced. Hence, ultra-low power operation is a crucial requirement for battery powered IoT/M2M devices.

Coverage: The range of operations requires both long range as well as short range communications. Typically, LPWAN needs to provide long range communication up to 10–40 km in rural/desert zones and 1–5 km in urban zones with +20 dB gain over the legacy cellular networks. For applications involved in monitoring and collecting data, coverage may need to be provided for indoor, hard to reach locations like underground locations and basements. Coverage needs to be consistent with expectations on adaptable data rates and managed data error rates. Use of the sub-GHz band helps most of the LPWANs to achieve robust and reliable communication with a lower power budget because the lower frequencies of the sub-GHz band have better propagation characteristics as compared with the 2.4 GHz and higher bands. Additionally, the low modulation rates used for LPWAN put more energy for each bit, and hence increase the coverage. A lower modulation rate also helps the receivers in demodulating the signal correctly.

Location Identification: Location identification for devices is a crucial requirement for some applications. Location accuracy plays a key role in applications such as logistics and livestock monitoring. The resolution range may vary from a few centimetres to metres. Monitoring and security for sensing unusual events such as changed device location and facilitating the proper level of authentication need to be supported. Location identifications can be achieved by global positioning system (GPS), GPS-like systems, or running smart algorithms with the help of network infrastructure.

Security and Privacy: The security requirements for LPWAN devices are particularly stringent because of the massive number, vulnerabilities, and simplicity of the devices. The essential attributes of authorization, authentication, trust, confidentiality, data security, and non-repudiation need to be supported. The security support should be able to handle malicious code attacks (such as worms); handle hacking into LPWAN devices and system; and manage eavesdropping, sniffing attacks, and denial of service (DoS) attacks. It is also important to protect the device identity and its location privacy from the public. Additionally, it should also support security for the forward and backward transmission as required in various applications.

Cost Effectiveness: LPWAN applications are particularly sensitive to device and operational cost. In addition to the standard requirements of low deployment and operating costs for the network, the large number of devices involved puts major constraints on cost, operational expenses, and an imperative of low power consumption. Software upgradability without changing hardware is a key attribute that needs to be supported. Besides, it becomes imperative to support scalability, easy installation, and low cost maintenance [10].

Reduced Device Hardware Complexity: To handle the large number of devices, low cost operation, and long range coverage, the design of small-sized low complexity devices becomes an essential requirement. The reduced hardware complexity structure enables the reduction of the power consumption in battery-powered devices, without sacrificing too much performance. The devices generally are expected to possess low processing capabilities. Simple network architecture and protocols need to be supported by the hardware. From a technology point of view, to achieve the required adaptability of the LPWAN devices, radio transceivers need to be flexible and software reconfigurable.

Operations, Interrelationships, and interworking:
The network should be able to handle heterogeneous devices. These large number of devices may share the same radio resources causing intra- and internet work and technology interference, resulting in a degradation of network performance. Hence, LPWAN devices should possess the ability to connect and operate in varied LPWAN technology environments with interference tolerance, handling, and mitigation capabilities. The network should be able to enable connectivity of devices irrespective of hardware infrastructure and application programming interface (API). Seamless end-to-end interoperability needs to be supported between different network technologies. This may require standardization and gateways with adaptability protocols between various communications technologies. Full end-to-end application integration is expected [11].

In summary, the LPWANs are resource-constrained networks and have the critical requirements for long battery life, extended coverage, high scalability capabilities, low device cost, and low deployment cost.

VI. NB-Fi – EMERGING LPWAN TECHNOLOGY

NB-Fi is a LPWAN protocol that supports secure bidirectional communication for IoT, machine-to-machine (M2M), Smart Grid, Smart Utilities, Smart City and industrial applications.

NB-Fi is a protocol that was developed by WAVIoT and designed for secure wireless transmission of small volumes of data over long distances with low energy consumption. NB-Fi is an open standard with disclosed format of NB-Fi messages and relevant technical data required for manufacturers to produce compatible end-devices.

In February 2019, the Federal Agency for Technical Regulation and Metrology of the Russian Federation approved NB-Fi as a preliminary national standard "Narrow-Band Radio Modulation Based Wireless Data Transmission Protocol (NB-Fi)". The document became effective in April 2019 [12]. In 2022, NB-Fi is expected to be approved as a permanent national standard.

