Design, Implementation, and Research on Security Vulnerabilities of Smart Water Meter Network.

Capstone Project MINT 709

by

Sparsh Sharma

Master of Science in Internetworking

Department of Electrical and Computer Engineering

University of Alberta

Abstract

In the late 1940s and early 1950s in the United States and Europe, there were few mobile telephone systems, such as car-based telephone systems, prior to the introduction of cellular technologies. These systems used the push-to-talk technique, and communication was done over a single channel. The transmission and reception of signals were done in half-duplex mode with a single channel and a single antenna at each device, but due to limited capacity and bad service quality, those systems were not efficient. In order to enable a larger number of mobile stations, the Mobile Telephone System (MTS) and Improved MTS (IMTS) were introduced later.

The first generation (1G) provided basic mobile voice functionality, whereas the second generation (2G) added capacity and coverage. The third-generation (3G), which sought faster data speeds in order to open the doors to a genuinely "mobile broadband" experience, was followed by the fourth generation (4G). The fourth-generation (4G) provides access to a wide range of telecommunication services, including advanced mobile services, which are supported by increasingly packet-based mobile and fixed networks, The fifth generation of technology should be more intelligent and capable of interconnecting the entire globe. The fifth-generation is capable of providing a low latency network that uses low power, which was not present in fourth-generation technology.

The main objective of this project is to research on security vulnerabilities of smart water meter networks and choose the best communication technologies for SMW by comparing the existing technologies like LoRA and NB-IoT. Furthermore, we studied how massive IoT will be built on top of NB-IoT and one use case of massive IoT. In the end, we discussed the security vulnerabilities of Smart water meters and covers the potential vulnerabilities associated with various attack surfaces in the smart meter, their security and threat consequences, and lastly, it suggests appropriate security controls and countermeasures.

Acknowledgment

I would like to express my gratitude to my primary mentor **Mrs. Sandeep Kaur**, who guided me throughout this project. She offered me the freedom to work on my project while keeping ensuring that I stayed on track and did not stray from my subject's core. Without her wise instruction, my thesis would not have been possible.

I would also like to thank **Mr. Shahnawaz Mir**, my program coordinator, for providing me with such a wonderful opportunity and for allowing me to choose a project of my own choosing.

I wish to extend my special thanks to **Dr. Mike McGregor**, who allowed me to start this project.

I would also like to express my heartfelt gratitude to all the instructors, professors, seniors, classmates, colleagues, and the entire University of Alberta who has assisted me in this study, either directly or indirectly, and have been supportive and cooperative at all times in helping me achieve my goal.

Table of Contents

Table of Figures:

List of Tables:

1. Evolution of Cellular Technologies

1.1 Introduction

A wireless mobile communication technology in which users can send data, high-quality videos at high data rates.

In 1981, 1st generation system was introduced which we call as Advanced Mobile Phone System in North America than every 10 years a new mobile generations appeared like 2G Global System for Mobile Communication in 1992, 3G Wideband Code Division Multiple Access in 2001, and 4G standards International Mobile Telecommunications started to roll out in 2011, Then in the twenty-first century, Fifth Generation 5G Wireless Innovative System for Dynamic Operating Mega Communication Concept with high data rates and a large variety of services are introduced.

Developments

1.2 First Generation (Analog):

The first-generation mobile system is basically an analog cellular system, which is used for the transmission of speech services. It is named as an advanced mobile phone system, the bandwidth allocation for the channel is 30khz [1]. For medium access of multiple users, Frequency division multiple access (FDMA) schemes were adopted, and in order to carry voice traffic Frequency Modulation scheme was used. In 1979 the first cellular system became an operation in the world by the Nippon Telephone and Telegraph (NTT) in Tokyo, Japan, then in 1982, the AMPS was launched in the United States [2]. The system was allocated 40 MHz bandwidth within 800 to 900 frequency band (825-845 MHz for uplink and 870-890 MHz for downlink traffic, respectively) which is allocated by Federal Communication Commission (FCC) [3].

Disadvantages [4]:

- Poor voice quality
- Large phone size
- Poor battery life
- No security
- It makes use of the mobile phone with the analog signal more difficult, and this signal is suffered from an interference problem
- Limited capacity
- Poor hand-off reliability
- Very slow speed

1.3 2G:

The Drawbacks of the First Generation are low data rate, less capacity, and analog voice signal transmission and to improve the system, these analog voice signals are then converted into the digital cellular system. Short messaging services (SMS) and Multi-Media services are developed in the second generation. In terms of spectrum efficiency, 2G offers much higher than the first generation, and more advanced roaming was offered by 2G Systems.

2G cellular systems were deployed worldwide and they are represented by four major standards, namely Global System for Mobile Communication (GSM), Interim Standard (IS)-136, cdmaOne, and Pacific Digital Cellular (PDC). Except for IS-95 (cdmaOne), the other three system works on TDMA (Time Divison Multiple Access) for medium access and it allows multiple users to share the same channel in the frequency domain by allocating different time slot.

In countries like the United States, the frequency range assigned is 850 MHz -1900 MHz and for the rest of the world, it is 900 MHz – 1800 MHz. The maximum data rate of 2G cellular systems is 64 Kbps only [5].

1.3.1 Global System for Mobile Communication (GSM)

Global system for mobile communication supports two frequency bands, namely GSM-1900 and GSM-1800 with 124,372 and 299 radio channels. The global system for mobile communication was basically used for voice channels and the bandwidth allocated per channel is 200 kHz. The maximum data transmission speed is 270.83 Kbps [6].

1.3.2 Interim Standard (IS-136)

In IS-136, only three users can access the available channel of the 30 kHz frequency band. The maximum data transmission speed is 48.6 Kbps [6].

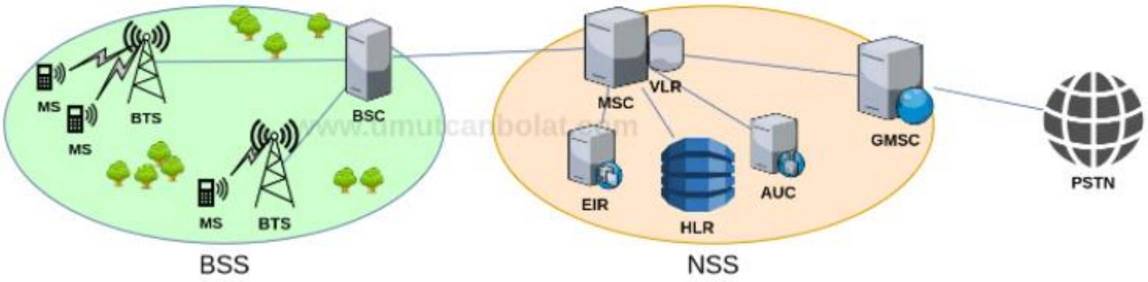
1.3.3 Pacific Digital Cellular System (PDC)

The pacific Digital cellular system contains a 25 kHz frequency band and only three users can access it within that band. The maximum data transmission speed is 48.6 Kbps, it almost the same as the Interim standard (IS-136) [6].

1.3.4 Code Division Multiple Access (CDMA)

CDMA is a multiple access technique in which unique code is assigned to each user using the channel at that time which increases the bandwidth utilization efficiency. and at the same time, a large number of consumers can use the same channel. [7].

1.4 2G/GSM Network Architecture



1: 2G Network Architecture Model [8]

The overall GSM network can be seen above. It is split into two sections. NSS (Network Station Subsystem) and BSS (Base Station Subsystem) (Network Switching Subsystem) [8] [9].

1.4.1 MS (Mobile Station)

A mobile subscriber is a device that can be a cell phone which is having a sim card that can communicate with the GSM network. MS is referred to as UE in 3G systems (User Equipment) [8] [9].

1.4.2 BTS (Base Transreceiver Station)

The BSC is the brain behind the BTS. It can control several BTSs. If two cells are under the authority of the same BSC, the BSC also controls the handover between them. (Handover between BTS and BSC). Alternatively, if transmission at a specific frequency is unfeasible due to certain reasons, the BSC can alter the mobile device's frequency within the same BTS. This is referred to as intra-BTS handover [8] [9].

1.4.3 BSC (Base Station Controller)

The BSC is the brains behind the BTS. It can control several BTSs. If two cells are under the authority of the same BSC, the BSC also controls the handover between them. (Handover between BTS and BSC). Alternatively, if transmission at a specific frequency is unfeasible due to certain reasons, the BSC can alter the mobile device's frequency within the same BTS. This is referred to as intra-BTS handover [8] [9].

1.4.4 MSC (Mobile Switching Center)

The MSC is the most important component of the Network Switching Subsystem (NSS). It is in charge of routing voice and SMS calls. MSC establishes a subscriber-to-subscriber circuit-switched connection [8] [9].

1.4.5 GMSC (Gateway MSC)

A GMSC is a type of MSC used to route calls outside of the mobile network. Whenever a call from the outside mobile network lands on the mobile subscriber, then it is routed through the GMSC. [8] [9].

1.4.6 HLR (Home Location Register)

HLR is a carrier's major and most essential database. It contains the subscriber information like its current position, similar to the GSM technology. [8] [9].

1.4.7 VLR (Visitor Location Register)

VLR contains the subscriber details which is quite similar to HLR and MSC will use that information in the future. MSC and VLR are always linked. The VLR connected to that MSC will request subscriber data from the HLR when an MS (Mobile Station) arrives in a new MSC area [8] [9].

1.4.8 EIR (Equipment Identity Register)

EIR maintains the database of mobile stations which keeps the track of whom to give access to and whom to not. This makes it possible to track down gadgets that have been misplaced or stolen. The IMEI number is used to identify mobile stations (International Mobile Equipment Identity) [8] [9].

1.4.9 AuC (Authentication Center)

AuC is a function that is used to verify the identity of a mobile subscriber trying to connect to the GSM network. Authentication is accomplished by the identification and verification of the SIM card's authenticity [8] [9].

Authentication center provides encryption and security whenever a user authenticates. TMSI (Temporary Mobile Subscriber Identity) is assigned to a subscriber to ensure privacy while they are under the authority of the MSC connected with the AuC. Instead of IMSI, TMSI is used. Because TMSI is generated at random, whereas IMSI is unique. As a result, the subscriber's identity is safeguarded [8] [9].

1.4.10 Advantages

- Data transfer rates of up to 64 kbps are possible.
- Instead of analog signals, digital signals are used.
- SMS and MMS (Multimedia Message Service) enabled services improved the quality of voice calls.
- It had a 30 to 200 kHz bandwidth.

1.4.11 Disadvantages

- Complex data, such as videos, cannot be handled.
- Strong digital signals were required.
- If digital signals are weak, there will be no network coverage in that location.

1.5 2.5 G

In the second generation, the data rate speed was very slow and limited, so 2.5G technology is developed to increase the data rate without changing the instruments. Various technologies for 2.5G are discussed below [10]:

1.5.1 High-Speed Circuit Switched Data (HSCSD)

HSCSD is a technique that is capable of communicating with circuit-switched communication media such as PSTN (Public Switched Telephone Network) & Integrated Service Digital Network (ISDN), the channel contains a 200 kHz frequency band & HSCSD uses two techniques to increase the data rate. First, By using the TDMA technique, different time slots can be used and each channel is divided into eight-time slots and each time slot is allocated to a different user, this makes the channel more efficient and can serve eight users on one radio channel. HSCSD also performs the error correction that enhances the quality of the radio channel [7]**.**

1.5.2 General Packet Radio System (GPRS)

To support the high-speed data transmission rates and without changing the network infrastructure, General Packet Radio Service (GPRS) was introduced in the year 2000. The data transmission speeds are 57.6 Kbps on a channel with a frequency band of 200 kHz.

At the radio access network there were two major enhancements were done when switching from GSM to GPRS, First enhancement allows users to occupy 5-time slots for uplink traffic 20 Kbps, and for downlink traffic, 114 Kbps are achieved. Secondly in the core network, two entities SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node) are introduced, and with the help of Packet Data Protocol (PDP), and GPRS Tunnelling Protocol (GTP) end-to-end IP services can be achieved.

Another advancement in GSM systems was achieved in 2003 with the development of Enhanced Data Speeds, which is a GPRS radio access network system expansion that increased data rates up to 384 Kbps. [11]**.**

1.6 Third Generation (3G)

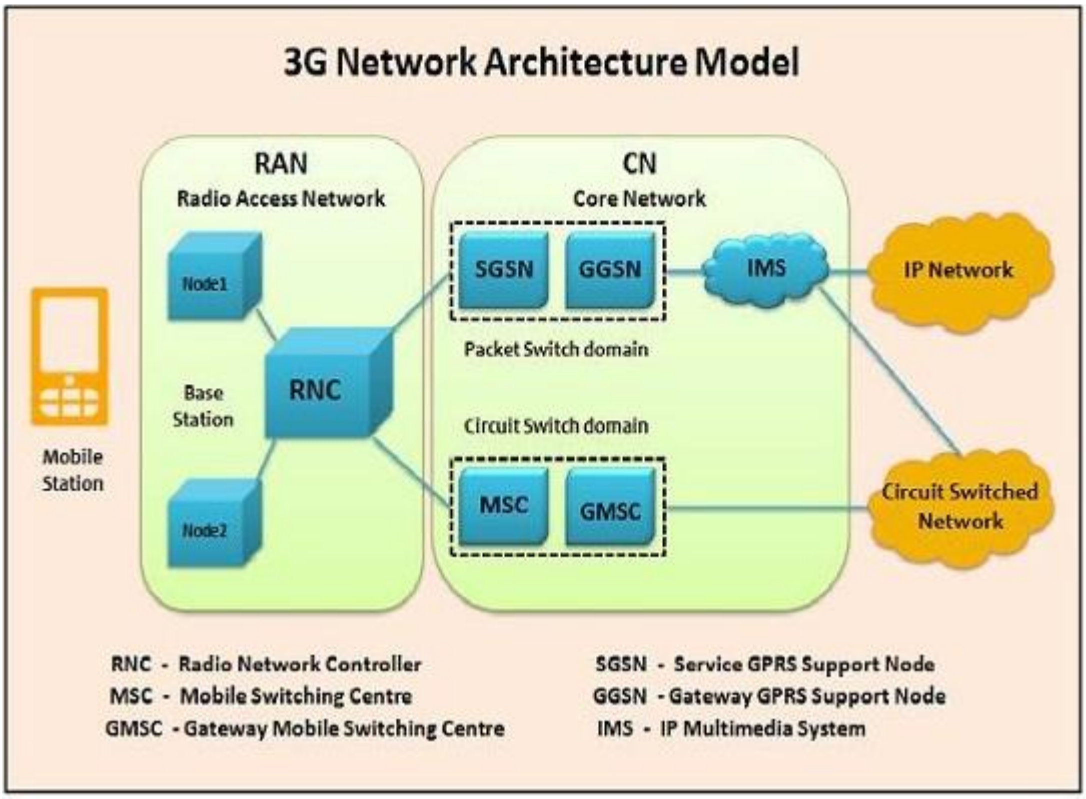
In the 3rd generation, as the data rate is high so video calling facility is possible, which was not possible with Edge [10]. In Edge, high volume data transfer was possible but when the packet goes through the air it behaves like a circuit switch which degrades the connection efficiency. The maximum data rates are increased up to 8 Mbps. QoS requirements are based on service for example, if the user wants to transmit voice, then lower data rates are assigned and for the video calls, higher data rates are assigned. An organization called the 3rd Generation Partnership Project has defined the mobile system that cooperates with IMT-2000 Standard [12].

UMTS is Europe's 3G wireless Standards which was ETSI (European Telecommunication Standard Institute) driven.

Universal mobile telecommunication system includes Wideband CDMA and a combination of CDMA & TDMA. CDMA is a mechanism in which each user is given a unique code and the entire available bandwidth is used after that. WCDMA uses a wide band of frequencies due to which more users can be accommodated as compared to CDMA [12]**.**

The only disadvantage of CDMA-2000 is that it is inconsistent with W-CDMA since it uses different chip rates and a different technique known as multicarrier. In the third generation, data is sent to packet switching and voice calls are interpreted through circuit switching. The bandwidth of the channel is 5MHz. 3G uses a layered architecture approach which enables the efficient use of voice and data services, the layered approach helps the network operators to roll out the new features as it is standardized with open interfaces, better spectral efficiency can be achieved [10] [6]**.**

1.6.1 3G Architecture:


3G Network Architecture Model
RAN
Radio Access Network
Node1
Base Station
RNC
Node2
Mobile Station
CN
Core Network
SGSN
GGSN
Packet Switch domain
Circuit Switch domain
MSC
GMSC
IMS
IP Network
Circuit Switched Network
RNC - Radio Network Controller
MSC - Mobile Switching Centre
GMSC - Gateway Mobile Switching Centre
SGSN - Service GPRS Support Node
GGSN - Gateway GPRS Support Node
IMS - IP Multimedia System

2: 3G Network Architecture Model [13]

As seen in the diagram above, the 3G Core Network has four major roles.

These are the following [13]:

1.6.2 Circuit Switching:

In a Circuit Switched Network, a dedicated channel is assigned to the users for a time window [13].

1.6.3 Mobile Switching Centre:

MSC oversees circuit-switched calls.

1.6.4 Gateway Management Switching Centre:

GMSC manages the link between internal and external networks and also manages the circuit-switched calls.

1.6.5 Packet-switching:

It employs an IP network, in which IP addresses are responsible for data transmission and reception between two or more devices. The following are the two functions associated with Packet Switching:

Mobility management, session management, billing, and communication with other regions of the network are all functions supplied by the SGSN (Serving GPRS Support Node) [13]**.**

1.6.6 GGSN (Gateway GPRS Support Node):

It's a complicated router that manages internal operations between external packet-switched networks and UMTS packet-switched networks [13]**.**

1.7 Advantages

- Existing systems will be relieved of overcrowding by the new radio spectrum.
- More bandwidth, security, and dependability are all advantages.
- Interoperability is the capacity for service providers to communicate with one another.
- There are two types of data rates: fixed and variable.
- Data rates are asymmetric.
- Devices are compatible with the previously deployed networks.
- Devices that are always connected.

1.8 Disadvantages

- Different handsets are required.
- Inadequate bandwidth.
- They are more expensive and necessitate a closer base station.
- Spectrum license cost.
- The cost of 3G phones is really high.
- Handset with 3G capability.

1.9 Fourth Generation (4G) Long Term Evolution (LTE)

4G Systems are designed to operate 5 to 10 times the data rates of 3G give enhanced video quality with less distortion. Higher Spectral efficiency can be achieved with a lower cost bit than 3G systems [14]. On June 23rd, 2005, the first field trial was conducted in Tokyo, Japan, and NTT DO CO MO was successful in achieving the 1Gbps packet transmission.

The data speed provided by the 3G was not up to the mark as per the ongoing usage of Internet access via mobile phones. In 2008, the ITU Radiocommunication sector came up with the solution and developed a new system known as IMT-Advanced. The major requirements for this system include supporting of 1Gbps peak data rate, roaming capability worldwide, scalable bandwidth up to 100 MHz, Interoperable with 2G and 3G systems, and improved spectral efficiency, those who could meet up these requirements are termed as 4G systems [15]. Because LTE does not match the standards of 4G, the 3GPP developed LTE-Advanced, which is a major standard for 4G systems. LTE (Long Term Evolution) employs multi-carrier CDMA or OFDM (orthogonal frequency division multiplexing), as well as FDD and TDD operations, and Single Carrier Frequency Division Multiple Access to improve uplink power efficiency (SC-FDMA). Flexible bandwidth allotment up to 20 Mhz allows for larger data rates; in LTE systems, maximum uplink speed is 50 Mbps and maximum downstream speed is 100 Mbps.

Due to such high data rates, bandwidth-hungry applications like online gaming, live streaming, Videoconferencing, and voice-over IP are supported by 4G systems [16].

In 4G Architecture, Terminal mobility is a feature that can provide wireless service at any time, anywhere. It allows users to roam across the geographic boundaries of the wireless network. For efficient delivery of services to the mobile users, mobility management is the main concern for the market so they developed the service where they can proactively determine before the service is delivered. Mobility management has two important components- Location management and Handoff management.

1.9.1 4G LTE Architecture:

1.9.2 Mobility Management

Mobility management is one of the most essential and difficult problems for wireless communication to maintain the mobile user connection as the number of subscribers is increasing day by day. [17].

1.9.3 Location Management

Location Management tracks the location of the mobile nodes as it moves to different nodes. It does two major things 1) location registration and 2) paging.

In location Management the mobile phone sends signals to make the network of its current location so that the database is kept updated instantly. Once the location of the subscriber is updated in the database then the paging process is invoked, and based on that information the paging or call delivery happens and it queries with the network and delivers the call successfully to the mobile device.

Following issues must be addressed while designing the Location Management: (i) signaling overhead and latency in the service delivery should be minimized (ii) Guaranteed Quality Of service should meet for the applications (iii) Areas where too much congestion and overlapping network an efficient system must be designed so at a time of registration network selection becomes smooth and system should decide where and how frequently location information should be stored with the exact location of a mobile device with specific time frame.

1.9.4 Handoff Management

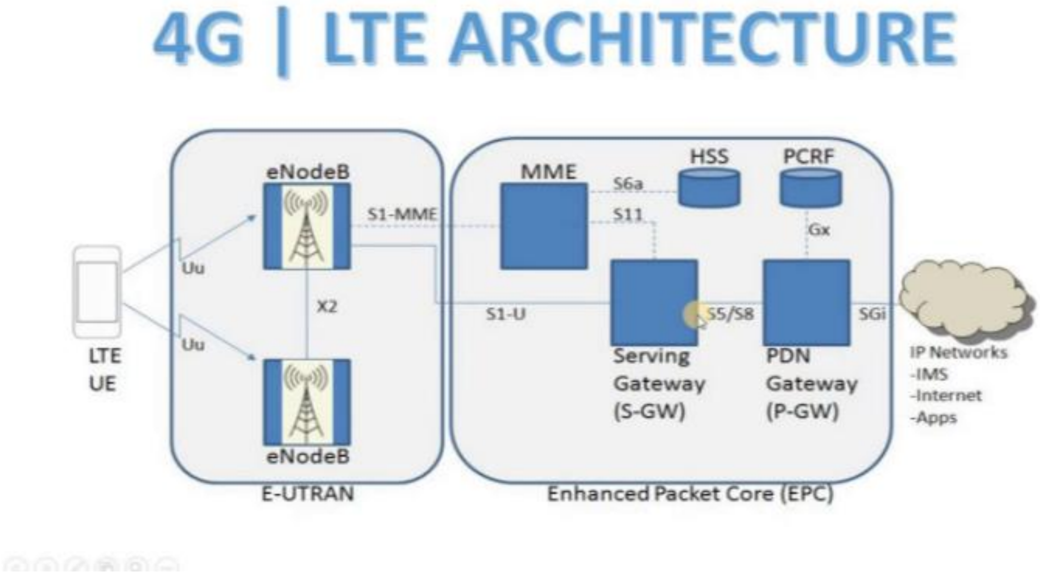
Process of keeping the mobile node active when it moves from one access point to another. The handoff process is divided into three steps, In the first step whenever a mobile device changes its network position the handoff process is triggered. As the handoff process is triggered so the next step is to look for resources for the network. Finally, as per the agreed QoS data flow happens between the old connection path to the new connection path.

The mobile device keeps on updating its location so there are two types of handoff: (i) intra-system handoff (ii) Inter-system handoff.

Intra-system handoff occurs when signal strength becomes low in the serving base station (BS) that is below the certain threshold value and typically occurs in homogeneous networks.

Inter-system handoff occurs between the heterogeneous networks it may arise i) when the user moves out from the serving network and enters the overlying network, ii) When a connected user chooses to handoff to a strong network for the subscriber requirement.

The design of hand-off management must address the following issues: (i) For processing the hand off messages requires more power, so make it more reliable power requirements and signaling overhead should be minimized, ii) quality of services should be fixed as per the requirement, iii) usage of network resources should be done in an efficient manner, iv) handoff mechanism should be robust and reliable [17].



