A WIRELESS COMMUNICATION SYSTEM WITH HIGH RELIABILITY AND LOW LATENCY FOR THE INTERNET OF THINGS: ISSUES, FOUNDATIONS, AND TECHNOLOGIES.

Priyabrata Mohapatra

MTech in Electronics and Communication

Odisha University of Technology and Research, Bhubaneswar

Abstract: ***The Internet of Things (IoT) has seen substantial technological and application development. By 2020, it is predicted that wireless IoT networks will connect more than 25 billion devices. The whole communication protocol stack for wireless IoT networks has to be reconsidered directly in the research, researchers examine numerous HRLL wireless IoT network application scenarios, underlying performance constraints, and possible future technologies. Researchers also get across the network structure that has been adjusted to reduce latency. Many IoT applications, such as industrial automation, vehicle-to-everything (V2X) networks, smart grids, and remote surgery, will demand strict transmission latency and reliability requirements in addition to ubiquitous connectivity, which may not be provided by current systems. Because they need low-latency, high-reliability links to maintain stability, high-performance internet of things control systems with tens to hundreds of sensors and actuators use wired connections between all of their parts. However, the wires lead to many reliability issues that switching to wireless links would solve. So, they are made for either high-throughput or low power communication between a pair or a limited number of terminals, current or proposed wireless system can provide the latency and dependability required by the control algorithms. It is proposed to employ low-rate coding, semi-fixed resource allocation, and reliable broadcasting to achieve low-latency operation in a wireless system. The sixth-generation (6G) system, a new wireless communication paradigm with full AI support, is anticipated to be put into use between 2027 and 2030. Beyond 5G, some essential concerns that need to be solved include larger systems capacity, faster data rate, lower latency, higher security, and enhanced quality of service (QoS) compared to the 5G system. The number of wireless gadgets will exceed the number of people in the near future, and most of these devices will communicate with each other rather than with humans.***

The Internet of Things (IoT) will require low-latency, high-reliability communication with reasonable data rates. High-performance industrial control is one of the few applications that have IoT-like needs at this time. People-centric networks don't require high data speeds to function closed loop. As providing low-latency and high-reliability operation for a significant number of users, present WLAN and cellular systems struggle. An early wireless system architecture is intended to address this problem. Utilizing numerous, cooperating access points that are dispersed across the system, similar to coordinated multipoint in cellular networks, is one possibility. Another choice is based on distributed space-time codes. The second section of the paper examines the analogue front end, modulation, baseband processing, and multiple access protocol

as they relate to constructing the physical layer of the suggested cooperative relaying system architecture. The use of as many building pieces from existing systems as feasible is prioritised. High-reliability wireless systems must have efficient hardware, and error control decoders are a crucial component. The construction of a low-latency, low-power LDPC decoder for the IEEE 802.11ad standard, whose LDPC codes include numerous properties suitable to wireless control, is covered in the third section of this study. The decoders deeply pipelined, highly parallel, coding architecture strikes a balance between power and latency. Row-merging, multi-codeword processing simultaneously, lower memory accuracy due to marginalisation, and back-biasing to effectively balance active and leakage power further cut down on latency and power. Authors give a thorough explanation of the functions of 6G in several fields many potential IoT applications across five core categories, including the Internet of Things for Healthcare and the Internet of Things for Vehicles and Satellite, Unmanned Aerial Vehicles, and Autonomous Driving Industrial Internet of Things .

Chapter 1

INTRODUCTION

1.1. Introduction

Our societies and industries have grown more intelligent as a result of the quick development of computing and communication technology; this is known as a "smart society" or "smart industry." 4.0(also known as a smart factory) Several enabling technologies, including for linking, IoT (Internet of Things) is essential different heterogeneous smart society/factory technology. Unlike the majority of currently operating mobile networks are human-cantered IoT aims to link many people through communications of equipment that requires no or little human input [1]. The programs involve control, intelligent identification, and monitoring Location, tracking, and monitoring, among other things, for the diversity of the technological diversity of IoT networks' devices and applications, IoT network needs can range widely and sometimes may be rather difficult. several applications for IoT networks might need to be very reliable and responsive high reliability and low-latency. (HRLL), like commercial such as vehicle-to-everything, industrial automation, Smart grids, (V2X) networks, remote surgery, etc. In the existing systems, the devices were frequently linked together by means of small networks, such as Highway Addressable Remote Transducer (HART)and MIMO [2], Wireless Interface for Sensors and Actuators Wireless Networks for Industrial Automation for Process Automation (WIA-PA) [3], and WIAFA , which are based on the IEEE 802.11 series standards. These standards depicted as in figure 1.1, however, are unable to gradually meet the latency and reliability requirements of future applications. IoT networks must be able to offer high dependability, low latency, and huge connection in numerous circumstances (large scale). There have been several recent research attempts on HRLL IoT to suit the objectives.

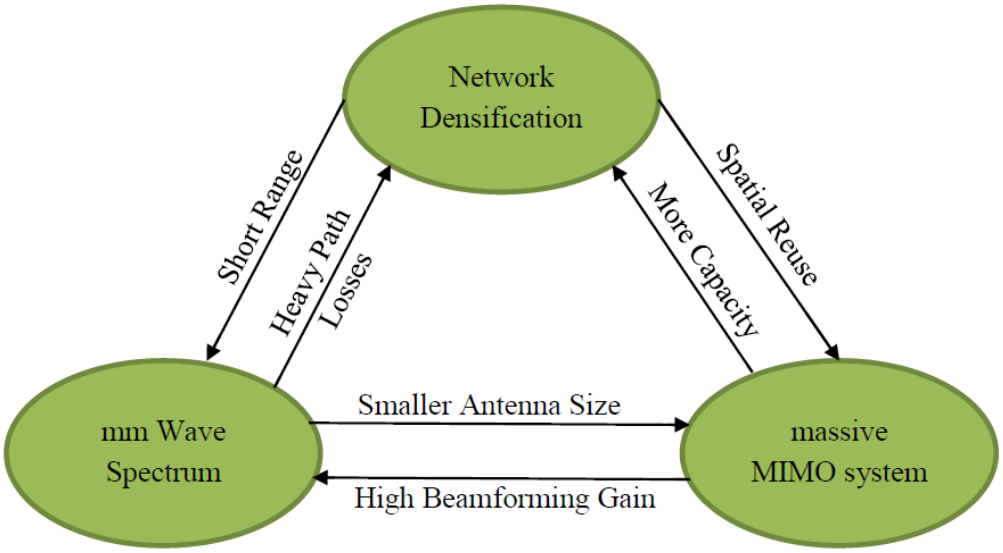

Figure 1. 1: Relation between Three-design Aspects for Upcoming Wireless Communication Systems.

- Millimeter Wave Spectrum - Shift towards higher available bandwidth
- Massive MIMO and Beamforming. - Higher Spectral Efficiency
- Small Cells - Network densification to overcome heavy path losses

Communication is the process of accurately recreating information at a sink after it has been correctly sent from a source over a physical channel. Analog or digital methods can be used to transfer the information. In analogue communication, the source signal is often used to modulate the amplitude or frequency of the carrier signal. Am/FM radios and conventional telephones are two examples of such systems. Digital communication, on the other hand, changes the source signal into symbols and delivers a unique signal for each symbol value [3]. There are many examples of digital systems, such as the telegraph and any packet switching network. Before the invention of the transistor and the discovery of information theory, both kinds of communication were widely used, but since then, digital communication has taken over and is a crucial component of everyday of life. These "Smart Cities" must now be affordable and energy-efficient in order to compete. When battery-powered operation is required, Low Power Wide Area Networks (LPWAN) have become an efficient wide area connection option. There are several various short range Wireless Personal Area Network (WPAN) and Wireless Local Area Network (WLAN) technologies that may be used to link IoT devices to the Internet, including Wi-Fi, Bluetooth, ZigBee, X-Bee, Z-Wave, M-Bus, etc[4]. The figure 1.2 presents a symbolic view of the evolution of associated user services from 2G to 5G.

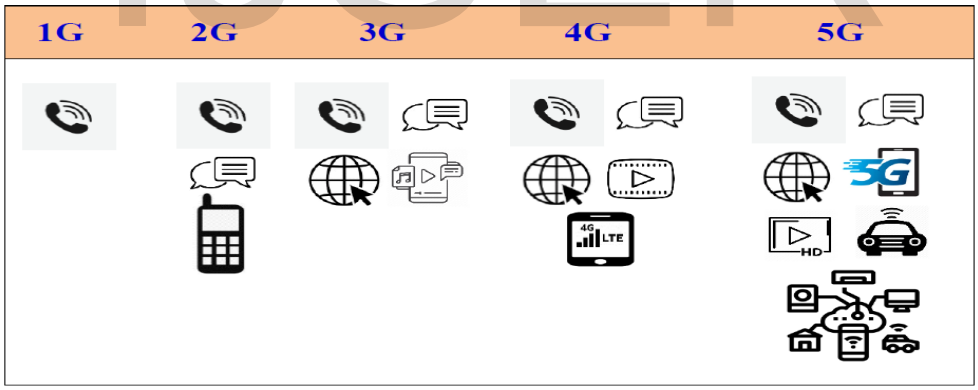

Figure 1. 2: Evolution of Services form 2G to 5G.

1.2. HRLL IoT Networks Application Scenarios

Following, we'll go into great depth on a few typical HRLL IoT network application scenarios, such as smart grids, vehicle networks, and industrial automation.

- **Industrial Automation**

A new generation of industrial revolution, known as industry 4.0, has significantly altered our industry's production process as a result of advancements in computer, control, and communication

technology. Industry IoT (IIoT), a crucial enabling technology of industry 4.0, has recently gained a lot of academic interest. Many of the current industrial communication networks are really built on wired networks, such Ethernet or optical fibre. However, replacing wired networks with wireless ones has been a current IIoT trend[5]. The first industrial wireless network has been utilised in real-time control applications due to its potential advantages, such as cheap cost, flexibility, and appropriateness in harsh settings or mobile circumstances. Following then, several initiatives for the development and standardisation of connected devices Examples include Wireless HART, WIA-PA, and the WIAFA. The benefits of using wireless networks over wired ones are numerous and include: (1) Wireless networks may result in significantly lower costs for materials, installation, commissioning, and maintenance; (2) Wireless networks may be more reliable in many situations, such as those involving cables subject to ageing and breaking, and it may be simpler to obtain redundancy links with wireless networks, even in the presence of channel fading or interference[6].

Another category of HRLL standardization is conducted by IEEE and International Electrotechnical Commission (IEC). Based on IEEE 802.15.4, the version 7 of the HART protocol (WirelessHART) is decided as wireless access for process monitoring and control applications in the industrial environments [7], [8]. WIA-PA is the Chinese industrial wireless communication standard for process automation, which was approved by IEC in 2008 and became the second wireless communication standard for the industrial in the world after WirelessHART. WISA was developed by ABB corporation and used widely in industrial field to connect devices in several. different environments . It can offer less than 20ms endto-end latency. Based on IEEE 802.11, WIA-FA was the first wireless technology specification developed specifically for factory, high-speed, automatic, control applications and officially approved in 2017 . The new dedicated industrial wireless communication system, i.e. Wireless HP, is expected in the near future. For V2X networks, in order to support Vehicle-to-Vehicle (V2V) connection, Dedicated Short Range Communications (DSRC), which is based on the IEEE 802.11p/1609, is used as wireless access in vehicular environment (WAVE) protocols. DSRC uses half-clocked mode with the 10 MHz bandwidth in physical layer, and borrowed Enhanced Distributed Channel Access (EDCA) idea from IEEE 802.11e to satisfy the rigorous QoS requirements in MAC layer.