NB-Fi Network and WAVIoT Platform: NB-Fi devices transmit data via NB-Fi radio protocol to base stations, then base stations forward data packets to the cloud server – WAVIoT IoT platform. Processed data is displayed in a cloud platform (frontend) and can be transferred to any third-party app via API. WAVIoT IoT platform provides bidirectional communication (uplink and downlink messages) for end-user devices.

WAVIoT devices operate in unlicensed ISM bands, which are different in different countries. The distinctive feature of the NB-Fi standard is using narrowband phase-modulated signals, which in combination with interference-resistant encoding

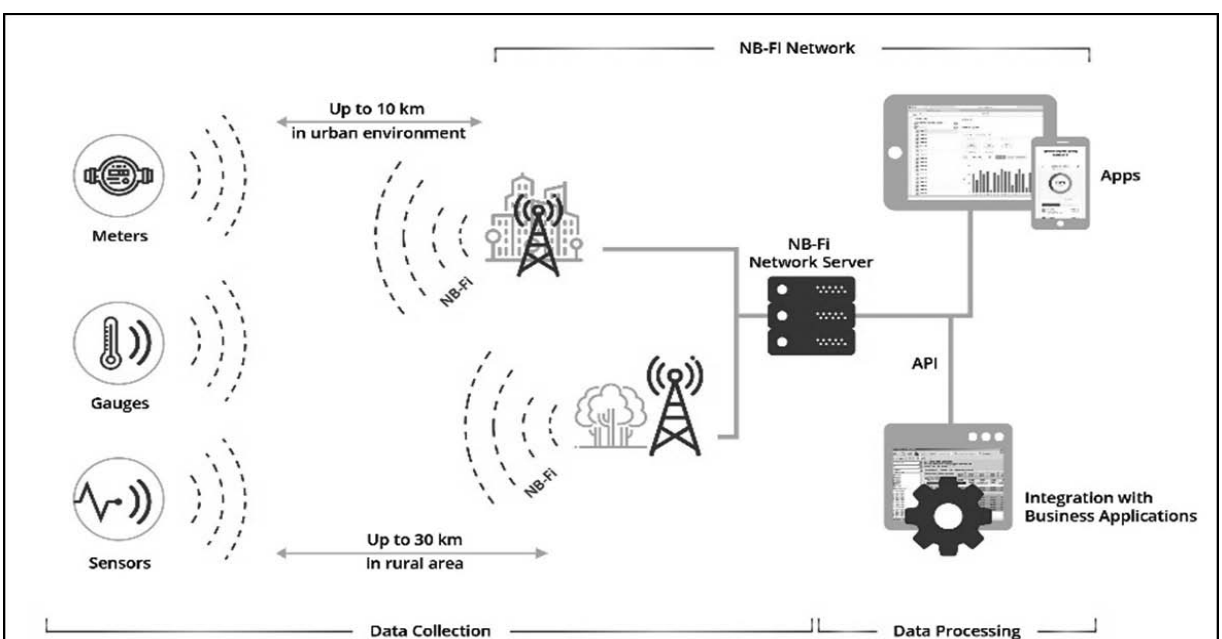

Figure 4. Secure wireless communication via NB-Fi.

can achieve very high level of reception sensitivity, while the total frequency band for simultaneous transmission of a large number of channels remains quite narrow [13]. NB-Fi base stations receive signals from NB-Fi devices with signal power as little as the noise level, and NB-Fi transceivers ensure long operational time of devices on a single charge (more than 5 years from an A-size battery, subject to operating parameters).

Specification of the NB-Fi Protocol: NB-Fi standard supports bidirectional (Uplink and Downlink) communication. This is primarily required for such devices like electricity meters, where a Downlink channel allows controlling the meter: to synchronize the time, to update the tariff schedule, to switch off the load relay. The NB-Fi transceivers, built-in into devices, together with sophisticated algorithms for receiving signals, provide almost symmetrical communication channel in both directions.

All WAVIoT devices with bidirectional communication support the adaptive data rate – if the signal level is good, devices will automatically switch to a higher data rate, which allows to use the spectrum efficiently and also reduce the power consumption for transmitting data.