3: 4G LTE Architecture [18]

1.9.5 The PDN Gateway (P-GW)

PDN is also in charge of data traffic between S-GW and other networks such as IMS or the internet. This function can be described as a portal to the internet. One of P-key GW's responsibilities is to assign IP addresses to UEs. It's in charge of sorting downlink user IP packets into the various QoS-based bearers [18] [19].

1.9.6 Home Subscriber Server (HSS):

This server is in charge of keeping customer profile data as well as creating authentication vectors that are submitted to MME. It also contains data on the PDNs to which the user has access. It also has the job of storing dynamic data, such as the identity of the MME to which the user is currently associated or registered. The authentication center (AUC), which creates authentication and security key vectors, may likewise be included in the HSS.

Policy and Charging Rules Functions (PCRF): This group is in charge of supplying QoS data to P-GW. Rules for billing, flow control, and traffic priority may all be included in this data.

1.9.7 Serving Gateway (S-GW)

The Serving Gateway (S-GW) is in charge of exchanging traffic between the P-GW and the 4G RAN. IP packets sent by the user are forwarded by S-GW. When UE switches eNodeBs, it acts as a local mobility anchor for data carriers. S-GW is also in charge of some administrative tasks, such as collecting information from networks concerning charging.

1.9.8 Mobility Management Entity

The Mobility Management Entity (MME) is in charge of providing User Equipment with mobility and session management. The control node is in charge of communicating between the UE and the CN. NAS protocols are the protocols that flow between the UE and the CN. Bearer management and connection management are the two core functionalities of MME. The establishment and maintenance of bearers are also part of bearer management. Connection management is concerned with the establishment of a secure connection between the network and the user equipment [18] [19].

1.10 Challenges and Issues

Different types of heterogeneous networks are coupled in 4G networks to facilitate handoff, and these systems are designed independently to handle different data speeds, different types of services, and different sorts of users. The development of 4G networks has significant hurdles in terms of ensuring secure and efficient operations. In 4G systems, both mobile users and wireless networks work together to provide the best data speeds and service to the user.

Challenges are listed below:

A. Network Discovery: 4G network devices are multi-access devices, which means they can access numerous networks for different purposes at the same time. As a result, the terminal must be able to discover which networks are available. This problem can be mitigated by employing the Software Defined Radio approach. Components that were formerly implemented in hardware are now implemented using software on a personal computer or embedded systems under this technique.

B. Access Technologies: Mobile users migrate between access networks to preserve service continuity and quality on a 4G network, which consists of several radio technologies that may overlap radio coverage. The 4G network is a heterogeneous network and coping with such a large network will almost certainly result in design challenges. Furthermore, choosing a network that will meet the existing service's QoS needs will be difficult.

C. Network Conditions: The wireless network's network circumstances, such as bandwidth, jitter, and delay, may fluctuate, resulting in a fluctuation in the service quality given to the user. In wireless networks, concerns such as maintaining service quality and coping with network fluctuation must be addressed.

D. Security: Each network has a distinct level of security, and the more intricate the network is, the more vulnerable it is to assaults. Monitoring, detecting, and analyzing wired networks is difficult, but monitoring, detecting, and analyzing a combination of wired, wireless, and mobile networks is much more complex.

1.11 Advantages of 4G system

i) **More Devices and Applications**: 4G network bandwidth is higher so more devices can be connected to use data-consuming applications.

ii) **Speed**: The speed of 4G Systems is up to 100 Mbps for high mobility ad 1Gbps for low mobility.

iii) **Faster Response time:** One of the major benefits of using 4G technology is the lower latency of about 10ms.

1.12 Disadvantages:

The operational area is one of the primary disadvantages of using 4g Systems. Existing networks do not adequately serve rural areas and many buildings in urban areas. Other disadvantages include a higher battery usage compared to other systems, which is difficult to achieve and requires complex hardware. Another downside of adopting 4G networks is incompatibility, which forces customers to purchase a new gadget that supports 4G.

1.13 5G technology of Mobile Communication:

When it comes to 5G technology, the mobile consumer has taken precedence over all others. It makes use of mobile phones with extremely high bandwidth, and the average mobile user has never seen data at such a fast pace.

Above the 4G-Advanced standards, 5G represents the next significant phase of mobile communication technologies. IEEE 802.16 is a Wireless Broadband standard that standardizes the air interference functions associated with wireless local loops. The 5G technology has capabilities that make mobile technology more powerful. Users can connect their 5G phones to laptops to access high-speed internet. The fifth generation has a data capability of over 1Gbps, As an advancement calls are handled by software that is cloud-based. The fundamental benefit of 5G technology is that it allows users to connect to different wireless technologies and switch between them, thanks to IPv6 capability. 5G technologies have a maximum data throughput of up to 10 Gbps.

1.13.1 Key terms of 5G Technology:

1) 5G is a full wireless communication system with additional capabilities such as HD TV and high speed, allowing users to watch high-quality television programs.

2) It can also be referred to as WWWW: Worldwide Wireless Web because data transfer speeds are faster than prior generations.

3) 5G is a wireless technology where users can connect to 2G,3G,4G, and 5G mobile networks at the same time and switch between them.

4) Cognitive radio technology enables different radio technologies to efficiently share the same spectrum by locating unused spectrum and delivering it according to the technology needs. This radio resource management is carried out in a distributed manner, utilizing software-defined radio.

1.13.2 Protocol Stack for 5G

Application Layer	Application (Services)
Presentation Layer	
Session Layer	Open Transport Protocol (OTP)
Transport Layer	

Network Layer	Upper Network Layer
	Lower Network Layer
Data Link Layer (MAC)	Open Wireless Architecture (OWA)
Physical Layer	

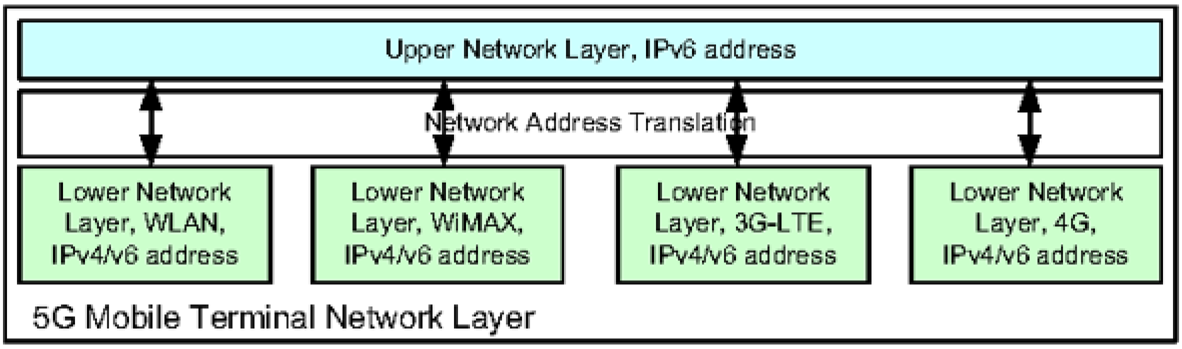
Physical/MAC layer

OSI layer 1 (Physical layer) and layer 2(Data link Layer) define the wireless technology, for these two layers 5G mobile network will be Open Wireless Architecture [20].

Network Layer

The network layer is the IP (Internet Protocol) because there is no competition today on this level. The IPv4 has several problems such as limited address space has no QoS support per flow. These issues are solved in the IPv6 but that increases the packet header [20].

The two layers are the lower network layer and the upper network layer. Network address translation is done between the upper layer (IPv6) and the lower layer (IPv4 & IPv6)


Upper Network Layer, IPv6 address
Network Address Translation
Lower Network Layer, WLAN, IPv4/v6 address
Lower Network Layer, WiMAX, IPv4/v6 address
Lower Network Layer, 3G-LTE, IPv4/v6 address
Lower Network Layer, 4G, IPv4/v6 address
5G Mobile Terminal Network Layer

4: 5G Mobile Phone Network Layer [20]

Open Transport Protocol (OTA) Layer

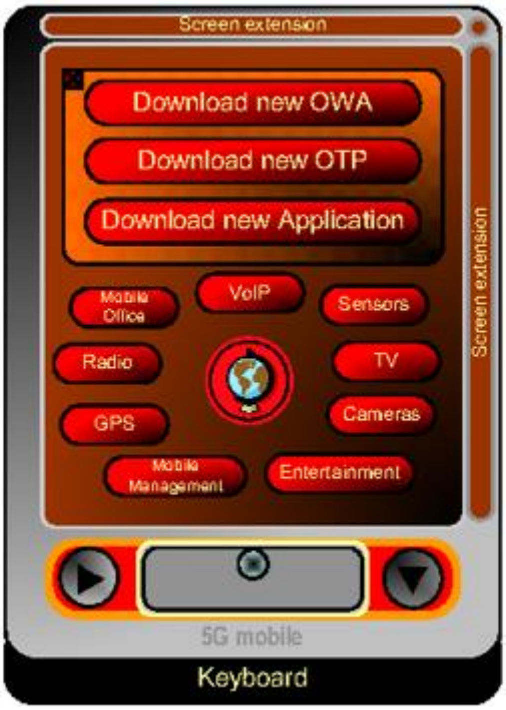
In the Transport layer, the mobile and wireless networks are different from the wired network. The basic idea of all TCP versions of the lost segment is due to network congestion but in the wireless network it is due to the bit error ratio in the radio interface; moreover, the 5G mobile should be compatible to download the TCP, RTP, or new transport protocol) which is targeted to a specific wireless technology this is called Open Transport Protocol (OTP) [21].

Application Layer

In the application, the request from the 5G mobile network is to provide the QoS management over a variety of networks. Today, the mobile phones themselves chose the wireless interface for internet service without knowing the QoS history to select the best wireless connection.

The 5G mobile database will contain the parameters such as delay, losses, and bandwidth which can be used by the mobile terminal to provide the best QoS service. In the future, there will be low complexity of implementation and efficient means end-users and wireless infrastructure [21].

1.13.3 5G Mobile Phone Design



5: Mobile Phone Design [21]

The 5G is being developed to meet the QoS requirements for major applications like Video chat, Mobile TV, Video broadcasting. The main role of 5G is to provide excellent service to the user by giving more RF coverage. [21].

1.13.4 Evolved Packet Core (EPC)

The Evolved Packet Core is an IP-based core network architecture that supports the convergence of licensed (2G/3G/4G) and unlicensed (Wi-Fi) radio technologies by providing data services. EPC also enables IP-based communication and services for both wireless and wireline networks, as well as a unified subscriber identification for mobility, billing, policy, and charging.

BSC's major job is to collect calls from many base stations, allot radio channels, and facilitate handoff between base stations before passing the call to a more centralized mobile switching center. [21]**.**

1.14 5G Core Network

While the 4G Core has grown into the 5G Core, it has gained new capabilities and some functions have been separated into several functions, the overall architecture has remained the same. The separation of control and user plane tasks is one of the most fundamental differences between 4G and 5G core networks [19] [22].

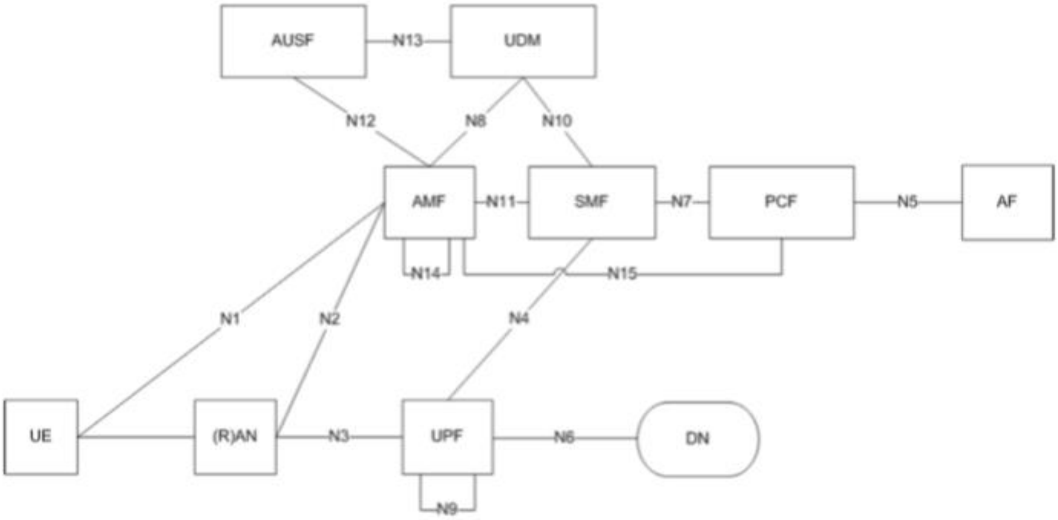
As previously stated, the 5G core network includes more functions due to the division of various functions. The following are the 5G Core Network Functions:

- Access and Mobility Management Function (AMF) supports: Termination of NAS signaling, NAS ciphering & integrity protection, registration management, connection management, mobility management, access authentication and authorization, security context management.
- Session Management Function (SMF) supports session management (session establishment, modification, release), UE IP address allocation & management, DHCP functions, termination of NAS signaling related to session management, User plane function (UPF) supports packet routing & forwarding, packet inspection, QoS handling, acts as external PDU session point of interconnecting to Data Network (DN), and is an anchor point for intra- & inter-RAT mobility.
- Policy Control Function (PCF) supports unified policy framework, providing policy rules to CP functions, access subscription information for policy decisions in UDR.
- Authentication Server Function (AUSF) acts as an authentication server.
- Unified Data Management (UDM) supports the generation of Authentication and Key Agreement (AKA) credentials, user identification handling, access authorization, subscription management.

- Application Function (AF) supports application influence on traffic routing, accessing NEF, interaction with policy framework for policy control.
- Network Exposure Function (NEF) supports exposure of capabilities and events, secure provision of information from an external application to 3GPP network, translation of internal/external information [19] [22]**.**
- NF Repository function (NRF) supports service discovery function, maintains NF profile and available NF instances.
- Network Slice Selection Function (NSSF) supports selecting of the Network Slice instances to serve the UE, determining the allowed NSSAI, determining the AMF set to be used to serve the UE.

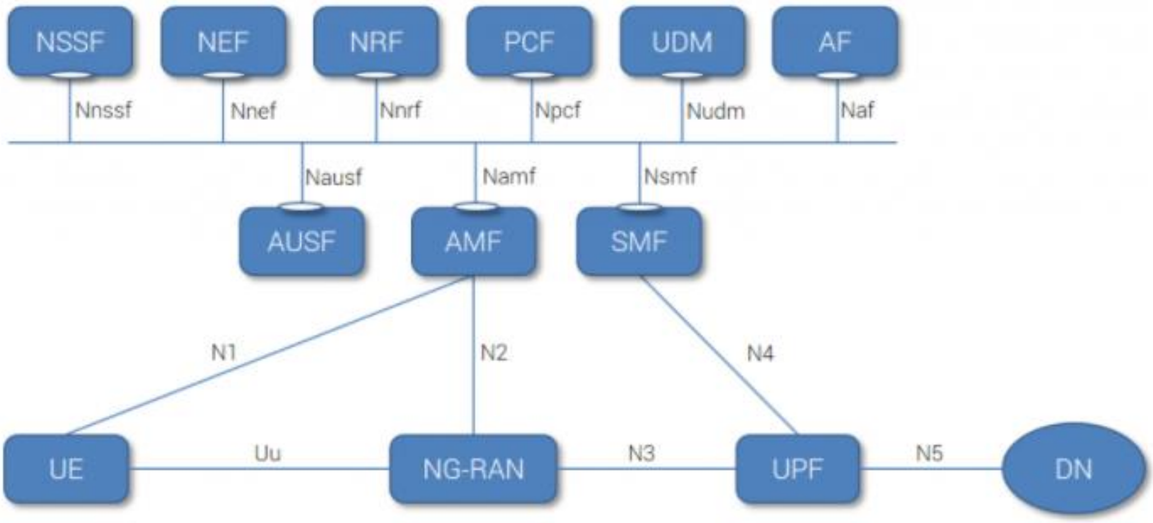
The 5G Core Network is represented in two ways. The reference point architecture and the service-based architecture are two of them. They almost tell the same story in terms of functional features.

It is considerably more akin to classic 3GPP architecture in terms of reference point architecture, which defines functions and interfaces between them. The disadvantage of this architecture is that adding a new network function to the system will involve reconfiguring the entire architecture [19] [22].



6: Reference Point Architecture of 5G Core Network [22] [19]

It has the advantage of being reusable APIs. Both designs share the same functional parts and the same user-plane processing channel between the UE and the rest of the network. The control plane is where reference point architecture and service-based architecture vary the most. The control plane functions have no set interfaces, thus NRF is used to discover and communicate with one another.



7: Service-based Architecture of 5G core Network [19]

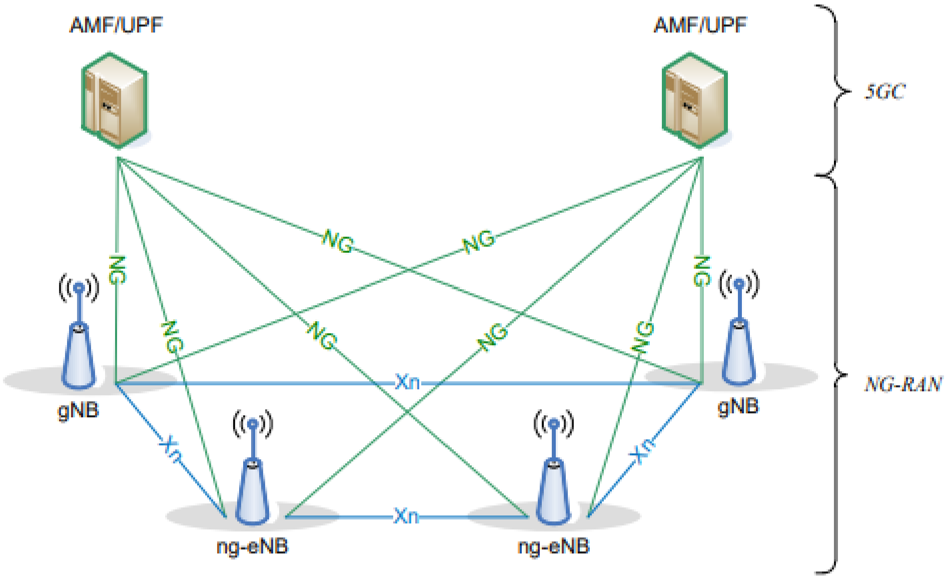
The above architecture depicts the control plane and data plane. The upper part is mostly responsible for signaling between different core network functions and the lower is for data traffic.

1.14.1 NG-RAN Architecture:

An NG-RAN node is either:

- a gNB, providing NR user plane and control plane protocol terminations towards the UE; or
- an ng-eNB, providing E-UTRA user plane and control plane protocol terminations towards the UE.

gNBs and ng-eNBs use Xn interface to connect each other and it is also connected to 5GC, more specifically to the Access and Mobility Management Function. [23].



8: NG-RAN in relation to the 5G system [23]

1.14.2 Functional Split

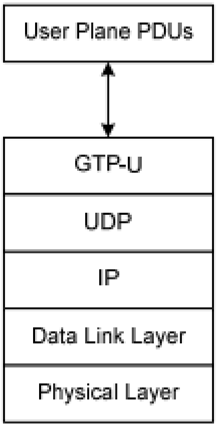
The gNB and ng-eNB host the following functions:

- Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);
- IP header compression, encryption, and integrity protection of data; - Selection of an AMF at UE attachment when no routing to an AMF can be determined from the information provided by the UE.
- Connection setup and release.
- Scheduling and transmission of paging messages.
- Scheduling and transmission of system broadcast information (originated from the AMF or OAM);
- Measurement and measurement reporting configuration for mobility and scheduling.
- Transport level packet marking in the uplink.
- Session Management; - Support of Network Slicing.
- QoS Flow management and mapping to data radio bearers.
- Support of UEs in RRC_INACTIVE state.
- The distribution function for NAS messages.
- Radio access network sharing.
- Dual Connectivity.
- Tight interworking between NR and E-UTRA

1.14.3 Network Interfaces

1.14.4 NG User Plane

The NG-RAN node and the UPF has the NG user plane interface sandwiched between them and the network layer is built on top of IP transport. GTP-U carries the protocol data units between NG-RAN and UPF. The user plane protocol stack of the NG interface is shown below [23]**:**

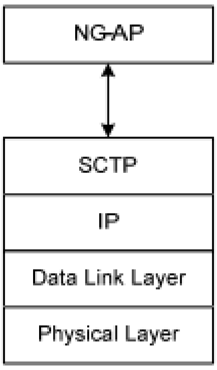


9: NG User Plane [23]

1.14.5 NG Control Plane

Between the NG-RAN node and the AMF, the NG control plane interface (NG-C) is defined. IP transport serves as the foundation for the transport network layer.

SCTP is added to IP for the reliable delivery of signaling messages. SCTP layer transfer the application layer messages. In the transport, IP layer point-to-point transmission is used to deliver the signaling PDUs [23].



10: NG control Plane [23]

NG-C provides the following functions:

- NG interface management.
- UE context management.
- UE mobility management.
- Transport of NAS messages.
- Paging.
- PDU Session Management.
- Configuration Transfer.
- Warning Message Transmission.

1.15 FUTURE SCOPES

From the physical layer up to the application layer, 5G technology is designed as an open platform. Many advancements have been made, and the new 5G technology is now available in the market at low prices and with greater reliability than previous technologies.

For enthusiastic users, 5G technology provides great resolution, allowing us to view an HD TV channel and high-quality videos on our mobile phones without interruption. A new revolution in 5G technology is set to commence, as this technology will put standard desktops and laptops in direct competition, lowering their market value.

2. Internet of Things (IOT): An Overview and its Applications

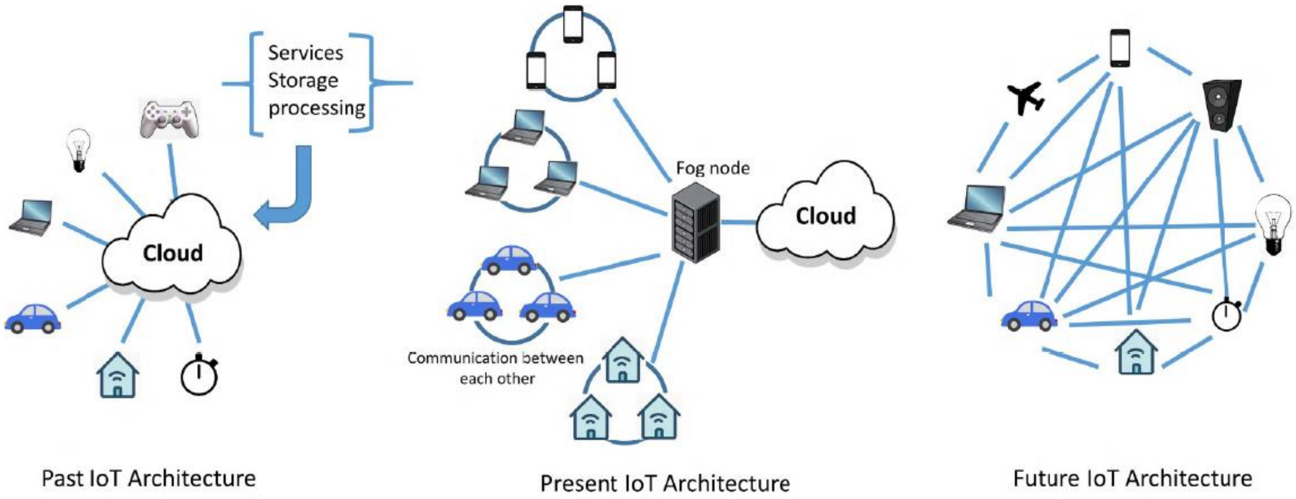
The Internet of Things (IoT) is a cloud-based "universal global neural network" that connects numerous gadgets. To face this new challenge, the Internet of Things (IoT) is intelligently connected devices and systems made up of smart machines talking with other machines, infrastructure, Radio Frequency Identification (RFID), and sensor network technologies will be developed. As a result, massive amounts of data have been collected, saved, and processed into meaningful actions that can "command and control" the things and technologies that can make our lives much easier and safer. Internet of things makes physical devices send and receive data without interruption. Certain IoT applications aim to automate various operations and empower physical objects to behave without the need for human interaction. Existing and forthcoming IoT applications have a lot of promise for improving consumers' comfort, efficiency, and automation. To create such a large network, strong levels of security, privacy, authentication, and attack recovery are required.

