BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF ELECTRICAL ENGINEERING
AND COMMUNICATION

DEPARTMENT OF RADIO ELECTRONICS

ADVANCEMENTS IN ULTRA-HIGH FREQUENCY COMMUNICATIONS

HABILITATION THESIS

AUTHOR Ing. Aleš Povalač, Ph.D.

BRNO 2023

To my beloved wife Iva and our wonderful children Alfréd, Hubert, and Žofie.

Contents

1 Introduction

In an era characterized by rapid technological progress, the intersection of electronics, communication, and space technologies shows significant potential for altering perceptions of connectivity, data, and space communication. An increasingly interconnected world necessitates effective, efficient, and far-reaching communication capabilities. This work explores the domains of Ultra-High Frequency (UHF) Radio-Frequency Identification (RFID), Low-Power Wide-Area Networks (LPWANs), and nanosatellite electronics, aiming to expand the horizon of communication and push its boundaries beyond Earth.

This thesis offers an exploration of my recent research years, providing both a comprehensive overview and a detailed examination of each distinct area. While the subjects vary greatly, they are bound by a common theme: the continuous pursuit of innovation and refinement of current technologies for a more connected future in the UHF band.

The structure of this thesis is carefully designed to stitch together research contributions, offering a clear and comprehensive overview of my academic work. Each section illuminates different technological areas, shaped by both collaborative and individual efforts. Moreover, the included appendix details educational contributions, scientific projects, and outreach activities. This is complemented by abstracts of selected projects and papers that constitute the foundation of my research journey.

1.1 The Significance of the UHF Band

The Ultra-High Frequency (UHF) band, spanning frequencies between 300 MHz and 3 GHz, serves as a critical link that connects the distinct realms of RFID, LPWANs, and nanosatellites. Its significance is deeply rooted in its unique physical properties and its historic and evolving applications in the field of communication.

The UHF band gained prominence with its use in television broadcasting, establishing it as a fundamental component of mass communication. Its ability to penetrate through obstacles, such as buildings and foliage, made it a preferred choice for various applications, particularly in urban and densely populated settings. As technological paradigms evolved, the UHF band adopted new roles, extending from mobile communication to the realms of IoT.

The significance of the UHF, notably the 433 MHz and 868 MHz subbands, becomes more apparent through this work. Its favorable propagation characteristics make it suitable for RFID systems that require dependable communication in the presence of potential interferences. For LPWANs, specifically LoRaWAN, the UHF band supports long-range transmissions with low power consumption. Similarly, in the vastness of space, nanosatellites utilize this band to ensure robust communication with ground stations.

1.2 Scope of the Thesis

The thesis presents a comprehensive exploration of RFID, LPWANs, and nanosatellite communications within the UHF band. Chapter 2 elucidates the evolution and principles of UHF RFID. Chapter 3 expands the scope to encompass LPWANs, providing an in-depth view of technologies such as LoRaWAN and the prevailing challenges. Chapter 4 investigates the intersection of nanosatellites and UHF communication in space. The concluding Chapter 5 integrates the insights, drawing overarching conclusions.

In addition, each chapter is supplemented by information on related projects, applied results, and publications, which are extensively documented in the appendices and bibliography. These references are intended to place my work in the context of the research and findings presented in the thesis.

Supplementary content is provided in the appendices. Appendices A and B provide an account of my academic journey, encompassing teaching, efforts aimed at popularization, and research projects. Appendix C emphasizes the applied results, presenting the tangible outputs of my research.

In Appendix D, careful consideration was applied in the selection of papers. The first two are conference journals on UHF RFID ranging, distinguished by their high citation count in the Scopus database. The following papers are journal articles indexed in the esteemed Web of Science in the SCIE collection. Joint work with TU Delft explores nanosatellite bus architectures. A specific study focuses on the unique attributes of the UHF channel sounder. Two articles examine LoRaWAN, with the second featuring lead authorship in a Q2 ranked journal. The final article, a Q1 ranked piece, encapsulates international collaborative efforts on a scientific nanosatellite and the capability to participate in such a substantial project.

2 Concepts and Evolution in UHF RFID

2.1 History and Evolution of RFID

The history and evolution of Radio-Frequency Identification (RFID) technology encompasses decades of scientific research, commercial applications, and ongoing advancements. Its roots lie in radar identification systems used during World War II, with early developments in RFID aimed at differentiating friendly aircraft from enemy ones [1]. Commercial RFID applications began to appear in the late 1970s and 1980s, predominantly using Low-Frequency (LF, 125–134 kHz) and High-Frequency (HF, 13.56 MHz) bands with inductive coupling for diverse applications (Fig. 2.1), including animal tracking and access control.

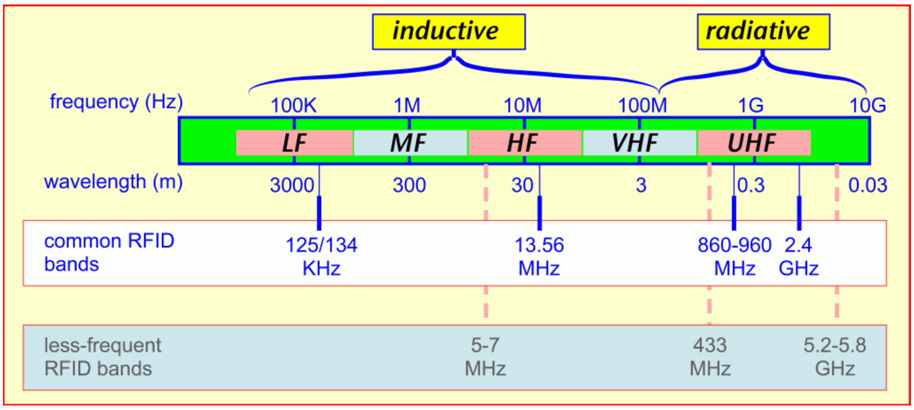


Fig. 2.1: Overview of RFID communication bands with coupling type [1].

A significant turning point for RFID occurred with the introduction and widespread adoption of Ultra-High Frequency (UHF, 860–960 MHz) band technology, which employs radiative coupling. This shift, especially after the international acceptance of the EPC Gen2 standard, allowed passive RFID to extend the read range up to 12 meters under optimal conditions and increase data transfer rates. These enhancements facilitated bulk reading capabilities, leading to transformative changes in industries such as retail, logistics, and supply chain management.

2.2 Principles of UHF RFID

Related papers: [2]

The operation of RFID technology is primarily based on the backscattering principle [1]. In this process, an active device, often referred to as an interrogator or reader, initiates communication by transmitting a modulated RF signal toward an RFID tag. The tag receives this signal with its antenna. In the case of passive tags, this energy also powers their internal circuits. The tag modulates the impedance of its antenna in response, creating a "scatter" in the RF field. The interrogator detects this modulated backscatter and decodes it to retrieve the information or identification code carried by the tag.

The interrogator is a complex device often designed with multiple antennas to handle a variety of propagation issues, especially in the UHF band. It generates the radio frequency field that powers passive and semi-passive tags, enabling them to return data. The RFID tag consists of an antenna and an integrated circuit (IC). The antenna captures the RF energy from the interrogator, while the IC stores identification data and manages the logic required for communication.

RFID tags are primarily categorized into passive, semi-passive, and active types. Passive tags, without an internal power source, derive all their operational energy from the RF field emitted by the reader. These tags are cost-effective with an essentially unlimited operational life, but they offer limited read ranges—usually only a few meters in the UHF band. Semi-passive tags include a battery to power the internal electronics, but still use backscattering for communication with the interrogator. These tags have extended read ranges compared to passive tags and are often used in environments that require sensors or data loggers. Active tags, equipped with an internal battery, can initiate communication with the reader, as we examined in [2]. They have the longest read range, often exceeding 100 meters, but are more expensive and have a limited operational life due to their reliance on battery power.

2.2.1 Signal Propagation in UHF

Related projects: B.2, B.5, results: C.1, C.2, papers: [3, 4, 5, 6, 7]

The initiation of the backscatter radio link (Fig. 2.2) occurs when an interrogator emits a continuous wave (CW) signal to an RFID tag. The antenna of the tag captures this energy, utilizing it to power its integrated circuit. For information transmission back to the interrogator, the impedance of the tag's antenna is

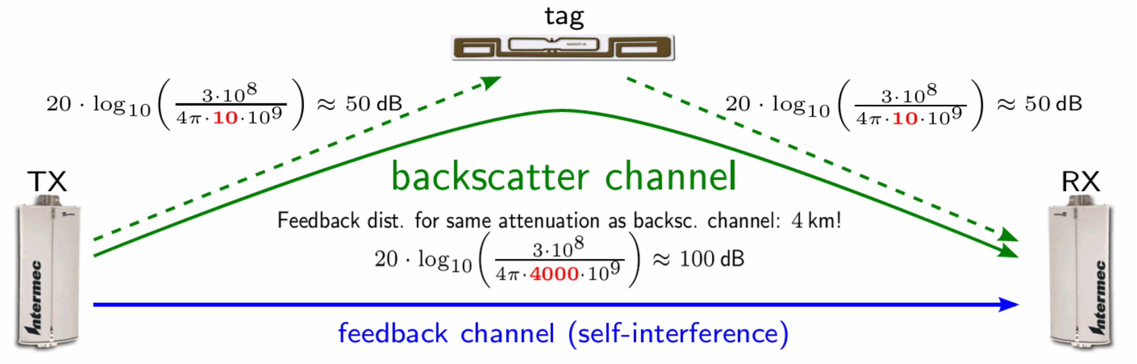

tag
$20 \cdot \log_{10}\left(\frac{3\cdot 10^8}{4\pi\cdot 10\cdot 10^9}\right) \approx 50$ dB
$20 \cdot \log_{10}\left(\frac{3\cdot 10^8}{4\pi\cdot 10\cdot 10^9}\right) \approx 50$ dB
TX
RX
backscatter channel
Feedback dist. for same attenuation as backsc. channel: 4 km!
$20 \cdot \log_{10}\left(\frac{3\cdot 10^8}{4\pi\cdot 4000\cdot 10^9}\right) \approx 100$ dB
feedback channel (self-interference)
Intermec
Intermec

Fig. 2.2: Signal propagation in a degenerated RFID channel [1]. The red numbers correspond to distance in the path loss formula, i.e. a backscatter channel with a distance of 20 m has a similar attenuation as a 4 km feedback channel.

altered, modifying the antenna's reflection coefficient [8]. In effect, the impedance discrepancy introduced by the tag results in the reflection of a portion of the incident CW signal back to the interrogator, carrying the tag's information along with it [3,9].

Although the backscattering principle appears straightforward, its practical application presents substantial difficulties, including the challenge of capturing the weak backscattered signal at the interrogator, which we addressed in [4, 5]. The interrogator must perpetually emit a high-power CW signal for tag activation and communication, while concurrently detecting a notably weaker backscattered signal close to its transmitted frequency [6]. This situation creates a significant sensitivity issue for the interrogator's receiver section, necessitating a well-devised isolation mechanism between the transmitted and received signals. Circulators, filters, and bistatic antennas are typically employed to address this issue, but attaining high isolation remains a formidable engineering task with significant influence on system performance, as we described in [7].

2.2.2 EPC Gen2 Protocol

The Electronic Product Code Class-1 Generation-2 UHF RFID Protocol, or EPC Gen2 for short, operates in the 860–960 MHz range and is a cornerstone in UHF RFID systems [10]. GS1 EPCglobal ratified this globally accepted standard, which lays the foundation for the physical and logical aspects of a passive backscatter RFID system and enables communication between RFID tags and interrogators. A defining feature of this protocol is the air interface specification, describing the essential modulation and demodulation processes for RF communication. The protocol supports various modulation schemes, including Double-Sideband Amplitude Shift Keying (DSB-ASK), Single-Sideband Amplitude Shift Keying (SSB-ASK), and Phase-Reversal Amplitude Shift Keying (PR-ASK). EPC Gen2 also provides different data rates for the forward and reverse links, adding flexibility in system design.

The EPC Gen2 standard incorporates framing and encoding rules, which determine the structure of data frames or communication blocks. The protocol prescribes the frame structure for commands, responses, and data, and allows the use of encoding schemes like FM0 and Miller encoding. These encoding methods optimize the read rate and range of RFID tags. The standard includes an efficient anti-collision mechanism, ensuring accurate identification of multiple tags in the reader's field. A "Query" command initiates the inventory round with a probabilistic slot-counter approach (Fig. 2.3). Each tag selects a random time slot to respond (an approach known as Slotted ALOHA [1]), minimizing collision likelihood and enabling efficient bulk reading.

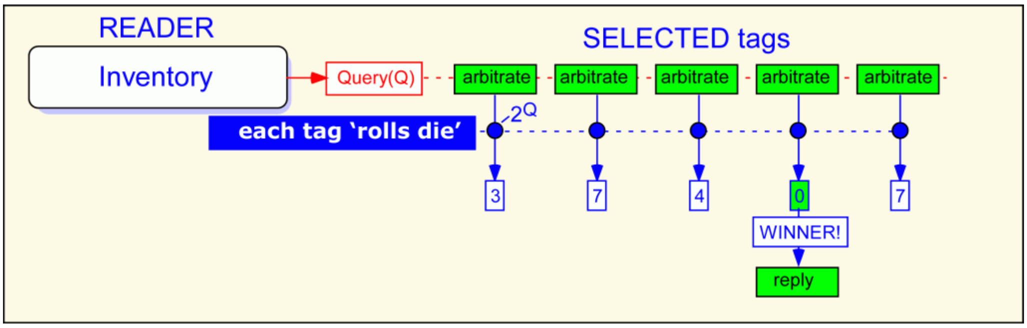


Fig. 2.3: Structure of the EPC Gen2 "Query" command [1].

The EPC Gen2 standard also addresses memory organization. Tags include multiple memory banks: *Reserved*, *EPC*, *TID*, and *User*. The *Reserved* memory holds critical access and deactivation passwords, while the *EPC* memory stores the identification code. The *TID* generally contains the tag's make and model, and the *User* memory may hold additional data. Password protection for these memory banks is possible, enhancing data security.

2.3 Software-Defined UHF RFID Radio

Related results: C.8, papers: [11, 12]

Software-Defined Radio (SDR) has emerged as a versatile tool in the realm of UHF RFID, enabling an array of customizations and innovations. Fundamentally, SDR facilitates the implementation of radio functions primarily in software, rather than hardware, providing increased flexibility. In an SDR-based UHF RFID structure (Fig. 2.4), the components reliant on hardware are reduced, with a majority of the processing executed in the digital domain [11, 13].

A monostatic arrangement is typically used in such systems, whereby the same antenna fulfills both transmitting and receiving functions. Signal splitters are utilized to distinguish the transmitted and received signals, facilitating concurrent operation. On the receiving (RX) path, the initial stage commonly includes a Low Noise Amplifier (LNA) which amplifies the weak incoming signals. This is succeeded by a filter purposed to eliminate out-of-band interference, after which an I/Q demodulator separates the signal into its in-phase (I) and quadrature (Q) components. Analog-to-Digital Converters (ADC) subsequently digitize these components for additional digital processing, where software algorithms execute tasks such as demodulation, decoding, and error correction.

On the transmission (TX) path, the originating signal is produced in the digital domain. A Digital-to-Analog Converter (DAC) transforms this digital signal into an analog form. Following this, an I/Q modulator merges the in-phase and quadrature

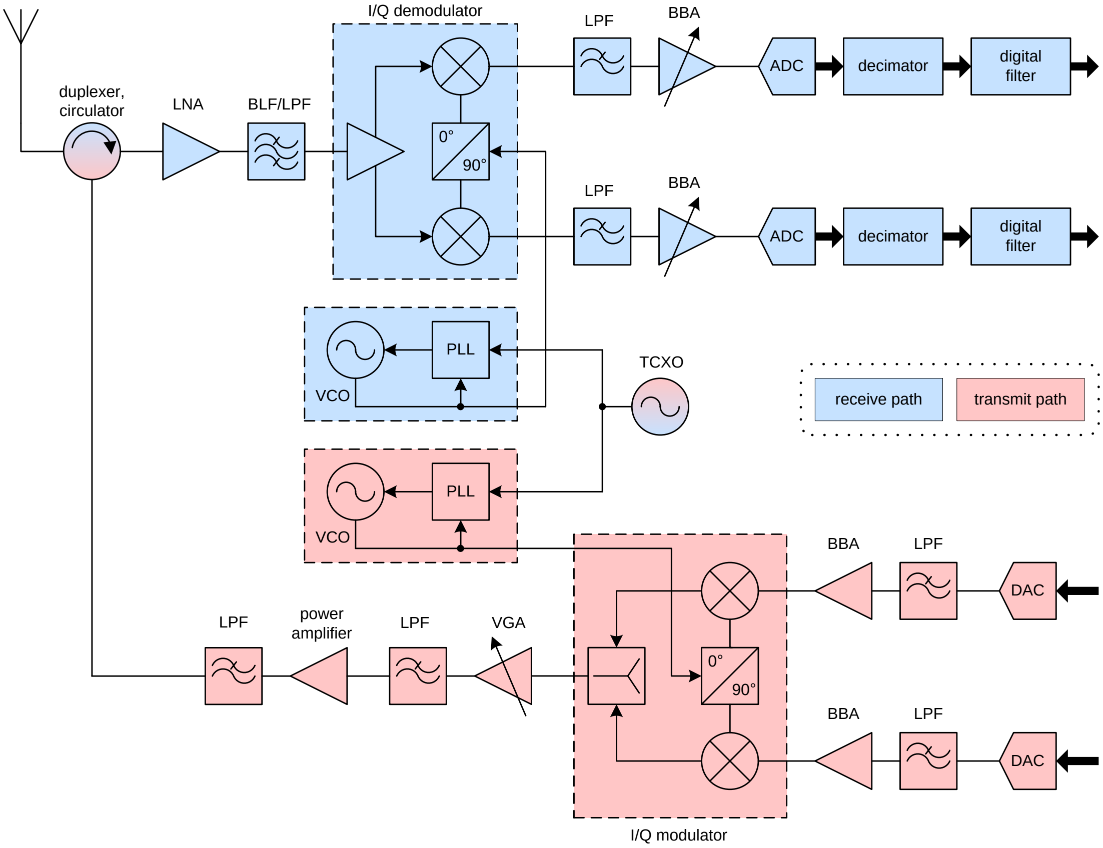


Fig. 2.4: I/Q transceiver architecture for a software-defined radio [12].

components, succeeded by a filter that shapes the signal to adhere to spectral requirements. Finally, a Power Amplifier (PA) enhances the signal prior to its transmission through the antenna.

Certain components are common to both RX and TX paths, influencing the overall system performance. A Temperature-Compensated Crystal Oscillator (TCXO) is often utilized as a stable clock source, and frequency synthesis techniques are employed to generate the various frequencies required for the system's operation.

Active carrier cancellation (Fig. 2.5) plays a crucial role in SDR-based RFID systems, particularly in a monostatic configuration [13]. As the same antenna is utilized for both transmission and reception, the received signal could be dominated by the powerful transmitted signal. Active carrier cancellation techniques are adopted to mitigate the effects of the transmitted carrier in the received signal, facilitating more precise and sensitive tag reading, as we described in [12].

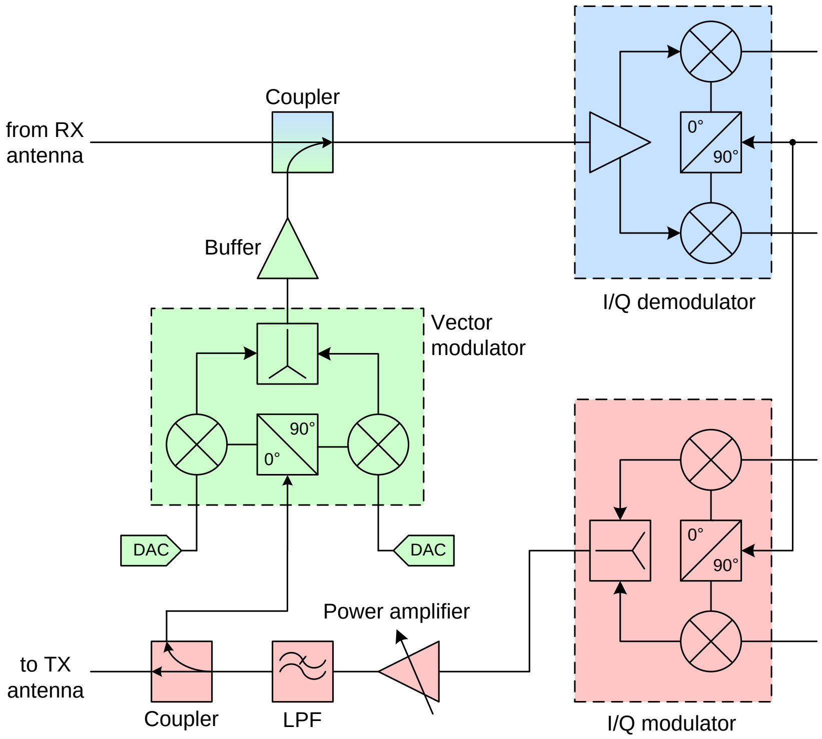


Fig. 2.5: Carrier cancellation by a destructive interference integrated in an SDR [12].

2.4 Ranging and Localization

Related projects: B.3, results: C.3, C.6, papers: [12, 14, 15, 16]

Ranging and localization are crucial in extending the capabilities of UHF RFID systems beyond mere identification [17]. The spatial position of a tag, when understood, bolsters the system's capabilities, becoming valuable for applications like asset tracking, navigation, and inventory management. A variety of techniques have been developed to meet these goals, generally falling into categories based on their underlying principles: ranging, angle, radio map matching, and proximity [18].

Triangulation, trilateration, and multilateration serve as fundamental principles typically invoked in localization (Fig. 2.6). Triangulation estimates the tag's location using the angles between the lines of sight from multiple known points. Conversely, trilateration uses the distances between known points and the tag to determine its location. While triangulation relies on angles, trilateration uses only distance measurements. Multilateration, an extension of trilateration, utilizes distance measurements from more than three points, thus improving accuracy.

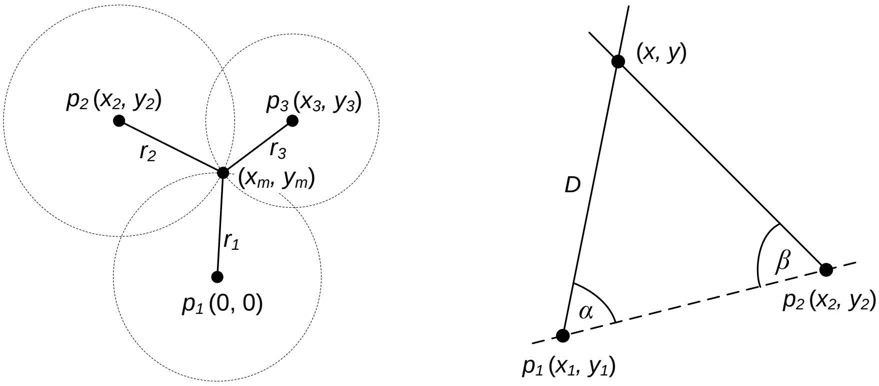


Fig. 2.6: Trilateration and triangulation positioning [12].

In the realm of ranging, various methods are used to estimate the distance between a tag and an interrogator. Among the simplest is the Received Signal Strength (RSS)-based method, where the distance is calculated based on the received signal power. However, RSS-based methods often face challenges due to multipath signal propagation, environmental noise, and interference. Time of Arrival (ToA) and Time Difference of Arrival (TDoA) methods calculate distance based on the time the signal takes to travel between the tag and the interrogator. While these methods generally offer more accuracy than RSS-based approaches, they are more complex to implement. Phase of Arrival (PoA) and Phase Difference of Arrival

(PDoA) methods, which use the phase of the received signal to estimate distance, can provide a potentially higher degree of accuracy under certain conditions [19]. We have significantly contributed to the research area of PDoA ranging in [12,14,15,16].

Angle-based methods typically employ the Direction of Arrival (DoA) principle, where the angle of the incoming signal relative to a reference is used to pinpoint the tag's location. Usually, multiple antennas or an antenna array are required for this technique, and it is often paired with ranging methods to improve accuracy.

Radio map matching techniques, often referred to as fingerprinting, utilize pre-collected data to construct a "map" of signal characteristics within an environment [20]. Real-time signal readings are subsequently matched with this map to localize the tag. Although this method can withstand environmental changes, it necessitates a comprehensive initial survey. Proximity methods, being the simplest, merely indicate when a tag is in close proximity to an interrogator. While not suitable for precise localization, they are effective for applications like doorway monitoring or basic asset tracking. These methods were also used in our project described in Appendix B.3, resulting in demonstrators presented in Appendix C.3 and Appendix C.6.

2.5 Future Directions

Related results: C.8, papers: [11, 12]

The evolution of UHF RFID technology in recent decades has facilitated transformative applications, particularly in logistics, retail, and supply chain management. Nevertheless, ongoing research seeks to broaden the capabilities and performance of these systems. This includes advancements in tag and reader hardware [12, 13], refinement of air interface techniques, and the application of software-defined radio principles [11].

A significant hardware challenge lies in enhancing the read range and reliability of passive UHF RFID tags, which currently achieve around 10 meters at their peak. Innovative antenna topologies, ICs with greater sensitivity, and techniques such as beamforming present potential improvements [18]. Moreover, the creation of hybrid active-passive tags may provide enhanced performance. On the reader side, mitigation of interference, isolation mechanisms, and cancellation of interference are critical areas that require further development.

In relation to the air interface, the optimization of modulation, encoding, and anti-collision protocols for specific applications remains a vibrant area of research. Real-time adaptation of parameters such as TX power, data rate, and Q-factor tuning contributes to reliable tag detection in dynamic environments. Further standardization and regional harmonization of UHF RFID bands also favor adoption.

SDRs open up various opportunities, including sophisticated interference emulation, over-the-air testing, and prototyping of non-standard scenarios, which we demonstrated with a device presented in Appendix C.8. Such SDR also enables functions such as coarse localization and sensing by facilitating channel characterization, determination of the angle-of-arrival, and phase-based ranging [22].

The rapid progression of UHF RFID is tied to the utilization of innovative hardware, the enhancement of communication strategies, and the application of software-defined radio principles. However, confronting challenges in tag sensitivity, interference, localization, and real-time adaptation requires concentrated research efforts.

3 Exploring LPWANs in the UHF Band

3.1 Introduction to LPWANs

Low-Power Wide-Area Networks (LPWANs) represent a significant transformation in wireless communications, especially for Internet of Things (IoT) applications (Fig. 3.1). IoT ecosystems increasingly necessitate interconnected devices to oversee, control, and automate a broad spectrum of functions, from industrial machinery and agricultural systems to home automation and healthcare apparatus. These devices often require long-term operation on minimal power while demanding extensive geographic coverage [23].

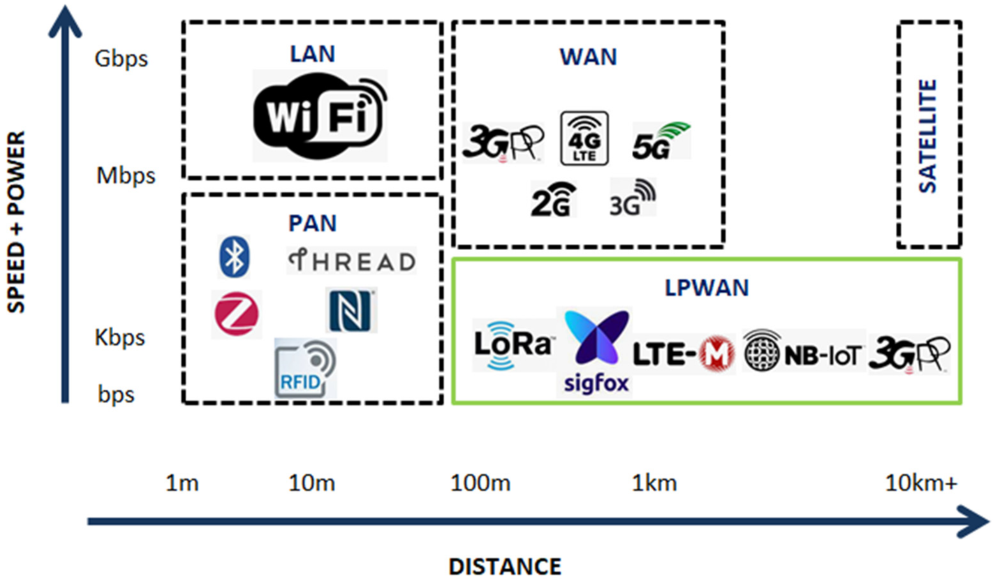


Fig. 3.1: LPWAN compared with the other existing technologies [24].

LPWANs operate at sub-GHz frequencies, taking advantage of better signal propagation characteristics compared to higher-frequency bands. These networks are designed to simultaneously optimize power consumption and spectral efficiency, employing techniques such as spread spectrum modulation and adaptive data rate selection to ensure robustness against interference and facilitate multiple devices' coexistence within the same network [25]. Technologies like LoRaWAN, Sigfox, and NB-IoT present a powerful combination of long-range communication up to tens of kilometers, low-power operation, and the ability to accommodate a large number of nodes. These attributes identify LPWANs as a key technology for IoT applications that demand long battery life, extended reach, and scalability.

3.2 LoRaWAN and Other LPWAN Technologies

Related projects: B.3, results: C.7, papers: [2, 26]

LoRaWAN (Long Range Wide Area Network) is a specific protocol and architecture for LPWANs, built upon the LoRa (Long Range) modulation (Fig. 3.2). Its flexibility is notable, providing various classes of service to accommodate the diverse needs of IoT applications [25]. Unlike other LPWAN technologies, such as Sigfox and Narrowband IoT (NB-IoT), LoRaWAN functions in unlicensed frequency bands and is often commended for its low power consumption, relatively high data rate, and open architecture that fosters a more expansive ecosystem. Although Sigfox is also power-efficient, it typically allows fewer transmitted bytes and is considered more appropriate for applications that transmit very small and infrequent data bursts. Conversely, NB-IoT operates in licensed bands and is often incorporated into existing cellular networks, making it more suitable for applications necessitating higher quality of service guarantees at the potential cost of increased power consumption. Thus, the selection among these technologies hinges on a project's specific needs, such as data rate, range, battery life, and scalability, but LoRaWAN frequently excels due to the balance it strikes among these attributes and its broad applicability in a variety of IoT applications [27].

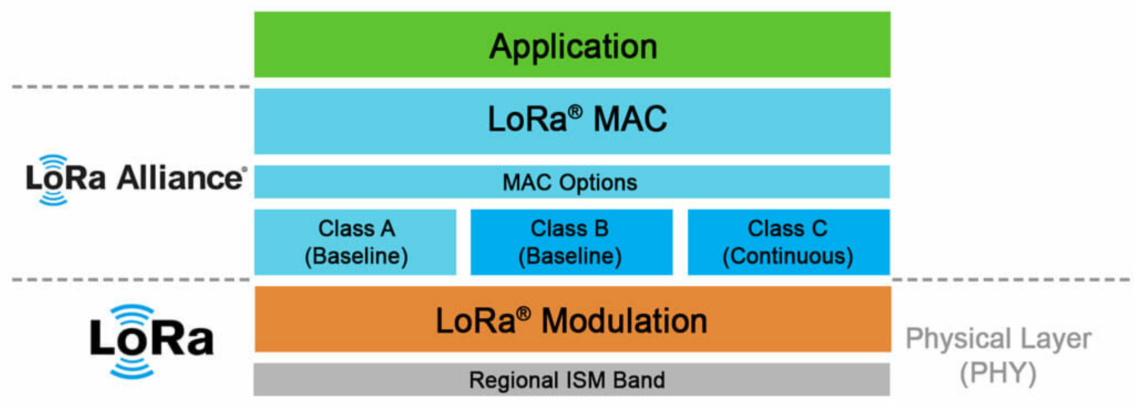


Fig. 3.2: Physical and Communication layers of a LoRaWAN Network [28].

LoRaWAN is a media access control (MAC) layer protocol designed for large-scale public networks. It depends on the LoRa physical layer and includes features such as adjustable data rates, two-way communication, and multiple device classes, making it adaptable for a range of applications, as de demonstrated in [26]. With a typical RF power constraint of 25 mW, LoRaWAN supports a communication range of up to 5 km in urban settings. These diverse capabilities have led to its widespread adoption across various sectors, placing it as a key component in the evolving IoT landscape.

The physical layer of LoRa employs a unique modulation scheme known as Chirp Spread Spectrum (CSS). This method improves long-distance communication and resilience to narrow-band disruptions by disseminating the information signal across a wider bandwidth [29]. LoRa modulation is characterized by its spreading factors (SF). The spreading factor represents the degree of spreading code applied to the original data signal. Basic LoRa includes six such factors, from SF7 to SF12, with a larger factor indicating a signal's enhanced ability to travel further without errors.

LoRaWAN classifies devices into three distinct classes——A, B, and C——to accommodate different application needs and power constraints [30]. Class-A devices, being the most energy-efficient, are optimal for use cases requiring sporadic communication, featuring short receiving windows after each transmission. Class-B devices strike a balance between downlink latency and power usage by synchronizing with network beacons and using timed receive slots. Class-C devices prioritize downlink latency minimization at the cost of energy efficiency, keeping receive windows open for near-instantaneous communication. Furthermore, end devices utilize a random access transmission approach known as ALOHA, allowing them to communicate without the need to be paired with a specific gateway.

The LoRaWAN Class-A communication was engaged in our project described in Appendix B.3, resulting in a communication system prototype presented in Appendix C.7 and [2].

3.3 Traffic Monitoring

Related papers: [31, 32]

The importance of real-world, quantitative data for understanding network environments and deployments is recognized in the IoT research community [33, 34, 35]. In line with this understanding, we collected and analysed an extensive dataset of LoRaWAN traffic from four European locations, employing a custom-built hardware sniffer [31]. The design of this sniffer is publicly accessible online. Distinguishing our open dataset [32] is the inclusion of uplink, downlink, and Class-B traffic, which expands the scope of what previous datasets offer. Wireshark's LoRaWAN decoding capabilities were also enhanced to facilitate analysis. The sniffer, operating autonomously when connected to a power source, captures all LoRaWAN traffic in accordance with the EU868 frequency plan, including the RX2 channel. It is capable of both uplink and downlink reception, which exhibit differing chirp signal polarities at the physical LoRa layer, and can receive Class-B beacons transmitted on the RX2 channel.

3.3.1 EU868 Channel Plan

LoRaWAN operates in the unlicensed radio band, comparable to Wi-Fi, thus allowing usage without the requirement of licensing fees. However, its radio frequencies necessitate region-specific regulations, resulting in slightly varied implementations across different parts of the world. To address these variations, the LoRa Alliance has developed a Regional Parameters document [36]. These parameters provide a common basis for channel plans, data rates, and other settings, but also accommodate country-specific variations and additional customization by network server operators.

The focus here is on the EU863–870 band (commonly referred to as EU868), which is regulated by the ETSI standard, and is widely used in European countries and even some outside Europe [37]. This UHF band includes three default channels for end devices to send join messages, with frequencies of 868.1 MHz, 868.3 MHz, and 868.5 MHz. The specification allows for a total of up to 16 channels. Although the default ones cannot be modified in devices compliant with LoRaWAN version 1.0.x, changes can be implemented in newer versions. Additional channels and specific frequencies for downlink are also in use, especially by networks such as The Things Network. A typical channel plan is shown in Fig. 3.3.

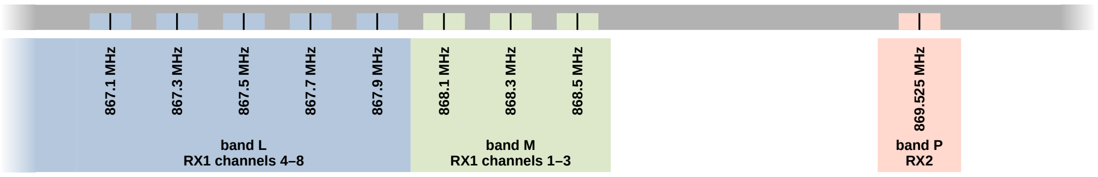


Fig. 3.3: LoRaWAN EU868 channels [31].

3.3.2 Encryption and Security

Related papers: [31, 38]

LoRaWAN packets are typically partially encrypted, with decryption keys unavailable to devices that might intercept the communication, as we explained in [38]. However, certain attributes of LoRaWAN transmissions remain analyzable without these keys [30]. Unencrypted fields in a LoRaWAN packet include:

- **Message Header (MHDR)**: Contains information on the message type (MType) and the version of LoRaWAN in use.
- **Device Address (DevAddr)**: A unique 32-bit identifier that differentiates an end device within a specific network.
- **Frame Control (FCtrl)**: Provides details such as the Adaptive Data Rate (ADR), Frame Options length, and extra control flags.
- **Frame Counter (FCnt)**: A 16-bit counter that grows with each uplink frame, providing protection against replay attacks.
- **Frame Options (FOpts)**: Contains optional MAC-level commands.
- **Frame Port (FPort)**: Designates the port number for application-specific or MAC layer interactions.

Both the application payload (FRMPayload) and the Message Integrity Code (MIC) are encrypted in uplink and downlink packets, requiring the corresponding keys for decryption and verification.

LoRaWAN includes two activation methods: OTAA (Over-the-Air Activation) and ABP (Activation By Personalization). OTAA involves an end device sending an encrypted *Join Request* with a pre-set AppKey. The network server validates this request, generates session keys (NwkSKey for MIC and AppSKey for payload), and returns a *Join Accept* message, which includes the allocated DevAddr. Tools like Wireshark can decrypt these packets for detailed analysis if provided with the right keys. Conversely, ABP circumvents the need for a join procedure by pre-loading the end device with session keys and a DevAddr, potentially increasing security risks if the same keys are used for prolonged periods.

Maintaining the confidentiality of encryption keys is crucial, as our study [31] has demonstrated that exposed keys are exploited in active LoRaWAN networks. For instance, Semtech's default key (`2B7E151628AED2A6ABF7158809CF4F3C`) [35] was found in use by RisingHF devices in the Brno region as the AppKey for OTAA activation. A significant number of packets from ABP-activated devices also used this key for both NwkSKey and AppSKey. The Milesight default key (`5572404C69-6E6B4C6F52613230313823`) [39] was found in OTAA-activated devices in various locations, including Vienna, Brno, and Liege, primarily on The Things Network

(TTN). If an unauthorized party captures the complete *Join Request* and *Join Accept* pair, they could compute both the NwkSKey and AppSKey, fully decrypting the communication stream for the affected device. Such key exposure carries substantial security implications, threatening data integrity and confidentiality.

3.4 Research Challenges

Related projects: B.1, papers: [2,31,38]

Despite its increasing popularity and adoption, LoRaWAN encounters several challenges. These challenges have guided various research trends:

- **Scalability and Capacity**: As the number of IoT devices in use rises, it becomes crucial to ensure that LoRaWAN can manage this increase without a decline in performance. Hence, research dedicated to optimizing network capacity holds significant importance [27,38].
- **Security**: In light of escalating threats in the digital sphere, securing LoRaWAN networks is a pressing concern. Strategies to mitigate potential vulnerabilities, ranging from device authentication to advanced cyber-attacks, represent a primary research focus [31,40].
- **Energy Efficiency**: For IoT devices dependent on battery power, energy consumption is a vital consideration. Thus, further investigation into energy use reduction, from optimizing transmission power to refining sleep cycles, is necessary [2,27].
- **Quality of Service (QoS)**: Maintaining consistent and reliable data transmission in diverse environments, particularly urban areas with numerous obstructions, presents a challenge. Research aimed at enhancing QoS, through approaches like adaptive data rate algorithms, is of paramount importance [41].
- **Class-B in LoRaWAN**: Class-B devices in LoRaWAN provide a balance between Class-A's low power and Class-C's continuous connectivity. They enable scheduled receive windows, thus offering greater responsiveness than Class-A devices without the high power consumption of Class-C. Active research is underway to optimize the performance and application scenarios for Class-B devices [31].
- **IoT MESH Networks**: MESH networks, characterized by non-hierarchical device connections and data relay capabilities, offer redundancy and improved coverage. The integration of LoRaWAN with MESH networking principles has the potential to bolster network robustness, especially in challenging terrains

or dense urban environments [42]. Research in this area, presented also in the project described in Appendix B.1, centers on routing algorithms, energy efficiency, and scalability.