NB-Fi standard supports up to 4.3 billion devices in a single network with a 32-bit ID for each device. NB-Fi does not use the IP addressing (IPv4, IPv6) to optimize the size of payload. IoT devices such as sensors and gauges can transmit tiny data packages, only a few bytes. As the minimum size of the IP header is 20 bytes, the Non-IP Data Delivery (NIDD) approach allows to develop simpler and cheaper devices. Data exchange between devices and third-party applications is possible via the WAVIoT IoT platform's API [14].

TABLE 1 -- NB-Fi STANDARD SPECIFICATIONS (FOR UPLINK PACKETS)

Modulation technique	DBPSK
Data rates	50, 400, 3200, 25 600 bps
Channel separation method	Time and Frequency
Number of simultaneously received channels in 51.2 kHz bandwidth	1,024 (for 50 bit/s speed) 128 (for 400 bps) 16 (for 3,200 bps) 2 (for 25,600 bps)
Maximum receiver sensitivity	-148 dBm (for 50 bps speed) -141 dBm (for 400 bps speed) -132 dBm (for 3,200 bps) -123 dBm (for 25,600 bps)
Uplink packages capacity for one base station	20 Mbit/day

TABLE 2 -- SPECIFICATIONS FOR MAC AND TRANSPORT LAYERS OF NB-Fi PROTOCOL

Network capacity	4.3 billion devices (2^{32})
Data transfer rates (for Uplink packets)	10, 80, 640, 5120 bps
Data transfer rates (for Downlink packets)	Depending on the implementation of a specific radio transceiver
Encryption algorithm	AES-256 or other symmetric block cipher algorithm with 256-bit encryption key
Payload for one NB-Fi packet	8 bytes
Maximum payload length for group packet at Transport layer	240 bytes

LPWAN systems are used to transmit data over long distances successfully, using both narrowband and broadband signals. Each of these systems has its pros and cons – the right technology chosen depends on technical requirements and other considerations.

NB-Fi technology is focused on energy efficiency and long-life device autonomy without frequent power element replacement, as well as solutions that require fast and inexpensive rollout of IoT network while achieving 100% data collection rate from devices [16]. The comparison table of NB-Fi and other LPWAN technologies is in Fig.5.

VII. KEY ADVANTAGES OF THE NB-Fi TECHNOLOGY [17]

Exceptional receiver sensitivity: WAVIoT base stations have the highest possible receiver sensitivity down to -148 dBm (at a data rate of 50 bps), which allows to achieve the maximum possible line budget in the NB-Fi network and a long range of data transmission. NB-Fi transceiver also has a high receiver sensitivity down to -148 dBm (at 50 bps data rate).

Sophisticated cryptographic algorithms: The implementation of secure data exchange between the NB-Fi device and cloud server ensures the confidentiality and integrity of the information not only between the device and the base station, but also between the base station and WAVIoT IoT Platform. NB-Fi use the AES-256 encryption, also other symmetric block cipher algorithms with 256k encryption key may be used.

Working in license-free ISM band: NB-Fi protocol requires only 200 kHz of license-free spectrum. NB-Fi devices by WAVIoT comply with European (ETSI EN 300-220 V2.1.1) and North American (FCC part 15.247 and 15.249) regulations.

Full technology stack range and wide NB-Fi products portfolio: WAVIoT develops full range of products for the IoT network from the NB-Fi transceiver to the various types of IoT devices