2.1 INTRODUCTION

The rate at which physical devices around the world are connected to the Internet is continuously expanding. The researcher says there will be around 8.6 billion connected IoT devices and the number is expected to grow by 22.4 billion by 2022 [24]. The number of machine-to-machine (M2M) connections is expected to grow from 5.8 billion in 2016 to 28 billion in 2024 [24].

By itself, this increase in numbers indicates IoT to be one of the most important emerging markets that might become a foundation of the growing digital economy. [25].

The figure shows the past, present, and future of the IoT. In the Future, the devices are not only expected to connect to the internet and other local devices but are also expected to communicate with other devices on the internet directly. There is another concept of social IoT is emerging, SIoT will enable different social networking users to be connected to the devices and users can share the devices over the Internet[26].



11: Present and Future architecture of IoT [26]

2.1.2 Comparison of IT devices and IoT devices

Table 1 Comparison of security of IT devices and IoT devices.

Widespread IT security	IOT Security
Devices are resource-rich	IOT devices need to be carefully provisioned with
Wide security and lower capabilities	Only lightweight algorithms are preferred

complex algorithm are implemented	
High security is due to similar technology.	IoT devices that use diverse technology generate a lot of data streams, which increases the attack surface.

IoT applications have a vast spectrum so maintaining security and privacy is a big challenge, without a trusted and interoperable IoT system the IoT applications cannot reach high demand and may lose all their potential. IoT and cellular networks have their own security issues such as privacy issues, authentication issues, management issues, and information storage.

The above table summarizes various factors due to which securing an IoT environment is much more complex than securing IT devices. Due to all these issues and vulnerabilities, IoT applications are more prone to cyber threats. Mirai attack in the last quarter of 2016 was estimated to infect around 2.5 million devices connected to the internet and launch distributed denial service (DDoS) attack [27]. Hajime and reaper are the botnet attacks that are launched against IoT devices. [27].

The major disadvantage of using IoT as it is very low power and less secure so these devices can be deployed into the home and corporate networks which makes it very easy to access the user data. Attackers around the world attack the implanted devices in human bodies to track the condition of the organs or can manipulate the data in it. [26].

2.2.1 IOT ARCHITECTURE

Three-layer Architecture

IoT is frequently composed of perception layer, network layer, and application layer as shown in the table below [26]:

Application Layer:

Intelligent building	Intelligent traffic	Intelligent logistics
Cloud Platforms	Middleware	Data analysis

Network Layer:

Special line network	Mobile comm.	Satellite comm.

WiFi	Zigbee	Ad-hoc

Perception Layer:

Camera Pickup	Body induction	Automatic recognition
Sensor	RFID/EPC	Timing & Positioning

Three-Layer Architecture of IoT

2.2.2 Perception layer:

The perception layer is the bottom layer. It collects the information person, physical object by use of perception tools. There are many perception tools available for a specific type of IoT application, which includes various types of sensors, RFID, timing and poisoning terminal (GPS), human body infrared sensor, and automatic recognition equipment. When a gathering of information is done then this layer will do the processing and packaging of the information and during this process network layer will send control information through the executive devices [28].

2.2.3 Network Layer:

It is the middle layer of the three-tier architecture and can also be called as transmission layer. It transfers the information from the perception layer to the application layer safely and reliably, since it is a transmission layer, so it includes short distance and remote data transmission. The short distance data transmission depends upon wired or wireless communication networks for example WiFi, Ad-hoc, Zigbee and remote data transmission depends upon Mobile communication, satellite communication, etc [28].

2.2.4 Application layer:

The application layer collects information from the below two layers and analyzes it according to the applications. Application layer work as an interface between users and IoT device to deliver the application data according to the user needs. For example, intelligent building, intelligent traffic, vehicle navigation, and security monitoring. To provide support to the above intelligent applications requires cloud computing technology, data mining technology, middleware technology, etc [28].

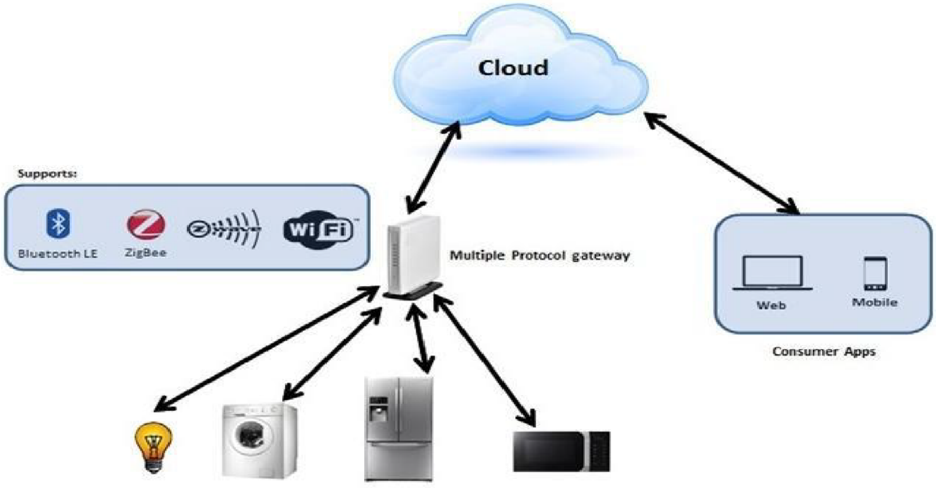
2.3 APPLICATIONS OF IOT IN DIFFERENT FIELDS

2.3.1 IoT in Industry:

Monitoring of oxygen levels and toxic gas inside chemical plants to ensure the safety of the workers. It also keeps an eye on the temperature in the food plant to ensure that the meat stays fresh. Information is collected from the controller area network (CAN) Bus to send real-time alarms to emergencies.

2.3.2 IoT for Smart Home:

Internet of things plays a vital role in making an automated home into a smart home. With different types of sensors, smart systems, IoT connects everyday objects to a network, enabling them to communicate with each other without human intervention or input, moreover, you can connect your smart home with your smartphone, tablet, or computer.



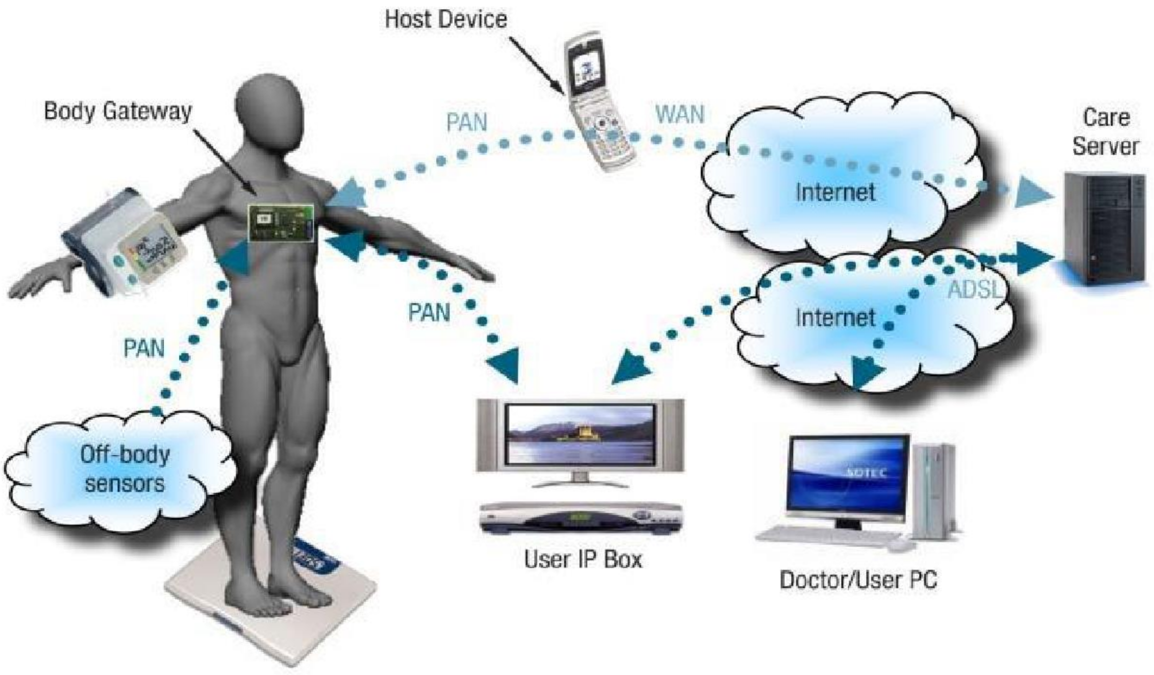
12: IOT for smart home [29]

2.3.3 IoT for Agricultural Production:

IoT in the agriculture field collects the information from the sensors to maintain the quality of the crop and to prevent it from insects, but sometimes due to slight changes in condition and a poor prediction, that makes it very difficult to control agriculture products. To overcome it, IoT based monitoring system analyzes the crop environment and methods to improve the efficiency of decision making by analyzing the harvest statistics.

2.3.4 IoT for Health Care:

IoT in the healthcare application is used to monitor and observe the health condition of the patient especially it is more useful when patient location is remote. It can remotely monitor the patients be affected by various disorders thus it increases the quality of care and reduces the cost of care [29].



13: IOT in Healthcare. [29]

2.3.5 Smart Retail

In Smart retail various applications have been developed to monitor the storage conditions of the goods as they move along the supply chain. IoT can be used to track the location of the products in the big warehouses so that stocking can be done easily. The use of augmented reality techniques to give the experience of online purchasing to offline merchants has also been developed. Some of these companies include Apple, Home Depot, JP Morgan Chase, and Sony [30].

2.4 Five Key Challenge Areas

2.4.1 Security:

For any IoT, application security is the biggest concern where all big companies spend lots of money to protect their infrastructure. There are a lot of chances of malware entering the IoT network because it connects a lot of devices in the network. The integration of middleware and machine-to-machine communication produces lots of complexity and security issues.

2.4.2 Trust and Privacy:

New compliance frameworks to deal with the IOT's serving to distinguish it from others' problems can evolve. Social and political issues during this space may make it difficult for IoT adoption

2.4.3 Complexity, Confusion, and integration problems:

Testing & integration of IoT devices is a big challenge due to its multiple platforms' support and compatibility with various protocols. The uncertainty about what is happening around evolving standards is nearly bound to slow adoption.

2.4.4 Evolving Architectures, protocol wars and, competitive Standards:

With such a large number of players attached to the IoT, there are sure to be in progress area wars as legacy corporations ask to shield their proprietary systems blessings and open systems proponents try and set new standards.

2.4.5 Concrete use cases and compelling worth propositions:

Lack of clear use cases can cut down adoption of the IoT through technical specifications, theoretical uses, and future ideas that might serve for a few early adopters, thought adoption of IoT would force reasoned, customer-oriented communications and electronic communication around "what's in it on behalf of me." [31]

3. IoT based Smart Water Metering System

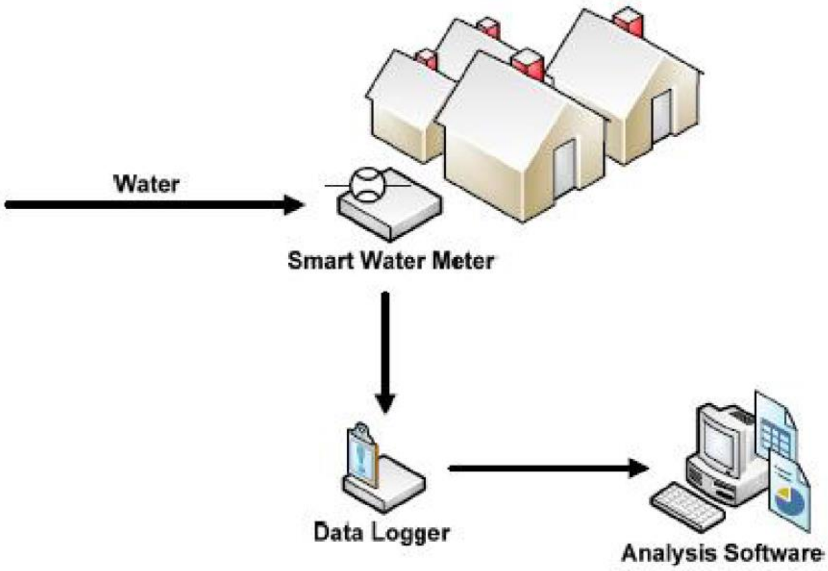
3.1 Introduction

More than 75 percent of the earth's surface is covered with water. Despite the seeming abundance of water, 97.5 percent of all water on Earth is salt water, leaving only 2.5 percent as freshwater. Nearly 70% of that freshwater is frozen in the icecaps; the rest is available as soil moisture or in deep underground aquifers as groundwater that is not suitable for human consumption. Only 1% of the world's freshwater is available for direct human use.

All types of life require water to survive. It is required in practically all human endeavors. Safe drinking water is today considered a universal human right. As a result, water conservation is becoming increasingly vital around the world as a result of population expansion, changing lifestyles, and climate change. Understanding water use is the first step in water conservation. Smart water meters are an integral part of the smart metering system.

3.2 Smart Water Meter

When the reality is so different, it's shocking to see how much uncertainty, misinformation, and fiction remains around smart water meters. SWM is an electronic device to read the water consumption of clients and provide them bills remotely.



14: Components of the typical Smart Water set-up for a residential household [32]

Smart water meters essentially fulfill three functions: they record, collect, and send real-time (or virtually real-time) water usage readings automatically and electronically. The data is in the form of an electrical signal that may be captured, logged, and analyzed in the same way as any other signal [32] [33]**.** Furthermore, modern data distribution technologies enable this signal to be easily delivered to any computer as well as to a central point for analysis or to a website for client viewing. When questioned, the data logger uploads water consumption data to a server, providing a water consumption value for the specified time period [34].

Smart meters can then convey the collected data to a wide range of people, including utility managers, consumers, and facility authorities. The components of a typical smart meter set-up for a residential household are shown in Figure 14.

3.2.1 Components of Smart water metering

The three primary functions of a smart water meter are to capture, collect, and communicate up-to-date information in real-time. The data is supplied in the form of an electrical signal that may be caught at a smart water meter, logged in a data logger, and analyzed with analysis software. When the data logger is questioned, it sends the water consumption data to a server, which returns the water consumption value for the specified time period.

Smart meters can then convey the collected data to a wide range of people, including utility administrators, consumers, and site managers. The components of a typical smart meter set-up for a residential household are shown in the diagram. SWM has three components namely, transmitter, data memory, and hardware for water flow detection.

3.2.2 Transmitters

The most fundamental component of a smart water meter is a transmitter (SWM). Wireless data transfer can be enabled by attaching a transmitter to an accumulation meter. Water meter readings are transmitted using radio waves by transmitters to a remote place (average range 1KM). However, data transmission over long distances necessitates the use of a GSM transmitter. Radio transmitters are used in most smart metering applications because they are less expensive than GSM transmitters.

3.2.3 Data loggers

Data loggers with data storing capabilities can be added to transmitters to improve them even more. This gadget is capable of both storing and transmitting interval data.

The time scale of the data recorder can be adjusted from one recording per second to one recording per month. Interval data recorder makes leak detection easier by the steady flow of the water. There is a lot of software out there that can determine the exact amount of water wasted over a period of time.

15: Smart water meter with data logger

3.2.4 Gateway

A gateway is a device that receives data from one or more data transmitting devices or SWM and transfers it to a remote destination. Radio transmitters are often used by smart water meters and data loggers to convey information to a gateway, which then relays all end-user data via telecom networking.

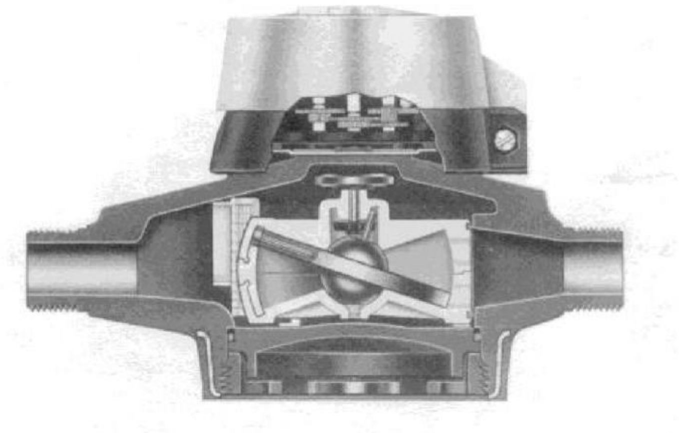
3.3 Types of smart water meters

Positive displacement and velocity meters are the two primary types of meters. There are variances in each of these meter types, giving the impression that there are multiple separate varieties.

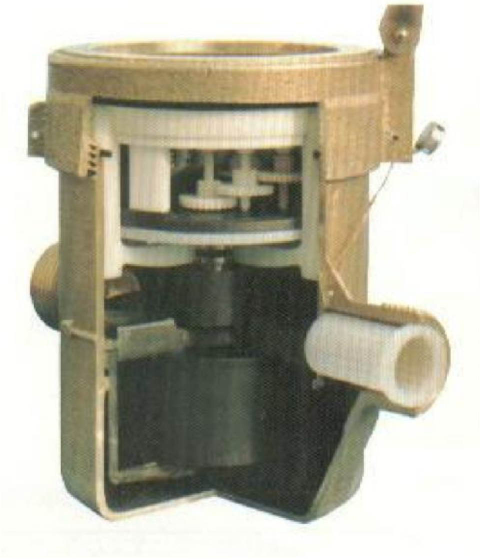
3.3.1 Positive Displacement Meters

A known volume of liquid in a tiny compartment flow with the flow of water in this sort of meter. Positive displacement water meters work by filling and emptying these compartments on a regular basis. The number of times these compartments are filled and emptied is used to compute the flow rate. A set of gears is driven by the movement of a disc or piston, which registers and records the volume of liquid exiting the meter. Positive displacement meters come in two varieties that can be used to measure water consumption:

Water meters with a rotating disc inside a cylindrical chamber are known as **nutating disc water meters** [33]. The disc is held in place by a spindle. As it passes a known volume of liquid through the cylindrical chamber, the disc nutates, or wobbles. The disk's rotation is subsequently transferred to the register, which records the amount of water that has passed through the meter.



16: Nutating disc water meter [33]



17: Piston water meter

Water meters with a piston that oscillates back and forth as water runs through them are known as **piston water meters**. For each revolution, a known volume of water is measured, and the motion is transferred to a register via a magnetic drive and gear assembly.

Positive displacement meters are sensitive to low flow rates and have a wide range of flow rates with great accuracy. Homes, small companies, motels, and apartment complexes all employ them.

3.3.2 Velocity Meters

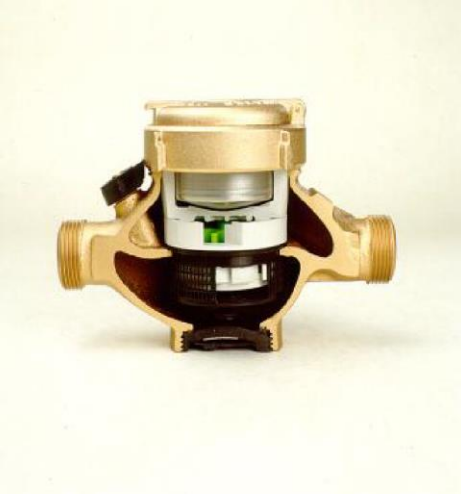
The velocity of flow through a meter with a known internal capacity is measured by a velocity-type meter. The volume of flow can then be calculated from the flow speed to ascertain the usage. With the exception of multi-jet meters, which are available in sizes between 5/8" and two inches, these meters are available in sizes of two inches and bigger.

Velocity meters come in different types, (see fig) including:

18: Fluidic oscillator [35]

19: Ultrasonic transit time [33]

20: Electromagnetic [36]



21: Multi-jet type water meters [37]

22: Single jet water meter [38]

3.3.3 Fluidic oscillator type water meters

A nozzle creates a jet of water that enters the fluidic oscillator [35]. When the jet first enters the flow chamber, it will be pulled to one of the two diffuser walls, where it will travel down the wall via the Coandă effect before exiting the flow chamber. The jet will flow towards the opposite diffuser wall when the local pressure is reduced by the opposite diffuser wall, causing it to oscillate between the two diffuser walls. Within the flow chamber, components such as a splitter post and feedback channels have been carefully adjusted to offer oscillation throughout a wider flow range.

While flow is present, this oscillation between the diffuser walls continues, with each oscillation representing a specific volume that has gone through the meter Electrodes are installed close to each diffuser wall, and a pair of powerful permanent magnets create an electrical current in the jet, which is measured by electrodes. When the oscillations happen, the sensing electronics record them and total the volume passed, presenting the total volume on a liquid crystal display.

3.3.4 Ultrasonic transit time water meters

The difference in the passage time of ultrasonic pulses traveling in and against the flow direction is measured by this sort of water meter. Transit The average velocity of the water along the path of the ultrasonic beam is measured by the time difference. Changes in water velocity are electronically converted to changes in flow rate [33]**.**

3.3.5 Electromagnetic or “Mag” water meters

Faraday's law governs the operation of mag meters. As the fluid flows through a constant magnetic field, its velocity is precisely proportional to the induced voltage (electromotive force). The induced voltage rises as the velocity of the water rise, and the volume of water measured rises as well [36]**.**

3.3.6 Multi-jet meters water meters

Create several water jets against an impeller whose rotation speed is dependent on the velocity of the water flow by using various ports surrounding an interior chamber. Multi-jets are extremely accurate at low flow rates, but they lack the straight-through flow channel required for high flow rates in big pipe diameters. In most multi-jet meters, an internal strainer mechanism protects the jet ports from being clogged [37].

3.3.7 Single jet water meter

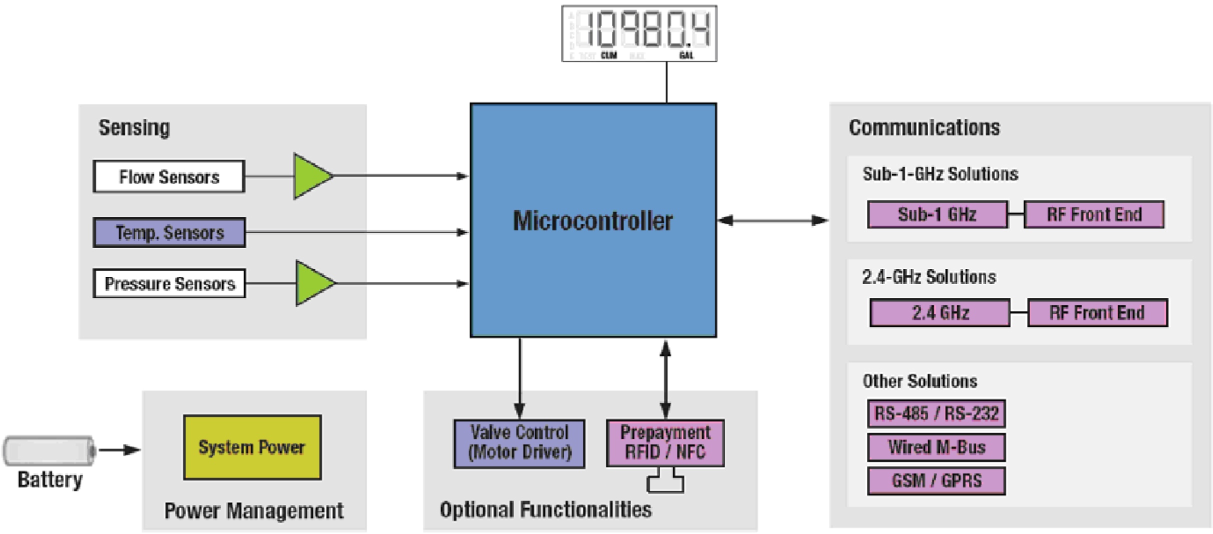
Before striking the turbine, the water jet is canalized by an injector. The flow profile is straightened by the single jet tapered injector. Clogging is prevented by the huge bore area, which prevents meter Overspeed [38].