These domains encapsulate the primary challenges and research directions that will influence the future of LoRaWAN and its function within the IoT framework. As industries and cities become more interlinked, the advancements in LoRaWAN will have a significant impact in fostering innovation and ensuring dependable connectivity in an increasingly digital world.

4 Communication with Nanosatellites

4.1 Introduction to Nanosatellites

Related papers: [43, 44, 45]

The complexity and high expense of traditional satellites have been longstanding challenges. With the emergence of nanosatellites, also known as Cubesats or PocketQubes, satellite development has become more affordable and accessible, initially for university students and now increasingly for commercial applications [46].

A typical Cubesat consists of modular units, each of a standard size of 10×10×10 cm and a maximum weight of 1.33 kg. These units can be combined in multiples such as 1.5U, 2U, 3U, and so forth, to create a larger satellite structure, as illustrated in Fig. 4.1. While this design approach offers flexibility, it also imposes constraints of size and weight [47].

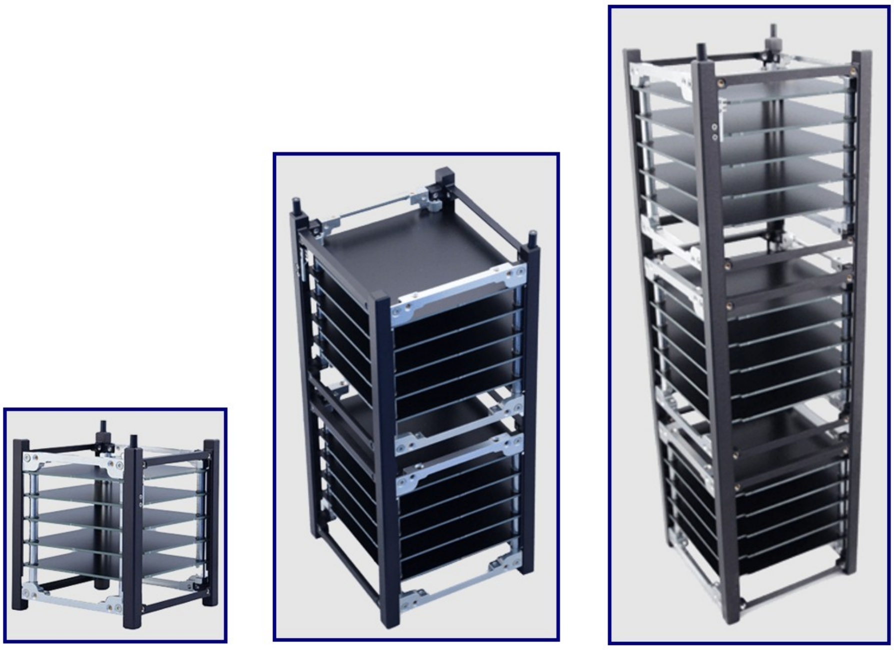


Fig. 4.1: Various sizes of Cubesat chassis.

The deployment of Cubesats involves a unit called the Poly-picosatellite Orbital Deployer (P-POD), which is integrated into the launch vehicle. The standardization brought about by this deployment method has significantly reduced launch costs by establishing fixed dimensions and features [48].

PocketQube is another, smaller format with dimensions of 5×5×5 cm and a weight limit of 0.25 kg. Like Cubesats, PocketQubes can be modular, with typical configurations such as 2P (5×5×10 cm, weight up to 0.5 kg). The miniaturization of electronics has been managed successfully; however, energy management presents a significant challenge. Despite this, PocketQubes are generally less expensive to launch than Cubesats [49].

Nanosatellites are typically deployed in Low Earth Orbit (LEO), which extends up to 2000 km from Earth. In practical terms, they usually operate within a height range of 200–800 km [50]. This orbit provides an orbital period of approximately 90 minutes and is the location of most artificial objects in space, including the International Space Station (ISS). The two main orbits for nanosatellites are the one based on the ISS and the heliosynchronous orbit.

Nanosatellites have found a broad range of applications, which can be grouped into three main categories. Firstly, they support scientific research by enabling remote observations of celestial bodies such as the Sun, Moon, and Earth. Maintaining position stabilization is a known challenge for these cost-effective units during precise observation missions. They also perform localized tests, such as temperature and electromagnetic field measurements, where directional accuracy is less crucial. Our recent research includes the detection of gamma-ray bursts [43, 44]. Secondly, nanosatellites have proven valuable for engineering tests, particularly hardware evaluation, as we presented in [45]. Commercial off-the-shelf (COTS) components are often used, especially in LEO applications, and have presented few problems. These satellites also enable experiments in fields such as propulsion, stabilization, and satellite networking. Lastly, nanosatellites have been used in artistic projects, merging technical data collection with artistic expression. For example, recorded radiation levels could be converted into sound or visual art, and some initiatives even involve sending unique art pieces into space.

4.2 Nanosatellite Electronics

Nanosatellite systems have emerged as a crucial component in space exploration and commercial applications. Central to their design and operation is the field of electronics, facilitating a range of functionalities from payload data collection to communication. This chapter delves into the distinct electronic subsystems of a typical nanosatellite, with a particular emphasis on areas such as the onboard computer (OBC), communication system (COM), electrical power system (EPS), attitude determination and control system (ADCS), and antenna release mechanisms [46].

4.2.1 Onboard Computing Systems

At the core of the nanosatellite lies the onboard computer (OBC). The OBC is instrumental in managing various operations of the satellite, including telemetry management and payload data collection [46]. The architecture of the OBC includes a main microcontroller, memory components, and communication interfaces. Technologies utilized range from Raspberry Pi or Arduino-based COTS systems to bare-metal C code operating on processors including Microchip AVR, TI MSP430, and ARM Cortex-M. Linux systems on hardware-optimized boards with enhanced reliability are also deployed for missions necessitating complex payload data processing.

OBC architectures can follow either a centralized or decentralized model. The centralized model, where all subsystems interact through the OBC, carries the risk of being a single point of failure, potentially threatening the entire mission if the OBC fails. Contrarily, decentralized architectures permit subsystems to communicate independently, increasing resilience despite the increased complexity of the setup.

Regarding robustness, components hardened against radiation (Fig. 4.2) are designed to resist radiation but are costly and generally not required for Cubesats. Redundancy serves as another strategy for enhancing reliability. An example of this is the use of dual OBCs, permitting automatic transition to a backup in the event of a malfunction.

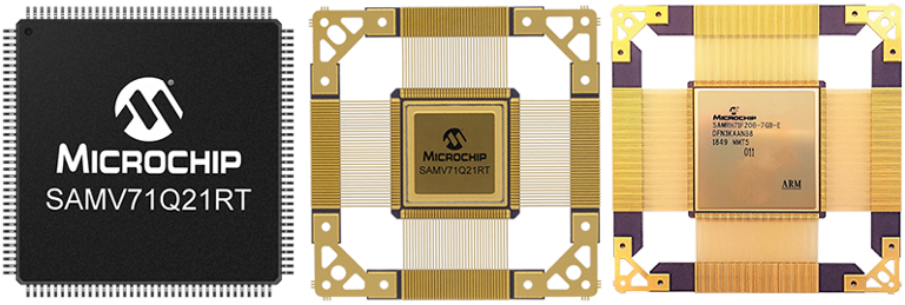


Fig. 4.2: Comparison of COTS and rad-hard component [51].

4.2.2 Communication Systems

Communication forms a critical component of any satellite mission. Nanosatellites frequently operate within VHF and UHF amateur radio bands, although for larger data transmission, L-band and S-band are employed [46]. While a significant number of nanosatellites are classified as amateur to access these frequencies, the increased commercial use of Cubesats is leading to regulatory challenges.

The transmission protocol typically employs direct frequency modulation at the physical layer or audio signal frequency modulation at standard speeds. Recent studies have investigated the use of LoRa modulation, which enables reception even below noise limits, albeit at slower transmission speeds [52]. Additionally, full-duplex linear transponders are sometimes used to enable ground station communication via the satellite.

Antennas used for communication often utilize shape-memory materials like nitinol or tape measures (Fig. 4.3). Deployment is usually achieved by melting a nylon wrap using a heating element. Redundant mechanisms are frequently implemented to mitigate potential failures. The design of communication transmissions must consider signal fading due to the satellite's rotation. As antennas typically function as dipoles, they possess a radiation minimum in one axis, resulting in periodic signal dropouts.

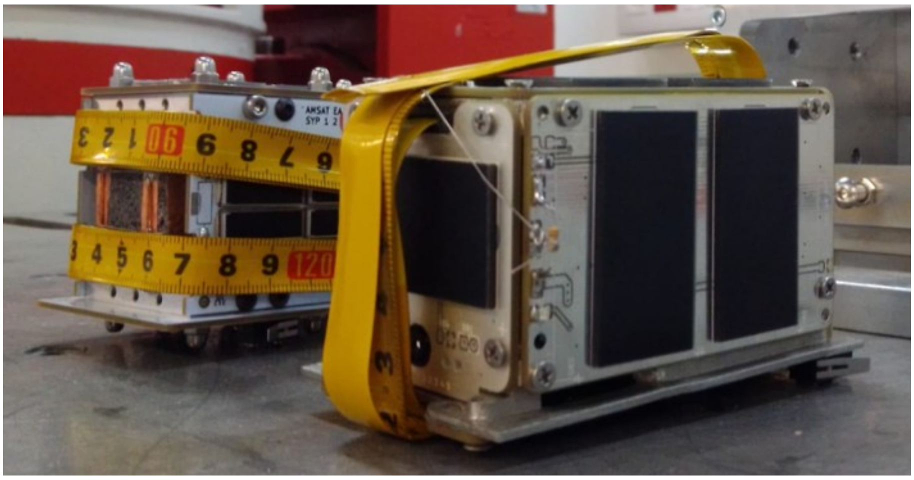


Fig. 4.3: Antennas from a tape measure on the HADES satellite.

4.2.3 Electrical Power Systems

The Electrical Power System (EPS) incorporates solar panels (Fig. 4.4) and batteries. GaAs-based triple-junction solar panels, achieving efficiencies close to 30%, remain commonplace despite their steep pricing [46]. The use of lithium-ion batteries is on the rise, although they necessitate complex management systems. More resilient battery technologies like NiCd and NiMH maintain their usage, given their space heritage and resilience to mishandling.

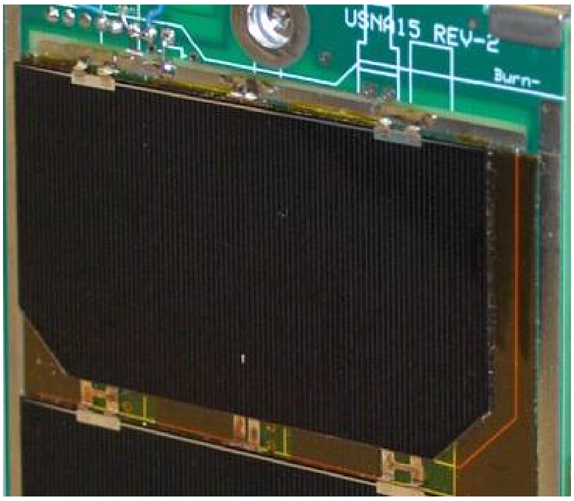


Fig. 4.4: Part of a solar panel on PSAT-2.

The EPS also comprises multiple power lines, typically 3.3V and 5V for digital electronics, and V_{bat} for amplifier output stages. Integrated monitoring and protections contribute to the system's resilience.

4.2.4 Attitude Determination and Control Systems

The Attitude Determination and Control Systems (ADCS) is critical for preserving the satellite's spatial orientation. The advent of MEMS technology has encouraged the use of magnetometers for this task. Stabilization might be passive, utilizing a permanent magnet, or active, using reaction wheels or magnetorquers. While complex systems leverage torque rods for adjustments, basic designs frequently depend solely on passive stabilization [46].

4.3 Internal Satellite Connections

Related papers: [53]

Compact nanosatellites, such as Cubesats and PocketQubes, depend on complex internal communication systems for efficient operation. These systems enable different subsystems within the satellite to interact, exchange data, and carry out commands [54]. Four dominant communication interfaces used in these satellites include RS-485, I2C, UART, and CAN.

- **RS-485**: A serial communication standard employing differential signaling, it provides robustness against electrical noise. It's utilized for its capacity to facilitate reliable long-range communication. RS-485 is useful for UART communication, offering an industrial-grade yet energy-consuming physical layer. Its differential characteristic ensures effective elimination of common-mode noise, crucial in harsh space environment.
- **I2C (Inter-Integrated Circuit)**: A synchronous bus system, I2C employs a clock and data line for communication. Despite its widespread use in satellite systems, it faces inherent problems. One significant issue with I2C is the possibility of bus lock-ups. These can occur when the master module resets during clock signal generation, causing slave modules to be stuck in a transaction [53]. The I2C standard does not have an inbuilt timeout, which can complicate matters. However, a variant, differential I2C (dI2C), provides a stronger physical layer, although it necessitates more wires and specialized driver circuits.
- **UART (Universal Asynchronous Receiver Transmitter)**: UART is an essential component in numerous microcontrollers and is utilized for asynchronous serial communication. As a point-to-point communication system that doesn't require a clock signal, it's simpler than I2C. In satellite applications, UART is frequently used for direct connections, particularly when interfaced with RS-485 for extended-distance communication.
- **CAN (Controller Area Network)**: Although CAN has an efficient physical layer, the higher protocol layers are more intricate due to its automotive sector targeting [53]. However, with appropriate libraries, CAN-based communication becomes a robust and refined solution. CAN is notably resilient to errors and offers fault confinement features, beneficial under the strict conditions of space. The CAN protocol enables multi-master operation and prioritizes messages, making it an excellent choice for systems requiring real-time capabilities.

The communication interface selection often hinges on the specific needs of the satellite mission. For example, the long-distance capability of RS-485 might be chosen for satellites where subsystems need to be placed at large distances, whereas the synchronous nature of I2C might be favored for compact systems where timing is essential.

Moreover, the integration of these communication systems comes with its own set of challenges. Ensuring compatibility between subsystems, particularly when sourced from different manufacturers, is vital. The PC-104 standard, popular in Cubesats, is based on a 104-pin connector system. Although it offers a sturdy connection, it isn't universally standardized across all satellites, leading to potential compatibility issues.

In [53], we stressed the need for a streamlined standard that fulfills future requirements. RS-485, for example, is often chosen for its good balance between power consumption and effective data throughput, outperforming other interfaces such as I2C and CAN under specific conditions (Fig. 4.5).

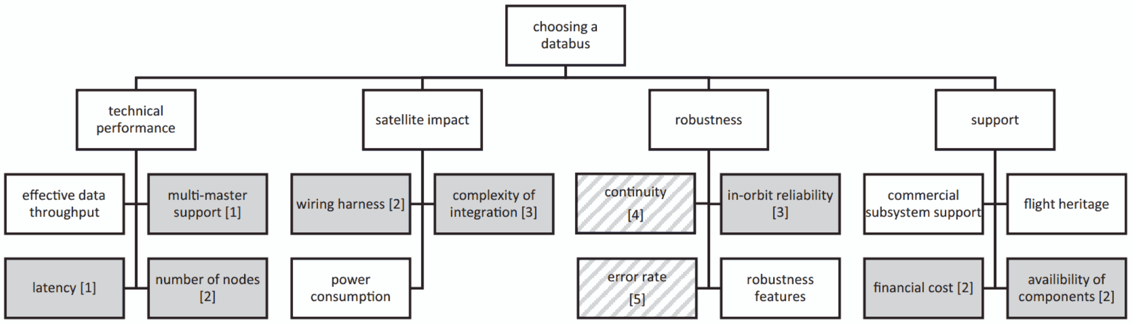


Fig. 4.5: Derivation tree for nanosatellite bus selection [53].

In conclusion, while RS-485, I2C, UART, and CAN each play a crucial role in satellite communication, the selection and implementation of each are contingent on the specific needs and limitations of the satellite mission. Guaranteeing robust, reliable communication while minimizing potential issues like bus lock-ups or incompatibilities is a key determinant of any successful satellite mission.

4.4 UHF Communication in Space

Related papers: [44]

The indispensability of radio communication in space missions cannot be overstated as it serves as the primary conduit for data transmission and command relay between satellites and terrestrial control centers. For nanosatellites, operating within the specific constraints of size and power, the selection of communication frequency is of critical importance. VHF (Very High Frequency) and UHF (Ultra High Frequency) have emerged as the frequencies of choice for these applications.

Space transmission primarily adopts a digital approach, where direct frequency modulation is employed at the physical layer [47]. Two modulations are notably prevalent among the standard speeds widespread in the amateur radio community:

- **AFSK (Audio Frequency Shift Keying)**: Typically used for 1200 Bd transmissions, AFSK modulates digital data into audio tones. Its popularity is due to its straightforward implementation and effectiveness, especially in environments with minimal noise interference.
- **FSK (Frequency Shift Keying) with G3RUH standard**: For higher speeds, specifically 9600 Bd, the G3RUH FSK modulation is utilized [55]. Named after its developer, this modulation provides a more robust solution for data transmission in space, ensuring clearer signals, even under challenging conditions.

At the L2 link layer, the AX.25 protocol is commonly used. This protocol enables a direct link between two points. A Terminal Node Controller (TNC) implements the protocol, serving as a bridge between the audio output of the transceiver and the data input of a computer. The TNC and the computer typically communicate using the KISS protocol.

Recently, research has explored LoRa modulation, a chirp-based modulation, which is a form of frequency keying. LoRa's unique capability allows for reception below the noise limit, resulting in high efficiency [52]. However, this efficiency sacrifices transmission speed, leading to prolonged transmission times.

Over the past decade, the Cubesat Space Protocol (CSP) has been adopted for use also in smaller Cubesats like GRBAlpha, as presented in our work [44]. Designed with a decentralization approach, this protocol treats individual components of a satellite as distinct nodes. Any node can be addressed, be it a conventional On-Board Computer (OBC) collecting data or another subsystem. Despite its more complex setup, the CSP's decentralized structure offers the advantage of maintaining some functionality if one of the subsystems fails.

In addition to digital transmission, full-duplex linear transponders are occasionally utilized. These transponders transpose a segment of the radio spectrum from one frequency band to another, enabling ground stations to communicate through the satellite with each other. Such systems are usually modulation independent.

The typical power output for a transmitter on a nanosatellite is around 1 W for Cubesats. In the case of PocketQube satellites, the power can be as low as hundreds of milliwatts. Given the mission-critical nature of communication, maintaining a reliable connection is essential. In terms of data budget, the VHF and UHF bands encounter limitations imposed by channel bandwidth. Speeds of 1200 Bd and 9600 Bd are feasible, making them suitable for telemetry and command, but not for transmitting larger data volumes, such as images.

4.4.1 Ground Stations

A ground station is equipped with several essential components for effective satellite communication. Antennas, typically with circular polarization, are mounted on an azimuth-elevation rotator (Fig. 4.6) that requires annual mechanical maintenance due to weather-induced wear. This rotator is controlled by a PC running satellite tracking software and is connected to a transceiver via a Terminal Node Controller (TNC).

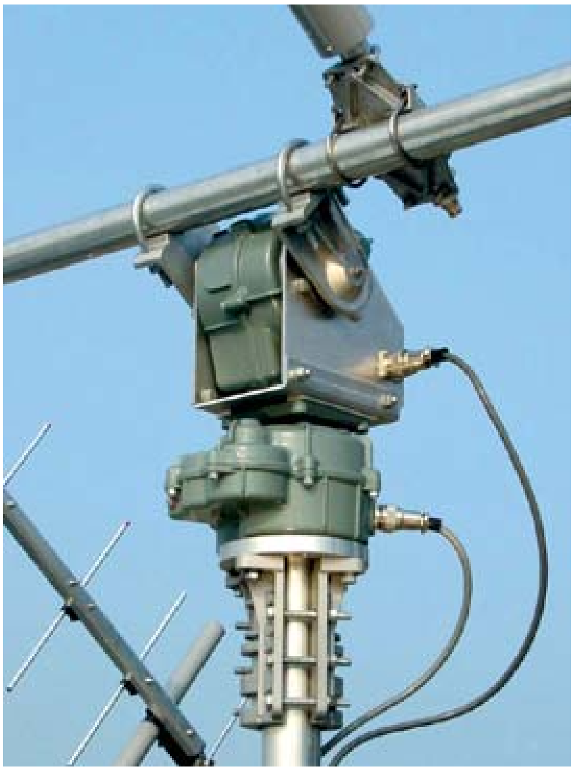


Fig. 4.6: Azimuth-elevation rotator.

Additional components like narrowband filters or Low Noise Amplifiers (LNAs) are often included to improve signal quality, especially over longer cable distances. For initial experiments, simpler ground-plane antennas can be used in place of rotators; these antennas offer variable gains based on the satellite's elevation.

The community network SatNOGS provides an open-source solution for satellite reception [56]. Full members with their own ground stations can schedule recording of satellite passes and even directly decode known telemetry. Overall, the ground station serves as a multifaceted hub for reliable satellite communication, requiring regular maintenance and offering various customization options.

4.5 Low-Cost Nanosatellite Imaging Using SSTV

Related results: C.4, C.5

Nanosatellites, due to their compact and cost-effective design, have introduced a new chapter in space exploration. Among their numerous applications, imaging using Slow-Scan Television (SSTV) has gained attention because of its unique methodology and broad acceptance in the radio amateur community [57].

SSTV operates by transforming static images into audio signals for radio frequency transmission. The transmission speed in SSTV is determined by the chosen mode. Various modes are utilized, such as Robot 36, which transmits an image in approximately 36 seconds, and Robot 72, taking 72 seconds. The selection of mode often strikes a balance between transmission speed and image resolution, with slower modes generally providing more detailed images.

An example of a cost-effective solution tailored for radio amateurs is the SatCam PQ, a compact imaging module that we specifically designed for nanosatellites, as presented in Appendix C.4. It incorporates the OV2640 camera module and is controlled by the STM32F446 microcontroller. With dimensions of 38×38 mm, it easily fits within PocketQube format satellites. The camera captures images and prepares them for transmission as SSTV audio.

The practical use of SatCam PQ is demonstrated in the PocketQube HADES mission, led by AMSAT-EA. Moreover, an earlier version of this module was integrated into the PSAT-2 Cubesat, a project of the US Naval Academy, together with a PSK transponder presented in Appendix C.5. This Cubesat not only employed the SSTV camera for imaging but also supported redundant telemetry, giving insights into various parameters like temperature, voltage, and light conditions.

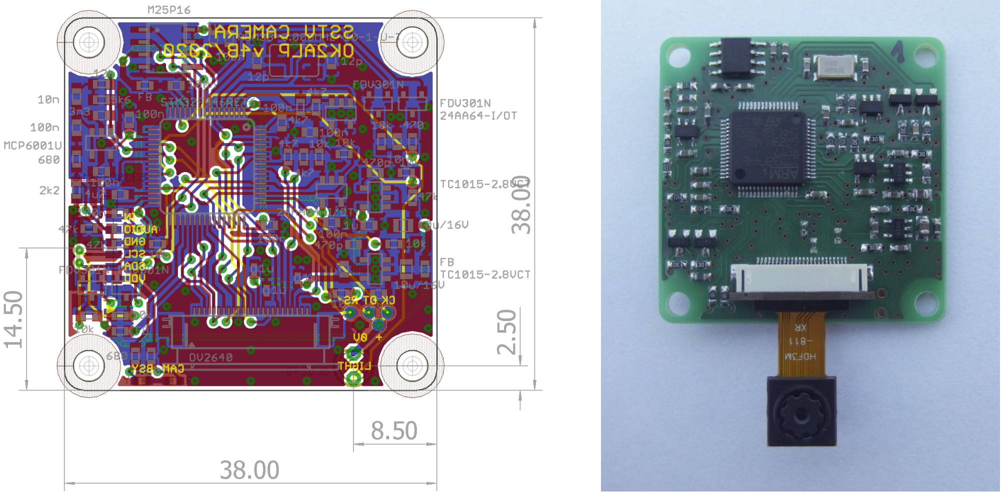


Fig. 4.7: SSTV camera for PocketQubes.

A considerable advantage of using SSTV for imaging in nanosatellites is its broad acceptance within the radio amateur community. As an established mode, SSTV is familiar to numerous radio enthusiasts. This familiarity ensures that images transmitted using SSTV from nanosatellites can be quickly identified, received, and decoded by anyone with the necessary knowledge and equipment. This open and cooperative approach not only encourages engagement but also ensures the transmitted data is accessible to a wide audience.

The integration of SSTV into nanosatellites demonstrates the potential of using established radio communication protocols in contemporary satellite technology. It represents the combination of tradition and innovation, enhancing the inclusivity and collaboration in space exploration and data acquisition.

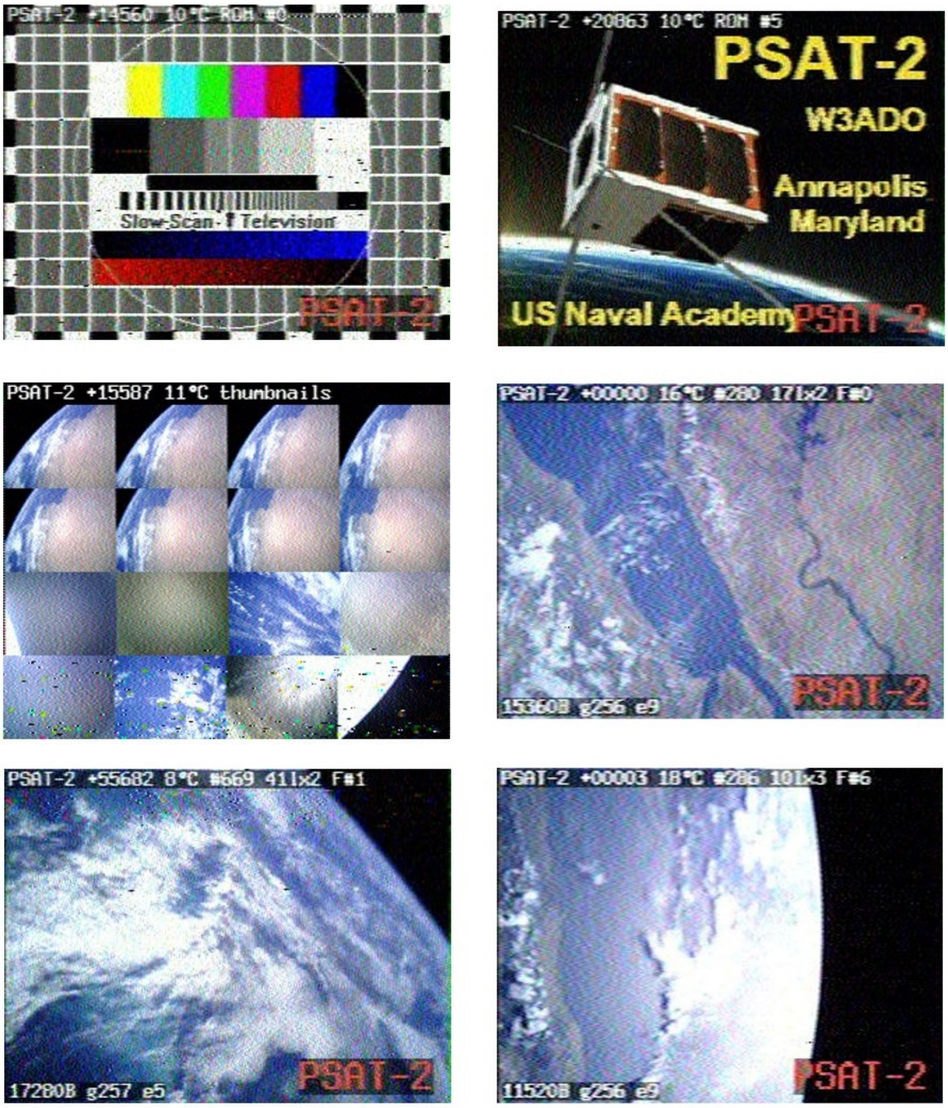

PSAT-2 +14560 10°C ROM #0
Slow-Scan Television
PSAT-2
PSAT-2 +20863 10°C ROM #5
PSAT-2
W3ADO
Annapolis
Maryland
US Naval Academy
PSAT-2
PSAT-2 +15587 11°C thumbnails
PSAT-2 +00000 16°C #280 171x2 F#0
15360B g256 e9
PSAT-2
PSAT-2 +55682 8°C #669 411x2 F#1
17280B g257 e5
PSAT-2
PSAT-2 +00003 18°C #286 101x3 F#6
11520B g256 e9
PSAT-2

Fig. 4.8: Images from the space transmitted by PSAT-2.

5 Conclusions

This habilitation thesis facilitates a comprehensive exploration of radio frequency communication technologies, bridging the distinct yet interconnected domains of RFID, LPWANs, and nanosatellite communication. The work serves as a nexus, integrating the research papers presented in Appendix D. These papers, previously published in peer-reviewed journals, represent the original scientific contributions, each illuminating a different aspect of the overarching research theme. Despite originating from various fields of application, the mentioned technologies coalesce within the UHF band, highlighting it as the integral theme connecting this research.

Chapter 2 provides an in-depth examination of UHF RFID systems. The historical evolution of RFID is traced, highlighting the significance of the emergence of UHF technology in transforming passive RFID capabilities. Fundamental operating principles centered around backscattering are clarified, accompanied by a detailed analysis of EPC Gen2, the globally accepted UHF RFID protocol. Ranging and localization methods are surveyed, pointing out the extended functionalities of RFID beyond identification. The flexibility imparted by software-defined implementations is also discussed.

Chapter 3 shifts focus to the growing field of LPWANs for IoT applications. LoRaWAN's design and adaptability are underlined, distinguishing it as a foremost LPWAN solution. Network monitoring activities yield quantitative datasets that address gaps and expand the pool of available real-world LoRaWAN data. Ongoing research challenges, from security to Class-B optimization, are highlighted as key directions guiding innovations in this domain.

The sphere of nanosatellite communication, an emerging frontier, is explored in Chapter 4. Cubesats and their electronic subsystems are characterized in detail. Communication protocols and ground station components tailored for nanosatellites in the UHF band are analyzed. Cost-effective SSTV imaging presents a novel application of UHF transmission from nanosatellites.

In conclusion, this thesis and its attachments offer an in-depth perspective on three advanced wireless communication technologies, examining their individual attributes as well as their convergence within the UHF frequency spectrum. It encompasses both a wide range of areas and a depth of technical investigation in each domain. The original contributions presented here, from LoRaWAN traffic monitoring to SSTV nanosatellite imaging, provide valuable insights that push the boundaries of knowledge and may guide future engineering endeavors. By bridging academic research with practical applied results, this thesis aims to highlight the pursuit of innovation that drives advancements in wireless communication systems.

Bibliography

[1] D. M. Dobkin. *The RF in RFID: Passive UHF RFID in practice*. Newnes, Burlington, MA (USA), 2007.

[2] A. Povalac, T. Mikulasek, and F. Zaplata. Ultra-low power identification in explosive environments. In *29th International Conference Radioelektronika – Microwave and Radio Electronics Week*, 2019.

[3] A. Povalac, K. Witrisal, and J. Sebesta. Degenerate RFID channel modeling for positioning applications. *Radioengineering*, 21(4):1163–1170, 2012.

[4] E. Kassem, J. Blumenstein, A. Povalac, J. Vychodil, M. Pospisil, R. Marsalek, and J. Hruska. Wideband UHF and SHF long-range channel characterization. *Eurasip Journal on Wireless Communications and Networking*, 188:1–16, 2019.

[5] Z. Raida et al. Communication subsystems for emerging wireless technologies. *Radioengineering*, 21(4):1036–1049, 2012.

[6] A. Povalac, M. Zamazal, and J. Sebesta. Firmware design for a multi-protocol UHF RFID reader. In *Proceedings of 20th International Conference Radioelektronika*, pages 199–202, 2010.

[7] M. Dusek, V. Derbek, A. Povalac, J. Sebesta, and R. Marsalek. Hardware and software stack for an SDR-based RFID test platform. In *4th International EURASIP Workshop on RFID Technology*, pages 41–45, 2012.

[8] A. Paulraj, R. Nabar, and D. Gore. *Introduction to Space-Time Wireless Communications*. Cambridge University Press, Cambridge, 2003.

[9] P. V. Nikitin and K. V. S. Rao. Antennas and propagation in UHF RFID systems. In *Proceedings of the IEEE International Conference on RFID*, pages 277–288, 2008.

[10] Class-1 Generation-2 UHF RFID protocol for communications at 860 MHz – 960 MHz, 2008. Version 1.2.0.

[11] M. Harvanek, V. Derbek, J. Kral, M. Pospisil, and A. Povalac. SDR Interference Emulator for RFID Applications. In *31st International Conference Radioelektronika*, 2021.

[12] A. Povalac. Spatial Identification Methods and Systems for RFID Tags. Dissertation thesis, Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Radio Electronics, Brno, 2012.

[13] R. Langwieser, G. Lasser, C. Angerer, M. Rupp, and A. L. Scholtz. A modular UHF reader frontend for a flexible RFID testbed. In *Proceedings of the International EURASIP Workshop on RFID Technology*, pages 1–12, 2008.

[14] A. Povalac and J. Sebesta. Phase of arrival ranging method for UHF RFID tags using instantaneous frequency measurement. In *ICECom: 20th International Conference on Applied Electromagnetics and Communications*, 2010.

[15] A. Povalac and J. Sebesta. Phase difference of arrival distance estimation for RFID tags in frequency domain. In *IEEE International Conference on RFID-Technologies and Applications*, pages 188–193, 2011.

[16] A. Povalac and J. Sebesta. Backscatter phase evaluation based on scatterplot cluster detection. In *24th International Conference Radioelektronika*, 2014.

[17] D. Arnitz. Tag localization in passive UHF RFID. PhD thesis, Graz University of Technology, Austria, 2011. `http://www.spsc.tugraz.at/sites/default/files/phdthesis-arnitz_online.pdf`. Accessed 2023-01-24.

[18] Y. Zhang, X. Li, and M. G. Amin. *RFID systems: Research trends and challenges*, chapter Principles and techniques of RFID positioning, pages 389–415. John Wiley & Sons, Chichester, 2010.

[19] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao. Phase based spatial identification of UHF RFID tags. In *Proceedings of the IEEE International Conference on RFID*, pages 102–109, 2010.

[20] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil. LANDMARC: Indoor location sensing using active RFID. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications*, pages 407–415, 2003.

[21] M. Fojtlin, J. Fiser, J. Pokorny, A. Povalac, T. Urbanec, and M. Jícha. An innovative HVAC control system: Implementation and testing in a vehicular cabin. *Journal of Thermal Biology*, 70:64–68, 2017.

[22] P. B. Kenington. *RF and Baseband Techniques for Software Defined Radio*. Artech House, Norwood, MA (USA), 2005.

[23] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials*, 19(2):855–873, 2017.

[24] N. Peladarinos, V. Cheimaras, D. Piromalis, K. G. Arvanitis, P. Papageorgas, N. Monios, I. Dogas, M. Stojmenovic, and G. Tsaramirsis. Early Warning Systems for COVID-19 Infections Based on Low-Cost Indoor Air-Quality Sensors and LPWANs. *Sensors*, 21(18):6183, 2021.

[25] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors*, 18(11):3995, 2018.

[26] R. Juran and A. Povalac. Field Sensor Network for Microclimatological Measurements. In *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, pages 149–153, 2020.

[27] F.S.D. Silva, E.P. Neto, H. Oliveira, D. Rosário, E. Cerqueira, C. Both, S. Zeadally, and A.V. Neto. A Survey on Long-Range Wide-Area Network Technology Optimizations. *IEEE Access*, 9:106079–106106, 2021.

[28] LoRa and LoRaWAN Timing. `https://ecsxtal.com/lora-lorawan-timing/`. Accessed 2023-09-19.

[29] Semtech. AN1200.22 LoRa™ Modulation Basics. `https://www.semtech.com/products/wireless-rf/lora-connect/sx1276`. Accessed 2023-05-02.

[30] LoRa Alliance. TS001-1.0.4 LoRaWAN® L2 1.0.4 Specification. `https://lora-alliance.org/resource_hub/ts001-1-0-4-lorawan-l2-1-0-4-specification/`, 2019. Accessed 2023-05-02.

[31] A. Povalac, J. Kral, H. Arthaber, O. Kolar, and M. Novak. Exploring LoRaWAN Traffic: In-Depth Analysis of IoT Network Communications. *Sensors*, 23(17):7333, 2023.

[32] A. Povalac and J. Kral. LoRaWAN Traffic Analysis Dataset. `https://doi.org/10.5281/zenodo.8090619`, June 2023.

[33] L. Bhatia, M. Breza, R. Marfievici, and J.A. McCann. LoED: The LoRaWAN at the Edge Dataset: Dataset. In *Proceedings of the Third Workshop on Data: Acquisition To Analysis*, page 7–8, New York, USA, 2020.

[34] M. Aernouts, R. Berkvens, K. Van Vlaenderen, and M. Weyn. Sigfox and LoRaWAN Datasets for Fingerprint Localization in Large Urban and Rural Areas. *Data*, 3(2):13, 2018.

[35] N. Blenn and F. Kuipers. LoRaWAN in the Wild: Measurements from The Things Network. `https://doi.org/10.48550/arXiv.1706.03086`, 2017. Accessed 2023-09-07.

[36] LoRa Alliance. RP002-1.0.3 LoRaWAN® Regional Parameters. `https://lora-alliance.org/resource_hub/rp2-1-0-3-lorawan-regional-parameters/`, 2021. Accessed 2023-05-02.

[37] ETSI EN 300 220-2 V3.2.1: Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for access to radio spectrum for non specific radio equipment. `https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf`. Accesed 2023-05-04.

[38] R. Fujdiak, K. Mikhaylov, J. Pospisil, A. Povalac, and J. Misurec. Insights into the Issue of Deploying a Private LoRaWAN. *Sensors*, 22(5), 2022.

[39] Milesight. 3D ToF People Counting Sensor User Manual. `https://www.milesight.com/static/file/en/download/datasheet/3d-tof/Milesight-3D-ToF-People-Counting-Sensor-User-Manual-en.pdf`. Accessed 2023-05-04.

[40] H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors*, 22(9):3127, 2022.

[41] J. Haxhibeqiri, F. Van den Abeele, I. Moerman, and J. Hoebeke. LoRa Scalability: A Simulation Model Based on Interference Measurements. *Sensors*, 17(6):1193, 2017.

[42] J.R. Cotrim and J.H. Kleinschmidt. LoRaWAN Mesh Networks: A Review and Classification of Multihop Communication. *Sensors*, 20(15):4273, 2020.

[43] J. Ripa et al. The peak flux of GRB 221009A measured with GRBAlpha. *A&A*, 677:L2, 2023.

[44] A. Pal et al. GRBAlpha: The smallest astrophysical space observatory – I. Detector design, system description, and satellite operations. *A&A*, 677:A40, 2023.

[45] M. Kosut and A. Povalac. CubeSat Demonstrator for Educational Purposes. In *Proceedings II of the Conference Student EEICT*, pages 176–179, 2022.

[46] C. Cappelletti, S. Battistini, and B. K. Malphrus, editors. *CubeSat handbook.* Academic Press, Amsterdam, 2021.

[47] G. Maral, M. Bousquet, and Z. Sun. *Satellite communications systems.* John Wiley & Sons, Hoboken, N.J., 2020.

[48] NASA. State-of-the-Art of Small Spacecraft Technology: Structures, Materials, and Mechanisms. https://www.nasa.gov/smallsat-institute/sst-soa/structures-materials-and-mechanisms/, 2023. Accessed 2023-11-01.

[49] NASA. CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers. https://www.nasa.gov/wp-content/uploads/2017/03/nasa_csli_cubesat_101_508.pdf, 2017. Accessed 2023-11-01.

[50] O. Popescu. Power Budgets for CubeSat Radios to Support Ground Communications and Inter-Satellite Links. *IEEE Access*, 5:12618–12625, 2017.

