

Article

Novel AMI in Zigbee Satellite Network Based on Heterogeneous Wireless Sensor Network for Global Machine-to-Machine Connectivity

Chia-Lun Wu ¹, Tsung-Tao Lu ¹, Chin-Tan Lee ^{2,*}, Jwo-Shiun Sun ¹, Hsin-Piao Lin ¹, Yuh-Shyan Hwang ¹ and Wen-Tsai Sung ^{3,*}

¹ Department of Electronic Engineering, National Taipei University of Technology, Taipei City 106008, Taiwan; tl108369007@ntut.edu.tw (C.-L.W.); tl108369011@ntut.edu.tw (T.-T.L.); jssun@ntut.edu.tw (J.-S.S.); hplin@ntut.edu.tw (H.-P.L.); yshwang@ntut.edu.tw (Y.-S.H.)

² Department of Electronic Engineering, National Quemoy University, Jinning 892009, Taiwan

³ Department of Electrical Engineering, National Chin-Yi University of Technology, Taichung City 411030, Taiwan

* Correspondence: ktleee@nqu.edu.tw (C.-T.L.); songchen@ncut.edu.tw (W.-T.S.); Tel.: +886-082-313539 (C.-T.L.); +886-4-23924505 (ext. 7225) (W.-T.S.)

Abstract: This study endeavored to enhance the efficiency and utility of microcomputer meters. In the past, their role was predominantly confined to remote meter reading, entailing high construction and communication transmission costs, coupled with subsequent maintenance and operational expenditures. These factors collectively impacted the enthusiasm of various stakeholders to invest in this realm. Hence, in alignment with the smart city development initiative, the natural gas industry has pioneered the establishment of an advanced metering infrastructure with heterogeneous wireless sensor networks (HWSNs) at its core. This visionary leap incorporates global machine-to-machine connectivity (G-M2MC) technology, interconnecting all facets of its operations, thereby positioning itself as a trailblazer within the industry. While advancing this endeavor, the project's scheduling aligns with the enterprise's sustainability goals in the early stages of digital transformation. This strategic allocation of resources is responsive to government policies and aspires to cultivate a digitally connected smart green energy hub, thereby expediting the transformation of the living environment. The objective is to provide a stable, secure, cost-effective, and reliable system that can be shared among peers. Furthermore, this study delved into the analysis of congestion avoidance in intelligent Zigbee satellite transport networks based on the HWSNs-GM2MC of non-synchronous satellite orbit system (NGSO) pivotal technologies, utilizing them to integrate the smart LNGas management system (SGMS). Concurrently, it developed application services through the smart meter application interface (SMAPI), distinct from conventional microcomputer meters. However, it is imperative to acknowledge that cloud computing, while processing sensitive data, grapples with issues of latency, privacy, efficiency, power consumption, and zero-trust security risk information management and ethical authority management capabilities in the defense of disaster relief responses.

Keywords: heterogeneous wireless sensor networks; global M2M connectivity; non-geosynchronous satellite orbit; smart LNGas management system; smart meter application interface



Citation: Wu, C.-L.; Lu, T.-T.; Lee, C.-T.; Sun, J.-S.; Lin, H.-P.; Hwang, Y.-S.; Sung, W.-T. Novel AMI in Zigbee Satellite Network Based on Heterogeneous Wireless Sensor Network for Global Machine-to-Machine Connectivity. *Electronics* **2024**, *13*, 1421. <https://doi.org/10.3390/electronics13081421>

Received: 22 February 2024

Revised: 21 March 2024

Accepted: 3 April 2024

Published: 9 April 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Semiconductor technologies, networking, and material sciences persist in their relentless advancement, fueling the utilization of HWSN architectures for wireless transmission and sensing communication. This, in turn, is poised to alleviate costs. Consequently, wireless, low-power, and cost-effective network applications are poised to dominate the communication landscape. Presently, ZigBee applications garner widespread favor. ZigBee is prized for its attributes of simplicity and energy efficiency. It found a natural niche in

transmitting data from low-rate sensor components, encompassing industrial and domestic sensors, interactive gaming, and various other domains. Idealizing the utilization of ZigBee is, therefore, a judicious choice.

Within the realm of ZigBee transmissions, signals originating from sensors or network nodes may embark on lengthy journeys in search for the nearest connecting node for data transmission. Subsequently, they proceed to establish a connection with the primary device through a single hop or multiple hops, culminating in a successful transfer of data.

Presently, ZigBee chips available in the market either lack the capability for hopping transmissions or exhibit an immature hopping transmission feature. This paper elucidates the design and practical implementation of the hopping transmission function utilizing the 2.4 GHz frequency band modulation system. It expounds upon the design principles of the 802.15.4 base frequency system, thereby fostering a comprehensive grasp of the design philosophy and principles underpinning the ZigBee hopping transmission system analysis [1,2].

Furthermore, this study delved into the technical architecture of cloud computing management systems, acquainting us with their principal components and applications [3]. In this journey, we employed Zigbee sensing equipment to empirically evaluate the feasibility of integrating wireless signals into an SGSM. We explored diverse application technologies of the management system, culminating in the amalgamation of data feedback from the ZigBee sensing platform through the nexus of the management and communication systems. These elements were coalesced into an integrated service application system, thereby affirming the viability of this application design.

These elements play an important role in fulfilling the goals of operation in multi-radio access technology (Table 1). Important requirements for the goals of operation in multi-radio access technology (M-RAT) include the following three key features:

1. Technologies: The novel advanced metering infrastructure (AMI) architecture is becoming increasingly popular, such as in M-RAT, Multi-Layer, and Multi-Vendor technologies, that is integrated in wireless communication adoption applications and provides the benefits of modularization and interoperability.
2. Networks: An HWSN infrastructure can easily solve the reliability, performance, and compatibility issues of these systems, which operators believe will improve transmission limitations.
3. Systems: Low-power node environments with low capital costs, low implementation risk, and fast roll out allow operators to try these SGMS platforms.

Table 1. Important requirements for the operation of M-RAT.

Solve Problem		
The Taiwan liquefied natural gas operator (LNGasO) must install simple and stable systems to improve signal intensity within high buildings, congregate housing, toutingcuo, and apartments to facilitate integration with and the extension of existing architecture, reserve active and passive equipment space necessary for a next-generation novel system, and improve the quality of the communication network.		
	Technologies	Business Requirement
Multi-Radio Access Technology Multi-Layer Multi-Vender	Capacity Enhancement Global M2M Connectivity (G-M2MC) Technology	Modularization Interoperability
Spectrum Extension Spectrum Efficiency Network Densification	HetNets-WSNs Software Defined Wide Area Networks (SD-WAN)	Reliability Performance Compatibility
Low-Power Nodes (LPNs) Reinforcement Learning (RL) Fiber to the Wireless (FTTW) Cable Modem to Wireless (CMTW)	LPN + RL + FTTW/CMTW = Novel AMI Architecture Smart LNGas Management System (SGMS) Distributed Antenna Systems (DASs)	Fast Roll Out Low Capital Costs Low Implementation Risk

Henceforth, while operating on the principles of cloud computing, an SGMS shall be overseen, operated, and managed by telecommunications operators upon its completion. Leveraging internet transmission, system administrators can remotely access client information and exert control over smart meters [4]. This platform, cultivated through mobile telecommunication networks, enables a gas operator to forge a “gas cloud” exclusive to the natural gas operator, founded upon a cooperative and mutually advantageous model [5–7].

The smart meter communicates data encompassing parameters such as temperature, pressure, and issues alerts through a wireless apparatus [8–10]. Subsequently, it conveys this information from a controller to an intelligent meter cloud server management platform within the innovative information and communication technology (ICT) framework of the Telecom operator employing LTE-Advanced (LTE-A) and fifth-generation (5G) cellular systems [11–13]. Telecom operators use software-defined wide area network (SD-WAN) technology to transform the traditional distributed network control architecture into a centralized control architecture through a centralized controller (SDN controller), which can effectively improve network usage efficiency. The core spirit of flexible management and control is to provide a virtual abstraction of the entire network and programmability of application services, and to provide more network services and novel smart meter cloud management through applications [14].

Currently, the access network equipment mainly deployed (e.g., GPON, LTE, NB-IoT, xDSL & FTTX, Satellite) is still based on the traditional distributed management architecture. Therefore, how to introduce the current access network equipment into SDN-WAN management to obtain the advantages of programmable management and control of application services and network resources is shown in Figure 1. Users can also access the usage status of smart meters through communication terminal equipment [15–18].

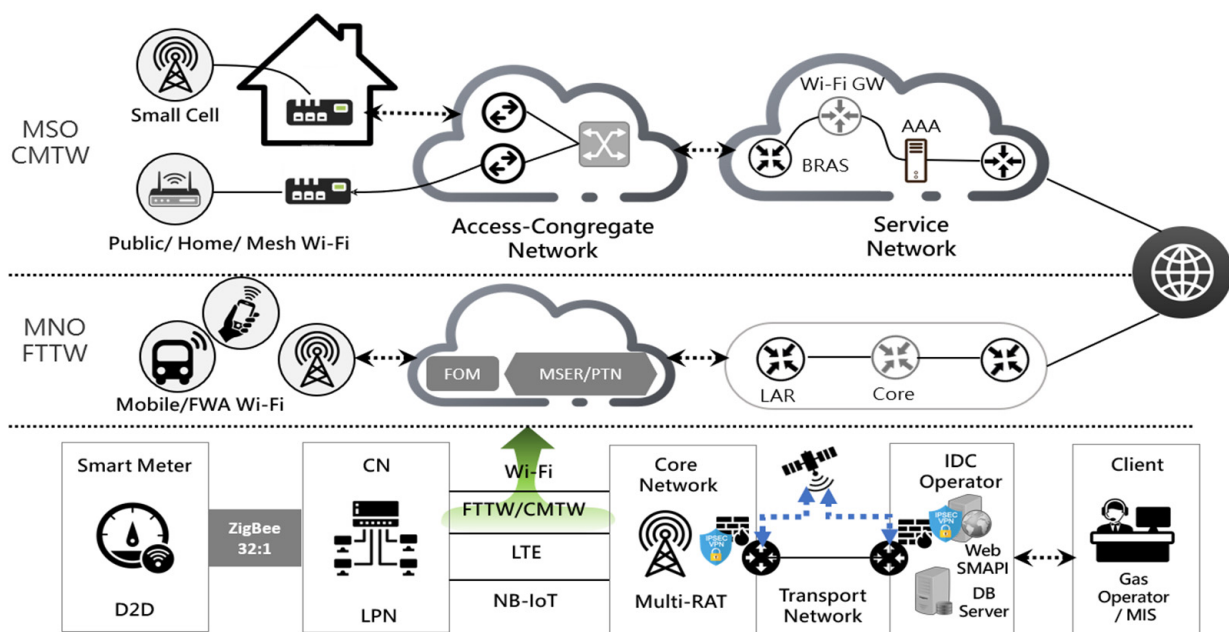


Figure 1. A novel AMI in a Zigbee satellite network.

This architectural design is predicated upon the noble principle of enhancing the critical infrastructure of the nation while seamlessly amalgamating the distinctive attributes of multi-layer heterogeneous networks. The symbiosis of a mobile network operator (MNO) and multimedia service provider (MSO) exemplifies a commendable instance of heterogeneous integration, poised to fortify the burgeoning wave of multi-vendor network amalgamation and enhance the network resilience of smart cities.

The structure of this paper is based on the hierarchy of global M2M connectivity (G-M2MC) technology, as depicted in Figure 2. It unfolds as follows: Section 2 elucidates the design principles governing the AMI for heterogeneous wireless sensor networks (HWSNs). Subsequently, Sections 3–5 delve into investigations concerning key determinants and resolutions pertaining to the SD-WAN network within the context of the SGMS system’s AMI architecture, aligned with IEEE802.15.4-TG4g. Finally, Section 6 culminates in a conclusion.

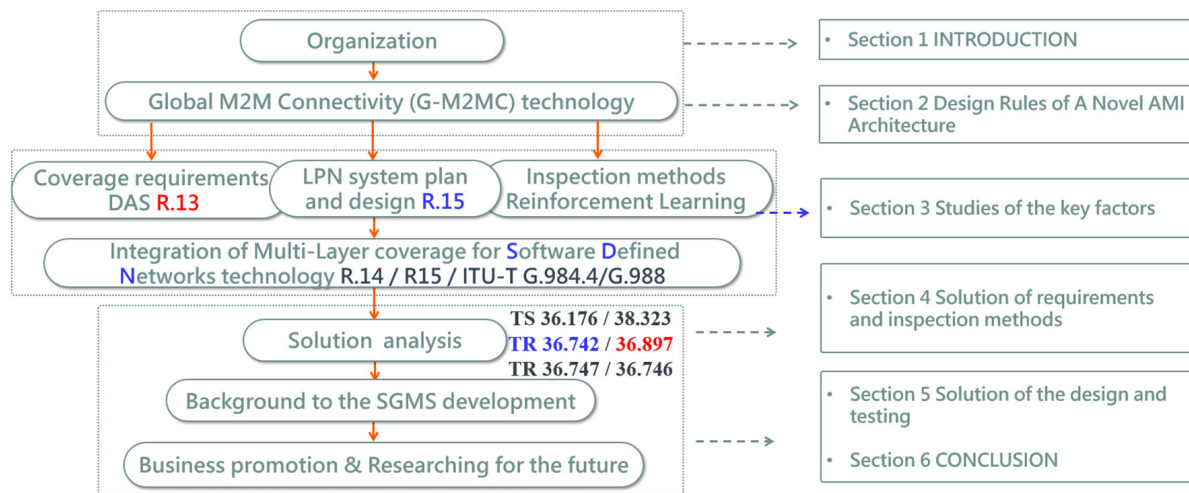


Figure 2. Hierarchy of global M2M connectivity technology.

2. Design Principles for Mesh Networks

The bedrock of wireless communication systems for intelligent meters lies in MIMO and ZigBee wireless technologies.

2.1. Multi-Input, Multi-Output

A MIMO configuration is applied in novel wireless multi-radio access technologies (Multi-RATs), Wi-Fi, LTE, and NB-IoT. While wireless Wi-Fi devices can boast two to four antennas, smart meters typically accommodate no more than two antennas. The augmentation of antennas on diminutive terminals hinges upon the sophistication of superconducting materials.

The expanse for MIMO’s proprietary advancement seems somewhat constrained. Lately, the technology spotlight has gravitated toward methods employing a solitary antenna to achieve heightened gain across multiple directions, eclipsing the prominence of superconducting materials. Furthermore, MIMO technology embodies non-line-of-sight transmission capabilities, transcending the mere consideration of transmitting and receiving antenna quantities.

At present, MIMO functions as a conduit for point-to-multipoint communication between communication nodes and smart meters. Multipoint-to-multipoint communication techniques must be extended to commensurate with environmental prerequisites, optimizing both bandwidth utilization and communication steadfastness. Consequently, the application of MIMO configurations within mesh networks is poised to dominate forthcoming communication landscapes.

MIMO technology endows the prospect of array gain, interference abatement, diversity gain, and multiplexing gain, promising an amplification of system coverage, heightened link quality, augmented system capacity, and spectral efficiency enhancement, thus elevating data transmission speeds. Additionally, in tandem with the swift evolution of modern digital signal processing technology and the perpetually escalating processing capabilities of digital computing chips, the computational intricacies accompanying MIMO have experienced significant reductions, rendering it more practicable than ever.

In envisioning the requisites of prospective wireless communication systems, MIMO proffers dual categories of gain—spatial diversity gain and spatial multiplexing gain. These, respectively, augur enhancements in link quality and data transmission speeds.

2.2. IEEE802.15.4-TG4g

This section delves into an assessment of ZigBee's cutting-edge performance benchmark known as the smart utility network (SUN). Its scope encompasses the next echelon of intelligent power grids. It is envisaged that a progression toward employing numerous intelligent meters and multiple communication nodes for data exchange with base stations within the communication system architecture will emerge as a prevailing trajectory [19–22]. This standard lays the groundwork by delineating the initial two layers of the OSI model, catering to low-rate wireless personal area networks (LR-WPANs).

The physical (PHY) layer meticulously defines the requisite attributes that wireless radio frequencies should embody. It lends support to two disparate radio frequency spectra, situated at 868 MHz, 915 MHz, and 2450 MHz. The radio frequency range of 2450 MHz bestows the capability of delivering data rates of 250 kbps, accompanied by 16 message channels. In contrast, the 868/915 MHz spectrum designates 868 MHz for a single message channel, operating at a data rate of 20 kbps, while 915 MHz graciously offers ten message channels, with data transmission cruising at 40 kbps.

Meanwhile, the Media Access Control (MAC) layer shoulders the mantle of facilitating data interchange among proximate devices. It shoulders the responsibility for forging connections and orchestrating network synchronization, thereby establishing a robust linkage between two devices. ZigBee introduces a triumvirate of network topologies at the network layer: the star topology, tree topology, and mesh topology networks. In Figure 3, we encounter simplified representations of these three network topologies, encompassing (a) the star topology, (b) the tree topology, and (c) the mesh topology [23,24].

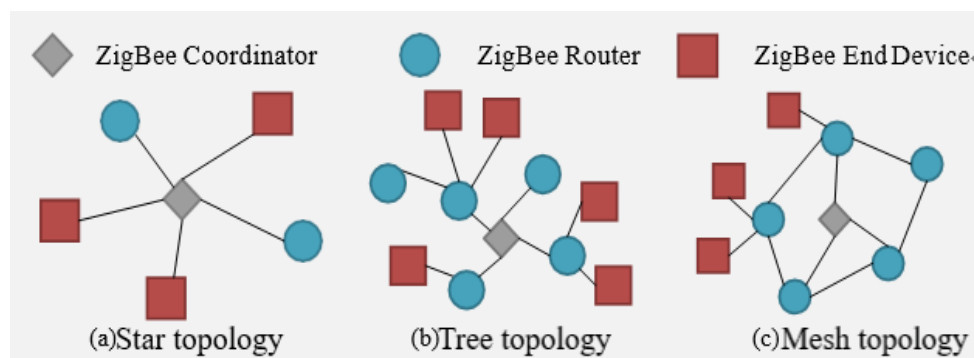


Figure 3. Diagram of three ZigBee network topologies.

In each topology, a solitary ZigBee coordinator assumes the solemn duties of the inauguration, perpetuation, and governance of the network. Within the precincts of the star topology, devices are confined to the exchange of data solely with the coordinator. In the realms of the tree and mesh topologies, devices engage in reciprocal communication through the agency of a multi-hop routing mode. The structural scaffolding of both tree and mesh topologies consists of a coordinator supported by an array of routers. The discerning contrasts between the three topological paradigms are elucidated in Table 2.

Upon the network's commencement, the fully fledged devices within its domain engage in a spirited competition, each vying for the esteemed title of ZigBee coordinator. Upon successful ascension to this pivotal role, the coordinator embarks upon a comprehensive survey of all wireless frequency bands, meticulously selecting a well-suited channel for reference. Subsequently, a network address is bestowed upon devices through the auspices of the beacon's transmitting entity, serving as a distinctive insignia for forthcoming data transmissions. Channel scanning, an innate function, is entrusted with the responsibility of

detecting activity or extraneous interference within a channel. This physical layer consideration enables network protocols to discern whether any channels within a designated frequency band might impede communication among nodes.

Table 2. Comparison of star tree and mesh topologies.

Topology	Star	Tree	Mesh
Protocol	Slotted CSMA/CA	Slotted CSMA/CA	Unslotted CSMA/CA
Pros.	1. Easy to synchronize 2. Low latency	1. Router consumes low energy 2. Can support sleep mode 3. Support large-scale network	1. Support multipoint connection 2. High flexibility of network architecture 3. Low latency 4. Support large-scale network
Cons.	1. Small scope	1. Data transmission consumes more energy 2. High latency	1. Cannot support sleep mode 2. Router consumes more energy

Frequency flexibility is a hallmark of the network, endowing it with the capacity to adapt its operating channels for all nodes, ensuring seamless operation even when channels become afflicted by interference. The efficacy of message transmission stands to be enhanced through the incorporation of a confirmation mechanism. Upon a successful reception of a packet, the receiving node dutifully dispatches a confirmation signal to the originating transmitter. This duality of point-to-point acknowledgment and message retries significantly mitigates the probability of packet loss. The point-to-point acknowledgment feature engenders a heightened assurance that packets shall not suffer the misfortune of being lost, a paramount concern in sprawling point-to-multipoint networks under positioning via delivery access algorithms [25].

2.3. Network Structure and Address Allocation

The ZigBee network layer protocol prescribes a distributed network address allocation algorithm used to endow devices with network addresses. During network formation, the coordinator initially delineates three parameters in accordance with user-defined preferences:

1. Cm: The maximum number of child devices that both the coordinator and routers can accommodate.
2. Rm: The maximum number of routers (Rm) among the child devices situated between the coordinator and other routers.
3. Lm: The maximum depth (d) of the network.

In adherence to the specification, Cm must be greater than or equal to Rm, thereby ensuring that the ZigBee coordinator and routers can connect to a minimum of (Cm – Rm) end devices. Within this specification, device network addresses are assigned by their parent node, which is typically a Parent Router. For coordinators and routers, the address sub-block they possess, available for allocation to sub-devices, is divided into (Rm + 1) segments, deducting those already assigned to sub-end devices. The remaining address sub-blocks are uniformly apportioned to each sub-router, ensuring that they possess address sub-blocks to allocate among their respective child devices.