3.4 Smart meter structure

Mechanical meters are the most common type of conventional water meters. This type of meter turns the flow of water into the rotation of a disc. Each spin corresponds to a specific volume of water. The display of water flow measurement using mechanical pointers is one of the functionalities of mechanical water meters. Mechanical water meters are rapidly being phased out in favor of electronic or smart meters as technology advances. A sensor in smart water meters (see fig. 4) turns the water flow to an electrical signal that the MCU can receive and process.

To count and quantify water usage, most smart mechanical water meters use reed switches or hall-effect sensors [39]. A magnet is installed on one of the mechanical meter's rotating discs in this type of meter. The reed sensor is installed on a printed circuit board and detects the magnet every time it completes a rotation, sending a pulse signal to the microcontroller unit (MCU). The water flow data is sent to an information management system after being processed by the MCU in the electronic module.

Low-power RF radios are commonly used to communicate between a battery-powered water meter and another meter in a mesh network or a data collector on top of a traditional wired solution such as wired MBUS. The meter can also receive tariff information, firmware updates, or shut-off valve actuation, which is often used in conjunction with prepayment and is occasionally done through a near field communication (NFC) technology.



23: Block diagram of a smart water meter [40] [41]

Flow meters manufacturers face a dilemma because battery life is expected to last anywhere from 10 to 15 years. The proper power supply design must be combined with the right power output and radio performance to maintain the required power output and radio performance without exhausting the battery. For example, the TPS62730 step-down converter and MSP430TM microcontroller, in combination with Texas Instruments' growing portfolio of Sub-1 GHz ws M-Bus solutions, such as the SimpleLinkTM CC1120 RF transceiver, is perfectly suited to deliver the industry's best selectivity and blocking performance. The system-level approach also has the lowest system power consumption, ensuring that the meter can be left in the field for many years without the need for a battery replacement [42].

A transmitter is the most fundamental component of smart water meters. Wireless data transfer can be enabled by attaching this gadget to a water meter. Transmitters are radio-wave-based devices that send water meter readings to a remote site. The typical range of a transmitter employing wireless radio for smart metering applications is about 1. A GSM transmitter is required when transmitting data over a long distance. Radio transmitters are used in most smart metering applications since they are about three times less expensive than GSM [43].

Data storage facilities can be added to transmitters to increase their performance. A data logger is a device that can both store and send interval data. An accumulation meter has a data logger attached to it, just as the transmitter.

Data loggers can record data on a variety of time scales, from one recording per second to one recording per month. Interval data tracking has the immediate benefit of making leak detection easier. Leaks are discovered when there is a consistent flow of water over a long period of time. The precise amount of water lost over a period of time can be calculated via software analysis.

A gateway is a device that receives data from one or more data sending devices and passes it to a remote destination. Radio transmitters are often used by smart water meters and data loggers to transfer information to a gateway, which subsequently relays all end-user data via GSM networking. The gateway can store several data points and send them to the retailer in packets by functioning as a huge data logger. This kind of data storage and transmission eliminates the need for data to be relayed across long distances on a regular basis.

3.4.1 What they Send and Receive

One of two factors governs the operation of smart meters. Those that just communicate data on household usage patterns and those that can receive data from the network in addition to transmitting it [44].

Information sent to the utility includes

- alarms
- usage as per the user
- monitoring data

Information received by the meter includes

- disconnect/reconnect instruction
- alarm and load share by the meter
- date and time
- information on prices
- how meter behaves (programming)

Through a network in the home, a smart meter can connect with appliances at home. It has the ability to communicate with:

- display monitors
- water meter
- water heater

3.4.2 Flow and Pressure monitoring

Monitoring of water flow: The sensors save data on a variety of important aspects, including site settings and serial numbers, which are typically required during installation, maintenance, or replacement.

It's crucial to keep track of how much water is utilized in commercial and residential structures. Water is delivered to households and businesses by a public water delivery system. Water meters can also be used to calculate the flow rate of a specific system component in water sources or the entire water system.

Pressure monitoring: The force required to bring water into the mains and domestic piping is known as water pressure. Bars are the units of measurement for pressure. One bar is equal to the force necessary to lift water to a height of ten meters. Understanding the water pressure in the distribution system is consequently crucial for water utilities in controlling their community's water supply.

Contamination of the groundwater system can occur as a result of pressure loss. The physical integrity of the pipes can be harmed by pressure changes. Increased pressure can cause leaks, serious breaks, and shorten the infrastructure's lifespan. Pressure management can also help you save money. System operators can use precise pressure data to reduce leakage volumes, energy costs, system maintenance costs, customer complaints, and water quality issues.

3.4.3 Water Quality Monitoring

Water quality monitoring is essential so that we can reduce the impact on customers' health. A smart sensor array could be installed in the network to offer real-time water monitoring. Water quality characteristics such as pH and turbidity can be considered.

pH

The pH value describes how much acidity is present in the water. In the range of 0 to 14, the pH scale is a logarithmic scale with a neutral point of 7. A basic or alkaline solution has a value over 7, while an acidic solution has a number below 7. The solubility of hazardous metals and compounds is also improved at extreme pH levels. The temperature has an inverse relationship with pH, meaning that as the temperature rises, so does the pH.

Turbidity

Turbidity, like smoke in the air, is the cloudiness or haziness of a fluid generated by enormous numbers of small particles that are normally imperceptible to the naked eye. The measurement of turbidity is an important indicator of water quality. Turbidity must not exceed 1.0 nephelometric turbidity units (NTU) [45].

3.4.4 Monitoring Sensors

The monitor interfaces with data loggers wirelessly to capture leak data, which it then sends immediately to an office computer. This eliminates the need for costly site visits. Instead, leakage data can be sent to the monitoring station automatically. The device includes a built-in radio receiver as well as an SMS transmitter. To save battery life, it goes into a low-power "sleep" mode when it is not receiving or transmitting data. Data is provided through the radio from data recorders within range, and the machine subsequently sends the information to a monitoring station running the appropriate software via SMS. When one of the loggers reports a potential leak, the online monitor can be set to transmit an immediate leak warning.

3.5 Smart Water Meter Communication Technologies:

SWM communication is of four types which are discussed below: [44]:

- telephone line
- fiber optic cable
- wireless communication
- power line communication

3.5.1 Telephone dialup

The meter connects to the utility's computer once a day, usually late at night, using a built-in dial-up modem. It can utilize the same phone line as the rest of the house, or it can use a separate phone line. Some pay-per-view television systems are comparable to this. If the meter is connected to a separate phone line, the utility computer can dial up the meter several times per day.

3.5.2 Fiber optic cable

The smart meter sends short light pulses along a glass fiber line to communicate. The high-speed, secure, and stable communication provided by this technology, as well as the fact that the fiber cable does not radiate, are all advantages.

The cost of installation is a disadvantage. This method is also one of the safest, though it does require the use of a digital meter, which has its own set of problems. Smart meters with fiber optic wires are currently only used in a few cases. They are most likely only practical in densely populated places.

3.5.3 Radio communication

These are the most basic wireless systems available. They primarily communicate in one direction. The utility is unable to remotely program the meters or communicate with them in any other way. Typically, these meters can only transmit their readings.

There are two versions:

- wake-up
- bubble-up

The wake-up meters wait for a signal that tells them it's time to start transmitting data. They don't transmit if they don't have to. The bubble-up meters only transmit once in a while, usually every 15 or 30 seconds. It could be once a day or once every five seconds.

A utility truck with an onboard receiver goes through the area once a month to read the meters. As it travels through without stopping, it merely picks up the signals sent out by the bubble-up meters within range. Whether the utility vehicle is present or not, the meters continue to transmit (at least every 30 seconds).
If wake-up meters are employed, the truck transmits a signal to all meters within range, instructing them to transmit. A stationary receiver (collector) in the area can also pick up the wake-up and bubble-up meters. It's usually attached to a utility pole or a lamp post. The information is then sent to a central computer by this collector.

3.5.4 Cellular communication (GPRS)

This is the most basic arrangement. The meter has a modem that can connect to a water utility system to gather the information data. It might not be feasible to send more than a couple of times per day [44].

3.5.5 Wi-Fi

In a Wi-Fi system, a wireless signal is transmitted from the router to a nearby device which converts those radio signals into data. The Wi-Fi uses 2.4GHz or 5GHz frequency.

A WiFi network is essentially an internet connection shared by a wireless router with several devices in a house or business. The router connects to your internet modem directly and functions as a hub, broadcasting the internet signal to all of your Wi-Fi enabled devices. As long as you're within your network's service area, you'll be able to stay connected to the internet.

Wi-Fi has several advantages, including unlicensed radio spectrum, lower costs, increased availability, roaming support, and disadvantages are High power consumption, interference due to unlicensed spectrum, and interoperability issues.

3.5.6 Fixed wireless network

In a wireless network, each meter talks two-way with a neighborhood central station, which then connects directly with the utility. This control station, which is normally installed on a utility pole or a light pole, is known as a "collector," "access point," or "gatekeeper." The collector is sometimes incorporated into a smart meter that is installed on a building.
In simple networks, each meter might simply switch on its transmitter once a day, wait for a pause in the transmissions of the other meters, and then send its data to the collector. The collector may then provide fresh rate information, as well as the current time, back to the collector.

In a given area, a central collector may communicate with 500-5000 smart meters. It could have a stronger transmitter than smart meters.

The meters communicate with the collector throughout the day in a more complex network (often referred to as a LAN). The meters may send far more frequently than is required for billing purposes, resulting in a large amount of wireless data. To promptly detect line faults, the added information may include the current-voltage of the line and the status of each meter.
These networks may connect using Wi-Fi (2.4 GHz) or a proprietary technology (900 MHz). The collector connects to a central computer through dialup phone, dialup cell phone (GPRS), DSL/ADSL, satellite link, or other means. A wireless network will very certainly necessitate the construction of a separate set of transmitters on lamp posts and utility poles all around the neighborhood.

3.5.7 Zigbee

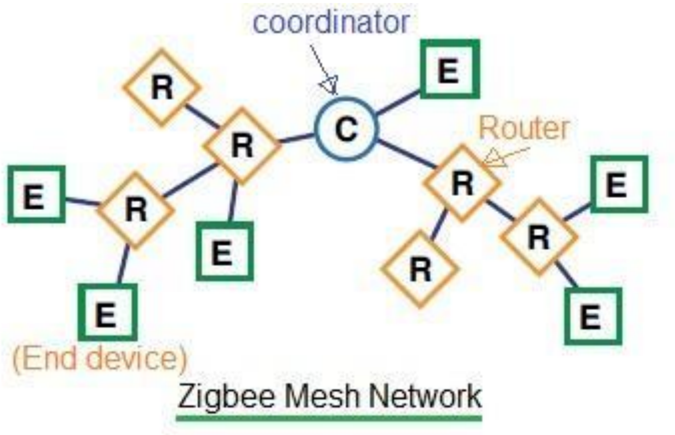
With the advancement of network and communication technology, the difficulty of wire is eliminated from people's lives, and the Wireless sensor network has a wide range of applications and practicality in the areas of remote sensing, industrial automation control, and household appliances, among others. Near-field wireless communication technology, such as Bluetooth, wireless local area network (WLAN), and infrared, is now widely employed. However, they have a lot of drawbacks, including complexity, high power dissipation, short distance, and small-scale networking. As the times demand, a new form of wireless net technology-Zigbee emerges to meet the demand for low power consumption and low speed among wireless communication devices.

The IEEE 802.15.4 standard is the cornerstone of Zigbee, although it only defines the physical (PHY) layer and the medium access control (MAC) sub-layer. The Zigbee Alliance then builds on this foundation by providing the network (NWK) layer and a defined API. It may be integrated into a wide range of devices, support Geo-location, and be widely used in areas such as industrial monitoring, safety systems, smart homes, and so on; the protocol is implemented using a protocol stack.

3.5.8 Architecture of Zigbee Network

Zigbee supports a variety of network architectures, the most common of which are the star, tree, and mesh networks. The Coordinator, the Router, and the End Device make up this group. Full function (FFD) is required for the coordinator and router; however, the end device can choose between full function (FFD) and reduced function (RFD) (RFD). RFD is solely used to collect data and relay it to its parent node; it is not utilized to complete tasks like data transmission, route finding, or route maintenance.

RFD's responsibilities include creating a new network, transmitting network beacons, controlling network nodes, and storing network information, among other things. A star network is made up of a Coordinator and one or more end devices. Because the end device can only communicate with the coordinator and not with the other end devices, the star network is referred to as a single-hop network. Because tree and mesh networks contain routing capabilities, they are referred to as multi-hop networks.



24: Zigbee Mesh Network [46]

Normally, each node in a mesh network relays or routes data until it reaches the destination node. Mesh networking has a lot of power when it comes to data routing. Each node in a mesh collaborates with neighboring nodes to ensure that data is distributed evenly.

A simple Zigbee mesh network with a coordinator, routers, and end devices is shown in Figure. All nodes in this network can send and receive data, but they all have different responsibilities and purposes. Because Zigbee is an open standard, interoperability between devices from different vendors is simple.

• To create a Zigbee network, only one coordinator is required. It keeps track of all the important details about the Zigbee network, including encryption keys.

• Routers are intermediate nodes that assist in data transmission between devices.

• There are two sorts of end devices: decreased function and full function. Reduced-function devices are unable to transmit data and must communicate with their parent devices (routers/coordinators) to do so. Full-function devices, on the other hand, perform the relaying. Full-function devices are used in the Zigbee Mesh network.

3.5.9 LORAWAN (Low Power)

For low-power embedded devices that are dedicated to a single activity, cost-effective Internet access is critical. When it comes to coverage (communication range), energy consumption, and cost, traditional wireless communication methods are inadequate. LPWAN intends to address these issues in a way that is scalable and suited for large-scale deployments of low-power end devices. Low-power wide-area networks are designed to have kilometer-range coverage from dense urban to suburban areas by operating at low data rates.

These functionalities are effectively provided by LoRaWAN, SigFox, NB-IoT, Weightless, and other sub-GHz communication technologies; however, LoRaWAN has captured the interest of enterprises, communities, and researchers and has become a popular LPWAN technology.

LPWANs share several characteristics that set them apart from traditional communication networks.

- Low power consumption

- The entire ecosystem, from devices to applications, need strong security mechanisms.

- When considering indoor deployments, built-in localization is a benefit.

- In densely populated urban areas, radio networks jam on the same or adjacent channels. Modulation with a high level of (interference resistance) is required.

- At the end of the day, nodes generate data, which must be correctly managed.

The term "LoRa" stands for "Long Range" and refers to a physical layer technology patented by Semtech. The LoRa Alliance has suggested an open protocol called LoRaWAN, which enables the network's MAC layer.

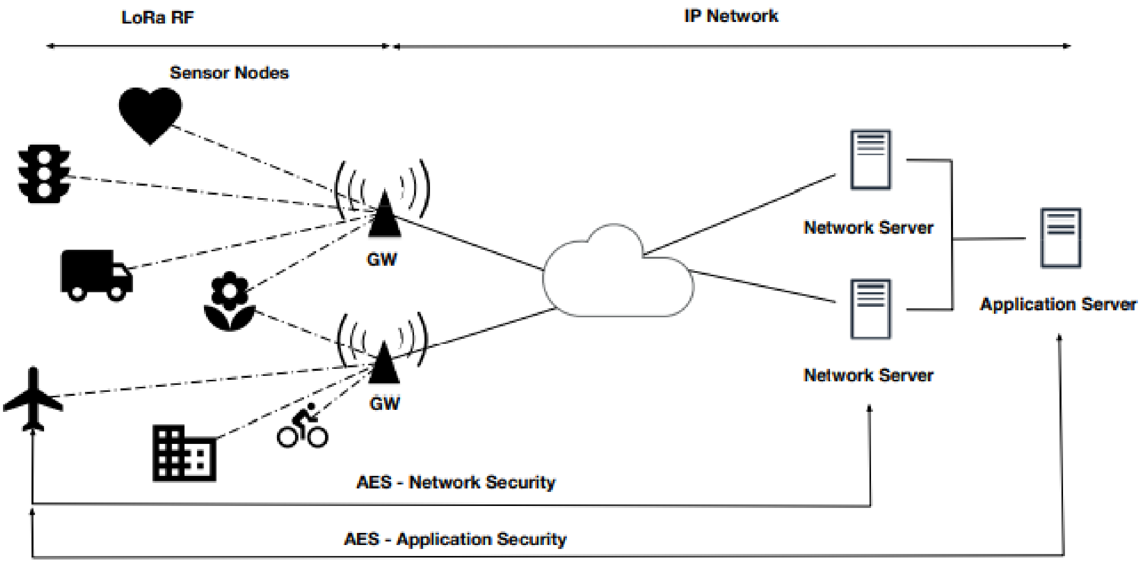
3.5.10 LoRa & LoRaWAN Technologies

The physical layer in the OSI reference model correlates to LoRa, which is an RF modulation. LoRaWAN, on the other hand, is a MAC layer standard that coordinates the media.

Architecture

The physical layer in the OSI reference model correlates to LoRa, which is an RF modulation. LoRaWAN, on the other hand, is a MAC layer standard that coordinates the media.

The LoRaWAN network features a star-of-stars topology, and the system comprises three primary components (i) network servers, (ii) gateways (GWs), and (iii) end nodes) from an architectural standpoint. End nodes use GWs to connect with the network server (or data server), and node-to-GW communication can be LoRa or FSK modulation, with variable data rates and channels. Data frames supplied through end nodes, received by GWs, and routed through the network server are managed by network servers using standard IP technology.



25: LoRAWAN Architecture

3.5.11 LoRa Gateways:

A LoRaWAN node is linked to a specific gateway. Any data sent by the node is relayed to all gateways, and each gateway that receives a signal sends it to a cloud-based network server. Mobile devices in cellular communications connect to several base stations and data is not directly delivered to the server.

The sole responsibility that the gateways should be responsible for is the downlink message time. This time must be precise for the message to be received in the device's reception window.

3.5.12 Network Servers:

The network server possesses all intelligence. It checks security, filters duplicate packets from several gateways and sends ACKs to the gateway. Finally, if a packet is intended for an application server, the network server transfers it to that application server.

3.5.13 LoRa Nodes / End Points:

Sensors or applications that perform sensing and control are known as LoRa endpoints. These nodes are frequently located in remote locations.

LoRaWAN is a MAC layer protocol that intends to address medium management and network congestion. Following features are available for LoRaWAN protocol:

- Channel management
- Energy efficiency
- Adaptive data rate
- Security
- GPS-Free geolocation

3.5.14 Advantages:

- Long transmission distance
- Low power LoRa module
- Strong anti-interference ability
- LoRa devices have a longer battery life

3.5.15 Disadvantages:

- Low Transmission rate
- Longer Latency time

4. Narrow Band Internet of Things (NB-IoT)

4.1 Introduction:

IoT technologies have advanced greatly in the last 20 years, and they are now used in a variety of fields. Specifically, practically anything may be connected via an IoT network. IoT communication services can be roughly divided into two groups based on transmission rate: high-data-rate services (such as video services) and low-data-rate services (such as meter reading service) [46].

IoT communication technologies have recently matured and spread as a result of the development of IoT. IoT communication technologies can be divided into two categories based on transmission distance: short-distance communication technologies and long-distance communication technologies. Zigbee, Wi-Fi, Bluetooth, and other wireless technologies are examples of the former. The smart home is a typical application for them [47].

The Narrow-Band Internet of Things (NB-IoT) is a large-scale Low Power Wide Area (LPWA) data perception and acquisition technology suggested by 3GPP for intelligent low-data-rate applications. Smart metering and intelligent environment monitoring are two common uses. Furthermore, it is backed up by a strong cellular communication network. As a result, NB-IoT is an exciting technology [48].

4.2 Brief review of NB-IOT development history and Standardization.

For a long time, cellular mobile communications were primarily used to offer human-oriented telephony and mobile broadband services. 3GPP has been researching cellular networks (such as GSM, UMTS, and LTE) for Machine-Type Communication (MTC) services since 2005. As stated in Table 1, relevant feasibility and improvement research aims to make MTC a major component in 5G networks [49].

After further refining and clarifying MTC service demands and features, the 3GPP announced in R12 GSM access network advancements about the design of low-cost MTC terminals, security requirements, and network system architecture.

Due to its software upgrades and core network reuse deployed in permitted frequency bands, the 3GPP LPWA technology (represented by NB-IoT) attracts more industry attention than non-3GPP LPWA technology. In 2017, cost reduction and commercial promotion of the NB-IoT terminal chip are expected to occur progressively. China's IMT2020 workgroup presented important NB-IoT technologies in February 2015. Since then, the IMT2020 has steadily improved its technical proposal and development research in the areas of the principle sample machine and terminal chip. To summarise, the 3GPP employs a two-step technique to address the technology issues posed by MTC services. The first stage is to develop a transition strategy that will allow MTC services to be delivered using and optimizing the current network and technology. The second stage is a long-term strategy centered on the adoption of a new air interface technology for NB-IoT to allow large-scale MTC service growth while maintaining core competitiveness against non-3GPP LPWA technology.

4.2.1 History and Development of NB-IoT

Table 2: Brief history of development and course of standardization of NB-IoT [50]

Standard number	Start time	Freezing time	Version	Technologic fields of concern

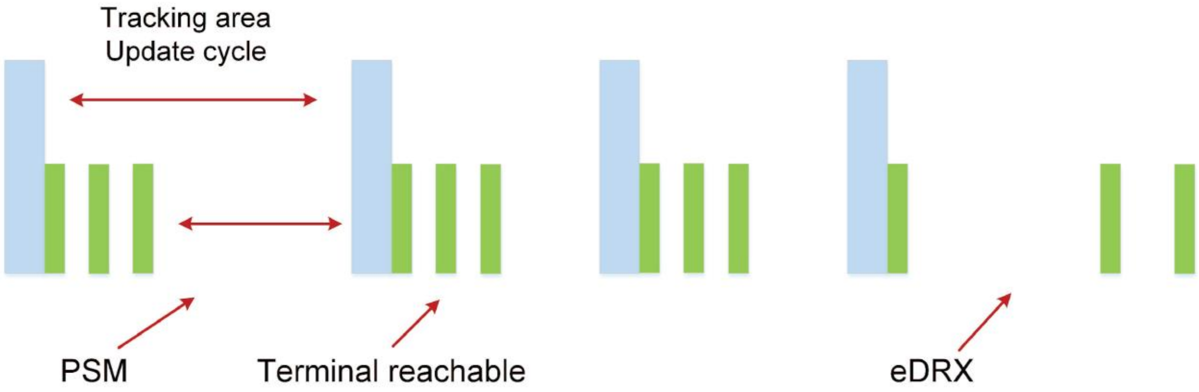
22.868	2005	2008	R8	Billing, addressing, security, communication mode, massive user
33.812	2007	2009	R9	Remote subscription management, security requirements, security architecture enhancement
22.368	2009	2015	R10	General and exclusive service requirements
37.868	2010	2012	R11	Service features and modeling, access network enhancement, and congestion control
43.868	2010	2014	R12	Service features and modeling, GERAN enhancement (such as resource allocation, overload and congestion control, addressing format and energy-saving mode)
22.888	2012	2014	R12	The architecture of network system, localization, and IMS enhancement
33.868	2012	2014	R12	Security requirements, security architecture enhancement
37.869	2013	2014	R12	Signaling editing, UEPCOP

23.789	2014	2015	R13	MONTE
23.770	2015	2015	R13	Discontinuous reception of expansion (eDRX)
45.820	2014	2016	R13	Enhanced indoor coverage, supporting the massive, small-data terminal, lower terminal complexity and cost, higher power utilization ratio, latency feature, compatibility with existing systems, the architecture of network system (prototype of NB-IoT)
22.861	2016		R14	Typical use case and service requirements for mMTC
22.862	2016		R14	Typical use case and service requirements for uRLLC

4.3 NB-IoT Features:

4.3.1 Low power consumption

The power conservation mode (PSM) and enhanced discontinuous reception are two of NB-primary IoT's features (eDRX). PSM technology has been added to Rel-12 in which the terminal is still registered but cannot be accessed by signaling to put the terminal into a deep slumber for a longer period to save power. Extended discontinuous reception (eDRX) was added which extends the sleep cycle for terminals in idle mode. In comparison to PSM, eDRX dramatically improves downlink accessibility. Figure 1 depicts the PSM and eDRX power-saving mechanisms.