[51] Rad-hard ARM Cortex-M7 MCUs for Space. https://www.electronicsweekly.com/news/products/micros/rad-hard-arm-cortex-m7-mcus-space-2021-04/, 2021. Accessed 2023-09-19.

[52] L. Fernandez, J.A. Ruiz-De-Azua, A. Calveras, and A. Camps. Assessing LoRa for Satellite-to-Earth Communications Considering the Impact of Ionospheric Scintillation. *IEEE Access*, 8:165570–165582, 2020.

[53] J. Bouwmeester, S.P. van der Linden, A. Povalac, and E.K.A. Gill. Towards an innovative electrical interface standard for PocketQubes and CubeSats. *Advances in Space Research*, 62(12):3423–3437, 2018.

[54] J. Bouwmeester, M. Langer, and E. Gill. Survey on the implementation and reliability of CubeSat electrical bus interfaces. *CEAS Space Journal*, 9:163–173, 2017.

[55] T. A. Summers, J. Schmandt, E. Cheung, C. Gentry, and Y. Chen. Cost effective, flexible ground architecture using software defined radio and GNU Radio. In *Proceedings of the 32nd Annual AIAA/USU Conference on Small Satellites*, 2018.

[56] SatNOGS. SatNOGS Network. https://network.satnogs.org/, 2023. Accessed 2023-11-03.

[57] D. Selva and D. Krejci. A survey and assessment of the capabilities of Cubesats for Earth observation. *Acta Astronautica*, 74:50–68, 2012.

A Author’s Profile

This appendix offers a concise overview of the author’s professional background, focusing on three key areas: Teaching Experience, Supervised Theses, and Popularization Activities. Each subchapter delves into specific contributions and achievements within these areas.

A.1 Teaching Experience

The author’s tenure at Dept. of Radio Electronics involved active engagement in teaching, with a primary focus on master’s degree programs. The following sections describe notable teaching activities in various subjects.

Microcontrollers and Embedded Systems (MKS)

The Microcontrollers and Embedded Systems (MKS) course forms a central part of the author’s pedagogical efforts. This course is built upon two other courses––Microcontrollers for Advanced Applications (MIA) and Microprocessors with ARM Architecture (POA)––under the author’s responsibility since 2013. The aim of the course is to deepen students’ knowledge in microprocessor technology and C programming, familiarize them with the ARM Cortex-M core and STMicroelectronics STM32 microcontrollers, and equip them with practical skills in designing hardware and creating firmware for commonly used peripherals. Consistent positive feedback has been received from student surveys. Oversight of the course is provided, all teaching materials are authored, and most lectures and selected exercises are conducted. Both in-person and combined formats of the course are offered, with instruction in both Czech and English languages.

Nanosatellite Design and Electronics (NDE)

The Nanosatellite Design and Electronics (NDE) course aims to offer fundamental knowledge in designing nanosatellites, particularly of the Cubesat and PocketQube types. Basic components, structural design, and design procedures are covered. Hands-on satellite construction projects constitute a significant portion of the laboratory exercises. Oversight has been provided for this course since 2022, specifically for the newly created study program Space Applications (SAP), taught exclusively in English. Almost half of the lectures consist of invited talks by industry experts, and laboratory exercises are designed as group projects, during which selected subsystems of a nanosatellite are independently developed by students, who then present their progress and results.

Radiofrequency Identification (RFI)

Two lectures for the course in Radiofrequency Identification (RFI) were developed, drawing upon the author's specialized expertise. These lectures, one on anti-collision protocols for Gen2 RFID tags and another on ranging and localization for RFID, wireless sensor networks, and energy harvesting, have been delivered annually since 2012.

Computer and Communication Networks (PKS)

The Computer and Communication Networks (PKS) course involves complex computer exercises that necessitate a deep understanding by the instructors. Covered in the lab exercises are: 1. Communication using UDP, traffic analysis; 2. Security, firewall – configuration, NAT, traffic analysis; 3. Routing and addressing in IP networks; 4. Implementation of network interface in embedded systems; 5. Domain Name System; 6. IPv6. In addition to selected exercises being taught, the course materials were significantly updated between the years 2012 and 2014 to align with advancements in the field.

A.2 Recent Supervised Theses

- J. Lokaj. Educational nanosatellite in PocketQube format. Master's thesis, Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Radio Electronics, 2023.
- J. Sýkora. Supportive landing module for scientific stratospheric probes. Master's thesis, Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Radio Electronics, 2023.
- M. Košút. Návrh a realizace výukového CubeSatu. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2022.
- M. Uhlíř. Bezdrátový komunikační modul v pásmu 868 MHz s podporou MESH sítě. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2022.

- M. Krejčí. Inteligentní LED světlo. Bakalářská práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2022.
- F. Langr. Bezpečnostní systémy vozidel. Bakalářská práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2022.
- M. Obšitník. RFID Reader for 13.56 MHz Band. Master's thesis, Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Radio Electronics, 2021.
- M. Virgl. Měření teplot v reaktoru VVER 440. Bakalářská práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2021.
- M. Ambrož. Systém domovního vytápění s hybridní komunikací. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2020.
- R. Juráň. Field sensor network for microclimatological measurements. Master's thesis, Brno: Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Radio Electronics, 2020.
- T. Lorenc. Měření vlastností LoRa/LoRaWAN komunikace. Bakalářská práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2020.
- O. Jeřábek. Signálová analýza LoRa s využitím SDR. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2018.
- M. Děcký. Referenční návrh HID periferie Touch Pad. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2018.
- J. Václavík. Aktivní výhybka s využitím DSP. Diplomová práce, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav radioelektroniky, 2018.

A.3 Popularization Activities

The author has been engaged in the popularization of electronics, communication systems, and embedded technologies among youth and the general public for an extended period. This chapter briefly outlines the most significant activities in this domain.

Radioklub OK2KOJ při VUT v Brně

Radioclub OK2KOJ, associated with the Brno University of Technology (BUT), has a tradition spanning nearly 70 years and remains one of the few active radio clubs in Brno. With collaboration stated in its name, the club boasts around 30 members, many of whom are current or former BUT students and employees, primarily from the Faculty of Electrical Engineering and Communication and the Faculty of Mechanical Engineering. The primary activity involves participation in radio competitions. The club enjoys a good reputation among radio amateurs. The club's nature is unique, as most of its student members are not from Brno and often leave after their studies. Therefore, there's a constant need to educate new enthusiasts. The author is a member of the club since his student days, and acts as the chairman since 2014.

Every year, a course is arranged for the club members to prepare them for amateur radio licensing exams. Public events such as *Science Night* (2012, 2013) and *Electrical Engineering Day at the Museum* (2012) have also seen the club's active participation. Media engagements include member features in *Good Morning* on ČT2 (2009 and 2020) or a discussion in *ArtCafé* on ČRo Vltava (2023).

Outreach Events and Workshops

Regular attendance at *Bastlfest*, organized by VIDA! Science Center, is another activity carried out under the oversight of both the radio club and the Brno University of Technology. This popular weekend event attracts hundreds of visitors. Workshops are organized for the attendees, focusing on practical electronics for children and youths. Participants choose a simple electronic kit, which they assemble and bring to life under expert supervision. Thanks to the support from the university and industrial partners, these kits are made available free of charge during the event.

Active participation in the university events targeting youth is maintained. Earlier activities included the *Radioelectronics Workshop*, and in recent years, aside from *Open Doors Day*, events like *Mini Erasmus* and *VUT Junior* have also been part of the outreach effort.

Satellite Technology and Media Appearances

Satellite technology is prominently featured, primarily at the AMPER trade fair. The author presented the PSAT-2 nanosatellite (2016) and the Slow-Scan Television (SSTV) camera module for PocketQube format (2022). Contributions have also been made to the Czech Television report about the Space Applications study program. In parallel, satellite activities were communicated to a broader audience during launches via online articles.

B Selected Research Projects

This chapter summarizes selected projects funded by notable grant providers. For each project, the title, original abstract, identifier, grant provider, partnering company, and research period are provided. A summary of the author's contributions made in each project is also included. The aim is to present an overview of research involvement across multiple disciplines and collaborations.

In addition to the projects described herein, involvement in various projects through direct university-company collaborations has been experienced, with industrial partners including companies such as Škoda Auto, EVOTECH, CISC Semiconductor, INTRIPLE, and Omicron Welding Machines.

B.1 Adaptive Mesh Communications for Secure Control and Sensing Systems

TAČR TK04020173, ACRIOS s.r.o., 2022–2024

Author's responsibility: Collection and analysis of statistical data from current LoRaWAN networks in European cities.

The project goal is to develop a System for Adaptive Mesh Communications (SAMC) and test this system in the created test installation. SAMC extends the communication protocol Long Range Wide Area Network (LoRaWAN) and increases the communication robustness and availability while preserving a high level of security. This is important in the key systems for the energy industry. The current LoRaWAN protocol will be extended by a new class of communication in mesh (Class-M). The new class will intrinsically guarantee communication availability during the failures of the infrastructure fragments. The proposed system combines the advantages of the spread-spectrum modulation and the robustness of the mesh topology. We expect a fast adoption of the proposed SAMC by customers.

B.2 Digital Communication Platform for Aerospace Applications

OP PIK CZ.01.1.02/0.0/0.0/20_321/0024955, MESIT asd, s.r.o, 2021–2023

Author's responsibility: Design of communication platform demonstrator with STM32F4 microcontroller using 100BASE-T1 Ethernet, firmware development.

The project deals with the development of a voice and data communication system for a wide spectrum of aeronautical applications (civil and military). The result of the project will be a prototype of a functional electronic system for voice and data communication, based on state-of-the-art digital audio signal processing technologies. Due to the requirements for high intelligibility and functionality in environments with high ambient noise, emphasis will be placed on the implementation of advanced software speech enhancement and noise suppression techniques.

B.3 System for Remote Administration and Economy Control of Fleet Vehicles with Priority in Waste Management

TAČR TH03010222, EVOTECH s.r.o., 2018–2021

Author's responsibility: Global system architecture design, hardware and firmware development, project management.

The aim of the project is to create a coherent ecosystem of devices and applications whose overall task is to automate and streamline the operation of fleets and directly related issues of operation. The intention is primarily aimed at corporate clients in the field of waste management, namely companies operating in the areas of collection, disposal and treating. The system will be able to be used in certain modifications in other areas such as agricultural businesses, freight transport, earthworks, construction, raw materials extraction and road maintenance. In these operations, the system and its components have to deal with the automation of processes of movement records, manipulation and general fuel economy, records of persons and machinery movement.

B.4 Digital Spectrometer of Mixed Neutron and Photon Fields

MPO FV20453, VF a.s., 2017–2019

Author's responsibility: Development of PH32 strip detector concentrator firmware with FreeRTOS.

The main objective of the project is development of a completely new measurement device (spectrometer system) that enables real-time characterization of low-energy mixed fields of neutron and gamma radiation ranging from 1 kEv to 1 MEv.

Nowadays measurement of such fields is performed using devices and methods that require significant amount of time (not real-time) and personal effort (potential risk of irradiation). The newly developed system effectively eliminates both of these disadvantages. Planed project outputs (functional demonstrators): Laboratory low-energy neutron spectrometer, Integrated neutron radiation dose monitoring device with energy compensation. Parameters of the newly developed system will outperform measurement instruments and devices currently used for operational measurements in research facilities and metrological laboratories in the area of nuclear physics. Moreover, it will be used by producers of neutron radiation generators and laboratories equipped with high-energy particle accelerators, like so called “proton centers” and radiopharmacology laboratories.

B.5 Radio for Smart Transmission Networks (RSTN)

TAČR TA04011571, RACOM s.r.o., 2014–2017

Author’s responsibility: Design of instrumentation for radio channel measurements in 1.3 GHz and 5.8 GHz bands, field measurements, and processing of results.

The project aim is applying and validating the latest research results in the field of advanced signal processing methods and devising an optimal solution of the physical layer for a new generation of wireless communications equipment. The equipment is intended for communication over long distances under NLOS (Non Line Of Sight) conditions. The proposed project addresses the area of radio industrial communication networks that work under conditions where the existing networks such as 3G, LTE or WiMAX cannot sufficiently ensure good operating parameters.

B.6 Innovative Control of a Car Cabin HVAC System as a Part of an Advanced Driver Assistance System

TAČR TA04031094, Škoda Auto, a.s., 2014–2017

Author’s responsibility: Design of electronics for CAN vehicle communication, design of equivalent temperature sensors, and firmware programming.

The project will focus on improving the safety of vehicles and reduce accidents. The aim of the project is to develop a system that would help avoiding dangerous situations in which the driver gets in particular because of thermal discomfort in the cabin (i.e., high or low temperature for each segment of the body surface) and consequently often difficult manipulation with the controls of the heating / cooling system such as directional manipulation of ventilation outlets, switching positions and fan performance. The aim is to develop hardware, software, algorithms and visualization system for temperature control of significant segments of the human body (those are the head, chest, arms and feet), so that the driver obtain a clear visual information about a possible imminent risk of segmented thermal discomfort and could very easily by touching the screen affect the setting of the air conditioning system.

C Selected Applied Results

C.1 Channel Sounder for 1.3 GHz Band

Kind: Functional specimen (RIV-G/B)
Year: 2015 (50%)

Channel Sounder for 1.3 GHz Band

Aleš POVALAČ, Jiří BLUMENSTEIN, Josef VYCHODIL

TAČR TA04011571: RSTN - Radio for Smart Transmission Networks
Centre of Sensor, Information and Communication Systems (SIX)

Abstract – The developed functional specimen of channel sounder is suitable for monitoring of radio channel parameters in the 1.3 GHz band. The primary use of the device is a research of NLoS radio channel in 23 cm band. Together with appropriate MATLAB and LabVIEW control software, the system allows to record and evaluate the radio channel with 120 MHz bandwidth.

Transmitting station is based on programmable RF generator Rohde&Schwarz SMU200A, controlled from MATLAB. The signal from the generator is filtered, amplified through a power amplifier and connected via a circulator to a directional antenna. The power amplifier is built with ITB MD220L-1296-48V module, which has been modified and tuned for class A.

Receiving station consists of a directional antenna, low noise preamplifiers, and band pass filters. Signal is fed to the system National Instruments PXIe-5665, which serves to digitize and record the signal.

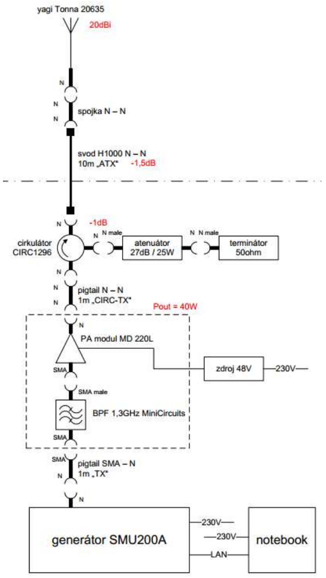


Fig. 1: TX diagram

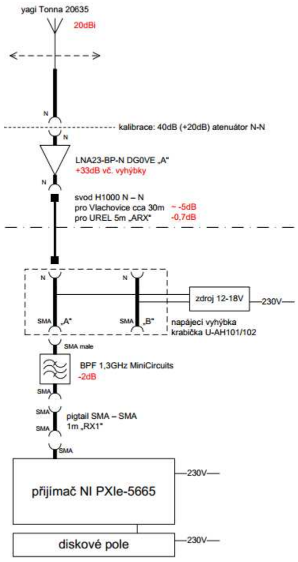


Fig. 2: RX diagram

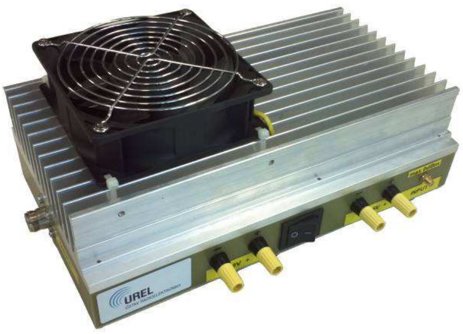


Fig. 3: Power amplifier

C.2 Channel Sounder for 5.8 GHz Band

Kind: Functional specimen (RIV-G/B)
Year: 2015 (50%)

Channel Sounder for 5 GHz Band

Aleš POVALAČ, Jiří BLUMENSTEIN, Josef VYCHODIL

TAČR TA04011571: RSTN - Radio for Smart Transmission Networks
Centre of Sensor, Information and Communication Systems (SIX)

Abstract – The developed functional specimen of channel sounder is suitable for monitoring of radio channel parameters in the 5 GHz band. The primary use of the device is a research of NLoS radio channel in 6 cm band. Together with appropriate MATLAB and LabVIEW control software, the system allows to record and evaluate the radio channel with up to 600 MHz bandwidth.

Transmitting station is based on programmable RF generator Rohde&Schwarz SMU200A, controlled from MATLAB. The signal from the generator is filtered, amplified with a two-stage power amplifier and connected to a directional antenna. The power amplifier is built with Hittite HMC408LP3 and DG0VE PA6-1-8W modules, which has been set to class A.

Receiving station consists of a directional antenna, low noise preamplifiers, and band pass filters. Signal is fed to the system National Instruments PXIe-5665, which serves to digitize and record the signal.

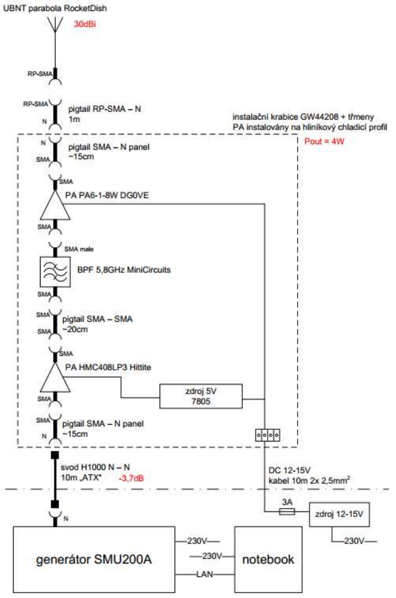


Fig. 1: TX diagram

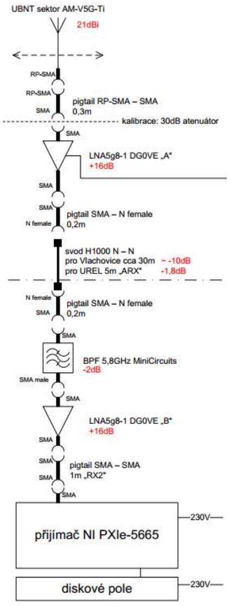


Fig. 2: RX diagram

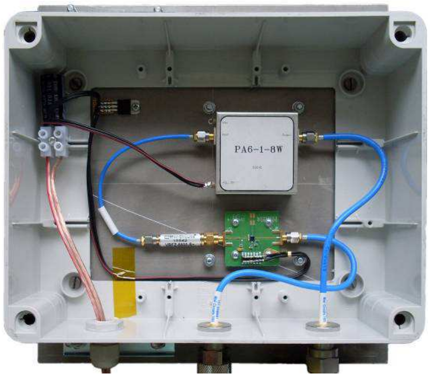


Fig. 3: Power amplifier

C.3 ANT Technology Demonstrator for Vehicle Identification

Kind: Functional specimen (RIV-G/B)
Year: 2016 (50%)

ANT Technology Demonstrator for Vehicle Identification

Aleš POVALAČ, Tomáš MIKULÁŠEK

Project no. HS18657099 with EVOTECH s.r.o.
Centre of Sensor, Information and Communication Systems (SIX)

Abstract – The functional specimen is supposed for technology demonstration and validation of basic parameters of ANT communication protocol in the unlicensed 2.4 GHz band. It integrates all functions for maximum energy savings which is possible with Nordic Semiconductor SoC solution. The hardware is designed for long-life primary batteries, such as LiMnO2 or LiFeS2 types.

Developed firmware allows to run the demonstrator in master or slave mode. The other side of the communication is provided either by another piece of the demonstrator with suitable firmware or by the commercially available development kit nRF51-DK. In the master mode, the demonstrator periodically transmits its unique identification together with current status, such as battery voltage, chip temperature etc. As a slave, it supports the synchronization and reception of ANT messages, which are sent to a supervising PC together with data from an accelerometer and other connected peripherals.

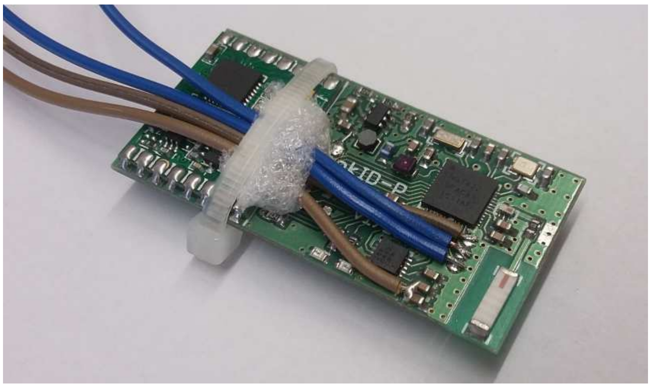


Fig. 1: ANT technology demonstrator

PODPOŘIL Kraj Vysočina FOND VYSOČINY

C.4 Camera for PSAT-2 Experimental Satellite

Kind: Functional specimen (RIV-G/B), **M17+ grade 4**
Year: 2017 (80%)

Experimental Satellite Psat-2 Camera

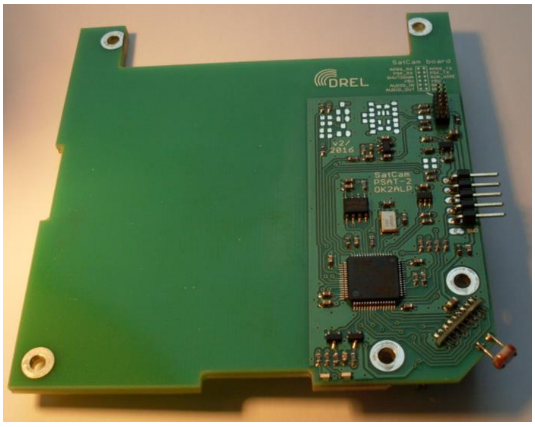
Aleš POVALAČ, Tomáš URBANEC

LO1401 Interdisciplinary Research of Wireless Technologies (INWITE)
FEKT-S-17-4713 Microwave technologies for future wireless systems
Centre of Sensor, Information and Communication Systems (SIX)

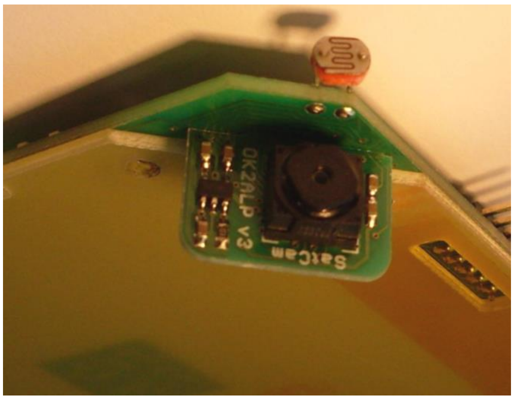
Datum: 2.2.2017

Abstract – The camera is functional part of experimental satellite Psat-2. It allows picture acquisition in the viewing angle of the satellite and their transmission through satellite transmitters.

The camera consists of controlling microprocessor STM32, camera module OV2640 and nonvolatile memory for storing of obtained pictures before their transmition to Earth with the use of satellite transmitters. Pictures are made in resolution of 320*240 color pixels and it is possible to send them to Earth in various modes with diverse quality which is directly proportional with transmission time in the SSTV mode. There are implemented modes Robot 36, 72, MP73 and 115. Camera can be requested of time sequence or depending on irradiance of picture sensor viewing angle. The testing pictures are also stored in the microprocessor memory with known content. This allows investigating the transmission channel even in the case of camera module fault. Camera is fully integrated into experimental satellite Psat-2 of US Navy Academy, Maryland.



Obr.1 Camera control board



Obr.2 Position of camera module

C.5 Transponder for PSAT-2 Experimental Satellite

Kind: Functional specimen (RIV-G/B), **M17+ grade 4**
Year: 2017 (20%)

Experimental Satellite Psat-2 Transponder

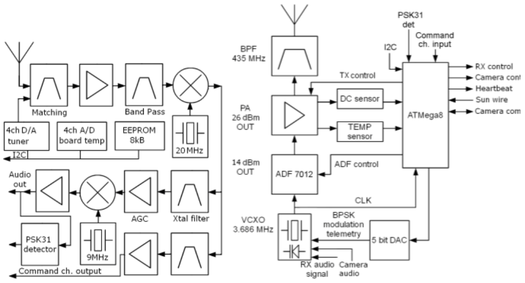
Tomáš URBANEC, Aleš POVALAČ

LO1401 Interdisciplinary Research of Wireless Technologies (INWITE)
Date 1.2.2017
FEKT-S-17-4713 Microwave technologies for future wireless systems
Centre of Sensor, Information and Communication Systems (SIX)

Abstract – The Transponder is functional part of experimental satellite Psat-2 dedicated to retransmission of narrow bandwidth modulation signals from 29.5MHz to 435MHz.

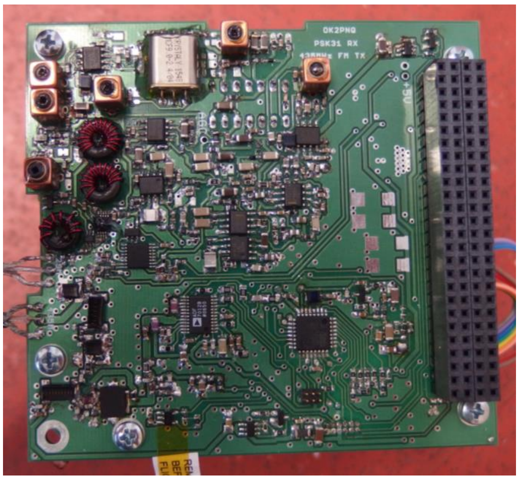
Transponder consists of narrowband receiver for frequency 29.480MHz with bandwidth 3kHz and transmitter with frequency 435.350MHz and frequency modulation. Further there is microprocessor which takes care of transponder control, with the use of settings and satellite state. For the parameter control, there is implemented the control signal detector. Microprocessor generates also modulation signal of BPSK31 beacon, which transmits telemetry of transponder and whole satellite. Transmitter allows connection of other modulation signals. Transponder is fully integrated into experimental satellite Psat-2 of US Navy Academy, Maryland.

Transponder board size
90.2 mm x 95.8 mm
Receiver operating frequency
29.480437MHz - 29.482637MHz
Receiver dynamic range 60dB
Transmitter operating frequency
435.350MHz



Obr.1 Transponder block diagram

Transmitter output power 26dBm
Power supply 5V
Current consumption RX=25.4mA
TX=316mA
MCU=4.8mA



Obr.2 Transponder picture

C.6 Testbed for Wireless Communication with High Energy Efficiency

Kind: Functional specimen (RIV-G/B)
Year: 2018 (50%)

Testbed for Wireless Communication with High Energy Efficiency

Aleš POVALAČ, Tomáš MIKULÁŠEK, Filip ZÁPLATA, Martin POSPÍŠIL

TH03010222 - System for Remote Administration and Economy Control of Fleet Vehicles with priority in Waste Management
LO1401 - Interdisciplinary research of wireless technologies

Date: 7.11.2018

Abstract – For wireless communication in beacon mode with the required battery life over 5 years, 2.4 GHz ANT technology was selected based on the Nordic Semiconductor nRF51 chipset. The testbed functional sample consists of the nRF51-DK development kit, a precision IoT current measurement kit STMicroelectronics X-NUCLEO-LPM01A, and a sample tag with integrated battery and an antenna designed to be sealed in epoxy resin.

The antenna was developed with respect to the permittivity of the selected epoxy resin and verified by simulation and measurement in an anechoic chamber. The tag firmware, created for the arm-gcc and the S210 softdevice, performs the beacon transmitting identification along with the battery status and temperature periodically every second. The sample of the tag will be used to develop the prototype of the future automated fuel accounting system.

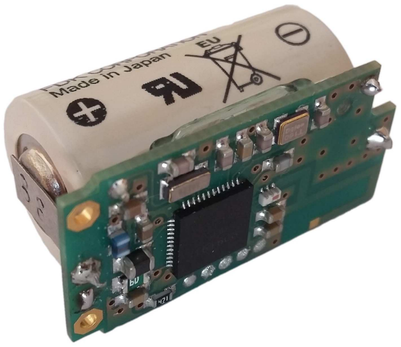


Fig. 1: ANT tag demonstrator

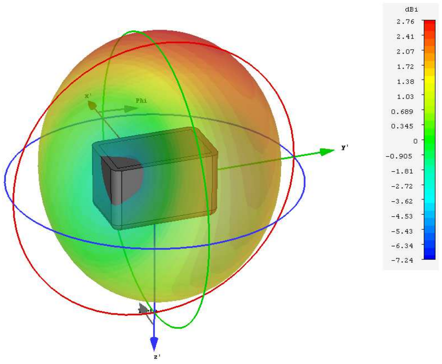


Fig. 2: Antenna simulation at 2.4GHz

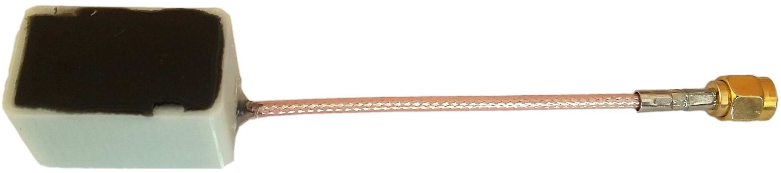


Fig. 3: Measurement setup for antenna testing

C.7 Automatic Registration System for Fuel Dispensing

Kind: Prototype (RIV-G/A), **M17+ grade 3**
Year: 2019 (45%)

Automatic Registration System for Fuel Dispensing

Aleš POVALAČ, Tomáš MIKULÁŠEK, Filip ZÁPLATA, Martin POSPÍŠIL, Pavel KLÍMA, Karel DOKULIL

TH03010222 - System for Remote Administration and Economy Control of Fleet Vehicles with priority in Waste Management
LO1401 - Interdisciplinary research of wireless technologies

Date: 2.12.2019

Abstract – The system consists of several separate units that communicate wirelessly. It provides automation and central registration of fuel dispensing and vehicle movement, eliminating the human factor in fuel type mix up and attempted misuse when refueling.

Individual vehicles are fitted with beacons that transmit their identification in the 2.4GHz band. The service life of the beacons is about 10 years; they are completely sealed in a non-flammable resin and contain an integrated battery and antenna developed with respect to the permittivity of the sealing material.

Data collection is provided by the unit located in the body of the refueling gun. It searches for beacons in the vicinity and transmits the acquired data along with other data to the master system via communication in the 868MHz band. The entire unit except the batteries is sealed in a non-flammable material. The unit is in sleep mode when suspended in a rack.

The collection unit is used to receive messages from individual refueling guns and forward them to the database backend. Together with the backend, it authorizes fuel dispensing for individual refueling. It also allows autonomous gun configuration during installation.

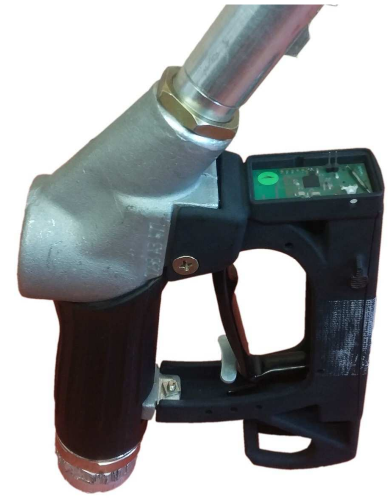


Fig. 1: Refueling gun

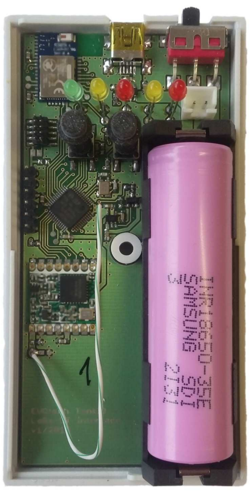


Fig. 2: Collection unit

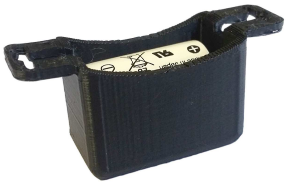


Fig. 3: Beacon before sealing

C.8 SDR Interference Emulator

Kind: Functional specimen (RIV-G/B)
Year: 2020 (20%)

1 Overview

The SDR Interference Emulator (SDR-IE) is a powerful modular Software Defined Radio (SDR) platform that provides wireless communications designers an affordable means for developing communication systems such as interference emulation and measurements, radio frequency testing and many more. The SDR-IE refines user experience making SDR prototyping more accessible by delivering the optimum balance between simplicity and performance. It is ideal for a wide range of application areas and as an alternative for widespread SDR produced by Ettus research and National instruments (NI).

The SDR-IE features high-performance FPGA SoC and supports variety of commercially available RF front ends from NI/Ettus[1] for various frequency bands and applications. Figure 1 displays the SDR interference emulator. The 250 MS/s sampling frequency makes this device suitable for spectrum sensing with >200 MHz frequency bandwidth as well as for cognitive radio applications.

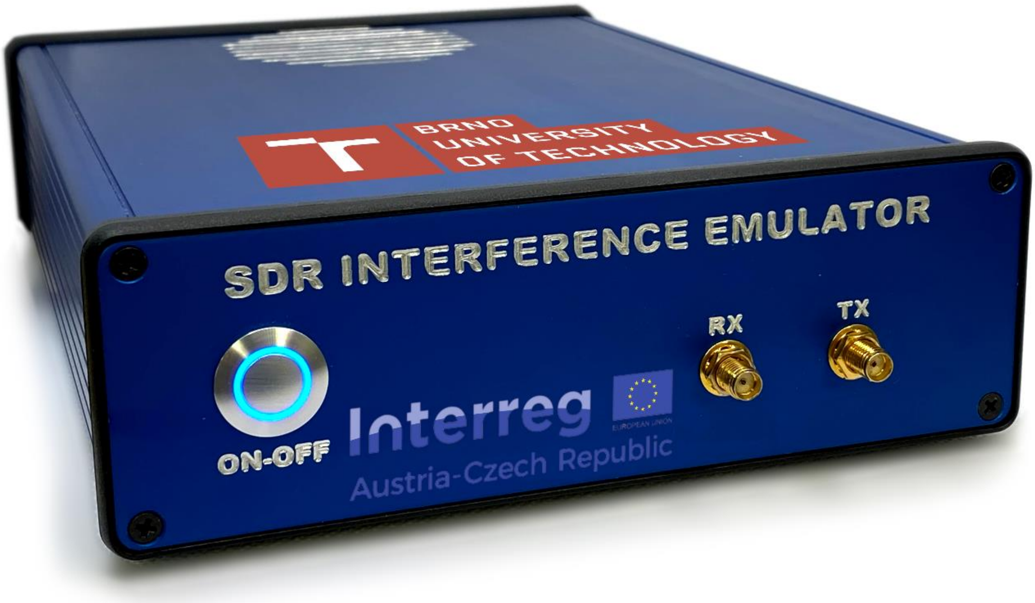


Figure 1: SDR Interference Emulator

D Selected Papers

- A. Povalac and J. Sebesta. Phase of arrival ranging method for UHF RFID tags using instantaneous frequency measurement. In *ICECom: 20th International Conference on Applied Electromagnetics and Communications*, 2010. **Conference Paper in Scopus, 95%, 25 citations.**

- A. Povalac and J. Sebesta. Phase difference of arrival distance estimation for RFID tags in frequency domain. In *IEEE International Conference on RFID-Technologies and Applications*, pages 188–193, 2011. **Conference Paper in Scopus, 95%, 62 citations.**

- J. Bouwmeester, S.P. van der Linden, A. Povalac, and E.K.A. Gill. Towards an innovative electrical interface standard for PocketQubes and CubeSats. *Advances in Space Research*, 62(12):3423–3437, 2018. **Web of Science, SCIE Q3, 40%, 7 citations.**

- E. Kassem, J. Blumenstein, A. Povalac, J. Vychodil, M. Pospisil, R. Marsalek, and J. Hruska. Wideband UHF and SHF long-range channel characterization. *Eurasip Journal on Wireless Communications and Networking*, 188:1–16, 2019. **Web of Science, SCIE Q3, 25%, 3 citations.**

- R. Fujdiak, K. Mikhaylov, J. Pospisil, A. Povalac, and J. Misurec. Insights into the Issue of Deploying a Private LoRaWAN. *Sensors*, 22(5), 2022. **Web of Science, SCIE Q2, 5%, 5 citations.**

- A. Povalac, J. Kral, H. Arthaber, O. Kolar, and M. Novak. Exploring LoRaWAN Traffic: In-Depth Analysis of IoT Network Communications. *Sensors*, 23(17):7333, 2023. **Web of Science, SCIE Q2, 80%.**

- A. Pal et al. GRBAlpha: The smallest astrophysical space observatory – I. Detector design, system description, and satellite operations. *A&A*, 677:A40, 2023. **Web of Science, SCIE Q1, 10%.**

Phase of Arrival Ranging Method for UHF RFID Tags Using Instantaneous Frequency Measurement

Aleš Povalač, Jiří Šebesta
Dept. of Radio Electronics, Faculty of Electrical Engineering and Communication,
Brno University of Technology, Purkyňova 118, 612 00 Brno, Czech Republic
E-mail: *ales.povalac@phd.feec.vutbr.cz*

Abstract

The paper gives an overview of the phase of arrival (PoA) and time of arrival (ToA) techniques for distance measurement of UHF RFID tags. It introduces a new method based on the evaluation of received signal phase change during a linear frequency modulation (LFM) chirp. The phase of signal arrival is converted to the instantaneous frequency of a FMCW beat using a delay-multiply FSK demodulator with signal level normalization. Range estimation is afterwards calculated from the averaged instantaneous frequency. The mathematical description is verified by the simulation of the ranging process in MATLAB. The final part describes the techniques for commercial EPC Class-1 Generation-2 RFID tags which allow the backscattering of defined harmonic frequency for a known time.

1. INTRODUCTION

In recent years, RFID systems working in the UHF range (860 – 960 MHz) have moved into mainstream usage. There are many commercial applications using passive RFID tags and related backscattering principles [1]. One of current research goals in this area is ranging and localization of individual tags.

New application areas for RFID technology appear if the distance information of a specific tag can be evaluated. Such tags can be used for example in objects tracking.

There are three basic principles for tag ranging. The simplest one is based on received signal strength (RSSI). It is simple but inaccurate. The other methods are based on the measurement of received signal phase or its time delay (PoA, ToA), eventually on their difference between several samples (PDoA, TDoA).

Time measurement methods are common for FMCW radars. They are based on the evaluation of low frequency signal produced by mixing of transmitted and received chirps [2]. Its basic implementation requires large sweep bandwidth which is unavailable in UHF RFID bands. For this reason, a double frequency system has been proposed [3].

Phase of arrival based measurement is more suitable concept but it fights with phase wrapping. It is necessary to perform the evaluation on multiple frequencies which need to be carefully selected [4].

2. DISTANCE MEASUREMENT

The proposed range estimation method is based on the phase measurement of the backscattered tag signal and its change during a chirp (i.e. a linear frequency sweep). The desired range is determined by the rate of phase change and by chirp parameters.

A chirp signal, also known as linear frequency modulated (LFM) signal, can be expressed as:

$$s_{TX}(t) = \sin\left(2\pi\int_0^t (f_0 + \mu t')dt'\right) = \\ = \sin\left(2\pi f_0 t + \mu\pi t^2\right), \tag{1}$$

where f_0 is the frequency at time $t = 0$ and μ is the chirp rate, defined as a frequency change B over time T:

$$\mu = \frac{B}{T}. \tag{2}$$

Frequency and time domains of a chirp signal are shown at Fig. 1.