In this computational endeavor, the coordinator and routers employ the aforementioned parameters in conjunction with the current depth (d) to calculate the parameter Ctrip(d). Subsequently, they employ Ctrip(d) to compute the network addresses for their sub-routers and sub-end devices. The significance of Ctrip(d) resides in its determination of the size of the address sub-block that a router at depth d provides to a sub-router, tasked with allocating addresses to sub-devices that encompass both the sub-router itself and all subsequent depth branches. This is elegantly represented in Equation (1):

$$C_{trip}(d) = \begin{cases} 1 + C_m \times (L_m - d - 1), & R_m = 1 \\ \frac{1 + C_m - R_m - C_m \times R_m^{L_m - d - 1}}{1 - R_m}, & \text{Otherwise} \end{cases} \quad (1)$$

The coordinator must be at depth 0, and the network address must also be 0. After the parameter $C_{trip}(d)$ is calculated, whenever a node wants to join the network, the parent node connected to it uses the following formula to allocate network addresses:

1. For the k th router, as shown in Equation (2):

$$A_k = A_{\text{parent}} + C_{trip}(d) \times (k - 1) + 1 \quad (1 \leq k \leq R_m) \quad (2)$$

2. For an n th end device, as shown in Equation (3):

$$A_n = A_{\text{parent}} + C_{trip}(d) \times R_m + n \quad (1 \leq n \leq C_m - R_m) \quad (3)$$

In the above equations, when a child device is a router, k represents the number of child routers currently owned by the parent node; the following formula is used when the child device is an end device, and n represents the number of child end devices currently owned by the parent node.

For example, assuming that the network topology of $D_m = 1$, $R_m = 2$, and $L_m = 3$, substitute it into Equation (1). In calculating $C_{trip}(d)$, you can obtain $C_{trip}(-1) = 22$, $C_{trip}(0) = 10$, $C_{trip}(1) = 4$, and $C_{trip}(2) = 1$. Figure 4 shows a summary diagram; the numbers in the diagram represent the network addresses.

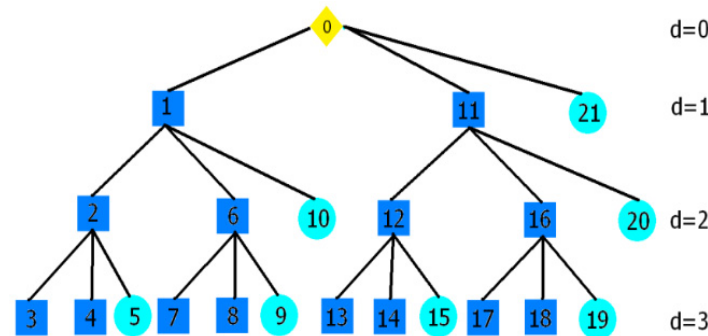


Figure 4. ZigBee tree topology address allocation diagram.

$$\therefore C_m = R_m + D_m = 2 + 1 = 3$$

$$\therefore [R_m, D_m, L_m] = [2, 1, 3] \rightarrow [C_m, D_m, L_m] = [3, 2, 3]$$

Equation (1)

$$C_{trip}(-1) = 1 + 3 - 2 - 3 \cdot 2^{3-(-1)-1} / (1 - 2) = 2 - 3 \cdot 2^3 / -1 = 22$$

$$C_{trip}(0) = 1 + 3 - 2 - 3 \cdot 2^{3-(-0)-1} / (1 - 2) = 2 - 3 \cdot 2^2 / -1 = 10$$

$$C_{trip}(1) = 1 + 3 - 2 - 3 \cdot 2^{3-(1)-1} / (1 - 2) = 2 - 3 \cdot 2^1 / -1 = 4$$

$$C_{trip}(2) = 1 + 3 - 2 - 3 \cdot 2^{3-(2)-1} / (1 - 2) = 2 - 3 \cdot 2^0 / -1 = 1$$

$$1 \leq k \leq R_m = 2, 1 \leq n \leq C_m - R_m = 3 - 2 = 1$$

As: d = 0

$$A_{\text{parent}} = 0,$$

$$\text{Router A1} = 0 + C_{trip}(0) \cdot (1 - 1) + 1 = 10 \cdot 0 + 1 = 01$$

$$\text{Router A2} = 0 + C_{trip}(0) \cdot (2 - 1) + 1 = 10 \cdot 1 + 1 = 11$$

$$\text{ED A3} = 0 + C_{trip}(0) \cdot 2 + 1 = 10 \cdot 2 + 1 = 21$$

As: d = 1

$$A_{\text{parent}} = 1,$$

$$\text{Router A1} = 1 + C_{trip}(1) \cdot (1 - 1) + 1 = 1 + 4 \cdot 0 + 1 = 2$$

$$\text{Router A2} = 1 + C_{trip}(1) \cdot (2 - 1) + 1 = 1 + 4 \cdot 1 + 1 = 6$$

$$\text{ED A3} = 1 + C_{trip}(1) \cdot 2 + 1 = 1 + 4 \cdot 2 + 1 = 10$$

$$\begin{aligned}
A_{\text{parent}} &= 11, \\
\text{Router A1} &= 11 + \text{Ctrip}(1) \cdot (1 - 1) + 1 = 11 + 4 \cdot 0 + 1 = 12 \\
\text{Router A2} &= 11 + \text{Ctrip}(1) \cdot (2 - 1) + 1 = 11 + 4 \cdot 1 + 1 = 16 \\
\text{ED A3} &= 11 + \text{Ctrip}(1) \cdot 2 + 1 = 11 + 4 \cdot 2 + 1 = 20 \\
\text{As: } d &= 2 \\
A_{\text{parent}} &= 2, \\
\text{Router A1} &= 2 + \text{Ctrip}(2) \cdot (1 - 1) + 1 = 2 + 1 \cdot 0 + 1 = 3 \\
\text{Router A2} &= 2 + \text{Ctrip}(2) \cdot (2 - 1) + 1 = 2 + 1 \cdot 1 + 1 = 4 \\
\text{ED A3} &= 2 + \text{Ctrip}(2) \cdot 2 + 1 = 2 + 1 \cdot 2 + 1 = 5 \\
A_{\text{parent}} &= 6, \\
\text{Router A1} &= 6 + \text{Ctrip}(2) \cdot (1 - 1) + 1 = 6 + 1 \cdot 0 + 1 = 7 \\
\text{Router A2} &= 6 + \text{Ctrip}(2) \cdot (2 - 1) + 1 = 6 + 1 \cdot 1 + 1 = 8 \\
\text{ED A3} &= 6 + \text{Ctrip}(2) \cdot 2 + 1 = 6 + 1 \cdot 2 + 1 = 9 \\
A_{\text{parent}} &= 12, \\
\text{Router A1} &= 12 + \text{Ctrip}(2) \cdot (1 - 1) + 1 = 12 + 1 \cdot 0 + 1 = 13 \\
\text{Router A2} &= 12 + \text{Ctrip}(2) \cdot (2 - 1) + 1 = 12 + 1 \cdot 1 + 1 = 14 \\
\text{ED A3} &= 12 + \text{Ctrip}(2) \cdot 2 + 1 = 12 + 1 \cdot 2 + 1 = 15 \\
A_{\text{parent}} &= 16, \\
\text{Router A1} &= 16 + \text{Ctrip}(2) \cdot (1 - 1) + 1 = 16 + 1 \cdot 0 + 1 = 17 \\
\text{Router A2} &= 16 + \text{Ctrip}(2) \cdot (2 - 1) + 1 = 16 + 1 \cdot 1 + 1 = 18 \\
\text{ED A3} &= 16 + \text{Ctrip}(2) \cdot 2 + 1 = 16 + 1 \cdot 2 + 1 = 19
\end{aligned}$$

3. Study of the Pivotal Factors

The advanced metering infrastructure is currently witnessing fervent development efforts in Europe, the United States, Japan, and various other nations. These endeavors center around the creation of smart meters with a resolute aim of energy conservation and carbon reduction. The overarching smart grid, encompassing low-power node (LPN) environments, power generation, transmission, distribution, and user terminals, is instrumental in achieving these objectives. Within the realm of natural gas management, the prevailing system architecture is demarcated into three distinct segments: smart meter (SM), communication node (CN), and device-to-device (D2D) robust architectures integrated into the smart LNGas management system (SGMS).

Beyond the obsolescence of manual meter reading, the system boasts an intrinsic capability to accommodate diverse natural gas rates, bestowing upon the user valuable insights into their energy consumption patterns, thereby guiding them toward voluntary energy conservation, cessation, and recovery. Moreover, it streamlines gas management, augments asset management for natural gas smart meter equipment, and presents several other advantageous facets.

Upon meticulous scrutiny, the natural gas industry anticipates prioritizing the widespread deployment of natural gas smart meters within key community edifices by the year 2020. This strategic endeavor is poised to catalyze the growth of industries closely intertwined with AMIs by capitalizing on the technological prowess within the nation's information and communication technology (ICT) sector. For low-pressure gas consumers, concomitant with the Energy Bureau's policies and a thorough benefits assessment, the proliferation of microcomputer meters among end users shall transpire progressively.

The objectives underpinning the establishment of an AMI by natural gas operators are as follows:

- (1) The facilitation of remote automated meter reading:

Curtailing the need for meter-reading personnel and the associated energy consumption stemming from travel.

- (2) The enhancement of gas safety:

By capturing and dissecting parameters from intelligent microcomputer meters, the system facilitates the issuance of pertinent event alarms.

(3) The amplification of emergency repair efficiency:

The management platform equips stakeholders with critical information, such as accident locations and event classifications, streamlining emergency repair operations.

(4) The mitigation of gas consumption loss:

In juxtaposing historical gas consumption data and records of anomalous events and integrating them with the monitoring system at pressure regulator stations, losses attributable to aging pipelines can be minimized.

(5) The promotion of the domestic energy information and communications industry:

This endeavor bolsters the domestic information and communication industry's entry into the natural gas domain, fostering the establishment of independent AMI technologies.

3.1. Modulation Data and Spread Spectrum Specifications

The physical layer specification delineates three spectral realms for ZigBee, precisely 2.4 GHz, 915 MHz, and 868 MHz. Each operating spectrum lays claim to specific channels, numbering 1, 10, and 16. The 2.4 GHz spectrum encompasses bands ranging from 11 to 26, aggregating 16 channels. The physical layer, positioned as the foundational stratum within the OSI model, bears the solemn responsibility of enabling and interrupting wireless communication transceiver devices. Its purview extends to the transmission and retrieval of information, the execution of signal energy detection across the present spectrum, and the capture of frame signals. The ambient channel diligently carries out pilot signals, which is essential for the detection of link characteristics. The data modulation and spread spectrum technical specifications, tailored for disparate frequency bands, are meticulously cataloged in Table 3 [2,26].

Table 3. Modulation and spread spectrum technical specifications.

PHY	Frequency Band	Spreading Parameters			Data Parameters	
		Chip Rate	Modulation	Bit Rate	Symbol Rate	Symbols
868/915 MHz PHY	868–868.6 MHz	300 k chip/s	BPSK	20 kb/s	20 k symbols/s	Binary
	902–928 MHz	600 k chip/s	BPSK	40 kb/s	40 k symbols/s	Binary
2.4 GHz PHY	2.4–2.4835 GHz	2.0 M chip/s	O-QPSK	250 kb/s	62.5 k symbols/s	16-ary Orthogonal

Regarding the spread spectrum factor within the international ISM Band, which operates at the 2.4 GHz communication mode, it is imperative to recognize that symbol data are intricately linked to chip values. Within this context, it is noteworthy that every grouping of four bits coalesces into a singular symbol, with each symbol being intrinsically associated with a chip value spanning a length of 32. The cyclic interplay between these chip codes is elegantly elucidated in Table 4 [2,26,27].

Table 4. The cyclic relationship between symbol data and chip value.

Data Symbol (Decimal)	Data Symbol (Binary) (b0 b1 b2 b3)	Chip Values (c0 c1 ... c30 c31)
0	0000	11011001110000110101001000101110
1	1000	11101101100111000011010100100010
2	0100	00101110110110011100001101010010
3	1100	00100010111011011001110000110101
4	0010	01010010001011101101100111000011
5	1010	00110101001000101110110110011100

Table 4. Cont.

Data Symbol (Decimal)	Data Symbol (Binary) (b0 b1 b2 b3)	Chip Values (c0 c1 ... c30 c31)
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 1 0 0 0 0 0 0 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 1 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

After the meticulous alignment of symbol codes with their corresponding chip codes, the ensuing step involves subjecting these chip codes to an initial process of half-chord shaping. Subsequently, the signal undergoes modulation utilizing the sophisticated offset quadrature phase shift keying (OQPSK) technique. In this modulation method, the even-numbered chip codes within the sequence are harmoniously shifted to the same phase, while the odd chip codes experience a shift to the quadrature phase.

It is pertinent to note that the quadrature phase sampling point elegantly lags behind the in-phase counterpart due to the introduction of a displacement phasor, often referred to as an “Offset”. This displacement phasor aligns itself with a specific time slot, precisely a chip time slot. The intricacies of this relationship between in-phase and quadrature phases are visually depicted in Figure 5 [26,28].

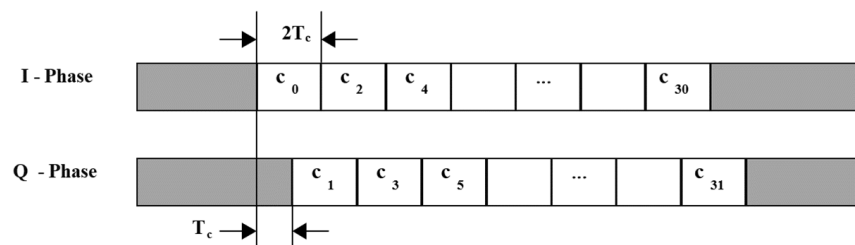


Figure 5. OQPSK chip offsets.

The half-sine wave shaping results from the $P(t)$ function relationship of each chip code value, as shown in Equation (4):

$$P(t) = \begin{cases} \sin(\pi \frac{t}{2T_c}), & 0 \leq t \leq 2T_c \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

The waveform after half-sine wave shaping is shown in Figure 6.

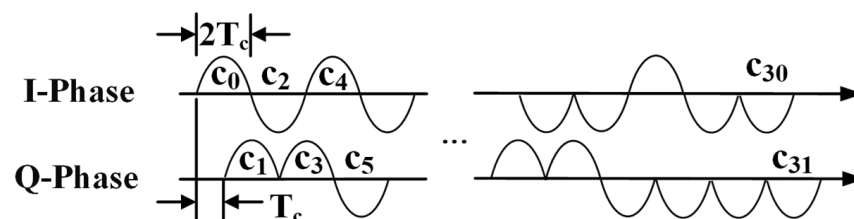


Figure 6. OQPSK of base-band frequency sampling impulse responded.

The modulation technique known as offset quadrature phase shift keying (OQPSK), enriched with the graceful addition of a half-sine wave, is often referred to as minimum shift keying (MSK). MSK stands as an exemplar of continuous phase frequency shift keying (CPFSK), and it is distinguished by its remarkable attribute of imposing a maximum frequency deviation precisely twice the transmission bit rate, rendering its modulation index a resplendent 2.

In the realm of MSK/OQPSK modulation, an elegant latency is meticulously introduced to the Q-phase signal relative to its counterpart, the I-phase signal, spanning a duration of T_b . This artful orchestration serves the noble purpose of effectively subduing the disconcerting phenomenon of a 180° phase crossover distortion within the modulated signal.

It is of utmost importance to acknowledge that MSK's waveform shaping gracefully mitigates the predicament of nonlinear distortion that can afflict the signal during the demanding demodulation process at the receiving terminus. To provide a visual representation of this, Figure 7 elegantly encapsulates the architectural essence of the MSK signal [27–29].

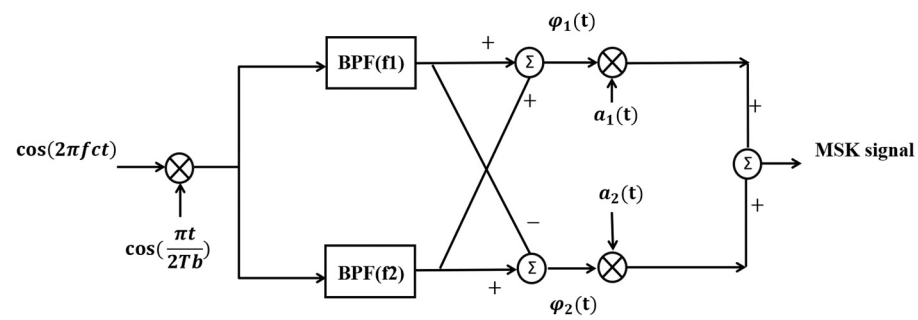


Figure 7. MSK signal architecture.

Minimum shift keying emerges as a refinement of the venerable quadrature phase shift keying (QPSK) modulation technology. While QPSK stands as an epitome of transmission efficiency, it grapples with an inherent quandary during signal transmission—a proclivity for zero-point crossings, leading to a diminishment in modulation energy and the unwelcome specter of signal discontinuity. This, in turn, necessitates a broader bandwidth, requiring the creation of an enhanced modulation technique, offset quadrature phase shift keying (OQPSK).

OQPSK, a pioneering innovation, adroitly tackles the conundrum of zero-point crossover distortion. Yet, its metamorphosis of the QPSK's matching circuit introduces a new intricacy: an intentional delay of the Q-phase by half a symbol. This artistic maneuver, while mitigating the previous distortion, births an unexpected challenge: an oscillation phenomenon at higher frequencies, which is a perilous dance with the very essence of signal synchronization.

In response to this enigmatic dance, MSK gracefully steps onto the stage, augmenting OQPSK with an elegant sine wave. MSK elegantly unfurls as a harmonious union of an I-phase cosine function wave and a Q-phase sine function wave. Their amplitudes unite in a symphonic convergence, steadfastly held at the sum of their squared counterparts (1), a numerical symphony that finds resonance in Zigbee's carrier transmission.

However, MSK, despite its refinement, still bears an Achilles' heel. Its alternating phases unfurl a spectrum that refuses concentration. Thus, the realm of modulation technology witnessed the ascent of gaussian minimum shift keying (GMSK), a celebrated maestro in the symphony of modern mobile communications.

In the realm of communication, GMSK orchestrates a harmonious resolve to the intricate dance of digital modulation's trifecta frequency, phase, and amplitude. It elegantly solves the conundrum of zero-point crossings, ushers in a world of continuous phase, retains an unwavering amplitude, and finally ushers the spectrum into a sublime concord.

In summation, the veracious conclusion unfurls: GMSK reigns supreme, eclipsing MSK, which in turn surpasses OQPSK, and finally, QPSK. The modulation factor of GMSK stands as the epitome of prowess. The intricate relationship between the 2.4 GHz frequency band's modulation and spread spectrum signal processing dances elegantly within the confines of Figure 8 [28,30,31].

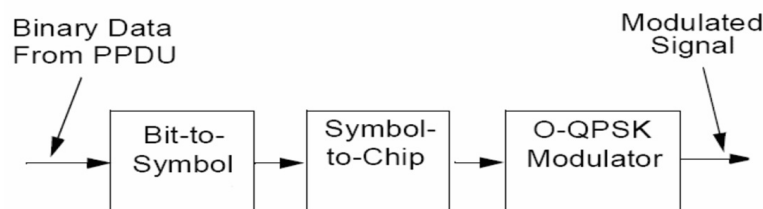


Figure 8. Modulation and spread spectrum signal process.

The employment of the IEEE 802.15.4 hopping application serves as a catalyst for its ubiquitous utilization in the realm of data modulation within communication modes. Behold, an illustrative diagram of hopping, adorned with the resplendent function of diversity reception, graces us in Figure 9.

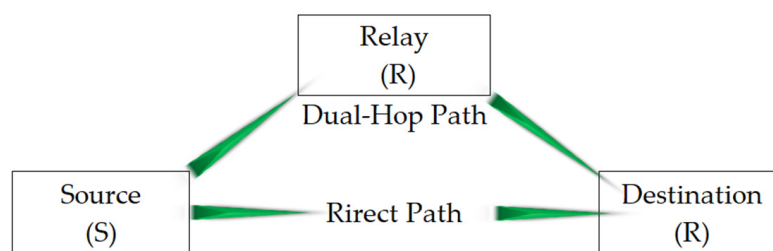


Figure 9. Schematic of hopping with diversity reception function.

Upon conducting signal simulation in MATLAB(MATLAB & Simulink), delivering the functionality in VHDL, and conducting circuit tests with Max Plus II, the incorporation of IEEE 802.15.4 hopping can be seamlessly integrated into the application sans detriment to transmission performance, thereby rendering the entire system more comprehensive.

3.2. IEEE 802.15.4 Hopping Design Method

3.2.1. TX Terminal

In the creation of a radio frequency communication system, it is imperative to encompass a transmitter, the transmitted signal, the wireless channel, and a receiver. The flow of the transmitter signal is depicted in Figure 10.