1.3. Application Scenarios of HRLL IoT Networks

In what follows, we will discuss a few typical application scenarios for HRLL IoT networks, including factory automation, vehicular networks and smart grids in detail.

1.4. Industrial Automation

With the development of computing, control and communication technologies, a new generation of industry revolution, namely, industry 4.0 has largely changed our industry producing process. As a key enabling technology of industry 4.0, industry IoT (IIoT) has attracted a lot of research interests recently. Many of existing communication networks for the industries are actually based on wired networks, e.g., Ethernet or optical fiber. However, recently, a new trend of IIoT is to replace wired

networks with wireless ones . Motivated by promising benefits in e.g., low cost, flexibility and suitability in harsh environments or mobile scenarios, the first industrial wireless network has been implemented in real-time control applications [9]. After that, there have been lots of efforts for development and standardization for connecting devices in the industrial, e.g., WirelessHART, WIA-PA, and the WIAFA, etc. Relative to wired networks, the advantages of using wireless ones are multi-folded: (1) Wireless networks may lead to significantly reduced costs of materials, installation, commission and maintenance; (2) Despite of channel fading or interference, wireless may be more reliable in many scenarios, e.g., the scenarios of cables subjective to aging and breaking, and easier to get redundancy links with wireless networks; (3) Wireless networks may be deployed in many scenarios where installing cables is impractical, such as moving robots, harsh industrial environments (high temperature or high voltage) and long distance (e.g., very high tower).

In emerging smart factories, IIoT is widely used to sense various environmental information and the sensed information is sent back to the controller for making decision. Then the decision based on the collected information is sent to the actuators. For many (if not the most) of these applications, latency and reliability are among the most important technical requirements. For instance, in the mining sector, remote blasting and rock-breaking control procedures are increasingly used to enhance performance and the safety of workers. Clearly, sensing and control of blasting time and magnitude are critical for efficiency and safety, which must be sensed, transmitted and processed timely and reliably. Factorial robotics are also among typical scenarios with stringent requirements on latency and reliability. Flexible manufacturing systems (FMSs) automatically adapt and react to changes in the environment, production flow, and products types. FMSs will rely on the cooperation among intelligent robots, often mounted over automatic guided vehicles. Fast running FMS is only possible with the supports of HRLL communications systems. Briefly, the basic requirements for industrial IoT networks include:

Low latency: Many applications have rigorous demands on latency, in which short packet, simple transmitters/receivers and access protocols are preferred. • High reliability: Some control objectives are highly valued or even dangerous, and very small transmission error could be fatal. Yet the reliability normally decreases with increasing latency requirement. For example, adopting short codeword may cause the loss of coding gain. • Throughput: Some applications require to transmit highresolution images or videos and thus high throughput is needed. • Interference-robust capability: The industrial environments may be hazard. There may be strong interference generated by other communication systems and electrical equipments, e.g., powering on/off electrical engines. • Fading-robust capability: Factory building and facilities (e.g., robot arms in assemble lines) could frequencyselectively reflect and scatter the wireless signal. This will degrade the reliability. • Energy efficiency: Due to the low spectral density power and some terminals are power limited (power supplied by battery), energy efficiency may be critical for some applications. • Communication range: Most of one-hop transmissions occur within 100 meters , [10]. Yet, some applications may need up to

1000 meters (e.g., power system protection), which may be challenging for HRLL IIoT networks. Moreover, in many IIoT networks, the limited mobility support is acceptable. Thus the networks can be deployed statically and the channel is near-static. Other non-typical issues such as life cycle, volume, cost, heterogeneous networks configuration, security and safety should be taken into consideration as well. V2X IoT Networks for Transportation With the development of various intelligent technologies, our society has never encountered such a big challenge for transportation systems before. The number of vehicles is increasing dramatically with the new wave of urbanization and the development of transportation capacity. Moreover, emission and energy-efficient regulations have been much more stringent than ever before. With the assistance of the latest wireless communication and IoT technology, it is optimistic to achieve the goal of increasing the transportation capability and efficiency. For V2X networks, the requirements on latency and reliability are stringent. For example, as one of the most important application scenarios for the 5G, the objective of V2X communication networks is to enable high-efficiency and accident-free cooperative automated driving, which shall use the available roadway efficiently. To achieve this objective, the communication networks should accommodate a diverse set of use cases, each with a specific set of requirements.

The basic requirements for V2X communication networks include:

• Low latency: Though the latency requirement may not be as rigorous as certain extreme industrial control scenarios, it is still beyond the capacity of current mobile networks (e.g., 4G or below). • High reliability: Transmission for vehicular control signaling may need extremely high reliability since the transmission errors may cause fatal accidents.

• Throughput: Some V2X applications, e.g. remote controlling and environment sensing of the traffic, require to transmit high-resolution images or videos. Accordingly, the requirements on throughput may be rather high.

• Interference-robust capability. There may be significant interference generated by other communication systems and automobile igniters.

• Fading-robust capability: Mountains and city buildings may frequency-selectively reflect and scatter the signal, which may degrade reliability further.

• Communication range: The distance of one-hop V2X transmissions may vary from dozens of meters to hundreds of meters.

• Mobility support: For city vehicles, the relative velocity may be larger than 28km per hour. For high speed trains, the speed could be more than 350km per hour. Thus, communication channels are fast time-varying. For these scenarios of high mobility, we need to design transmission schemes considering Doppler effect to improve reliability. The most popular communication scenarios for V2X networks include [11]: 1) Vehicle-to-Vehicle (V2V) communications, in which information is exchanged among vehicles; 2) Vehicleto-Infrastructure (V2I) communications, which occur between vehicles and roadside units (RSUs), traffic lights, and base stations; 3) Vehicle-to-Pedestrian (V2P)

communications, in which vehicles communicate with people who are along the side of the road; and 4) Vehicle-to-Network (V2N), where the vehicles connect to an entity in the networks e.g., a backend server or a traffic information system.

Smart Grid Smart grid refers to intelligently produce, transmit and consume electric with the aid of sensors, actuators, communication networks and central controllers. Smart grid is a power network enabling a variety of nodes of smart appliances, e.g.,

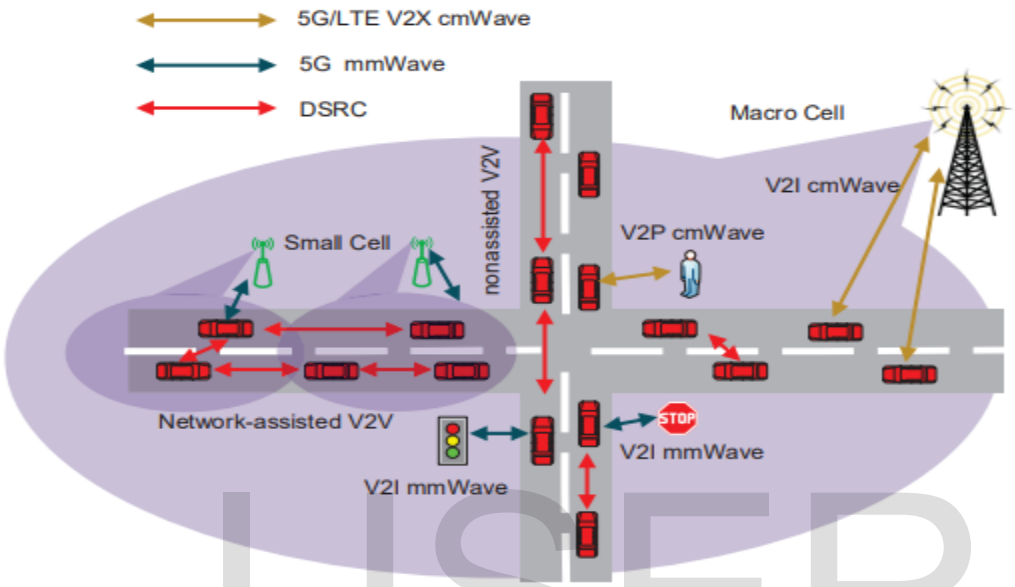

Figure. 1.3. A possible deployment of future V2X networks.

efficient energy generation, smart meters, smart billing and renewable energy resources. Therefore, many new applications and services are developed based on these techniques, such as Energy Management System (EMS), Demand Response (DR), Frequency Regulation (FR) and Peer-to-Peer Energy Trading (P2PET). To support two-way energy transferring in heterogeneous smart grids, the underlying communication systems should have high performance in terms of latency, rates and reliability. For instance, to enable advanced applications such as real-time pricing, a low-latency two-way real-time communication system is required.

1.5. Physical Layer for HRLL Communications

In this section, we will first discuss the system model for IoT, and then its fundamental limits under the latency constraints. Then the more practical design principles such as frame structure, preamble design and channel coding will be given.

System Model An IoT end-to-end wireless transmission system model can be shown in Figure. 1.3. With one/multiple antennas, the model can also be expressed as the following formula

$$Y = HX + W,$$

where X denotes the transmitting complex symbols (vectors) and Y is the corresponding received signal, H is the channel gain due to fading and W is additive Gaussian noise. The latency defined here is the time consuming for the successful end-to-end transmission of one packet/codeword

Fundamental limits for HRLL communications in IoT In wireless communication systems, it is a challenging task to achieve high reliability and low latency simultaneously, particularly for resource limited communications e.g., IoT. Many traditional techniques (e.g., strong channel codes) have been proposed to improve reliability, but often have to sacrifice latency. On the other hand, reducing latency with short packet length could cause decreasing reliability, because short block length cannot secure the large coding gain, and the size of overhead symbols in packets (metadata), such as pilot symbols, header and preambles, may be comparable with information length. Fundamental results in information theory show that when the packet length goes to infinite, there always exist a channel coding scheme, with which the transmitting symbols can be recovered with arbitrarily small error probability, if the communications rates are equal to or smaller than channel capacity.

1.6. Networks for V2X IoT in Transportation

Our civilization has never faced such a significant issue for transportation networks as is present now due to the emergence of numerous sophisticated technologies. With the new wave of urbanisation and the growth of transportation capacity, the number of automobiles is significantly rising. Regulations governing emissions and energy efficiency are also stricter than they have ever been. It is optimistically possible to increase the capability and efficiency of transportation with the aid of modern wireless communication and IoT technologies[12]. The standards for latency and reliability in V2X networks are very strict. The goal of V2X communication networks, for instance, is to enable highly effective and accident-free cooperative autonomous driving that effectively utilises the available road space. This is one of the most significant application scenarios for 5G. Our civilization has never faced a challenge as significant as the one presented by the emergence of diverse intelligent technology.

The communication networks must support a wide range of use cases, each with its own unique needs, in order to accomplish this goal. The following are the fundamental conditions for V2X communication networks.