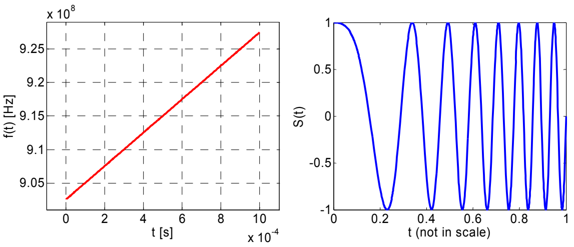


Fig. 1. Linear chirp signal

Two chirp signals with 90 deg phase difference are necessary for baseband mixing:

$$s_I(t) = \sin\left(2\pi f_0 t + \mu\pi t^2\right) \\ s_Q(t) = \cos\left(2\pi f_0 t + \mu\pi t^2\right). \tag{3}$$

One of these signals, e.g. $s_I(t)$, is transmitted by the reader and propagates through an environment. It is reflected by numerous targets, as well as by the selected RFID tag. The backscattered tag signal needs to be distinguished from other targets. This can be done using tag modulation:

$$s_m(t) = \cos(2\pi f_m t), \tag{4}$$

where f_m is the backscatter modulating frequency. As a result, the desired signal received by the reader consists among others of the AM-modulated signal shifted by a propagation time τ:

$$s_{RX}(t) = s_I(t-\tau) \cdot s_m(t). \tag{5}$$

Other multi-path propagations are neglected for this simplified scenario. The received signal is mixed into the baseband in both I and Q channels:

$$\begin{aligned} s_{BB,I}(t) &= s_I(t) \cdot s_{RX}(t) \\ s_{BB,Q}(t) &= s_Q(t) \cdot s_{RX}(t). \end{aligned} \tag{6}$$

Unwanted frequency conversion products are filtered out using a band-pass filter tuned around the tag frequency f_m.

The I and Q signals are demodulated in the next step, resulting in $s_{demod,I}$ and $s_{demod,Q}$. A coherent demodulator or a simple envelope detector can be used. The relationship between the demodulated signals in I and Q channels denotes the phase of received signal at particular frequency:

$$\phi(t) = \arctan \frac{s_{demod,I}(t)}{s_{demod,Q}(t)}. \tag{7}$$

At this time, we can measure the phase of arrival (PoA) over the frequency range defined by the bandwidth B. As the measurement takes place in a continuous chirp, there is no ambiguity typical for phase difference of arrival (PDoA) methods [4]. The signal phase as a change in time can be expressed using the instantaneous frequency:

$$f_i(t) = \frac{1}{2\pi} \frac{d}{dt} \phi(t), \tag{8}$$

which corresponds to the beat frequency of conventional FMCW radars. This frequency depends on chirp rate and signal round trip time:

$$f_b(t) = \mu \cdot \frac{2d}{c}. \tag{9}$$

The result from the equality of (8) and (9) determines the range estimate:

$$d = \frac{c}{2} \cdot \frac{\overline{f_i(t)}}{\mu} = \frac{cT}{4\pi B} \cdot \overline{\frac{\Delta}{\Delta t}\phi(t)}. \tag{10}$$

The instantaneous frequency is computed for every sample and averaged. As we can see from (10), the range estimation depends only on chirp rate and averaged instantaneous frequency.

3. SIMULATION AND RESULTS

The described principle of range estimation has been simulated in MATLAB environment. Following simulation results correspond to individual steps described in previous section.

Firstly, we prepare I and Q signals in 900 MHz band according to (3) and create received modulated signal as described by (4) and (5). These signals are mixed into baseband (6) and higher frequency products are filtered out. An additive white Gaussian noise is added into the received signal. Resulting signals are shown in Fig. 2.

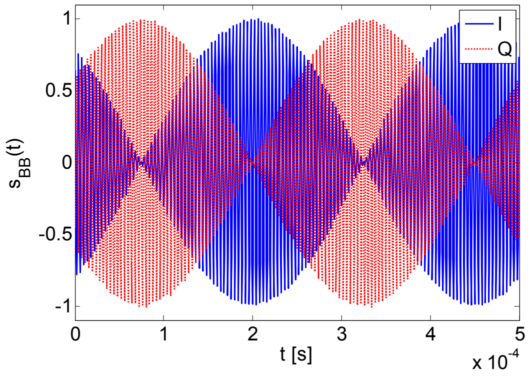


Fig. 2. Baseband I and Q signals

The amplitude demodulation can be done in several ways. For this simulation, we have implemented an envelope detector, consisting of a digital rectifier and a low-pass FIR filter. The results of AM demodulation are in Fig. 3. First samples of the signal are corrupted by filter initialization.

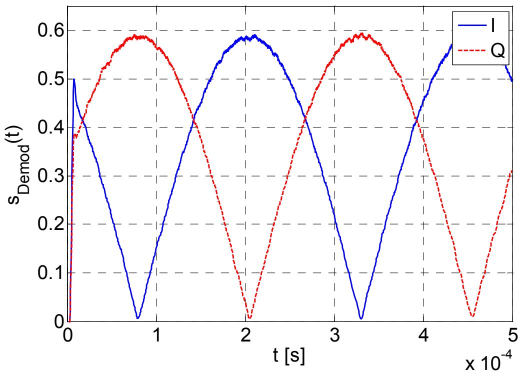


Fig. 3. I and Q signals after AM demodulation

3.1. Baseband phase measurement

In the next step, the phase of received signal is computed from I and Q amplitudes using arctangent function. The phase change shown as the solid line in Fig. 4 is not monotonic (sawtooth shaped) as a result of information lost during envelope AM demodulation. The dotted line depicts the recovered phase from following steps.

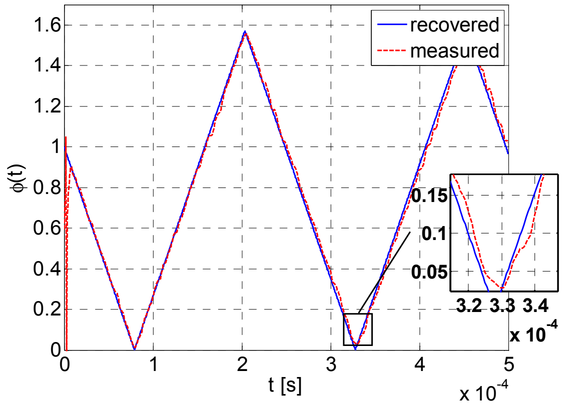


Fig. 4. Phase of received signal

A numerical differentiation (difference between consequent values) is calculated and shown in Fig. 5. The sign of the difference denotes the slope direction. For the purpose of instantaneous frequency recovery, we rectify the direction by computing the absolute value of it.

The arctangent function is undefined for infinite argument. Also the measurement of AM amplitude is inaccurate for small I or Q values. For this reason, we discard samples with I or Q values under a defined threshold. Afterwards, the averaged value of accepted instantaneous frequency samples is computed, as well as the resulting distance according to (10).

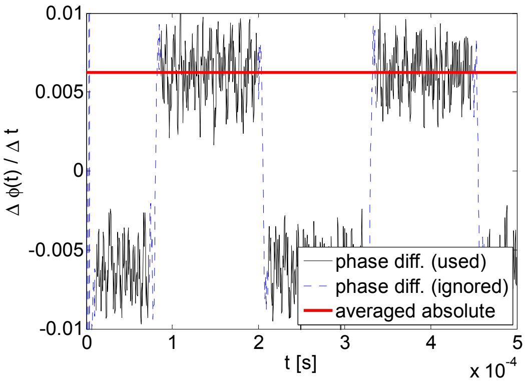


Fig. 5. Phase differentiation in time, averaging

The experimental results obtained from a series of 20,000 simulations with $T = 0.5$ ms, $B = 25$ MHz, $f_0 = 902.5$ MHz, $d = 6.000$ m, $SNR = 10$ dB are shown as a histogram in Fig. 6.

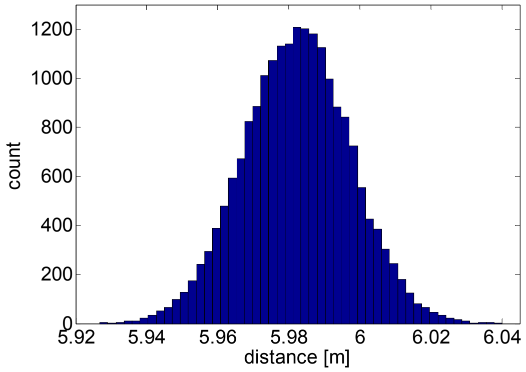


Fig. 6. Histogram of range estimates

The simulated results have a normal distribution with the mean value of 5.982 m and the variance of $2.255 \cdot 10^{-4}$ m^2. The mean value is lower than the input value because of the slope rectification which can also corrupt the sign of an excessive noise.

3.2. Arctangent implementation

The arctangent function used in (7) is very computational intensive for a real-time implementation. Fortunately, there are other methods for digital frequency demodulation. The delay-multiply FSK demodulator [5] with signal level normalization is shown in Fig. 7.

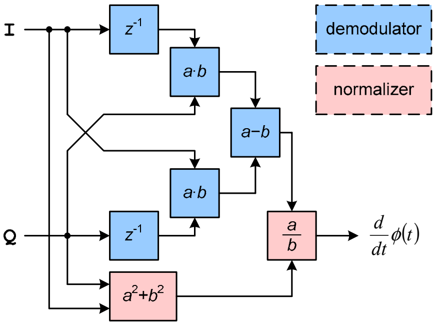


Fig. 7. Delay-multiply FSK demodulator

This demodulator is more efficient, as it utilizes only delay blocks, multipliers, and an adder. The output amplitude is normalized using squarers, an adder, and a divider. Similar results can be obtained if the amplitude of I and Q input signals is normalized in another way, i.e. by an automatic gain control (AGC) circuit.

3.3. Tag modulating signal

Tag modulation is used for the distinction between signals backscattered from the tag and from other objects. Its function is described by (4).

There are several ways how to instruct the tag for harmonic backscattering with selected frequency. Besides custom command method described in [3], we can use two principles suitable for standard EPC Class-1 Generation-2 UHF RFID tags [6].

The first method uses tag preamble with higher Miller subcarrier modulations. For long preamble and M8 coding, we are able to obtain 140 periods of modulation signal. The advantage of this approach is that the measured preamble can be repeated in every transmission.

The second method requires a tag with blank User memory, i.e. filled with zeros. Up to 512 periods of modulation signal can be obtained using FM0 coding and conventional 512 bit tag chips, such as Impinj Monza 4U or NXP UCODE G2XM. In this case, the tag needs to be instructed by Gen2 Read command to backscatter its entire memory contest at once. The measurement is processed on this answer.

4. MEASUREMENT FREQUENCY STEPPING

The proposed distance measurement method requires linear chirp which is usually not available on simple hardware testbeds with PLL frequency synthesizers. This limitation can be solved by a frequency hopping technique. In this case, several consequent measurements are performed on selected discrete frequencies.

The increase of frequency step converts the described method into traditional phase difference of arrival (PDoA) measurement. An extreme case of such approach with only three unequally spaced frequencies is described in [4].

Another important feature of the measurement using discrete frequencies is that it does not need to be performed during a single tag answer. Every phase measurement can be done on a single tag reply, allowing longer averaging. On the contrary, continuous measurement needs to be done during a chirp with its length defined by 512 backscattered tag periods at most.

5. CONCLUSION

In this paper, we have proposed a new approach to the estimation of RFID tag distance. Described method does not have problems with the phase ambiguity typical for PDoA measurements.

Several simulations have been done using the method of instantaneous frequency averaging. The accuracy of range estimation is very high even in a noisy channel. On the other hand, real measurements will naturally fight with multipath propagation and fading, which can decrease the accuracy remarkably.

6. ACKNOWLEDGEMENT

The research and development presented in this paper was supported by grants no. GD102/08/H027 and no. MSM0021630513. It is a part of the COST action IC 0803, which is financially supported by the Czech Ministry of Education under grant no. OC09016. A. Povalac is a recipient of the Scholarship for Talented Ph.D. students.

7. REFERENCES

[1] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Newnes, Burlington, MA, 2008.

[2] Y. Huang, P. V. Brennan, A. Seeds, "Active RFID location system based on time-difference measurement using a linear FM chirp tag signal", *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008*, pp. 1-5, Cannes (France), September 2008.

[3] J. Heidrich, D. Brenk, J. Essel, G. Fischer, R. Weigel, S. Schwarzer, "Local Positioning with Passive UHF RFID Transponders", *IEEE MTT-S International Microwave Workshop on Wireless Sensing, Local Positioning, and RFID, IMWS 2009*, pp. 1-4, Cavtat (Croatia), September 2009.

[4] X. Li, Y. Zhang, M. G. Amin, "Multifrequency-Based Range Estimation of RFID Tags", *IEEE International Conference on RFID 2009*, pp. 147-154, Orlando (FL, USA), April 2009.

[5] W. L. Betts, W. H. Smith, M. R. Deakley, "Frequency Shift Keyed Demodulator", *U.S. Patent No. 4,612,509*, September 1986.

[6] *Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz*, version 1.2.0, EPCglobal Inc., 2008.

Phase Difference of Arrival Distance Estimation for RFID Tags in Frequency Domain

Ales Povalac, Jiri Sebesta
Department of Radio Electronics
Brno University of Technology
Brno, Czech Republic
e-mail: ales.povalac@phd.feec.vutbr.cz

Abstract—**The paper gives an overview of phase based ranging techniques, focusing on the phase difference of arrival method measured in frequency domain (FD-PDoA). After a theoretical overview of distance estimation and localization, it introduces an experimental RFID front-end prototype used for FD-PDoA measurements. Proposed modular design is very flexible and allows easy replacement of any block, as well as direct access to all required low-level signals. The main part of the article is devoted to range estimation experiments in an anechoic chamber, using the developed front-end and signal processing in a PC with MATLAB. Several measurement problems are addressed, such as demodulator phase imbalance correction, wrapped phase recovery, etc. Ranging is performed with common passive EPC Gen2 RFID tags.**

Keywords–RFID; UHF; RTLS; ranging; FD-PDoA; EPC Gen2

I. Introduction

Radio frequency identification (RFID) systems working in the UHF range (860 – 960 MHz) are primarily supposed to the identification of items and objects with RFID tags. There are many commercial applications and this technology is widely used now [1]. Real time locating systems (RTLS) may be employed to track the position of objects using these inexpensive tags. This paper describes the experiment with one of the ranging methods, based on a signal phase difference of arrival measured in frequency domain.

For a traditional positioning in 2D space, we need to know at least three distances (trilateration) or at least two direction angles (triangulation), both measured from known locations. A good overview of positioning algorithms can be found in [2], [3]. The measurement accuracy of the distance or the angle is fundamental for precise spatial identification.

There are several methods of distance measurement, required for trilateration positioning. The simplest and most common one is based on received signal strength (RSS). Although this method is implemented in some way on almost all RFID readers, the accuracy is usually not sufficient for reasonable range estimation, because it is strongly affected by the propagation environment. Typical ranging mean absolute error is over 1 m even for systems that use reference tags for propagation estimation, e.g., LANDMARC [4]. Better results can be obtained using methods based on signal phase measurement, exploiting the coherence of backscattered signal [5].

In this paper, we have focused on one of the phase difference of arrival (PDoA) methods. We present an experiment in anechoic chamber using common EPC Gen2 tags, custom experimental RFID reader, digitizer system, and a signal post-processing in MATLAB.

II. Theory of Phase Based Ranging

Phase-based techniques of RFID ranging allow coherent signal processing and they achieve better performance than traditional RSS approach [2], [6]. On the other hand, simple phase-of-arrival measurement fights with phase wrapping. In the 900 MHz RFID band, the phase wraps during ca. 17 cm round-trip flight. It is therefore necessary to perform multiple measurements and use their phase difference only.

A. Phase Difference of Arrival Method

Traditional approach of PDoA ranging is based on a dual-frequency radar technique for range estimation [2]. Because of the phase wrapping, it is necessary to use at least three measurement frequencies [7].

Another method for phase wrapping elimination uses continuous-time frequency change realized by a linear FM chirp signal [8–10]. This time domain (TD-PDoA) measurement also allows the estimation of tag velocity vector [5], as it gives the Doppler shift information.

Linear chirp needs to be fitted into tag harmonic transmission, which is quite short using standard EPC Gen2 tags – 512 signal periods at the most using blank memory method described in [8]. This approach gives very high chirp rates with large sweep bandwidth necessary for reasonable measurement accuracy. It is therefore much simpler to perform multiple consequent measurements on discrete frequencies.

B. Measurement in Frequency Domain

The frequency domain phase difference of arrival (FD-PDoA) method features the robustness to signal strength variations and allows reliable ranging. The RFID tag must be stationary during the measurement. The range estimation using linearly spaced measurement frequencies is:

$$d = \frac{c}{4\pi \cdot \Delta f} \cdot \overline{\Delta\varphi} - l_{corr}, \tag{1}$$

The research presented in this paper was supported by grants no. GD102/08/H027, no. 613/2011/G1, and no. MSM0021630513. It is a part of the COST action IC 0803, which is financially supported by the Czech Ministry of Education under grant no. OC09016. A. Povalac is a holder of Brno PhD Talent Financial Aid.

where $\overline{\Delta\varphi}$ is an average of phase change between consequent frequencies and l_{corr} is a distance correction, discussed later in Section IV. The estimation d therefore includes the real distance between a reader antenna and a tag, signal propagation delay in RFID front-end and antenna cable, and tag backscatter phase offset. The last two components are nearly constant and can be subtracted or calibrated out from the result, leaving the real range estimation itself.

C. Positioning in 2D Space

Using multiple receiving reader antennas, it is possible to simultaneously measure the distance from several points and perform the tag localization in 2D or 3D space. This method can also be accompanied by PDoA in spatial domain [5] to perform a triangulation and combine the localization result.

Antenna configuration for the simplest multiple-input single-output (MISO) localization system is proposed in Fig. 1. The transmitter patch antenna is beaming to one side only, while the receiving antennas are omnidirectional. Using this setup, the signal propagation is not back and forth and the positioning circle transforms to an ellipse.

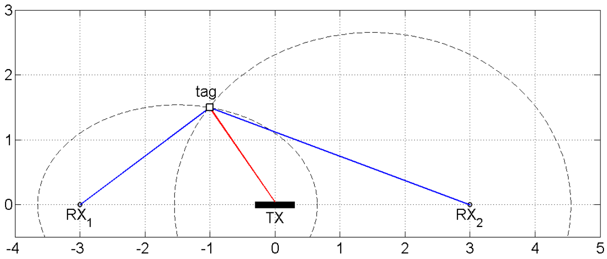


Figure 1. Localization using ellipses intersection in a MISO system.

The tag can be localized in the intersection of two ellipses. Each ellipse is defined by its foci corresponding to the positions of TX and RX antennas and the major radius resulting from the measured distance. For the configuration with two RX antennas, there are two intersections of the ellipses. The correct solution can be selected using directional TX antenna as proposed above or using another RX input.

Equation (1) can be simply adapted to a MISO system, the range estimation d is equivalent to the ellipse major radius a, i.e., $d = a$. Finding the intersections of two ellipses is a common geometrical problem [11].

Ranging method described later assumes traditional positioning with the measurement of round-trip distance, i.e., with one antenna for both TX and RX.

III. Experimental Setup and Measurement

The FD-PDoA distance estimation has been tested in an anechoic chamber (Fig. 2). Tag responses have been captured in the RFID band according to the US regulation, i.e., frequencies from 902 MHz to 928 MHz with 250 kHz step.

Measurements have been performed using an experimental UHF RFID front-end with 23 dBm output power, connected to the Poynting PATCH-A0025 antenna. The overall block diagram of the measurement setup is in Fig. 3.

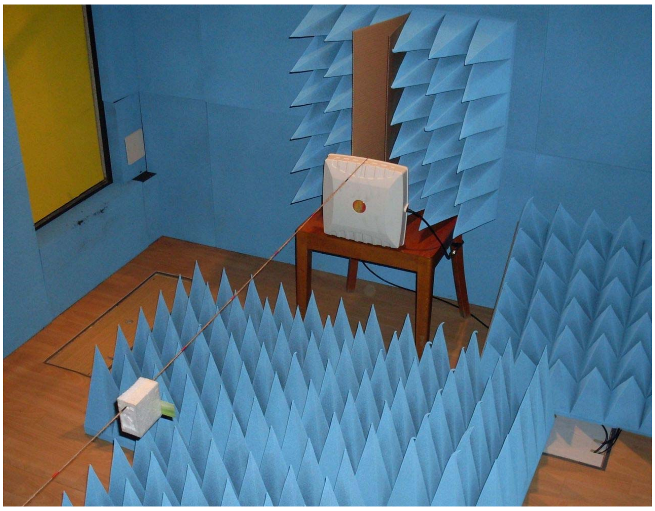


Figure 2. Measurement setup in an RF anechoic chamber.

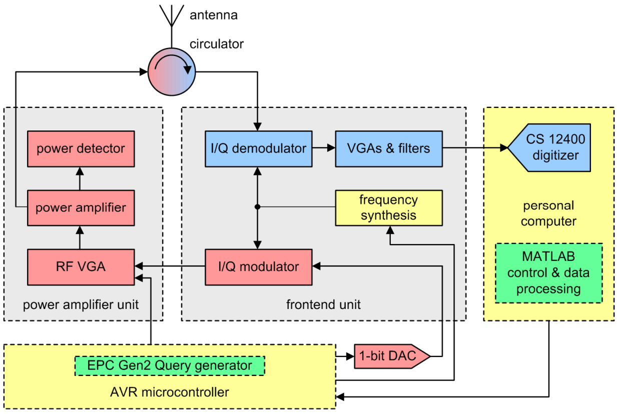


Figure 3. Block diagram of the measurement system.

A. Interrogator Testbed

The front-end consists of three main blocks: front-end unit, power amplifier unit and circulator [12]. It is capable of operation in the frequency range from 860 to 960 MHz, which covers both the EU and the US bands for UHF RFID systems. The design is modular, i.e., each block can be removed or replaced by a new version (Fig. 4). It has been created on purpose of ranging experiments.

Main front-end board is based on ADF9010 IC by Analog Devices [13], which comprises the frequency synthesis, TX quadrature modulator, external RX quadrature demodulator, and RX baseband filters with programmable gain and cutoff frequency. Conversion between RF signals in 900 MHz band and baseband I/Q signals is direct without any immediate frequencies. This concept ensures high linearity and low noise signal paths [14].

The carrier leakage into the RX causes a self blocker signal, which is inherent for all RFID reader systems. In this configuration, the self blocker is converted into DC offset at I/Q channels and can be filtered out. This is not possible by an application of multiple-IF receiver [15], [16], where the carrier cancellation is necessary for obtaining an optimal reception.

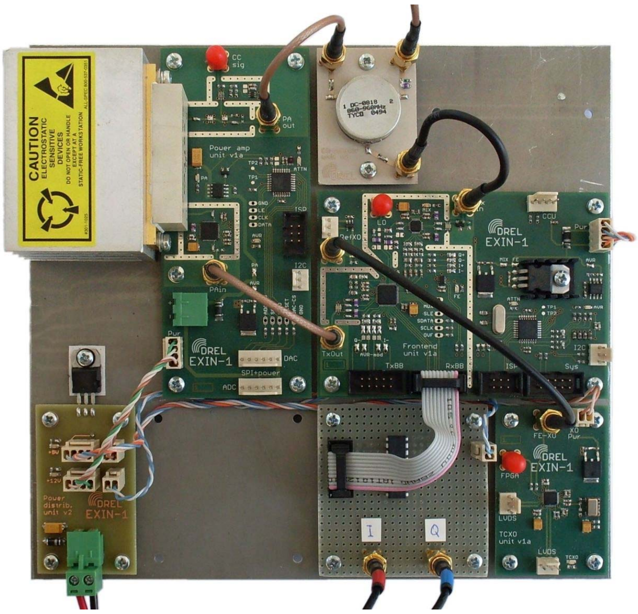


Figure 4. Experimental UHF RFID front-end.

TABLE I. QUERY COMMAND STRUCTURE

ASK data	Parameter	Description
preamble	*Tari* = 25 µs	Tari length
	RTcal = 75 µs	R→T calibration
	TRcal = 133 µs	T→R calibration
1000	*Query*	Command ID
1	*DR* = 64/3	BLF: 160 kHz (with TRcal)
00	*M* = 8	Miller-8 coding
1	*TRext* = 1	Use pilot tone
00	*Sel* = All	Don't test SL flag
00	*Session* = S0	S0 powers-on in A target
0	*Target* = A	Query A tags
0000	*Q* = 0	One slot in the round only
01011	*CRC-5*	CRC-5 over the Query

The baseband RX functions include continuous time low pass filters with programmable cut-off frequency and a VGA with programmable gain from 0 to 24 dB in 3 dB steps [13]. Amplified and filtered baseband signal can be sampled by a high-speed AD converter and processed by an FPGA.

For a simplified operation, we bypassed the external DA converter, so the modulator input has been connected directly to the output of an AVR microcontroller, effectively forming a simple 1-bit DA converter. The spectrum of transmitted signal will not comply with FCC standard requirements but this is not a problem for a laboratory experiment in an anechoic chamber.

B. *Measurement Characterization*

Tag responses have been captured on all 105 applicable frequencies, varying the distance between antenna and tag from zero to 2.4 m with 0.2 m step. The tag was placed on a simple nonconductive hung (Fig. 6). Measurements have been done using UPM ShortDipole^{x} tags with NXP U-Code G2XM chips, which comply with EPC Class-1 Generation-2 UHF RFID protocol [17].

Data in I/Q baseband channels have been captured by a PC using GaGe CompuScope 12400 PCI bus 12-bit digitizer card with 20 MS/s sampling selected.

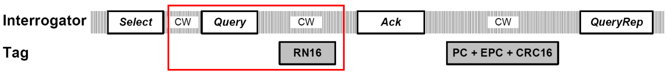


Figure 5. EPC Gen2 interrogation process with Query command.

Fig. 5 shows a basic Gen2 inventory round. The tag population to participate in the round is selected at first, followed by the Query command. The tag responses with random number RN16, which should be acknowledged by the reader. After correct acknowledgement the tag backscatters its EPC and changes its inventoried flag. Another tag may respond to succeeding QueryReps in the inventory round.

For the received signal phase measurement, it is sufficient to capture the response of one RFID tag only. Therefore it is necessary to transmit single Query command only (with $Q = 0$) and observe the RN16 response (highlighted in Fig. 5). As the internal protocol processing in the tag times out (T_2 parameter in [17]), the Query (see Tab. 1) may be repeated without any other commands as many times as necessary.

Fig. 8 depicts the transition between reader command and tag backscatter. Large DC offsets in both I and Q baseband channels produced by the downconversion of self-blocker signal are removed using AC coupling with manually triggered boost, which quickly charges the coupling capacitors to the desired common voltage level. The response starts with a pilot tone (140 periods of harmonic backscatter in total [8]) and continues with RN16 modulated using Miller-8 coding.

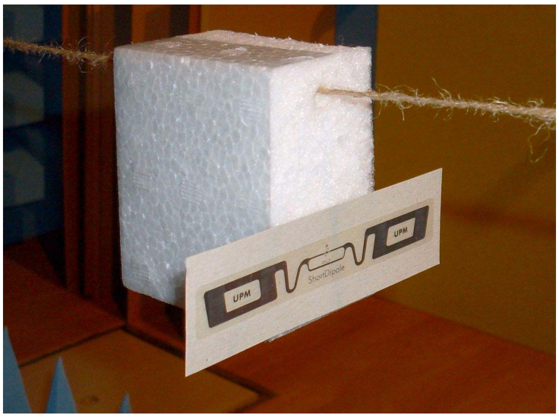


Figure 6. UPM ShortDipole^{x} tag mounted on a positionable holder.

Signal phase information is calculated using RSS value measured at both in-phase and quadrature baseband channels (dashed lines in Fig. 9). As can be seen, there are two problems related to this measurement: excessive wideband noise corrupting lower values of RSS and phase imbalance between I and Q channels related to the demodulator.

C. RSS with Goertzel's Algorithm

The output signal from quadrature demodulator is disrupted by noise but the beginning of the measurement signal is narrowband, as it consists of harmonic backscatter only. It is therefore possible to filter the pilot tone response in frequency domain.

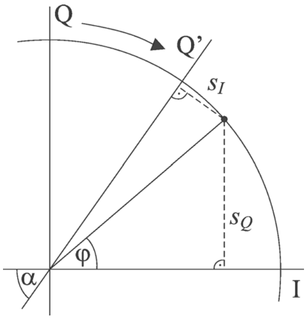


Figure 7. Phase imbalance correction.

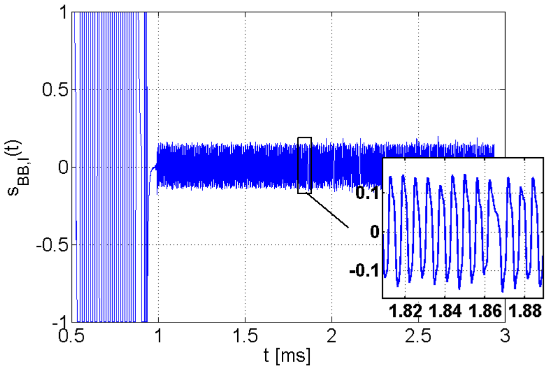


Figure 8. In-phase baseband signal received from the tag.

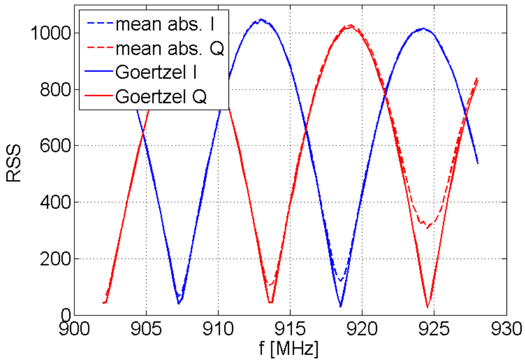


Figure 9. Raw RSS values for I/Q channel and the influence of RSS processing with Goertzel's algorithm.

Tag backscatter link frequency (BLF) is given by Query command specified in Tab. 1. For these parameters, the BLF is 160 kHz ± 10% according to [17]. An effective way to measure the power of this frequency component is to use the Goertzel's algorithm [18]. It computes a sequence $s(n)$ using sampled signal values:

$$s(n) = x(n) + 2\cos(2\pi\omega)s(n-1) - s(n-2), \tag{2}$$

where $s(-2) = s(-1) = 0$ and ω is the tested BLF frequency in cycles per sample.

For the purpose of BLF signal strength measurement, we are only concerned with the corresponding power:

$$X(\omega)X'(\omega) = s(n-2)^2 + s(n-1)^2 - 2\cos(2\pi\omega)s(n-2)s(n-1). \tag{3}$$

The Goertzel's algorithm is more efficient than the FFT when computing only a few DFT frequencies. It reduces the number of real-valued multiplications in comparison to the DFT equation. Solid lines in Fig. 9 show the normalized values of signal power computed using this algorithm.

The RSS is an absolute value, which causes problems with phase calculation. It is desirable to recover RSS sign using the phase information contained in the baseband signal, as can be seen in the zoom in Fig. 8. The RSS sign is determined by the polarity of the first pulse. Final RSS values measurement after Goertzel's algorithm processing and sign recovery is shown in Fig. 10.

D. Phase Imbalance Correction

In an ideal case, the phase of received signal at particular frequency is denoted by a simple inverse trigonometric function:

$$\varphi = \arctan\frac{s_I}{s_Q}. \tag{4}$$

The actual quadrature demodulator in the front-end unit together with its matching transformer and other circuits corrupts the ideal 90 deg phase shift between in-phase and quadrature channel, resulting in a rotation of Q axis from 90 deg to an angle α.

According to Fig. 7 we need to determine the angle φ from s_I and s_Q amplitudes:

$$\frac{s_I}{s_Q} = \frac{\sin(\alpha - \varphi)}{\sin\varphi}, \tag{5}$$

which can be solved for φ:

$$\varphi = \arctan\frac{\sin\alpha}{\frac{s_Q}{s_I} + \cos\alpha} \tag{6}$$

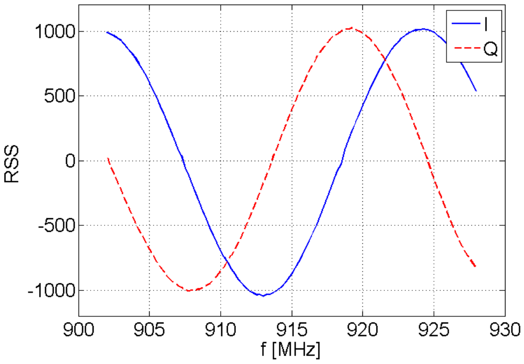


Figure 10. RSS values for I/Q channel after phase recovery.

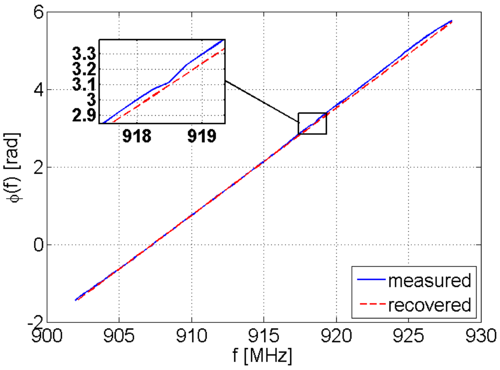


Figure 11. Measured and recovered phase information of received signal.

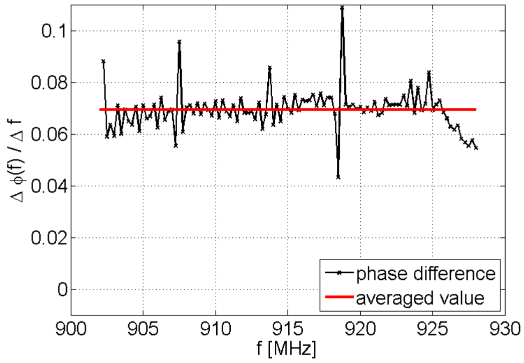


Figure 12. Phase differentiation in frequency domain, averaging.

The demodulator angle α between I and Q axes can be measured with an RF generator connected to the front-end input. Using an oscilloscope, we have measured the phase shift $\alpha = 79$ deg for our system.

E. Phase Recovery and Differentiation

The phase of received signal is computed from I and Q amplitudes using (6). The range of principal value for arctangent is a periodical function, with period equal to 180 deg. This overlapping can be easily unwrapped and the result is shown as a solid line in Fig. 11. The dashed line depicts the recovered phase from following steps.

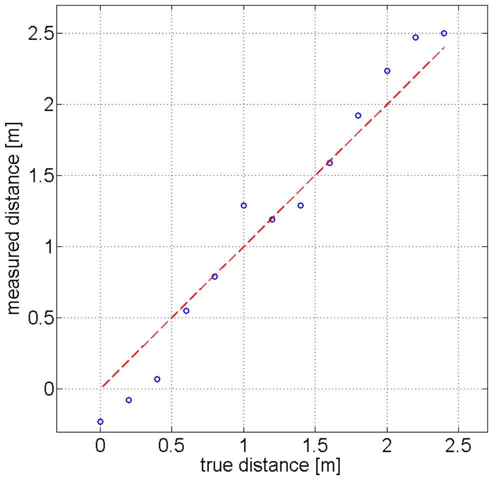


Figure 13. Distance estimation results.

A numerical differentiation (difference between consequent values) is computed and shown in Fig. 12. There are several samples more influenced by noise, typically when $s_I \approx 0$ or $s_Q \approx 0$. Finally, an average value is computed.

IV. Distance Estimation Results

The distance estimation is calculated from the phase difference average using (1). The result includes the propagation through antenna cable, delays caused by RF part of the front-end, and phase offset of the tag backscatter.

These factors are incorporated in l_{corr} correction distance. The measured correction has been obtained as an average of differences between measured and real distances. In our measurement setup the correction was $l_{corr} = 5.42$ m. It includes the propagation delay on antenna cable (physical length 2.06 m with velocity ratio 81%, i.e., electrical length 2.54 m), phase delay caused by the tag reflection (typical value ca. 1 m according to [19]), and various delays of the front-end, primarily of the power amplifier.

Fig. 13 shows the results of range estimation for all carried measurements with altering distance between the antenna and the tag. The mean absolute error (MAE) of the range estimation was 0.14 m. Ranging inaccuracy is caused by several factors, such as variation of l_{corr} over frequency and temperature, non-ideal anechoic chamber etc. Initial measurements took place in near field of the antenna, where the phase recognition is problematic.

The range measurements were repeated several times with very low variance (below 10% of ranging MAE). This implies that the error was not caused mainly by stochastic influences such as noise.

V. Conclusion

In this paper, we have focused on the phase of arrival ranging in frequency domain. The developed UHF RFID testbed has been presented. Using this system together with the signal processing in MATLAB, we have done a set of FD-PDoA ranging estimations in the anechoic chamber.

Similar measurements have been performed using modified commercial reader (Metra RFI21.1 [20]). The performance of this reader was inferior in comparison to our experimental interrogator, mainly because of very small shift between in-phase and quadrature demodulator channels at frequencies over 900 MHz. Moreover, the demodulator shift depended on both frequency and temperature, so there was no simple way to correct it.

The presented ranging method gave reasonably accurate results in the anechoic chamber, where almost no multipath propagation takes place. In a real environment, the distance estimation will produce less accurate results.

In the future work, we would like to add an FPGA signal and protocol processing to our experimental reader, develop the MISO architecture with multiple receiving antennas, and implement the localization in 2D space. It will also be necessary to address the problem of multipath propagation.

References

[1] D.M. Dobkin, "The RF in RFID: Passive UHF RFID in practice," Burlington, MA: Newnes, 2007.

[2] Y. Zhang, X. Li, and M. Amin, "Principles and techniques of RFID positioning," in RFID Systems: Research trends and challenges, M. Bolic, D. Simplot-Ryl, and I. Stojmenovic, Eds. Chichester: John Wiley & Sons Ltd., 2010, pp. 389-415.

[3] A.H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," in IEEE Signal Processing Mag., vol. 22, no. 4, pp. 24-40, July 2005.

[4] L.M. Ni, Y. Liu, Y.Ch. Lau, and A.P. Patil, "LANDMARC: Indoor location sensing using active RFID," in Proc. IEEE Int. Conf. Pervasive Computing and Communications, pp. 407-415, Dallas-Fort Worth, TX, March 2003.

[5] P.V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K.V.S. Rao, "Phase based spatial identification of UHF RFID tags," in Proc. IEEE Int. Conf. RFID, pp. 102-109, Orlando, FL, April 2010.

[6] C. Hekimian-Williams, B. Grant, X. Liu, Z. Zhang, and P. Kumar, "Accurate localization of RFID tags using phase difference," in Proc. IEEE Int. Conf. RFID, pp. 89-96, Orlando, FL, April 2010.

[7] X. Li, Y. Zhang, and M.G. Amin, "Multifrequency-based range estimation of RFID tags," in Proc. IEEE Int. Conf. RFID, pp. 147-154, Orlando, FL, April 2009.

[8] A. Povalac and J. Sebesta, "Phase of arrival ranging method for UHF RFID tags using instantaneous frequency measurement," in Proc. Conf. ICECom, pp. 1-4, Dubrovnik, September 2010.

[9] Y. Huang, P.V. Brennan, and A. Seeds, "Active RFID location system based on time-difference measurement using a linear FM chirp tag signal," in Proc. IEEE Int. Symp. PIMRC, pp. 1-5, Cannes, September 2008.

[10] J. Heidrich, D. Brenk, J. Essel, G. Fischer, R. Weigel, and S. Schwarzer, "Local positioning with passive UHF RFID transponders," in Proc. IEEE MTT-S IMWS on Wireless Sensing, Local Positioning, and RFID, pp. 1-4, Cavtat, September 2009.

[11] D. Eberly, Intersection of ellipses. Geometric Tools LLC, 2010, pp. 1-5. Available: http://www.geometrictools.com/Documentation/IntersectionOfEllipses.pdf [online].

[12] A. Povalac and J. Sebesta, "Experimental front-end for UHF RFID reader," unpublished.

[13] ADF9010: 900 MHz ISM band analog RF front end (datasheet). Analog Devices Inc., pp. 1-28, August 2008.

[14] M. Keaveney, J. Morrissey, P. Walsh, M. Tuthill, M. Chanca, I. Collins, and P. Hendriks, "A high performance RF front end for UHF RFID reader applications," in IET Sem. on RF and Microwave IC Design, pp. 1-7, London, 2008.