	NB-Fi	Sigfox	LoRaWAN	NB-IoT
Topologies supported	Typically Star, Mesh possible[1]	Star	Typically Star, Mesh possible	Star
Maturity level	In use commercially	In use commercially	In use commercially	Early stages - pilot deployments
Modulation technique	Ultra narrow band	Ultra narrow band	Spread Spectrum	LTE-based
Modulation	DBPSK	BPSK	Chirp spread spectrum (CSS)	QPSK
Frequency	Unlicensed ISM bands	Unlicensed ISM bands	Unlicensed ISM bands	Licensed LTE frequency bands
Bandwidth	50 Hz – 25 600 Hz	100 Hz	250 kHz and 125 kHz	200 kHz
Channels in 50 kHz	1 024 (for 50Hz bandwidth)	512	0	0
Channels in 500 kHz	10 240 (for 50Hz bandwidth)	5 120	4	2
Maximum data rate	25 kbps	100 bps	50 kbps	200 kbps
Bidirectional	Yes, Full-duplex for base stations, Half-duplex for devices	Limited, Half-duplex	Yes, Half-duplex	Yes, Half-duplex
Maximum messages/day	For UL: 3 mln, up to 20 Mbit per 1 base station per day For DL: 100k, up to 10 Mbit per 1 base station per day	For UL: 140 For DL: 4	Similar to NB-Fi, no exact data[2]	Unlimited
Maximum payload length for group packet	240 bytes	12 bytes (UL) 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Authentication & encryption	AES 256-bit	AES 128-bit	AES 128-bit	LTE encryption
Adaptive data rate	Yes	No	Yes	No
Standardization	NB-Fi standard was approved as a preliminary National Standard by Russian Federal Agency on Technical Regulating and Metrology in February 2019	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network	LoRa-Alliance	3GPP
Battery efficiency	High TX and RX dominated by payload data	High TX and RX dominated by payload data	Low TX and RX dominated by leader sequence	Low TX and RX dominated by leader sequence

Sources: [1] A comparative study of LPWAN technologies for large-scale IoT deployment, https://doi.org/10.1016/j.icte.2017.12.005; [2] Analysis of WAVIoT company
[1]With NB-Fi transceiver
[2]Unlimited according to [1], though has the same limits as NB-Fi

Figure 5. NB-Fi vs. other LPWAN technologies comparison.

and IoT Platform. This allows building corporate or global IoT network to use single NB-Fi technology for various use cases.

An open NB-Fi protocol for developers: WAVIoT provides to developers NB-Fi libraries and relevant technical data that allows to develop their own IoT devices. Customers can rollout their own private/corporate network or use the global IoT platform. WAVIoT propose NB-Fi Development Kits and NB-Fi transceivers that support the NB-Fi standard at the physical level.

Scalability and reliability of NB-Fi network: NB-Fi allows to build global, stable and scalable IoT networks with millions of NB-Fi devices connected to a single IoT platform. Noise stable NB-Fi network ensures the 100% of uptime – NB-Fi network could not be restrained by legal way and without specialized equipment.

VIII. UNLICENSED RADIO SPECTRUM – *OXYGEN FOR IOT ECOSYSTEM*

Devices relying on the unlicensed spectrum have become indispensable for providing low-cost connectivity in countless products used by people across the globe. It would be hard to overstate the importance of the unlicensed wireless spectrum in the Indian economy. Still, majority of telecom industry relies upon unlicensed wireless technologies that depend on unlicensed spectrum access to function.

Soon driverless cars, smart homes, drones, telemedicine, and smart cities will require more bands of spectrum and will add millions of workers directly employed in the telecommunications sector. For the stakeholders and industry experts in this sector, there is a clear indication for the urgent requirement of more unlicensed spectrum to be made available to the industry for the development of in-house innovation for upcoming technologies where seamless connectivity of machines and humans is much of a need, like in case of 5G, Wi-Fi, M2M and IoT.

Technological advancements such as the IoT, Wi-Fi, LPWAN, and others have demonstrated that when an opportunity for cost-efficient and flexible spectrum usage requirement is presented in the form of unlicensed spectrum, the market is likely to respond through innovation and expansion.

The unlicensed spectrum also plays a very important role in the broader innovation ecosystem for IoT. IoT enterprises across the country are building the next generation of Internet applications, connected devices, and innovative services—all of which rely on access to unlicensed spectrum [18].

Unlicensed spectrum is used to deliver the data services, again, that many enterprises have harnessed to offer new products and services. The most evident of these unlicensed technologies is Wi-Fi, which is now one of the important mediums for carrying Internet traffic. Unlicensed spectrum has also allowed for the emergence of connected devices, also known as the IoT. As per the McKinsey's report, the IoT is expected to grow to 43 billion connected "devices" by 2023, an almost threefold increase from 2018 [19].