1.7. Wireless data delivery in IoT

- **The principles of radio signal propagation are introduced in this section.**

Typically, wireless signals are delivered as electromagnetic waves that move through the propagation space. A transmitter and a receiver antenna are used in wireless communication, and they are affixed using some geometry. A straightforward wireless communication model is shown in Figure 1.3. The carrier signal is used by the transmitter to broadcast a signal that has been modulated. To distinguish the carrier signal from the information, the receiver conducts demodulation. There are several methods for modulating the carrier wave, including amplitude modulation (AM) and frequency modulation (FM) (AM)[13].

1.8. Internet layer IoT network technologies

Technologies in the OSI Layer 3 of the Internet Layer are used to locate and route data packets. This layer contains several frequently used IoT technologies, including IPv6, 6LoWPAN, and RPL. IPv6

Devices are recognised by IP addresses at the Internet layer. As opposed to IPv4, IPv6 is frequently utilised for IoT applications. Compared to the present number of linked

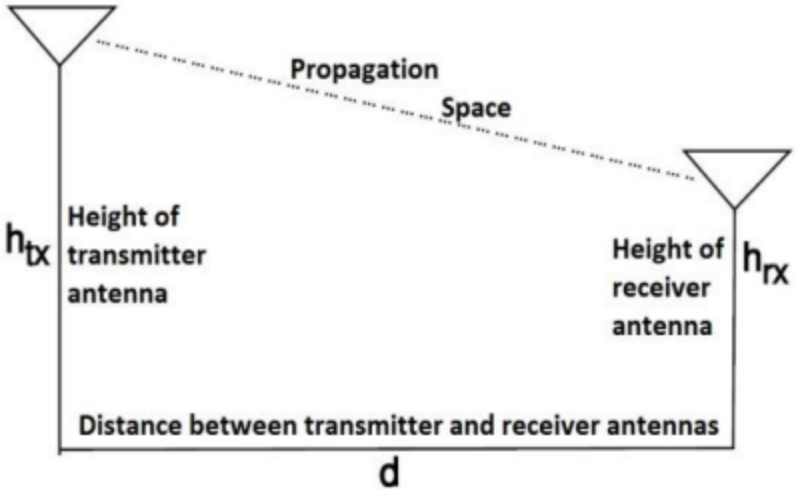

Figure 1.4,Wireless communication model.

IoT devices, IPv4 is restricted to 32-bit addresses, which only supply around 4.3 billion addresses overall. By contrast, IPv6 utilises 128 bits and offers 2 128 addresses, which amounts to over 3.4 10 38 or 340 billion addresses. Not all IoT devices actually require public addresses [14]. The IoT is predicted to link tens of billions of items over the next several years, but many of those devices will be set up in private networks that only communicate with other things on external networks using private address ranges. 6LoWPAN Using IPv6 over 802.15.4 wireless networks is possible thanks to the IPv6 Low Power Wireless Personal Area Network (6LoWPAN) protocol. Wireless sensor networks frequently employ 6LoWPAN, and home automation systems also use Thread over 6LoWPAN.

RPL Routing is covered by the Internet Layer. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is intended to route IPv6 traffic across networks powered by low power sources, such as 6LoWPAN networks. In restricted networks, such as wireless sensor networks, where not all devices are always available and there is significant or unexpected packet loss, RPL (pronounced "ripple") is developed for packet routing. RPL may determine the best route by creating a graph of the network's nodes depending on dynamic measurements and restrictions like reducing latency or energy use.

- The M2M Communication The term "machine-to-machine communication," or M2M, refers to the exchange of data between two machines without the use of a human interface or other human involvement. In the industrial Internet of Things, this comprises wireless communications, powerline connections (PLC), and serial connections (IoT).
- The move to wireless has made M2M communication considerably simpler and allowed for the connection of additional applications. In general, cellular connectivity for embedded devices is frequently meant when someone mentions M2M communication. In this instance, M2M

communication examples include vending machines transmitting inventory data or ATMs receiving authorisation to dispense cash. [15]

- M2M and IoT are nearly synonymous, with the caveat that M2M can refer to any two machines that are talking with one another whether they are connected or wireless. M2M has traditionally concentrated on "industrial telematics," which is a fancy term for data transfer for some kind of economic gain. But many of the initial M2M applications, such as smart metres, are still relevant today. Since the introduction of 2G cellular networks in the middle of the 2000s, cellular has dominated wireless M2M. Due of this, the cellular industry has attempted to position M2M as something that is intrinsically cellular by providing M2M data plans. However, cellular M2M should not be viewed as a cellular-only space because it is but one segment of the industry.[16].

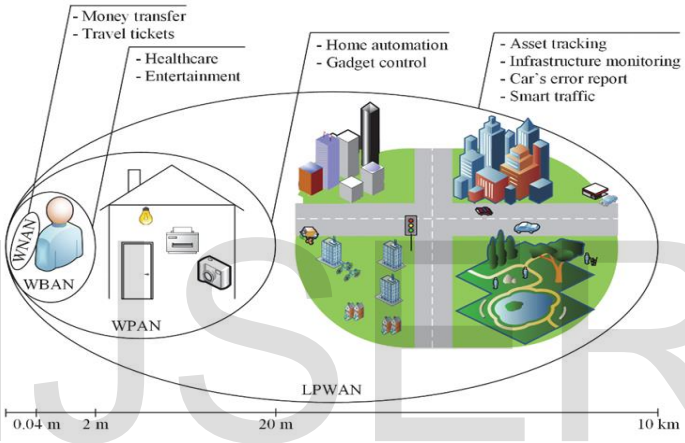

Figure 1.5, Distance between a transmitter and a receiver,

How M2M Works

The Internet of Things is made feasible through machine-to-machine connectivity, as was previously mentioned. Forbes claims that M2M technologies, which allow for the connection of millions of devices inside a single network, are among the connected device technologies that are now seeing the highest market growth. Anything from vending machines to medical equipment to automobiles to structures is included in the variety of linked devices. Any object that contains sensor or control technologies can be linked to a wireless network. Although the notion behind this seems complicated, it is actually rather straightforward[17]. M2M networks are essentially LAN or WAN networks with the exception that they are only utilised to support machine, sensor, and control communication. These devices transmit the data they gather to other network nodes. Through this procedure, a person (or intelligent control unit) is able to evaluate the state of the whole network and give the relevant orders to participating devices. IoT computing and networking resources might differ significantly from IT environments' equivalents. The physical form factors of equipment used by IT and OT differ significantly. Their practical distinctions, however, might not be as clear. To properly handle the target assets, it is necessary to comprehend these operational distinctions. The majority of IT settings

have to deal with dust accumulation, which can get very concentrated because of the action of cooling fans.[18].

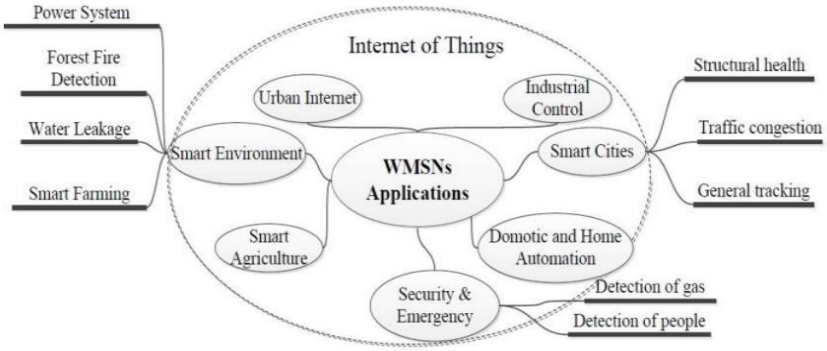

Figure 1.6. Applications of WMSNs in different environments.

Due to greater particle concentrations, that problem may accelerate in less regulated IT environments. Equipment corrosion may also result from hazardous site design. Caustic substances can affect the connections that carry electricity or communications. And they could coat the heat transfer surfaces, which could lead to decreased thermal efficiency. Many industrial computing and communication devices are installed inside an enclosed area, such a control cabinet, where they will be mounted vertically on a DIN rail.

1.9. Low Latency

End-to-end latency E2E delay consists of the delay in over-the-air broadcasting, the delay in queueing, delays in processing compiling and retransmissions, when required. achieving a 1 ms round-trip delay Because due to restrictions imposed by the speed of light (300 km/s), the farthest distance that the distance to the receiver's location is around 150 kilometres. User plane latency (3GPP) is the amount of time required to correctly transmit a packet or message from the radio protocol layer to the application layer radio protocol entry point entry point of the either an uplink or a downlink radio interface in the network for a certain service under little load (Given that the user equipment (UE) is assuming an active condition). User plane latency minimum requirements are eMBB takes 4 ms and URLLC takes 1 ms, assuming a single user [19]. (3GPP) Control plane latency: defined as the period of time between the commencement of continuous data transfer and the state that is the most "battery efficient" (for example, the idle state) (e.g., active state). Control plane latency must be no less than 20 ms.

- **User plane latency (3GPP) [21:** defined as the one-way time it takes for an application layer packet or message to successfully travel from the radio protocol layer ingress point to the radio protocol ingress point of the radio interface in the network for a given service under unloaded conditions (presuming the user equipment (UE) is in an active state). For eMBB and URLLC, respectively, the minimal user plane latency requirements are 4 ms and 1 ms, respectively, assuming a single user.

- **Control plane latency (3GPP) [21]:** defined as the transition time from a most "battery efficient" state (e.g., idle state) to the start of continuous data transfer (e.g., active state). The minimum requirement for control plane latency is 20 ms.

1.10. High Reliability

Reliability is often defined as the likelihood that data of size D will be successfully transported within time T. In other words, dependability requires that both the latency bound and packet delivery success be met. Other meanings can be found, though. Reliability (3GPP) [20]: The capacity to transmit a specific volume of data with a high chance of success within a particular time frame. 1 105 success chance of sending a 32-byte layer 2 protocol data unit within one millisecond is the very minimum criteria for dependability.

- **Reliability per node:** This is determined by the likelihood of transmission errors, queue delay violations, and proactive packet discarding. The likelihood of correctly decoding the scheduling grant or other metadata is referred to as control channel reliability.
- **Availability:** The likelihood that a specific service is offered is defined as availability (i.e., coverage). In the case of 99.99 percent availability, this translates to one user out of 10,000 not receiving enough coverage. We stress that the 3GPP and ITU criteria are more narrowly focused, whereas the URLLC service requirements are end-to-end.
- Reliability (3GPP) [21]: capacity to send a specific quantity of traffic in a specific length of time with a high success rate. The success probability of delivering a layer 2 protocol data unit of 32 bytes in 1 ms is 1105, which is the minimal criteria for dependability. The probabilities of proactive packet dropping, queue delay violations, and transmission errors are the components of reliability per node.[21].
- Control channel reliability: defined as the probability of successfully decoding the scheduling grant or other metadata [22].
- Availability: defined as the probability that a given service is available (i.e., coverage). For instance, 99.99% availability means that one user among 10000 does not receive proper coverage [23].

This synopsis' contributions may be summarized as follows:

There is a brief discussion of the rising trends in wireless connection and mobile data.