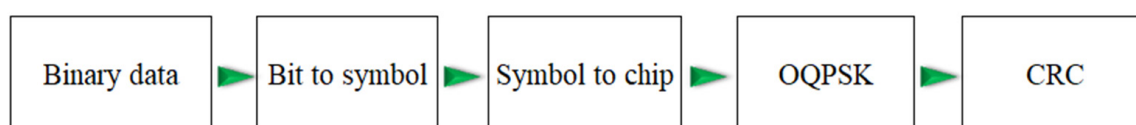


Figure 10. Transmitter signal flowchart.

To delineate the transitions from bit to symbol and symbol to chip, as well as the shifts from serial to parallel, we employed a meticulous analysis and juxtaposition. These two comparative methodologies served as the foundation for assembling the schematic illustrating the conversion from bit to chip elegantly depicted in Figure 11.

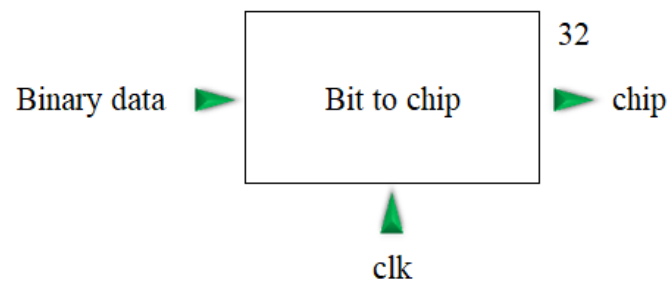


Figure 11. Bit to chip diagram.

Upon inputting a binary signal consisting of two bits for testing and subjecting it to a serial-to-parallel transformation, the acquired four bits are temporarily held in storage, yielding a corresponding 32-bit output. The outcomes are elegantly illustrated in Figure 12.

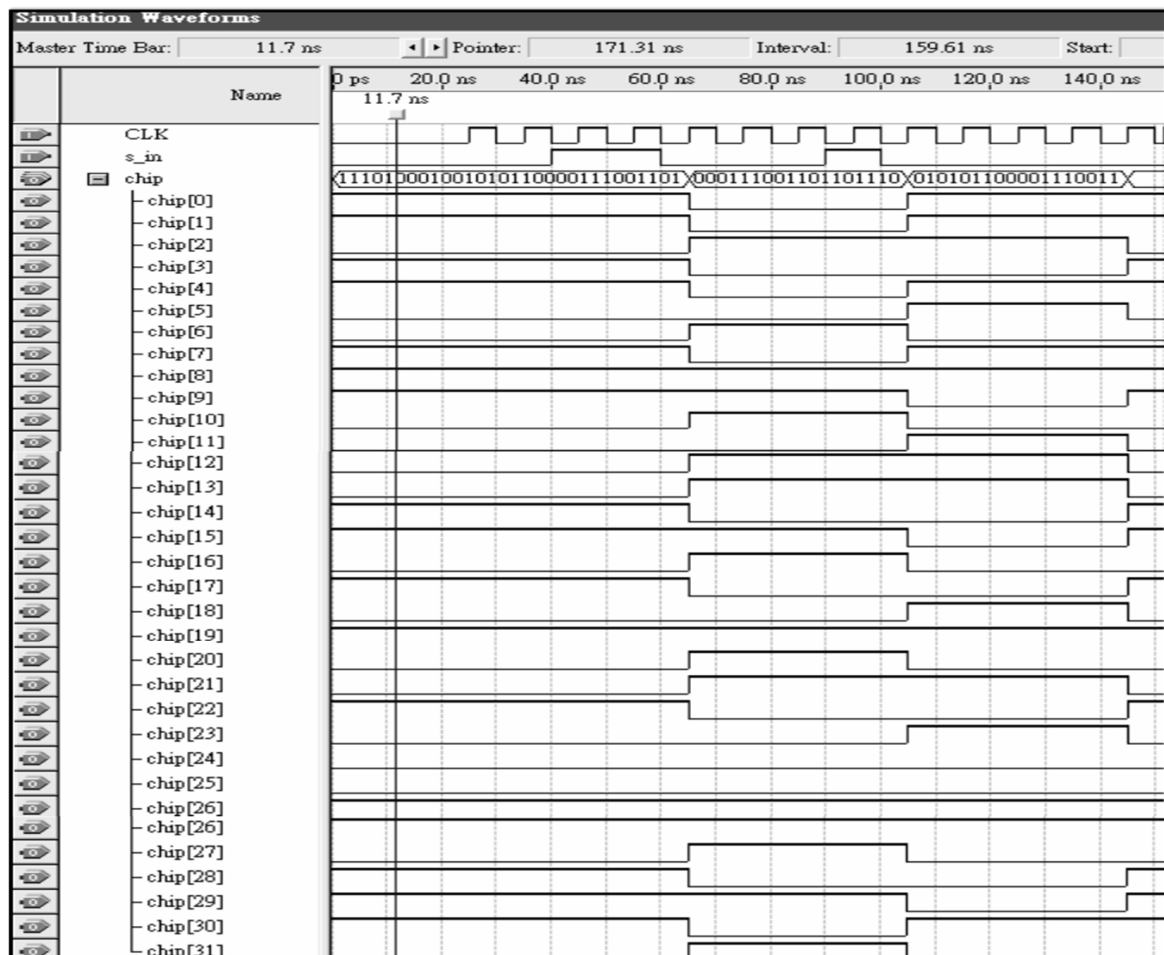


Figure 12. Bit-to-chip timing diagram.

In the segment dedicated to QPSK modulation, the existing 32-bit signal is partitioned into two distinct components: the I-phase and Q-phase. These components are elegantly depicted in Figure 13. The “b-up” represents the I-phase, composed of 16 bits of data, while the “b-down” represents the Q-phase, likewise consisting of 16 bits of data.

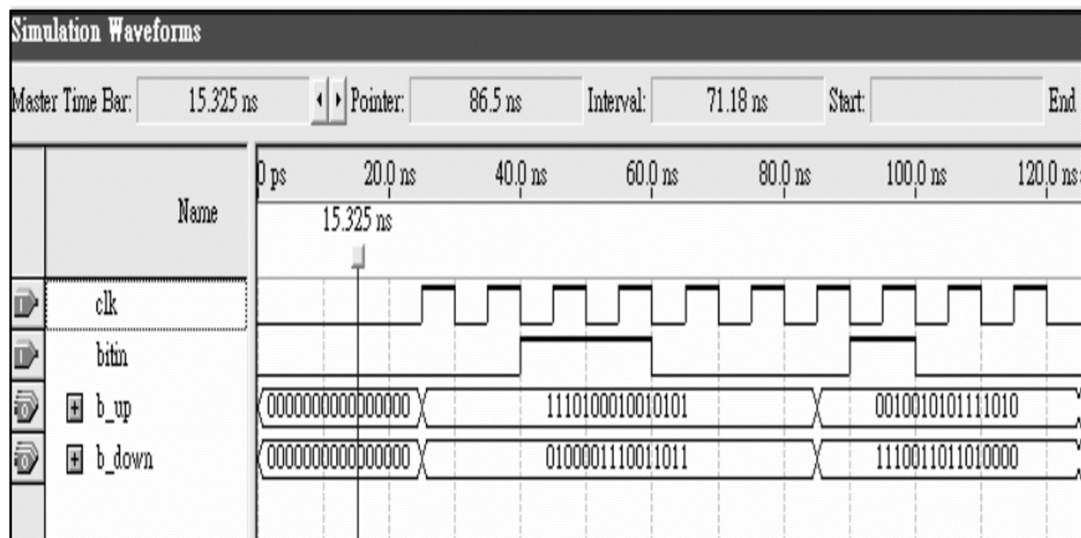


Figure 13. Distinguishing between I-phase and Q-phase.

Following the application of half-chord shaping, the even-numbered terms within both the I-phase and Q-phase are subjected to multiplication through a phase hysteresis of 180° , achieved through the application of a negative half-sine wave (0, -1 , 0).

The signal undergoes alterations due to environmental factors during the transmission process, thereby exerting an influence on the signal's reception at the recipient's end. Consequently, the bit error rate of the signal ascends significantly. As a remedy, a technical measure known as the Cyclic Redundancy Check (CRC) is introduced. This process hinges on polynomial division, chiefly aimed at yielding a value following the execution of CRC. It is computed both before and after transmission, with a subsequent comparison to discern the presence of any erroneous bits. The pertinent polynomial employed here is $G(x) = x^{16} + x^{12} + x^5 + 1$. The stepwise procedure is elegantly elucidated in the diagram depicted in Figure 14 [29,30].

CRC-16 Generator Polynomial : $G(x) = x^{16} + x^{12} + x^5 + 1$

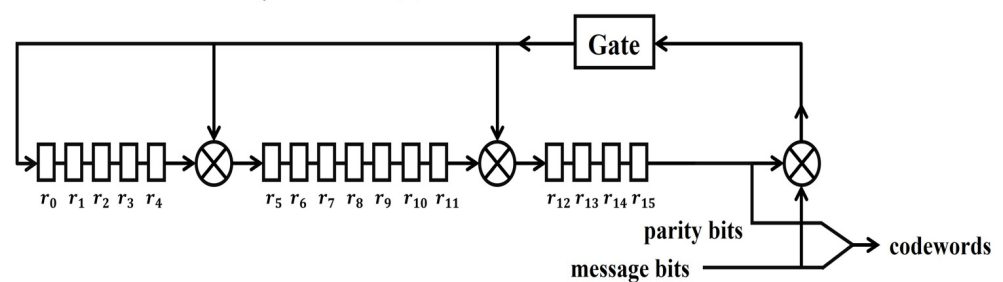


Figure 14. Polynomial division processing diagram.

A CRC-16 is created by differentiating between the I-phase and Q-phase. CRC-up and CRC-down shall each comprise 32 code words. To enhance the error correction capabilities, an error correction code is incorporated into the data volume. In reference to the CPLD code, Max Plus II is utilized for the computations, as elucidated by the outcomes presented in Figure 15.

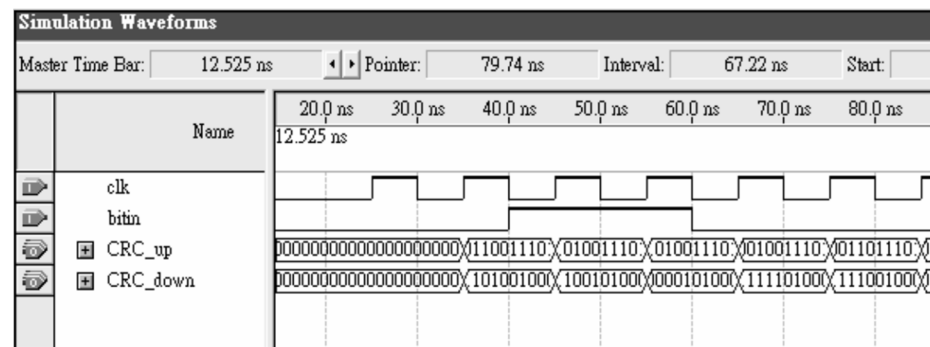


Figure 15. CRC-16 encoder calculation result.

3.2.2. RX Terminal

The operation of the receiver entails an inverse transposition process relative to that of the transmitter. The signal's progression is illustrated in Figure 16.



Figure 16. Receiver signal flowchart.

A Phase-Locked Loop (PLL) is employed to manage the synchronization aspect of the circuit, as depicted in the CRC-16 circuit block diagram illustrated in Figure 17 [30,31].

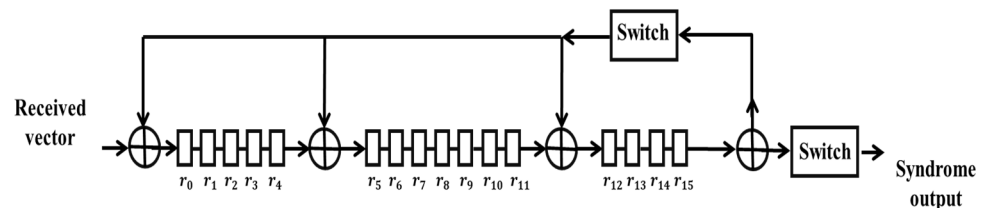


Figure 17. Polynomial division processing diagram.

The received I-phase and Q-phase signals undergo error correction testing. Subsequently, the data are meticulously restored to their original 16-bit forms. Following this restoration, the data can be subjected to half-sine wave shaping and OQPSK modulation, a technique akin to MSK modulation. A schematic for the MSK receiver is elegantly illustrated in Figure 18 [29,32,33].

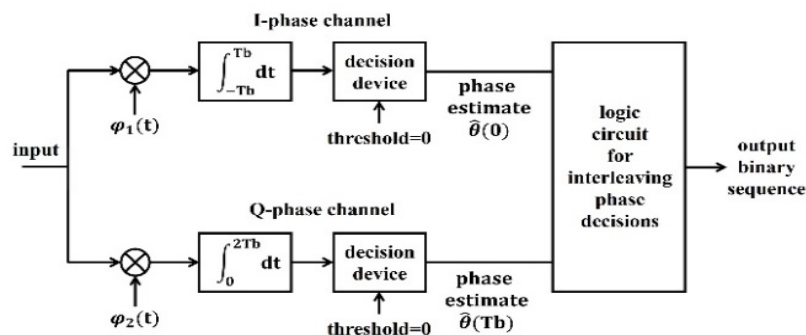


Figure 18. MSK receiver processing diagram.

Upon receiving the meticulously restored CRC-16 data, they are delicately fed into the OQPSK decision circuit for discernment. Following this, they are elegantly integrated into a 32-bit sequence of data, thus enabling the transition from chip to symbol. The waveform of this chip-to-symbol conversion is gracefully depicted in Figure 19 [34].

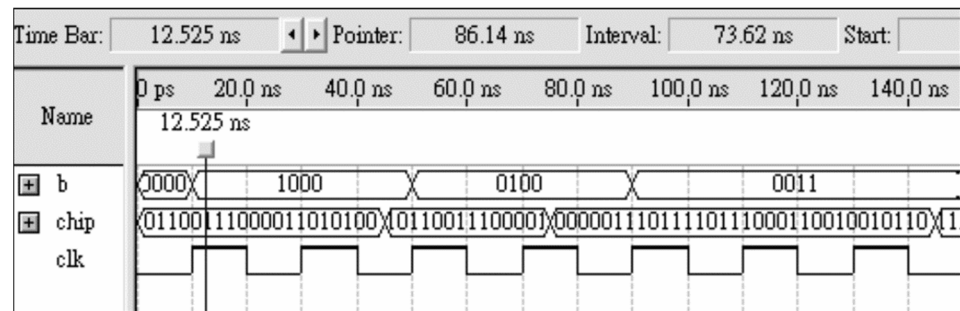


Figure 19. Chip-to-symbol timing diagram.

In accordance with the exposition of the aforementioned core technology [35], the pivotal aspects for integration into the comprehensive framework of the operational system encompass two fundamental elements:

- (1) The control apparatus for communication nodes.
- (2) The seamless incorporation of repeater units for advanced signal expansion.
- (3) The salient features encapsulated within these utilization directives are expounded as follows:
 - Possess a robust waterproof rating of IP67, designed for outdoor applications with inherent waterproofing.
 - Operate on an electrical supply ranging from AC 90 V to 220 V (non-waterproof), tailored for the purpose of linking with intelligent timepieces and the CHT mobile network.
 - Facilitate connectivity with a maximum of 32 intelligent timepieces.
 - Adhere to the Taiwan standard double-hole plug design (for outdoor use, paying meticulous attention to waterproofing is advised).

Establish seamless communication between the control apparatus for communication nodes (CNs) and smart meters within a range of less than 40 m, as elegantly illustrated in Figure 20.

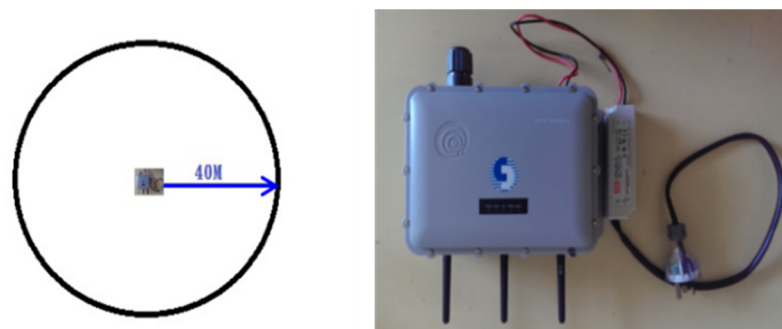


Figure 20. Communication node control device.

The repeater device has the following features:

- Possesses an impermeable IP67 rating, meticulously crafted for outdoor deployment, rendering it inherently waterproof.
- Operates on an electrical supply spanning AC 90 V to 220 V, with a design tailored for non-waterproof environments.
- Serves the noble purpose of extending the communication range between smart meters and a communication node control apparatus (it is imperative to note that this does not augment the capacity for smart meter connections).
- Adheres to the Taiwanese standard double-hole plug configuration (for outdoor usage, vigilance toward waterproofing is advised).

Ensures seamless communication, spanning over 40 m, from the communication node control apparatus to the smart meter, as elegantly depicted in Figure 21.

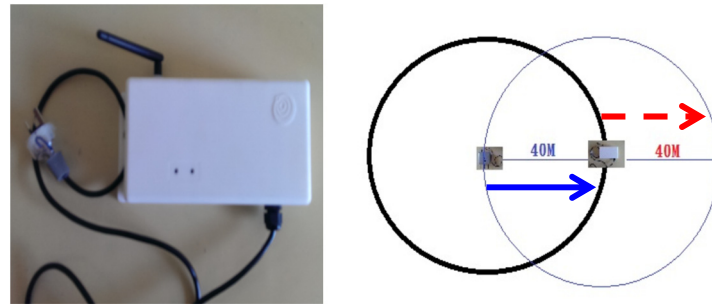


Figure 21. Repeater device.

The harmonious integration of these two apparatuses bestows upon the communication node control device a sphere of influence spanning 40 m from its epicenter. Within this expansive realm, it graciously accommodates all transmissions from the ensemble of smartwatch communication modules. Remarkably, each communication node control device wields the capacity to adroitly oversee as many as 32 smartwatches concurrently. Should the demand for control exceed this threshold, the judicious addition of supplementary communication node control devices is requisite.

Furthermore, in scenarios where the count of smart meters falls beneath the threshold of 32, yet the radius emanating from a communication node control device surpasses 50 m, the intervention of a repeater device becomes imperative. The primary function of this repeater device, once again, lies in the augmentation of service coverage, without any augmentation in the number of smart meter services provided.

4. Solution of Requirements and Inspection Methods

4.1. Open-Flow Proxy Construction

Based on software-defined wide area network (SD-WAN) technologies in accordance with the service requisites elucidated in Figure 22 of this investigation, an apparatus conforming to the SD-WAN OpenFlow standard [36–38] has been deployed. Its principal function resides in orchestrating the metamorphosis of a data exchange framework. Concretely, it engaged in the judicious parallel processing of traffic data, which, upon ingress into the data convergence table scheduling, is overseen by an SD-WAN controller [39] predicated on the functionality intrinsic to traffic features delineated in the Flow/Group/Meter Table. Following this, the data emanate from the converter and, guided by the scrutiny of pertinent form functionalities, discern the egress port of the data flow packet or the modality corresponding to the disposition.

Therefore, if traditional network infrastructure aspires toward SD-WAN optimization and OpenFlow protocol support, with absent alterations to the hardware framework, it becomes imperative to imbue the system software with functionalities pertinent to the data flow table (Flow/Group/Meter Table) and Packet-In. For instance, certain commercially available manufacturers of Wi-Fi access points or traditional switches may, through the incorporation of OpenWRT firmware or the integration of the open switch software suite, metamorphose into SDN-enabled switching devices supporting the OpenFlow protocol.

Within the domain of challenges and resolutions in SDN optimization for GPON networks, the ITU-T G.984.4/G.988 management standards delineate the ONT management control interface (OMCI) protocol. This specification elucidates services that can be initiated proactively through the GPON optical line terminal (OLT) through the OMCI protocol on the optical network unit (ONU), including the following:

1. The initiation and termination of GPON encapsulation method (GEM) connections between the OLT and ONU.
2. The configuration of VLAN settings for application services [40] and the management of a user network interface (UNI).
3. The compilation of performance statistics.

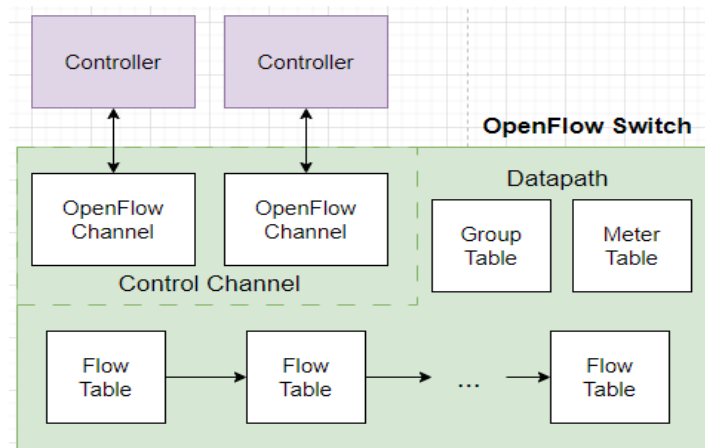


Figure 22. Architecture of the open-flow exchange function.