It is well known that LoRa which is a long range, low power

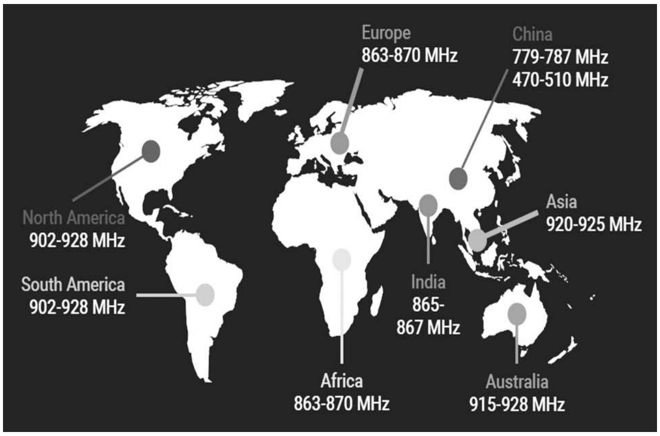

Figure 6. Unlicensed spectrum world-wide for IoT (LoRa) usage.

wireless platform is also one of the popular technology for IoT networks worldwide.

LoRa can work with many frequency bands in the ISM band of frequencies, but the most popular bands being in use for LoRa are:

- 868 MHz – EU (ITU Region 1)
- 915 MHz – Americas (ITU Region 2).

That's why most of the OEMs dealing with LoRa and IoT, are manufacturing their equipment to work in these bands of frequencies *i.e.* 868 MHz – EU (ITU Region 1) and 915 MHz – Americas (ITU Region 2). In India license-exempt band ends at 867 MHz (from 865 MHz to 867 MHz) because of which benefits of this technology are not leveraged to its full potential [20].

To expand IoT ecosystem in India, no doubt, more license-exempt spectrum is required. Hence, it is important that complete 868MHz band and 915MHz band as available in ITU Region 1 and Region 2 respectively, is delicenced for a technology-neutral usage.

Also, the recent decision of US FCC for the incorporation of the all-new 6 GHz band in Wi-Fi 6 marks the most significant update to Wi-Fi and IoT sector enterprises. Which is very welcome step and probably, most impactful, for the future. With this (Wi-Fi 6E) update coming into the picture, one can forget about the congestions that arise on the current spectrum offerings (both 2.4 GHz and 5 GHz) and expect a stable connection with seamless speeds and reduced latency. Not to mention, this will provide reasonably larger bandwidth that offers better performance with ever-increasing IoT and smart devices in homes and ensures there is almost no interference and network congestion in the years to come. This Wi-Fi 6E update has very huge potential, so huge that it can transform entire Wi-Fi and IoT industry. Just to utilize its potential, on 23rd April 2020, FCC, USA signed new regulation releasing 1.2 GHz of new spectrum for Wi-Fi and other unlicensed use in the 6 GHz band. "*As per the research carried by Dr. Raul Katz, a leading scholar of economics and telecommunications policy, this great step taken forward by FCC, will add $183.44 billion to U.S. economy by 2025"*[21].

India needs to adopt learnings from all these international developments and should move ahead in this direction not only for the adoption of more spectrum being made unlicensed but also to fulfil our goals as illustrated in our NDCP-2018. These steps as taken by US are bold, praiseworthy, and very much essential for more innovation and efficient performance of networks. We should take cognizance of these steps taken by US.

IX. STANDARDISATION FOR LPWAN TECHNOLOGIES

Standardization is one of the core pillars in a robust and vibrant IoT ecosystem. A standardized technology provides a rigorous and transparent technical framework to fuel both vertical and horizontal interoperability. Given its significance, we want to clarify what makes a standard-based technology and why it matters for the end user.

In the LPWAN realm, we have seen many industrial alliances established around proprietary solutions to promote standard development. However, these efforts do not ratify the viability of the technology and more notably, might not cover the whole network stack. It's common that only the MAC layer is made open, while the physical layer remains entirely proprietary, as in the case of the LoRa Alliance (*i.e.* LoRaWAN is the MAC layer and LoRa is the proprietary physical layer by Semtech). By making (part of) the technical specifications publicly available on a royalty-basis, many LPWAN vendors attempt to claim their technologies as "open standards." Nevertheless, this is not really the case.

Strictly speaking, an industry standard – must undergo a stringent evaluation process by an established Standards Development Organization (SDO). This guarantees the quality and credibility of the technology. Dominant global SDO examples include ETSI, IEEE, IETF, 3GPP (3rd Generation Partnership Project) [22], etc. So far, there have been only two camps of LPWAN technologies that have succeeded in standardization efforts and are endorsed by formal standard organizations [23]. One is cellular LPWAN that implements 3GPP standards, and the other is the Telegram Splitting technology based on the newly released ETSI standard on Low Throughput Networks – TS 103 357.