[15] R. Langwieser, G. Lasser, Ch. Angerer, M. Rupp, and A.L. Scholtz, "A modular UHF reader frontend for a flexible RFID testbed," in Proc. Int. EURASIP Workshop on RFID Tech., pp. 1-12, Budapest, 2008.

[16] Ch. Angerer and R. Langwieser, "Flexible evaluation of RFID system parameters using rapid prototyping," in Proc. IEEE Int. Conf. RFID, pp. 42-47, Orlando, FL, April 2009.

[17] Class-1 Generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz, version 1.2.0, EPCglobal Inc., September 2008.

[18] A.V. Oppenheim, R.W. Schafer, and J.R. Buck, Discrete-time signal processing. Upper Saddle River, NJ: Prentice Hall, 1999, pp. 633-635.

[19] V. Viikari, P. Pursula, and K. Jaakkola, "Ranging of UHF RFID tag using stepped frequency read-out," IEEE Sensors J., vol. 10, no. 9, pp. 1535-1539, September 2010.

[20] A. Povalac, M. Zamazal, and J. Sebesta, "Firmware design for a multi-protocol UHF RFID reader," in Proc. Int. Conf. Radioelektronika, pp. 1-4, Brno, April 2010.

Available online at www.sciencedirect.com

ScienceDirect

Advances in Space Research 62 (2018) 3423–3437

ADVANCES IN SPACE RESEARCH
(a COSPAR publication)

www.elsevier.com/locate/asr

Towards an innovative electrical interface standard for PocketQubes and CubeSats

J. Bouwmeester [a,*], S.P. van der Linden [a], A. Povalac [b], E.K.A. Gill [a]

[a] Delft University of Technology, Faculty of Aerospace Engineering, Kluyverweg 1, 2629 HS Delft, The Netherlands
[b] Brno University of Technology, Faculty of Electrical Engineering and Communication, Technicka 12, 616 00 Brno, Czech Republic

Received 19 May 2017; received in revised form 29 March 2018; accepted 30 March 2018
Available online 10 April 2018

Abstract

Developers experience issues with the compatibility, connector size and robustness of electrical interface standards for CubeSats and PocketQubes. There is a need for a lean and robust electrical interface standard for these classes of satellites. The proposed interface standard comprises a linear data bus which is used for housekeeping data, internal commands and small-to-moderate payload data. A community based analytic hierarchy process is used for the trade-off of design options, resulting in the selection of RS-485 as standard data bus, mainly due to its low power consumption and high effective data throughput compared to other candidates. Several switched and protected battery voltage lines are distributed from the central electrical power subsystem unit to the other subsystems to enable a simple and efficient power distribution. The harness comprises a 14 and 9 pin stackable connector for CubeSats and PocketQubes, respectively, occupying very little board space.

Keywords: CubeSat; PocketQube; Interfaces; Standard; Data-bus; Power distribution

1. Introduction

CubeSat and PocketQube Developers experience issues with the compatibility, connector size and robustness of electrical interface standards. This paper describes the process towards a lean electrical interface for CubeSats and PocketQubes which should tackle these issues. The primary objective of this paper is to select an appropriate data bus based on extensive analysis and (future) needs of satellite developers. The secondary objective is to show targets and aggregate results of prior studies towards the definition of a lean electrical interface standard.

In this paper, the results of an extensive trade-off for the electrical interfaces for PocketQubes and CubeSats are presented. The standard electrical interfaces typically comprise one or more digital data busses used for the transport of data between subsystem and power distribution lines. Optionally, an electrical interface standard can also comprise lines for baseband radio signals, analogue signals and general input/output.

Based on design targets specified in Section 1.2, an appropriate standard data bus architecture is presented in chapter 2. Chapter 3 describes the trade-off process and chapter 4 provides trade-off results for the data bus. Chapter 5 provides a brief analysis on power distribution. In chapter 6 a new electrical bus interface standard for PocketQubes and CubeSats is proposed, which is lean, facilitates efficient power distribution and ensures inter subsystem compatibility. Finally, conclusions and a future outlook is provided in chapter 7.

* Corresponding author.
E-mail addresses: jasper.bouwmeester@tudelft.nl (J. Bouwmeester), spvdlinden@gmail.com (S.P. van der Linden), povalac@feec.vutbr.cz (A. Povalac), e.k.a.gill@tudelft.nl (E.K.A. Gill).

https://doi.org/10.1016/j.asr.2018.03.040
0273-1177/© 2018 COSPAR. Published by Elsevier Ltd. All rights reserved.

1.1. Background

In a worldwide survey on CubeSat electrical interfaces, it became clear that many CubeSat developers experience issues with the de-facto standard electrical interface based on the PC/104 connector, part of the PC/104 standard and the I^2C data bus (Bouwmeester et al., 2017). Documents which describe the pin allocation for PC/104 connectors for CubeSats do not exist and it was previously found that subsystems from different commercial suppliers use different pin allocations (Bouwmeester and Santos, 2014).

A proposal for a dedicated CubeSat electrical interface standard comes from UNISEC (Busch, 2015). It defines, amongst others, a standard 50 pin stacked connector between subsystems comprising power distribution at various voltage levels, several options for data interfaces (I2C, UART, JTAG), reset lines and several General Purpose Input/Output pins (GPIOs).

At this moment I^2C is dominant in CubeSats. However, many developers experience in-orbit issues with this bus (Bouwmeester et al., 2017). Specifically, in-orbit bus lock-ups of the I^2C data bus, the large connector, lack of a clear standardized power bus distribution and protection and lack of a fixed pin allocation were identified as key issues. The Delfi-C^3 CubeSat suffered from a high bit-error rate and bus lock-ups (Cornejo et al., 2009) with I^2C in-orbit. From these lessons learned, it can be concluded that the theoretical behavior of a data bus does not always apply in practice.

Another study proposes a split data and power interface using daisy chained connections (Riot et al., 2014) and call this the CubeSat Next Generation Bus (CNGB). For the data interface, the CAN bus was chosen with the high level of hardware supported features and extensive heritage in the automotive industry as main reasons. Details on the trade-off are, however, not provided. The paper mentions extensibility to larger than-3U-CubeSats as one of the programmatic goals. The split data and power connectors in a daisy-chained configuration is far from a small and lean solution and would not be suitable for smaller CubeSats or PocketQubes.

For PocketQubes, the only existing standard is PQ60 (Becnel et al., 2015). This standard is more clearly defined than the PC/104 implementation on CubeSats. It defines the connector, the pin allocation and the printed circuit board outline. It supports several different power outputs, SPI and I^2C data interfaces and many GPIOs. It uses a proprietary connector which is limited in current (0.2 A per pin).

The literature described above shows that most used and proposed electrical data busses are aimed at versatility, leaving a large design freedom to the subsystem developers. The disadvantage for these standards is that they do not guarantee compatibility and are far from optimal in terms of wiring harness. A lean standard with a minimum amount of clearly defined interfaces would counter these issues, but the lack of design freedom require a careful trade-off of the data bus and architecture for power distribution.

1.2. Design targets for a standard electrical interface

Following the findings described in Section 1.1, the following top level targets for electrical bus interfaces have been determined:

1. The interface is lean in volume and wiring harness.
2. The interface has a consolidated data bus and power distribution allocation.
3. The interface supports expected future performance demands.
4. The interface enables a high satellite power efficiency.
5. The interface is low in complexity.
6. The interface is expected to receive support in the community.
7. The interface is robust and reliable.

2. Standard data bus architecture and candidates

Before selecting an appropriate data bus or busses for an electrical interface standard, it is helpful to define a suitable data bus architecture for a typical CubeSat or PocketQube.

2.1. Data bus architecture

For this study, it is assumed that both satellite form factors make use of a distributed computing architecture, in which each physical subsystem of the satellite has its own microcontroller (or processor) to manage the local functionality. Some physical subsystems have components for which a digital interface is required, such as temperature sensors and reaction wheels. When they are physically implemented on the same board, a local data bus can be used, which can be of different kind and/or network topology (e.g. SPI). A central Onboard Computer manages the satellite by commanding the local microcontrollers and acquiring (housekeeping) data. Very advanced concepts, for example fractionated spacecraft or decentralized real time operations without a master node (central OBC), is considered out of scope for this study. While these concepts may have potential in the future, it is unlikely that these would receive wide community support in the short term.

For CubeSats and PocketQubes it is expected that for housekeeping data and internal commands, a linear bus connected to all physical subsystems will suffice. In a linear bus network topology, the same set of wires or lanes are used to connect multiple nodes on the bus together. This is different from a point-to-point bus, which can only connect two nodes together. A linear bus has the major advantage for very small satellites that the amount of wiring is limited when stacked connectors or some form of bus backbone is used. Secondly, the pin-out is fixed for all subsystems and the amount of potential nodes is not constrained by the amount of wiring.

A higher data rate of a linear data bus will support modest payloads connected to the same bus, which maintains a simple architecture. A linear data bus is, however, limited in speed because of cumulative electrical capacitance on the bus when adding nodes and the increasing demands on all nodes in terms of clock frequency and data handling capacity. Sophisticated and demanding payloads such as optical instruments produce, besides some modest housekeeping data, large amounts of payload data which may need to be stored and sent to selected ground stations over a high speed radio transmitter (Selva and Krejci, 2012). In a study on CubeSat science missions (Poghosyan and Golkar, 2017), it was found that high-speed radio links up to 100 Mbit/s are currently commercially available and being integrated in CubeSats. For these type of payloads it is expected that point-to-point busses will be required between the payload, potential data storage and a high speed radio.

Wireless communication inside a CubeSat is not common(Bouwmeester et al., 2017), but a few experiments have been performed with a wireless sun sensor (de Boom et al., 2011) using a proprietary wireless standard. A custom optical variant of the CAN bus has even been demonstrated as main data bus (Arruego et al., 2016). The advantages of wireless communication become most apparent for sensors which are remote from the internal printed circuit board and could potentially be self-powered and thus completely wireless (Amini et al., 2009), e.g. sun sensors. Wiring, in this case, is typically a major burden. Whenever there is potential for these sensors to locally power themselves, wireless data busses may provide a great solution. In a previous study, Bluetooth 4.0 was evaluated as one of the current best options (Schoemaker and Bouwmeester, 2014). For data communication between the main subsystems, where a wired electrical interface is required for electrical power distribution, the potential reduction in wiring harness is limited while complexity would increase.

Fig. 1 shows the proposed data bus architecture, which is considered to be appropriate to fulfill the requirements of many CubeSat and PocketQube missions in the near and long term future. All subsystems and payloads connect to a linear housekeeping bus which is mastered by the Onboard Computer. Low speed payloads can use this bus for payload data as well. Sophisticated payloads, together with data storage and a high speed transmitter, use point-to-point busses to make a high data throughput possible while relieving the onboard computer for its critical tasks. Remote self-powered wireless sensors connect to the OBC and/or ADCS through either wireless links or dedicated local data bus branches. It should be noted that individual CubeSats and PocketQubes can deviate in terms of amount and types of physical subsystems. The centralized concept, where the OBC manages the satellite as a master device is a starting point for further analysis. In this architectural concept the OBC can still be physically relocated, physically combined with other subsystems or taken over by a redundant backup system.

2.2. Linear housekeeping data bus candidates

The primary focus for this study is currently on data busses which are specified by a physical layer (ISO layer 1). As the number of existing busses and their variants is large, first a selection has been applied based on the targets described in Section 1.2. Next to these targets, only data busses which are widely applied in terrestrial environments are considered. CubeSats and PocketQubes benefit from the associated wide availability of commercial integrated circuits, test equipment, documentation and user support for these data busses.

The candidates considered for the linear housekeeping data bus are: Inter-Integrated Circuit (I^2C), differential I^2C, Controller Area Network (CAN) and Recommend Standard 485 (RS-485).

I^2C is a single ended synchronous bus: it has clock and data lines (Leens, 2009). The lines are actively pulled high by a resistor (typically 4.7 kΩ) and have to be pulled low by its controller for communication. When applied in a small satellite, bus buffers need to be added to be able to isolate unpowered subsystems from the main data bus.

I^2C can be made differential by replacing the bus buffers by a dedicated differential driver (NXP Semiconductors, 2016), which yields four lines in total. As this is an easy-to-implement feature that slightly deviates from the standard while improving the robustness of the bus, this variant is added even though it is not widely implemented yet.

CAN is an asynchronous differential data bus developed for the automotive industry (Lawrenz, 2013). Some microcontrollers include a CAN controller, but most require an external controller connected to a local data bus that is supported internally by the microcontroller (e.g. SPI). An external differential driver is required in both cases.

RS-485 is an asynchronous differential data bus. It uses the Universal Asynchronous Receiver Transmitter (UART) that can be found on almost every microcontroller (Soltero et al., 2010). A dedicated external differential driver is required to make a RS-485 bus. This bus is the only one of the four options which is only specified on the physical layer and not on the higher OSI (Open System Interconnection) layers.

3. Trade-off process for housekeeping data bus

This chapter describes the trade-off method, criteria, test setup and community survey input.

3.1. Trade-off method

Trade-offs with multi-disciplinary criteria are sensitive to errors and subjective scoring and weighting. Furthermore, a typical pitfall is to assign scores relative to the option space rather than the overall project or system

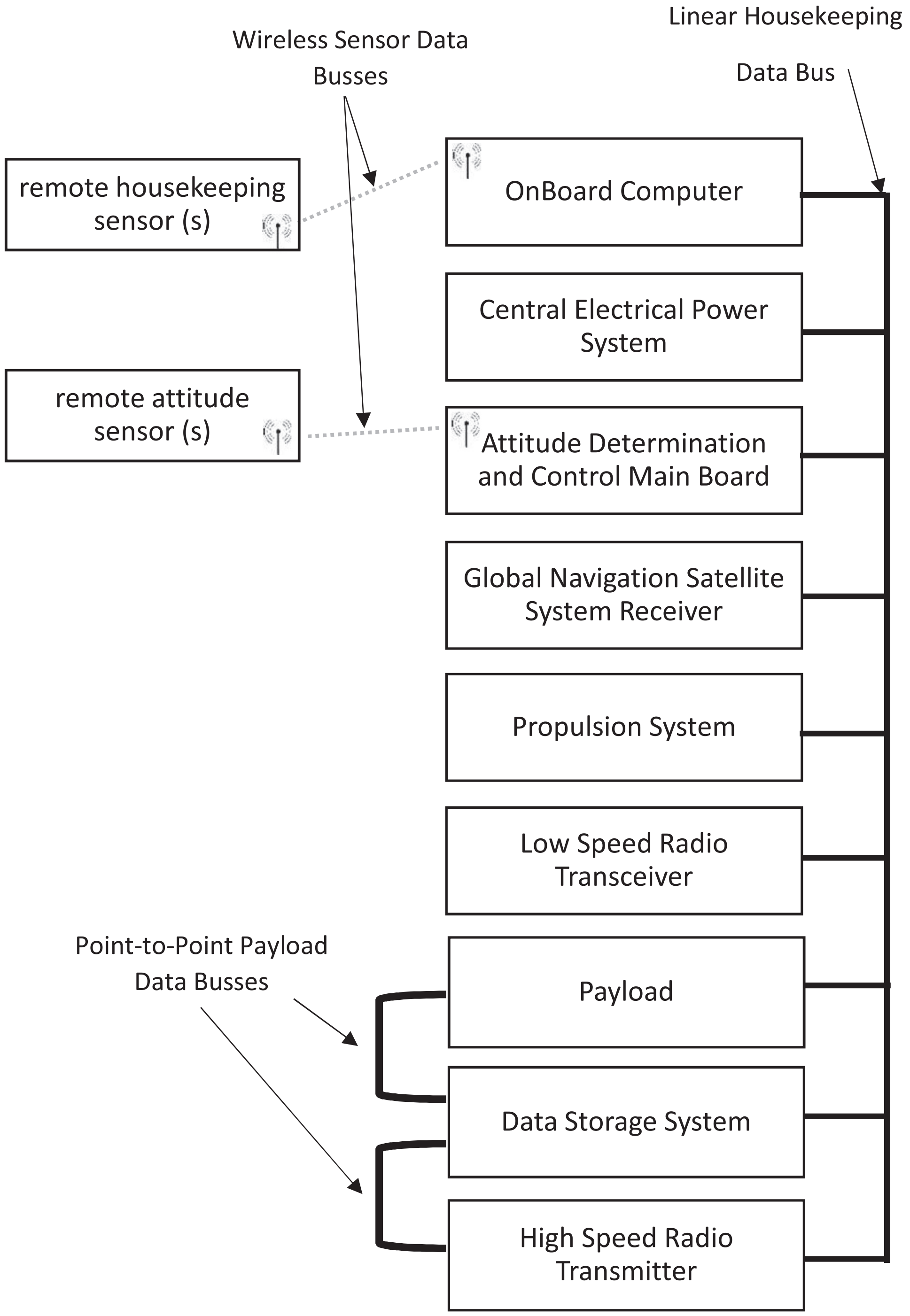

Linear Housekeeping
Data Bus
Wireless Sensor Data
Busses
remote housekeeping sensor (s)
OnBoard Computer
Central Electrical Power System
remote attitude sensor (s)
Attitude Determination and Control Main Board
Global Navigation Satellite System Receiver
Propulsion System
Low Speed Radio Transceiver
Point-to-Point Payload
Data Busses
Payload
Data Storage System
High Speed Radio Transmitter

Fig. 1. Proposed data bus architecture (example).

scope. For example: a component trade-off leads to the discovery of several options ranging from € 2 to € 20. If the option space would be used to define a linear scoring range from 1 to 10, the individual score would be equal to the component cost divided by € 2. The cheapest option receives a score of 1 and the most expensive receives a score of 10. This may make sense for a € 100 mobile phone, but not for a 100 k€ satellite project.

Methods dealing with some of the sensitivities of trade-offs exist, such as the well-established Analytic Hierarchy Process (AHP) (Saaty, 2008). This method provides a structured approach to derive criteria, relative weighting of these criteria and the grading of all options for each criterion. Saaty, however, also states that the *interpretation* of an option within a certain criteria, even if these itself are objective facts, is always subjective. The AHP method uses pair-wise comparisons between criteria and options to simplify the choices for the user. The fundamental scale used for these comparisons is presented in Table 1. Each pair-wise comparison enters together with its reciprocal in an

Table 1
Fundamental scale for pairwise comparisons in AHP (Saaty, 2008) schoe.

Intensity of importance	Definition	Explanation
1	Equal	Two elements contribute equally to the objective
3	Moderate	Experience and judgement moderately favor one element over another
5	Strong	Experience and judgement strongly favor one element over another
7	Very strong	One element is favored very strongly over another, its dominance is demonstrated in practice
9	Extreme	The evidence favoring one element over another is of the highest possible order of affirmation

n x n matrix, where n are the amount of options. When the table is filled, the normalized eigenvector of the matrix is calculated to provide the resulting priorities (weights) for the options. Different weights to multi-disciplinary criteria can lead to the most acceptable compromise between different subjective perspectives. While weighting between criteria are, per definition, subjective and require only high-level expertise, grading can be based on facts and requires more detailed insight into the topic. For the trade-off of the housekeeping bus it was chosen to derive the criteria and setup a grading table for the options per criterion between the authors of this paper and reviewed by several staff members at TU Delft with data bus experience. For the weighting between all criteria and the scoring of some criteria, the community is involved in the AHP using a questionnaire as elaborated in Section 3.5.

3.2. Derivation of trade-off criteria

In Fig. 4 a first derivation of trade-off criteria is presented, which come from the design targets described in Section 1.2.

Some of the identified criteria are omitted after theoretical analysis. These boxes are marked solid grey in Fig. 2 and the number between brackets refer to the following reasons:

1. These criteria are not considered to be very important. A housekeeping data acquisition and commanding cycle in the order of 1–10 Hz, managed by the Onboard Computer as master, is a typical approach (Bouwmeester et al., 2007) that works very well and does not require low latency or multi-master support.
2. The difference between the data bus options for these criteria are considered to be too small or out of scope. RS-485 supports 32 nodes and the others even a few hundred. RS-485, CAN and I^2C require 2 wires and dI^2C just 4. For all busses, the required integrated circuits are widely available from different manufacturers and are all very low in cost (a few €/US$).
3. There is no good metric or data available for these criteria. For complexity of integration, there is too limited community experience for RS-485, dI2C and CAN to aggregate subjective input. Sufficient statistical input for these busses is also missing for in-orbit reliability, which would give I^2C an unfair disadvantage (Bouwmeester et al., 2017).

As a next step, initial laboratory tests (see Section 3.4) have been performed to discover if the derived criteria can deliver appropriate results which can be used for comparison with a reasonable amount of effort. This lead to a further reduction in criteria after practical analysis, for which the boxes are marked patterned grey for the following reasons:

4. Continuity as criterion refers to the ability of the data bus to operate continuously with bus lockups or other events which cause temporary unavailability of the bus. The chosen metric for this is the amount of disruptive events per time unit, in which less than once per 24 h would receive the highest grade. In the initial tests all four data busses did not show any such disruption, even when subjected to electromagnetic interfere (see next point).

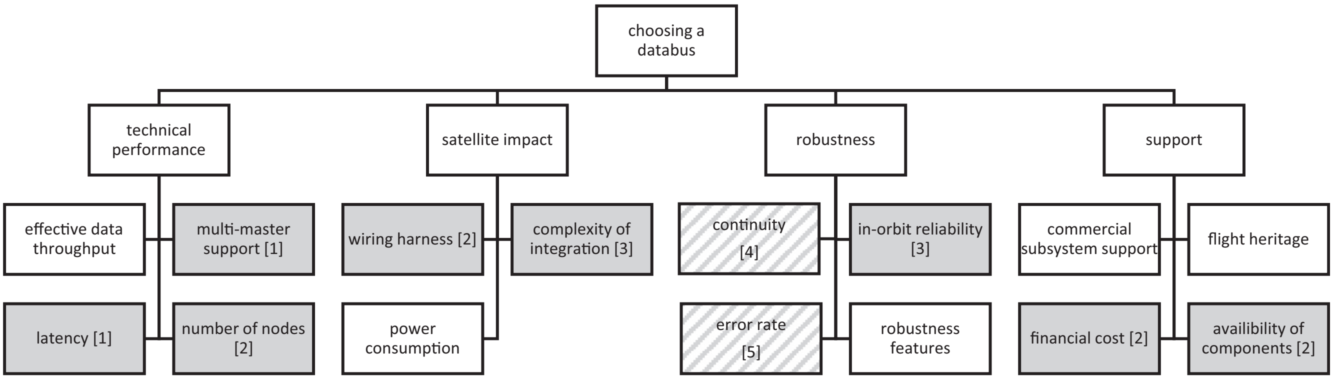


Fig. 2. Derivation tree for criteria (grey/patterned boxes are omitted after theoretical/practical analysis).

5. Error rate as criterion refers to the number of (bit) errors per number of transactions or bits. The chosen metric was the Packet Error Rate (PER) which could be discovered by a check of the CRC in each transaction. A packet error would indicate one or more bit errors within the transaction. A PER of less than one-in-a-thousand would receive the highest grade. All four data busses were tested for about 30,000 transactions each. In ambient conditions none of them showed packet errors. Tests have also been performed at high computational load on the microcontrollers (continuously calculating pi) and when the microcontrollers receive interrupts (up to 1000 Hz with high interrupt priority). In all those tests, no packet errors have been detected. Finally, tests have been performed by injecting simulated Electro Magnetic Interference (EMI). First by a direct injection of white Gaussian noise on the bus lines with capacitive coupling and a signal generator. All data busses withstood a noise injection up to 0.8 V RMS without any packet errors, but it must be noted that the peak-to-peak voltage levels generated by the used signal generator are, in this case, already beyond 10 V. This is significantly higher than the signal reference level of 3.3 V used by all data busses and beyond the electrical specification of their integrated circuits. Only at even higher noise levels, the busses showed packet errors and lock-ups. Lab experiments with a spare model of Delfi-C^3 and subsystems of Delfi-n3Xt (specifically the reaction wheels and magnetorquers) showed noise levels below 1 V. These satellites are not representative for all CubeSats and PocketQubes, but show that a sample selection of a few subsystems is not appropriate to identify EMI sources which do results in disruptions and communication errors. Other tests were performed to simulate power transients on lines with switching currents of several amperes, including in-rush currents of several tens of amperes. In all cases, there were no packet errors discovered. After several experiments it became clear that all busses are resilient to a significant amount of noise. Still, there is insufficient knowledge of EMI levels, characteristics and test methods which would be appropriate to simulate a wide scale of PocketQube and CubeSat configurations including more "exotic" components (e.g. pulsed plasma thrusters) within a reasonable amount of effort. It is therefore decided to omit test-based inputs for error rates and only focus on inherent robustness properties of the data busses themselves.

The experiences with the test setup are not in line with the in-orbit experiences with the I^2C data bus as described in Section 1.1. During the development of the test setup and even the initial EMI testing, bus lock-ups and significant errors appeared on all tested busses. This resulted in the discovery of several flaws in the software drivers of the test setup which have been corrected appropriately. The test setup used for this paper is based on all the same microcontrollers and the software is extensively debugged, which is different than for Delfi-C^3 and potentially also for other flown CubeSats. In the specific example of Delfi-C^3, it was found that the clock speed of the microcontrollers, the I^2C software drivers and differences between the I^2C hardware drivers within the microcontrollers have caused disruption and significant error rates (Cornejo et al., 2009). It is expected that I^2C problems on Delfi-C^3 could have been solved before launch but would have required extensive testing, debugging of software and even changes to the hardware. The experiences show that in-orbit experiences cannot directly be projected to the intrinsic reliability of a data bus and that a fair comparison on reliability can only be performed if the both hardware and software are extensively tested and corrected for development errors and/or inadequate choices for relevant components.

The remaining criteria are worked out further and for some sub-criteria are added. Fig. 3 presents the final trade-off criteria tree for choosing a data bus.

Effective data throughput refers to the maximum amount of data which can be transferred over the bus from the master (OBC) to the slaves and back. It is the sum of all message content over the bus, excluding addressing, protocol overhead and timing delays.

The power consumption of the linear data bus is dependent on the number of nodes and the data throughput. As this may vary between missions, three reference use cases for the linear data bus have been defined:

Basic: a satellite with 5 subsystem nodes with a data and command cycle of 1 Hz. Payload could be a very low data rate sensor or a technology demonstration of (part of) a subsystem.

Moderate: a satellite with 9 subsystem nodes with a data and command cycle of 1 Hz. Payload could be similar to the basic case or could be sophisticated using dedicated point-to-point data bus(ses) as depicted in Fig. 1.

Advanced: a satellite with 9 subsystem nodes at a relatively high data rate compared to the basic and moderate case. The high data rate can be attributed to a significantly higher data and command cycle and or a payload with moderate data rate which does not yet justify a dedicated point-to-point data bus. The effective data rate is fixed to approximately 250 kbit/s for this case, which was expected to be supported by the four chosen options.

The robustness features are EMI susceptibility and level of hardware control. The best attribute to judge EMI susceptibility on, based on the four options, is the difference between non-differential (I^2C) and differential (dI2C, RS-485 and CAN), where the latter is generally less susceptible due to common mode noise rejection. Testing under normal conditions did not show any errors including for regular I^2C. More intense EMI environments are unknown, so there is no quantitative metric based on value input possible for this criteria. It is therefore chosen to ask the com-

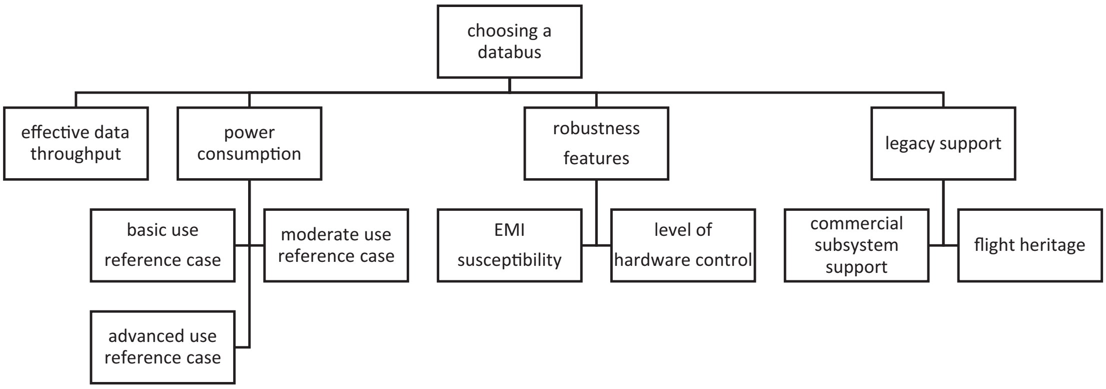

choosing a databus
effective data throughput
power consumption
robustness features
legacy support
basic use reference case
moderate use reference case
advanced use reference case
EMI susceptibility
level of hardware control
commercial subsystem support
flight heritage

Fig. 3. Final criteria tree for trade-off.

munity on their judgement, using the fundamental scale of AHP to determine the relative grades. For the level of hardware control, pairwise comparisons between three levels have been used:

- large part of the data protocol and potential error detection and failure handling needs to be implemented in the software (RS-485)
- a hardware controller for the full data protocol, but where the potential error detection and failure handling needs to be implemented in the software (I^2C & dI^2C)
- a hardware controller for the data protocol including internal error detection, correction and failure handling (CAN)

RS-485 required the full data protocol and any software error detection and correction to be fully implemented in software. The UART and the differential driver only provides the physical layer. This means that the microcontroller needs to allocate relatively the highest amount of resources to the data bus and potential software bugs or interrupt/state control within the microcontroller could more easily lead to anomalies on the data bus compared to hardware control. I^2C and dI^2C do have the data protocol defined and implemented in the hardware controller. This will offload the microcontroller and is less prone to software bugs. CAN even has error detection and correction included in the hardware controller, which would make it most robust in this respect. However, the statements above are only true if the hardware controller has no flaws in the state-machine. Practical experience with I^2C shows that this is not always the case (Cornejo et al., 2009) and the high amount of bus lockups experienced by developers in orbit (Bouwmeester et al., 2017) may be an indication of a larger problem. Given the high degree of subjectivity in this matter, grading for this criterion is again based on the community judgement in pair-wise comparisons.

Finally, the legacy support of the data busses are taken into account. One sub-criterion is the commercial subsystem support. The rationale is that, of all available commercial subsystems, one can more easily and quickly adopt the wiring interface if the data bus is already supported. Alternatively, one can use a relatively simple interface-to-interface connector for the new proposed electrical interface standard compared to a situation where the subsystem does not yet support this data bus. The second sub-criterion is the flight heritage, which is based on the results of a survey performed on CubeSats (Bouwmeester et al., 2017). Both criteria are value based, but in terms of relative grades they do not have a direct technical impact on the satellite such as the effective data rate or power consumption. Therefore the community is asked to define the grading range for each.

3.3. Grading for final criteria

As next step, the grading is determined for the trade-off, which is presented in Table 2. The grade ranges for criteria using quantitative input are based on internal experience as well as studies of worldwide CubeSats (Bouwmeester and Guo, 2010).

The AHP method uses normalized grades and weights in which the individual grades for the options and the weights of the criteria need to add up to 1. Therefore, some of the grades from Table 2 need to be normalized before entering the next step of the trade-off. It also should be noted that community experience for CubeSats is also considered as input for PocketQubes as it involves flight heritage on very small satellites and public documentation on implementation lessons learned.

3.4. Housekeeping data bus comparative test setup

This section describes the final test setup for the input for grading effective data throughput and power consumption.

The test setup comprises up to nine Texas Instrument's MSP432 microcontroller development boards. The MSP432 is a modern microcontroller which is chosen as the default controller for the Delfi-PQ PocketQube of TU Delft due to its low power over computational load ratio. The data bus specific hardware is placed on daughter boards which can be stacked on top of the development

Table 2
Grading table for linear housekeeping data bus.

Criterion	Grade
Effective Data Throughput	$= \frac{D}{1000\ \mathrm{kbit/s}}$ where D = effective data throughput *if $D < 6$ kbit/s → reject option*
Power Consumption	$= 1 - \frac{P}{T}$ P = total power consumption for data bus T = threshold For PocketQube/CubeSat: T_{basic} = 50 mW/200 mW $T_{moderate}$ = 100 mW/400 mW $T_{advanced}$ = 200 mW/800 mW *if $P > T$ → reject option*
Robustness Features	Fully AHP survey based, see Section 3.2
Legacy Support	$= \frac{1+(S-1)\cdot I}{S+1}$ S = AHP scale factor, see Table 1 $I_{COTS\ S/S\ support}$ = implementation rate fraction on commercial CubeSat or PocketQube subsystems in which a standard UART support counts half for RS-485 and regular I^{2}C counts half for dI^{2}C $I_{flight\ heritage}$ = implementation rate fraction on CubeSats from survey (Bouwmeester et al., 2017)

boards. A ribbon cable connects all boards. The power consumption is measured at the input power which is run to all boards by means of a high precision current meter. Before each test, the power consumption of each developments board is measured without the daughter boards. This value is subtracted from the measured power during the data bus tests. The complete setup is shown in Fig. 4.

For I^{2}C, the dedicated internal controller on the MSP432 is used and a data bus buffer is added per board. The circuit is represented in Fig. 5. For differential I^{2}C, the data bus buffer is replaced by a dedicated differential driver as shown in Fig. 6. For RS-485, the UART of the MSP432 is used and a dedicated differential driver is added to the UART as shown in Fig. 7. For CAN, both an external controller and a driver are required as shown in Fig. 8. CAN is the only data bus under consideration which is not supported with an internal controller onboard the microcontroller chip. It has to be noted that there are some

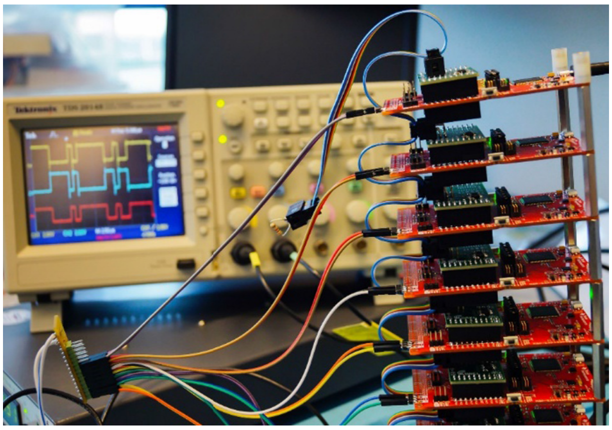


Fig. 4. Test setup for data bus characterization.

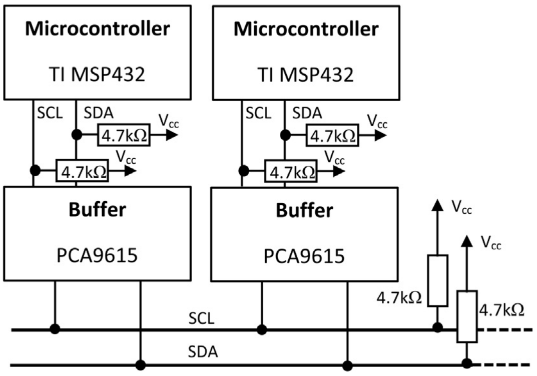


Fig. 5. I^{2}C circuit.

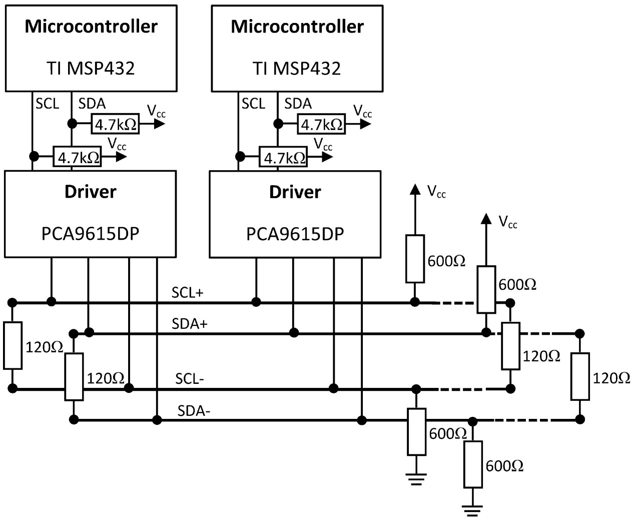


Fig. 6. dI^{2}C circuit.

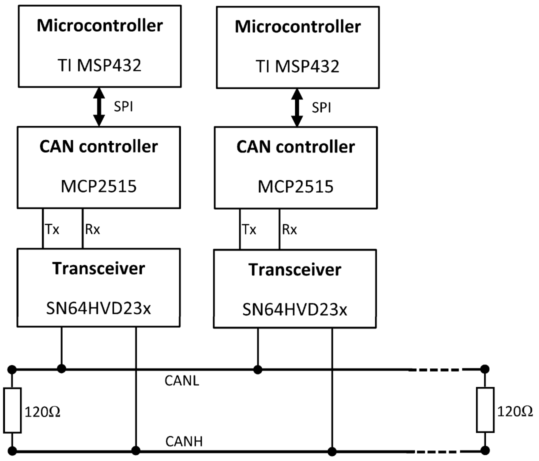


Fig. 7. CAN circuit.

microcontrollers available with internal CAN controllers. This may positively influence the power consumption, but this will limit the choice of microcontrollers severely and may require major adaptations of existing subsystem designs. For all data busses, a list of potential components are selected which operate at 3.3 V level. From this list, the ones with the lowest power consumption according to the manufacturer specification is selected out of a list of options from different manufacturers. For all busses, bias and termination resistors are chosen following the recommended specification to ensure optimal behavior and noise rejection.

For testing the power consumption and throughput efficiency, a reference case communication scenario has been established in Table 3 which is based on both the architecture and example provided in Fig. 1. It is assumed that this standard communication set is cyclic at 1 Hz. The data packet size are based on experience with Delfi satellites and commercial CubeSat hardware. Large packets, not supported by a data bus (e.g. CAN), will be broken up in sequential packets.

While the reference communication set is a realistic representation of the architecture and subsystem structure provided in Fig. 1, it does not apply for satellites with modest payloads that may not require dedicated payload data busses. Also, the frequency of 1 Hz is arbitrary and can be higher or lower depending on the specific needs of the mission. To determine the maximum effective throughput of the data bus, the set in Table 3 is simply looped continuously without pause. For satellites with payloads using relatively large data packets, the average overhead may decrease and thus the effective throughput maybe higher. It is, however, expected that the variations for different scenarios will not lead to very large deviations in outcome and will be even more marginal, in a relative sense, between data busses.

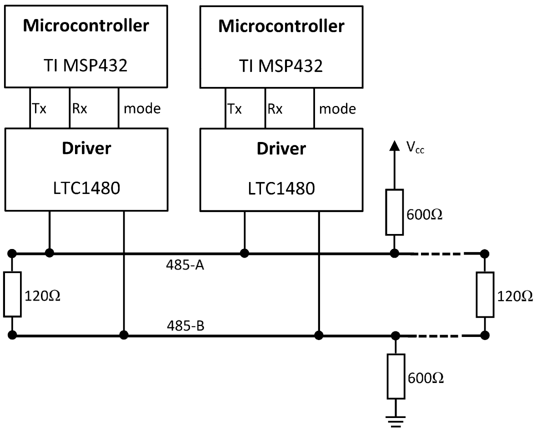


Fig. 8. RS-485 circuit.

Table 3
Reference communication set for linear housekeeping data bus.

Source node		Recipient node		Size [bytes]
1.	OBC	3.	EPS	2
3.	EPS	1.	OBC	30
1.	OBC	4.	ADCS	2
4	ADCS	1.	OBC	120
1.	OBC	6.	GNSS	2
6.	GNSS	1.	OBC	30
1.	OBC	7.	Propulsion	2
7.	Propulsion	1.	OBC	10
2.	OBC	2.	H/K radio	2
2.	H/K radio	1.	OBC	10
1.	OBC	5.	payload	2
5.	Payload	1.	obc	10
1.	OBC	9.	Data storage	2
9.	Data storage	1.	OBC	10
1.	OBC	8.	P/L radio	2
8.	P/L radio	1.	OBC	10
1.	OBC	9.	Data	250
1.	OBC	2.	H/K radio	250
Total of node 1–5, 9 packets:				*428*
Total of node 1–9, 18 packets:				*746*

3.5. AHP questionnaire for community input

A questionnaire has been set up and sent in March 2017 to 36 and 453 members of the PocketQube and CubeSat community respectively. It has been decided to keep these communities separate, as the characteristics of these two different form factors are very different (in terms of volume, power, sophistication of payloads, flight heritage, etcetera). The questionnaire was sent out in March 2017 and had a response of 34 participants from the CubeSat community, representing 30 different development parties from around the world. Likewise, there were 15 participants representing 10 different development parties from the PocketQube community.