However, within the context of SD-WAN-related standards, a commensurate managerial approach is notably absent. Consequently, the integration of GPON into SD-WAN management necessitates the infusion of pertinent functionalities. Given that GPON OLT platforms often employ traditional switch chips lacking support for data flow tables and lack hardware backing for OpenFlow matching fields, the implementation of Packet-In and associated data flow tables on GPON OLT platforms mandates the routing of all packets entering the OLT system to the CPU on the OLT platform for processing. This approach imposes a substantial computational load on the CPU, resulting in a significant diminution of GPON transmission efficiency.

Thus, this strategic initiative deploys a groundbreaking AMI HWSN OpenFlow Proxy. This proxy seamlessly integrates traditional GPON devices into SD-WAN management without necessitating any alterations to the hardware architecture. Significantly, this framework obviates the need for additional modifications to the SD-WAN controller management module. It effortlessly virtualizes the conventional GPON network into an SD-WAN switch, readily subject to the governance of the SD-WAN controller. Consequently, the GPON network attains the advantages of heightened flexibility and emancipated management characteristic of SD-WAN networks. Moreover, it facilitates the extension of SD-WAN application services, such as network slicing, to the access network. Coupled with its compatibility with the SD-WAN OpenFlow switch architecture, this amalgamation collectively forms a virtual switch that is supportive of SD-WAN. Leveraging the SD-WAN switch, it achieves Packet-In event reporting and accommodates data flow table configurations, enabling a seamless integration of the GPON network system into SD-WAN controller management and assimilating the GPON network system into the realm of software-defined networking.

1. The OpenFlow Proxy module

This module operates as a socket daemon on the Linux operating system of the GPON OLT system. Its role is to facilitate the transmission of control commands between the SD-WAN controller and the OpenFlow switch. The primary functionalities include the following:

- Receiving and transmitting control messages between the OpenFlow switch and SD-WAN controller and modifying field data to ensure the accurate transmission of virtual ports messages to both the SD-WAN controller and the OpenFlow switch.

- Utilizing the OLT management API to convert the PON-Port status into a virtual port status and transmitting it to the SD-WAN controller.
- Handling statistics request control commands initiated by the controller. This acquires packet delivery data for virtual ports through the OLT management system, transmitting it back to the controller for calculations in management algorithms such as load balancing and QoS.

The design of the OpenFlow Proxy software module is primarily divided into three components, as shown in Figure 23. The control channel module, encompassing command parser and dispatcher functionalities, adheres to the specifications outlined in the OpenFlow specification. It processes the exchange of control messages as per OpenFlow ports, the OpenFlow control channel, and the OpenFlow switch protocol. Additionally, it rewrites pertinent message field data to achieve the virtualization of ONU ports.

1. The virtual port module

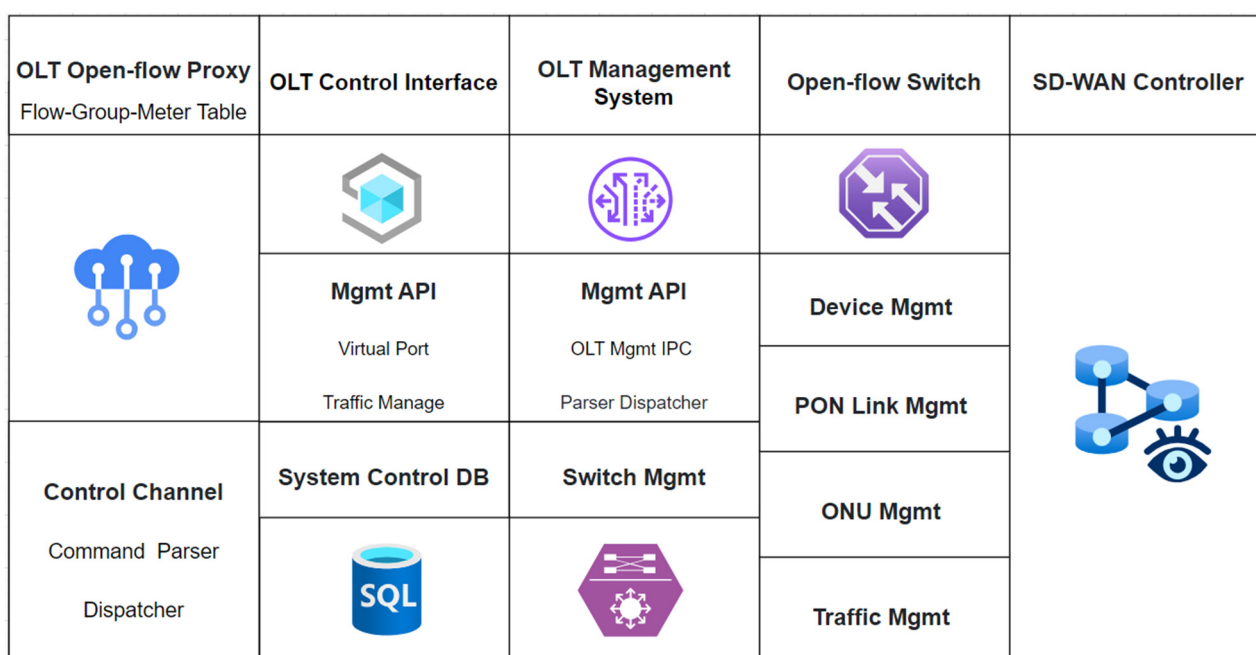


Figure 23. Flowchart of the GPON OLT OpenFlow proxy.

This module functions as an intermediary for communication within the database system. When the control channel module receives or necessitates the dispatch of control messages, this module adeptly translates and modifies port number field data, ensuring the precise alignment of ONU Ports with VLAN tags [41] to attain the desired effect of virtual ports.

Conversely, the traffic management module establishes communication with the ONU management API. Through instantaneous inter-module communication, it conveys the real-time connection statuses of virtual ports and facilitates pertinent management configurations within the GPON network.

The control channel module's paramount function lies in the maintenance and transmission of OpenFlow control messages. It deciphers packet control message types, invoking the corresponding management API for processing. Illustrated in Figure 24 the control channel operates with a status diagram delineating the connection between the switch and controller. Upon the initiation of the proxy, the connection status is denoted as Not Ready. At this juncture, the operating system kernel opens ports in readiness to receive connection initiation from the OpenFlow switch. Upon the receipt of the connection packet from the switch, the proxy, in turn, rewrites the destination field of the control message, forwarding it to the SD-WAN controller.

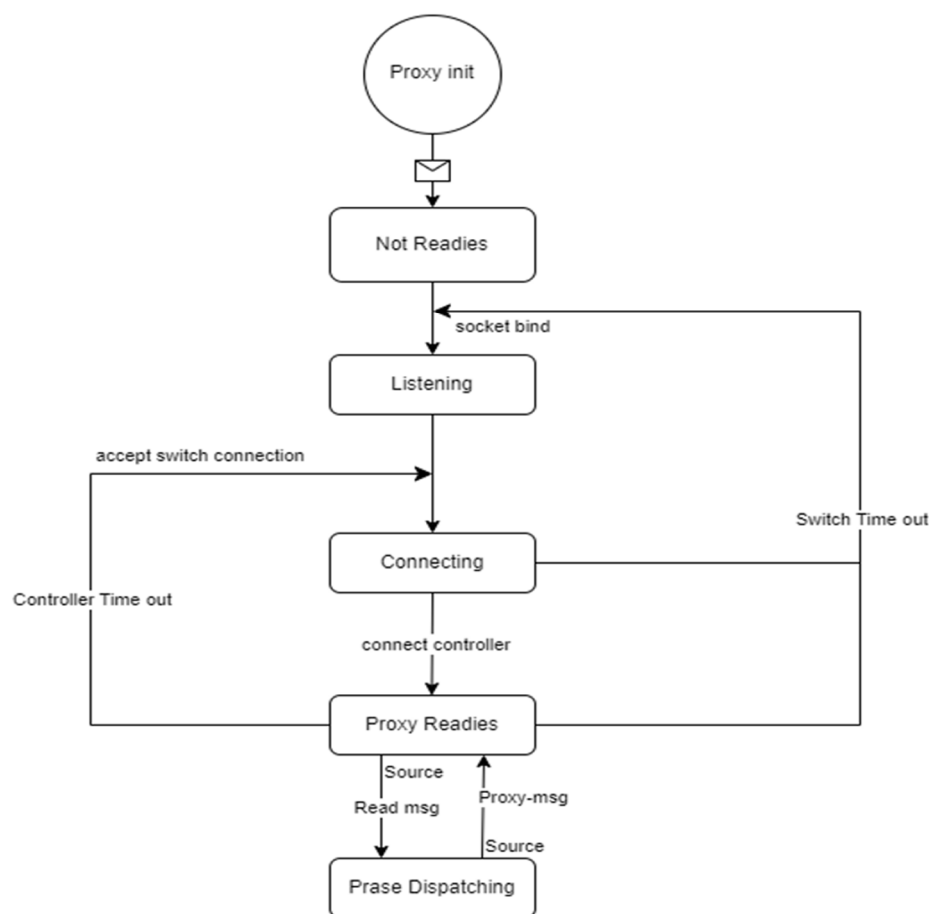


Figure 24. Status diagram of the control channel module.

Upon the completion of the exchange of OpenFlow messages, the module transitions into a state of proxy readiness. It initiates the discernment of control messages received through the port, parsing their types, effectuating processing, modifying field data, and subsequently dispatching the data message, thereby concluding a processing cycle.

2. Virtual port module

It is an aim of the GPON SD-WAN virtual switch to encapsulate each ONU as a port within a conventional switch, enabling the SD-WAN controller to perceive the GPON system as a singular OpenFlow switch under its aegis, without encroaching upon the functionality of the GPON. This module, in consonance with diverse control messages, adjusts the transmitted control message fields. It aligns virtual ports with the appropriate VLAN tags, facilitating the SD-WAN controller and OpenFlow switch to attain virtualization devoid of any requisite modifications, as delineated in Figure 25, a flowchart of the virtual port module.

Pursuant to the control messages delineated by the OpenFlow Protocol, the packet fields undergo individualized processing. Within the packets transmitted from the native OpenFlow Switch to the SD-WAN controller, the port number consistently designates the port linked to the GPON OLT, accompanied by the VLAN Tag stipulated by the OMCI specifications. In order to realize the aim of the GPON SDN virtual switch, this module revises the port number field in the packet to denote the virtual port number corresponding to the VLAN tag. This modification enables the SD-WAN controller to disregard this mechanism, perceiving the GPON as a customary OpenFlow switch, and furthermore, meticulous attention is dedicated to managing the port state control messages in the port modification- and multi-port-related OpenFlow instructions.

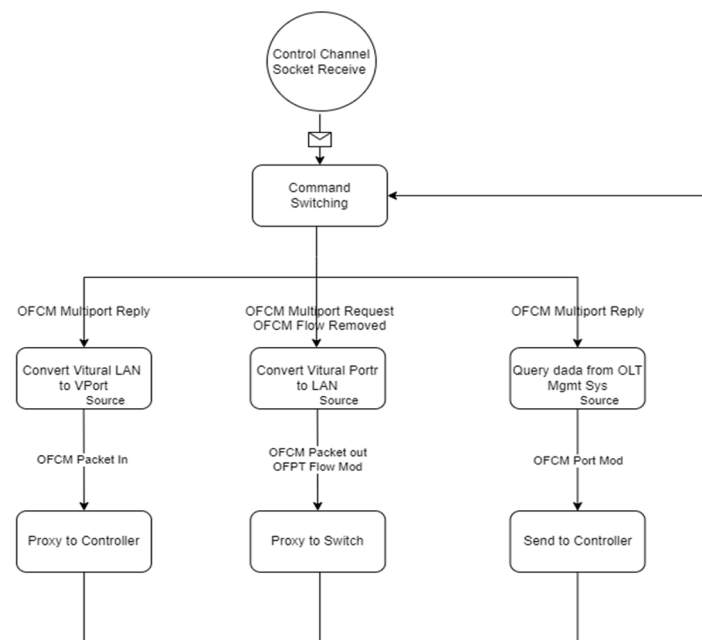


Figure 25. Flowchart of the virtual port module.

The ports established and interrogated through the SD-WAN controller should pertain to the tangible ports of the ONU. Consequently, an amendment is imperative to interrogate the pertinent configurations of the OMCI physical ports from the OLT management module, and the outcomes are relayed back to the SD-WAN controller.

3. Traffic Management Module

In the commencement of the GPON SD-WAN virtual switch, this module engages with the ONU Management API. It oversees the activation and disconnection statuses of ONU devices to disseminate OpenFlow port status messages. For ONUs that have concluded ranging, this module institutes a traffic channel, autonomously discerning a VLAN tag as the virtual port number. Furthermore, upon the receipt of signals indicating ONU deactivation or disablement, it relinquishes the VLAN tag. In Figure 26, the operational chronology processing of this module is delineated.

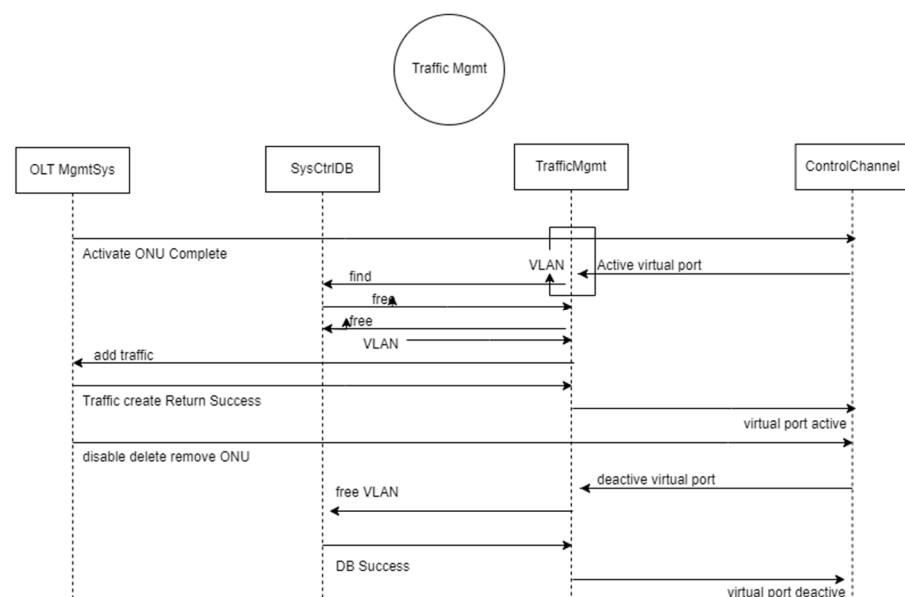


Figure 26. The operational chronology processing of traffic management.

The reception of notifications pertaining to alterations in ONU devices by the control channel management module invokes this module to undertake the governance of VLAN tags and the initiation of traffic channels. In practical terms, strict adherence to the GPON OLT and GPON ONU devices, in accordance with the ITU-T G.984 specifications, is meticulously upheld. The configuration and commencement of GPON OLT and GPON ONUs are orchestrated through the OLT network management system software. This expedites the provisioning of GPON network services, as illustrated in Figure 27.

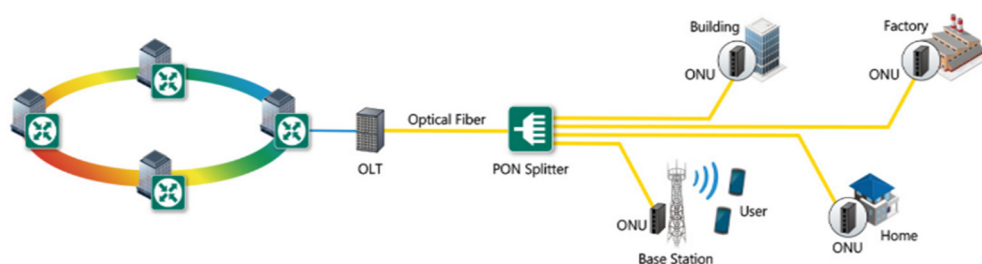


Figure 27. Passive optical LAN.

Following the execution of the OpenFlow proxy, it accommodates connections from the pre-established OpenFlow switch. In consonance with the exposition in Section 4.1, pertinent data fields undergo modification, and the refined information is transmitted to the SD-WAN controller. Subsequently, upon the ONU completing registration with the OLT, the configuration for VLAN is consummated, establishing the GEM connection. Concurrently, port status control messages are dispatched to the SD-WAN controller, apprising it of the commencement of the virtual port activation.

Upon the advent of the packet, initially transmitted from the ONU side and arriving at the OpenFlow switch, the OpenFlow proxy, harnessing the VLAN tag within the L2 packet header, transmutes the source port in the packet in control command to the virtual port number of the GPON virtual switch.

It then conveys this directive to the SD-WAN controller to facilitate the packet in control command for the GPON virtual switch. Likewise, as the algorithms of the SD-WAN controller discern routing rules, the proxy can transfigure the virtual port number in the data flow entry into a physical port number that the OpenFlow switch can adeptly manage.

It judiciously appends the accurate VLAN tag, crafting a data flow in accordance with the GPON virtual switch. Through the choreography of port status, Packet-In, and flow entry, the entire GPON network system seamlessly integrates into the purview of SD-WAN controller management, thereby exerting control over the transmission or disposition of packets within the GPON network.

4.2. Microservice of the Open-Flow Proxy Service Construction

In the realm of ZigBee-based IoT service applications, as alluded to earlier, a novel advanced metering infrastructure architecture, rooted in the Smart Liquid Natural Gas (LNG) Management System for heterogeneous wireless sensor networks (HWSNs), shall be employed. Employing software defined wide area network (SD-WAN) technology [42,43] within a centralized management and control architecture, it aggregates ZigBee information. Despite being a wireless network protocol tailored for low-speed and short-distance transmissions, it exhibits the attributes of “subdued velocity and diminished power consumption”, as elucidated in Figure 28.

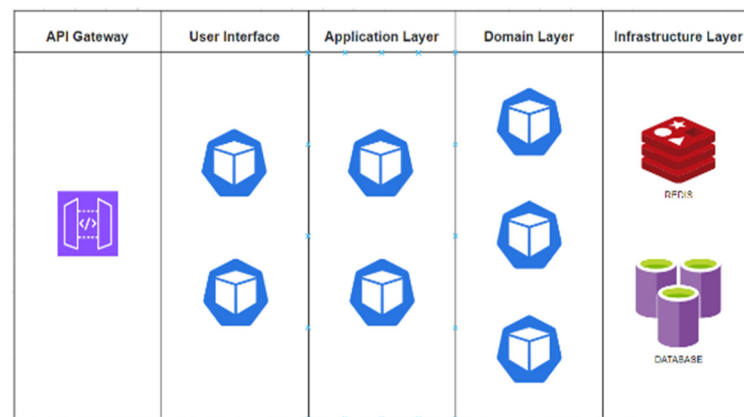


Figure 28. Microservice architecture.

The utilization of the OpenFlow proxy microservice architecture predominantly contemplates the previously mentioned scenario of information acquisition and the sudden deluge of voluminous data.

Employing the microservice architecture confers the following advantages:

- **Autonomy:** The service scale being relatively modest permits autonomous deployment and individual updates for each service.
- **Elevated Scalability:** Services can undergo dynamic horizontal expansion based on hardware resources, service status, and similar metrics.
- **Pliability in Development and Maintenance:** The minimized scale of the service facilitates a clear understanding of the code base by team members, enabling swift contributions.

As services embrace miniaturization, it has evolved into a norm in the software industry to directly furnish APIs from services with diverse attributes, thereby precipitating concerns about API security and management.

1. API gateway controller

In alignment with the peculiarities of the Internet of Things (IoT), the operational convergence process of IoT may herald an instantaneous deluge of copious data. Consequently, the architectural design of the service must retain a degree of flexibility. The architectural design adopts the OpenFlow proxy microservices paradigm, complemented by an API gateway controller management module serving as the external communication conduit for the service, as delineated in Figure 29.

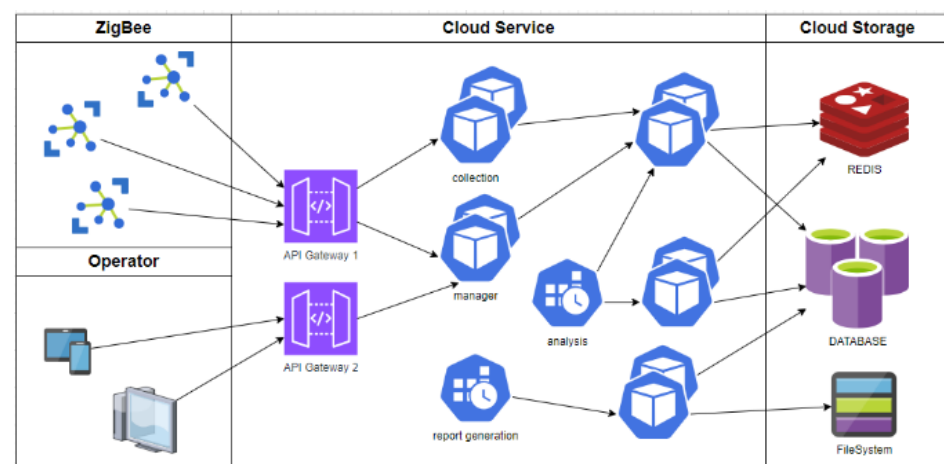


Figure 29. Paired API gateway controller management module.