- ❖ The 6G communication system's potential entry points are discussed.
- ❖ Discussion is held about anticipated service requirements for 6G communication.
- ❖ A quick comparison of the anticipated 6G communication system with the 4G and 5G systems is made.
- ❖ Presenting emerging 6G technology.
- ❖ Different technologies' responsibilities in the 5G and 6G networks, respectively, are explored.
- ❖ The needs and anticipated 6G applications are shown.

- ❖ Related ongoing and existing 6G projects are reviewed.
- ❖ The 6G goal's potential obstacles and future research areas are discussed.

1.11. Role of URLLC in Operating IoT

Although URLLC has the essential components for successful IoT operations, mMTC is particularly classified and created to fulfil IoT requirements. Figure 1.7, illustrates how several operators may remotely operate time-critical equipment, and how latency and reliability are crucial to the efficient operation the functionality of IoT devices. Operating mission-critical and real-time IoT is quite difficult wirelessly connecting devices [24]. enormous multiple input, many output (MIMO) Recently, technology has improved in its ability to control a vast array of devices. However, it's still difficult to fulfil latency and reliability criteria.

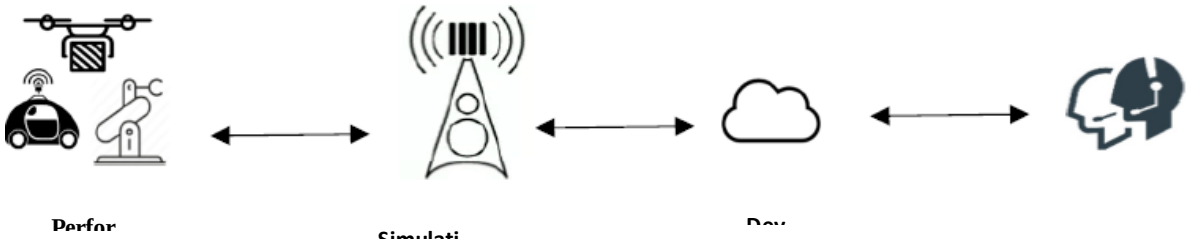

Figure 1.7. Basic IoT operation over tactile internet on massive multiple-input multiple-output (MIMO).

IoT Energy Efficiency (EE)

1.12. URLLC and Massive Device Connectivity

Present mobile services and specifications are not completely equipped to deliver URLLC cost-effectively at scale [25]. Furthermore, they lack the capacity to deliver a reliable low latency communication to multiple users at the same time. It is particularly difficult to ensure link-level reliability and latency over a wide area and in a remote scenario, As wide-area cases involve many elements such as transitional nodes, backhaul, core/cloud, and fronthaul, they can play a vital role in degrading latency. However, the resources such as energy and computing power of IoT devices also play a vital

role when operating over URLLC. To meet the latency requirements for URLLC, the IoT devices are forced to utilize excessive power and processing ability that is not appropriate for the life span of IoT devices. However, most of the IoT devices have limited resources.

1.13. On-Device Artificial Intelligence and URLLC

Traditionally, communication networks are designed with the concept of achieving high data rates with centralized management of resources. To accomplish the upcoming extreme latency and reliability requirements, the communication network architecture is now being pushed to be more non-centric and proactive. Most of the IoT devices are designed to be remotely controlled or to operate in a limited non-complex environment. However, some of the machines/applications require

machine learning (ML) or artificial intelligence (AI) in order to be more effective and efficient to achieve the goals of the applications. Clearly, the customary machine learning approach based on the centralized architecture, as shown in Figure 1.8, is not very suitable for delicate latency applications [26]. However, most of the IoT devices have limited resources [27], and such devices may not be able to carry out ML or AI based algorithms effectively while meeting the latency requirements. Consequently, researchers are investigating decentralized approaches such as distributed ML or AI on edge that involve collective problem solving . Even with on-device machine learning, devices require a significant amount of storage and computational ability, which most of the IoT devices lack. Most of the AI algorithms usually require a large data set to provide effective results. In URLLC, however, it is a challenge to provide such a big data set for the mission-critical IoT devices with reliability and low latency.

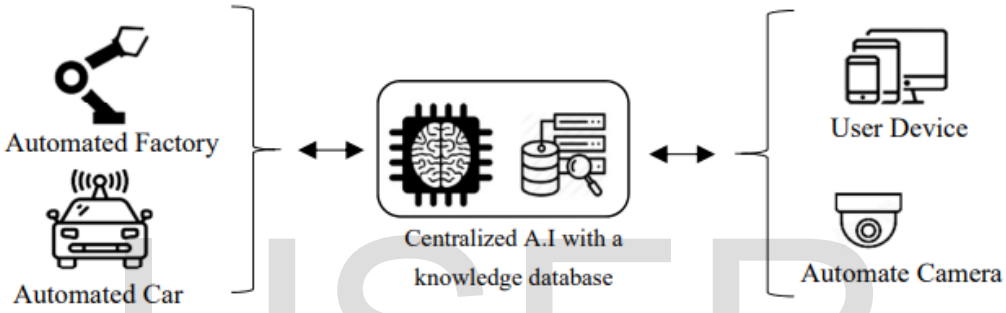

Figure 1.8. Traditional machine learning (ML) concept (centralized). AI, artificial intelligence.

1.14. URLLC and Vehicle-to-Vehicle (V2V)

One of the most promising and important applications of the future 5G network is V2V communication. V2V communication is one of the technologies that can lead to an intelligent transport system . Naturally, for V2V, road safety (distance awareness to avoid any collision, speed limits, location-based traveling, environment information, road condition) plays a vital role and is extremely time-critical, as shown in Figure 1.9.

Figure 1.9. Basic vehicle-to-vehicle (V2V) road safety.

Because of the safety concern, European Telecommunications Standard Institute (ETSI) has standardized safety protocols based on two awareness-based messages: decentralized environmental notification message (DENM) and cooperative awareness message (CAM) . To reflect vehicles based

on the mentioned safety standards, V2V communication should have the low latency characteristic of URLLC.

1.15. IoT Energy Efficiency (EE)

In IoT and machine-to-machine (M2M) communications, EE will play an important role, especially with sensor-type equipment with limited resources, for example, limited battery and computing power . A number of URLLC applications require a lot of computation, which is not handled by some IoT devices. From a PHY perspective, it is a challenge for URLLC to achieve low latency and high reliability in mission-critical IoT devices. The use of short packet in order to achieve low latency can degrade channel-coding gain, and it causes reliability issues in wireless channels. To mitigate reliability issue, re-transmission is required, but it involves additional resources and increases latency.

1.16. Base Station Densification and Device-to-Device (D2d) Communications

In typical automated industry, clusters of sensors and actuators are working in a fixed area. One of the crucial use cases for the 5G URLLC is to support the wireless industrial automation (e.g., Industry 4.0 [44]). With the emerging industrial automation, M2M and D2D communications require URLLC features to deliver short messages from a controller to a cluster of sensors or machines. A reasonable amount of traffic is expected to be handled by WiFi and small-cell-technology based on mm Wave frequencies, as shown in Figure 1.10 The METIS project estimated that dense metropolitan areas might have up to 200 devices per km^2, with an expected data volume generated by each device could be 500 Gbyte/month [28]. Such an immense number of devices could force a drastic change in network infrastructure to avoid congestion and availability of service. With the limited frequency bands, improvement of the spectral efficiency (SE) could be an answer to support massive data.

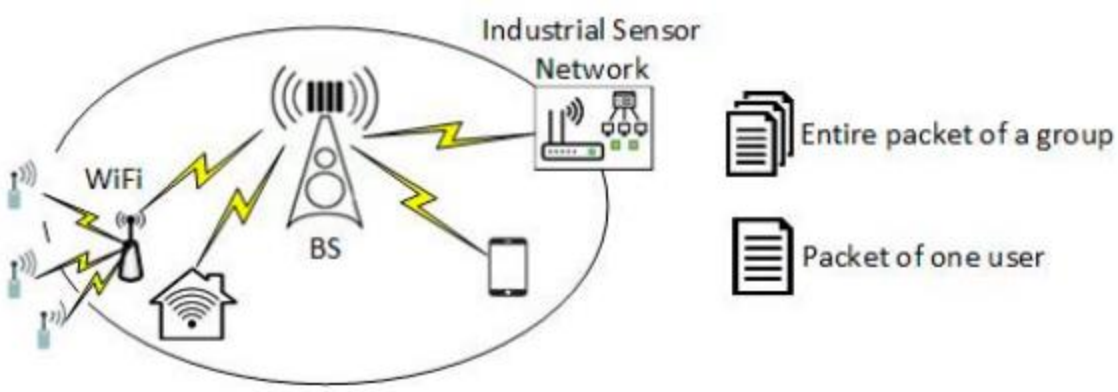

Figure 1.10. Illustration of a single user data packet and multiple user data packets relayed by a server/cluster head.

1.17. Motivation

The lower frequency bands, or those with less than 100 MHz, are given a second look in this thesis since they might have a big influence on how communications are handled in next WBANs. The best

wireless radio technology should be used to execute a variety of applications over links that range from a few millimetres to many kilometres. Even though a variety of wireless IoT devices are currently commercially available off-the-shelf (COTS), further study is still required to increase things like energy efficiency and ecological impact [29]. A wake-up receiver (WUR) idea is also investigated in this research. WUR increases the energy efficiency of sensor nodes while maintaining low latency connections. It is anticipated that WURs will be incorporated onto the same chip as the data radio once they reach a certain degree of development. IoT device proliferation is expected to result in a substantial increase in problems. When considering handover-related concerns in mobile contexts, the transport layer must also be taken into consideration. The IoT as a technology is fairly advanced, enabling the manufacturing of many sorts of prototypes and testing them in a range of wireless/wired networks, even though there is still opportunity for performance improvements. Other methods, such mathematical analysis or simulations, most likely could have produced results that were comparable, but empirical investigations are frequently required before commercial goods can be developed.

With the development of various new applications, the HRLL IoT networks will be more and more common, and their concrete technical requirements are quite diverse. Motivated by the promising applications, significant research has been conducted over recent years to increase the reliability and simultaneously to decrease the transmission delay. The contributions of this tutorial can be summarized as follows:

• We review comprehensively key techniques for HRLL IoT. Although different scenarios may have different performance requirement and thus different system designs for HRLL, the underline techniques they adopted share many common grounds, which have been developed substantially in recent years.

• We also give the insight for these enabling key techniques from the fundamental theory perspective. Short packet length transmission is essential to achieve the low latency. We review the information theory fundaments of short packet communications. Moreover, in addition to short length coding, we also discussed fundamental techniques adopted in physical, MAC and network layers of HRLL IoT networks. For example, we discuss the design principles for determining the appropriate packet size, obtaining preamble, grant-free access and code rate tradeoffs, choosing practical channel codes, optimizing access process and network structure etc

. • We review typical application scenarios of HRLL IoT communications, e.g., industrial automation, V2X communications and smart grids. Typical performance requirements of these scenarios are given. We also review the standardization of HRLL communications.

Chapter 2
LITERATURE REVIEW

2.1. Background information

This chapter focuses mostly on the history of wireless communication technologies and the big picture of the Internet of Things. The introduction of wireless communication technologies will come first. The IoT's organisational structure is also discussed, along with several key elements related to its wireless communication applications. The existing telecommunications networks and other information carriers serve as the foundation for the Internet of Things. IoT is a growth of the traditional Internet. The machine (PC, server), which runs a variety of apps, is the Internet terminal. Internet is only a means for computer-to-computer data processing and transfer [30].