26: Power saving mechanisms of PSM and eDRX [52]

For typical low-rate low frequency service, NB-IoT requires a constant-volume battery to have a terminal service life of 10 years. According to TR45.820 simulated data, if a 200-byte message is sent once per day via terminal with a coupling loss of 164 dB with both PSM and eDRX, the service life of a 5-Wh battery can be 12.8 years [51].

Table 3 Estimation on service life of battery in integrated PA [51]

Message size / message interval	Coupling loss = 144 dB	Coupling loss = 154 dB	Coupling loss = 164 dB
50 bytes / 2 Hours	22.4	11.0	2.5
200 bytes / 2 Hours	18.2	5.9	1.5
50 bytes / 1 Day	36.0	31.6	17.5
200 bytes / 1 Day	34.9	26.2	12.8

4.3.2 Enhance coverage and low latency sensitivity

In independent deployment mode, the covering power of NB-IoT may reach 164 dB, and simulation tests for both in-band and guard band deployment were completed. The NB-IoT uses low-frequency modulation and retransmission. In 3GPP IoT, the acceptable latency is 10s [51].

4.3.3 Transmission mode

The development of NB-IoT is based on LTE, as illustrated in Table 4. The changes are mostly made to essential LTE technology to accommodate NB-unique IoT features. The NB-IoT physical layer's RF bandwidth is 200 kHz. In the downlink, the NB-IoT uses a QPSK modem and OFDMA technology with a 15 kHz sub-carrier spacing. For IoT terminals with low power and low rate, a single sub-carrier technology with sub-carrier spacing of 3.75 kHz and 15 kHz is suitable. 12 continuous sub-carriers are defined for sub-carrier spacing of 15 kHz, and 48 continuous sub-carriers are defined for sub-carrier spacing of 3.75 kHz. Multiple subcarrier transmission allows for 15 kHz subcarrier spacing and defines 12 continuous sub-carriers that can be concatenated into 3, 6, or 12 sub-carriers. Because of the higher power spectral density, the coverage capabilities of 3.75-kHz spacing is greater than that of 15-kHz spacing. Because the Narrow Physical Random-Access Channel (NPRACH) requires single sub-carrier transmission with a spacing of 3.75 kHz, most equipment enables single sub-carrier transmission with a spacing of 3.75 kHz for uplink transmission. Following the introduction of single subcarrier transmission with a 15 kHz spacing and multiple subcarrier transmission, the choice is made adaptively based on channel quality at the terminal. The NB-IoT high layer protocol (the layer above the physical layer) is created by modifying some LTE features, such as multi-connection, low power consumption, and limited data transmission. [52].

4.3.4 Spectrum Resource

Because IoT is the fundamental service that will draw a larger user group on the communication service market in the future, the development of NB-IoT has received strong support from China's four main telecom operators, each of whom owns NB-IoT spectrum resources, as detailed in Table 4 [53].

4.3. Spectrum Specifications of NB-IoT

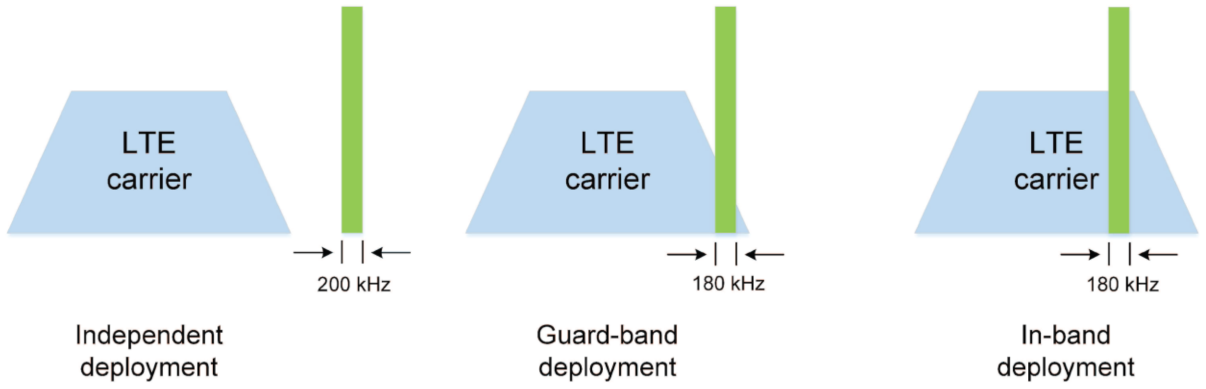
Table 4 Spectrum division for NB-IoT by telecom operators

Operator	Uplink Frequency band/MHz	Downlink frequency band/MHz	Bandwidth/MHz
China Unicom	909-105 1745-1765	954-960 1840-1860	6 20
China Telecom	825-840	870-885	15
China Mobile	890-900 1725-1735	934-944 1820-1830	10 10
SARFT	700	700	Undistributed

4.3.6 Working mode of NB-IoT

NB-IoT supports only FDD transmission mode with a bandwidth of 180 kHz and has 3 deployment modes [53]:

- Independent deployment (Stand-alone mode), uses an independent frequency band that does not overlap with the frequency band of LTE.
- Guard band deployment utilizes the edge frequency band of LTE.
- In-band deployment utilizes an LTE frequency band for deployment, it takes one physical resource block of LTE band for deployment.



LTE：Long term evolution NB-IoT: Narrow-Band Internet of Things

27: Deployment modes of NB-IoT [54]

4.3.7 NB-IoT network

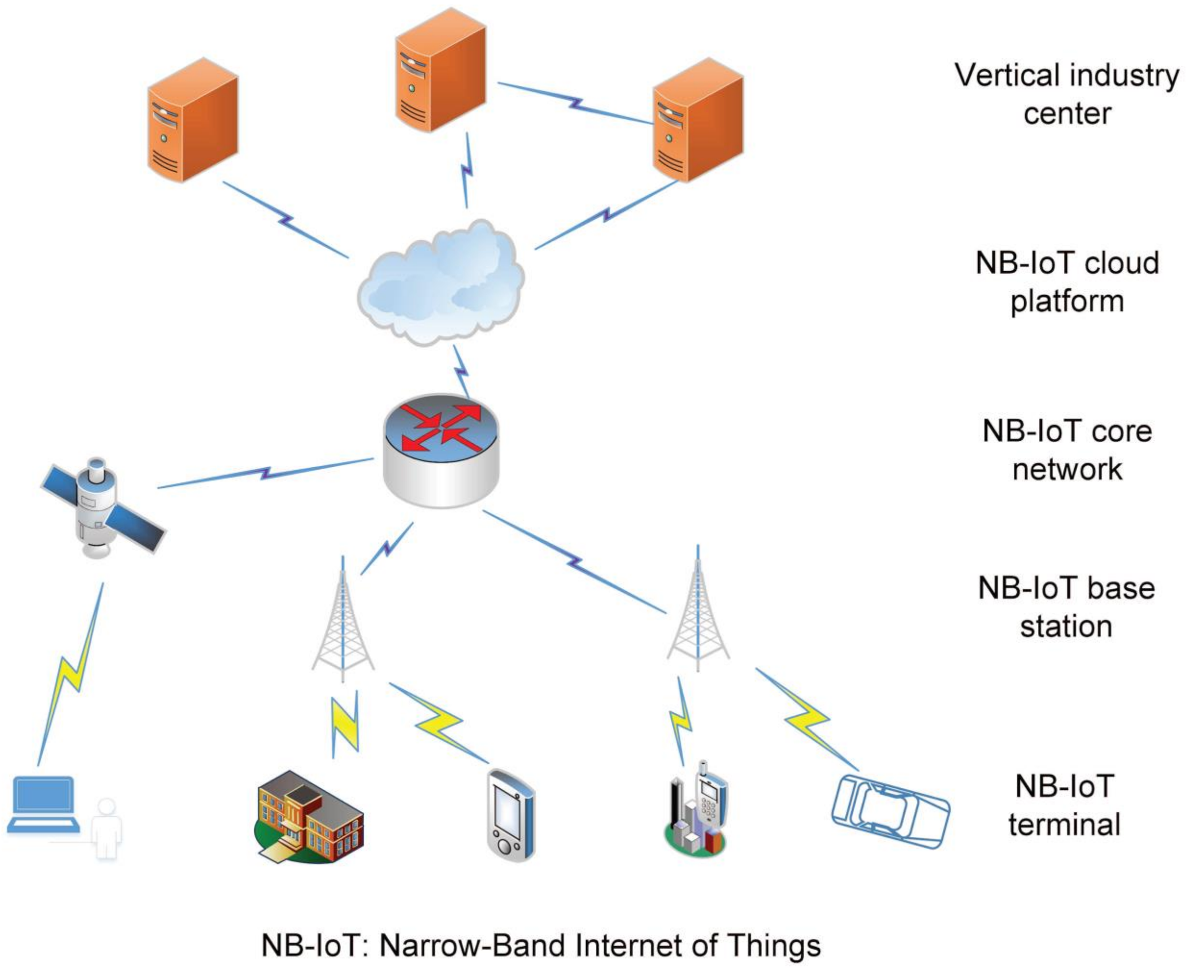
Nb-IoT consists of 5 parts is shown in figure 5 [53]:

NB-IoT terminals are IoT devices that can connect to the NB-IoT network if a SIM card is attached.

- An NB-IoT base station has been deployed by a telecommunications company and supports three types of deployment: stand-alone, in-band, and guard-band deployment.
- NB-IoT core Network: NB-IoT base stations can connect to the NB-IoT cloud via the core network.
- The NB-IoT Cloud Platform provides a variety of services, with the results being sent to the higher layer, which is a vertical business center.
- The NB-IoT service data is stored in the vertical business center, which can also control the NB-IoT terminal.

4.3.8 Data retransmission

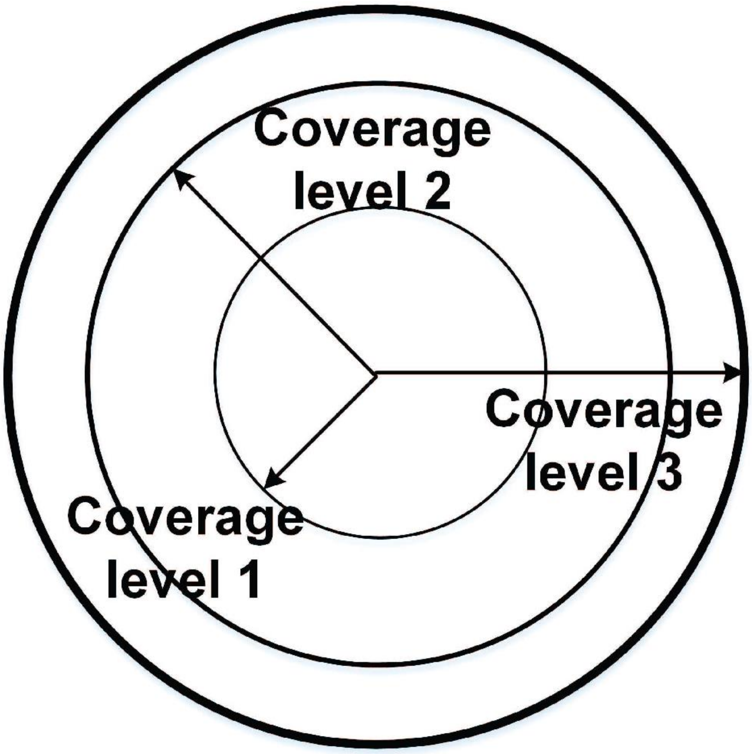
To increase demodulation and coverage performance, NB-IoT uses a data retransmission mechanism to obtain time diversity gain and low order modulation. Data retransmission is possible on all channels. [55].



28: NB-IoT networking [55]

4.3.9 Semi-Static Link Adaption

Because it is difficult for NB-IoT to offer long-term and continuous notification of channel quality change in most of the target service scenes, NB-IoT uses a coverage level instead of a dynamic link adaptation mechanism. The semi-static link adaptation is achieved by selecting modulation, coding mode, and data transmission repeat periods based on the coverage class of terminals.



29: Coverage levels of NB-IoT [56]

4.3.10 Coverage enhancement mechanism

NB-narrow-band IoT's modulation and sub-GHz deployment can improve receiving sensitivity and increase coverage. Furthermore, 3GPP proposed a new augmentation mechanism based on coverage classes (CCs), a new concept developed by 3GPP for NB-IoT. There are currently few relevant studies on it, but the essence of the mechanism is a type of special link adaption technology, in which terminals determine the coverage class based on the transmission environment and then execute the appropriate coverage augmentation technique [57].

4.3.11 Ultra-Low power technology

3GPP introduced the power conservation mode and enlarged discontinuous reception based on lower transmitting power to achieve ultra-low power consumption for NB-IoT. However, modeling findings showed that if data is transferred once per day, the expected service life of a terminal equipped with a 5-Wh battery can be 10 years, which is an optimal condition for most NB-IoT applications [58]. As a result, one of the key responsibilities of 3GPP R14 is to further assess energy efficiency mechanisms and to propose better strategies. The majority of extant DRX energy consumption models focus on the power consumption level of a single terminal, with the interaction between control signals and terminal operating modes switchover being the core point of modeling. In other words, a single NB-IoT terminal's energy consumption is influenced not only by its operating mode switchover but also by the operating mode switchover of other NB-IoT terminals [59]. As a result, researchers are attempting to investigate the space-time correlation of NB-IoT application scenarios and their impact on NB-IoT operating modes in order to assess the collective energy consumption level of NB-IoT terminals. The individual energy consumption level of NB-IoT terminals can be examined using group energy consumption. Finally, using that data, a design technique for optimizing the energy usage of NB-IoT systems and terminals can be completed. Furthermore, according to certain research, an NB-IoT terminal in an idle state can only finish an entire data transmission after random access. During the random access procedure, the number of backoff times of the terminal grows dramatically in the case of strong service burstiness. Because power control strategies with power climbing mechanisms are common in random access processes, the corresponding power consumption rises dramatically; therefore, evaluating the energy consumption level in random access processes with power climbing mechanisms is particularly important for NB-IoT [60].

4.4 Comparison between NB-IoT and other wireless communication technologies

Because of the rapid rise of intelligent low-data-rate IoT services, LPWA technology is becoming increasingly popular in the industry, and its market share is steadily expanding. Table 4 shows how intelligent IoT applications can be divided into three groups based on data transmission rate needs in 2020.

1. A high data transmission rate is required. The data transfer rate is greater than 10 megabits per second. 3G, 4G, and Wi-Fi are possible to access technologies. They are mostly utilized in television direct broadcast, electronic healthcare, automotive navigation systems, and vehicle entertainment systems, among other applications. This type of IoT application is predicted to have a 10% market share.

1) The data transmission rate is moderate. The data transfer rate is less than one megabit per second. 2G and MTC/eMTC are the available access technologies. POS machines, smart homes, and M2M return links are examples of such uses.

2) There is a slow data transmission rate. The data transfer speed is less than 100 kilobits per second. NB-IoT, SigFox, LoRa, and short-range wireless communications like ZigBee are among the possible access technologies. Sensors, smart metering, products monitoring, logistics, parking, and intelligent agriculture are all examples of LPWA

technologies. This type of IoT application is predicted to have a market share of 60%. However, there are still a lot of job openings in the related market. As a result, NB-IoT has a promising future.

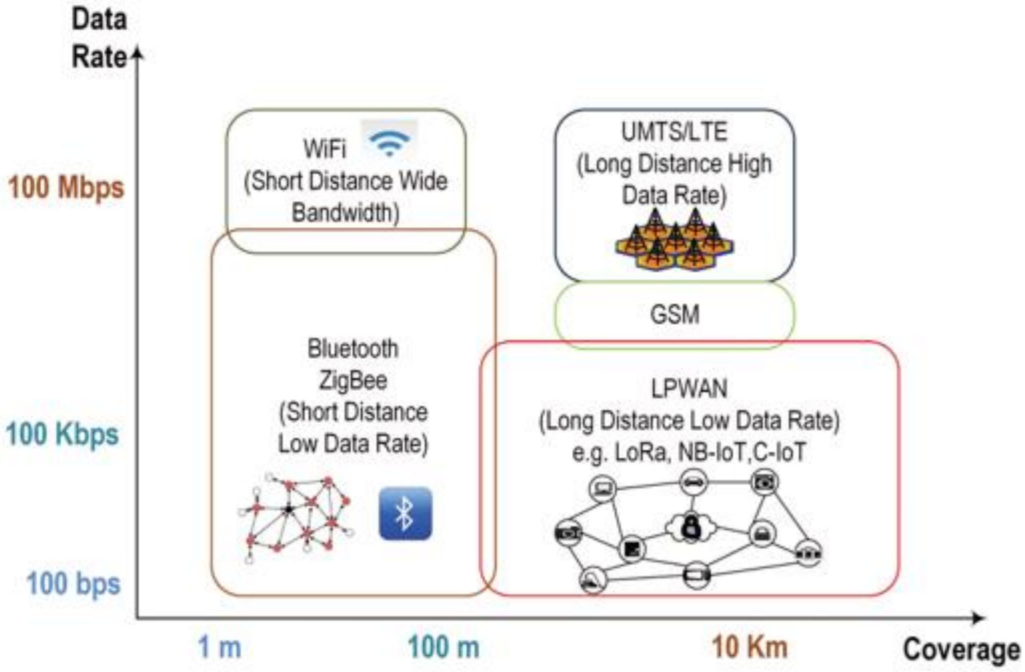
4.4.1 Connection Technology of IoT

Table 5: Distribution figure for connection technology of Intelligent IoT in 2020

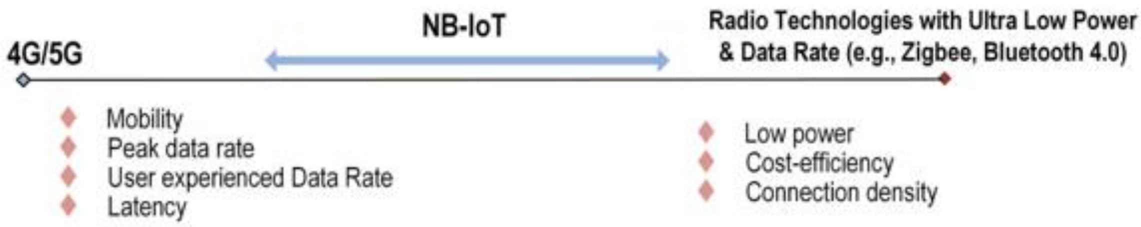
Global M2M/IoT connection distribution in 2020	Category	Network connection techniques	Fine-grained market opportunity
10 %	High data rate (>10Mbps), e.g., CCTV, eHealth	● 4G: LTE/LTE-A ● WiFi 802.11 technologies	Big profit margin for car navigation/ entertainment system
30 %	Medium data rate (<1Mbps), e.g. POS, Smart Home, M2M Backhaul	● 2G: GPRS/CDMA2K1X ● MTC/eMTC	2G M2M could be replaced by MTC/eMTC techniques
60 %	Low data rate (<100Kbps), e.g., Sensors, Meters, Tracking Logistics Smart Parking,Smart agriculture.	● NB-IoT ● SigFox ● LoRa ● Short Distance wireless connection, e.g. Zigbee	Various application cases; Main market for LPWA; Market vacancy

Fig. 30 shows a comparison between NBIoT's LPWAN and a variety of other connection types from various angles. We categorize them in Fig. 30 based on their coverage area and data transmission rate. The maximum coverage for short-range and high-bandwidth communication technologies like Wi-Fi can reach 100 m, and the data transmission rate can reach 100 Mbps. This type of communication technology is best for applications that demand a limited range and a lot of bandwidth. The maximum coverage area for short-range and low-data transmission rate communication technologies like Bluetooth and Zigbee is also 100 m, and the data transmission rate can be up to 100 Kbps. GSM, on the other hand, has a maximum coverage area of 10 kilometers and a maximum data transmission rate of 100 kbps. Long-range and low-data transmission rate communication technologies, such as LPWA, have a coverage range of 10 kilometers with a maximum data transmission rate of 100 kilobits per second.

Figure 31 depicts the trade-off design of NB-IoT technology. It combines the benefits of 4G/5G technology, such as mobility, peak rate, and user-experienced data transmission rate, with the benefits of low-power wireless communication technologies (such as Zigbee), such as intensive transmission and low cost. NB-IoT is a narrow-band technology that aims to achieve low-power consumption and wide-area wireless connectivity.

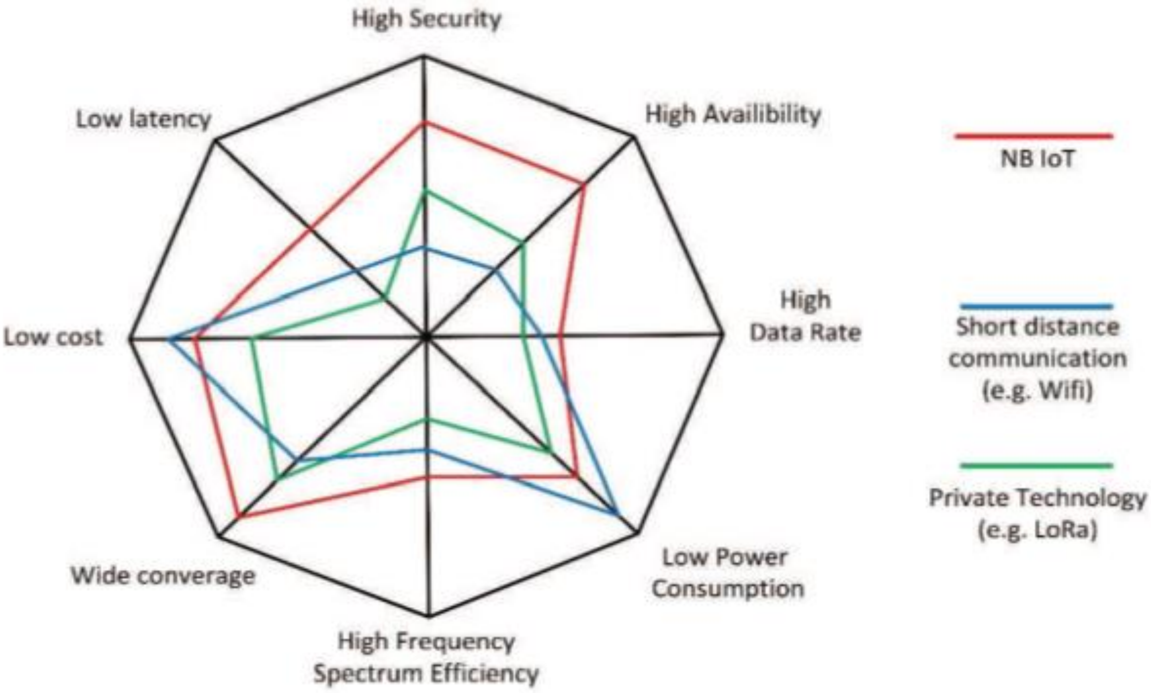

Data Rate
100 Mbps
100 Kbps
100 bps
WiFi
(Short Distance Wide Bandwidth)
UMTS/LTE
(Long Distance High Data Rate)
GSM
Bluetooth
ZigBee
(Short Distance Low Data Rate)
LPWAN
(Long Distance Low Data Rate)
e.g. LoRa, NB-IoT,C-IoT
1 m
100 m
10 Km
Coverage

30: Comparison of different wireless communication technologies


NB-IoT
4G/5G
Radio Technologies with Ultra Low Power & Data Rate (e.g., Zigbee, Bluetooth 4.0)
Mobility
Peak data rate
User experienced Data Rate
Latency
Low power
Cost-efficiency
Connection density

31: NB-IoT design trade-off

In Figure 32, we compare NB-IoT, short-distance communication technology (such as Wi-Fi), and private technology in terms of pricing, latency, security, availability, data transfer rate, energy consumption, spectrum efficiency, and coverage area (such as LoRa). Both short-distance communication technology and private technology, as indicated in Fig. 8, have advantages and disadvantages. NB-IoT, on the other hand, has greater performance. For example, in terms of low latency, high security, high availability, high data transfer rate, high spectrum efficiency, and large coverage area, NB-IoT outperforms the other two technologies.