While the API gateway possesses the capability to oversee diverse services, we posit that the fundamental nature of service types delineates a distinction, notably between data collection and service management. Hence, in effecting segregation within the API gateway controller, each API gateway assumes its own sphere of responsibility.

API Gateway 1: Tasked with the compilation of ZigBee CN data. Beyond the orchestration of APIs, API gateway 1 is endowed with the capacity to monitor service magnitude.

API Gateway 2: Facilitates administration through mobile devices or computers. This form of administration encompasses platform oversight, data scrutiny, and the discernment of ZigBee endpoints' device statuses, among other facets.

The utilization of the API gateway proxy-based solution for a service segregation design has been undertaken, allowing a heightened flexibility for data collection and unfettered service management to operate through distinct channels. Moreover, this facilitates the extension of network slicing and additional SD-WAN application services to the access network, thereby ensuring the preservation of fundamental information security for the service.

2. Digital twin smart AI

In addition to the antecedently enumerated merits of “autonomy, elevated scalability, facile development, and maintenance”, the selection of a microservices framework assumes paramount significance. As a global M2M connectivity (G-M2MC) application service platform, greater accentuation is laid upon service steadfastness. The contemporary cloud computing capacities proffered by diverse public clouds empower the deployment of services in both private and public cloud domains. Leveraging Apigee to construct the computational prowess of the hybrid cloud ensures uninterrupted operation and fortifies the network resilience of the platform, seamlessly transitioning service control to the public cloud in the event of anomalies encountered by the private cloud.

This inquiry is grounded upon a hybrid cloud service architecture meticulously fashioned for platform resilience, as elucidated in Figure 30. In employing the functionalities inherent to Apigee, the integration of public and private clouds is orchestrated in a heterogeneous manner, with the Storage Sync mechanism employed to harmonize data on the backend.

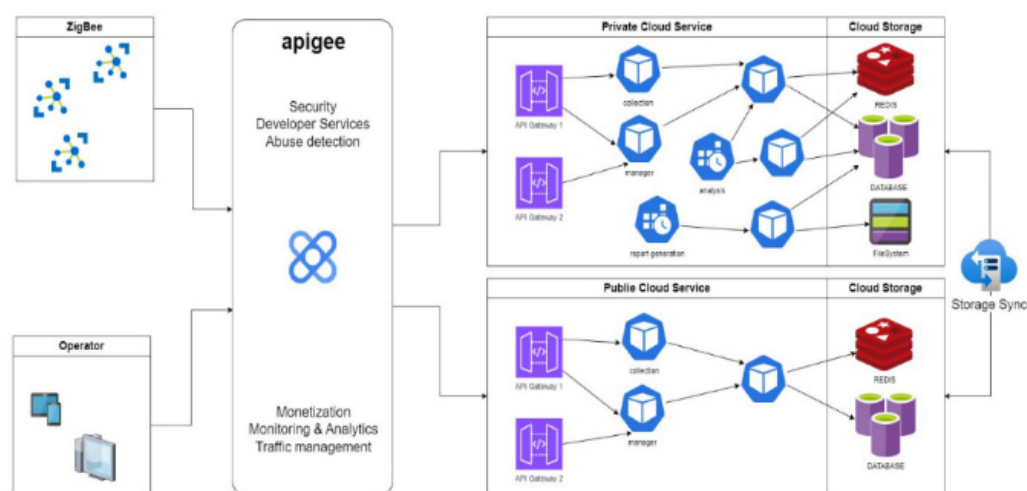


Figure 30. Hybrid SD-WAN cloud service of the G-M2MC architecture.

Moreover, service components of the API type may be deployed in the public cloud in accordance with the exigencies of actual services, while components governing the control and management of a batch nature are upheld within the confines of the private cloud. The service architecture is amenable to realization in the form of either Active-Active or Active-Standby. The former augments service capacity, whereas the latter curtails service

expenditures. Regardless of the methodology employed, both serve to fortify the resilience of the platform.

4.3. Active Defense Mechanism Enhances Broadband Network Resilience

In employing a backup mechanism primarily reliant on asynchronous orbit satellites, the distinct characteristics and maturity differentials of asynchronous orbit satellite domains pose significant challenges in selecting defensive and combat methodologies. In more mature domains, implementation is directed toward ground-based stations and user terminals:

- Detection: The implementation of malicious file analysis, network traffic analysis, user behavior analysis, and platform monitoring to identify potential malicious threats within low Earth orbit satellite domains.
- Isolation: Implementing program isolation measures, executable whitelists, blacklists, etc., to develop zero-trust mechanism scenarios suitable for asynchronous orbit satellite domains.

Furthermore, critical service servers are redundantly backed up to the cloud. Through satellite communication coupled with heterogeneous network connections to the international cloud 5G core network, significant changes and innovations have been brought to communication. The deployment of threats and vulnerabilities in the 5G cloud infrastructure also presents substantial challenges, such as malicious network actors successfully exploiting vulnerabilities to gain initial access to the 5G cloud system or launching attacks against individual cloud resources, triggering a chain reaction affecting the entire international cloud 5G core network. Distributed denial-of-service (DDoS) attack incidents, among others, are security concerns that need to be considered in the development of satellite communication networks and the deployment of international cloud 5G core network system architectures, ensuring, in extreme scenarios, that the transmission of our country's critical information is not compromised or leaked.

Traditional passive cybersecurity monitoring and management measures in predefined environments and application domains are insufficient to address the threats of high-speed network environments with seamless integration across land, sea, and air networks. This paper will pivot toward proactive cybersecurity defense practices, constraining damage within manageable limits. This study implemented a zero-trust data protection mechanism in the cloud network space to strengthen the delineation of trust and responsibility boundaries, protect information and data security at the source, progressively develop widely accepted network resilience frameworks, and advance the realization of digital resilience goals, thereby fortifying our country's digital resilience.

1. Asynchronous Orbit Satellite Cybersecurity Architecture

Wireless signal user threats refer to signals being subject to eavesdropping attacks, signal injection attacks, and signal spoofing during transmission by third parties. Ground system threats refer to satellite software and hardware typically adhering to an open-trust model, wherein ground stations are trusted by all equipment on the space station. The satellite ground station acts as a crucial bridge between the primary terrestrial network and the satellite, susceptible to hardware backdoors and physical access risks. Space platform threats encompass situations where sensor and RF system data are inadequately handled, or where there are hardware vulnerabilities in ground stations, making them susceptible to DDoS attacks, hardware backdoors, or malicious program attacks [44,45], as depicted in Figure 31.

To ensure the redundancy of critical service servers, they are backed up through satellite communication combined with heterogeneous network connections to the international cloud 5G core network, bringing about changes and innovations in communication. The threats and vulnerabilities in the deployment of the 5G cloud infrastructure also face significant challenges. Instances such as malicious network actors successfully exploiting vulnerabilities to gain initial access to the 5G cloud system or launching attacks against

individual cloud resources, thereby affecting the entire international cloud 5G core network, and DDoS attack events, are all security concerns that need consideration in the development of satellite communication networks and the deployment of international cloud 5G core network system architectures. This ensures that, in extreme scenarios, our country's critical information transmission is not compromised or leaked.

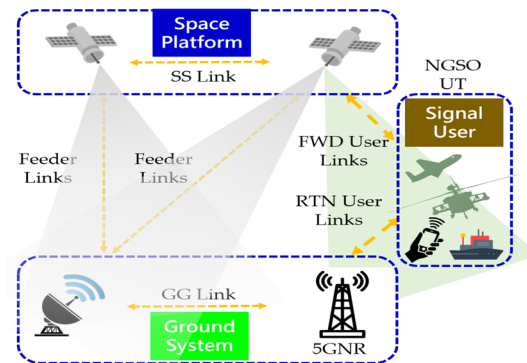


Figure 31. Satellite architecture threat diagram.

Traditional passive cybersecurity monitoring and management measures within pre-defined environments and application domains will prove inadequate in addressing the threats of high-speed network environments with seamless integration across land, sea, and air networks. Therefore, the proactive cybersecurity defense approach will be implemented, limiting damage within controllable limits. The subsequent focus will be on the active cybersecurity defense endpoint detection and response mechanism endpoint detection and response (EDR) for detailed explanations [46,47].

Through the deployment of the EDR mechanism, its primary function is to enhance the security of endpoint devices by continuously monitoring, detecting, and responding, safeguarding an organization's information and systems from various threats and attacks.

Furthermore, it aims to strengthen the resilience of a multi-broadband network backup architecture, introducing the cybersecurity technology institute—endpoint detection and response (CSTI-EDR) mechanism [48,49] into the 5G core network of satellite ground receiving stations for log containment and analysis. The primary objective is to enhance the security of the 5G core network and promptly detect and respond to potential cybersecurity risks, ensuring the stable operation of communication infrastructure and protecting critical data.

The introduction of EDR into the ground receiving station's 5G core network encompasses four main aspects:

- **Enhancing the Security of the 5G Core Network:** The 5G core network supports various critical applications, including the Internet of Things (IoT) and critical infrastructure. The implementation of EDR can help detect and block abnormal activities on endpoint systems that may pose threats to the 5G core network, thereby enhancing the overall security of the 5G core network.
- **Early Detection of Hacker Activities:** EDR solutions can monitor activities on endpoint devices and identify potential signs of attacks. This helps in the early detection of hacker activities, including unknown and novel attack methods, and allows for immediate measures to counter these attacks.
- **Rapid Response and Recovery:** When EDR detects abnormal activities, it can swiftly take corresponding mitigation measures, such as isolating infected devices to reduce the spread of damage and restoring affected systems when necessary. This helps reduce the damage and downtime caused by attacks.

- **Strengthening Overall Network Security:** The 5G core network is a complex network that includes many different components and access points. The introduction of EDR can provide more comprehensive security monitoring, including monitoring the core network and edge devices, to reduce the overall network cybersecurity risks.
2. **Implementation of Active Cybersecurity Measures for Asynchronous Orbit Satellites**

The establishment of the architecture in the asynchronous orbit experimental field includes the relevant setup and preliminary testing of internal log containment within the 5G core network. The contents encompass the establishment of log containment/forwarding mechanisms and the reinforcement of data transmission channel security, as depicted in Figure 32.

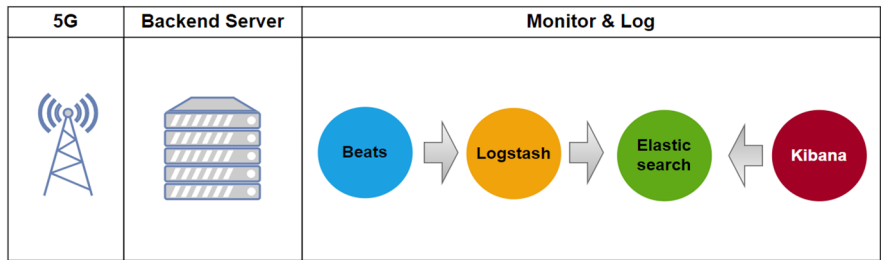


Figure 32. Operational flowchart for satellite—5GC NR log containment.

The endpoint detection and response mechanism (EDR), employing AI and intelligence analysis integration technology, detects abnormal behaviors and processes at endpoints. It gathers and automatically analyzes digital evidence with threat indicators, additionally referencing the MITRE ATT&CK framework proposed by the U.S. non-profit organization MITRE [48,50]. For each stage of the attack, MITRE collects the techniques and tools used by attackers. Referring to known threat patterns, it executes risk assessments, visualizes threats and risks, reports to the cybersecurity management team, and issues alerts.

The deployment of the EDR mechanism in the 5G core network of satellite ground receiving stations for log containment and analysis is illustrated in Figure 33. Corresponding with cybersecurity frameworks such as MITRE ATT&CK, D3FEND [51,52], as well as relevant guidelines and recommendations, it develops anomaly and attack behavior detection to uncover potential attack patterns. This involves the analysis of network architecture threat vulnerabilities and attack contexts, contributing to the development of proactive defense strategies and solutions.

(1). 5G NR

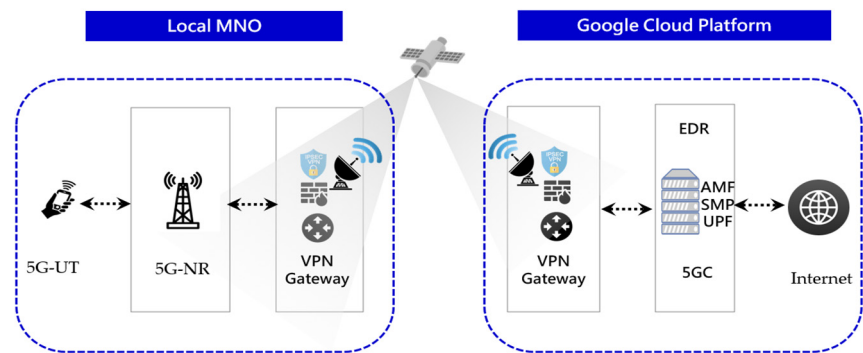


Figure 33. Illustration of EDR deployment in 5G core network.

The 5G core network commercial product developed by free 5G core network, an open-source architecture for the 5G core network, served as the experimental field for this study. The 5G core network complies with the specifications of 3GPP R15/R16, defining

the 5G core network as a decomposable network architecture aimed at introducing the concept of control and user interface separation. Its architecture is illustrated in Figure 34.

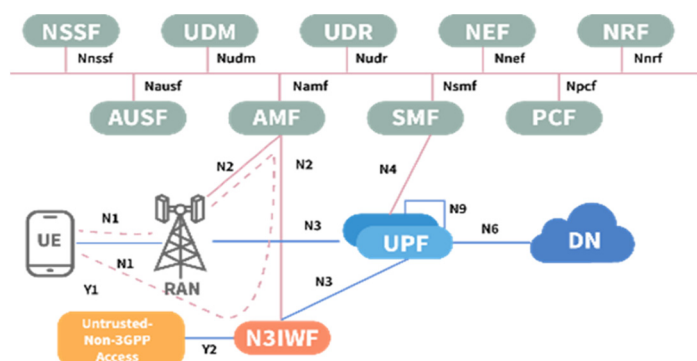


Figure 34. The log forwarding process.

Among these components, the network slice selection function (NSSF) selects suitable network slices through network slice selection assistance information (NSSAI) provided by user equipment (UE). Unified data management (UDM) is responsible for user data management, storage, and configuration. The policy control function (PCF) provides network policies for all control plane functions. The unified data repository (UDR) serves as a unified data storage for UDM and PCF. The network exposure function (NEF) manages external open data access interfaces. The network repository function (NRF) handles functions such as registration, management, and status detection for the NEF. The authentication server function (AUSF) authenticates UE access. The user plane function (UPF) manages user packet routing and forwarding, interactions with the data network (DN), quality of service (QoS) processing for the user plane, and traffic control implementation. The access and mobility management function (AMF) provides authentication and authorization for user access. The session management function (SMF) is responsible for call channel maintenance, IP allocation management, and UPF selection.

Additionally, in the context of the DN, composed of interconnected devices and systems for transmitting and exchanging data in communications, the UPF of the core network supports data routing, forwarding, inspection, and QoS. It serves as an external packet data unit (PDU) node interconnecting with the DN and acts as an anchor for intra- and inter-radio access technology (Inter-RAT) mobility.

The control interface of the core network employs a service-oriented architecture design principle. Different control interface network units provide various network function services through API services. This architectural design allows the core network to support multiple network function services and provides flexible integration and reconstruction capabilities. Through standardized interfaces, it enhances the flexibility and openness of the core network.

(2). Log Containment

The purpose of log containment is to record and trace critical events, errors, and network activities to assist network administrators in troubleshooting and network maintenance. When system issues or errors occur, log records can provide detailed messages about the occurrence of errors, helping to identify and resolve issues, thereby improving network availability and performance. Additionally, log containment can record security events, attack attempts, and potential vulnerabilities to detect and track potential security risks, safeguarding user networks from attack threats and enhancing network security.

The Linux rsyslog is employed to collect log messages from 5G core network base stations. Rsyslog, an enhanced version of syslogd, is used to receive, process, and forward log messages from the same host or other hosts. Messages are sent to local or remote log files, files, or other types of storage devices, with its primary format [48,53] shown in Table 5.

Table 5. Primary format of rsyslog.

Name	Type	Description
Tag	str	Event log
Priority	int	Priority: Facility $\times$ 8 + Severity
Time	date	Incident time
Host	str	The source host that sends syslog messages
Ident	str	Identify the device or application that generated the message
Pid	int	Process name: often used to analyze the continuity of the log generation process but does not guarantee reliability
message	str	The complete content of the event

Note all activities of the host, including logins, operational commands, process invocations, etc. The primary collected contents are shown [54,55] in Table 6.

Table 6. Rsyslog log collection source table.

Facility	Description
kernel messages (kern)	Most of the messages generated by the system core involve hardware detection and core function activation.
user-level messages (user)	Information generated at the user level, such as the user uses the logger command to record the function of the login file
mail system (mail)	Email sending and receiving
system daemons (daemons)	System daemon or service related, such as system-related information
security/authorization messages (auth)	Login authorization related, such as login, ssh, and su
messages generated internally by syslog (syslog)	Information generated by syslog related protocols; information generated by the rsyslogs program itself
LINE printer subsystem (lpr)	Print related
network news subsystem (news)	Newsgroup server related
UUCP subsystem (uucp)	Unix to Unix Copy Protocol, used in the early days to exchange program data between Unix systems
clock daemon (cron)	Routine work schedule
security/authorization messages (authpriv)	Similar to auth, but records more private account information, including the operation of the pam module
FTP daemon (ftp)	FTP communication protocol related

Information is gathered from different dimensions to enhance data reliability and traceability. For example, in the auth log, suspicious account logins are detected, and in the daemon log, malicious command operations are observed.

(3). Log Forwarding

Well-contained logs are forwarded, with the purpose of uniformly formatting the collected log data and then transmitting it to a centralized log system or storage location. This facilitates centralized management, analysis, and processing, making log data more accessible and searchable. Simultaneously, it achieves the comprehensive monitoring and management of the entire network.

The log forwarding process, as depicted in Figure 35, involves treating rsyslog logs as input, parsing their format into structured data through a parser, filtering targeted data, modifying, and adding, using a cache for buffering during file processing, and providing a unified and persistent mechanism for data storage. Routing identifies data labels and content matches to determine where this data should be output. Finally, logs are output to a database, network service, or local storage repository.

(4). Log Streaming

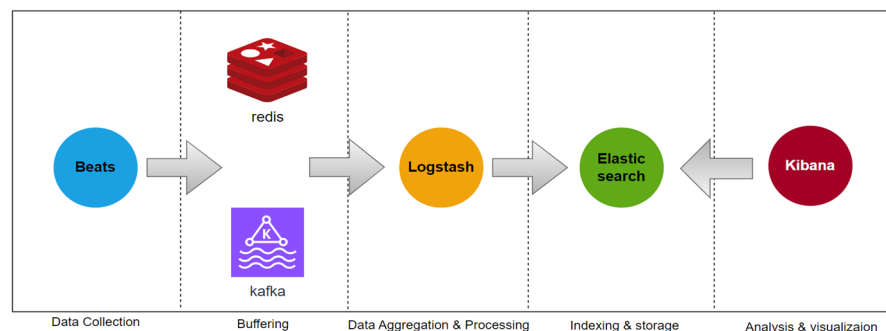


Figure 35. Log forwarding process flowchart.

For logs in the asynchronous satellite network, there may be thousands of log information records per second. When dealing with a large amount of data, it can lead to system overload. Therefore, through asynchronous processing, some time-consuming operations are changed to asynchronous processing to release system resources and enhance system parallel processing capabilities. The message queue provides a centralized queue, allowing senders to place messages in the queue, and receivers to retrieve and process messages from the queue. This architecture enables asynchronous processing, where there is no need for real-time communication between senders and receivers. It allows receivers to retrieve an appropriate number of messages based on their own resources and computing power for processing, ensuring increases in data flow and data integrity, as shown in Figure 36.

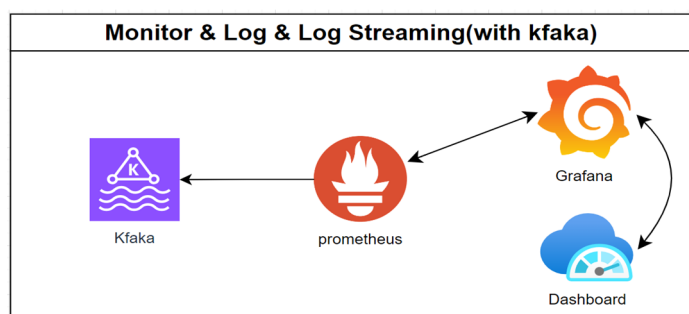


Figure 36. Message queue illustration.

Furthermore, the message queue can implement log streaming, distributing the same log content to different storage devices, such as databases, local or cloud, to achieve redundant storage. This approach allows storing copies of data in multiple locations or systems, reducing the risk of loss due to damage to a single location or system, ensuring data reliability, integrity, and availability.

5. Solution of the Design and Testing

5.1. Positioning and Construction

Real Case 1. Design and Network Architecture of Smart Town.