T. S. Rappaport et al. 2017To the best of our knowledge, there hasn't been an overview of HRLL methods for the Internet of Things, although there are general articles on URLLC/HRLL for industrial and V2X networks, or tactile Internet. Following, we'll provide a succinct evaluation of These studies are discussed along with how they differ from ours. In order to deliver one of the 5G requirements, URLLC using mobile networks for essential communication services. There a lot of tutorials exist on 5G URLLC [10] and its development roadmap However, a lot relies on how URLLC is used. Several studies specifically address URLLC/HRLL for industrial IoT. (IIoT).

E. Bjornson et al. 2016 [2]. The URLLC/HRLL for V2X networks is shown in a few surveys Use cases, application situations, and enabling methodologies were provided. The majority of them, however, are not universal HRLL IoT approaches; rather, they are pertinent to specific circumstances (e.g., solely on industrial control or V2X networks). This article, in contrast, aims to review the technology utilised by various HRLL IoT applications. The Tactile Internet, which is thought to be a key application of IoT, has been defined as the communication networks combining high availability, high dependability, high degree of security with low latency and very short transmitting time for real-time interactive applications. Tactile Internet has been the subject of several reviews[31].

Another survey work [32] also discusses about the security and privacy issues in IoT. Moreover, the paper clearly defined the hardware specifications, architecture for eight IoT frameworks on security. The paper also discussed about significant security needs of IoT such as access control, authentication, and cryptographic computations and so on. Another research work, [33] described about the restriction in IoT and the mitigation techniques for solving those issues. It is discussed in the paper that the high level of cryptographic computations requires higher battery utilization. For solving those issues, energy efficient and light weight security models are to be derived with several IoT authentication models and frameworks.

The IoT architecture-based security and privacy model based on the combined efficiencies of cloud and fog computing is discussed [34]. Additionally, the authors have provided about the Cyber-Physical Systems (CPSs) and the differences between IoT and CPSs. It comprises of efficient resource

sharing, trust model and security derivations. The paper converses about the various security attacks that occur in each layer of IoT that interrupts the data sensing, data aggregation, mining and processing. The layers-based details are explained for effectively evaluating the security problems of Internet of Things. The layers are Perception Layer, Transportation Layer and Application Layer. The perception layer comprises of perception nodes and networks, transportation layer is with local area network (LAN), core and access network and the support layer and IoT applications are in the top most layers called application layer.

2.2. Standardization of HRLL

Mobile cellular networks are the foundation of one type of HRLL standards. However, although there has been some informal development of URLLC prior to 5G, Cellular mobile network modifications have HRLL functionalities available before 5G mobile. For example, the Global System the GSM-R standard for mobile communications for railroads, which used to send railway control and dispatch instructions maybe the initial iteration of such endeavours. It may provide extremely restricted end-to-end data transfer speed of 500ms delay. Additionally, several non-safety-critical V2X networks WCDMA systems have utilised services by specifying radio resource control (RRC) protocol states for vehicles Equipment (VE), whereas the WCDMA system's capacity is restricted, wherein many VEs can't consistently stay connected.
on the 5G standardisation process.

W. Hong et al. 2017 [35] The Internet does not use any more terminals (hardware). The Internet remains the primary concept behind IoT. In contrast to the Internet, embedded computer systems and the associated sensors may be thought of as terminals. They include more than just PCs and servers. To create a functioning interconnection network, it may join various types of autonomous items and enable them to operate together. This is the inescapable outcome of the advancement of computer science and technology. The computer must assist humans in a number of capacities, including as virtual reality gear, environmental monitoring gear, and so on. We refer to it as the "Internet of Things" as long as there is hardware or products connected to the Internet or there is data interchange.

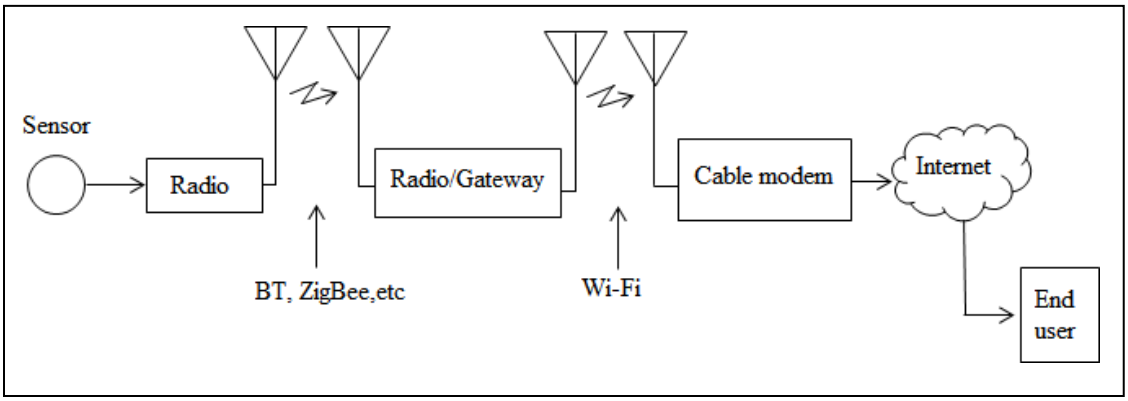

Figure 2 .1. Wireless-connection scenarios for IoT

Figure 2.1, depicts how the Internet of Things appears when connected wirelessly. Additionally, the Internet of Things uses six significant wireless communication protocol standards to meet its various

requirements. The literature lists a number of authentication strategies, such as biometric-based, sensor-based, and token-sensor-based authentication.

X. Wu et al. 2018 [4] Techniques for biometric-based authentication depend on the individuality of specific human physical characteristics. Fingerprints, finger knuckles, retinas, and walking patterns are a few examples of these characteristics. The main issue with biometric-based authentication methods is that they are difficult to replace if their security is breached. However, if they are lost or their security is compromised, token-based authentication solutions may be quickly reissued. Additionally, in a dark situation or when a soldier is wearing camouflage, visual facial recognition is ineffective. A low-bandwidth wide area network, or LPWAN, is one that connects battery-operated, low-bit-rate end devices over long distances. It is one of several types of wireless communications wide area networks. Small data packets may be sent over vast distances using LPWAN, which runs on batteries. Narrowband IoT (NB-IoT), Sigfox, LoRa, and other competing technologies in the LPWAN market offer coverage for short-, medium-, and long-range communication .

S. A. Busari et al. 2018 The high-speed capabilities of wireless local area network (LAN) systems have garnered interest. Optical wireless communication has been viewed as a potential method for indoor wireless networks because to its unique qualities, including its unregulated spectrum, affordable subsystems, and electromagnetic interference protection. The use of infrared radiation for interior applications has been studied and extensively explored since the ground-breaking work of Gfeller and Bapst [36]. The enormous bandwidth capacity for high-speed optical communications is the most promising aspect of transmission. At terahertz (THz) frequencies, the infrared spectrum is well understood and may theoretically sustain a bandwidth on the order of a few hundred gigahertz (GHz). Even if the prospect of such a vast potential bandwidth is appealing.

2.3. Important Communication Protocols in IoT

Electromagnetic waves are used in wireless communication to transport signals; however, these waves require line-of-sight. Long-distance communication is challenging to establish because of the curvature of the world. On Earth, several antennas or stations are constructed as a solution to this issue. The signal is transmitted directly from the ground into space so that Communications Satellites (CSs) may relay and amplify it, increasing the signal's range and intensity. The signal will then be relayed to the target destination on Earth at a different position. These signals may include calls, Internet data, radio broadcasts, and even television transmissions (Chris Woodford, 2016)[37].

Z. Mokhtari et al. 2019 [6] In mobile phone communication, CSs allow for a greater range of communication. For instance, GSM communication distances may reach up to 35 km. Additionally, there are several communications such as GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G), and so on depending on the connectivity speed. Even while a constant connection and universal compatibility are known as positives, CSs still have a high monthly cost to maintain them as well as a significant power consumption. The IoT should take into account all of these benefits and drawbacks as it develops, which is why satellites are mostly used for commercial purposes.

2.4. WiFi

WLAN is an IEEE802.11-based technology, also referred to as Wi-Fi. It is a wireless local area network (WLAN) that permits usage of the Internet by two or more mobile devices through a wireless connection. Users of this connection are free to roam about within a specific service area because it is based on an access point. Today, WiFi is widely used in many aspects of everyday life. It is accessible and reasonably priced. Devices operating in accordance with IEEE 802.11 specifications often communicate in the 2.4, 3.6, 5 and 60 GHz frequency ranges. The fundamental details of the 802.11 standards, including data rate and communication range, are shown in Table 1. It is simple to determine which is now the best based on the information in the table. The most widely used standard nowadays for high-end performance is IEEE802.11n. Higher power consumption is also required in order to attain the high-grade performance. WIFI is not advised for low-powered provided devices due to the power consumption issue. The majority of IEEE 802.11 networks operate at 2.4 GHz, where 14 channels have been divided from the complete 5 GHz spectrum with each channel having about 22MHz.

2.5. RFID

Radio Frequency Identification (RFID) is a wireless communication technology that allows radio signals to identify specific target, read and write related data without establishing a mechanical or optical contact between the system and a specific target. In RFID, two main devices are Tag and Reader.

Radio signals are using radio frequency electromagnetic fields to attach the data on the Tag and transmit it out, in order to automatically identify and track item. Tags will gain energy from the reader's electromagnetic fields, so they do not need battery. Moreover, some Tags also have power, they can send radio frequency by themselves. The Tag contains the information stored electronically; we can identify it within a few meters.

Radio frequency identification system mainly has the following several advantages:

1) Simple to read; RFID does not require a light source; thus readers may read from outside the packaging. The effective identification distance can reach up to 30 metres if the tag has its own battery.
2) Quick response time; the reader may read the data as soon as the tag enters the electromagnetic field. Reader may also handle multiple tags.
3) Large data storage; RFID tags can hold up to 10K numbers.
4) Long lifespan; sealed packing; suitable for usage in unfavourable conditions.
5) Real-time communication; the reader and tag may exchange information 50 to 100 times per second. Due to all of these factors, RFID technology is already being used in a number of industry sectors.[38].