All questions provide input for the mutual weighting of sub-criteria followed by the main criteria in pair-wise comparisons using the AHP scale (see Table 1). Some of the final grades and all mutual weights are determined using the input and an Excel-based tool (Goepel, 2013) that calculates the AHP output.

4. Housekeeping data bus results

4.1. Power consumption

The test results on the power consumption of the data busses are presented in Figs. 9 and 10. The graphs shows the total power consumption of each data bus for the amount of bus nodes attached. The standard deviation between the four independent test runs for all test points is 6.5 mW. The confidence interval can be determined by:

$$\left(\bar{x} - z^* \frac{\sigma}{\sqrt{n}}, \bar{x} + z^* \frac{\sigma}{\sqrt{n}}\right) \tag{1}$$

where

$\bar{x}$ = mean
z^* = confidence interval index
σ = standard deviation
n = number of measurements

The 95% confidence interval ($z^* = 1.96$) for the four test runs ($n = 4$) is +/− 6.4 mW for the data presented in Figs. 9 and 10.

For the trade-off, the input data are taken from the 5 node and 9 node points in Fig. 9 and the 9 node points from Fig. 10. The values are presented in Table 4. The reference use cases are described in Section 3.2 and elaborated in Section 3.4. The power consumption for 9 nodes at the maximum data throughput is also provided.

The grades are calculated by entering the data from Table 4 into the grade equation in Table 2. As a next step, the grades have been normalized to the sum of one (required by AHP) and are subsequently multiplied by the calculated relative weights per participant following from the community survey. This yields individual priorities (grades) for the criterion of power consumption. For CubeSats, the mean weight of all participants are 0.29 for the basic, 0.31 for the moderate and 0.40 for the advanced use reference case. For the PocketQubes these are 0.42, 0.16 and 0.42 respectively. The priorities are presented in Fig. 11 which shows a boxplot for the spread of individual priorities. The end of the legs show the minimum and maximum, the end of the boxes show the first and third quartile of all participants and the line in the middle shows the median. Additionally, the cross shows the mean of all participants and the dot shows the relative amount of participants for which the specific data bus received the highest priority.

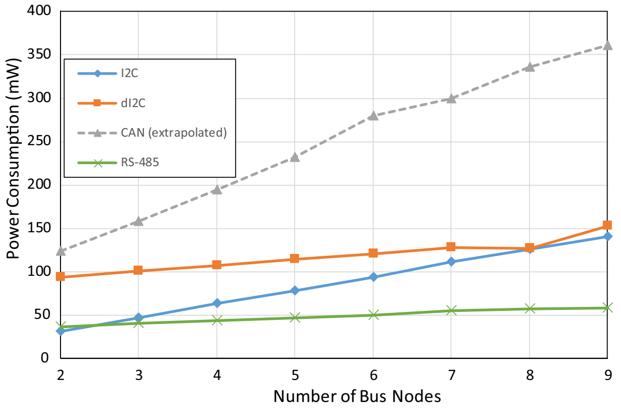


Fig. 10. Power consumption for 250 kbit/s.

Table 4
Power consumption for the trade-off use reference cases.

Use case	Power consumption [mW]			
	I^2C	dI^2C	CAN	RS-485
Basic	52	36	139	9
Moderate	95	63	268	11
Advanced	141	153	362[a]	59
Maximum	139	154	318	108

[a] Extrapolated from maximum data rate of 136 kbit/s and idle consumption.

From Fig. 11 it can be concluded that for PocketQubes, RS-485 has a clear advantage over the other busses. CAN, on the other end, does not meet the rejection threshold and should therefore be omitted as option for PocketQubes. Because of limitations of the AHP method, it still is included in the final trade-off with the grade for this criterion set to zero. For CubeSats, the spread of priorities for this criterion is significantly less, which can be explained by the higher reference power levels as presented in Table 2.

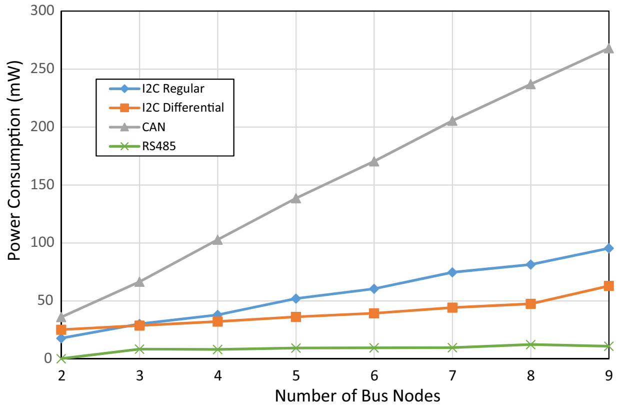


Fig. 9. Power consumption for one communication set per second.

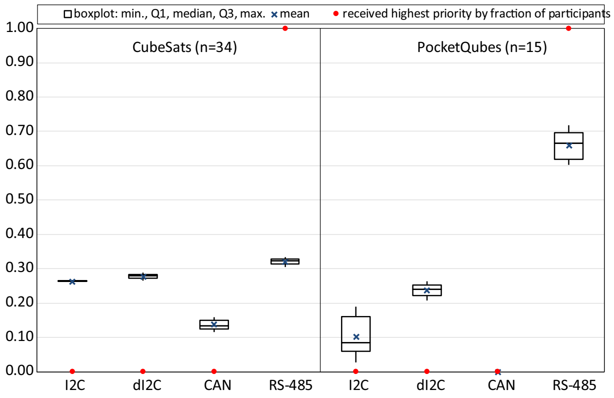


Fig. 11. AHP priorities on power consumption.

4.2. Effective data throughput

Table 5 provides the effective data throughput at the advanced reference case which is used for input of the trade-off. The initial grades based on Table 2 are normalized to calculate the AHP priority.

I^2C, dI^2C and RS-485 both have a theoretical calculated data efficiency of about 80% for the communication set in Table 3. The measured efficiencies are lower, which can be attributed to the latencies of about 20% of total transaction time within the microcontroller of handling the data.

One of the reasons for the relatively low effective data throughput and also low data efficiency of CAN be found in the protocol overhead. A CAN frame with the maximum of 64 bits of message content is, in total, 114 bits (for the base frame format) including protocol overhead, so the efficiency is at best 56%. For a small 16-bit message, the total CAN frame is 66 bits, yielding an efficiency of 24%. Due to Non-Return-to-Zero (NRZ) encoding, bit stuffing is needed, which reduces efficiency up to 20%. The expected data rate in Table 5 is based on the communication set in Table 3 and 10% bit stuffing. Including the probable latency factor of the microcontroller, one would still expect an efficiency of approximately 40%. The best explanation for the gap between theory and test results are the latencies caused by the additional SPI interface between the microcontroller and the CAN controller. There is thus a potential gain in effective data throughput if internal controllers are used. The sensitivity of final trade-off for a theoretical improvement up to 400 kbit/s for CAN is investigated in Section 4.5.

4.3. Robustness features

For determining the priorities on the main criterion ‘robustness features’, the AHP community survey is used for prioritization of the sub-criteria. This is explained in Section 3.2. The priorities are shown in Fig. 12. CAN receives the highest priorities since it is a differential bus and has a high degree of hardware control. The mean relative weighting between the two sub-criteria is almost equal for CubeSats and PocketQubes, leading to a balance between I^2C and RS-485 and a slight advantage for dI^2C.

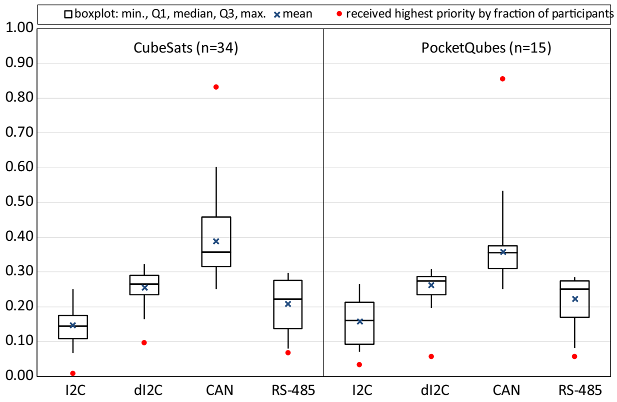


Fig. 12. AHP priorities on robustness features.

4.4. Legacy support

The input used for the legacy support is presented in Table 6. For CubeSats, a wide survey of the market has been performed within this study with a large variety of commercial suppliers and (for each supplier) different subsystems. In total 56 different main physical subsystems coming from 23 different manufacturers have been selected. For the grade input, dI^2C receives 50% of result for I^2C support and whenever UART is mentioned instead of RS-485 explicitly, this is counted for 50% as well. The rationale is that the change from I^2C to dI^2C and generic UART to RS-485 require small modifications for which a major part of the legacy support is maintained. For PocketQubes, only 3 commercial systems were found. This is very low, making this a sensitive input for which the impact on the final result will be checked.

For this criterion, the grade input data is scaled to the AHP range as determined from the survey (see Table 2). The priorities for the legacy support are provided in Fig. 13. I^2C receives the highest priorities, which can be explained by the input data. However, the levels of priorities are reduced in range compared to the input values as for both sub-criteria and both satellites form factors, the mean importance is rated moderate to strong. Some participants have given equal priority to each level of support, which is the reason that I^2C does not score 100% of the received highest priorities.

4.5. Final trade-off

Finally, the weights between the four main criteria are determined using the AHP community survey and provided in Fig. 14. The relative priority of each criterion is multiplied by its relative weight and summed for each option, leading to the final priorities as provided in Fig. 15.

For PocketQubes, RS-485 received the highest priority for 12 out of 14 participants. This is explained by the high

Table 5
Effective data throughput at advanced reference case.

Data bus	Baud rate of controller	Expected data efficiency	Measured effective data throughput	Data efficiency	AHP priority
I^2C	400 kHz	80%	248 kbit/s	62%	0.20
dI^2C	400 kHz	80%	258 kbit/s	65%	0.21
CAN	1 MHz	51%	136 kbit/s	14%	0.11
RS-485	1 MHz	79%	600 kbit/s	60%	0.48

Table 6
Grade input data for data bus legacy support.

	CubeSat flight heritage (n = 56)	CubeSat commercial subsystem support (n = 52)	PocketQube commercial subsystem support (n = 3)
I2C	78%	40%	60%
dI2C	39%	20%	30%
CAN	5%	20%	0%
RS-485	4%	20%	10%

relative weight for power consumption in combination with the high relative priority on this criterion for RS-485.

For CubeSats, RS-485 also received the majority of highest priorities (19/34), followed by CAN (11/34). For CubeSats the criterion ‘robustness features’ received a high weight, which is in favor of CAN. Still, the combined weights on effective data throughput and power consumption and the relative good performance of RS-485 on these aspects swings the trade-off for many participants towards this data bus.

As mentioned in Section 4.4, the trade-off is potentially sensitive to the limited available commercial subsystems for PocketQubes for this study. If the sub-criterion would be omitted, the final priorities only changes slightly in favor of CAN and RS-485 while the distribution of highest priorities over the data bus options remain the same.

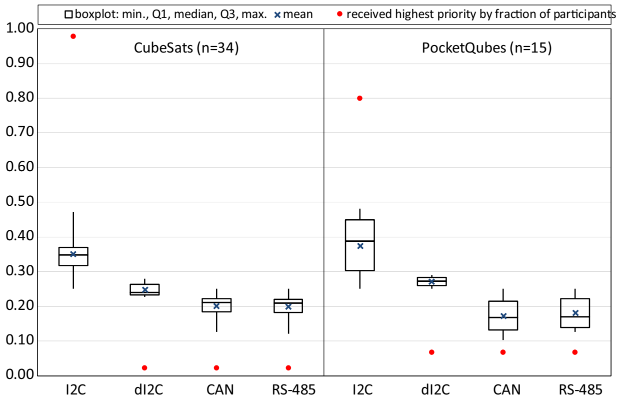


Fig. 13. AHP priorities on legacy support.

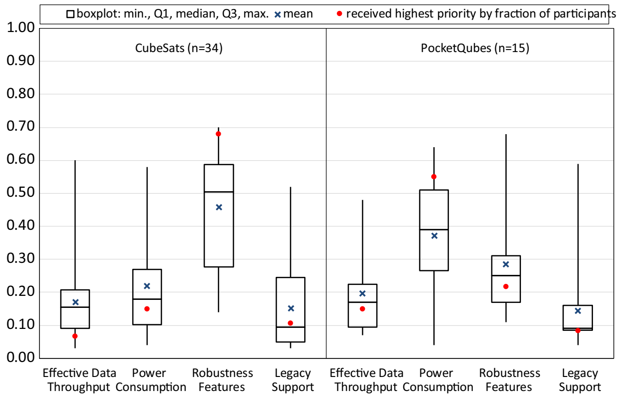


Fig. 14. AHP weights of main criteria.

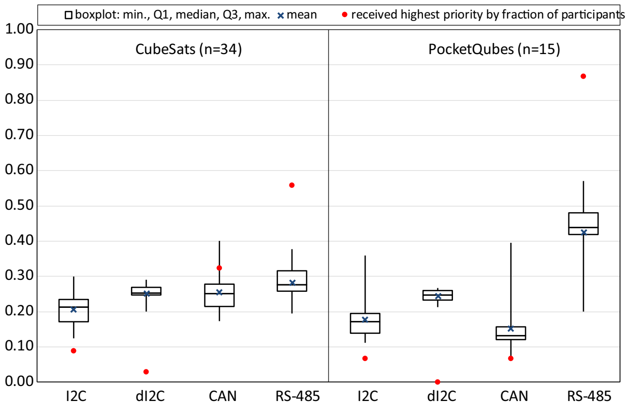


Fig. 15. Final AHP priorities.

As mentioned in Section 4.2, the effective data throughput of CAN in the test setup has been found to be significantly lower than expected. If this data rate would be improved to a theoretical data rate of 400 kbit/s, CAN would receive the highest priority by 13 out of 34 participants for CubeSats, while RS-485 would drop to 16 out of 34 participants. For PocketQubes, there is no effect on the final outcome of highest priorities.

5. Electrical power distribution

In a previous study on the distribution of electrical power in CubeSats (Bouwmeester and Santos, 2014), the following conclusions and recommendations for a new interface standard were made:

- Limit the amount of supply voltages and fix the topology for all subsystems.
- Limit the amount of conversion steps needed.
- Fix the pin definitions such that incompatibility cannot occur.
- Fix the range of variable bus voltages, which is e.g. used by the battery.
- Use flex-rigid wiring in combination with side-mounted connectors to save board space.

The study concludes with two suggested options, of which the most simple and power efficient solution (based on the design targets in Section 1.2) is chosen for the proposed interface standard in this paper. In Fig. 16, a schematic overview of the power distribution is presented in which the unregulated battery bus is distributed via 4 or 8 configurable current protected switched outputs. Regulation occurs at the subsystems locally.

Single event upset and software state errors can lock up a data bus or halt the operations of the OBC. In the current philosophy, subsystem redundancy concepts are omitted.

The central EPS can solve some issues with a power cycle of the full satellite, either at a default fixed interval (e.g. once per day) or when it does not receive e.g. a repeating synchronization message for a while from the OBC. Still, such methods do not mitigate all errors, such as on the central EPS itself. A reset line from the primary radio receiver to the EPS is recommended. The radio receiver should be able to decode a reset tele-command and pull the reset line high. The line is pulled low by a resistor and a decoupling capacitor near the input at the central EPS unit. At the central EPS, the power of the EPS microcontroller and all distribution lines are taken down for a few seconds to enforce a true power cycle of all systems.

6. Proposed electrical interface standard

Based on the trade-off results on the data bus and the analysis on the power distribution as well as the design targets stated in Section 1.2, the simplest solution for an electrical interface standard is defined and presented in Fig. 17 and Table 7. For the PocketQube, a 9 pin interface connector is defined (the first 9 pins in the figure) and is called PQ9. For CubeSats, a 14 pin connector is defined in similar fashion, by adding 4 power distribution lines, and is called CS14. The first nine pins of CS14 are similar to PQ9, but due to the different voltage range, not identical. However, since the power distribution requires local regulation, it is very well possible that the local DC-DC convertors can handle the entire input range from 3.0 to 8.2 V. This would create an opportunity to easily create a CubeSat version of a PocketQube system or to stack several of these PocketQube boards on a CubeSat motherboard.

In a previous study (Bouwmeester et al., 2017), a flex-rigid backbone in combination with side-mount connectors was suggested for wiring harness with main rationale to limit the amount of board space. However, since the number of pins selected in this paper is very low, such a solution would not be optimal in terms of board space. The final type of connectors and/or wiring harness chosen is a single row 2 mm pitched stackable pin header connection. These connectors are low in cost, available in different stack heights, sold by different manufacturers and proven in space since they are very similar to the PC/104 connector. The mechanical outline of the printed circuit boards for PQ9 and CS14 are shown in Figs. 18 and 19. A hardware example of PQ9 is provided in Fig. 20. When comparing PQ9 to PQ60 it has about 15% of the pins and 30% of the connector footprint area. For CS14 compared to PC/104 this is 13% and 8% respectively.

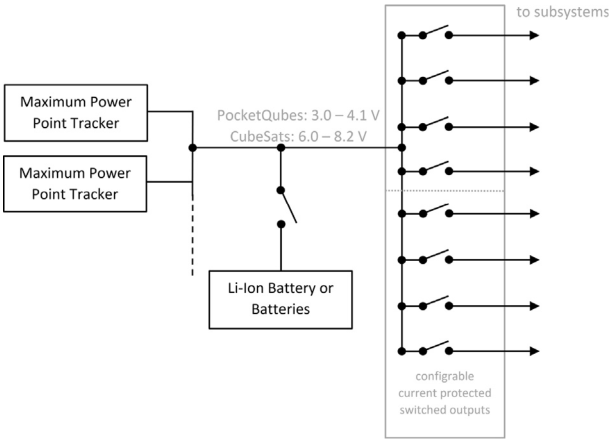

to subsystems
Maximum Power Point Tracker
Maximum Power Point Tracker
PocketQubes: 3.0 – 4.1 V
CubeSats: 6.0 – 8.2 V
Li-Ion Battery or Batteries
configrable current protected switched outputs

Fig. 16. Power Distribution Schematic Overview.

7. Conclusions and outlook

A proposal for an electrical interface standard for CubeSats and PocketQubes has been established. The main target is towards a lean standard which meets expected future demands as opposed to existing versatile standards which exhibit the risk of incompatibility between subsystems from different developers.

Based on the defined set of selection criteria, community survey input and the AHP trade-off method, RS-485 is favored as housekeeping data bus for both PocketQubes and CubeSats. Tests results show that it outperforms I^2C, dI^2C and CAN in terms of power and effective data throughput. In terms of robustness features, it comprises differential signaling, but a low level of hardware control. In terms of legacy support is scores relatively low, but this is a criterion which can easily be improved in the future if the proposed electrical interface is adopted by multiple parties. For a future study it is recommended to test the RS-485 bus for very high data rates such that it can be used as a point-to-point payload data bus for demanding payloads (or RS-422, which is very similar in point-to-point configuration), data storage and high speed radio transmitters. Also, it is recommended to perform in-orbit tests with self-powered sensors over a wireless Bluetooth Low Energy connection to be able to reduce wiring harness to components which cannot be integrated in the internal stack of subsystems.

Power distribution can best be done by supplying the unregulated battery voltage over switched and protected lines to (groups) of subsystems. This limits the number of pins used and reduces conversion losses. Power protection features and duty cycling of subsystems to save power can be implemented at the central EPS unit. Together with the chosen data bus, this yields a 9-pin (PQ9) and 14-pin (CS14) standard electrical interface for PocketQubes and CubeSats respectively. PQ9 has only 15% of the electrical interface lines compared to PQ60, CS14 only 13% compared to PC/104. This saves in both cases significant board space, but more importantly leads to a very lean interface which with a lower risk for incompatibilities between physical subsystems. However, it comes at the cost of versatility and developers freedom.

An important assumption made in this study is that CubeSats and PocketQubes do not use redundancy for main subsystems. While the proposed interfaces do not prohibit this per se, the lack of a redundant data bus and

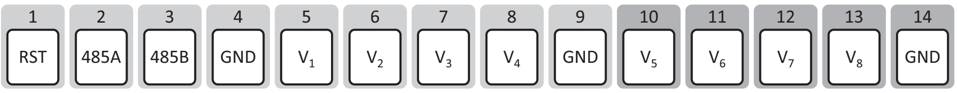


Fig. 17. PQ9 (pin 1–9) and CS14 (pin 1–14) interface connector.

Table 7
Pin allocation for PQ9/CS15 standard interface.

Pin	Signal	Allocation
1	RST	System reset line (60 Ω to gnd)
2	485-B	RS-485 inverting signal
3	485-A	RS-485 non-inverting signal
4	GND	Ground
5	V_1	rec.: OBC (PQ: + Radio)
6	V_2	rec.: ADCS (PQ: + GNC)
7	V_3	rec.: propulsion
8	V_4	rec.: primary payload(s)
9	GND	Ground
10	V_5	rec.: radio
11	V_6	rec.: GNC
12	V_7	rec.: data storage & payload data transmitter
13	V_8	rec.: secondary payload(s)
14	GND	Ground

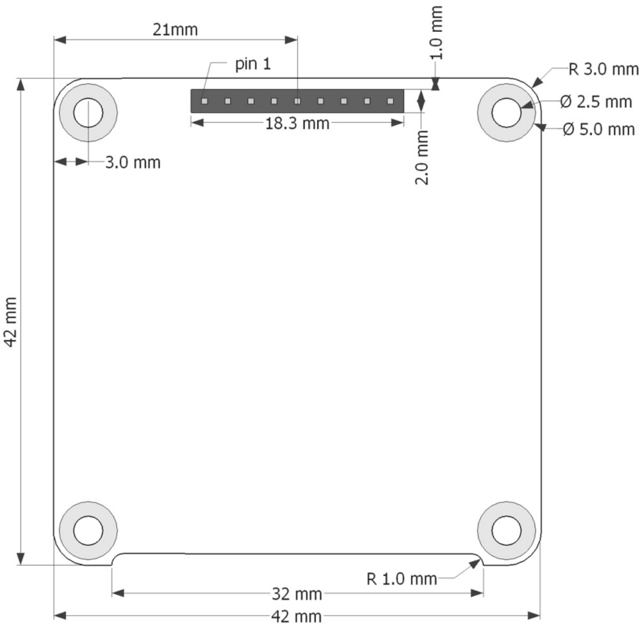


Fig. 18. PQ9 printed circuit board outline.

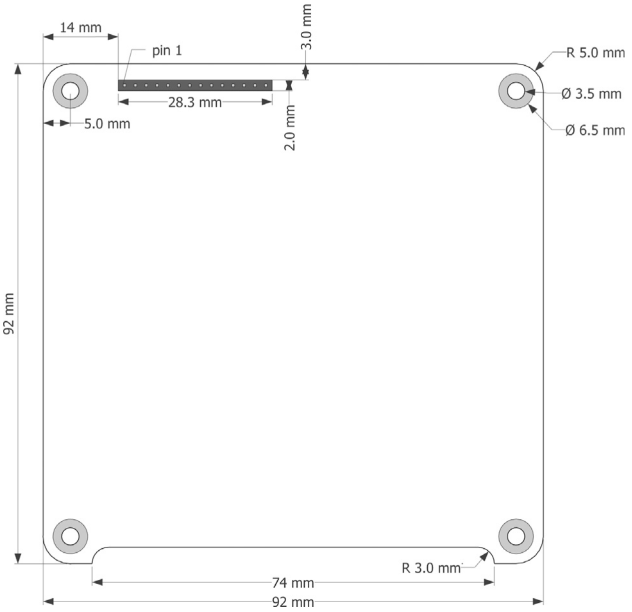


Fig. 19. CS14 printed circuit board outline.

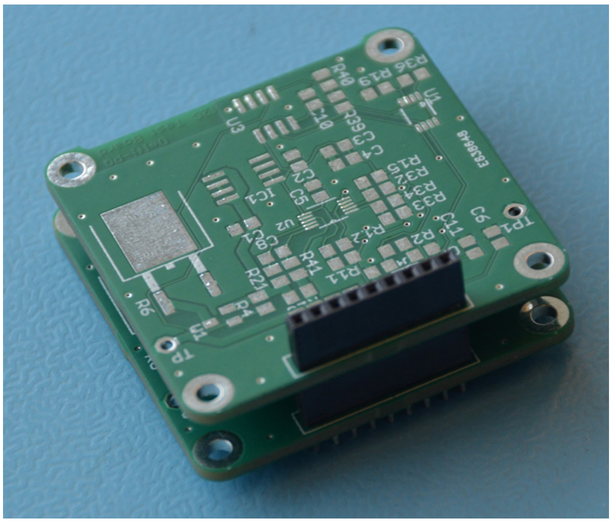


Fig. 20. PQ9 PocketQube boards with stackable pin connector.

the limited amount of power distribution lines make a true single-point-of-failure free design impossible. A follow-up study is recommend to investigate the impact on the overall reliability for these small satellites under these assumptions.

A topic not addressed in this paper is the development of (mega) constellations of very small satellites. Present day examples are the Flock CubeSats from Planet (Boshuizen et al., 2014) and the Lemur CubeSats from Spire (Hand, 2017). In relation to an electro-mechanical interface standard, it is expected that technical criteria are more important than community support. The rationale behind this expectation is that the main players have sufficient finances to develop many iterations of the spacecraft before the final mission and have the financial means to optimize the satellite and when necessary customize subsystems and even the interfaces to enhance the performance of the satellite. Next to this, the financial aspect of series production in relation to the electro-mechanical interface becomes important. The proposed PQ9 and CS14 interface standards can be implemented with just a few very cheap components (few Euros/Dollars) and assembly will take only a few minutes by an solder expert or can even be fully robotized.

Next steps are to define the data protocol for RS-485, the electrical characteristics of the reset line and to perform extensive testing with engineering models of PocketQube systems using the PQ9 interface. The final goal is to publicly release documentation on the new interface standards PQ9 and CS14.

Acknowledgements

The authors would like to thank all participants in the AHP survey, all Delfi-PQ team members for their critical review and inputs of the trade-off process and Laurens Buijs for his contribution in testing the data busses. Part of this research is supported by the National Sustainability Program of the Czech Republic under grant LO401.

References

Amini, R., Gaydadjiev, G., Gill, E., 2009. Smart power management for an onboard wireless sensors and actuators network. In: AIAA Space 2009 Conference and Exposition.

Arruego, I., Rivas, J., Martinez, J., Martin-Ortega, A., Apestigue, V., De Mingo, J.R., Jimenez, J.J., Alvarez, F.J., Gonzalez-Guerrero, M., Dominguez, J.A., 2016. Practical application of the Optical Wireless communication technology (OWLS) in extreme environments. In: IEEE International Conference on Wireless for Space and Extreme Environments, WiSEE 2015. https://doi.org/10.1109/WiSEE.2015.7392981.

Becnel, E., McAndrew, S., Strass, L., Walkinshaw, T., Worrall, K., 2015. PQ 60 Standard Document (v1.1).

Boshuizen, C.R., Mason, J., Klupar, P., Spanhake, S., 2014. Results from the planet labs flock constellation. In: 28th Annual AIAA/USU Conference on Small Satellites. AIAA, Logan, p. SSC14-I-1.

Bouwmeester, J., Amini, R., Hamann, R.J., 2007. Command and data handling subsystem for a satellite without energy storage: Delfi-C3. 58th International Astronautical Congress 2007. IAF.

Bouwmeester, J., Guo, J., 2010. Survey of worldwide pico- and nanosatellite missions, distributions and subsystem technology. Acta Astronaut. 67, 854–862.

Bouwmeester, J., Langer, M., Gill, E., 2017. Survey on the implementation and reliability of CubeSat electrical bus interfaces. CEAS Sp. J. 9. https://doi.org/10.1007/s12567-016-0138-0.

Bouwmeester, J., Santos, N., 2014. Analysis of the distribution of the electrical power in CubeSats. The 4S Symposium. ESA, Valetta.

Busch, S., 2015. CubeSat Subsystem Interface Definition (v0.3). Wuerzbrug.

Cornejo, N.E., Bouwmeester, J., Gaydadjiev, G.N., 2009. Implementation of a reliable data bus for the delfi nanosatellite programme. 7th IAA Symposium on Small Satellites for Earth Observation. IAA, Berlin.

de Boom, C.. W., van der Heiden, N., Sandhu, J., Hakkesteegt, H.C., Leijtens, J.L., Nicollet, L., Bouwmeester, J., van Craen, G., Santandrea, S., Hannoteau, F., 2011. In-orbit experience of TNO sun sensors. In: 8th International Conference on Guidance, Navigation and Control. ESA, Karlovy Vary.

Goepel, K.D., 2013. Implementing the analytic hierarchy process as a standard method for multi-criteria decision making in corporate enterprises – A new AHP excel template with multiple inputs. In: Proceedings of the International Symposium on the Analytic Hierarchy Process. Creative Decisions Foundation, Kuala Lumpur, pp. 1–10.

Hand, E., 2017. CubeSat networks hasten shift to commercial weather data. Science (80-.). 357, 118–119. https://doi.org/10.1126/science.357.6347.118.

Lawrenz, W., 2013. CAN System Engineering. Springer-Verlag, London. https://doi.org/10.1007/978-1-4471-5613-0.

Leens, F., 2009. An introduction to I2C and SPI protocols. IEEE Instrum. Meas. Mag. 12, 8–13. https://doi.org/10.1109/MIM.2009.4762946.

NXP Semiconductors, 2016. PCA9615 (Datasheet).

Poghosyan, A., Golkar, A., 2017. CubeSat evolution: Analyzing CubeSat capabilities for conducting science missions. Prog. Aerosp. Sci. 88, 59–83. https://doi.org/10.1016/j.paerosci.2016.11.002.

Riot, V., Simms, L., Carter, D., Decker, T., Newman, J., Magallanes, L., Horning, J., Rigmaiden, D., Hubbell, M., Williamson, D., 2014. Government-owned CubeSat next generation bus reference architecture. AIAA/USU Conference on Small Satellites. AIAA, Logan.

Saaty, T.L., 2008. Decision making with the analytic hierarchy process. Int. J. Serv. Sci. 1, 83. https://doi.org/10.1504/IJSSCI.2008.017590.

Schoemaker, R., Bouwmeester, J., 2014. Evalution of bluetooth low energy wireless internal data communication for nanosatellites. The 4S Symposium. ESA, Valetta.

Selva, D., Krejci, D., 2012. A survey and assessment of the capabilities of Cubesats for Earth observation. Acta Astronaut. 74, 50–68. https://doi.org/10.1016/j.actaastro.2011.12.014.

Soltero, M., Zhang, J., Cockril, C., Industrial, H.P.A, Zhang, K., Kinnaird, C., Kugelstadt, T., 2010. RS-422 and RS-485 Standards Overview and System Configurations, Configurations.

Kassem *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:188
https://doi.org/10.1186/s13638-019-1505-2

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Wideband UHF and SHF long-range channel characterization

Edward Kassem[1], Jiri Blumenstein[1]*, Ales Povalac[1], Josef Vychodil[1], Martin Pospisil[1], Roman Marsalek[1] and Jiri Hruska[2]

Abstract
This paper presents an outdoor long-range (from 315 m up to 5.3 km) fixed channel campaign for both ultra high frequency and super high frequency bands with co-polarized horizontal and vertical antenna configurations. It investigates the channel characteristics of device to device communication scenarios underlaying the 5th generation networks by providing detailed research. Both line of sight and non-line of sight measurements in 1.3 GHz and 5.8 GHz frequency bands with bandwidth up to 600 MHz were conducted. The path loss, root mean square delay spread, coherence bandwidth, and channel frequency response variation are characterized. We observed that the variation is negligible in microcell line of sight environment for both above mentioned frequencies, whereas it significantly increases with frequency in different macrocell non-line of sight environments. The distance dependency of path loss was also derived. It was observed that the root mean square delay spread decreases with frequency for both line of sight microcell and non-line of sight macrocell measurements. A dependency between the root mean square delay spread and transmitter-receiver distance in non-line of sight environments was also captured. The relation between the coherence bandwidth and the root mean square delay spread was depicted. It demonstrates an exponential function in all considered channel combinations.

Keywords: Channel model, Device to device, Line of sight, Non-line of sight, Super high frequency, Ultra high frequency

1 Introduction

Device to device communication [1, 2] is an important technology which enables data flow not only between humans but also between machines without human intervention. It can be used underlying the available cellular networks. The 5th generation system technology, 3rd Generation Partnership Project Release 15, will have to support high performance in spectral efficiency and throughput measurements. The 5th generation network is one of the most suitable environments for device to device communication since it is an IP-based network that enables to control any connected devices using internet protocols. Moreover, it is able to send large amounts of data with a high rate and low latency and support a large amount of connected devices. It is a good solution to reduce the eNB traffic load and the end to end delay. In order to develop a reliable wireless device to device communication network [3, 4], an accurate description of the wireless channel impulse response measurements should be presented. The channel impulse response describes spreading, echoing, multipath propagation, and Doppler effects that occur when an impulse is sent between the transmitter and the receiver. Knowledge of the channel impulse response characteristics enables system designers to ensure that inter symbol interference does not dominate and hence lead to an excessive irreducible bit error ratio [5].

1.1 Literature review

As mentioned above, propagation measurements are necessary for creating statistical channel models that support the development of new standards and technologies for wireless communications systems. Channel models that predict signal strength and multipath time delays are required for a proper system design. There have been a number of studies for channel sounding using different input signals over the past 10 years.

*Correspondence: blumenstein@feec.vutbr.cz
[1] Department of Radio electronics, Brno University of Technology, Technicka 12, Brno, Czech Republic
Full list of author information is available at the end of the article

As a sample of typical work, there is a paper which studied the frequency dependence of the channel characteristics at the 2–4 GHz frequency band [6]. Line of sight and obstructed line of sight scenarios were considered. Angle of arrival and delay of arrival of the main paths were investigated. A rich multipath environment was observed, with intensive path components existence in both angle and delay domains.

Outdoor measurements were conducted in an open-area test site at the National Metrology Institute of Germany [7], to study the scattering effects of a traffic sign on vehicles moving along the road. The outputs are analytical modeling, simulation, measurement, and implementation of the bi-static radar cross section of the traffic signs.

A paper on outdoor sounding [8] highlighted the propagation path loss models for 5th generation urban micro and macro cellular scenarios. It compares the alpha-beta-gamma and the close-in free space reference distance models. A wide range of frequencies 2–73.5 GHz over 5–1429 m distances were used. The output showed very comparable modeling performance between close-in and alpha-beta-gamma models. The close-in model offers simplicity and a conservative non-line of sight path loss estimate at large distances, whereas the alpha-beta-gamma model is more complex and offers a fraction of a decibel smaller shadow, less loss near the transmitter, and more loss far from transmitter.

Another paper [9] described the achieved results for line of sight and non-line of sight measurements between the User Equipment and the base station in Nanjing Road, Shanghai. The received signals were 20 MHz bandwidth with 2.1376 GHz carrier frequency. The delays and the complex attenuations of multipath components have been estimated by applying the space-alternating generalized expectation-maximization algorithm. The distance between transmitter and receiver in line of sight/non-line of sight scenarios, the life-distance of the line of sight channel, the power variation at line of sight to non-line of sight transition, and the transition duration were extracted.

The authors in [10] presented a sounding system that uses an orthogonal frequency division multiplexing signal at 5.6 GHz with 200 MHz bandwidth. The power delay profiles and the excess delay were presented.

An open-pit mine campaign performed a 25-MHz wide frequency band sounding immediately below the unlicensed 2.4-GHz ISM band [11]. A continuously repeating maximum-length or m-sequence with $K = 2047$ sequence length was adopted as a transmitted signal. It was transmitted at a rate of 25 MS/s. Four measurement realizations of the impulse response with different transmitter-receiver separations that vary between 425–1670 m were recorded. The calculated delay spread of the channel was often more than 10 μs.

A channel measurement campaign was conducted to study the frequency dependence of the propagation channel for a wide range of frequencies 3–18 GHz [12]. Urban macro and micro cellular environments were covered. The root mean square delay spreads, coherence bandwidth, path loss, shadow fading, and Ricean factor were characterized. It is mentioned that the path loss exponents vary significantly with frequency (from 1.8 to 2 dB in a line of sight environment and from 2.71 to 4.34 dB in non-line of sight). Shadow fading and the Ricean factor increase with frequency, whereas the root mean square delay spread values decrease with frequency in a line of sight environment. However, the root mean square delay spread in a non-line of sight environment and the coherence bandwidth values in both line of sight and non-line of sight environments do not show significant changes.

An outdoor wideband channel sounding at 2.4 GHz is described in [13]. The distance between the transmitter and the receiver varied from 50 to 150 m. The distance-power gradient is 2.532, path loss (with 9 dB standard deviation), small-scale or multipath fading (with 5 dB standard deviation) are reported. The maximum observed multipath fade is 28 dB.

Another campaign was conducted in Seoul [14]. The measurements were done using a wideband channel sounder at 3.7 GHz with a 100 MHz bandwidth. Both line of sight and non-line of sight environments are investigated. The output was presented as a spatial correlation coefficient of low-height links in an urban environment.

A wideband propagation channel at 2.45 and 5.2 GHz was presented in [15]. Channel characteristics as power delay profile, the mean delay, and the delay spread were studied. It was mentioned that the parameters are frequency-independent, whereas the higher frequency signal shows considerably larger path loss than the lower one. Both the correlator-based and recursive Bayesian filter-based ranging estimators were evaluated; both of them provide better performances at 2.45 GHz compared with 5.2 GHz. The performance difference increases with decreasing the received power.

Urban macro environment was investigated in [16]. Wideband multiple-input multiple-output measurements around 800 MHz with 50 MHz bandwidth were presented. The antennas with 360° of azimuth and 90° of elevation were used for the transmitter and the receiver. The output report contains path loss (path loss exponent $n = 3$), shadow fading (with 8.4 dB standard deviation), delay spread (with 123 ns mean value and 73.2 ns standard deviation), angular spread (with 30.8° mean value and 12.5° standard deviation for angular spread of departure and 66.9° mean value and 15.1° standard deviation for angular spread of arrival), and Ricean K-factor (with 5 dB mean value and 6.7 dB standard deviation).

Measurement campaign [17] at the center frequency of 2.35 GHz with 50 MHz bandwidth was conducted in order to evaluate the performance in an outdoor propagation environment. Signal to noise ratio, spatial diversity, and capacity of different transmission schemes (direct transmission, amplify and forward, and decode and forward relaying) were investigated. Both line of sight and non-line of sight scenarios were involved. The results were depicted in terms of signal to noise ratio, spatial diversity, and capacity. Both amplify and forward, and decode and forward schemes improve the Signal to Noise Ratio, whereas direct transmission improves the capacity in small distances of a line of sight environment. However, by increasing transmitter-receiver distance, the capacity provided by the decode and forward exceeds that provided by the direct transmission. The spatial diversity was also significantly improved by applying the decode and forward scheme. Most of the abovementioned papers depict indoor channels or even outdoor channels but only up to 2 km and with only vertical co-polarization. Therefore, we filled these gaps by considering both line of sight and macro non-line of sight scenarios over 1.3 GHz and 5.8 GHz frequencies with longer distances 2.089 km, 4.11 km, and 5.429 km and both vertical and horizontal co-polarization dependence of multipath propagation channel measurements.