1. Mandates of coverage and methodologies of scrutiny.

The orchestration of wireless mesh networks typically entails two schemata. One involves the positioning of nodes, the frequency channels allocated to the transceivers mounted on these nodes, the count of transceivers dedicated to inter-node communication, and the routers shouldering the gateway role. Concurrently, an alternative deployment methodology permits nodes to autonomously configure a wireless mesh network. These nodes possess the capability to discern the existence of a wireless mesh network in

their proximity, configure settings automatically, and seamlessly integrate into the wireless network. The evaluation of wireless network deployment necessitates scrutiny on two fronts [56,57].

➤ Channel allocation

When optimizing, network throughput stands as a paramount consideration in the wireless network; a node can be equipped with multiple transceivers. ZigBee devices strategically delineate 16 available channels within the frequency spectrum of 2400–2483.5 MHz, employing four-phase modulation direct-sequence spread spectrum technology.

Within a multi-channel milieu, a node can adopt two techniques to exploit multi-channel technology as follows:

- Equip a node with several wireless transceivers, each operating on a channel distinct from the others.
- Employ a solitary wireless transceiver on a node that dynamically switches between different channels.

The subsequent elucidation delves into two divergent paradigms in reference to planning.

○ Load-aware channel allocation

A centralized algorithm for channel allocation endeavors to fulfill the network traffic demands of each link, allocating channels based on the anticipated load of each link. The connection's capacity hinges on the channel allocation algorithm [58], dictating how the path is determined. The initial capacity of a connection is computed by dividing the total aggregated channel capacity of the two nodes by the number of other connections within the interference range of the two nodes.

Each channel is assumed to operate at 250 kbps in two nodes, with a planned availability of four channels, yielding a total channel capacity of 1000 kbps. If within the radio frequency range of the two nodes, there exist six other links, the initial capacity for the two nodes is calculated as $1000/6$ kbps. Channels are allocated based on the acquired expected load and the number of transceivers on each node, ensuring that the available channels on each link are at least commensurate with the anticipated load.

In this process, introducing a parameter founded on the “degree of interference” implies that the interference range between the two nodes falls within the interference range. If the channel assigned to the link and the channel to be assigned to the link together encompass the total expected load, then, in two nodes with three planned channels, five interference degree values are calculated, and the channel with the lowest interference degree is selected and allocated to the two nodes.

If both nodes have received designated channels, prior to data transmission, a check is conducted to ascertain the existence of a common channel. Subsequently, a channel with minimal interference between the two nodes is identified for use.

○ Channel assignments

In the aforementioned method of channel allocation, to ensure the preservation of the network topology, if the transceivers of two nodes operate on different channels, universality between the two points is forfeited. Hence, a channel allocation method is proposed for connection maintenance, ensuring that the shortest path between any two points in the network remains unaltered post channel allocation.

Each node is assigned an initial priority order in a fixed topology, alongside a priority order in a fixed path. The algorithm sequentially assigns the sending and receiving methods to each node device. When all transceivers of a node have been allocated, the priority is elevated to its maximum, as depicted in Figure 37.

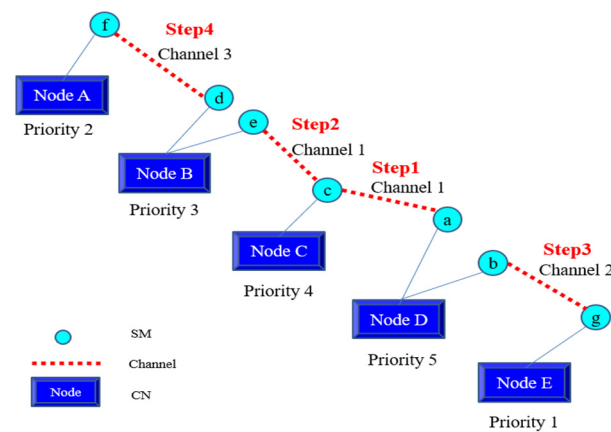


Figure 37. Topology connection maintains channel allocation.

Assume that node A to node E is assigned random priority values ranging from 1 to 5, with node D holding the highest priority. After detecting interference values, the transceiver of node D utilizes channel 1 to connect with node C. Post connection completion, with remaining unconnected transceivers, the connection is passed to the next one with the highest weight without entirely sacrificing flexibility. At this juncture, the c transceiver in node C has used only channel 1, so in Step 2, channel 1 is also employed to connect with the e transceiver in node B. Node B, having lost its elasticity entirely, sees the highest-weighted connection returned to node D, connecting with the g transceiver of node E through channel 2. Eventually, the one with the highest weight returns to node B, employing channel 3 to connect transceivers d and f.

2. Gateway distribution of routing nodes

The strategic allocation of gateways necessitates prudent consideration, as an excessive number may amplify the expenses of network deployment. Conversely, an abundance of gateways has the potential to metamorphose into a performance bottleneck, precipitating the tardy conveyance of service data packets or gridlock. In assuming initial knowledge of all node locations, the gateway positions of designated routes, and the traffic requisites for each node, the objective of the gateway placement algorithm is to ascertain which channels can be opened or closed. The algorithm persists its computation until all traffic aligns with user requirements or until the entirety of the traffic conduits is operational.

This algorithm, designated the maximum-flow algorithm, computes the cumulative traffic volume [59]. In the network deployment delineated in this investigation, owing to the absence of a substantial need for transmitting an extensive volume of packet messages in response to the tag signals received by each device, and given the vast expanse of the smart community, it is judicious not to predetermine the closure of all gateways and other routing devices, opting instead to activate them as necessary.

3. Positioning principle

Positioning technologies germane to wireless networks predominantly encompass the utilization of signal strength, denoted as the received signal strength index (RSSI), the Time of Arrival (ToA), the Angle of Arrival (AoA), and the Phase of Arrival (PoA), complemented by an Assisted Global Positioning System (A-GPS).

In this architectural framework, location information assumes a pivotal role, ameliorating data dissemination across the wireless network and proficiently regulating packet quantity. Low-power GPS sensing devices designed for expansive environments have been employed, and the ensuing discourse delves into prevailing positioning methodologies.

(1) Signal strength positioning

The envisioned application environment for this case study predominantly embraces outdoor positioning methodologies, primarily within unobstructed, open spaces. Hence, the chosen method entails utilizing the signal transmission strength to calculate distance.

The signal attenuation model, elucidated in Equation (5), serves as the foundation for estimating the transmission distance based on signal strength.

$$PL(d) = \alpha \left(\frac{d}{d_0} \right)^n \quad (5)$$

Here, $PL(d)$ embodies a function encapsulating the signal attenuation entwined with distance. The variable 'n', typically within the range of 2 to 4, signifies the rate of signal attenuation concerning distance.

The estimation of transmission distance is frequently enshrouded in substantial measurement discrepancies, a manifestation induced by a myriad of uncontrollable environmental variables and the intricacies of signal propagation. This complication imparts heightened challenges to the development of a positioning system reliant on signal strength for distance measurement. To delineate this signal attenuation model accurately, a stochastic variable is introduced to elucidate the nuanced relationship between the measured distance and the ultimate positioning, stemming from signal drift [60], as articulated in Equation (6):

$$PL(d) = PL(d_0) + 10n \times \log\left(\frac{d}{d_0}\right) + X_\sigma \quad (6)$$

(2) Tree point positioning

The maximum likelihood method is employed to ascertain the position of the target object. The underlying concept revolves around gauging the likelihood of the label coordinates (x, y) on the plane, extrapolated from the positions of three reference points. As expressed in Equation (7), where $\sigma_{(x,y)} = \min \sigma_{(x,y)}$:

$$\sigma_{(x,y)} = \left| \sqrt{(x - x_A)^2 + (y - y_A)^2} - r_A \right| + \left| \sqrt{(x - x_B)^2 + (y - y_B)^2} - r_B \right| + \left| \sqrt{(x - x_C)^2 + (y - y_C)^2} - r_C \right| \quad (7)$$

In this formulation, r_A , r_B , and r_C denote the distances estimated by A, B, and C, respectively.

Subsequently, the minimum $\sigma_{(x,y)}$ is utilized to ascertain the position of the target object, as illustrated in Figure 38.

(3) Sample comparison method

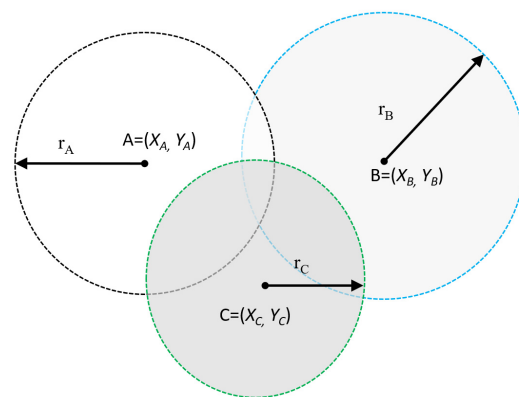


Figure 38. Utilized to ascertain the position of the target object.

This positioning approach harnesses the principles of reinforcement learning (RL) and leverages the characteristics of signal strength, juxtaposing each training location in the positioning database with the corresponding entries.

Effectively mitigating positioning errors arising from the fluctuating environmental signal strength, this methodology necessitates a division of the positioning process into the reinforcement learning framework, as depicted in Figure 39.

- Training phase

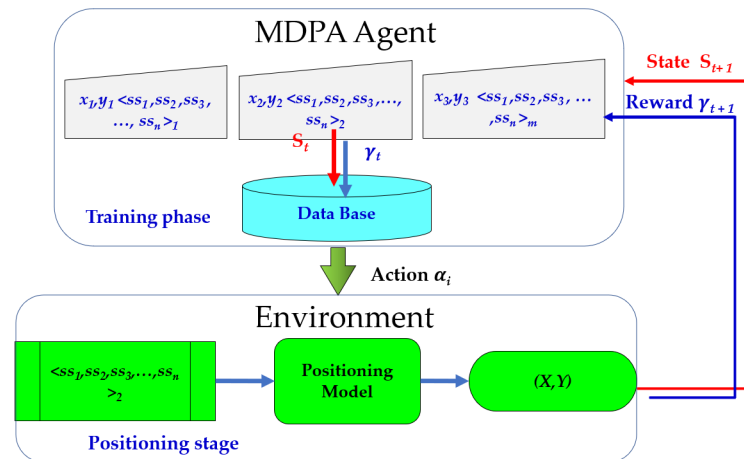


Figure 39. Flowchart of reinforcement learning framework.

When initiating with the determination of coordinates for training positions, approximately 50 to 100 intensity signals are collected from neighboring ZigBee devices at these training locations. During this phase, the database accumulates numerous records structured as $x_1, y_1 < ss_1, ss_2, ss_3, \dots, ss_n >$ in the database, where x and y denote the coordinates of the training position.

- Positioning stage

The ZigBee tags are compared to discern the training position where the signal sample, received during the localization of the target object, may manifest.

(4) Nearest Neighbor in Signal Strength:

In the positioning stage, predicated on the sample signal $S = < ss_1, ss_2, ss_3, \dots, ss_n >$, the geometric distance (Euclidean distance) of each characteristic vector in the positioning module is calculated, as shown in Equation (8):

$$\|S, C_i\| = \sqrt{\sum_{j=1}^n (ss_j - c_j^i)^2} \quad (8)$$

where, i in $c_j^i = < c_1^i, c_2^i, \dots, c_n^i >$ signifies the training position, capturing the average of all signals received from device j .

5.2. Environmental Assessment and Measurement Practice

1. Assessment of outdoor positioning

The realm of outdoor positioning diverges significantly from its indoor counterpart. Outdoors, the necessity for an overly dense array of wireless sensing points diminishes. This discourse delves into pertinent research regarding the strategic deployment of outdoor access nodes. It advocates for the utilization of a centralized context in the placement methods of the Multi-Delivery Positioning Access (MDPA) algorithm. These methods exert influence over the signal strength and the actions at each training location, grounded in the measurement data derived from the CN [61]. These methods encompass the following:

- Arranging peripheral nodes and inner nodes at a 60° separation.
- Arranging peripheral nodes and inner nodes at a 90° separation.

Nevertheless, given the outdoor positioning application requirements, a hybrid approach emerged. A fusion of the “120° segmentation and layout method” with the “feasible path node sample comparison method”, rooted in geographical location characteristics, can efficiently carve out blocks in the most streamlined fashion.

Research findings indicate that the initial 60° access point layout method is well-suited for expansive outdoor deployments. Conversely, the second method finds its niche in rectangular area deployments. However, its coverage area is confined to either 60° or 90°, delivering effective coverage solely within the ambit of the wireless radio frequency. Alas, it remains insufficient for practical use in regional positioning.

This article posits a third methodology, judicious for the economical deployment of ZigBee devices, preserving practicality. This approach amalgamates the “120° split deployment method” and the “feasible path-like node sample ratio”, anchored in geographical location characteristics, yielding optimal outcomes.

(1). Node Placement Strategy

It is posited that the communicative expanse of a Zigbee routing apparatus equates to its communicative radius. Deliberations encompass the ascertainment of the communicative realm, interference precinct, coverage expanse, and debilitation quotient predicated upon this radius. Several routing contrivances have employed this methodology to deduce the authentic communicative realm subsequent to amalgamation, directing an enhanced deployment. The enveloping domain consists of the overall coverage span of the routing mechanism $[(A + B) - (A \cap B)]$. The area of interference denotes the intersecting region of the two routing contrivances $(A \cap B)$, and the total area of the routing device is depicted in Figure 40.

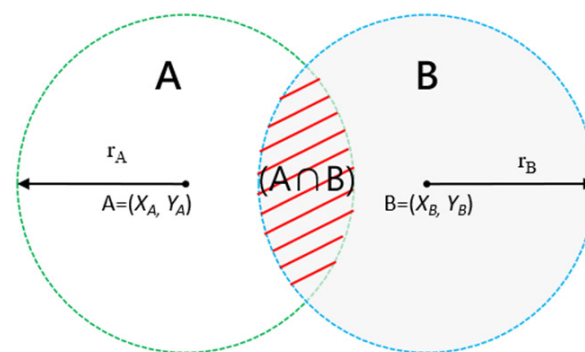


Figure 40. Schematic of the intersection placement of devices A and B.

In assuming the communicative radius of both routing devices is denoted as R , the combined area of the routing devices amounts to $2\pi R^2$. The impairment quotient signifies the proportion of area relinquished subsequent to coverage by the routing device, divided by the total area of the routing device expressed as $((A \cap B) / (A + B)) \times 100\%$. In scenarios involving multiple routing devices, this methodology is applied to compute the genuine communicative realm subsequent to the amalgamation of routing devices, instrumental in discerning a more judicious deployment approach.

(2). 60° Bisecting Arrangement

The 60° bisecting arrangement entails that the intersection arc of each inscribed circle and circumscribed circle is precisely 60°. Commencing from a designated reference point, each device intersects with the next at an angle of 60°, as depicted in Figure 41.

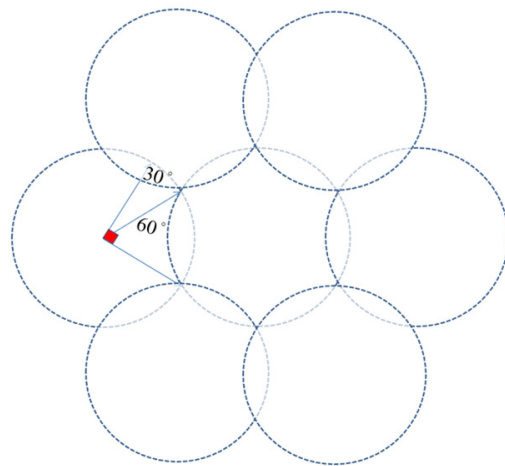


Figure 41. The 60° split-layout method.

Nonetheless, it may intersect with other CNs, and it will conclude once the deployment surpasses the anticipated position.

(3). Bisecting Arrangement

The 90° segmented layout method signifies that the intersection arc of each inscribed circle and circumscribed circle measures precisely 90 degrees. In the course of deployment, originating from a predetermined reference point, the intersection arc between each device and its successive counterpart is set at 90 degrees, as illustrated in Figure 42.

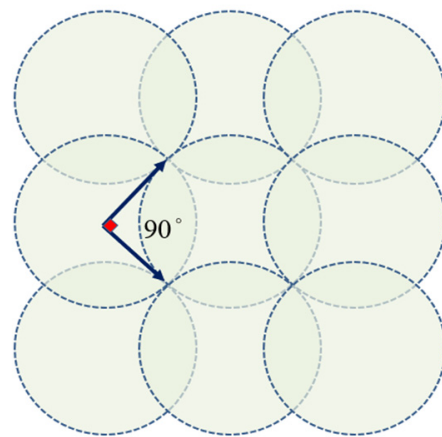


Figure 42. The 90° split-layout method.

Nevertheless, it may intersect with other CNs, and it will conclude once the deployment surpasses the anticipated position.

(4). Optimization for the Installation Technique

Concerning outdoor sensing device equipment, the findings in this scholarly article reveal that within the 90° split layout method, the CN position aligns along both the X-axis and the Y-axis on the coaxial line. Therefore, this proves highly suitable for deployment in a rectangular area. Nevertheless, the intersection area of the two circles exceeds 15%, surpassing that of the 60° split-layout method by more than 10% [62], as depicted in Figure 43.



Figure 43. The 90° sensing device placement.

The ZigBee sensing range is designated as the radius 'r'; hence, when positioned at 90° on the X and Y axes, the distance between two nodes becomes 'd₁'. When assuming 'r' to be 100 m, the distance 'd₁' should measure 140 m, as per Equation (9):

$$d_1 = 2r \times \cos 45^\circ \quad (9)$$

For expansive deployments, this experiment opted for a 60° division approach, as illustrated in Figure 44. In setting the ZigBee sensing distance as the radius r, arranging nodes at a 60° angle in an open expanse yields a distance d₂ between any two nodes. When assuming r is 100 m, the anticipated distance d₂ should be 173 m, per Equation (10):

$$d_2 = 2r \times \cos 30^\circ \quad (10)$$

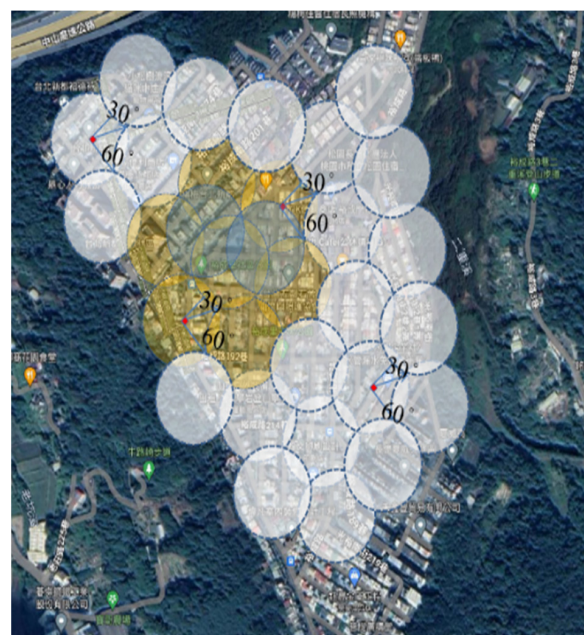


Figure 44. The 60° sensing device placement.

The framework of this investigation revolves around a wireless sensing apparatus embedded within an intelligent community, complemented by a smart meter in an alfresco milieu. At periodic intervals, the smart meter autonomously dispatches messages to the self-organizing network sensing node, denoted as the CN. Upon the receipt of the transmission, the sensing node meticulously logs pertinent details into the ephemeral registry's data repository, encompassing the smart meter's identifier, communication quality metric, received signal strength index, and other relevant parameters. This orchestrated system employs a polling mechanism to harvest smart meter data from each sensing node through the ZigBee network. Subsequently, leveraging the amassed data, it delineates the geographical domain of the smart meter's existing location distance relative to a specific node's service area.

5.3. Positioning and Construction

Real Case 2. Implementation and Measurement Practices of the Smart Town.

The empirical approach of this scholarly inquiry involved the utilization of ZigBee device CN-xxx, crafted by Freestyle Technology in Australia, which functioned as the node tasked with message reception. It was designated as the reference point for coordinate establishment, configuring an expansive outdoor positioning quadrant. In the realm of mobile anchor points, SM-ooo served as the ZigBee tag. Various data streams, encompassing signal strength and signal quality, transmitted by SM-ooo, were meticulously acquired through the CN-xxx. The analytical scrutiny of this pragmatic validation unfolded as follows.

(1). System apparatus

The distance considerations between blocks were as follows:

1. Network planning system aspect: The best suggestion for positioning the arbitrage comparison device in conjunction with the natural gas company's geographical information system was 0 to 100 m.
 2. The CN-xxx device, the best service area was based on 100 m: The empirical approach of this inquiry involved the utilization of the ZigBee device CN-xxx functioning as the node tasked with message reception. It was designated as the reference point for coordinate establishment, configuring an expansive outdoor positioning quadrant.
 3. SM-ooo device specifications, the best service area was based on 100 m: In the realm of mobile anchor points, SM-ooo served as the ZigBee tag. Various data streams, encompassing signal strength and signal quality, transmitted by SM-ooo, were meticulously acquired through CN-xxx, as delineated in Tables 7 and 8.
- The technical delineations of the CN-xxx device are presented in Table 8.
 - Technical delineations of the SM-ooo device, as shown in Table 9.