2.6. NFC

NFC stands for "Near Field Communication". It is an additional type of RFID. NFC, on the other hand, differs from RFID in that it uses a short-range, high-frequency wireless communication technology to enable non-contact point-to-point data transfer between electronic devices at a distance of just 10 cm (GSMArena, 2016). It may select a transmission speed of 106kbps, 212kbps, or 424kbps. The absence of pair devices in NFC makes it different from Bluetooth. The distinction makes the connection setup process simpler. In nowadays, NFC is normally implemented in cell phones. There are five main applications with NFC technology:

1) Touch-and-go; the phone functions as a key.
2) Touch and Pay; to make a purchase using "Apple Pay," the user must touch the NFC component to the POS device.
3) Touch and connect; peer-to-peer data transfer can be used to link two phones. For instance, this programme allows users to download music, share contacts or photos, and more.
4) Touch and explore; by scanning an NFC-enabled smart public phone or a banner on the street, the user may obtain traffic information.
5) After loading and touching, the user can download the data and access a payment

2.7. Wireless IoT connectivity technologies

Since there will be billions of different kinds of connected devices in future IoT applications, it is urged to develop various technologies to support their connectivity. In this section, we discuss the existing wireless technologies for IoT connectivity and classify them into two categories in terms of coverage range, namely short-range technologies and longrange technologies. For short-range technologies, dominant technologies like Bluetooth, ZigBee, WiFi and the emerging OWC technologies are to be discussed. For long-range technologies, depending on service features and requirements, LTE and 5G, and LPWAN technologies including unlicensed and licensed LPWAN, are introduced. In Figure. 1, we illustrate a diagram including the existing IoT connectivity technologies with respect to data rate, coverage range, and latency.

Short-Range Technologies

Short-range wireless technologies for IoT applications are usually used to support connectivity within a small coverage area. There are a number of short-range technologies with different features and performance for given application requirements. Bluetooth, ZigBee, WiFi and OWC, as the mainstream technologies of this kind, are briefly reviewed as follows.

1) Bluetooth: Bluetooth, standardized by the Institute of Electrical and Electronics Engineers (IEEE) 802.15.1 , is originally created by Nokia during the late 90s as an inhouse project. However, it quickly became a popular wireless technology that is primarily used for communications between portable devices distributed in a small area (a maximum of 100m coverage range). Technically, Bluetooth sends short data packets over several channels of bandwidth 1MHz between 2.402GHz to 2.480GHz and its data rate varies from 1Mbps to 3Mbps .

2) 2) ZigBee: ZigBee is another short-range wireless technology for wireless personal area networks (WPAN), which is built on top of IEEE 802.15.4 . Currently, ZigBee has been widely considered for a variety of IoT applications including home automation, industrial monitoring, and health and aging population care . Similar to BLE, Zigbee is also a low-power technology. Zigbee operates in the unlicensed bands, i.e., mainly at 2.4GHz and optionally at 868MHz or 915MHz, and its default operation mode at 2.4GHz uses 16 channels of 2MHz bandwidth. ZigBee is able to connect up to 255 devices at a time with a maximum packet size of 128bytes. Depending on the blockage of environments, the transmission ranges between devices vary from a few meters up to 100 meters. ZigBee supports star and peer-to-peer topologies for connecting devices. In ZigBee, three types of devices are defined as follows: coordinator, router, and end device.
3) OWC: Another emerging short-range wireless technology developed to support the indoor IoT device connectivity is the OWC . OWC is a promising architecture that can be used to resolve the issues arising from high bandwidth and low latency indoor IoT applications. In OWC, visible light (VL), infrared (IR), or ultraviolet (UV) spectrum are used as propagation media in comparison to radio frequencies used in WiFi and other WLAN technologies [58], [39]. To date, different research groups from academia and industry have demonstrated low-complex optical wireless links that can operate at multi-gigabits per second data rate in an energyefficient manner under a typical in room environment to support various applications.
4) LTE and 5G LTE and 5G are the essential parts of cellular IoT technologies. As the standardized technology of the 4th generation (4G), LTE/LTE-Advance (LTE-A) has now been deployed successfully worldwide, which was mainly designed to support the conventional human-type communications (HTC) for highspeed transmissions. Since 2016, the 5G standardization has been progressed by the international telecommunication union (ITU) and 3GPP . Technically, the main advantage of 5G over LTE is its ability of providing 100x higher data rate, 10x lower latency, and supporting 100x more connected devices [86] by utilizing a new air interface that includes much higher frequencies such as millimeter wave (mmWave) and using more advanced radio technologies, e.g., massive multipleinput multiple-output (mMIMO), edge computing, full duplex, and Polar codes . Compared with LTE, 5G is expected to not only enhance HTC by handling far more traffic at much higher data rate, but also to support unprecedented missioncritical applications.

LPWAN Technologies Currently, LPWAN has been driven to fulfill the demand of emerging IoT applications to offer a set of features including wide-area communications and large-scale connectivity for low power, low cost, and low data rate devices with certain delay tolerance. In general, LPWAN can be divided into two categories, namely unlicensed and licensed LPWAN. In the sequel, we review the most prevailing LPWAN technologies. 1) Unlicensed LPWAN: The unlicensed LPWAN technologies refer to the LPWAN technologies that employ unlicensed spectrum resources

over the industrial, scientific, and medical (ISM) band. Thanks to the usage of the unlicensed band, the unlicensed LPWAN providers do not necessarily pay for spectrum licensing, as a result it reduces the cost of deployments. For the unlicensed LPWAN, LoRa and Sigfox are the two biggest competitors . 1) LoRa: LoRa, stands for Long Range. It is a physical layer LPWAN solution that modulates signals using a spread spectrum technique designed and patented by Semtech Corporation . Technically, LoRa employs the chirp spread spectrum (CSS) modulation that spreads a narrowband signal over a wider channel bandwidth, thus enabling high interference resilience and also reducing the signal-to-noise-and-interference ratio (SINR) required at a receiver for correct data decoding .
The spreading factor of the CSS can be varied from 7 to 12, which makes it possible to provide variable data rates and tradeoff between throughput and coverage range, link robustness, or energy consumption . Specifically, a larger spreading factor allows a longer transmission range but at the expense of lower data rate, and vice versa. Depending on the spreading factor and channel bandwidth, the data rate of LoRa can vary between 50bps and 300kbps. In 2015, a LoRa-based communication protocol called LoRaWAN was standardized by LoRa-Alliance . LoRaWAN is organized in a star-of-stars topology, where gateway devices relay messages between end-devices and a central network server . In LoRaWAN, three types of devices (Class A, B, and C) with different capabilities are defined . In particular, Class A is the class of LoRaWAN devices with the lowest power consumption that only require short downlink communication, and Class A devices use pure-ALOHA RA (please refer to Appendix A for more details and explanations on ALOHAprotocols) for the uplink. Class B devices are designed for applications with extra downlink transmission demands. In contrast, Class C devices have continuously received slots, thus always listening to the channel except when they need to transmit. Among the three classes, all the devices must be compatible with Class A . 2) Sigfox:
SigFox is another dominant unlicensed LPWAN solution on the market [10]. SigFox proposes to use an ultra-narrow-band (UNB) technology with only 100Hz bandwidth for very short-payload transmission. Thanks to the UNBtechnology, Sigfox enables less power consumption for devices and supports a wider coverage compared with LoRA at the cost of a lower data rate . Sigfox was initially introduced to support only uplink communication, but later it evolved to a bidirectional technology with a significant link asymmetry. However, the downlink transmission can only be triggered following an uplink transmission. In addition, the uplink message number is constrained to 140 per day and the maximum payload length for each uplink message is limited to 12bytes . Due to these inflexible restrictions, together with its unopened business network model , Sigfox has unfortunately shifted the interest of academia and industry to its competitor LoRaWAN, which is considered more flexible and open. In Table IV, the characteristics of Sigfox and LoRa are summarized.

2.8. Communication Technologies Used in a Smart Home Environment

Devices in a smart home environment can achieve certain functionalities by local control. However, they achieve full functionalities by remote control, which requires SHIoT devices' connection to the local and public communication network Ivan Cvitić et al. (2018). The communication infrastructure

used to connect SHIoT devices is also called HAN (Home Area Network). Depending on the area of operation, HAN includes LAN (Local Area Network) and PAN (Personal Area Network) or BAN (Body Area Network) communication networks and related communication technologies. Most of the communication technologies used in the HAN network were developed before the advent of the smart home environment, and most SHIoT device manufacturers use technologies such as Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4), Z-Wave or Bluetooth (IEEE 802.15.1) to achieve their network communication (Godina et al., 2015). According to Nobuyuki Hayashi, (2017), these technologies currently represent the basis of communication in the HAN network, which will continue after 2020.

The application of particular communication technology will depend on the SHIoT device's performance, purpose, and functionalities it supports. So SHIoT devices (e.g. smart thermostat) that use a battery as an energy source will also use energy-efficient communication technology (ZigBee or Z-Wave) and will communicate via IoT hubs. An IoT hub is a network device used as an intermediary in communication between two different communication technologies. This example will allow a device using ZigBee or Z-Wave technology to communicate with a wireless access point that uses Wi-Fi technology. SHIoT devices that are connected to an uninterruptible power supply (smart sockets, smart light bulbs) will most often also use Wi-Fi communication technology. Bluetooth technology will be used in the scenario of local connection and management of SHIoT devices. An example of such a scenario is a smart lock that detects the user's proximity using Bluetooth technology and performs the appropriate activity (e.g. unlocking the door). Due to SHIoT devices' dimensions and their potential number in the smart home environment, wireless communication technologies were primarily used due to the convenience and ease of connecting devices in the HAN network.

However, individual manufacturers in specific segments of HAN infrastructure also use wired connection method (ethernet). Figure 1 shows two scenarios for connecting smart lighting fixtures. Part A of the same figure shows the IoT concentrator's application and its wired communication with the network switch, while the communication between the IoT concentrator, the lighting device, andthe remote control is performed using ZigBee technology.

The purpose of an IoT hub is to connect multiple devices from the same manufacturer through the same hub. This approach aimed to create a homogeneous smart home environment where SHIoT devices from the same manufacturer would provide all functionalities. It is the result of competition and gaining a competitive advantage. However, according to Blumtritt (2019), the mentioned trend is declining, and the integration of such devices into the gateway device is expected in the future. Therefore, in the future, a more realistic connectivity scenario is shown in Figure 1b where a SHIoT device connects to a wireless access point without the need for intermediary communication devices.