X. FACILITATION BY GOVERNMENT OF INDIA FOR IoT LANDSCAPE AND OPPORTUNITY

Development of telecommunications, Govt. of India, has been providing limitless opportunities to exchange knowledge and information, to innovate the technological solutions for making life comfortable for the masses. Over the past 20 years, numerous wireless standards and networks have emerged to meet the demands of an ever-increasing volume of data transmission between masses and machines. In recent years, it is devices, not users, that are causing the rapid growth of traffic and are driving the development of new communication standards. Communication technologies for IoT open new opportunities for companies from various sectors of the economy, significantly improving the efficiency of internal processes and bringing the interaction with customers to a new level.

The role of India on the global IoT market is growing fast and India is becoming one of the world leaders in IoT. Key IoT market drivers in India today are Smart City mission (Smart Utilities & Energy, Industrial IoT), Digital India, Make in India programs.

IDC predicts the IoT global market revenue to reach approximately US$1.1 trillion by 2025 [24]. IoT market is deeply interconnected with other digital technologies, such as Big Data Analytics, Cloud Computing, Cybersecurity, Artificial Intelligence, Robotics, Blockchain, which provides huge opportunities for revenue.

According to NASSCOM report [25], the IoT market volume in India is expected to reach 9 billion dollars by end-2020. Utilities comprise the biggest share of IoT revenue in 2020, reaching 25% from total industry sectors revenue. 18% goes to Manufacturing, 13% - Transport and logistics, 11% - Automotive, 10% - Healthcare, 9% - Retail, 8% - Agriculture.

Predicted IoT market growth could be achieved with initiatives to create new IoT-enabled products and services, underpinned by a robust technical infrastructure through which public and commercial IoT products and services can be delivered directly to consumers. There is a great opportunity to collaborate with Russian Technology Regulator to research and co-create connectivity solutions in order to facilitate mass IoT deployment in India.

XI. WAY FORWARD FOR ALL PERVASIVE IOT CONNECTIVITY REALIZATION

While the sheer variety of today's available connectivity offerings can be formidable at first sight, the business cases to be tackled and their specific needs will act as the guiding hand to help you identify the best match. Note that for a future-proof wireless architecture, it's important to consider not only existing requirements but also those that might come up down the road. For example, how much radio traffic will be generated in the near future or can the network grow effectively to support thousands of devices once the need arises?

When it comes to IoT deployments that rely on vast networks of granular, battery-operated IoT sensors amid challenging physical environments, LPWAN emerges as the most pertinent solution. LPWAN has been seen as a crucial catalyst for latency-tolerant industrial and commercial applications like condition monitoring, asset management, smart metering, and environmental monitoring. Nevertheless, even within this wireless family, technologies can greatly vary based on different network criteria. As a general rule, technologies rooted in proven standards offer distinct advantages in terms of Quality-of-Service and long-term interoperability.

The IoT use cases span the breadth of personal lifestyle issues, to commercial/industrial use cases with GE monitoring 5,000 parameters per second from its aircraft engines to proactively optimize the performance and safety of its engines, to smart connected devices self-managing themselves to optimize electricity consumption and enabling environmental strategies. The real commercial benefits of IoT could be measured in the billions of rupees. If done right, not only can the IoT save us lot money, make the world a safer place, make for a greener planet, but also fundamentally change the way we live and work.

In addition to these benefits, another aspect of the IoT movement is the impact of millennials. Most technology advances have been constrained by our ability as humans to adopt change. If you look at the demographics around the world, by 2025 millennials will represent over 70% of the active workforce. They not only embrace this change, but in fact will accept nothing less than the personalized lifestyle enabled by the next generation of connected smart devices promised by the IoT. The current IoT adoption estimates point to 20-30 billion devices connected by end of 2020, and up to 500 billion devices by end of 2025. So, the question becomes: what could be the last mile barriers in the IoT taking over the world? What are the real last mile head winds that could bring the promise of the IoT to a grinding halt? To better understand that, let us examine the above uses case from a different perspective.