32: Strengths of NB-IoT over short distance communication

We did a simple comparison between NB-IoT and LoRa concerning WAN communication technology, and the findings are provided in Table.

The table illustrates that NB-IoT has a bright future in operator-level networks. Furthermore, NB-IoT might provide a variety of network options, including wide coverage, high connection density, and low-cost IoT. LoRa could potentially be used in smart cities, exclusive industrial, and business applications because of its speedy and flexible implementation. In commercial application, however, we can ensure that these two LPWA technologies are complementary. We compared the performance of LPWAN and mobile communication networks (represented by 4G and 5G) in eight areas: peak data rate, user experienced data rate, spectrum efficiency, mobility, latency, connection density, energy efficiency, and flow density, starting with the evolution of mobile communications.

4.4. Comparison between NB-IoT and LoRa

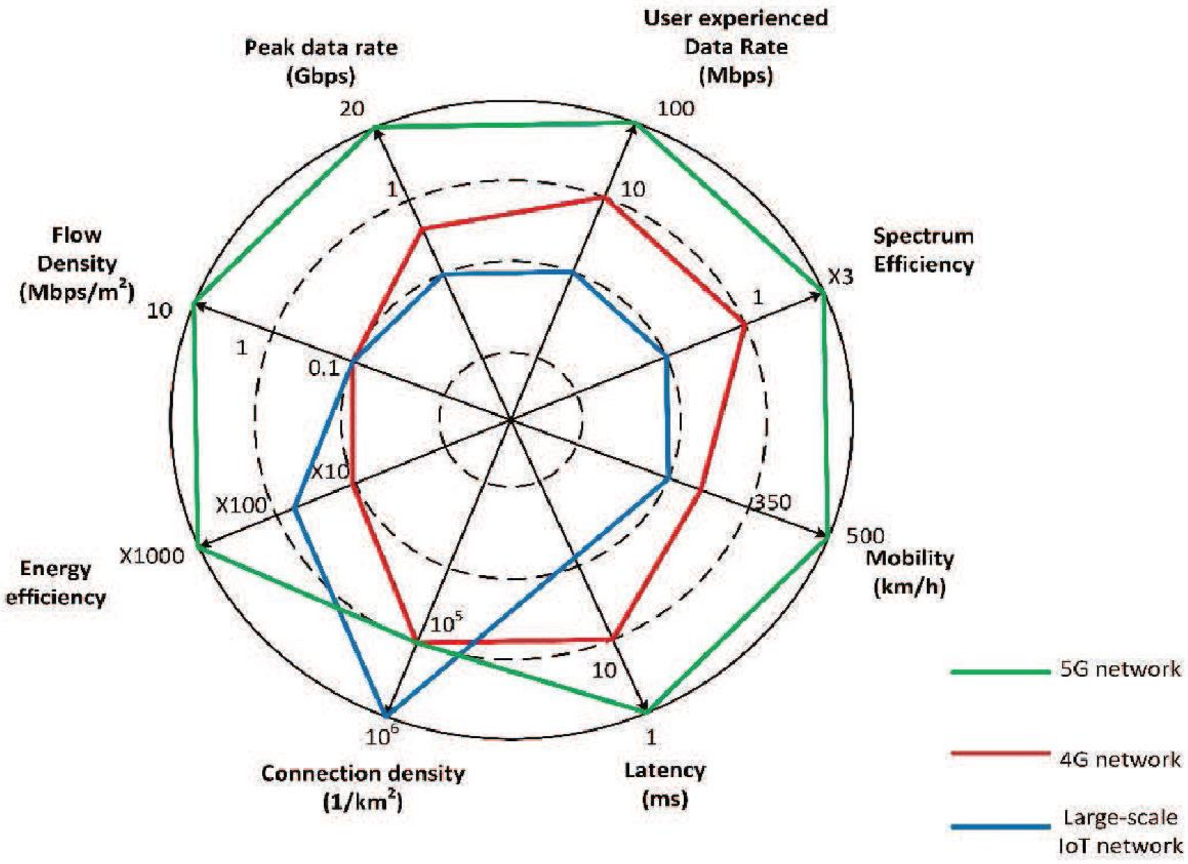
Table 6 Comparison between NB-IoT and LoRa

Item	NB-IoT	LoRa
Power consumption	Low (10 years battery life)	Low (10 years battery life)
Cost	Low	Lower than NB-IoT
Safety	Telecom level security	Slight interference
Accuracy rate	High	High
Coverage	<25 km (resend supported)	<11 km
Deployment	Rebuild supported based on LTE FDD or GSM	Inconvenience

The superiority of the 5G network is particularly clear. Furthermore, LPWAN has a higher energy efficiency than a 4G network but a lower energy efficiency than a 5G network. LPWAN can be used for applications that demand low energy consumption, low data transfer rates, and high connection density, as shown in Fig. 33. Another significant benefit of LPWAN is its low cost, which is not depicted in the diagram. As a result, LPWAN, as represented by NB-IoT, has a lot of potential in the IoT space. Furthermore, when compared to advanced LTE IoT technology, LTE-M (LTE-Machine to Machine) performance has vastly improved, compared to 1G, 2G, and 3G technologies. LTE-M has a 1-MHz bandwidth, whereas NB-IoT has a 200-kHz bandwidth and performs better. Both LTE-M and NB-IoT, on the other hand, cut the 20-MHz bandwidth used in the past, but their data transfer rate drops from 1 Mbps to 200 kbps. As a result of the lower band with a higher occupancy rate, NB-IoT is easier to promote and install.

Furthermore, NB-IoT, which presently has a coverage area of up to 20 kilometers, can achieve low power consumption and extensive coverage. It is generally recommended that NB-IoT be implemented at lower frequency bands, such as 700 MHz, 800 MHz, 900 MHz, or other frequency bands less than 1 GHz, to achieve goal coverage. We should also keep in mind that coverage entails not only distance but also penetrability. Its signal strength is 20 decibels stronger. As a result, we can achieve high-quality communication even in an indoor situation.

IEEE 802.11ah's current channel bandwidth is 1/2/4/8/16 MHz, which is similar to LTE bandwidth. M's Zigbee requires a channel bandwidth of 2-5 MHz in most cases. The exception is Zigbee, which operates at 868 MHz in Europe and uses an 800 kHz bandwidth, which is less than that of NB-IoT. The current distance is only 1 kilometer, which is significantly less than the NB-IoT distance, which ranges from several kilometers to twenty kilometers.



33: Performance comparison of LPWAN, 4G, and 5G networks.

Furthermore, we compared three technologies' related applications. Wearable electronics and energy management, or to be more specific, fitness-based smartwatches and household electricity usage control, are the primary applications of Category 0 as defined in 3GPP R12. The LTE-M with 1-MHz bandwidth, on the other hand, is projected to be used for item tracking (including pet lost, stolen bicycle, and other incidents), utility metering, online health diagnostic and monitoring, and municipal infrastructure construction (such as recording of a slot machine for parking and street lamp management). NB-IoT, on the other hand, is more suited to industrial applications like environmental monitoring and smart building.

Indeed, NB-IoT can compete with a wide range of current and future communication technologies. Furthermore, semiconductor companies have developed and pushed Sub-1GHz transmission plans, such as a smart grid and charging station for electric vehicles based on Zigbee with NAN (Neighbourhood Area Network) as a localization technology [9], IEEE 802.11ah, Wi-SUN, Wireless M-Bus, and others.

4.5 INTELLIGENT APPLICATION OF NB-IOT

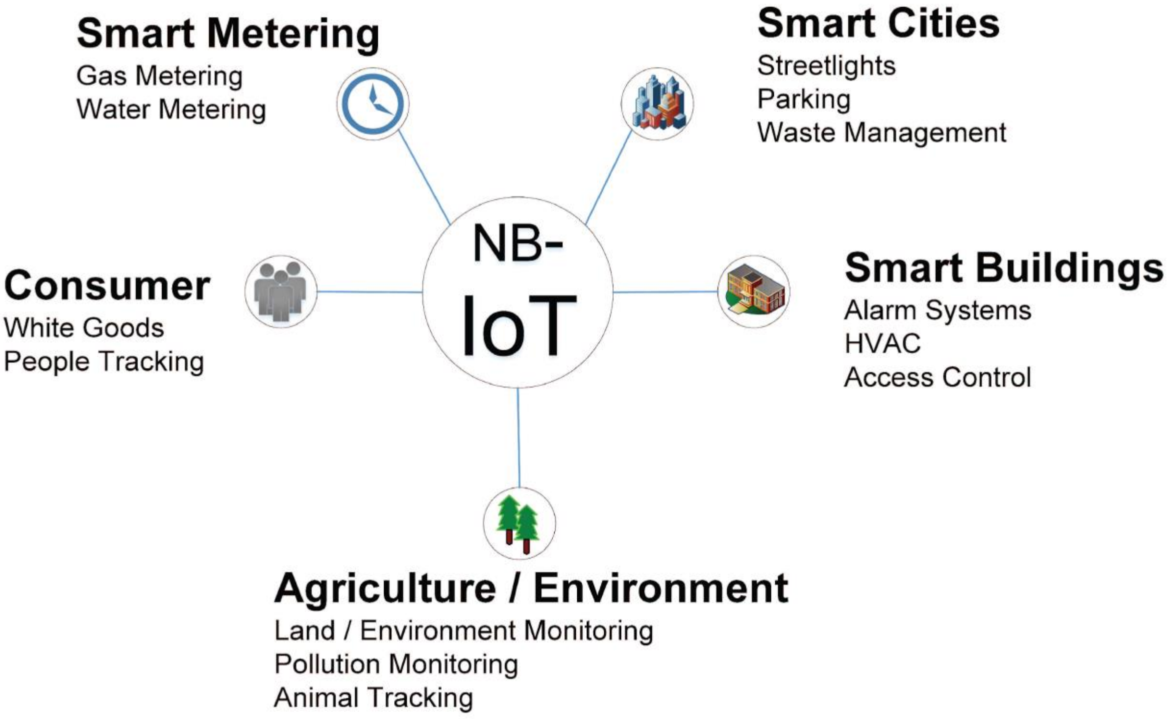
4.5.1 Application scenes of NB-IoT

The qualities of the NB-IoT technology allow it to meet the needs of low data transmission rate services with low power consumption/long standby time and wide coverage. Despite its enormous capacity, it is difficult to maintain high mobility. As a result, NB-IoT is better suited to static applications with low latency sensitivity. Discontinuous movement of real-time data transmission services. Below services are needs to be taken into consideration:

- Self-contained exception reporting services, such as smoke detector smart metering notices and others. Their uplink data size requirement is low (about 10 bytes), and their transmission period is typically a year or month.
- Autonomous reporting services with a daily or hourly transmission cycle and a small uplink data size need (at the level of 100 bytes). Typical applications include measurement reports for intelligent utility services (such as electricity, water, and gas), intelligent agriculture, and intelligent environment.
- Network command services. This category includes startup/shutdown, uplink report delivery, metering requirements, and other services.
- Upgrade service for software. The data quantities for software patches/upgrades are relatively large (at the level of 1,000 bytes), and the transmission period is often a day or an hour.

As shown in Fig. 34, the specialized application sceneries of NB-IoT include smart cities, smart buildings, intelligent environment monitoring, intelligent user services, and smart metering. Wearable technology, smart homes/white goods, intelligent trash cans, people tracking, and other intelligent user services are all included.

Smart cities aim to connect public facilities such as vehicles, roads, street lamps, parking spaces, well lids, dustbins, electricity meters, water meters, gas meters, and heat meters to achieve intelligent municipal management (such as intelligent management of infrastructure such as water, electricity, and gas in the city), intelligent municipal management (such as intelligent management of infrastructure such as water, electricity, and gas in the city), intelligent municipal management (such as intelligent management of infrastructure such as water, electricity, and gas in the city), intelligent municipal management (Traffic management (such as traffic flow control, road condition analysis, emergency response, and smart parking, all of which will aid in the development of the 5G Internet of Vehicles), and so on.



34: Intelligent application of NB-IoT [61]

The IoT network's communication range is the most important aspect of smart city implementation. With the widespread acceptance of the NB-IoT standard, it's easy to achieve scalability by leveraging operator experience in building large-scale networks in cities. A crucial feature of NB-IoT is its vast and deep coverage. It's also a good idea to cover the parking lot and the basement. As a result, several industrial issues from the past are overcome without difficulty. The challenge with NB-IoT is that it requires operators to match and rebuild their traffic operating modes. Lu et al. developed the first NB-IoT framework to track unmanned aerial vehicles in smart cities, effectively preventing UAVs from falling out of the sky.

4.5.2 Instances for intelligent application of NB-IoT

Huawei worked with several international operators from China, Germany, Spain, the United Arab Emirates, and other countries to evaluate the performance of NB-IoT-based smart metering, intelligent parking, and intelligent waste services. At the end of 2015, Vodafone and Huawei conducted the first pre-commercial testing of pre-standard NBIoT in Spain, essentially integrating NB-IoT technology into Vodafone's existing mobile network. The water meter's IoT module received an NB-IoT message.

Water meters are usually positioned in a hidden location, such as a closet, and do not have access to electricity. NB-IoT satisfactorily addresses the challenges of low coverage and power consumption in these conditions. The following are some examples of NB-IoT applications:

- Huawei and China Unicom have collaborated to create an NB-IoT smart parking system. Thanks to Huawei's NB-IoT module, this intelligent parking system can execute operations including parking space reservation and sublet. Because of its low power consumption and high penetration, this method is more reliable.

- A smart well lid has been created by Zhongxing Telecom and China Mobile. In this approach, the state of good lids is monitored from every angle. It can keep track of whether the good lid is open or closed in real-time. This NB-IoT application's low cost, wide-coverage, low power, huge connection, and other advantages include the capacity to effectively enhance the coverage area of an intelligent well lid monitoring system, eliminate dead angles, and reduce construction and maintenance expenses.

- China Mobile, Ericsson, and Intel have collaborated on an environmental monitoring app.

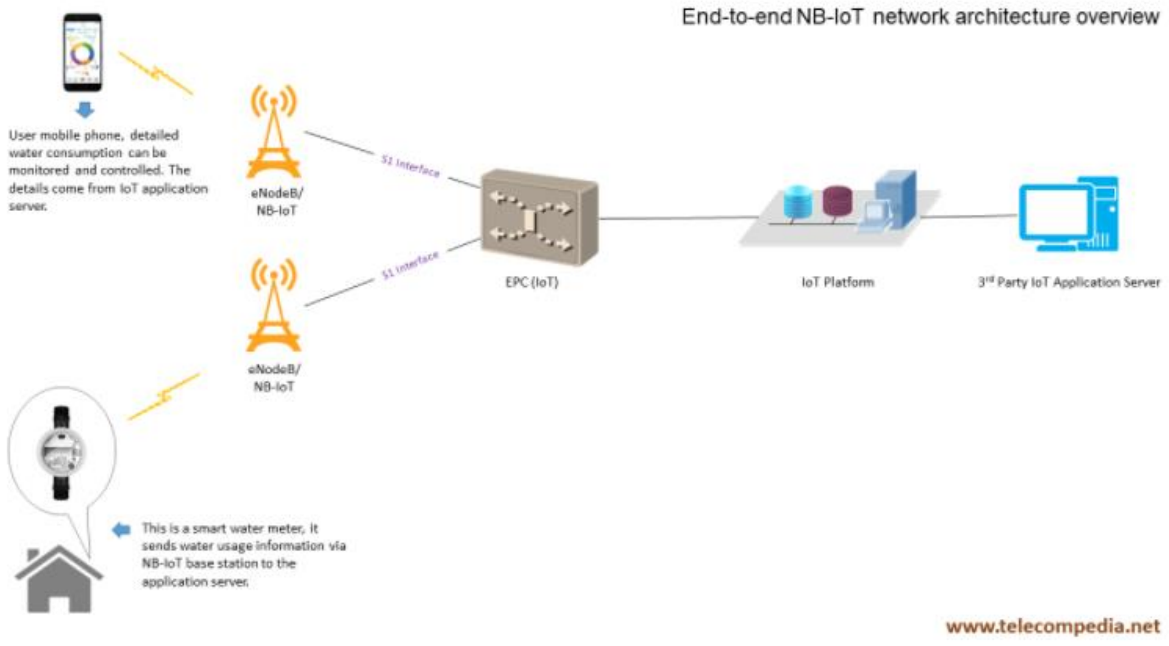
5. NB-IOT Based SMART WATER METER

The NB-IoT Smart Flow Meter gathers raw signals and sends them to a customer's automation system as pre-processed data. Water utilities and commercial applications will benefit from the NB-IoT water flow meter. Automatic data collecting and processing, data security, enhanced invoicing and accounting, and lower operational expenses are all features of the NB IoT smart flow meter.

The Internet of Things (IoT) water meter is a device that measures water usage directly and can be used as part of a water metering system. The NB-IoT smart water meter creates a direct GSM connection to a server using a secure MQTT protocol utilizing NB-IoT technology. It can be utilized as a development platform for an industrial smart water flow meter where IoT metering technologies are required.

5.1 NB-IoT network architecture:

The following figure depicts an overview of the NB-IoT network layout; in this case, a smart water meter was placed at home. It delivers water usage data to the appropriate destination regularly (3rd party application). On the other hand, the homeowner can use his or her smartphone to examine water usage information and statistics [62]**.**


End-to-end NB-IoT network architecture overview
User mobile phone, detailed water consumption can be monitored and controlled. The details come from IoT application server.
eNodeB/ NB-IoT
S1 Interface
S1 interface
eNodeB/ NB-IoT
EPC (IoT)
IoT Platform
3rd Party IoT Application Server
This is a smart water meter, it sends water usage information via NB-IoT base station to the application server.
www.telecompedia.net

35: End-to-end NB-IoT Network Architecture [62]

5.2 Key features of the NB-IoT smart water meter [63]:

- Acquires signals from a primary transducer.
- Pre-processes raw data (linearization, filtration, thermal correction, analytics)
- Manages and reports useful data such as total and instant flow rate, metering time on main/optimal/overload, battery level, temperature
- Detection of water consumption modes with separate counters for each mode
- Secured connection to a cloud/server using NB-IoT technology with MQTT protocol
- Extraordinary events can be sent to SMS and E-mail

- Secured 3 levels of access to calibrate, configure, and service check
- Self-diagnostics including a device e-passport
- Stand-alone application with 7+ years battery life

*MQTT (Message Queuing Telemetry Transport): MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc.

5.3 Which Technology to use for Smart Water Meter?

Comparison in terms of IoT factors:

When selecting a technology for an IoT application, numerous elements should be examined, including quality of service, latency, battery life, coverage, range, deployment model, and cost.

5.3.1 Quality of Service (QoS)

LoRa uses an unlicensed spectrum, it is based on chirp pulses modulation can resist multipath and interference but cannot compete with NB-IoT in terms of quality of service. This is because NB-IoT operates on a licensed spectrum, and its time-slotted synchronous protocol provides the best QoS. This benefit of QoS, however, comes at the sacrifice of cost.

5.3.2 Battery life & latency

Applications that require QoS should opt for NB-IoT, while those that do not require high QoS should opt for LoRa. As a result, LoRa is the greatest solution for applications that don't care about latency and don't have a lot of data to communicate. NB-IoT is the preferable option for applications that require low latency and large data rates.

5.3.3 Peak and Latency of LoRa & NB-IoT

Table 7 Peak & sleep currents and latency

	Peak Current	Sleep Current	Latency
LoRa	32 mA	1 µA	Insensitive to latency
NB-IoT	120/130 mA	5 µA	< 10s

5.3.4 Network coverage & range

The main benefit of LoRa is that it can cover an entire city with just one gateway or base station. For example, the LoRa network deployment in Belgium, a country with a total size of around 30500 km2, covers the entire country with generally seven base stations. NB-IoT is primarily focused on the MTC class of devices, which are put in locations that are out of normal reach. As a result, the coverage should not be less than 23 decibels. NB-IoT deployment is restricted to 4G/LTE base stations. The flexibility of the LoRaWAN ecosystem is a huge benefit. The network coverage of LoRaWAN is higher than the NB-IoT network. The below table shows the maximum coupling loss value and the range of NB-IoT and LoRaWAN.

5.3.5 MCL and Range of LoRaWAN and NB-IoT

Table 8 MCL and range of LoRaWAN and NB-IoT.

	Uplink MCL	Downlink MCL	Range
LoRaWAN	165 dB	165 dB	< 15 Km
NB-IoT	145–169 dB	151 dB	< 35 Km

5.3.6 Deployment model

NB-IoT can be deployed by repurposing and updating existing cellular networks, although deployments are limited to the cellular network's coverage region. Because the NB-IoT specification was released in June 2016, the NB-IoT network will take longer to set up. On the other hand, LoRaWAN can be deployed easily as its ecosystem is old and ready for the market.

Cost

Various cost factors must be considered, including spectrum costs, network costs, device costs, and deployment costs. The cost of NB-IoT and LoRa is shown in Table 4. It can be shown that LoRa has a significant cost advantage.

5.3.7 Cost of LoRa and NB-IoT

Table 9 Different cost of LoRa and NB-IoT

	Spectrum cost	Network& Deployment cost
LoRa	Free	$100–$1000/gateway
NB-IoT	>$500 million/MHz	$15000/base station

In conclusion, LoRa and NB-IoT have distinct advantages in terms of many IoT variables, as indicated in the table below:

5.3.8 IoT use Cases

Table 10: The IoT use cases along with parameters

Better Choice	Study cases	Major IoT categories	Parameters
	Logistics tracking Asset tracking Smart agriculture Intelligent building		

LoRa	Factories and industries Facility management Healthcare Airport management	IoT industries	Device cost, battery life,coverage
NB-IoT	Wearables Smart bicycle Kids monitoring Pet tracking Point of scale	IoT personal	Range,diversity,latency,QoS
	Smart metering Smart parking Alarm & event Detectors Smart garbage bins	IoT public	Range,diversity,latency,QoS
Depends on specific requirements	Refrigerators Air conditioner Microwave Printers Water coolers	IoT appliance	Range,diversity,latency,QoS

5.3.9 NB-IoT for Smart Water Meter

NB-IoT provides greater coverage and connectivity while consuming less power. For a smart water system, it is an ideal communications network technology.

NB-IoT is best suited for mostly static assets, such as meters and sensors in a fixed position (such as smart water meters), rather than roaming assets, despite network and tower handoffs becoming a difficulty.

6. MASSIVE IOT IN THE CITY

The Internet of Things can be divided into critical and massive applications. Traffic safety, driverless vehicles, industrial applications, and remote surgery in healthcare are examples of critical IoT applications with strict availability, latency, and reliability requirements.

Massive IoT, on the other hand, is defined by a huge number of connections, tiny data volumes, low-cost devices, and strict energy consumption restrictions; applications include smart buildings, smart metering, transportation logistics, fleet management, industrial monitoring, and agricultural [64].

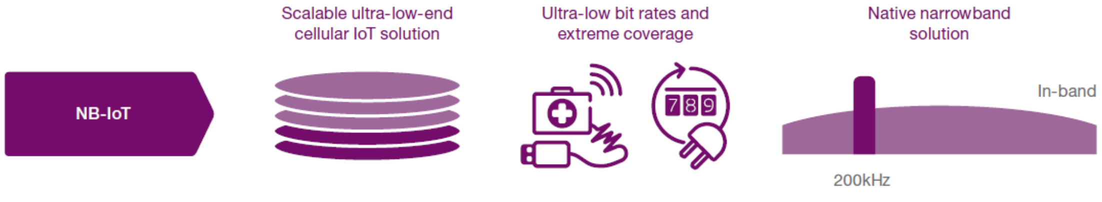
6.1 Complementary IoT technologies

These two segments cover a wide range of use cases, each with its own set of connectivity requirements. Although no single technology is adequate for all possible cases, cellular networks are suitable to handle both segments. Several cellular IoT technologies are being standardized to suit the use case needs of several possible large IoT applications, including Extended Coverage-GSM-IoT (EC-GSM IoT), Cat-M1, and Narrow Band-IoT. (NB-IoT). Depending on technology availability, use case needs, and deployment scenarios, these solutions may be complementary.