2.9. Summary

All of the layers communicate with one another, although they do so in different ways. They are capable of bidirectional communication. They are able to recognise, for the product in a certain application system, both static and dynamic information. Despite the fact that the IoT offers a variety of applications in intelligent industrial, intelligent transportation, intelligent health care, and other diverse domains. They all have this three-layer structure as their foundation, which is what unites them. In order to develop an IoT platform, five essential elements need be implemented. As follows:

- Controllers or sensors
- A gateway device,
- a communication network,
- processing software, and
- an end-user application service

Chapter 3
RESEARCH OBJECTIVES

Problem formulation

According to objects and their services, there are numerous types of identifiers with distinct identifying numbers. The methods used to identify items now differ from how they are used. It is necessary to use hierarchical identification techniques with the large evolved communication items. One example is the IPv6 address aggregation capability[40]. Different identification techniques are necessary depending on how things are categorised. Personal information is becoming more accessible, and unsolicited correspondence is on the rise. The diversity of the Internet with new device kinds and diverse networks worsens the overall issue. Improving Spectral Efficiency of Hybrid Architecture

- Reducing Hardware Complexity of Hybrid Architecture
- Reducing Computational Complexity of Hybrid Beamforming
- Reducing the High-Power Consumption.
- Maintaining Performance under Different Channel Conditions

The purpose of the research effort is to fulfil the following goals, which are based on the thorough review, research gaps, difficulties, and issue description offered in this section. In order to achieve the research objectives, wireless communication systems are being investigated:

I. **To performed a detailed literature review of the wireless communication system using the internet of things**
II. **To implement various applications of wireless communication technology with the aim of ensuring high reliability, low latency, and low interference**
III. **To describe the application of wireless communication technology in future engineering with the internet of things**
IV. **To study the process of wireless communication systems with high reliability of signal propagation in order to develop a communication system**
V. **To introduce the basic issues related to the processing and modulation of signals in the context of internet of things.**
VI. **To research signal modulation methods, particularly those involving high dependability, low latency, and the internet of things**
VII. **Compare the performance of the proposed method with existing methods and record the observation.**

Chapter 4
Research Methodology

4. Introduction

The Internet of Things (IoT) is the network that allows sensors, physical items, and other things to communicate with one another without the need for human intervention. WSNs are a key component of the Internet of Things' structural backbone. The two flexible fields of IoT and WSNs have encountered several challenges as well as essential and non-critical applications that touch almost every aspect of contemporary life[41]. These networks are, regrettably, predisposed to become increasingly vulnerable to security attacks. Security is therefore the most important component of IoT and WSNs. The fundamental constraint on these networks is their resource availability, as well. This chapter gives a thorough explanation of the research's general approach as well as its contributions. There have been several research done to examine stable key management in WSNs. But with IoT-enabled WSNs, creating reliable protocols is still an active research area. As a result, it's crucial to have a comprehensive grasp of the protection requirements for resource-constrained IoT networks, where knowledge of the fundamental network characteristics of IoT sensor networks and the restrictions of current security protocols is crucial. Resources such as processing power, battery capacity, and bandwidth resource limits, network infrastructure heterogeneity, mobility, and scalability are acknowledged as the most crucial WSN associated to IoT features[42]. Additionally, the security protocols' key management and authentication options are still too costly for IoT sensor systems with minimal power requirements. Consequently, the primary goal of this research is to design for restricted IoT using the available terms for authentication and key management. The focused research project is separated into organised phases that must be followed to accomplish the suggested study goals. Figure 4.1 illustrates the step-by-step process to be used for creating the ideal beamforming scheme and goes into greater detail.

- Study of wireless communication system for the internet of things that are used in high reliability and low latency
- Study of latest 5G network standards to find the requirement w.r.t. key performance metric.
- To assess the channel conditions and determine the frequency bands for various communication scenarios with internet of things challenges and technologies, a detailed review of the millimetre wave spectrum is required.
- A thorough analysis of enormous reliability and low latency in communication system beamforming techniques creates a solid knowledge basis that allows the most figures of research to be compared to one another to determine which is the best.

- The implementation of comparative analysis of well-known beamforming systems from the literature would improve knowledge of the variables influencing performance in various configurations/conditions[43].
- Analysis of the proposed beamforming scheme's performance using several performance measures and well-known beamforming techniques for various IOT, HRL, and LL configurations.

Every new project, the project team always needs to follow a methodology that helps them to satisfy the customer and work with peace of mind. So, several methods exist for this mission. This section presents a definition of selected methodologies for IoT domain. The selection of these methods is based on many previous surveys also on the 13th annual state of Agile report [6] which shows that the Scrum (54%) and Kanban (5%) are the most common agile methods used by organizations, in addition, the SAFe (30%) dominates scaling methodologies. In the other hand, we choose Ignite | IoT Methodology and IoT Methodology because they are the first methods created in IoT organizations specifically for IoT projects.

4.1. Ignite | IoT Methodology (Ignite)

Ignite is an open source methodology based on real-world experience that covering all aspects of IoT developing . It involves two main parts. The first part called "strategy execution", which defined IoT Strategy and prepared organization for IoT adoption, then created and managed a portfolio of IoT Project to support IoT strategy. The second is "solution delivery", which applied plan, build and run IoT solution.

4.2. IoT Methodology

IoT Methodology is an iterative methodology inspired by Lean startup and design thinking. Its objective is making the companies and smart cities innovated which aiming to provide a loosely structured ecosystem, and uses several steps for iteration, viz; CoCreate, Ideate, Q&A, IoT OSI, Prototype and Deploy

2.3. Scrum Scrum approach was influenced by lean development principles applying in Japanese industry. It has been developed as a set of guidelines helping team members understand how to work in order to produce a system in a constantly changing environment flexibly. This approach is simple to implement and works in any domain.

2.4. Kanban The notion of 'Kanban' comes from Japanese which means 'signboard'. It is a method highly flexible that required an explicit definition of process policies. It concentrates on the success of the software product by applying six principles which are Visualized the workflow, Limit Work in Progress, Manage the workflow, make processes/policies explicit, Implement feedback loops, Improve collaboratively. Like scrum, Kanban is designed to help teams at work together effectively.

4.3. Scaled Agile Framework (SAFe) SAFe comes to solve problems related to the development and delivery of software and systems in the shortest time. It is based on agile development, Systems thinking and Lean product development. It focuses on nine Lean-Agile principles such as Take an

Economic View; Apply Systems Thinking; Assume Variability, Preserve Options; Build Incrementally, with Fast Integrated Learning Cycles and so on

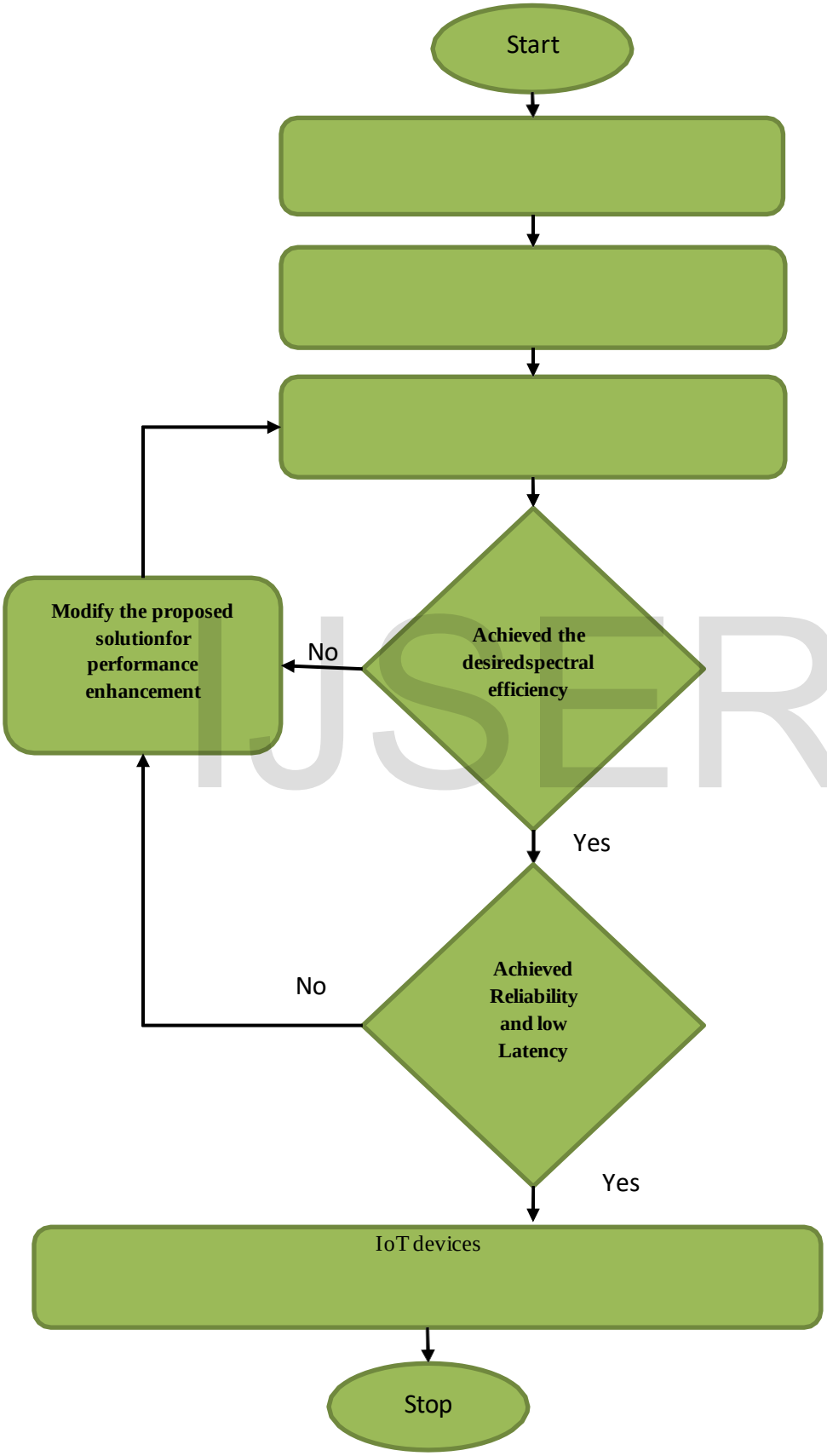

Figure 4.1: Research Methodology.

4.4. OVERALL RESEARCH METHODOLOGY

The research work focuses on the design of new WSN-IoT architecture security-based routing protocol. The entire design proposed for device is shown in Figure 4.2.

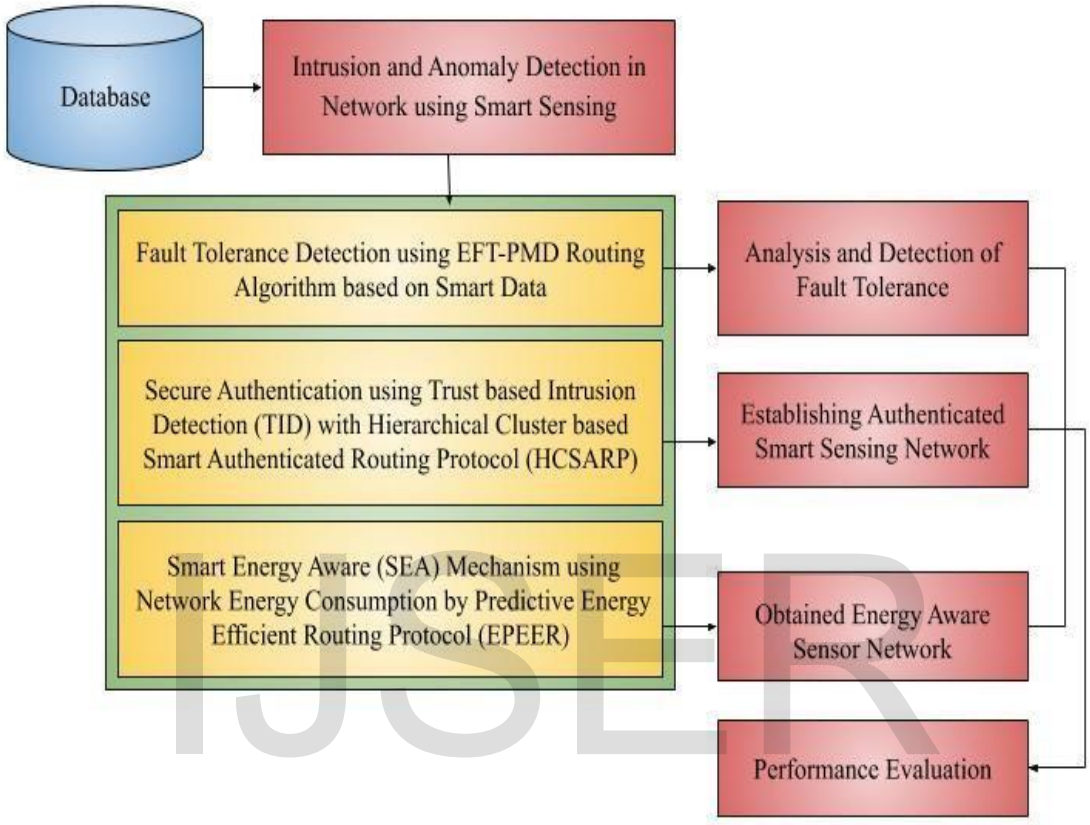

Figure 4.2, Overall Research Methodology Architecture

In IoT, communication takes place among smart objects, data are collected and some user requests are satisfied by various queried data. The drastic rise in energy consumption speeds up demand, resulting in a relative increase in the energy monetary value. This generates a critical market for implementing smart home applications that concentrate on energy efficiency in residential buildings. Developing energy efficient approaches to meet the challenges of IoT is crucial as IoT are wide and highly complex [27]. Recent WSNtechniques are not sufficient to work with IoT applications. So, this contribution proposes the Smart Energy Aware mechanism on basis of network performance using Energy consumption using Predictive Energy Efficient Routing Protocol (SEA-EPEER). This can improve the authentication and energy management system of network. For enhancing the network security, Hierarchical Cluster-based Smart Authenticated Routing Protocol (HCSARP) has been introduced with smart sensing. The results of the experiment carried out shows the improved security of the network.