The first consideration is *privacy*. To enable the lifestyle use case above, think of how much personal information about you, in aggregate, is being tracked by the various smart devices involved. All these devices are connected over the Internet. The Internet as we know it is only as secure as the last device connected to it. If any of these devices had a security vulnerability, it could be a window into all other devices, and therefore into your very personal world. The perceived risk to privacy is the first barrier that we will have to become comfortable with.

The second consideration is *security*. The devices may have access to personal financial and other sensitive information, like the stored value card above, which could be compromised if the security was breached. In addition, in commercial use, critical devices like the aircraft engines, if breached by wrong individuals, could create significant security [and safety] risks. Just like the benefits of the world of the IoT are not completely understood, the risks and associated remediation strategies required to ensure security are not well quantified either. To get IoT into a commercially viable domain, many of the downside risks will have to be understood and protected against. This will cost more and take a lot longer than what is currently being anticipated.

The third consideration is *connectivity*. As you drive down the road in your car in Delhi, you perhaps lose cell signal at least one to two times a day. That is just connecting the billion odd cell phones around the world. The cell phones are taxing our telecommunications networks. To support the IoT connectivity, our core networks will require significant upgrades and re-architecture to support the huge increase in edge connectivity, latency, bandwidth, and reliability requirements associated connecting smart devices. To connect and support 20 billion smart devices will require our core networks to be re-thought from the ground up. That means, there will be billions of unplanned investments that will have to be made in communications infrastructure around the world [26].

If all of the above challenges are addressed, the final frontier will be *interoperability*. All these devices will be manufactured by different companies in different countries. For them to communicate and interoperate effectively, global IoT standards will have to be developed and governed. This is something that takes time, effort, and industry sponsorship.

The IoT is clearly here to stay. It will transform our lifestyle in unimaginable ways. Time has come now for a collaborative beginning to Make India self-reliant *(Atmanirbhar)* in this compelling domain. Let us Make it Happen, together!!

REFERENCES

[1] https://www.mdpi.com/1999-5903/12/3/46/pdf
[2] Understanding the Internet of Things (IoT) – GSMA. https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf
[3] Introduction to Internet of Things – ITU. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Nov_IOT/NBTC%E2%80%93ITU-IoT/Session%201%20IntroIoTMZ-new%20template.pdf
[4] U. Raza, P. Kulkarni and M. Sooriyabandara, "Low power wide area networks: An overview," IEEE Communications Surveys Tutorials, vol. 19, no. 2, pp. 855-873, 2017
[5] H. Nguyen Nam Tuan Le, Pham Tung Lam, Nguyen Cong Hoan, Thanh Luan Vu, Minh Duc Thieu and Yeong Mil Jang, "The next generation architecture of low power wide area network for energy platform," in 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), Zagreb, Croatia, 2019.
[6] https://behrtech.com/
[7] https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/resources/innovation-technology/low-power-wide-area-technology
[8] Frost & Sullivan - Growing Industry Applications of LPWAN Technologies.https://rfdesignuk.com/uploads/9/4/6/0/94609530/murata_lpwan_study.pdf
[9] https://www.networkcomputing.com/wireless-infrastructure/new-lpwan-applications-expand-use-cases
[10] LPWAN Technologies: Emerging Application Characteristics. https://www.mdpi.com/1999-5903/12/3/46/pdf
[11] https://www.sciencedirect.com/book/9780128188804/lpwan-technologies-for-iot-and-m2m-applications
[12] http://nd.gostinfo.ru/document/6446213.aspx?fbclid=IwAR2c9BDd1vLvL21fHkluB6v9wo4FLvnitKyz5AIzT0wO47KiKxvYBcSmrj0
[13] WAVIoT NB-Fi LPWAN technology - products and tech description, [online] http://waviot.com/
[14] https://waviot.com/technology/nb-fi-specification/
[15] "Comparison of LPWAN technologies," WAVIoT, [Online]. https://waviot.com/technology/waviot-lpwantechnology-comparison.
[16] Augustine Ikpehai, Bamidele Adebisi, Khaled M. Rabie, Kelvin Anoh, Ruth E. Ande, Mohammad Hammoudeh, HarisGacanin and Uche M. Mbanaso, "Low-power wide area network technologies for internet-of-things: A comparative review", *Internet of Things Journal IEEE*, vol. 6, no. 2, pp. 2225-2240, 2019
[17] https://waviot.com/technology/waviot-iot-platform/
[18] P. M. John Burns and SelcukKirtay, "Future use of licence exempt radio spectrum," Plum Consulting, Tech. Rep., 2015. http://www.plumconsulting.co.uk/pdfs/Plum July 2015 Future use of Licence Exempt Radio Spectrum.pdf
[19] https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things
[20] Innovations in unlicensed spectrum bands – The Centre for Internet & Society. https://cis-india.org/telecom/unlicensed-spectrum-brief.pdf
[21] Institute of electrical and electronics engineers. [Online]. https://www.ieee.org
[22] The 3rd generation partnership project. [Online]. http://www.3gpp.org/
[23] European Telecommunications Standards Institute, "Short range devices; Low throughput networks (LTN); Protocols for radio interface A", European Telecommunications Standards Institute, ETSI TS 103 357, 2018.
[24] http://ficci.in/spdocument/23092/Future-of-IoT.pdf
[25] https://www.nasscom.in/sites/default/files/media_pdf/indian-iot-market-set-grow-upto-usd-15-bil-
[26] Internet of Things, The Realization of The Last Mile. https://www.siliconindia.com/magazine_articles/Internet-of-Things-Iot-The-Realization-of-The-Last-Mile-MNCM126910522.html