(2). Validate Operational Approaches

Table 7. CN-xxx specifications.

Item	Specification
Frequency	2.4 GHz
Modulation	O-QPSK
Maximum Transmission Rate	250 kbps
Receive Sensitivity	−104 dBm
Transmission Distance	1200 m (LOS)
Channel No.	16 (5 MHz)
Tx	−6 to +208 dBm
Power Consumption Tx	<204 mA
Power Consumption Rx	<54 mA

Table 8. SM-000 specifications.

Item	Specification
Frequency	2.4 GHz
Modulation	O-QPSK
Maximum Transmission Rate	250 kbps
Receive Sensitivity	−95 dBm
Transmission Distance	100 m (LOS)
Channel No.	16 (5 MHz)
Tx Power	−24 dBm to 0 dBm
Power Consumption Tx	<24 mA
Power Consumption Rx	<76 μ A

The functionalities of the device were ascertained utilizing ZigBee for network reference point localization. Upon receiving a message packet, the device autonomously appended an RSSI value to the informational packet. The system necessitated the provision of three to eight pixels before initiating the computation of the positioning coordinates. The coordinate value, the RSSI value of the reference point, and the A and n values of the reference must be inputted through the settings, as delineated in Equations (11) and (12).

$$RSSI = -(10n \log_{10} d + A) \quad (11)$$

where the variables are denoted as follows:

n: constant representing signal propagation;

d: representing the distance from the transmitter;

A: signal strength received at one meter.

The correlation between the measured distance and the known RSSI, A, and n values is articulated in Equation (12).

$$d = 10^{((RSSI) - A) / (10^n)} \quad (12)$$

(3). RSSI and LQI measurements

Based on two pivotal metrics in the localization, we scrutinized the data records of the signal strength information and LQI to unveil the data outcomes received at the recipient's end due to distance-related factors. Presented below are the authentic measurement outcomes of the ZigBee equipment. The association between the RSSI and the receiving distance is delineated in Table 9.

An RSSI is a value that measures the strength of the signal received at the receiving end, as shown in Equation (13).

$$SSI = 10 \times \log \frac{P_{RX}}{P_{ref}} \quad (13)$$

Table 9. Measurements of RSSI and distance intensity.

Distances (m)	RSSI (dB)
0	210.69
10	173.93
20	172.49
30	171.73
40	171.15
50	165.13

Table 9. Cont.

Distances (m)	RSSI (dB)
60	166.86
70	167.16
80	164.53
90	161.57
100	162.89
110	161.75
120	162.07

At the transmitting end, P_{TX} was employed, and at the receiving end, P_{RX} was utilized. G_{TX} represents the gain value of the transmitting end, and G_{RX} is the gain value of the receiving end, as articulated in Equation (14).

$$P_{RX} = P_{TX} \times G_{TX} \times G_{RX} \left(\frac{\lambda}{4\pi d} \right)^2 \quad (14)$$

where λ signifies the wavelength, and d denotes the distance in the signal energy distribution curve between the transmitting device and the receiving device. It is evident that the RSSI value of the tag is at a direct viewing distance, as portrayed in Figure 45. In considering a 90° segmentation as an instance, the energy distribution of the smart meter (SM) within the sensing range may yield distinct RSSI intensity-sensing indicators at varying distances.

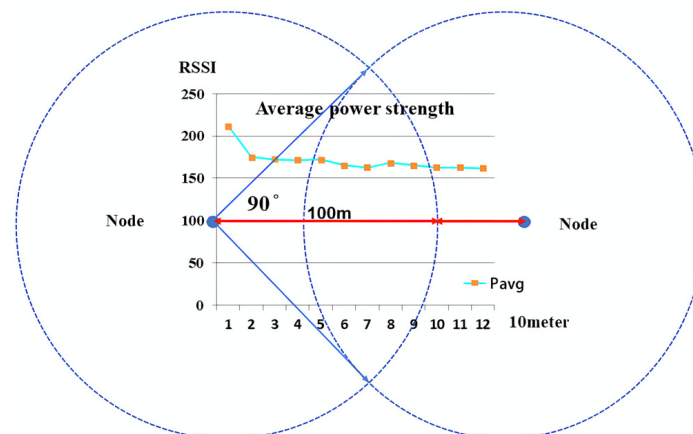


Figure 45. The relationship between the sensing of the devices using the 90° segmentation method.

The RSSI intensity received by the ZigBee device reference node is observable. In response, the RSSI value within the range of 0 to 20 m exhibits relative elevation. The mean RSSI index remains above 172; however, the gradient of the entire curve is remarkably gentle, rendering almost imperceptible distinctions in terms of distance.

As illustrated in Figure 46, within the interference region where the two circles intersect in either the 90° segmentation method or the 60° segmentation method, the intensity exhibits minimal variation. Consequently, the effective distance becomes challenging to ascertain. Hence, additional auxiliary methods should be introduced to discern the label's location.

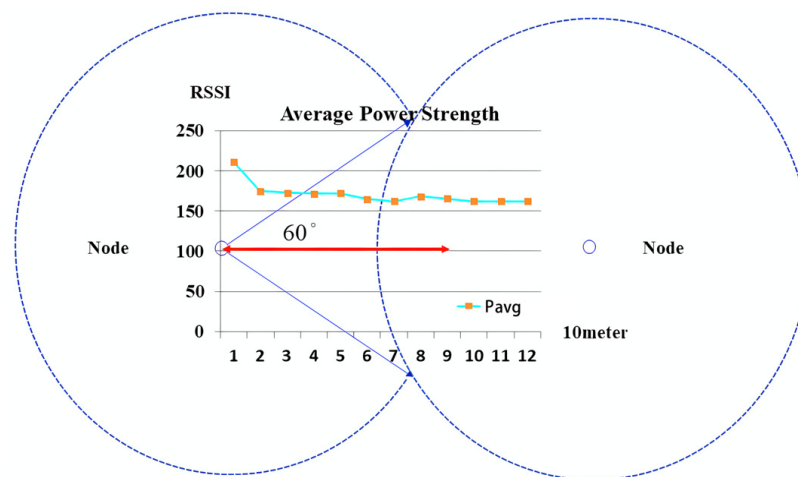


Figure 46. The relationship between the sensing of the devices using the 60° segmentation method.

An alternative means of gauging distance involves employing an additional metric to assess its potential impact on the precision of positioning determinations. This metric is denoted as the LQI [63,64], primarily revealing the quantity of packets necessitating retransmission to reach the receiving terminus.

The testing methodology entailed designating one of the two sensing nodes as a label and continually dispatching packets in a cyclic manner, while the counterpart device logged the LQI value. Throughout the testing procedure, the location from which the SM emitted the signal was adjusted and gauged from 0 to 45 m, reiterated over 20 cycles, and executed with three distinct tags.

Based on the LQI measurement outcomes that the MDPA algorithm, the findings were consolidated thread transection results, as shown in Figure 47.

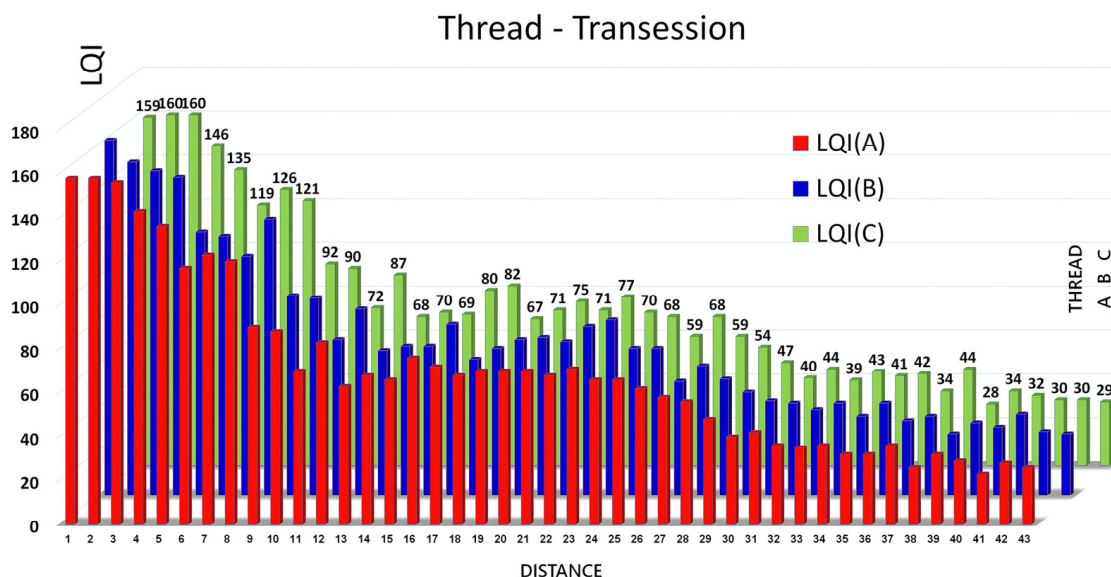


Figure 47. SM-ooo device received anchor point quality indicator LQI.

While the quality of wireless packet transmission naturally diminishes with increasing distance, an examination of the aforementioned figure revealed distinct characteristics among three different tags. When observed directly and without impediments, both the LQI and RSSI exhibit descending traits. The LQI value, ranging between 0 and 255, serves as an indicator where the maximum value signifies an optimal state of link quality. However, in principle, the LQI lacks a deterministic dependence on distance. Parties in communication

may be widely separated, and despite the signal's feebleness, a high LQI value can still be attained under conditions of low background noise or if the modulation method itself boasts robust anti-noise capabilities. Typically, the LQI primarily finds application in network optimal cost routing and data diffraction return coordinators [59]. The numerical derivation in the LQI is computed based on the bit error rate, as demonstrated in Equation (15):

$$RED = (47 - MED) \times 6 \quad (15)$$

If $(ED < 0)$, then $ED = 0$; if $ED > 255$, then $ED = 255$. MED represents the intensity level of the gain value for receiving a packet message. In the chip design of this apparatus, there are 47 levels, each commencing with a 2dB interval. According to the IEEE 802.15.4 standards, the assessment of a received signal strength across various channels is termed energy detection (ED). Its purpose lies in the computation of the channel selection at the network layer. The ED duration spans the transmission time of eight symbols, and a minimum ED value of 0 indicates that the received power is less than 10 dB, surpassing the sensing range of the receiving end. The ED value within the range of received signal strength must be no less than 40 dB.

(4). Establish a Positioning Model

○ Analysis of the Model

After utilizing the 120° segmentation approach, given the limitation of not being able to densely position reference points outdoors, and considering that outdoor positioning typically falls within the line of sight, this study advocates for the application to be structured with utmost cost efficiency (i.e., deploying the fewest readers at the lower reference point) to achieve an optimal positioning accuracy.

The 90° layout method was refined, giving rise to the inaugural 120° reference point layout method. The configuration of the wireless signal interference area generated using this method is elucidated in Figure 48.

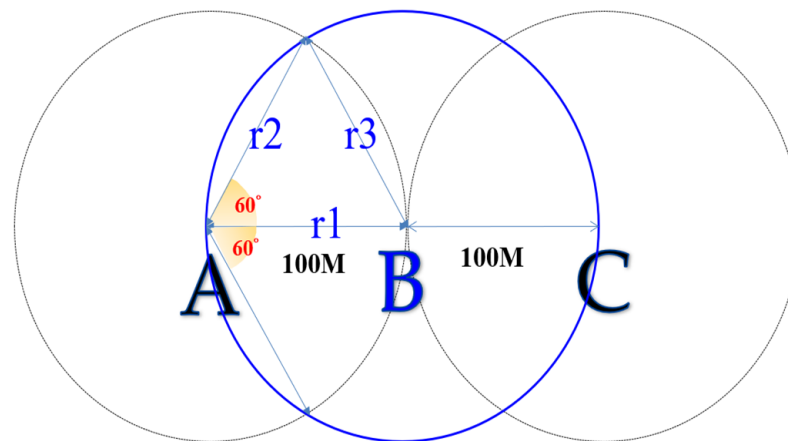


Figure 48. The 120° segmentation method.

It is evident that the radii of circles A and B extend to 100 m each, resulting in each side of the equilateral triangle formed by r_1 , r_2 , and r_3 precisely matching the radii of A and B. Consequently, the intersection arc between the two circles spans 120°, forming a 120° layout, as depicted in Figure 49.

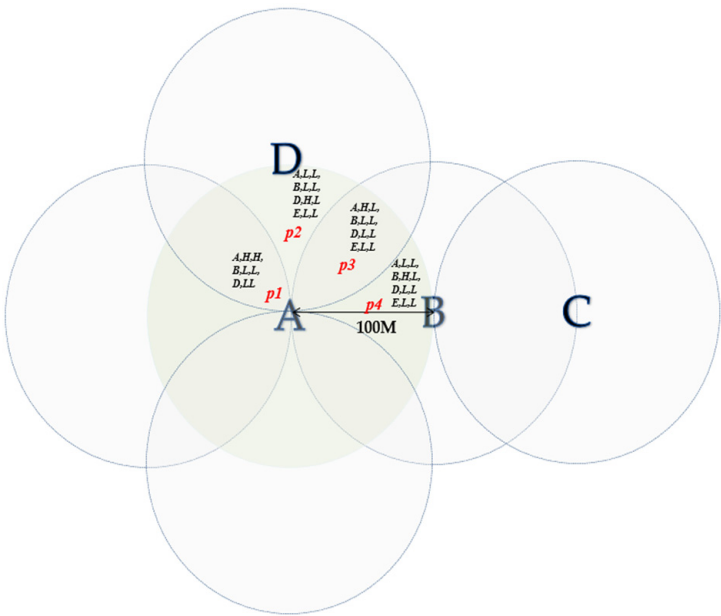


Figure 49. Coverage area under the 120° deployment method.

The positioning reference coordinates engendered through this layout methodology are succinctly compiled following empirical measurements, as delineated in Table 10.

Table 10. Actual measurements of RSSIs and LQIs corresponding to different reference points.

Ref. / Take	Reference Point A		Reference Point B		Reference Point C		Reference Point D	
	RSSI	LQI	RSSI	LQI	RS SI	LQI	RSSI	LQI
p1	174(H)	85	162	-	-	-	-	-
p2	165	30	-	-	-	-	171	60
p3	172(H)	40	163	30	-	-	165	42
p4	168	42	172 (H)	55	-	-	-	-

(H) in Table 11 designates that it surpasses the presumed dB value of 172, signifying that the signal’s potency received at the positional juncture is elevated, warranting its designation as a criterion for proximity to the reference point. Consider p2 in Table 7 as an example. If, in the process of assessing the signal’s dB value, no reference point registers a value exceeding 172, the one closest to 172 will serve as the determinant for establishing the receiving range, thereby identifying the reference point closest to it.

Table 11. Establishing positioning partition model.

Ref. / Take	Ref. Point A		Ref. Point B		Ref. Point C		Ref. Point D		Ref. Point E	
	RSSI	LQI	RSSI	LQ I	RSSI	LQI	RSSI	LQI	RSSI	LQ I
p2	L	L	L	L	L	L	H	L	L	L
p3	H	L	L	L	L	L	L	L	L	L
p4	L	L	H	L	L	L	L	L	L	L
p5	L	L	L	L	L	L	L	L	H	L
p6	L	L	L	L	-	-	-	-	-	-

According to the substantiated outcomes from practical observations, the fluctuations in the RSSI and LQI intensities manifest a gradual demeanor beyond a radius of approximately 20 m from the reference point, persisting until the 100 m mark. This implies that, within the 20 m radius, precise intensity delineation is achievable. In the formulation of future positioning algorithms, an RSSI intensity exceeding >172 dBm and an LQI index surpassing 60 can be deemed indicative of a specific reference point within the outdoor 20 m radius, as illustrated in Figure 50.

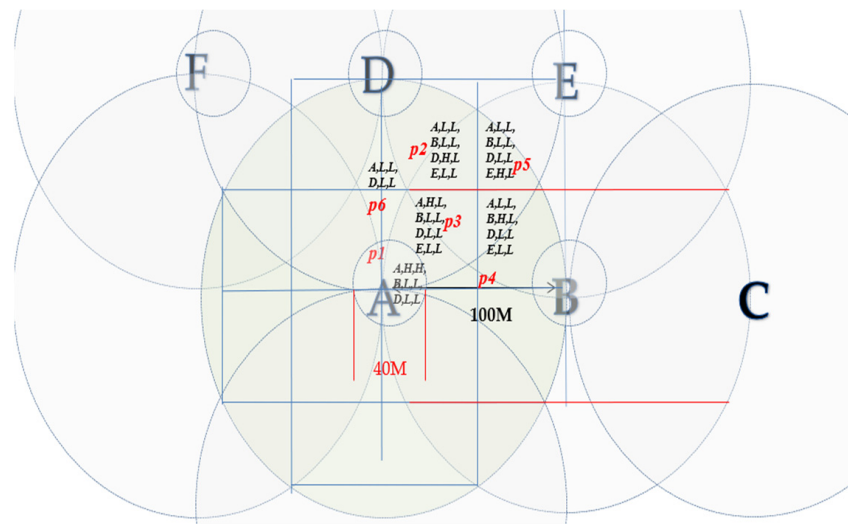


Figure 50. The 120° layout method used to establish a regional segmentation model.

The label p1 denotes the recorded data at reference point A, with an acquired RSSI value of 174 and an LQI value of 85. In the architectural blueprint for an SM application crafted within this inquiry, a deliberate strategy was conceived, asserting that the unobstructed range spanning 20 m to 50 m outdoors does not pose a susceptibility to connection lapses. This strategic alignment perfectly complements the ZigBee outdoor measurement architecture's application. In confining the two positioning tags within a span of less than 50 m, there arises no imperative for the ZigBee devices to mimic the density requisites of indoor positioning, yet their functionality remains potent for pragmatic applications.

Consequently, the entire expanse of the sensing positioning realm is compartmentalized into distinct blocks, with p1 to p6 representing the tag locations. Given that P1 falls within the 20 m radius of the reference point's core, no additional positioning blocks are delineated, as depicted in Figure 51.

The initial codes of <A, L, L>, <B, L, L>, <D, H, L>, and <E, L, L>, cataloged in position P2, symbolize distinct reference points. The last two codes denote the RSSI and LQI correspondingly, where H signifies high, and L signifies low. If we stipulate that the RSSI is considered high when the average exceeds 172, and the LQI is deemed high when surpassing 60, and vice versa, a set of model rules is thus established through practical measurements, as elucidated in Table 11.

The precision of positioning in this inquiry does not demand meticulous location identification. Rather, the intent of this manuscript is to comprehend and accomplish the swiftest and most economically efficient deployment in an expansive outdoor setting. Thus, we capitalized on the attributes wherein the RSSI value of ZigBee decelerates beyond a radius of 20 m, and the LQI value diminishes exponentially with the extension of distance. Consequently, we formulated the subsequent outdoor Location Block Mode. The delineation of the 120° division approach is illustrated in Figure 51.

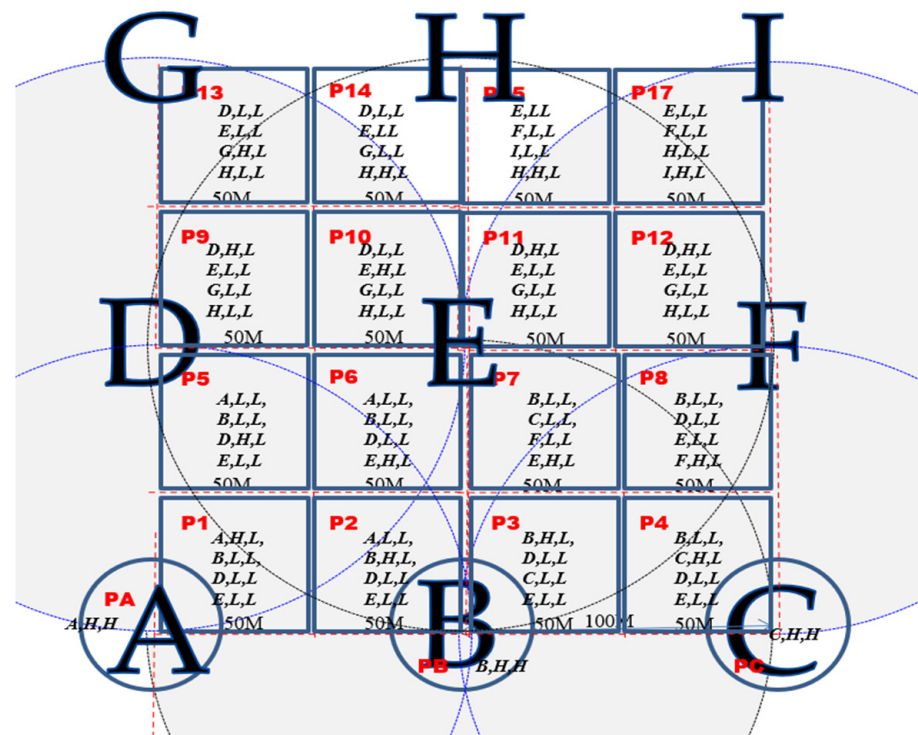


Figure 51. The 120° layout methodology employed for the establishment of a regional division model.