Chapter 5
Conclusion

Recent years have seen a significant increase in interest in HRLL IoT research because to developments in information theory, wireless communication methods, and novel applications. We looked into common application scenarios, methods, and numerous HRLL IoT network options. There are frequently trade-offs between reliability and latency for the various code length requirements. Thus, it might be difficult to achieve high dependability and low latency at the same time, especially in IoT networks with limited resources. Various tactics need to be optimised in order to meet HRLL standards. They affect things like preamble length, network/channel coding, multiple access, resource allocation, and network optimization. Sophisticated designs should be carried out, especially for some crucial applications like power systems automation, power electronics control, and industrial automation. Future work on this may involve creating functional plans and systems for diverse scenarios in accordance with their unique needs.

In HRLL IoT networks, there is still a lot of work to be done in the physical layer as well as the MAC and network layer (e.g., initial access, mm Wave transmission, non-orthogonal multiple access, etc.). The physical layer includes packet structure optimization, preamble/pilots design, massive MIMO, short and high reliable channel coding, synchronization, and channel modelling and estimation. The HRLL communication will be able to satisfy a number of the most demanding needs to be fulfilled in future radio transmission. In order to do this, we predict that HRLL communication will be crucial in next IoT networks. the proposed objective of the research focuses intrusion and anomaly detection with energy conservation using smart sensing. The research contribution methods used to design routing protocol for WSN-IoT architecture. The performance of various methods depends of the different factors which are discussed in detail in upcoming chapters.

References

1 Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, "Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/3229294.

2 D. C. Nguyen *et al.*, "6G Internet of Things: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, 2022, doi: 10.1109/JIOT.2021.3103320.

3 S. K. Pattnaik *et al.*, "Future Wireless Communication Technology towards 6G IoT: An Application-Based Analysis of IoT in Real-Time Location Monitoring of Employees Inside Underground Mines by Using BLE," *Sensors*, vol. 22, no. 9, 2022, doi: 10.3390/s22093438.

4 K. Montgomery, R. Candell, Y. Liu, and M. Hany, "Wireless User Requirements for the Factory Workcell NIST Advanced Manufacturing Series 300-8 Wireless User Requirements for the Factory Workcell," *Adv. Manuf. Ser. (NIST AMS)*, vol. 1, 2021.

5 I. A. Sria, "Webinar on SRIA NetWorld 2020 SRIA : Smart Networks in the context of NGI," 2021.

6 W. Communication, D. Digitalization, and P. Industry, "5G Wireless Communication for Driving Digitalization in the Process Industry," vol. 64, no. 2, pp. 105–110, 2021.

7 M. I. of T. and E. MITE, "Smart Objects : The ' Things ' in IoT," 2021.

8 G. Chen *et al.*, "Application of 5G Communication Technology in Power Communication and Research on Key Technologies," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 791, no. 1, 2021, doi: 10.1088/1755-1315/791/1/012151.

9 M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," *IEEE Open J. Commun. Soc.*, vol. 1, no. August, pp. 957–975, 2020, doi: 10.1109/ojcoms.2020.3010270.

10 D. Scarlet, "The 5G Evolution," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2020.

11 World Economic Forum, "The Impact of 5G: Creating New Value across Industries and Society," *World Econ. Forum*, no. January, p. 24, 2020, [Online]. Available: http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf

12 D. T. Do, T. T. T. Nguyen, C. B. Le, and J. W. Lee, "Two-way transmission for low-latency and high-reliability 5G cellular V2X communications," *Sensors (Switzerland)*, vol. 20, no. 2, pp. 1–21, 2020, doi: 10.3390/s20020386.

13 M. F. Ali, D. N. K. Jayakody, Y. A. Chursin, S. Affes, and S. Dmitry, "Recent Advances and Future Directions on Underwater Wireless Communications," *Arch. Comput. Methods Eng.*, vol. 27, no. 5, pp. 1379–1412, 2020, doi: 10.1007/s11831-019-09354-8.

14 M.Anantha Guptha, "INTERNET OF THINGS & ITS APPLICATIONS Lecture Notes MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY," *Auton. Inst. – UGC, Govt. India*, vol. 2, 2020.

15 A. Jiang, H. Yuan, D. Li, and J. Tian, "Key technologies of ubiquitous power Internet of Things-aided smart grid," *J. Renew. Sustain. Energy*, vol. 11, no. 6, 2019, doi: 10.1063/1.5121856.

16 Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-Reliability and Low-Latency Wireless Communication for Internet of Things: Challenges, Fundamentals, and Enabling Technologies," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7946–7970, 2019, doi: 10.1109/JIOT.2019.2907245.

17 G. G. K. W. M. S. I. R. Karunarathne, K. A. D. T. Kulawansa, and M. F. M. Firdhous, "Wireless communication technologies in internet of things: A critical evaluation," *2018 Int. Conf. Intell. Innov. Comput. Appl. ICONIC 2018*, no. June, 2019, doi: 10.1109/ICONIC.2018.8601226.

18 M. A. Siddiqi, H. Yu, and J. Joung, "5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices," *Electron.*, vol. 8, no. 9, pp. 1–18, 2019, doi: 10.3390/electronics8090981.

19 Cybersecurity and Infrastructure Security Agency, "The Internet of Things: Impact on Public Safety Communications," no. March, pp. 1–6, 2019, [Online]. Available: https://www.linux.com/news/who-needs-internet-things

20 M. Bennis, M. Debbah, and H. V. Poor, "Ultrareliable and Low-Latency Wireless Communication: Tail, Risk, and Scale," *Proc. IEEE*, vol. 106, no. 10, pp. 1834–1853, 2018, doi: 10.1109/JPROC.2018.2867029.

21 E. M. F. E. Series, "EMF Explained Series 1," no. March, pp. 1–12, 2018.

22 S. Tsoka, K. Tsikaloudaki, and T. Theodosiou, "Investigation Methods and Mitigation," *Energies*, 2020.

23 E. Kim, D. Kaspar, C. Gomez, and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing," *Rfc*, no. May, 2012.

24 W. Mengdi and W. Mengdi Vaasa, "Wireless Communiaction Technologies in Internet of Things (Iot)," no. September, pp. 1–57, 2016.

25 "Introduction_to_Wireless_Communication_S.pdf."

26 X. Zhang, "Advanced Wireless Communication Technologies for Energy Internet," *Front. Energy Res.*, vol. 10, no. April, pp. 1–4, 2022, doi: 10.3389/fenrg.2022.889355.

27 s. To *et al.*, "hybrid nsga inter-cluster heuristic algorithm for mobile sink in wireless sensor networks . Candidate ' s declaration," 2022.

28.]V. Krotov, "The Internet of Things and new business opportunities," Bus. Horiz., vol. 60, no. 6, pp. 831–841, Nov. 2017, doi: 10.1016/j.bushor.2017.07.009.

29. M. A. Feki, F. Kawsar, M. Boussard, and L. Trappeniers, "The Internet of Things: The Next Technological Revolution," Computer, vol. 46, no. 2, pp. 24–25, Feb. 2013, doi:

10.1109/MC.2013.63. [3] S. Elhadi, A. Marzak, N. Sael, and S. Merzouk, "Comparative Study of IoT Protocols," SSRN Electron. J., 2018, doi: 10.2139/ssrn.3186315.

30. I. Jacobson, I. Spence, and P.-W. Ng, "Is There a Single Method for the Internet of Things?," Queue, vol. 15, no. 3, pp. 25–51, 2017, doi: https://doi.org/10.1145/3106637.
31. D. Slama, F. Puhlmann, J. Morrish, and R. M. Bhatnagar, Eds., Enterprise IoT: Enterprise IoT: strategies and best practices for connected products and services. Beijing Boston Farnham Sebastopol Tokyo: O'Reilly, 2016.
32. VersionOne and CollabNet, "The 13th annual State of Agile report," 2018. [Online]. Available: stateofagile.com.
33. T. Collins, "A Methodology for Building the Internet of Things," p. 25.
34. "IoT Methodology – The Internet of Things project lifecycle guide for creative, technical and business people." http://www.iotmethodology.com/.
35. S. Merzouk, S. Elhadi, A. Cherkaoui, A. Marzak, and N. Sael, "Agile Software Development: Comparative Study," SSRN Electron. J., 2018, doi: 10.2139/ssrn.3186323.
36. M. L. DESPA, "Comparative study on software development methodologies," Database Syst. J. BOARD, vol. 5, p. 3, 2014.
37. J. Sutherland and K. Schwaber, "Nut, Bolts, and Origins of an Agile Framework," p. 224.
38. H. K. Flora and S. V. Chande, "A Systematic Study on Agile Software Development Methodologies and Practices," IJCSIT, vol. 5, no. 3, pp. 3626–3637, 2014.
39. D. J. Anderson, Kanban: Successful Evolutionary Change for Your Technology Business, Illustrée. Blue Hole Press, 2010.
40. R. Knaster, SAFe 4.0 distilled: applying the Scaled Agile Framework for Lean software and systems engineering. Boston, MA: AddisonWesley, 2017.
41. "What is SAFe | Scaled Agile." https://www.scaledagile.com/enterprise-solutions/what-is-safe/. [16] Ivar JACOBSON, "SAFe Principles," Ivar Jacobson International, Jun. 29, 2017. https://www.ivarjacobson.com/publications/blog/safeprinciples.
42. G. Görkem, T. Bedir, and T. Eray, "IoT System Development Methods," in Internet of things challenges, advances, and applications, Chapman & Hall/CRC Press, 2018, pp. 141–159.
43. C. Ebert and M. Paasivaara, "ScalingAgile," IEEE Softw., vol. 34, no. 06, pp. 98–103, 2017.