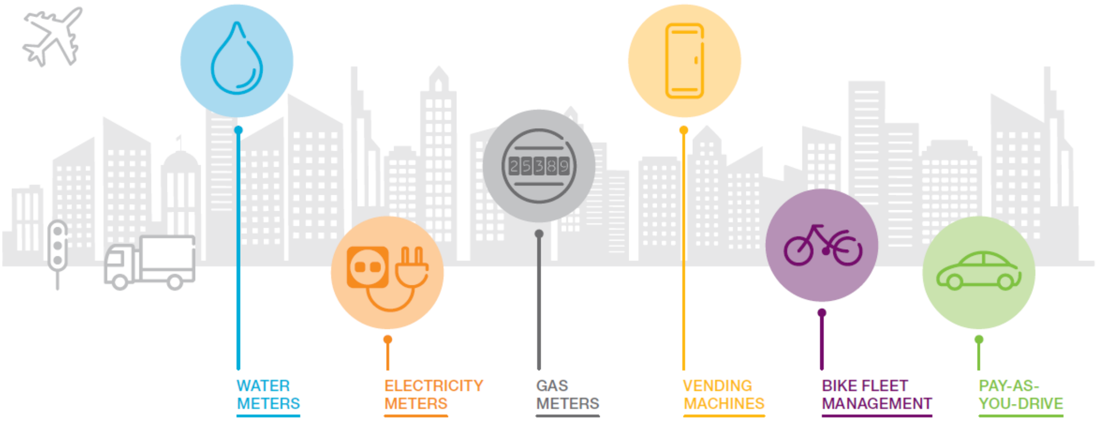
6.1.1 Ultra-low-end massive IoT applications

Knowledge of real-world IoT service scenarios and their network impact is necessary to assess cellular networks' ability to carry IoT traffic. The scenario comprises a traffic model that incorporates assumptions on message size and traffic intensity per device, as well as the number of devices deployed in a dense metropolitan area. It focuses on ultra-low-end IoT applications with modest throughput requirements, such as metering and monitoring use cases, as they are projected to be the first mass-market IoT services.

6.1.2 NB-IoT: tailored for ultra-low-end IoT applications [64]


NB-IoT
Scalable ultra-low-end cellular IoT solution
Ultra-low bit rates and extreme coverage
789
Native narrowband solution
In-band
200kHz

36: Traffic characteristics of deployed massive IoT connected devices in a city scenario [64]



37: Traffic Characteristics of deployed massive IoT connected devices [64]

Typical Message Size	100 bytes	100 bytes	100 bytes	150 bytes	150 bytes	150 bytes
Message interval	12 hours	24 hours	30 minutes	24 hours	30 minutes	10 minutes
Device Density	10,000/km2	10,000/km2	10,000/km2	150/km2	200/km2	2,250/km2

6.1.4 Massive IoT traffic scenario

The premise for a big IoT services scenario was a dense metropolitan environment with 10,000 residents per km - equivalent to the center areas of London, Beijing, or New York. A variety of linked device types, such as water, gas, and electricity meters, vending machines, rental bike position monitors, and accelerometers in cars1 tracking driver behavior, were projected to be placed in the area. The graphic above summarises the traffic characteristics for each device. This scenario's number of linked devices depicts a mature, large-scale huge IoT situation. Device density will be lower during the initial rollout phase, and the resulting traffic load will be lower.

The services reflect a realistic set of large-scale IoT use cases that are likely to be deployed in a city. These systems have different deployment environments and traffic models: a remote-controlled meter may have trouble with interior coverage, whereas a device placed on a bike is frequently found outside. Meters may just transmit once a day, however other devices may need to transmit every ten minutes.

The normal data packet for a service is roughly 100-150 bytes, accounting for a payload of the device ID, time stamp, and report data values. In addition, each packet comprises 65 bytes of IP overhead and upper-layer headers; the MAC layer overhead is 15 bytes, and normal control signaling inside the mobile network is 59 bytes per event for uplink. Each event creates around 250-300 bytes, which are relayed by the IoT device.

The resulting traffic demand is depicted in the diagram on the following page. It clearly shows that, despite the large density of devices, the low traffic per device restricts traffic per area unit to a few kilobits per second (kbps) per km2. In dense metropolitan locations, mobile broadband traffic is approaching gigabit per second (Gbps) per km.

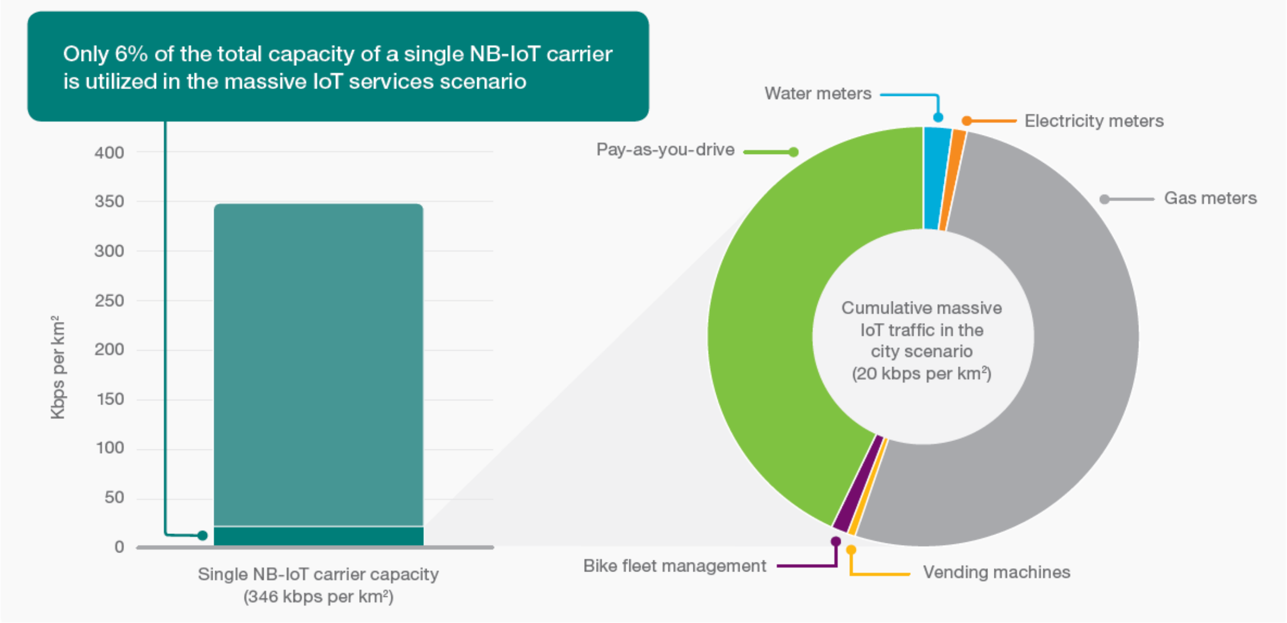
6.1.5 Deployment of an NB-IoT carrier for a massive IoT services scenario

NB-IoT is designed for extremely low-cost IoT applications. A base station may communicate with a device at the highest instantaneous data rate of 227/250 kbps in downlink/uplink, whereas the sustained maximum throughput per device is 21/63 kbps. This is more than enough to support the services in the city scenario. Despite its lesser capacity than mobile broadband, system-level simulations demonstrate that a single 180 kHz NB-IoT carrier can deliver tens of kbps, depending on carrier design.

In the city scenario, the figure below depicts the cumulative huge IoT traffic versus the capability of a single NB-IoT provider. The combined traffic from all enormous IoT services accounts for roughly 6% of total available capacity, implying that a 15-fold increase in massive IoT traffic volume over the examined scenario could be maintained before another NB-IoT carrier is required. In addition to NB-IoT, Cat-M1 enables even higher data rates and capacity.

In addition to the capacity required for traffic, coverage is required to reach devices in difficult locations. As a result, NB-IoT and Cat-M1 are intended to give far superior coverage than GSM and LTE.

6.1.6 Traffic versus capacity of a single NB-IoT carrier [64]



Only 6% of the total capacity of a single NB-IoT carrier is utilized in the massive IoT services scenario

38: Traffic vs capacity of single NB-IoT carrier [64]

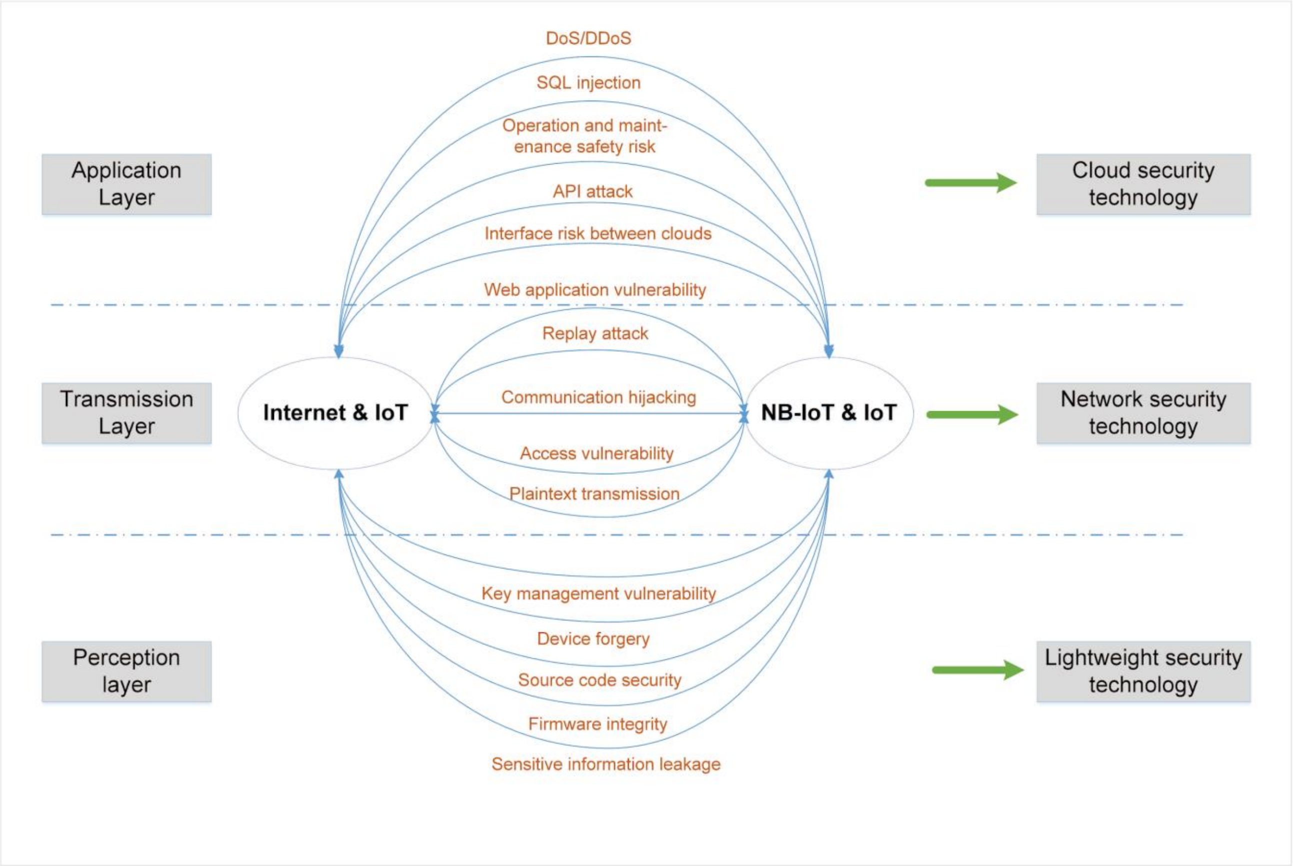
7. SECURITY REQUIREMENTS OF NB-IOT

The security requirements of NB-IoT are comparable to those of traditional IoT, as shown in the diagram. There are, however, several differences, most of which are connected to low-power IoT devices, network connection types, and actual service requirements. Traditional IoT terminal systems, for example, often have the significant processing power, complicated network transmission protocols, and more stringent security reinforcement plans; also, power consumption is typically high, and frequent charging is required. Low-power IoT equipment, on the other hand, has a low power consumption, computing capacity, and charging frequency, making security weaknesses more likely to affect terminals. Simple resource utilization can also lead to a denial-of-service problem. Furthermore, compared to traditional IoT, the number of low-power consumption IoT terminal devices implemented in practice is substantially higher. As a result, any tiny security issue might result in a large number of security incidents due to the terminal's embedded system being simpler and lighter, making it much easier for an attacker to obtain complete control of the system.

The following study focuses on the 3-layer architecture of the perception layer, transmission layer, and application layer to illustrate the security demands of NB-IoT [65].

7.1 Perception Layer

The NB-IoT perception layer is subject to both passive and aggressive attacks, just like the regular IoT perception layer. The passive assault just steals data without modifying it in any manner. Eavesdropping, traffic analysis, and other methods are all used often. Because NB-IoT relies on an open wireless network for transmission, attackers can steal data links and analyze traffic elements to gather information about NB-IoT terminals and start a series of following attacks.



39: The similarity between NB-IoT and traditional IoT in terms of security requirements [65]

In contrast to passive attacks, active assaults produce integrity damage and information fabrication; as a result, the level of injury caused by an active attack on an NB-IoT network is substantially higher than that caused by a passive attack. Data tempering, node capture, and replication are the most common attacks.

If an attacker obtains a user's NB-IoT terminal, for example, in a typical NB-IoT application, "smart meters," the attacker can modify and spoof the meter readings at will, causing direct harm to the user's critical interests.

7.1.1 How to prevent:

To prevent the above-mentioned attacks, cryptographic algorithms such as data encryption, identity authentication, and integrity verification might be used. Some of the most often used cryptology mechanisms include the random key pre-allocation mechanism, the deterministic key pre-allocation mechanism, and the identity-based password methodology. The battery life of NB-IoT equipment can theoretically last up to ten years. Because the throughput rate for perceiving data at NB-IoT nodes is low, a lightweight password (such as stream cipher and block cipher) should be employed in the perception layer for security and to reduce the computational load on terminals and extend battery life..

7.2 Transmission layer

Unlike traditional IoT, in which the transmission layer collects data and then feeds it back to the base station, NBIoT modifies the complex network arrangement in which the relay gateway takes data and then feeds it back to the base station. As a result, challenges including multinetwork networking, high costs, and high-capacity batteries have been addressed. Due to the separation of property services, a single network for the entire city can provide convenience for maintenance and management, as well as benefits like easy addressing and installation. However, new security threats have emerged:

- Access to high-capacity NB-IoT terminals

NB-IoT networks can connect up to 100,000 terminals in a single sector. To prevent hostile nodes from introducing misleading information, the main difficulty is to provide effective identity authentication and access control for these massive real-time high-capacity connections.

- Open network environment

Between the NB-IoT perception layer and the transmission layer, the wireless channel is utilized to communicate. The wireless network's fundamental flaw puts the system at risk. To disrupt communication, an attacker could, for example, send out an interference signal. Furthermore, because a single sector has a large number of nodes, an attacker might employ nodes under his control to launch a Denial of Service (DoS) assault, affecting network performance.

7.2.1 How to prevent:

Implementing an efficient end-to-end authentication and key agreement technique to assure data transmission confidentiality and integrity, as well as information legality identification, is the solution to the aforementioned concerns. For both computer networks and LTE mobile communications, key transmission security protocols include IPSEC, SSL, and AKA. The main challenge, however, is integrating these technologies into an NB-IoT system while maximizing efficiency.

On the other side, perfect intrusion detection and prevention systems should be constructed to detect illegal information inserted by malicious nodes. To be more specific, a collection of behavior profile configurations should be established and maintained for specific types of NB-IoT nodes.

7.3 Application Layer

The NB-IoT application layer's purpose is to store, analyze, and manage data efficiently. After flowing through the perception and transmission layers, a large amount of data converges in the application layer. Then large resources are constructed to offer data to a variety of applications. NB-application IoT's layer carries more data than prior IoT networks' application layers. The most significant security needs are as follows:

7.3.1 Identification and processing of massive heterogeneous data

Because of the variety of NB-IoT applications, the data generated in these applications is heterogeneous, increasing the complexity of data processing. As a result, the NB-IoT application layer's key challenge becomes detecting and administering these data efficiently while utilizing available computational resources. Real-time crisis tolerance, fault tolerance, and backup are other key factors to consider.

7.3.2 Integrity and authentication of data

The sole exception is when data integrity is compromised to varying degrees during data collection and transmission. Furthermore, insiders acting without authorization on data would compromise data integrity. As a result, the application layer's data usage may be impacted. The solution to these security challenges is to build effective data integrity checking and synchronization mechanisms. Data deduplication, data self-destruct, data flow auditing, and other technologies are also necessary to assure data security throughout storage and transmission procedures in both directions.

7.3.3 Access control of data

There are various user groups in NB-IoT. When it comes to data, different users have varying levels of access and operational authority. For users to communicate information in a controlled manner, proper authorities for different levels of users should be established. The most frequent data access control mechanisms now in use include mandatory access control methods, discretionary access control mechanisms, role-based access control mechanisms, and attribute-based access control mechanisms. Different access control measures should be established because the privacy of application scenes varies.

8. Security Vulnerabilities of Smart water Meter

Wireless water meters in an Advanced Metering Infrastructure or Smart Grid will offer the water utility a variety of relevant information to aid rate setting, leak detection, and infrastructure maintenance. On the other hand, it could expose an already weak drinking water system to further vulnerabilities.

8.1 Characteristic Vulnerabilities of Wireless Sensor Networks

A wireless water meter network is a type of Wireless Sensor Network, which is defined as a large network of resource-constrained sensor nodes that perform several functions, such as sensing and processing. The sensor nodes and the base station are the most important components of a WSN. Each water meter serves as a sensor node. There is a collection of knowledge on the vulnerabilities and security of wireless sensor networks that can be applied to wireless water meter networks. Based on the protocol stack, below is a taxonomy of probable attacks [66]:

Physical layer

(a) Jamming
(b) Radio interference
(c) Tampering or destruction

Data link layer

(a) Continuous channel access (exhaustion)
(b) Collision
(c) Unfairness – a partial DOS attack
(d) Interrogation – exhausts resources
(e) Sybil attack – single node presents numerous identities

Network layer

(a) Hello Flood
(b) Node capture – the capture of one node can allow the takeover of an entire network
(c) Selective forwarding/ Black Hole Attack (Neglect and Greed)
(d) Sybil attack
(e) Wormhole attack
(f) Spoofed, altered, or replayed routing information
(g) Acknowledgement spoofing
(h) Misdirection

(i) Internet smurf attack
(j) Homing

Transport layer

(a) Flooding
(b) De-synchronization attacks

Application layer

(a) Overwhelm attack
(b) Path based DOS attack
(c) Deluge (reprogram) attack

Wireless Sensor Networks face several security issues, including the wireless medium itself, unattended operation, unpredictable topology, and the difficulty of defending against insider attacks. To extract the information about the network and nodes, an attacker can sniff the packet and can modify the usage of the nodes. The sniffer allows the attacker to breach confidentiality by identifying the hardware platform being used, the type of application being used, the frequency of events being watched, and routing information [67].

8.1.1 What kind of damage could a hacker cause to the smart grid?

1) When the smart grid uses public IP addresses, DDoS assaults are possible.
2) Because each meter is a node in the smart grid network, an attacker who uses the smart meter's communication module might trigger network-wide modifications.
3) Because many meters lacked authentication and encryption, an attacker might pose as the control center and send unauthorized commands to meters or read metering data.
4) Because its impact is limited to a single customer household, the protocol between the master meter and slave meter is usually considered of lesser importance; however, this may allow the insertion of a "man in the middle" device to lower the usage reading, which could have a significant impact on the utility of such devices are mass-produced like pirate cable boxes [68].

8.1.2 How hacker can damage the water utility system?

1) Interfere with the functioning of chemical feed systems, resulting in dosage errors.
2) Make unapproved programming changes that result in disabled services, lower water pressure or reduced water flows into fire hydrants.

3) Change the software in the control system to cause unforeseen consequences.
4) To keep operators from being aware of alarm situations, block data or transmit fake information to them.

5) Alarm thresholds can be changed or disabled.
6) Multiple failures may occur, which may be too much for the facility to handle.
7) It could be used as ransomware.

8.2 Security Issues in Advanced Metering Infrastructure (AMI):

AMI system consists of three elements namely: Smart devices, communication networks, and data management systems. It provides utility providers with a wealth of data, including real-time measurements, voltage monitoring, load control, power outage detection, and much more, via two-way communication. This useful information can also be passed on to a third party for additional research. It also allows utility companies to control, connect, disconnect, and even configure the energy service remotely [69]. Consumers, on the other hand, can control their power usage, pay bills, and sell back electricity at different times of the day using a variety of Internet-based applications. This infrastructure connects the renewable energy generated on the consumer's property to the smart grid in an effective manner [70].

The smart meter collects metering data and sends it to the AMI host system through a fixed network, such as power line communications, fixed radiofrequency, or broadband over the power line (BPL). The data is then routed to data management systems for storage and processing, after which it is supplied to service providers or utilities.

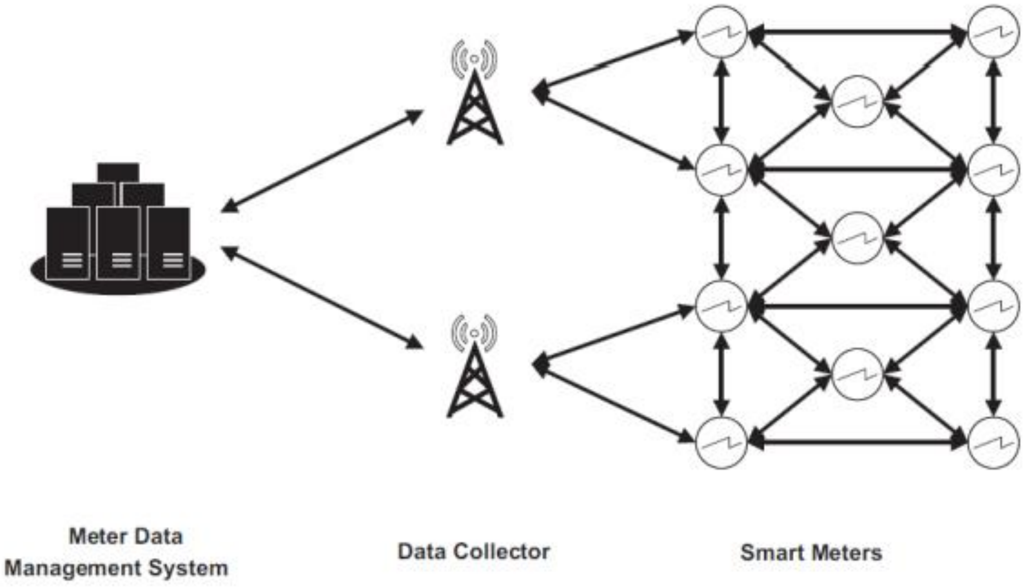
8.2.1 Smart Devices

The AMI is made up of many sorts of smart devices that differ depending on whether the user is a consumer or a supplier. Clients or consumers have smart meters installed in their homes that collect metering data and send it to the service provider. It also takes and acts on commands from both the consumer and the service provider. Other smart devices include an in-home display (IHDs), which assist users in being more aware of their energy consumption and controlling it, for example, using mobile applications. Service providers, on the other hand, are typically provided with load controlling devices (thermostats) to manage user use depending on various parameters.

Different sensors, including humidity, light, temperature, and motion detection sensors, can be utilized to collect other types of data that a smart meter might collect to help control energy consumption. Net metering, the capacity to interface with other intelligent equipment such as sensors, demand response directives, and time-based pricing are all characteristics of smart meters. Data encryption and energy theft detection are examples of other security measures [71].