Satya N. Gupta, FIETE is an expert in NGN technologies, regulation, interconnection and broadband with 40 years' experience in all aspects of telecom. Recognized as an analyst, author, advocate and advisor on ICT related policies, projects and business. After his post-graduation from IISc. Bangalore, he joined ministry of Communication in 1981 and Ministry of railways in 1983. Recipient of Minister of railways award for outstanding performance for digitalisation project.

A triple master in electronics design technology, IT management and telecom policy and regulation authored *Everything over IP-All you want to know about NGN.* Also authored a concept called "Job Factory- Converting Unemployment into Intraprenuership". His recent research-based work is "Long Tail - Walking the Extra Mile on Rural Broadband Business". Established and mentoring a consulting startup, SAAM CorpAdvisors.

He is Honorary Secretary General of ITU-APT Foundation of India and Vice-President and Trustee of PTCIF and Co-chairs BIF committee on rural digital infrastructure. He founded NGN Forum in India. Conducts training programs in NGN technologies, broadband policy and regulation, interconnection costing in NGN era, spectrum management, IPV6, artificial intelligence, blockchain and blue-ocean strategy. He is first Indian recipient of IPv6 Hall of Fame – 2019 by Global IPv6 Forum and also the Chairman of India IPv6 Council.

Presently, he is working as Chairman, Bluetown, India & BIMSTEC, S. Asia.

Dr. Alice Maltseva is Director WAVIoT Project Development, Moscow, Russia. Obtained Bachelor and Master degrees from Moscow State University of International Relations and PhD in Economics from the same University.

She is a Senior Lecturer at the Moscow State University of International Relations and conducting practical research for the Ministry of Foreign Affairs to determine the main problems for Indian companies while investing in the Russian Federation.

From 2012 till 2019, she was the Managing Director for External Relations at the Special Economic Zone Technopolis Moscow, which is a key driver of the "new Moscow" – focused on technology and industry. This Special Economic Zone was set up to create, build and develop an innovative ecosystem within the city that has hugely favorable conditions for the localization of hi-tech companies and industry.

Since 2012, Alice is responsible for attracting investors from international and domestic markets towards localizing production within Moscow city limits. Alice is also involved in raising investment into private projects in IT, biotechnology, smart city technologies, eco-friendly products etc.

Alice is a prominent speaker at seminars and conferences globally, and is fluent in English, Hindi and Russian.

Keshav Sharma (b.26.05.1991) is a graduate in Electronics and Communications Engineering from Guru Gobind Singh Indraprastha University, New Delhi. He is a qualified telecom professional with 7 years of experience with a strong understanding of telecommunication technologies, policies and regulations.

Currently, he is working as Global Business Intelligence & Research, at Bluetown India, part of a Danish innovation company that developed a Wi-Fi-based efficient internet access technology, specially designed for the needs and conditions in rural areas of the world.

Authored articles in international technical journals. Also, as part of his assignments, worked on WhitePapers, Thought Leadership Reports, presentations, and articles on the Telecomsector covering the issues and challenges encompassing the sector.