1.2 Contribution of the paper

We analyzed the channel frequency response variation, the path loss, the root mean square delay spread, and the coherence bandwidth with all above mentioned scenarios. Our achieved results expand the achieved results in [18] which were performed in an indoor environment. The main contributions of this paper are described in the following few points:

- Test the ability of deploying a device to device communication underlay 5th generation network in a wideband long-range channel for both ultra high frequency and super high frequency bands as a part of 5th generation new radio frequency bands allocation [19]
- For a microcell line of sight environment (with 315 m distance), we provided the channel frequency response variation, the path loss, and the root mean square delay spread distribution in the case of vertical and horizontal polarizations for both 1.3 GHz and 5.8 GHz center frequencies.
- For macrocell non-line of sight environments (with 2.089, 4.11, and 5.429 km distances), in additional of all previous mentioned parameters, distance dependence of the path loss and the root mean square delay spread are analyzed. The root mean square delay spread dependence of the coherence bandwidth is also investigated.

This paper is organized as follows. The "Materials and methods" section describes the channel measurement campaign of outdoor long-range environments and the sounder systems for ultra high frequency and super high frequency bands. The data processing procedure and channel characteristics calculation are also depicted. In the "Results and discussion" section, the channel measurement results are captured for line of sight and non-line of sight outdoor environments with different polarization combinations. Based on channel measurement results, the root mean square delay spread, the path loss, the channel frequency response variation, and the coherence bandwidth are analyzed. The last section concludes the paper.

2 Materials and methods

2.1 Measurement environments and setup

Our measurements were conducted in the South Moravian region, Czech Republic. Two types of setups: microcell and macrocell were considered.

In the microcell setup, the TX1 was placed on a small hill near the Faculty of Electrical Engineering and Communication building, Brno University of Technology (BUT) and mounted on a mast of 10 m height, whereas the receiver was allocated on the rooftop of the building (19-m height). The distance between the transmitter and the receiver for route R1 is 315 m. Both the transmitter and the receiver are surrounded by a rich scattering environment which consists of buildings, parked cars, moving cars, and people. However, because of the highly mounted antennas above the ground, line of sight measurements were realized.

In the macrocell setup, three different non-line of sight routes (R2, R3, R4) were tested. On the first two routes (R2, R3), the receiver was placed on the rooftop of the Faculty of Electrical Engineering and Communication building. The transmitter was allocated 2.089 km from the receiver (8-m height) for the R2 route, and 5.429 km from the receiver (3 m height) in the case of the R3 route. For the fourth route, R4, both the transmitter and the receiver were allocated in a rural area where the transmitter was surrounded with different building heights (up to 12-m height) and placed on the rooftop of the Racom company building (12-m height) mounted on a mast of 5-m height. The receiver was mounted on a mast of 19-m height in a pure rural area. Examples of transmitting antennas in the case of R2 and R3 and receiving antenna with their surrounding environments are presented on the left-hand side, the right-hand side, and the center of Fig. 1, respectively. The mast of the received antenna of the fourth route, R4, is captured on the right-hand side of Fig. 2.

In order to investigate line of sight and non-line of sight radio channel characteristics, two different channel sounder systems for 1.3 GHz and 5.8 GHz were

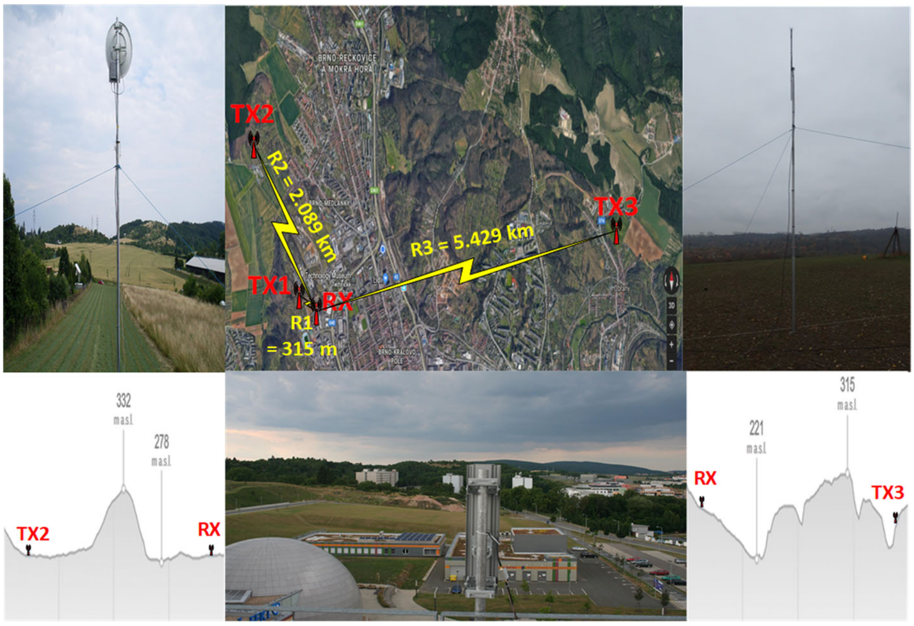


Fig. 1 Measurement locations for R1, R2, and R3 routes. Line of sight route R1 = 315 m and non-line of sight route R2 = 2.089 km with super high frequency band TX2 position on the left-hand side, R3= 5.429 km with ultra high frequency band TX3 position on the right-hand side and the position of the sector receiver antenna used for the super high frequency signal of TX2-RX measurements. Map source: Google.com, Mapy.cz

implemented. These sounders together with MATLAB and LabVIEW programs were used for channel evaluation up to 120 MHz and 600 MHz bandwidths for both 1.3 and 5.8 GHz, respectively.

The basis of the transmitting station is a programmable radio frequency generator (R&S SMU200A vector signal generator). The generated signal was filtered using a band pass filter, amplified by a power amplifier, and directed to the directional antenna transmitter using a circular connector. The amplifier module for the ultra high frequency band (MD220L-1296-48V) was modified to be used as a linear amplifier class A. However, the super high frequency band transmitter uses Hittite HMC408LP3 and DG0VE PA6-1-8W amplifying modules. The generated

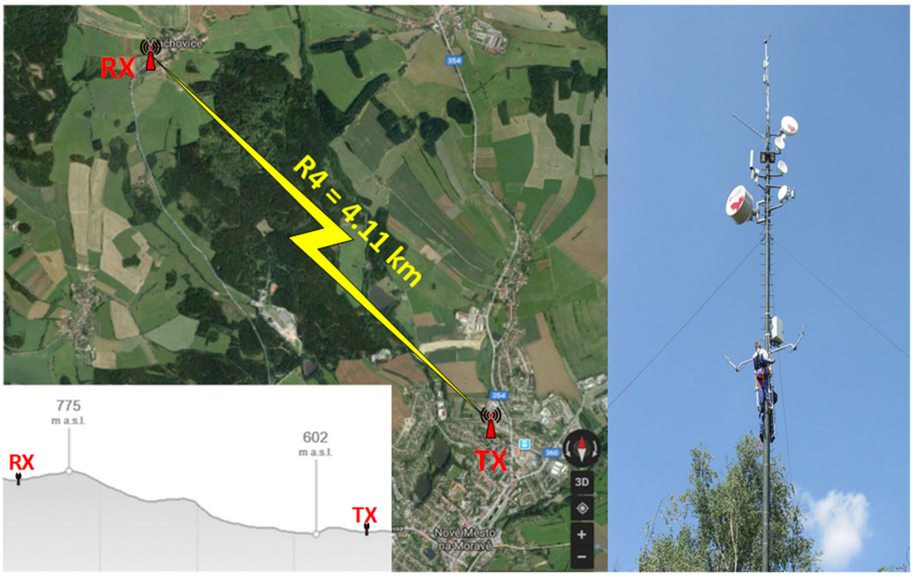


Fig. 2 Measurement location for R4 route. Non-line of sight R4 = 4.11 km route and the position of the receiver antenna on the middle of the mast. Map source: Google.com, Mapy.cz

ultra high frequency (1.3 GHz) signal was transmitted using 35-element Yagi Tonna antenna 20365 with 20 dBi of gain. The super high frequency (5.8 GHz) signal was transmitted by a parabolic RD-5G30-LW RocketDish with a gain equaling 30 dBi.

The receiver consists of a directional antenna, low-noise amplifier, and signal analyzer (National Instruments PXIe-5665) with three basic modules: PXIe-5653 RF synthesizer, PXIe-5605 downconverter, and PXIe-5622 150 MS/s 16-bit digitizer. The ultra high frequency and super high frequency signals were received by 35-element Yagi Tonna antenna 20365 (20 dBi gain) and sector antenna AM-V5G-Ti (21 dBi gain), respectively.

The developed software in LabVIEW environment for National Instruments PXIe-5665 was used for recording and processing the raw data received by the channel sounder. This software is able to record up to 600 MHz of bandwidth via stepped re-tuning by 50 MHz blocks with the ability to be synchronized with the transmitted signal. In order to save the achieved data with 50 MHz instance bandwidth and 16-bits precision, a redundant array of inexpensive disks with capacity of 12 TB and 16-bit dynamic range was used. MATLAB was also used for final data processing. Our in-house developed channel sounder operates with frequency modulated continuous wave, i.e., as a sounding sequence; we utilize frequency modulation chirps with a maximal measurement speed of 40 MHz/ms. Figure 3 depicts the schematics of the sounder for ultra high frequency (white blocks) and super high frequency (gray blocks) bands, whereas the characteristics (E and H planes) of both parabolic and sector antennas for vertical and horizontal co-polarizations are captured in Fig. 4.

2.2 Data processing

2.2.1 *Channel response*

The radio channel is commonly characterized by scattering, attenuation, reflection, refraction, and fading [20]. In both the wired and wireless communications, the Additive White Gaussian Noise channel is assumed as a basic channel model. More advanced models including fading effects, e.g. the International Telecommunication Union path loss models like Flat Rayleigh, Pedestrian (Ped), and Vehicular (Veh) [21]. The Flat Rayleigh fading channel has a constant attenuation factor during the subframe time and the whole allocated bandwidth. Other two models define two different test environments: outdoor to indoor pedestrian and vehicular well-established channel models used for research purposes in mobile communication systems. The impulse response h of the multipath channel can be calculated according to Eq. (1), where β_w, τ_w, and φ_w represent the amplitude, arrival time, and phase that characterize the N_p number of individual paths between the transmitter and the receiver [21].

$$h(t,\tau) = \sum_{w=1}^{N_\mathrm{p}} \beta_w(t) \cdot \delta\left(t - \tau_w(t)\right) e^{-j\varphi_w(t)} \qquad (1)$$

The frequency response can be measured directly by collecting the measurements of the s_{21} scattering parameter of a radio channel in the frequency domain. It can also be calculated by applying the Fourier transformation on the time domain measurements expressed in Eq. (1). The result could be given by Eq. (2) [22].

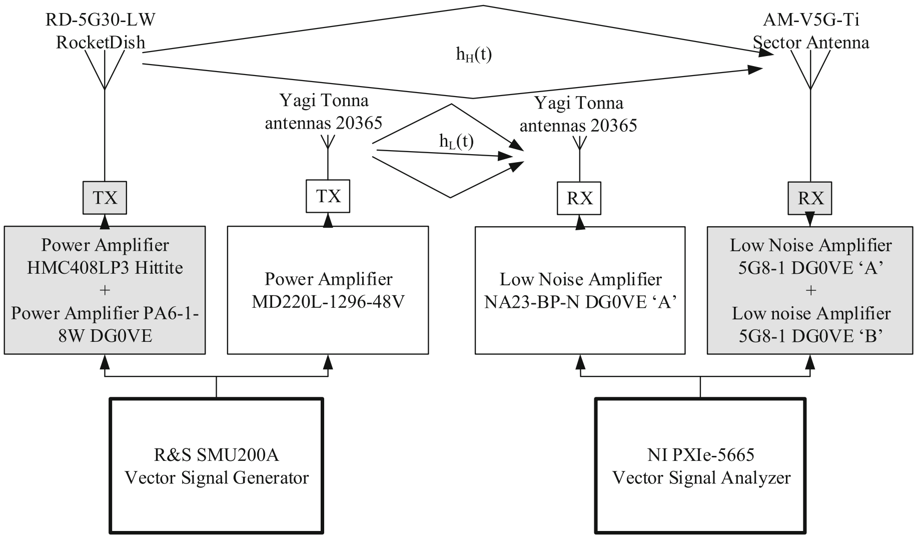


Fig. 3 Channel sounder setup. Channel sounding systems diagram with transmitter and receiver for both ultra high frequency (white colored) and super high frequency (gray colored) bands

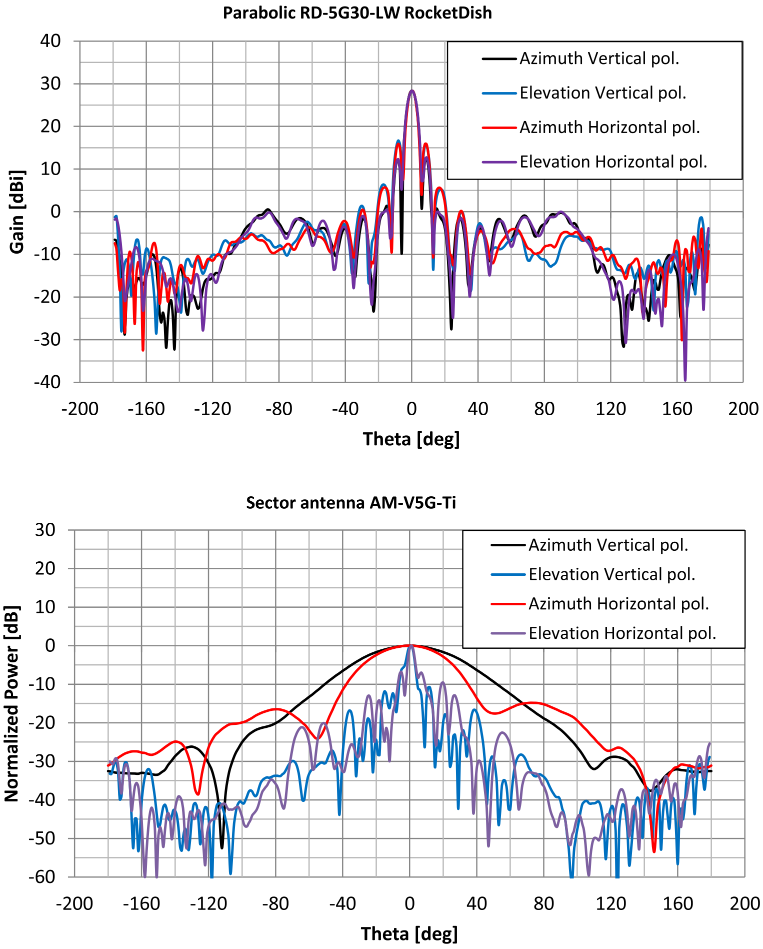


Fig. 4 Parabolic and sector antennas rectangular radiation. Both E and H planes in the case of vertical and horizontal co-polarizations are captured

$$H(f,t) = \int_{-\infty}^{\infty} h(t,\tau)\cdot e^{-j\omega\tau}\,d\tau = \sum_{w=1}^{N_\text{p}} \beta_w(t)e^{-j\varphi_w(t)}e^{-j\omega\tau_w(t)} \tag{2}$$

In a slowly time-varying channel, the multipath parameters of the channel remain constant during fractions of the coherence time of the channel; so the frequency response can be presented in Eq. (3).

$$H(f) = H(f,0) = \sum_{w=1}^{N_\text{p}} \beta_w e^{-j\varphi_w}e^{-j\omega\tau_w} \tag{3}$$

In practice, however, the measurement systems are band-limited. Therefore, the frequency response is defined in Eq. (4).

$$H(f) = H(f,0) = W(f)\cdot\sum_{w=1}^{N_p} \beta_w e^{-j\varphi_w}e^{-j\omega\tau_w} \tag{4}$$

where $W(f)$ represents the frequency domain RF filter characteristics in the frequency domain.

2.2.2 Path loss

The generalized form of the path loss model can be constructed from path loss offset PL_offset, the distance d between transmitter and receiver, the reference distance d_0, and the random shadowing effect χ_σ which is calculated as the deviation of the measured path loss from the linear model [12].

$$PL(d) = PL_\text{offset} + 10n\cdot\log\left(\frac{d}{d_0}\right) + \chi_\sigma \tag{5}$$

where n is a path loss exponent and $d_0 = 100$ m for long outdoor distances [20].

2.2.3 Root mean square delay spread

The root mean square delay spread is one of the most important parameters for the delay time extent of a multipath radio channel. It is caused by reflected and scattered propagation paths. It can describe different multipath fading channels and a guideline to design a wireless transmission system. If τ_w is the channel delay of wth path and $P(\tau_w)$ is its power, then the root mean square delay spread can be formulated in Eq. (6).

$$\sigma_\tau = \sqrt{\bar{\tau^2} - \tau_m^2} \tag{6}$$

where τ_m is the mean excess delay and it is given by Eq. (7).

$$\tau_m = \frac{\sum_{w=1}^{N_p} P(\tau_w)\tau_w}{\sum_{w=1}^{N_p} P(\tau_w)} \tag{7}$$

$$\bar{\tau^2} = \frac{\sum_{w=1}^{N_p} P(\tau_w)\tau_w^2}{\sum_{w=1}^{N_p} P(\tau_w)} \tag{8}$$

2.2.4 Coherence bandwidth

Coherence bandwidth is a statistical measure of range of frequencies over which the channel can be considered as a flat channel. In other words, coherence bandwidth is the range of frequencies over which two frequency components have a strong potential for amplitude correlation. In the case where the coherence bandwidth is defined as a bandwidth with correlation of 0.5 or above, it can be calculated using the frequency correlation function depicted in Eq. (10) [12].

$$S(\Delta f) \cong \int_{-\infty}^{\infty} H(f)H^*(f+\Delta f).df \tag{9}$$

$H(f)$ is the complex transfer function of the channel, Δf is frequency shift and * denotes the complex conjugate.

$$B_{c,0.5} \approx min\left(\Delta f : \frac{S(\Delta f)}{S(0)} < 0.5\right) \tag{10}$$

2.2.5 Channel frequency response variation

Let us consider that $H_s(f_k)$, $k = 1, 2, \cdots N_F$, $s = 1, 2, \cdots, N_T$ is the wideband channel frequency response at specific time for a specific frequency. Figure 5 depicts a sample ($N_T = 200$) of normalized channel frequency response in dB where $f_1 = 1.2702$ GHz, $f_2 = 1.31$ GHz, therefore $\Delta f = f_2 - f_1 = 39.758$ MHz, and $N_F = 1554$. The influence of variation and small-scale fading can be removed by averaging consecutive N_T channel frequency response characteristics [23] according to Eq. (11).

$$\overline{|H(f_k)|^2} = \frac{1}{N_T} \cdot 10 \cdot \log\left(\sum_{s=1}^{N_T} |H_s(f_k)|^2\right) \tag{11}$$

However, as is mentioned in [24], averaging keeps some small-scale fluctuations in the frequency domain; therefore, the median filter is applied. The median filter is a non-linear filter used to discard the noise from the signal. The main idea is to run through the whole signal and calculate the median of each window [25]. Note that in order to get a well-filtered signal, a proper window size of median filter (that keeps the deep fades effect) should be chosen. In our research, the window size will depend primarily on the deep fades where the signal strength can drop for more than 15 dB. Therefore, the window size of 10 is chosen as the average frequency distance of the deep

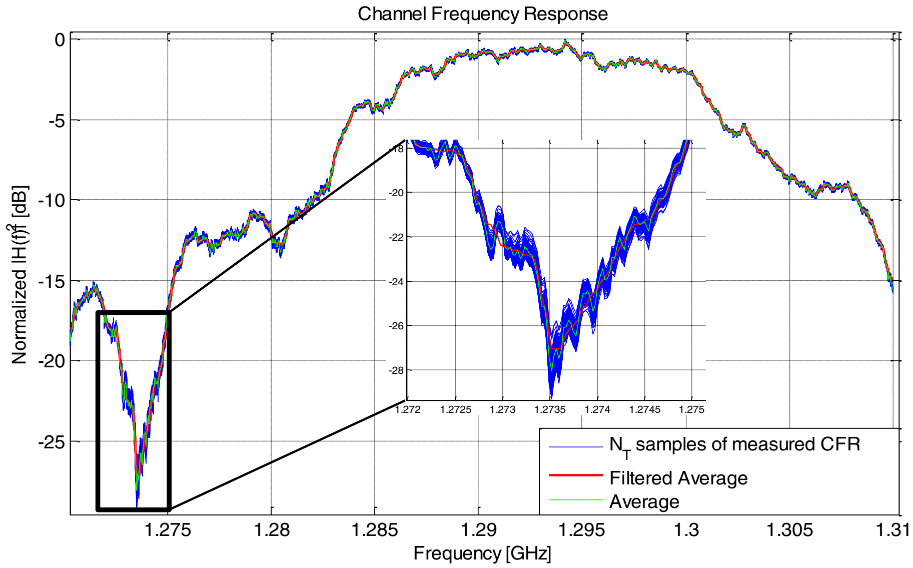


Fig. 5 Normalized $|H(f)|^2$ used to characterize the channel frequency response. The blue curve represents N_t measured channel frequency response during 8 s. The green curve represents the average value of the measured channel responses. The red curve depicts the smoothed version of channel frequency response after applying the median filter

fades. Finally, the channel frequency response variation is obtained through subtracting the filtered average channel frequency response from the measured channel frequency response.

$$\mathrm{CFRV} = \left|H_s(f_k)\right|^2 - \mathrm{filt}\left(\overline{\left|H(f_k)\right|^2}\right) \qquad (12)$$

3 Results and discussion

3.1 Path loss

Figure 6 presents the cumulative distribution function of the path loss for a line of sight environment. The cumulative probability of path loss values fit well with the normal distribution with μ mean and σ standard deviation parameters.

The path loss values of the R1 line of sight route are in the range of 87.6–88.5 dB with a mean value 88.1 dB and standard deviation 0.22 dB for 1.3 GHz with horizontal co-polarization, 88.2–89.9 dB with a mean value 89.04 dB and standard deviation 0.33 dB for 1.3 GHz with vertical co-polarization, 114.9–116.1 dB with a mean value 115.49 dB and standard deviation 0.23 dB for 5.8 GHz horizontal co-polarization, and 116.5–117.9 dB with a mean value 117.1 dB and standard deviation 0.24 dB for 5.8 GHz with vertical co-polarization.

The distribution shape is also depicted in Fig. 6 and presented in black, blue, magenta, and cyan colors for ultra high frequency horizontal co-polarization, ultra high frequency vertical co-polarization, super high frequency horizontal co-polarization, and super high frequency vertical co-polarization, respectively. The shape can provide useful information about the density of the calculated path loss. It can be observed that in the case of both 1.3 and 5.8 GHz, the path loss for vertical co-polarization exceeds the path loss of the horizontal one. This small difference (1–2 dB) is explained by the effect of suppression which can influence either the vertical or the horizontal polarization. That depends on the distance between transmitter and receiver, their heights, and the type of ground [26, 27]. It is also clear that the path loss increases with frequency as the higher frequencies tend to suffer greater signal absorption and scattering. The same characteristics are observed in [6, 8, 20] higher frequencies tend to suffer greater signal absorption.

Figure 7 presents the measured path loss for 1.3 GHz sounding system in the case of horizontal and vertical co-polarizations. Black circles represent the measured path loss values for horizontally transmitted and received signals, whereas blue circles represent the measured path loss values for vertically transmitted and received signals. The best line fit have been produced using a MATLAB function with path loss exponents equal to 3.9 and 3.7 for horizontal and vertical polarization cases, respectively. These results are comparable with the results specified in [8], where the path loss exponent value for distances up to 1.4 km varies between 2.9 and 3.1 for 2 GHz

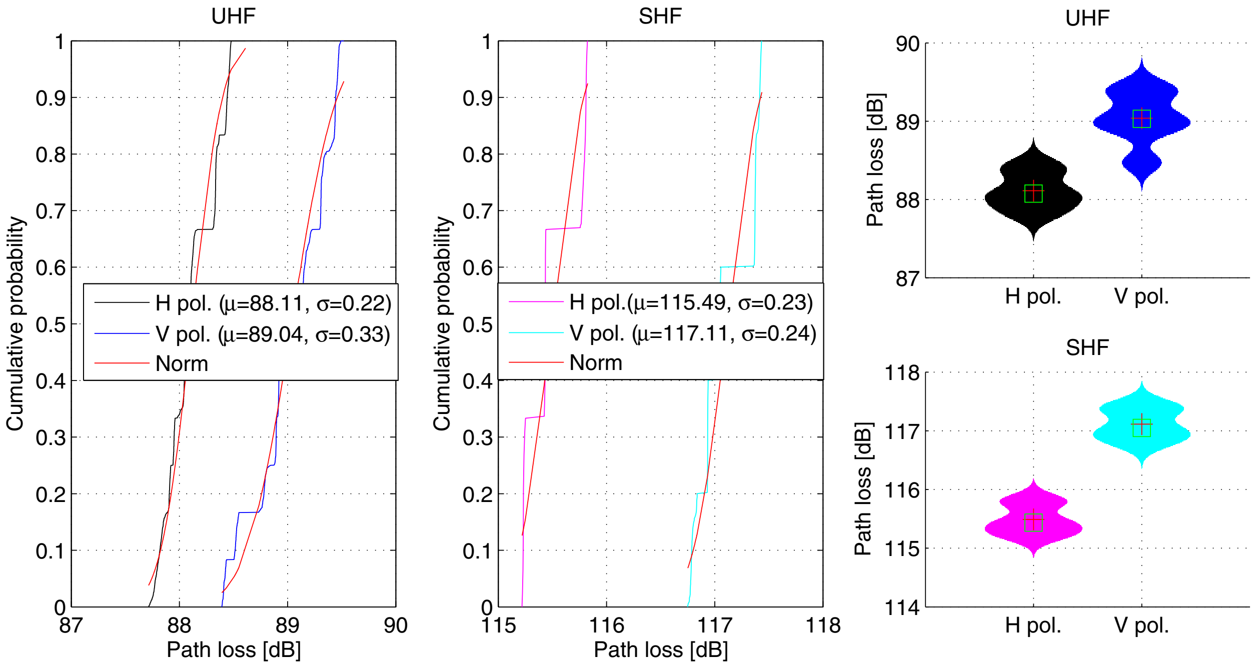


Fig. 6 Cumulative Distribution Function of the measured path loss in a line of sight environment. Both 1.3 and 5.8 GHz signals with horizontal and vertical co-polarizations antenna settings were transmitted. The curve colored in red represents the Normal distribution

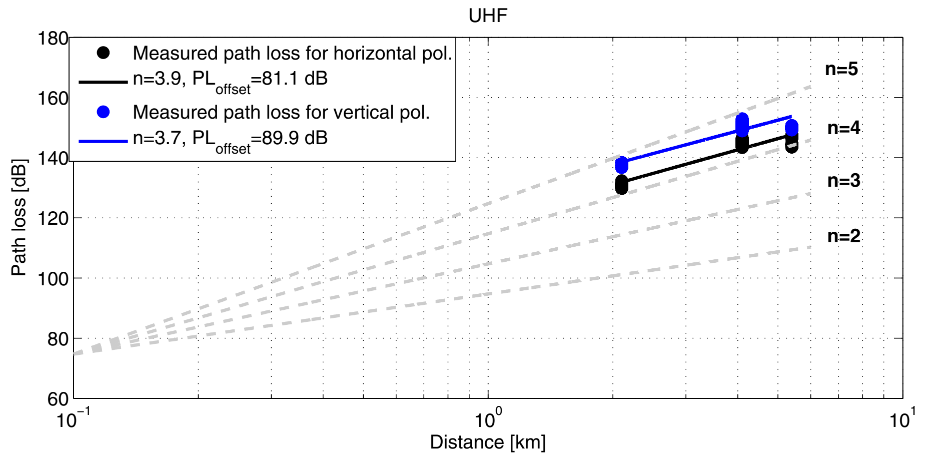


Fig. 7 The measured path loss for 1.3 GHz center frequency of the outdoor non-line of sight environment. The black and blue circles represent the measured non-line of sight path loss values for horizontal and vertical co-polarization, respectively

frequency. The path loss exponent value was also captured in an urban environment [16] for 800 MHz frequency and reached the value of $n = 3.3$.

Figure 8 depicts the measured path loss for a 5.8-GHz sounding system in the case of horizontal and vertical co-polarizations, represented by black and blue circles, respectively. The best line fit has been produced using a MATLAB function with path loss exponents n equal to 4.6 and 4.1 for horizontal and vertical polarization cases, respectively. These values can be compared with values achieved in [12], for frequencies 3–6 GHz where the path loss exponents between 3.92 and 4.7 were achieved. According to outdoor measurements presented in [28], the path loss exponent value changes from n equal to 2 to n equal to 4 at the breakpoints distance near 2.85 km. The dashed gray lines represent the theoretical path loss model in the case of different exponents. Note that the path loss exponent represents the slope of the path loss line, whereas $PL_{\text{offset}} = PL_F + PL_{\text{NLOS}}$ where PL_F and PL_{NLOS} are free space path loss and the path loss offset due to non-line of sight environment effects. More information about the path loss values for different line of sight and non-line of sight scenarios are listed in Table 1.

3.2 Root mean square delay spread

Figures 9 and 10 display the cumulative probability of the root mean square delay spread for the line of sight environment presented as R1 route and 2.089, 5.429, and 4.11 km non-line of sight environments presented as R2, R3, and R4 routes, respectively. The root mean square

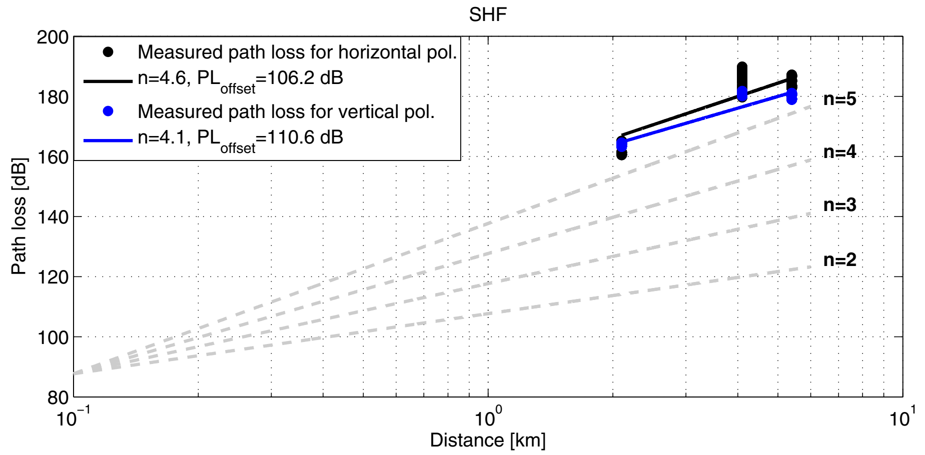


Fig. 8 The measured path loss for 5.8 GHz center frequency of the outdoor non-line of sight environment. The black and blue circles represent the measured non-line of sight path loss values for horizontal and vertical co-polarizations, respectively

Table 1 The path loss mean, standard deviation, minimum, and maximum values for different frequencies and co-polarizations in both line of sight and non-line of sight environments

Path loss

Route	Env.	Freq.	Pol.	μ [dB]	σ [dB]	Min [dB]	Max [dB]
R1	LOS	1.3 GHz	H-H	88.1	0.22	87.6	88.5
			V-V	89.04	0.33	88.2	89.9
		5.8 GHz	H-H	115.49	0.23	114.9	116.1
			V-V	117.1	0.24	116.5	117.9
R2	NLOS	1.3 GHz	H-H	130.84	0.37	129.77	132.31
			V-V	137.54	0.62	136.74	138.39
		5.8 GHz	H-H	162.34	1.92	160.5	165.13
			V-V	163.93	0.421	163.24	164.51
R3		1.3 GHz	H-H	144.6	0.72	143.37	146.54
			V-V	150.48	0.64	148.89	152.92
		5.8 GHz	H-H	184.48	2.88	179.68	189.86
			V-V	180.95	0.38	180.08	181.76
R4		1.3 GHz	H-H	145.61	1.46	143.55	147.54
			V-V	149.9	0.44	149.23	150.67
		5.8 GHz	H-H	183.34	1.33	180.41	187.17
			V-V	180.55	0.56	178.89	181.08

delay spread values for all routes and frequencies fit well with the normal distribution with μ mean and σ standard deviation parameters.

It can be distinguished that the R1 line of sight route offers smaller root mean square delay spread compared with all plotted root mean square values for non-line of sight environments in both 1.3 and 5.8 GHz. This behavior is expected. On the one hand, it can be due to a very strong line of sight component compared with the reflected or scattered path, leading to lower root mean square delay spread. On the other hand, in the case of a non-line of sight environment, the transmitted signal is blocked or severely attenuated causing multipath to arrive at the receiver over a large propagation time interval. Similar characteristics are observed in [12, 29].

The wideband root mean square delay spread for the R1 route is in the range of 15.11–18.42 ns for 1.3 GHz with horizontal co-polarization, 23.18–32.58 ns for 1.3 GHz with vertical co-polarization, 11.53–12.21 ns for 5.8 GHz horizontal co-polarization, and 15.82–16.62 ns for 5.8 GHz with vertical co-polarization.

It can be seen from Fig. 9 that in the case of the first route R1 line of sight, the higher frequency provides smaller mean root mean square delay spread in both horizontal and vertical polarization settings. This behavior was also mentioned in [12, 30]. It is also clear that in the case of both ultra high frequency and super high frequency frequencies, the vertical co-polarization shows higher mean root mean square delay than horizontal co-polarization.

For the R2 route, the root mean square delay spread is in the range of 52.99–99.70 ns for 1.3 GHz with horizontal co-polarization, 77.44–104.82 ns for 1.3 GHz with vertical co-polarization, 46.43–60.67 ns for 5.8 GHz horizontal co-polarization, and 72.15–87.63 ns for 5.8 GHz with vertical co-polarization.

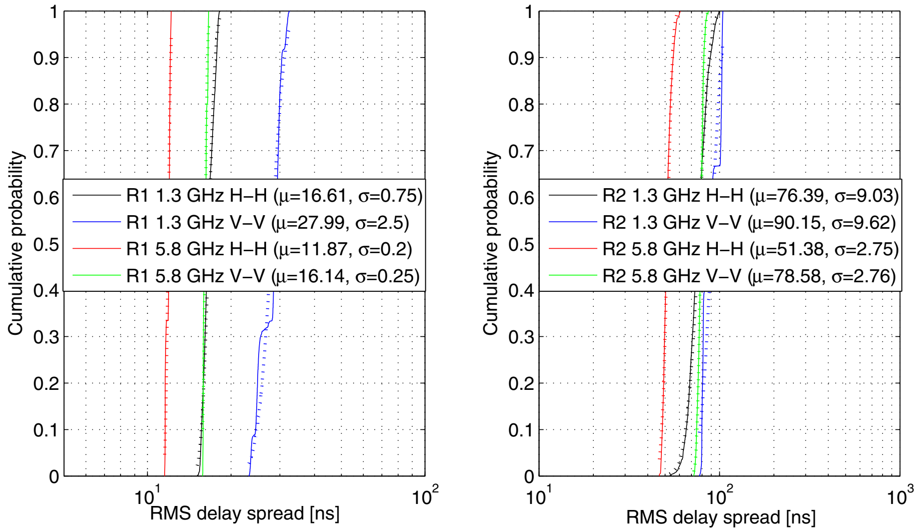


Fig. 9 R1 and R2 root mean square delay spread. Cumulative Distribution Function of the root mean square delay spread in [ns] for different frequencies and both horizontal and vertical co-polarizations of the first and second measurement routes (R1 and R2) in line of sight and non-line of sight scenarios, respectively. The colored dotted lines represent the Normal distribution of the corresponding frequency and polarization combinations

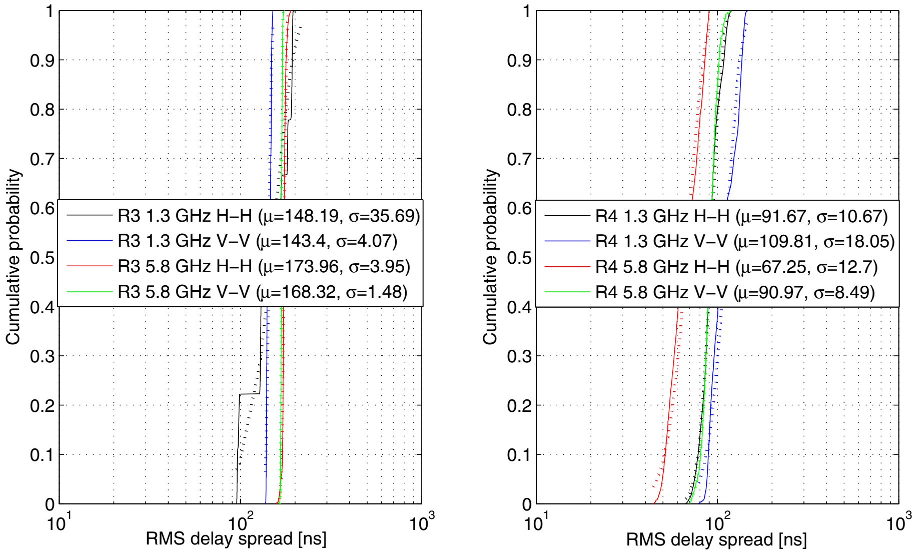


Fig. 10 R3 and R4 root mean square delay spread. Cumulative distribution function of root mean square delay spread in [ns] for different frequencies and both horizontal and vertical co-polarizations captured for the third and fourth measurement routes (R3 and R4). The colored dotted lines represent the normal distribution of the corresponding frequency and polarization combinations

In the case of the R3 route, the root mean square delay spread is in the range of 95.21–215.39 ns for 1.3 GHz with horizontal co-polarization, 137.24–151.27 ns for 1.3 GHz with vertical co-polarization, 157.7–189.54 ns for 5.8 GHz horizontal co-polarization, and 163.33–176.58 ns for 5.8 GHz with vertical co-polarization. For the R4 route, it is in the range of 66.85–119.73 ns for 1.3 GHz with horizontal co-polarization, 78.73–147.76 ns for 1.3 GHz with vertical co-polarization, 44.12–89.91 ns for 5.8 GHz horizontal co-polarization, and 70.44–119.11 ns for 5.8 GHz with vertical co-polarization. It can be observed that the horizontal co-polarization shows smaller mean root mean square delay spread than the vertical co-polarization for 1.3 and 5.8 GHz. However, the third route, R3, shows different characteristics. This can be due to the building's metal roof between the transmitter and the receiver, that cause depolarization. Table 2 combines all needed information about the root mean square delay spread values.

The effect of transmitter-receiver distance on the mean values of root mean square delay spread is also investigated. The mean root mean square delay spread values increase with the increasing distance between the transmitter and the receiver. A similar trend is observed in [31]. The relation between the mean root mean square delay spread and the distance can be fitted with linear mode $\sigma_{\tau\mathrm{UHF},H} = 20d+27$ for ultra high frequency with horizontal co-polarization, $\sigma_{\tau\mathrm{UHF},V} = 15d + 55$ for ultra high frequency with vertical co-polarization, $\sigma_{\tau\mathrm{SHF},H} = 34d - 33$ for super high frequency with horizontal co-polarization, and $\sigma_{\tau\mathrm{SHF},V} = 25d + 15$ for super high frequency with vertical co-polarization, where d is the distance between the transmitter and the receiver in kilometers. This characteristic is comparable with results published in [32, 33].