This involves determining the signal strength by considering the center of each circle as the focal point and establishing circles labeled A to I, each interconnected with adjacent circles. Within the effective transmission and reception range of ZigBee, set at a signal strength of 100 m, we devised a palace of grid-like blocks. Each grid was partitioned into a square measuring 50 m, precisely aligning with the characteristics sensed using the RSSI and LQI indicators, thus establishing a framework for interpretation.

Taking block P1 as an example, the RSSI intensity received at reference point A was most potent in blocks P1, P2, P5, and P6. In contrast, the signals received at reference points B, D, and E, due to their respective distances, experienced a swift decay to a more subdued level. This observation allowed us to infer that the positioning detection point lied within block P1. Additionally, if there existed a positioning point within a 20 m radius of reference point A, it was conclusively located in the block CN.

- The advantages of the 120° distribution method are as follows:
 - A. The reference point arrangement boasts minimal density, strategically positioned every 100 m, rendering it ideal for location determination in expansive outdoor settings. In contrast to conventional ZigBee reference points, which are typically spaced at intervals of 10 to 30 m, this approach significantly diminishes the cost associated with reference point deployment.
 - B. The positioning areas resemble a checkerboard pattern, segmented into areas with dimensions of 50 m in length and width.
 - C. The positioning blocks, designed as square segmented areas, facilitate the creation of straightforward and convenient practical positioning algorithms.
 - D. When leveraging ZigBee's mesh network configuration technology and energy-efficient characteristics, the placement locations encounter fewer restrictions in real outdoor environments. Consequently, the entire designated area can be deployed in close approximation to a square.
 - E. Within the central region of each reference point, such as A, an enclosed circular area with a 20 m radius defines a grouping of positioning blocks, augmenting the likelihood of precise positioning interpretation.

- F. The data essential for positioning can be readily accessed without the need for intricate calculations.
- G. A heightened level of efficacy is maintained even in scenarios with limited training point data.
- The cons of the 120° distribution method are as follows:
 - A. The distance between any two blocks may vary from 0 to 100 m, potentially impacting the precision of practical assessments.
 - B. While the 50 m² interval design is well suited for extensive villa areas, open-air residences, and communal apartments with expansive surroundings, it may not be optimal for locales characterized by vertical structures, national parks, or environments with diverse and dynamic scenery changes.

6. Conclusions

This paper expressed design pros of smart meters in detail thorough comparisons with existing AMI systems, specifically in terms of cost efficiency, system deployment speed, and information security risks in terms of the contribution to LNG consumers, as delineated in Table 12.

Table 12. Expressed design pros of smart meters in terms of the contribution to LNG consumers.

Key Factors	Descriptions	Operating Performance	Future Prospects
1. Optimal Cost Efficiency			
(1). System Infrastructure Expenditure	In embracing a cloud-based architecture, the company finds itself in a position where investments in system software and hardware infrastructure remain virtually unaltered. Moreover, as the system's application scope expands, the specter of augmented maintenance expenses is notably absent.		1. Fracture Analysis System
(2). Communication Expenses	Currently, NB-IoT/LTE SMS transmission incurs a fee of NT\$1.0 per instance. Actions such as meter readings, alarms, and other system functionalities, each treated as a distinct transmission, attract a monthly circuit rental fee. This fee is of paramount concern amongst industry peers who advocate for microcomputer watches. Remarkably, this study harnessed cutting-edge transmission technology and system architecture, compelling telecommunications providers to recalibrate their pricing model to align with the AMI system's characteristics. Consequently, a singular communication fee per meter per month is levied, eliminating supplementary charges, thereby substantially curtailing communication-related expenses.	Propelled by the relentless march of science and technology, we dared to conceive novel system architectures and operational paradigms. Our aspiration transcends the confines of the rudimentary AMR SM, and we set our sights squarely on the AMI horizon. Presently, industries incoming to business-promotion status comprise peers that have actively participated in cloud platform testing, offering invaluable insights to the project team, leading the world into a new realm of cross-domain Internet of Things with Taiwan's natural gas industry technology and applications to improve AMI network resilience and equipment's zero-trust security risk information management and contingency management in the defense of disaster relief responses.	2. Energy Efficiency Analysis System
(3). Maintenance Outlays	As previously highlighted, the cloud-based architecture obviates the need for additional software and hardware acquisitions. Post installation, there exist no exigencies for equipment maintenance, replacements, or the hiring of maintenance personnel. Coupled with the marked reduction in communication costs, post system deployment, the company's sole outlays comprise meter reading service fees and monthly communication fees for online message transmissions.		3. Deployment of a Digital Security System
2. Expedited Implementation	Telecom operators possess fully fledged network systems. The extant backend management platform and transmission technologies represent well-vetted offerings within the purview of intelligent cloud management systems. These have undergone meticulous modification and rigorous testing by collaborating manufacturers. Further, communication modules have secured NCC certification in R.O.C. In summation, the system environment is in a state of readiness and can be set into motion according to the internal timeline of the natural gas company.		4. Integrated Utilization of Mobile Data Devices

Table 12. Cont.

Key Factors	Descriptions	Operating Performance	Future Prospects
3. Mitigated Information Security Risks	Telecommunication operators stand as the nation’s foremost data communication firms, instilling a profound sense of confidence in their expertise regarding information security control mechanisms and technology. Consequently, the adoption of this model serves to alleviate information security risks and associated expenditures for natural gas operators. Furthermore, contracts act to standardize the legal obligations of telecommunications operators in data processing, transmission, and storage endeavors on behalf of natural gas operators.	Propelled by the relentless march of science and technology, we dared to conceive novel system architectures and operational paradigms. Our aspiration transcends the confines of the rudimentary AMR SM, and we set our sights squarely on the AMI horizon. Presently, industries incoming to business-promotion status comprise peers that have actively participated in cloud platform testing, offering invaluable insights to the project team,	5. Advancements in Customer Service Center Development
4. Synergistic Collaboration	Beyond the confines of system operations, both entities can furnish each other with operational platforms, fostering mutual collaboration and revenue augmentation. This platform can subsequently accommodate value-added services, with the telecommunications operator systems serving as an extension of the company’s customer service platform.	leading the world into a new realm of cross-domain Internet of Things with Taiwan’s natural gas industry technology and applications to improve AMI network resilience and equipment’s zero-trust security risk information management and contingency management in the defense of disaster relief responses.	

Author Contributions: Conceptualization, C.-L.W. and T.-T.L.; methodology, C.-L.W. and H.-P.L.; software, C.-L.W. and J.-S.S.; validation, C.-L.W., T.-T.L., C.-T.L., W.-T.S., Y.-S.H. and J.-S.S.; formal analysis, C.-T.L. and W.-T.S.; investigation, C.-L.W. and T.-T.L.; resources, Y.-S.H. and J.-S.S.; data curation, C.-T.L. and W.-T.S.; writing—original draft preparation, C.-L.W. and T.-T.L.; writing—review and editing, C.-L.W. and W.-T.S.; visualization, Y.-S.H. and J.-S.S.; supervision, H.-P.L. and Y.-S.H.; project administration, C.-T.L. and J.-S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Successful in alignment with the smart city development initiative, the research team enabling the smart natural gas meter management system has pioneered the establishment of an advanced metering infrastructure with HWSNs at its core. The system planning and indoor coverage of a coordinated multipoint operation architecture in a low-power node small cell enhancement system help design and maintenance engineers to properly perform planning, analysis, and maintenance operations. Based on this, the SM, CN, SGMS, CSTI-EDR Satellite platform, FTTW and CMTW equipment can solve open-area transmission problems for the signal coverage of hybrid telecommunication networks.

Acknowledgments: We would like to gratefully acknowledge the contribution of our colleagues at Ericsson, particularly Mike Chang and Taiwan Mobile Leon Hu. We would also like to thank our research teams. Writing this paper would not have been possible without their generosity and support throughout the process.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. ZigBee Alliance. ZigBee Specification. Available online: <https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-347-4-21-0csg-zigbee-specification.pdf> (accessed on 27 June 2015).
2. IEEE 802.15.4; Specification, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE: Piscataway, NJ, USA, 2015.
3. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [\[CrossRef\]](#)
4. Djahel, S.; Doolan, R.; Muntean, G.M.; Murphy, J. A Communications-Oriented Perspective on Traffic Management Systems for Smart Cities: Challenges and Innovative Approaches. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 125–151. [\[CrossRef\]](#)
5. Andreev, S.; Galinina, O.; Pyattaev, A.; Gerasimenko, M.; Tirronen, T.; Torsner, J.; Sachs, J.; Dohler, M.; Koucheryavy, Y. Understanding the IoT connectivity landscape: A contemporary M2M radio technology roadmap. *IEEE Commun. Mag.* **2015**, *53*, 32–40. [\[CrossRef\]](#)
6. Ericsson. *More than 50 Billions Connected Devices*; Ericsson: Stockholm, Sweden, 2011; Volume 1.
7. Wu, C.-L.; Lu, T.-T.; Lee, C.-T.; Sun, J.-S.; Lin, H.-P.; Hwang, Y.-S.; Sung, W.-T. Evolution towards Coordinated Multi-Point Architecture in Self-Organizing Networks for Small Cell Enhancement Systems. *Electronics* **2023**, *12*, 2473. [\[CrossRef\]](#)
8. Condoluci, M.; Sardis, F.; Mahmoodi, T. Softwarization and Virtualization in 5G Networks for Smart Cities. In Proceedings of the EAI International Conference on Cyber physical systems, IoT and sensors Networks (CYCLONE), Rome, Italy, 26 October 2015.
9. Sanchez, L.; Munoz, L.; Galache, J.A.; Sotres, P.; Santana, J.R.; Gutierrez, V.; Ramdhany, R.; Gluhak, A.; Krco, S.; Theodoridis, E.; et al. Smart Santander: IoT experimentation over a smart city testbed. *Comput. Netw.* **2014**, *61*, 217–238. [\[CrossRef\]](#)
10. Lien, S.Y.; Chen, K.C.; Lin, Y. Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. *IEEE Commun. Mag.* **2011**, *49*, 66–74. [\[CrossRef\]](#)
11. Zheng, K.; Hu, F.; Wang, W.; Xiang, W.; Dohler, M. Radio resource allocation in LTE-advanced cellular networks with M2M communications. *IEEE Commun. Mag.* **2012**, *50*, 184–192. [\[CrossRef\]](#)
12. Polese, M.; Centenaro, M.; Zanella, A.; Zorzi, M. M2M Massive Access in LTE: RACH Performance Evaluation in a Smart City Scenario. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016.
13. 3GPP. TS 36.300; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Rel. 11. 3GPP: Sophia Antipolis Cedex, France, 2012.
14. 3GPP. TS 36.388; Study on Provision of Low-Cost Machine-Type Communications (MTC) User Equipments (UEs) Based on LTE, Rel. 12. 3GPP: Sophia Antipolis Cedex, France, 2013.
15. Ben Dhaou, I.; Kondoro, A.; Kelati, A.; Rwegasira, D.S.; Naiman, S.; Mvungi, N.H.; Tenhunen, H. Communication and Security Technologies for Smart Grid. *Int. J. Embed. Real-Time Commun. Syst.* **2017**, *8*, 40–65. [\[CrossRef\]](#)
16. Shajahan, A.H.; Anand, A. Data acquisition and control using Arduino-Android platform: Smart plug. In Proceedings of the 2013 International Conference on Energy Efficient Technologies for Sustainability, Nagercoil, India, 10–12 April 2013; pp. 241–244.

17. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Trans. Ind. Inform.* **2013**, *9*, 28–42. [CrossRef]
18. Gallardo, J.L.; Ahmed, M.A.; Jara, N. LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. *IEEE Access* **2021**, *9*, 124295–124312. [CrossRef]
19. Ashok, K.; Reno, M.J.; Blakely, L.; Divan, D. Systematic Study of Data Requirements and AMI Capabilities for Smart Meter Analytics. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–14 August 2019; pp. 53–58.
20. Luambano, M.M.; Kondoro, A.; Dhaou, I.B.; Mvungi, N.; Tenhunen, H. IoT enabled Smart Meter Design for Demand Response Program. In Proceedings of the 2020 6th IEEE International Energy Conference (ENERGYCon), Gammarth, Tunisia, 28 September–1 October 2020; pp. 853–857.
21. Dai, X.; Xiao, Z.; Jiang, H.; Alazab, M.; Lui, J.C.; Dustdar, S.; Liu, J. Task co-offloading for d2d-assisted mobile edge computing in industrial internet of things. *IEEE Trans. Ind. Inform.* **2022**, *19*, 480–490. [CrossRef]
22. Yuan, H.; Yang, B. System Dynamics Approach for Evaluating the Interconnection Performance of Cross-Border Transport Infrastructure. *J. Manag. Eng.* **2022**, *38*, 04022008. [CrossRef]
23. Balador, A.; Cinque, E.; Pratesi, M.; Valentini, F.; Bai, C.; Gómez, A.A.; Mohammadi, M. Survey on decentralized congestion control methods for vehicular communication. *Veh. Commun.* **2021**, *33*, 100394. [CrossRef]
24. IEEE P802.15 Working Group for WPANs. Cluster Tree Network; April 2001. Available online: <https://mentor.ieee.org/802.15/file/05/15-05-0261-01-003c-generalization-and-parameterization-mmwave-channel-models.pdf> (accessed on 10 November 2023).
25. Zheng, J.; Lee, M.J. A Comprehensive Performance Study of IEEE 802.15.4. 2004. Available online: http://www.inf.ufes.br/~zegonc/material/Redes%20de%20Sensores%20sem%20Fio/IEEE_802.15.4-ARTIGO%20Comprehensive%20Performance%20Study%20of%20IEEE%20802.15.4.pdf (accessed on 22 June 2023).
26. ZigBee Alliance. Available online: <http://www.zigbee.org/en/index.asp> (accessed on 21 February 2024).
27. Laneman, J.N.; Wornell, G.W. Energy-efficient antenna sharing and relaying for wireless networks. *Proc. IEEE Wireless Commun. Netw. Conf.* **2000**, *1*, 7–12. [CrossRef]
28. Hasna, M.O.; Alouini, M. A performance study of dual-hop transmissions with fixed gain relays. *IEEE Trans. Wireless Commun.* **2014**, *3*, 1963–1968. [CrossRef]
29. IEEE Std 802.11; LAN-MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. IEEE: New York, NY, USA, 1997.
30. LAN-MAN Standards Committee of the IEEE Computer Society. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*; IEEE: New York, NY, USA, 2013.
31. Mahmoodi, T.; Seetharaman, S. Traffic Jam: Handling the Increasing Volume of Mobile Data Traffic. *IEEE Veh. Technol. Mag.* **2014**, *9*, 56–62. [CrossRef]
32. Koubaa, A.; Alves, M.; Tovar, E. A Comprehensive Simulation Study of Slotted CSMA/CA for IEEE 802.15.4 Wireless Sensor Networks. In Proceedings of the IEEE WFCSS 2006, Torino, Italy, 28–30 June 2016.
33. Kleinrock, L.; Toubagi, F.A. Packet Switching in Radio Channels: Part I—Carrier Sense Multiple Access Modes and Their Throughput-Delay Characteristics. *IEEE Trans. Commun.* **1975**, *23*, 1400–1416. [CrossRef]
34. Jurcik, P.; Koubaa, A. The IEEE 802.15.4 OPNET Simulation Model: Reference Guide v2.0. IPP-HURRAY Technical Report, HURRAY-TR-070509, May 2014. Available online: <http://www.open-zb.net> (accessed on 21 January 2024).
35. Cunha, A. On the use of IEEE 802.15.4/ZigBee as Federating Communication Protocols for Wireless Sensor Networks. HURRAY-TR-070902. Master's Thesis, Faculdade de Engenharia da Universidade do Porto, Porto, Portugal, 2007.
36. Open Networking Foundation ONF. Available online: <https://www.opennetworking.org/> (accessed on 21 February 2024).
37. ONF Specification. OpenFlow Switch Specification 1.0.0. December 2009. Available online: <https://opennetworking.org/wp-content/uploads/2013/04/openflow-spec-v1.0.0.pdf> (accessed on 10 November 2023).
38. ONF Specification. OpenFlow Configuration and Management Protocol 1.1.1. November 2013. Available online: <https://opennetworking.org/wp-content/uploads/2013/02/of-config-1-1-1.pdf> (accessed on 21 February 2024).
39. ONF Specification. OpenFlow Switch Specification 1.3.3. October 2020. Available online: <https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.3.0.pdf> (accessed on 21 February 2024).
40. Opendaylight Controller. Available online: https://wiki.opendaylight.org/view/OpenDaylight_Controller:Overview (accessed on 21 February 2024).
41. IEEE Std. 802.1D-2004; Media Access Control (MAC) Bridges. IEEE: New York, NY, USA, 2004.
42. IEEE Std. 802.1Q-2011; Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks. IEEE: New York, NY, USA, 2011.
43. Available online: <https://arxiv.org/abs/2112.11324> (accessed on 21 February 2024).
44. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges. *Comput. Netw.* **2022**, *216*, 109246. [CrossRef]
45. Muthukrishnan, A.; Charles Rajesh Kumar, J.; Vinod Kumar, D.; Kanagaraj, M. Internet of image things-discrete wavelet transform and Gabor wavelet transform based image enhancement resolution technique for IoT satellite applications. *Cogn. Syst. Res.* **2019**, *57*, 46–53. [CrossRef]

46. Available online: <https://www.nics.nat.gov.tw/EDR.htm> (accessed on 21 January 2024).
47. Sturdivant, R.L.; Yeh, J.; Stambaugh, M.; Zahnd, A.; Villareal, N.; Vetter, C.K.; Rohweller, J.D.; Martinez, J.F.; Ishii, J.M.; Brown, R.A.; et al. IoT enabled pico-hydroelectric power with satellite back haul for remote himalayan villages. In Proceedings of the IEEE Topical Workshop on Internet of Space (TWIOS), Anaheim, CA, USA, 14–17 January 2018; pp. 5–8. Available online: https://www.researchgate.net/publication/323714221_IoT_enabled_pico-hydro_electric_power_with_satellite_back_haul_for_remote_himalayan_villages (accessed on 21 February 2024).
48. Available online: <https://www.mitre.org> (accessed on 21 February 2024).
49. Ball, F.; Basu, K. Analysis of the Suitability of Satellite Communication for Time-Critical IoT Applications in Smart Grid and Medical Grade Networks. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Proceedings of International Conference on Wireless and Satellite Systems, Oxford, UK, 14–15 September 2017*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 231, p. 231.
50. Sturdivant, R.L.; Lee, J. Systems engineering of IoT connected commercial airliners using satellite backhaul links. In Proceedings of the IEEE Topical Workshop on Internet of Space (TWIOS), Anaheim, CA, USA, 14–17 January 2018; pp. 1–4.
51. Available online: <https://d3fend.mitre.org> (accessed on 21 February 2024).
52. Palma, D.; Birkland, R. Enabling the Internet of Arctic Things with Freely-Drifting Small-Satellite Swarms. *IEEE Access* **2018**, *6*, 71435–71443. [[CrossRef](#)]
53. Qu, Z.; Zhang, G.; Cao, H.; Xia, J. LEO satellite constellation for Internet of Thing. *IEEE Access* **2017**, *5*, 18391–18401. [[CrossRef](#)]
54. Available online: <https://www.rsyslog.com/> (accessed on 21 February 2024).
55. Huang, H.; Guo, S.; Liang, W.; Wang, K. Online Green Data Gathering from Geo-Distributed IoT Networks via LEO Satellites. In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
56. RFC 3164—The BSD Syslog Protocol. Available online: <https://datatracker.ietf.org/doc/html/rfc3164> (accessed on 21 February 2024).
57. Hills, A. Large-scale wireless LAN Design. *IEEE Commun. Mag.* **2001**, *39*, 98–107. [[CrossRef](#)]
58. Kamenetzky, M.; Unbehauen, M. Coverage planning for outdoor wireless LAN systems. In Proceedings of the 2002 IEEE International Zurich Seminar on Broadband Communications, Zurich, Switzerland, 19–21 February 2002; pp. 49–1–49–6.
59. Chuang, Y.S. Zigbee Research and Implementation in the Wireless Sensor Network. Master’s Thesis, Graduate Institute of National Taiwan University of Science and Technology, Taipei, China, 2005; pp. 12–14.
60. Chen, H.F. Context-Aware Services Based on ZigBee Wireless Sensor Network. Master’s Thesis, Graduate Institute of Computer and Communication Engineering, National Cheng Kung University, Tainan, China, 2007; pp. 11–14.
61. Wang, C.T. IEEE 802.11 WLAN Access Point (AP) Deployments. Master’s Thesis, Graduate Institute of National Central University, Taoyuan, China, 2003; pp. 15–20.
62. Google Map. Available online: <http://maps.google.com.tw/> (accessed on 21 February 2024).
63. Ding, J.H. Localization in Zigbee-based Sensor Networks. Master’s Thesis, Graduate Institute of National Tsing Hua University, Hsinchu, China, 2006; pp. 23–24.
64. Bahl, P.; Padmanabhan, V.N.; Balachandran, A. Enhancements to the RADAR User Location and Tracking System, MSR-TR-00-12, Microsoft Research Technical. 2000. Available online: <https://www.microsoft.com/en-us/research/publication/enhancements-to-the-radar-user-location-and-tracking-system/> (accessed on 21 February 2024).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.