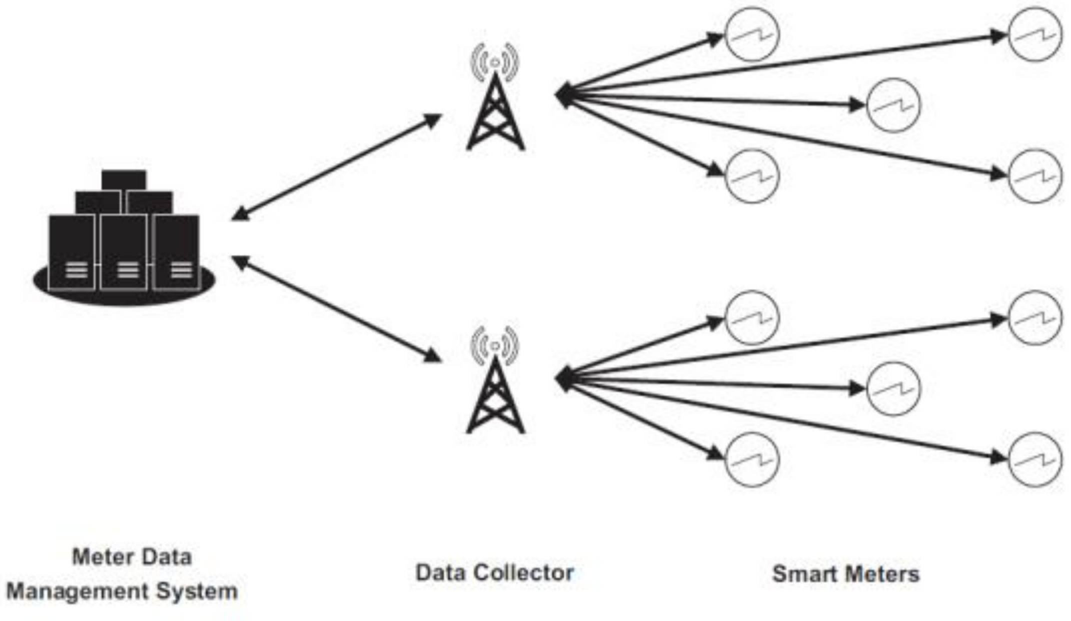
8.2.2 Networking

A dependable communication network is an important part of the AMI since it is responsible for transmitting metering data from smart meters and other smart devices to service providers and vice versa. As a result, it must be able to transfer large amounts of data, manage access, ensure data confidentiality, maintain the integrity and precision of the transferred data, and be cost-effective. The communication network may be mesh or point-to-multipoint in topology, depending on the implementation needs. Neighboring smart meters are daisy-chained in mesh networking to forward, receive, and store sent data until it is received by the data collector, as shown in Fig.



40: Mesh Network Topology [72]

Smart meters can connect with one data collector whereas data collectors can communicate with several meters in a point-to-multipoint network structure, as shown in Fig. When compared to the unlicensed ISM band, it usually uses the licensed RF spectrum, which has less noise. As a result, data collectors and meters are able to communicate with each other over long distances [72].



41: Point-to-multipoint Network technology [72]

8.2.3 AMI Main Components

Table 11: AMI MAIN COMPONENTS AND SUBCOMPONENTS [73]

Smart Meter	Data Collector	Communication Network
Control unit	Control unit	Smart Meter Collector (RF)
Metrology System	Smart Meter Collector	HAN (ZigBee)
Smart Meter Collector	GPRS Receiver	Optical Port
HAN	USB Interface	
Optical Interface	Ethernet Interface	

8.2.4 Data Collector Security

The data collector is the brain behind the AMI system. Its security is critical since it links to several smart meters and will affect a huge number of users. The control unit and smart meter collector in the data collector are identical to those in the smart meter. Attacking the main unit or the smart meter collector in the data collector, on the other hand, has a significant influence on metering operations and power denial. Furthermore, the hardware change would use an open interface to install malicious software to operate the machine, infecting all smart meters linked to it.

The GPS receiver is in charge of synchronizing all of the AMI component's data as well as their timestamps. Interception attacks could result in data manipulation result in manipulation of configuration and the bills of the consumers.

8.2.5 AMI Possible Attacks

Table 12: AMI POSSIBLE ATTACKS [73]

Attack	Attack Surface	Scope of Impact
Eavesdropping	Remotely through WAN or power line	Difficult to detect and expose consumer's privacy
Denial of Service (DoS)	Remotely through WAN	The whole or part of the grid including the AMI
Packet Injection	Through WAN	False billings for both consumers and service provider
Remote Connect/Disconnect	Through WAN	Ranges from single premises to the whole grid
Firmware Manipulation	Physical access to the smart meter/ Remotely upgrade through WAN via the gateway	Affect the metrological and nonmetrological part of the smart meter, can affect single to multiple gateways
Man-in-the-Middle	Inside local metrological network (LMN) or WAN	False measurements for one gateway in a case inside the LMN or all meters connected to the gateway in the case via WAN

Security Attacks

8.3.1 Eavesdropping

Eavesdropping is a passive attack in which the attacker listens in on information sent to service providers by a smart meter or a smart metering gateway.
This type of attack compromises client privacy and can be carried out very easily using a wireless communication channel or a power line. Such attacks are extremely difficult to detect. The WAN is the most common way for such an attack to be launched.

8.3.2 Denial of Service Attacks

This type of assault is aimed at the entire smart metering system, the smart grid, or a portion of it. An adversary may carry out such an assault by sending far more commands than expected to the smart metering gateways or, on the other end, the utility servers. This will overburden the system to the point where it will no longer be able to reply to legitimate queries. It will effectively shut down the grid, or at least a portion of it, for critical services. This attack targets the entire grid or portions of a grid. The majority of such attacks are carried out over the internet.

8.3.3 Packet Injection Attacks

Packet injection attacks can be done by inserting a malicious packet into the network. This might be done to disable elements of the smart metering system or to compromise the billing process by issuing erroneous bills, which would cost customers and utilities a lot of money. Typically, such attacks will be launched through the WAN.

8.3.4 Remote Connect / Disconnect

Attackers can use connect and disconnect attacks to make the grid into a halt situation. This attack might leave a number of people without access to electricity and water. Such attacks might range in scale from a single premise to the entire grid. The WAN can be used to launch such attacks.

8.3.5 Firmware Manipulation

The firmware of a smart meter or a metering gateway is manipulated in such attacks. Manipulation could be directed at either the metrological or non-metrological components. Manipulation of the pre-payment capability or misleading consumption status reporting to the remote readout entity are examples of this. Other goals can be obtained by manipulating the non-metrological portion. Physical access to a smart meter (or a smart meter gateway) can be used to carry out firmware tampering attacks. If the gateway allows remote firmware updating, such attacks can also be launched over the WAN. These attacks usually target a single person (or a single location/building), but they can also be carried out on a broad scale by remotely altering the firmware of a large number of gates.

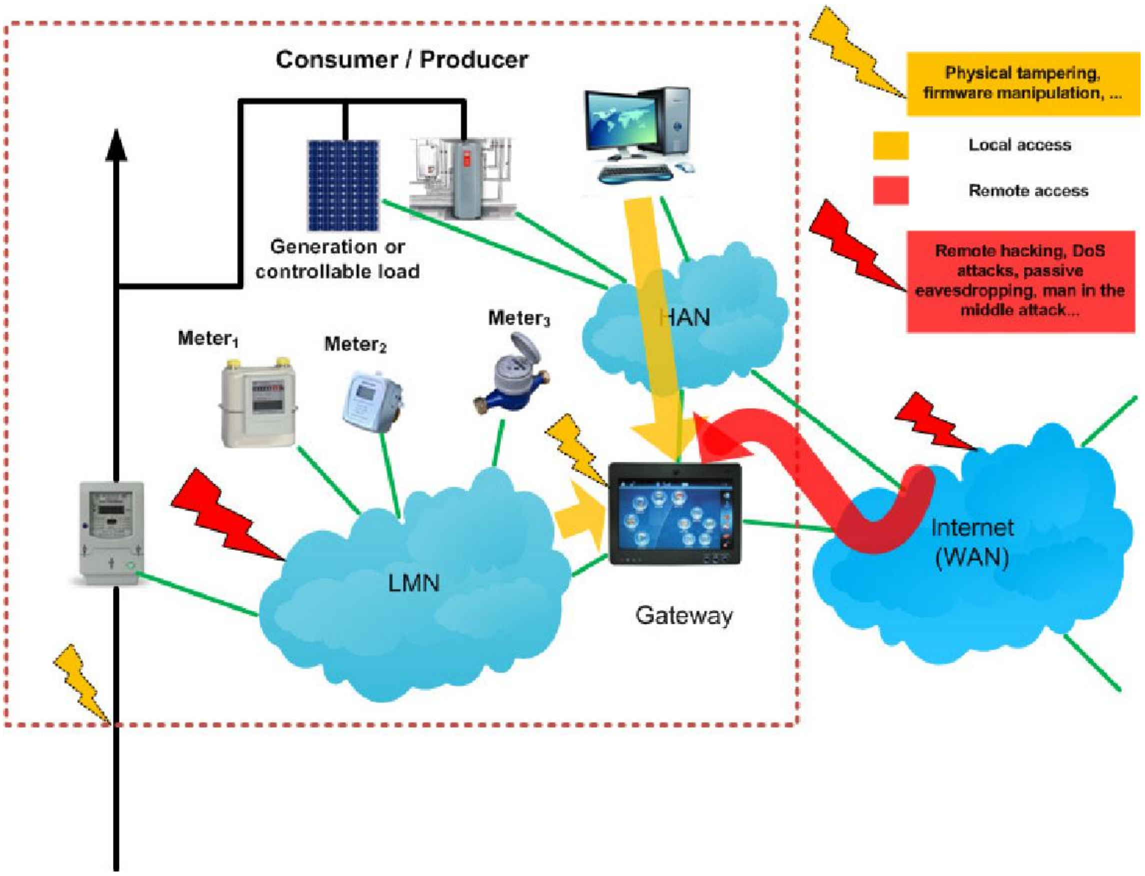
8.3.6 Man-in-the-middle Attacks

A man-in-the-middle attack is one in which an attacker "inserts" himself between two parties who are communicating. An attacker establishes a connection with both parties, intercepts their messages, and relays them to the other end, giving the impression that they are speaking directly to one another. As a result, the attacker has the option of passively listening in or actively altering the information being exchanged between the communication participants.

A man-in-the-middle attack can be undertaken inside the LMN or the WAN in the context of smart metering. It can be used to compromise communication between a meter and a gateway and deliver false feedback to the gateway if launched in the LMN. As a result, the gateway will send incorrect measurements. If an assault is conducted in the WAN, the entire communication's security and privacy may be jeopardized. The data in transit, such as the measurements of all the meters transferred by the gateway to the distant center, can be seen and tampered with. Attackers can also fabricate and spoof commands sent from a remote authorized entity to the gateway. This can be even more dangerous since if such attacks are carried out on a wide scale, the attackers may be able to bring down the entire grid and its related businesses, posing a threat to a country's national security. TLS alone is no longer considered secure enough to protect against man-in-the-middle attacks.

8.3.7 Communication Network Security

There are two main communication routes: one between smart meters and data collectors, and the other between smart meters and equipment in the consumer's home. RF and ZigBee standards are typically used in smart meter collectors and HANs in communication networks, respectively. Intercepting any of these standards exposes consumer data and compromises its integrity. Man-in-the-middle attacks, denial-of-service assaults, data theft, power theft, and grid disruption are all possible major threats [74].


Consumer / Producer
Generation or controllable load
Meter$_1$
Meter$_2$
Meter$_3$
HAN
LMN
Gateway
Internet (WAN)
Physical tampering, firmware manipulation, ...
🟨 Local access
🟥 Remote access
Remote hacking, DoS attacks, passive eavesdropping, man in the middle attack...

42: Security Attacks and the Location Where Attack Can Be Launched in the Network [74]

9. Security Controls and Countermeasures

To preserve the AMI's availability and efficiency, effective security countermeasures must be implemented:

9.1 Encryption

The AMI's communication between multiple nodes must be encrypted. Data secrecy can no longer be guaranteed by relying on the TLS protocol. As a result, other encryption techniques, such as RSA, must be included in both the application and transport layers. Another option is to use message authentication codes (MAC) to protect the AMI readings' integrity. Proposes another encryption approach in which aggregated data is encrypted at the gateway using homomorphic encryption, which permits selective calculations on the ciphertext to obtain encrypted outputs. When decrypted, the plaintext matches the results of the processes performed on it [75].

9.2 Authentication Mechanism

For the consumer to authenticate the AMI with whom He/she is speaking, as well as for the AMI to check the validity of the legitimate consumers, accurate verification of the source of the data is vital. The consumer, for example, is given a password to generate a public-private key that will be used to establish authentication between the AMI and the power utility.

9.3 Availability Mechanism

Several vulnerabilities, including network jamming and packet flooding, can have a significant impact on the AMI's availability. If the default channel is unavailable for a set amount of time, a robust AMI can be programmed to go through defined channels of other frequencies. Furthermore, limiting network traffic would prevent ping requests from overwhelming the network and rendering it inaccessible to legitimate users. Another method for mitigating DoS is to keep the ARP cache static, so that suspicious ARPs cannot change their content with malicious IP/MAC payloads. Furthermore, prohibiting high-speed traffic from reaching the meter's kernel would greatly reduce DoS assaults [75].

9.4 Gateway based Approach

Gateway is a new smart metering solution proposed by European countries such as Germany and the United Kingdom. A gateway is a technology that allows smart meters and the smart grid to communicate in the future. A gateway (also known as a smart metering gateway) serves as a communication link between the utility and the metering equipment on the customer's premises. The gateway is responsible for ensuring the customer's privacy as well as serving as a communication and control device between the meters and the utility. The gateway communicates with the utility servers through WAN regularly. The load distribution controller also sends instructions to the gateway based on the load in the smart grid.

9.5 Intrusion Detection and Prevention Systems

In the networks of a smart metering system, intrusion detection systems (IDS) and intrusion prevention systems (IPS) could be employed. This aids in the detection of intrusions, the detection of rogue nodes or attack sources, and the exclusion of these nodes from the future network connection.

10. Conclusion

The Internet of Things (IoT) is a new internet application that ushers in a new era of smart technology in which thing-to-thing communication replaces human-to-human communication. Every object in the world can be identified, connected, and make decisions on its thanks to the Internet of Things. In the not-too-distant future, the Internet and wireless technologies will increasingly connect disparate sources of data, such as sensors, mobile phones, and automobiles. The number of devices connected to the Internet is growing at an apparent exponential rate.

In this project, we studied the 5G Technologies their IoT applications, and lastly, the security vulnerabilities of the IoT-based smart water meter.

We have done this project in four parts.

In the first part, we studied the 5G technology and its protocol stack. We have studied the Core Network and the NG Ran (radio access network) Architecture and its future scopes.

In the second part, we studied the IoT and its applications, architecture, applications in IoT in different fields, and the security challenges.

In the third part, we studied the IoT-based smart water meter and its different types. We did some research on smart water meter communication technologies and after that, we concluded that NB-IoT is best suited for SWM. In the end, we shared one use case of Massive IoT traffic scenario.

In the fourth part, we studied the security requirements of NB-IoT, security vulnerabilities of smart water meter, AMI possible attacks, and known security attacks and their countermeasures.

References

[1] A.K.Pachauri, “5G technology-Redefining Wireless Communication in upcoming Years,” 2012.

[2] A. M. (. Mousa, “Prospective of Fifth Generation Mobile communications. International Journal of,” 2012.

[3] C. K. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems,” 2002.

[4] [Online]. Available: https://www.ecstuff4u.com/2018/05/1g-technology-advantages-and.html.

[5] T. N. rao, “5G Technologies Anecdote of Network service for the future proceedings of the JGRCS,” 2011.

[6] T.Rapaproot, “Wireless Communication and Networks 2nd edition,” 2011.

[7] W. Lee, “Cellular and Mobile Communication,” 2010.

[8] “telecombac.com,” [Online]. Available: http://www.telecomabc.com/g/gmsc.html.

[9] “Network_Switching_Subsytem,” [Online]. Available: https://en.wikipedia.org/wiki/Network_switching_subsystem.

[10] W. Stalling, “Data and Computer Communication,” 2011.

[11] G. A, “Wireless Communications,” Cambridge University Press, Cambridge,, 2005.

[12] A. W. &. S. Mishra, Fundamentals of Cellular Network Planning and Optimisation. John Wiley & Sons, 2004.

[13] “network-evolution-3g-vs-4g-vs-5g,” [Online]. Available: https://medium.com/@sarpkoksal/core-network-evolution-3g-vs-4g-vs-5g-7738267503c7.

[14] D. Y. L. Amit kumar, Evolution of Mobile Wireless networks: 1G to 4G, 2010.

[15] K. J, Introduction to 4G Mobile, Artech House, London,, 2014.

[16] Qualcomm, “The evaluation of Mobile Technologies: 1G, 2G, 3G, 4G LTE',” 2014.

[17] “intechopen,” [Online]. Available: (https://www.intechopen.com/chapters/9699).

[18] “techdifferences.com/difference-between-3g-and-4g-technology,” [Online]. Available: https://techdifferences.com/difference-between-3g-and-4g-technology.html.

[19] “discover-5g-core-network-functions-compared-4g-lte,” [Online]. Available: https://www.linkedin.com/pulse/discover-5g-core-network-functions-compared-4g-lte-paul-shepherd/.

[20] “5G mobile Technology Abstract Available,” [Online]. Available: http://www.seminarsonly.com/Labels/5g-Mobile-Technology-.

[21] M. Hata, Fourth Generation Mobile Communication Systems Beyond IMT-2000 Communications, 1999.

[22] “Network Evolution,” [Online]. Available: .http://www.u5gig.ae/5G%20Core%20Network%20Evolution%20for%20NSA%20and%20SA.pdf.

[23] E. T. 1. 3. V15.3.1, “3GPP TS 38.300 version 15.3.1 Release 15,” 2010.

[24] R. K. a. D. Furlonger., “Blockchain-Based Transformation.,” 2018. [Online]. Available: https://www.gartner.com/en/.

[25] “Gsma. Safety, Privacy and Security,” 2019. [Online]. Available: https://www.gsma.com/publicpolicy/resources/safetyprivacysecurity-.

[26] M. J. O. G. J. H. X. A. M. R. P. L. G. Yang, “IoT-based remote pain monitoring system,” 2018.

[27] “Flashpoint. Mirai Botnet Linked to Dyn DNS DDoS Attacks,” 2018. [Online]. Available: https://www._ashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/.

[28] Z. Z. R.-g. H. F. U. Chang-le Zhong, “Study on the IOT Architecture and Access Technology,” china, 2017.

[29] V. K.Yogitha, RECENT TRENDS AND ISSUES IN IOT, 2016.

[30] N. N. D. a. K. Johnston, The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses, 2016.

[31] M. S. P. D. (. B. T. Nandhini1, Survey on Internet of Things Architecture, 2016.

[32] R. W. ,. D. G. K. P. ,. G. C. R.A. Stewart, Web-based knowledge management system: linking smart metering to the future of urban water planning, 2010.

[33] “Badgemeter,” [Online]. Available: http://www.badgermeter.com.

[34] E. Idris, “Smart metering: a significant component of integrated water conservation system,” in *Proceedings of the 1st Australian Young Water Professionals Conference, International Water Association, Sydney, 2006*, sydney.

[35] "elsteramcowater," [Online]. Available: http://www.elsteramcowater.com.

[36] "sensus," [Online]. Available: http://sensus.com.

[37] "aem," [Online]. Available: http://www.aem.ro.

[38] "itron," [Online]. Available: https://www.itron.com.

[39] "Water Meter Implementation with MSP430FR4xx User's Guide," Texas Instruments, texas, 2014.

[40] "Microcontrollers in Flow Meters," Texas, 2012.

[41] N. Chang, "Smart Gas and Water Meter Trends: Impacts on Meter Designs," 2012.

[42] O. Monnier", " A Smarter Grid with the Internet of Things",," Texas Instruments October, 2013.

[43] P. C. K. R. Amanda Blom, "Developing a Policy Position on Smart Water Metering," 2010.

[44] "The Smart Meters:What are the different types, how do they work".

[45] K. A. F. R. I. R. H. M. G. K. A. N. P. H. H. R. R. M. a. F. S. M. Mamun, "Smart water quality monitoring system design and KPIs analysis," case sites of fiji surface water." Sustainability , 2019.

[46] Y. L. a. M. Chen, "Software-defined network function virtualization," 2015.

[47] Y. L. M. C. D. D. J. a. S. C. X. Hou, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," Transactions on Vehicular Technology, vol. 65, 2016.

[48] "5g wireless technology framework," IMT2020, Tech. Rep, 2015.

[49] "Standardization of Machine-type Communications,," 3GPP, 2014.

[50] "Feasibility Study on New Services and Markets Technology Enablers," 3GPP TR 22.862, 2016.

[51] D. g. a. Y. junhua, "Research on nb-iot background,standard development, characteristics and the service," Mobile," 2016.

[52] X. H. Y. W. M. C. Q. L. T. H. a. C.-X. X. Ge, "Energy efficiency optimization for mimo-ofdm mobile multimedia communication systems with qos constraints," 2014.

[53] D. x. a. W. q. Z. yulong, "Key technologies and application prospect for nb-iot," 2017.

[54] D. j. a. L. n. L. wei, "Nb-iot key technology and design simulation method," 2016.

[55] F. A. Tobagi, “Distributions of packet delay and interdeparture time in slotted aloha and carrier sense multiple access,” 1982.

[56] A. E. T. a. S. A. M. Islam, “A survey of access management techniques in machine type communications,” Communications Magazine IEEE vol. 52, 2014.

[57] Z. li, “Research on low cost mtc indoor coverage enhancement,” Ph.D. dissertation, 2014.

[58] “Cellular system support for ultra-low complexity and low throughput cellular internet of things,” 3GPP TR 45.820, 2015.

[59] S. J. a. D. Qiao, “Numerical analysis of the power saving in 3gpp lte advanced wireless networks,” 2012.

[60] L. L. G. V. a. S. B. N. M. Balasubramanya, “Drx with quick sleeping: A novel mechanism for energy-efficient iot,” IEEE Internet of Things Journal, vol. 3, no. 3, pp..

[61] R. Y. S. X. Y. Z. a. D. T. W. Zhong, “Software defined networking for flexible and green energy internet,” IEEE Communications Magazine, vol. 54, 2016.

[62] “telecompedia,” [Online]. Available: https://telecompedia.net/nb-iot/.

[63] “rd-technoton.com,” [Online]. Available: https://rd-technoton.com/nb-iot-smart-water-meter-industrial.html.

[64] Ericsson, “MASSIVE IOT IN THE CITY,” EXTRACT FROM THE ERICSSON MOBILITY REPORT, 2016.

[65] S. z. a. H. hanshu, Security issues of nb-iot, ZTE Technology,vol. 23, 2017.

[66] T. a. D. S. J. o. I. A. a. S. Kavitaha, “Security vulnerabilities in wireless sensor networks,” 2010.

[67] T. G. a. T. Dimitriou, “Weaponizing wireless networks: An attack tool for launching attacks against sensor networks,” 2010.

[68] “The Dark Side of the Smart Grid – Smart Meters (in)Security,” 2009.

[69] G. &. D. M. Barnicoat, “ The ageing population and smart metering: a field study of householders’ attitudes and behaviours towards energy use in Scotland,” 2015.

[70] Y. Q. H. S. a. D. T. Y. Yan, “A survey of smart grid communication infrastructures: Motivation, requirements and challenges,” 2013.

[71] T. I. R. S. O. &. T. K. Ueno, “. Effectiveness of an energy-consumption information system for residential buildings,” 2006.

[72] V. N. V. S. S. &. J. W. Aravinthan, “Wireless AMI application and security for controlled home area networks,” 2011.

[73] M. D. X. S. S. H. &. B. E. (. Nabeel, “Scalable end-to-end security for advanced metering infrastructures,” 2015.

[74] N. Z. C. R. Obaid Ur-Rehman, “Security Issues in Smart Metering Systems”.

[75] K. T. Z. A.-H. M. G. A. &. A. M. Shuaib, “Resiliency of Smart Power Meters to Common Security Attacks,” 2015.

[76] “Cellular system support for ultra-low complexity and low throughput cellular internet of things,” 3GPP TR 45.820, , 2015.