From these functions, it can be noticed that the line slope of the root mean square delay spread of super high

Table 2 The mean, standard deviation, minimum, and maximum values of root mean square delay spread for different frequencies and co-polarizations in both line of sight and non-line of sight environments

RMS delay							
Route	**Env.**	**Freq.**	**Pol.**	**μ [ns]**	**σ [ns]**	**Min [ns]**	**Max [ns]**
R1	LOS	1.3 GHz	H-H	16.61	0.75	15.11	18.42
			V-V	27.99	2.50	23.18	32.58
		5.8 GHz	H-H	11.87	0.20	11.53	12.21
			V-V	16.14	0.25	15.82	16.62
R2		1.3 GHz	H-H	76.39	9.03	52.99	99.70
			V-V	90.15	9.62	77.44	104.82
		5.8 GHz	H-H	51.38	2.75	46.43	60.67
			V-V	78.58	2.76	72.15	87.63
R3	NLOS	1.3 GHz	H-H	148.19	35.69	95.21	215.39
			V-V	143.40	4.07	137.24	151.27
		5.8 GHz	H-H	173.96	3.95	157.70	189.54
			V-V	168.32	1.48	163.33	176.58
R4		1.3 GHz	H-H	91.67	10.67	66.85	119.73
			V-V	109.81	18.05	78.73	147.76
		5.8 GHz	H-H	67.25	12.70	44.12	89.91
			V-V	90.97	8.49	70.44	119.11

frequency frequencies greater than the line slope of root mean square delay spread of ultra high frequency frequencies. Therefore, the mean root mean square delay spread for super high frequency frequencies more extremely increases compared with the mean root mean square delay spread of ultra high frequency frequencies. The same characteristics were captured in the case of comparing horizontal and vertical co-polarization where the horizontally polarized signal is more sensitive to distance changes. All above mentioned properties are depicted in Fig. 11.

3.3 Coherence bandwidth

Figure 12 depicts the root mean square delay spread dependency of the coherence bandwidth in 1.3 GHz non-line of sight environments where the coherence bandwidth in MHz and the root mean square delay spread in ns. This relation is fitted with an exponential model $B_{c,0.5} = 18.34 \cdot e^{-0.002\sigma_\tau}$.

Figure 13 depicts root mean square delay spread dependency of the coherence bandwidth in 5.8 GHz non-line of sight environments where the coherence bandwidth is in megahertz and the root mean square delay spread is in nanoseconds. The measurements represented by blue circles, which were achieved from R2, R3, R4 route measurements, fit with the exponential model $B_{c,0.5} = 121.5 \cdot e^{-0.014\sigma_\tau}$. A similar relation was observed in [34, 35].

3.4 Channel frequency response variation

Figure 14 depicts the cumulative probability of the measured wideband channel frequency response variation for different routes (R1, R2, R3, R4) of 1.3 GHz center frequency and horizontal and vertical co-polarizations. It can be observed that the channel frequency response variation values fit well with the Normal distribution which is plotted as a dotted curve colored according to a particular route. The channel frequency response variations have mean values of 0.044, 0.25, 0.288, and 0.182 dB and standard deviation of 0.036, 0.291, 0.403, and 0.196 dB in the case of horizontal co-polarization, whereas the mean values of 0.06, 0.127, 0.377, and 0.295 dB and standard deviation of 0.078, 0.172, 0.537, and 0.289 dB in the case of vertical co-polarization. It can be noticed that the channel frequency response variations have the smallest mean and standard deviation values in the case of the R1 route which corresponds to the line of sight scenario.

Figure 15 presents the cumulative probability of the measured wideband channel frequency response variation for different routes (R1, R2, R3, R4) of 5.8 GHz center frequency and horizontal and vertical co-polarizations. It can be seen that the channel frequency response variation values also fit well with the Normal distribution which is plotted as a dotted curve colored according to a particular route. The channel frequency response variations have mean values of 0.041, 3.083, 1.246, and 2.296 dB and standard deviation of 0.119, 2.902, 1.686, and 2.3 dB in the case of horizontal co-polarization, whereas the mean values of 0.044, 3.48, 1.621, and 1.491 dB and standard deviation of 0.119, 2.952, 1.621, and 1.478 dB in the case of vertical co-polarization. The same feature of lowest mean and standard deviation values appears for the first route R1 which represents the line of sight scenario.

It is also clear from Figs. 14 and 15 that the channel frequency response variations increase with frequency. This merit becomes more visible in the case of the non-line of sight scenario. The second route R2 shows the highest channel frequency response variation due to higher frequency signals which tend to scatter more than the lower ones. These scatter objects can be moving people and cars.

4 Conclusion

In this paper, a device to device outdoor long-range communication channel was utilized for a measurement campaign. Both ultra high frequency and super high frequency channels were sounded using Yagi Tonna antennas as a

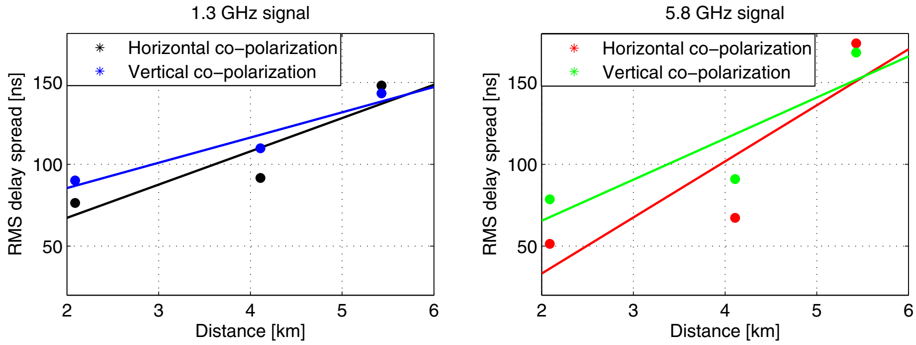


Fig. 11 Root mean square delay spread versus distance. The mean values of root mean square delay spread as a function of transmitter-receiver distance for different frequencies and co-polarizations in a non-line of sight environment

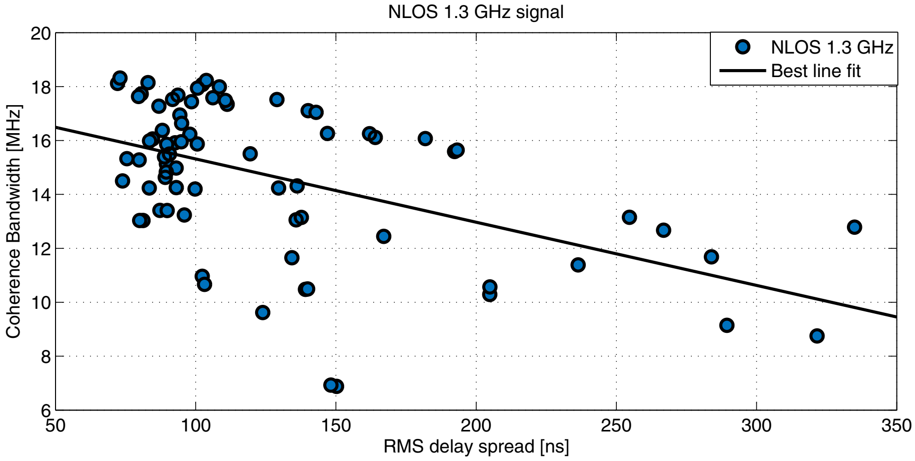


Fig. 12 Coherence bandwidth versus root mean square delay spread for 1.3 GHz. Scatter plot of the coherence bandwidth $B_{c,0.5}$ against the root mean square delay spread in the case of a transmitted signal with 1.3 GHz center frequency in non-line of sight environments

transmitter and a transmitter at 1.3 GHz and a parabolic RD-5G30-LW RocketDish antenna transmitter and AM-V5G-Ti sector antenna receiver at 5.8 GHz. The vertical and the horizontal co-polarizations were presented in both line of sight and non-line of sight scenarios. As output, channel characteristics such as root mean square delay spread, path loss, coherence bandwidth, and channel frequency response variation were extracted.

In the case of microcell LOS environment (with 315-m distance), the mean path loss value for vertical co-polarization exceeds the mean path loss value of the horizontal one by 0.93 dB and 1.62 dB in the case of ultra high frequency and super high frequency bands, respectively. It was observed that the path loss increases with frequency about 27 and 28 dB in the case of horizontal and vertical co-polarizations, respectively. Moreover, the higher frequency provides smaller mean root mean square delay spread in both horizontal and vertical polarizations settings. It was also mentioned that the vertical co-polarization shows higher mean root mean square delay than horizontal co-polarization. Finally the channel frequency response variations were negligible in the case of ultra high frequency and super high frequency channel sounding with horizontal and vertical polarization cases.

In the case of macrocell non-line of sight environments (with 2.089, 4.11, and 5.429 km distances), the path loss exponents for ultra high frequency are $n = 3.9$ for horizontal and $n = 3.7$ for vertical polarizations, and for super high frequency $n = 4.6$ for horizontal and $n = 4.1$ for vertical polarizations. All non-line of sight routes offer larger root mean square delay spread compared with the line of sight scenario. The vertically polarized

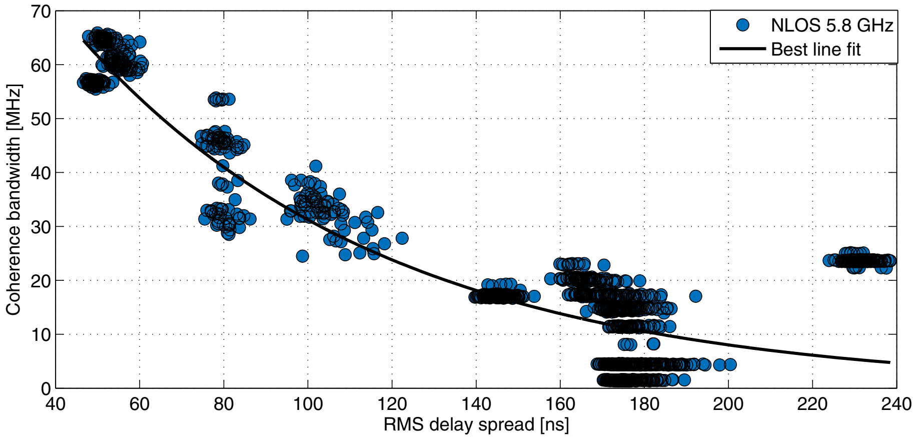


Fig. 13 Coherence bandwidth versus root mean square delay spread for 5.8 GHz. Scatter plot of the coherence bandwidth $B_{c,0.5}$ against the root mean square delay spread in the case of a transmitted signal with 5.8 GHz center frequency in non-line of sight environments

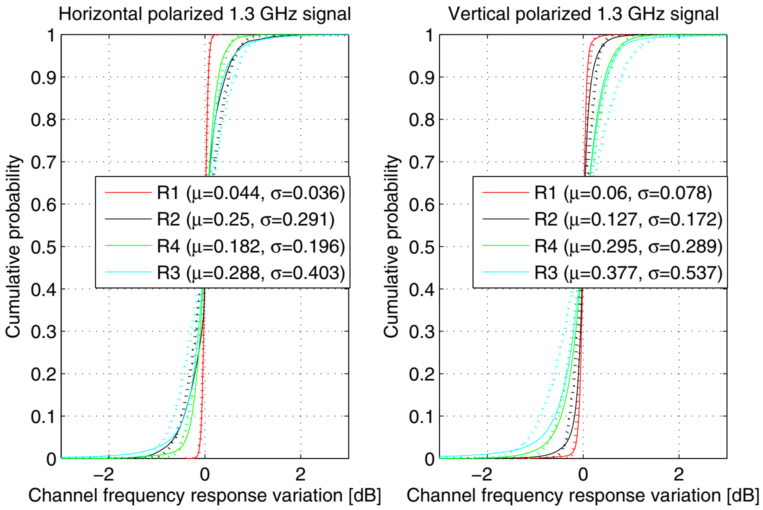


Fig. 14 Cumulative distribution function of channel frequency response variation of 1.3 GHz center frequency for both horizontal and vertical co-polarizations. The curve colored in red, black, blue, and green represent the calculated channel frequency response variation for the first to the fourth routes, respectively. The colored dotted lines represent the normal distribution of the corresponding measured channel frequency response variation values

signal shows higher mean root mean square delay than the horizontally polarized one in the case of ultra high frequency and super high frequency bands for R1, R2, R4 routes. However, an inverse relation was observed in the case of R3 which is explained by depolarization effects caused by the metal roof of the building between the transmitter and the receiver. It was also noticed that the mean root mean square delay spread values increase with the increasing distance between the transmitter and the receiver for all above-tested combinations. Furthermore, the relation between the coherence bandwidth and the root mean square delay spread was investigated. The relation is described by the exponential equation $B_{c,0.5} = k \cdot e^{-a\sigma_{\tau}}$ where the coherence bandwidth is in megahertz and the root mean square delay spread is in nanoseconds. The channel frequency response variations were also

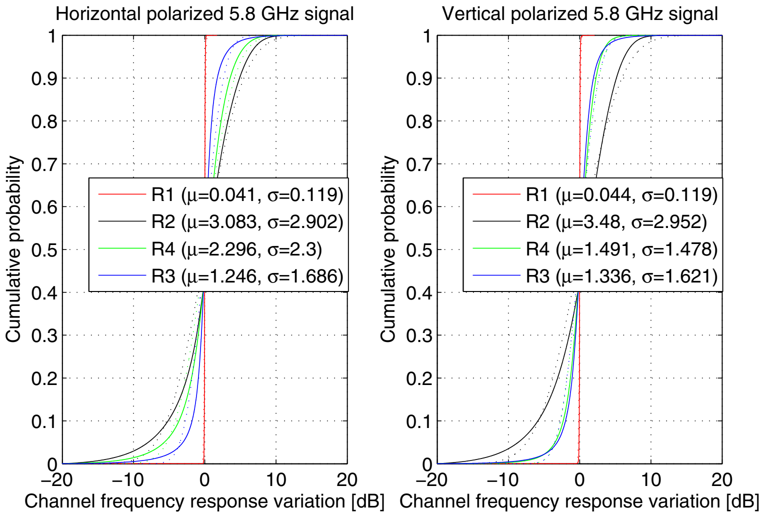


Fig. 15 Cumulative distribution function of channel frequency response variation of 5.8 GHz center frequency for both horizontal and vertical co-polarization. The curve colored in red, black, blue, and green represent the calculated channel frequency response variation for the first to the fourth routes, respectively. The colored dotted lines represent the normal distribution of the corresponding measured channel frequency response variation values

studied. It was observed that the variation increases with frequency and becomes more critical in the case of non-line of sight scenarios.

Abbreviations

3GPP: 3rd generation partnership project; 5G: 5th generation; ABG: Alpha-beta-gamma; AF: Amplify and forward; AoA: Angle of arrival; AWGN: Additive white gaussian noise; BER: Bit error ratio; BS: Base station; CDF: Cumulative distribution function; CFR: Channel frequency response; CFRV: Channel frequency response variation; CI: Close-in; CIR: Channel impulse response; D2D: Device to device; DF: Decode and forward; DoA: Delay of arrival; DT: Direct transmission; FM: Frequency modulation; FMCW: Frequency modulated continuous wave; ISI: Inter symbol interference; ITU: International Telecommunication Union; LOS: Line of sight; MIMO: Multiple-input multiple-output; NLOS: Non-line of sight; NR: New radio; OLOS: Obstructed line of sight; RAID: Redundant array of inexpensive disks; RCS: Radar cross section; RF: Radio frequency; RMS: Root mean square; RX: Receiver; SAGE: Space-alternating generalized expectation-maximization; SCC: Spatial correlation coefficient; SHF: Super high frequency; SNR: Signal to noise ratio; TX: Transmitter; UE: User equipment; UHF: Ultra high frequency

Acknowledgements

Not applicable.

Authors' contributions

EK was involved in analyzing, processing the measured data, deriving the results, and writing the manuscript. JB was responsible for proofreading this work and providing a meaningful feedback. JB, AP, JV, MP, RM, and JH were responsible for carrying out the measurement campaign. All authors read and approved the final manuscript.

Funding

Research described in this paper was financed by the Czech Ministry of Education within the frame of the National Sustainability Program under grant LO1401. It was also financed by the Czech Science Foundation, Project No. 17-27068S. For research, infrastructure of the SIX Center was used.

Availability of data and materials

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Department of Radio electronics, Brno University of Technology, Technicka 12, Brno, Czech Republic . [2]RACOM s.r.o, Mírova, Nove Mesto na Morave, Czech Republic .

Received: 23 December 2018 Accepted: 3 July 2019
Published online: 23 July 2019

References

1. C. Yu, K. Doppler, C. B. Ribeiro, O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks". IEEE Trans. Wirel. Commun. **10**(8), 2752–2763 (2011)
2. K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, K. Hugl, "Device-to-device communication as an underlay to lte-advanced networks". IEEE Commun. Mag. **47**(12), 42–49 (2009)
3. J. Wang, K. Liu, K. Xiao, C. Chen, W. Wu, V. C. S. Lee, S. H. Son, "Dynamic clustering and cooperative scheduling for vehicle-to-vehicle communication in bidirectional road scenarios". IEEE Trans. Intell. Transp. Syst. **19**(6), 1913–1924 (2018)
4. J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, J. Wang, *"Vehicle-to-vehicle communications: Readiness of v2v technology for application"*, (2014)
5. A. H. Kemp, S. K. Barton, "The impact of delay spread on irreducible errors for wideband channels on industrial sites". Wirel. Pers. Commun. **34**(3), 307–319 (2005). https://doi.org/10.1007/s11277-005-5230-2
6. W. Fan, I. Carton, J. Ø. Nielsen, K. Olesen, G. F. Pedersen, "Measured wideband characteristics of indoor channels at centimetric and millimetric bands". *EURASIP Jo. Wirel. Commun. Netw.* **2016**(1), 58 (2016). https://doi.org/10.1186/s13638-016-0548-x
7. K. Guan, B. Ai, M. L. Nicolás, R. Geise, A. Möller, Z. Zhong, T. Kürner, "On the influence of scattering from traffic signs in vehicle-to-x communications". IEEE Trans. Veh. Technol. **65**(8), 5835–5849 (2016)
8. Sun, Shu, et al., in *"Propagation path loss models for 5g urban micro- and macro-cellular scenarios"*. 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring). IEEE, 2016
9. J. Chen, X. Yin, L. Tian, N. Zhang, Y. He, X. Cheng, W. Duan, S. Ruiz Boqué, "Measurement-based los/nlos channel modeling for hot-spot urban scenarios in umts networks". Int. J. Antennas Propag. **2014**(Article ID 454976) (2014), pp. 12. https://doi.org/10.1155/2014/454976
10. J. li, Y. Zhao, C. Tao, B. Ai, "System design and calibration for wideband channel sounding with multiple frequency bands". IEEE Access. **5**, 781–793 (2017)
11. R. Nilsson, J. van de Beek, in *2016 IEEE Wireless Communications and Networking Conference*. "Channel measurements in an open-pit mine using usrps: 5g – expect the unexpected", (Doha, 2016), pp. 1–6. https://doi.org/10.1109/WCNC.2016.7564672
12. V. Kristem, C. U. Bas, R. Wang, A. F. Molisch, "Outdoor wideband channel measurements and modeling in the 3–18 GHz band". IEEE Trans. Wirel. Commun. **17**(7), 4620–4633 (2018)
13. A. Healey, C. H. Bianchi, K. Sivaprasad, in *2000 IEEE-APS Conference on Antennas and Propagation for Wireless Communications (Cat. No.00EX380)*. "Wideband outdoor channel sounding at 2.4 GHz", (Waltham, 2000), pp. 95–98. https://doi.org/doi:10.1109/APWC.2000.900150
14. J. Liang, J. Lee, M. Kim, J. Kim, in *2014 International Conference on Information and Communication Technology Convergence (ICTC)*. "Experimental wideband spatial correlation measurements of low-height mobiles in outdoor urban environments", (Busan, 2014), pp. 854–857. https://doi.org/10.1109/ICTC.2014.6983312
15. W. Wang, T. Jost, U. Fiebig, "A comparison of outdoor-to-indoor wideband propagation at s-band and c-band for ranging". IEEE Trans. Veh. Technol. **64**(10), 4411–4421 (2015)
16. E. Suikkanen, L. Hentilä, J. Meinilä, in *2010 Future Network Mobile Summit*. "Wideband radio channel measurements around 800 mhz in outdoor to indoor and urban macro scenarios", (Florence, 2010), pp. 1–9
17. X. Nie, J. Zhang, Z. Liu, P. Zhang, Z. Feng, in *2010 IEEE Wireless Communication and Networking Conference*. "Experimental investigation of MIMO relay transmission based on wideband outdoor measurements at 2.35 GHz", (Sydney, 2010), pp. 1–6. https://doi.org/10.1109/WCNC.2010.5506459
18. E. Kassem, R. Marsalek, J. Blumenstein, in *2018 25th International Conference on Telecommunications (ICT)*. "Frequency domain zadoff-chu sounding technique for USRPs", (St. Malo, 2018), pp. 302–306. https://doi.org/10.1109/ICT.2018.8464940
19. T.S.G.R.A.N., 3rd Generation Partnership Project, "User equipment (UE) radio transmission and reception, part 1: range 1 standalone (rel. 15)". 3GPP TS. **38**(V1.0.0), 101–1 (2018)
20. T. S. Rappaport, et al., *Wireless communications: principles and practice*, vol. 2. (Prentice hall PTR, New Jersey, 1996)
21. I.-R. Recommendation, *"Guidelines for evaluation of radio transmission technologies for imt-2000 Rec. ITU-R M. 1225,"*(1997), pp. 1–60
22. K. Pahlavan, A. H. Levesque, *Wireless information networks*, vol. 93. (John Wiley & Sons, 2005)
23. J. M. Molina Garcia Pardo, M. Lienard, P. Degauque, "Propagation in tunnels: Experimental investigations and channel modeling in a wide frequency band for MIMO applications". EURASIP J. Wirel. Commun. Netw. **2009**(1), 560571 (2009)
24. M.-G. Di Benedetto (ed.), *UWB communication systems: a comprehensive overview*, vol. 5 (Hindawi Publishing Corporation, 2006)
25. D. C. Stone, "Application of median filtering to noisy data". Can. J. Chem. **73**(10), 1573–1581 (1995)
26. R. G. Vaughan, "Signals in mobile communications: A review". IEEE Trans. Veh. Technol. **35**(4), 133–145 (1986)
27. W. C. Y. Lee, Y. Yeh, "Polarization diversity system for mobile radio". IEEE Trans. Commun. **20**(5), 912–923 (1972)
28. G. R. MacCartney, T. S. Rappaport, "Rural macrocell path loss models for millimeter wave wireless communications". IEEE J. Sel. Areas Commun. **35**(7), 1663–1677 (2017)

29. H. Hashemi, D. Tholl, "Statistical modeling and simulation of the rms delay spread of indoor radio propagation channels". IEEE Trans. Veh. Technol. **43**(1), 110–120 (1994)
30. T. S. Rappaport, G. R. MacCartney, M. K. Samimi, S. Sun, "Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design". IEEE Trans. Commun. **63**(9), 3029–3056 (2015)
31. S. Sangodoyin, S. Niranjayan, A. F. Molisch, "A measurement-based model for outdoor near-ground ultrawideband channels". IEEE Trans. Antennas Propag. **64**(2), 740–751 (2016)
32. L. Rubio, J. Reig, H. Fernández, M. R. P. Vicent, "Experimental uwb propagation channel path loss and time-dispersion characterization in a laboratory environment". Int. J. Antennas Propag. **2013**, 1–7 (2013)
33. S. M. Yano, in *Vehicular Technology Conference. IEEE 55th Vehicular Technology Conference*. "Investigating the ultra-wideband indoor wireless channel", vol. 3 (IEEE, VTC Spring, 2002), pp. 1200–1204
34. Y. Wang, W. Lu, H. Zhu, "Propagation characteristics of the lte indoor radio channel with persons at 2.6 GHz". IEEE Antennas Wirel. Propag. Lett. **12**, 991–994 (2013)
35. A. M. Tonello, F. Versolatto, B. Bejar, "A top-down random generator for the in-home plc channel". 2011 IEEE Global Telecommun. Confer. - GLOBECOM. **2011**, 1–5 (2011)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

sensors

Article

Insights into the Issue of Deploying a Private LoRaWAN

Radek Fujdiak [1,*], Konstantin Mikhaylov [2], Jan Pospisil [1], Ales Povalac [1] and Jiri Misurec [1]

[1] Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 61600 Brno, Czech Republic; xpospi90@vutbr.cz (J.P.); povalac@vut.cz (A.P.); misurec@vut.cz (J.M.)
[2] Centre for Wireless Communications, University of Oulu, Erkki Koiso-Kanttilan Katu 3, 90014 Oulu, Finland; konstantin.mikhaylov@oulu.fi
* Correspondence: fujdiak@vut.cz

Abstract: The last decade has transformed wireless access technologies and crystallized a new direction for the internet of things (IoT). The modern low-power wide-area network (LPWAN) technologies have been introduced to deliver connectivity for billions of devices while keeping the costs and consumption low, and the range of communication high. While the 5G (fifth generation mobile network) LPWAN-like radio technologies, namely NB-IoT (narrowband internet of things) and LTE-M (long-term evolution machine type communication) are emerging, the long-range wide-area network (LoRaWAN) remains extremely popular. One unique feature of this technology, which distinguishes it from the competitors, is the possibility of supporting both public and private network deployments. In this paper we focus on this aspect and deliver original results comparing the performance of the private and public LoRAWAN deployment options; these results should help understand the LoRaWAN technology and give a clear overview of the advantages and disadvantages of the private versus public approaches. Notably, we carry the comparison along the three dimensions: the communication performance, the security, and the cost analysis. The presented results illustratively demonstrate the differences of the two deployment approaches, and thus can support selection of the most efficient deployment option for a target application.

Keywords: IoT; LPWA; LoRaWAN; LoRa; indoor; private; public

Citation: Fujdiak, R.; Mikhaylov, K.; Pospisil, J.; Povalec, A.; Misurec, J. Insights into the Issue of Deploying a Private LoRaWAN. *Sensors* **2022**, *22*, 2042. https://doi.org/10.3390/s22052042

Academic Editors: Carlos Tavares Calafate, Miroslav Voznak, Peppino Fazio and Miralem Mehić

Received: 31 December 2021
Accepted: 1 March 2022
Published: 5 March 2022

1. Introduction

1.1. Internet of Things Connectivity

During the last decade, wireless communication technologies have advanced significantly [1], and it is expected that the number of connected devices will reach 26.4 billion by 2026 [2]. These technologies became the primary activators and essence for the new paradigm of the Internet of Things (IoT) [3], and we are now witnessing the rise of IoT applications [4]. Nowadays, the IoT covers many different areas, i.e., sensor networks, telemetry systems, and remote metering. These applications have very specific requirements, such as [5] long battery life, long communication range, a high number of nodes per base station, and high density of nodes. The conventional technologies were not prepared for new applications, and therefore they did not offer sufficient solutions. A new type of wireless solution has been introduced to fulfill these new and specific needs, known as low-power wide-area network (LPWAN) [6].

lAt present, there are many different technologies recognized as LPWAN, i.e., long-range wireless-area network (LoRaWAN), SigFox, narrowband IoT (NB-IoT), Weightless, Ingenu, Nwave, Waviot, Wi-Fi HaLow, Tlensa, Amber, and many others [7,8]. Each technology slightly differs from the others, but the main LPWAN parameters, such as long battery life, extended communication range, and relatively low cost, stay the same. However, the SigFox, LoRaWAN, and NB-IoT are the most discussed, with the LoRaWAN being currently the most adopted LPWAN technology for the IoT [9]. The LoRaWAN technology is an open global standard provided by the association of companies known as the LoRaWAN Alliance™ [10]. The LoRaWAN might be deployed as a public or private network, unlike other LPWAN such as SigFox or NB-IoT, which offer only a public variant. This feature offers a new perspective of LPWAN with different applications.

A major change in the IoT connectivity landscape is expected after the introduction and broad deployment of the 5G (fifth generation) mobile networks. The 5G networks will enable much lower latency, higher capacity, and the higher bandwidth compared to 4G technologies [11]. Notably, the 5G [12] will bring the evolution for NB-IoT and LTE-M. However, as discussed in [13], there is no universal solution or a single technology that fits all applications. Each connectivity option is more or less suitable for a specific application. In the same manner, the 5G NR (new radio) technology is of great interest and may enable a whole plethora of new use cases for tactile IoT in the context of industrial and medical verticals, for example. However, the communication range of high-bandwidth 5G connectivity is rather limited, and, as of today, not so many 5G-enabled locations are present in Czech Republic. For this reason, we expect that LPWAN technologies will still continue playing an important role in the future, while the 5G technology can serve their backbone links and more demanding applications and use cases.

1.2. Contribution and Structure of This Study

Many works focus on the technology itself or deal with either private or public network independently, as we discuss further in Section 2. The main contribution of this work is that we address both these deployment options and highlight the difference between them, with respect to three major metrics: the network performance, security, and costs. Namely, we first conduct an experimental measurement campaign to estimate the coverage and signal levels of the private and public LoRaWAN networks in the campus of Brno University of Technology, and compare the results of the two networks. Second, we deliver the analysis of the security procedures specified in the different LoRaWAN specification releases, and discuss the security aspects relevant to private and public network deployments. Third, we deliver the model and identify the cost components allowing to estimate the costs of LoRaWAN deployment and owning, and detail the steps one has to take to make a decision whether to go for public or private LoRaWAN deployment. To the best of our knowledge, the current work is the first one which analyzes and compares the two LoRaWAN deployment options, thus supporting selection of the one most suitable.

The rest of the paper is organized as follows: Section 2 provides an in-depth analysis of the advances in LPWAN focusing on the LoRaWAN technology. Section 3 introduces the experimental environment used for our measurements and experiments, while the main contribution (technological, security, and deployment evaluation) is included in Section 4. Finally, Section 5 summarizes our conclusions.

2. Background and State of the Art

The essence of LPWAN dates back to the 1980s–1990s, when technologies and networks with similar architectures were introduced, i.e., AlarmNet from ADEMCO [14], followed by 2G (second generation mobile network) technologies, and many others. However, the modern technological concept recognized as LPWAN started with SigFox in 2009 and continued with many new technologies such as Weightless, LoRaWAN, Ingenu, Waviot, NB-IoT, and others. Moreover, the first relevant scientific papers about LPWAN were published a few years ago, in 2015; since then, interest in LPWAN has grown steadily (see Figure 1).

LPWAN technologies differ from their precursors as well as from other conventional technologies, i.e., cellular technologies (2G+), mesh technologies (IQRF, Wirepas PINO™), and short-to-middle range radio access technologies (Wi-Fi, ZigBee, Bluetooth, RFID). The main difference is the combination of the long range with a long battery life, which, however, results in the low throughput and limited transmission frequency. This paper focuses on the most widely adopted LPWAN technology, namely LoRaWAN.

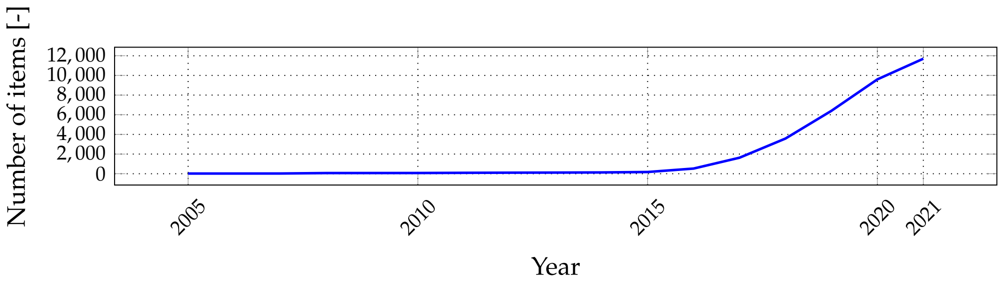


Figure 1. Results of keyword search of the term "LPWAN" in Google Scholar for selected years.

The LoRaWAN is an open standard technology based on the proprietary modulation known as the long-range (LoRa) derivative of the chirp spread spectrum (CSS) modulation. The LoRa modulation was introduced in 2007 by the Cycleo company and was taken over by the Semtech company in 2012. Nowadays, it is protected by patents EP2763321 [15] and US7791415 [16]. On the OSI (open systems interconnection) model layer structure, LoRa can be attributed to the physical layer of LoRaWAN, while LoRaWAN defines the MAC (medium access control) layer. Nowadays, the standard defines two main modulations for terrestrial LoRaWAN (long-range-LoRa; frequency-shift keying—FSK), and the network is deployed in the star topology, similar to cellular networks (see Figure 2). The gateways connect the end-devices (sensors, indicators, meters, and others) via the radio channel, covering selected areas. Subsequently, the data are transmitted via the transport technology (i.e., metallic Ethernet or cellular network) through the LoRaWAN server to the end-user application (e.g., remote monitoring or quality management). The LoRaWAN server is a combination of several different sub-servers—network server (NS), join server (JS), and application server (AS), which are handling different layers and processes (services) [17]. The NS terminates the LoRaWAN MAC layer for end-devices connected to the network. JS manages the over-the-air activation (OTAA) and activation-by-personalization (ABP) processes for end-devices. AS handles all the application layer payloads of the associated end-devices, provides the application-level service to the end-user, and generates all the application layer downlink payloads towards the connected end-devices. However, we will consider the LoRaWAN server as a complex co-located solution for hosting these servers [10].

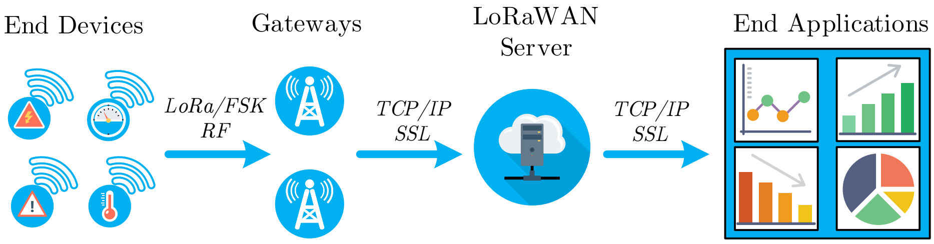


Figure 2. Architecture of the LoRaWAN from the end-device to end-application.

Many theoretical works and surveys have already been published, focusing on the main parameters of LoRaWAN as well as providing comparison of LoRaWAN and the other LPWAN technologies [9,18–24]. To give an example, Table 1 illustrates the data rate and the maximum communication range for LoRaWAN as defined by selected papers. The data rate negligibly differs, while the estimated communication range significantly changes through the different papers. The data rate varies mostly because of formal issues, such as not considering the frequency-shift keying modulation or packet overheads of different layers, rounding the values, estimating only the maximal value, and others. On the other hand, the estimates of the maximum communication range differ significantly-from 10 to 50 km; this shows that the experience of various scientists of the LoRaWAN technology differs across the field.

Table 1. Comparison of different parameter estimations based on the physical level in selected papers.

Paper	Data Rate (kb/s)	Communication Range (km)
[25]	0.29–50	15
[13]	0.29–50	less than 35
[5]	max. 50	5 (U), 20 (R)
[6]	0.3–37.5	3–10 (U), 30–50 (R)
[26]	0.3–37.5 (L), 50 (F)	10 (U), 50 (R)
[27]	27 (L), 50 (F)	2–5 (U), 15 (R)
[7]	0.25/5.5/11/50	2–15
[9]	max.50	5 (U), 20 (R)
[28]	0.3–50	up to 10
[29]	0.3–50	2–5 (U)
[30]	0.29–50	2–5 (U) 45 (R)

Note: L —LoRa; F—FSK; U—Urban; R—Rural.

One of the reasons for this is the fact that the main parameters of LoRaWAN strongly depend on many variables, which we discuss below [10,31–34]:

- **Selected channel (CH) or sub-band (f)** determines the maximum transmit power (10 mW, 25 mW, or 500 mW), which impacts, for example, the communication range, material penetration capability, signal propagation, and the duty-cycle (0.1%, 1%, 10%, or 100%), which impacts the allowed transmission frequency and thus the maximum data rate.
- **Bandwidth (BW)** established for Europe is either 125 kHz or 250 kHz.
- **Modulation (MOD)**; LoRaWAN specifies two types of modulation: (i) FSK, and (ii) LoRa modulation. The FSK demands higher signal-to-noise ratio (SNR) and thus is typically used when the communication channel is good and communication range is relatively short. Compared to FSK, the LoRa modulation offers a 13 dB better channel budget and Doppler resistance and approx. 10–20 dB increased interference immunity.
- **Spreading factor (SF)** is defined as $SF \in \{7; \ldots; 12\}$ and determines the symbol duration $T_s = 2^{SF}T_c$, where the chirp interval is defined by BW as $T_c = 1/BW$. Moreover, the SF together with BW define the physical layer bit-rate:

$$R_b = SF\frac{CR}{\frac{2^SF}{BW}}. \tag{1}$$

- **Code rate (CR)** is defined as $CR = \frac{4}{4+R}$, where the rate $R \in \{0, \ldots, 4\}$ and determines redundant bits used for forward error correction—FEC (impacts the ability to correct damaged messages and error-rates). LoRaWAN prescribes use of $R = 1$ for packet payload, and $R = 4$ for the packet header.
- **Device class**, which defines the type of media access for downlink traffic, which also affects the end-device’s power consumption (class A—downlink only after uplink and the minimum consumed power; class B—periodic downlink slots with slightly higher device consumption; class C—highest consumption for devices, but downlink can be sent any time).
- **Device settings** provide a number of other configuration capabilities, including activation (over-the-air activation—OTAA or activation by personalization—ABP), key-generation, firmware updates, data rate (adaptive data rate—ADR, or fixed data rate—FDR), and others).

A lot has been written about the general LoRaWAN parameters. Specifically, a number of the scientific papers provide a general overview of LoRaWAN parameters, metrics, and performance indicators, i.e., capacity [35], coverage [36], maximal range [37], free-space behavior [38], usage [39], energy-efficiency [40], technology comparison [41], performance [42], mobility [43], and other parameters [44]. The authors of [45] compare analytically-obtained parameters of the well-known LPWAN technologies. There are also articles offering datasets from the already functional LoRaWAN network, for the possibility of in-depth research, to mention a few [46,47].

Authors in [19,48] propose routing schemes to create multi-hop communication and routing protocols or decentralized architecture [49] in order to improve LoRaWAN performance. Still, it requires special devices in the network or the end-device modification. The authors in [50] are experimenting with multi-RAT (multiple radio access technology) devices, combining LoRaWAN and NB-IoT to improve mainly energy consumption. The authors of [51] propose LoRaWAN integration into 4G/5G network, where the gateway includes the eNB (LTE evolved Node B) protocols so it can be part of a mobile network. The study [52] examines the technical and economic feasibility of deploying LoRaWAN in a licensed access spectrum band. Currently, however, LoRaWAN network operators use only the unlicensed band.

These results are beneficial for understanding the basics of the LoRaWAN technology or for improving the public network. Nevertheless, the LoRaWAN technology usesboth public and private deployments, and there are major differences between these two approaches (basic differences):

- **Public network**—the network is always owned by a third party (public operator of national or international scale), gateways are deployed to provide coverage over large geographical areas (wide area network—WAN), and for the end-user: fixed parameters of the network, non-transparent and uncontrolled environment, expected lower capital (no need to build the infrastructure), questionable operational expenses (based on the fees and scale), simple and fast deployment, and low technological and management requirements.
- **Private network**—the network is owned by the end-user (i.e., city, company, or individual), gateways are typically deployed to provide coverage over smaller geographical areas (i.e., local, campus, or metropolitan), dynamical (customizable) parameters of network for end-users, transparent and controlled environment for end-users, expected higher capital and questionable operational expenses (based on scale), more complex deployment, and higher technological and management requirements.

Although the private approach is a promising topic, only a very limited number of papers have dealt with private LoRaWAN networks. For example, the authors of [53] work with an experimental self-developed and minimized private network. The paper shows the relation between SNR, data rate, transmission time, and energy consumption. Though the paper provides experimental results, only limited technical details of the experiment are given (i.e., antennas gain and power settings are missing, and information about LoRaWAN stack is missing). Related work [54] focuses on the coverage and signal propagation within the single-gateway network. Authors give sufficient background about the experimental settings and develop a simple visualization method for the chosen use case (apartment building). Another experimental measurement campaign for a private LoRaWAN deployed for industrial application was published in [55]. The paper reports small-scale measurements of signal strength (RSSI) and SNR in an industrial complex (approx. 30 points). Similar work [56] provides results from early-stage measurements of the packet-loss rate in five selected points for a one-floor scenario. The studies [53–56] report show-cases of early-stage results for the LoRaWAN technology. On the other hand, the work [57] reports complex measurements of power consumption, outdoor signal propagation, adaptive data rate performance, and indoor measurement for a single-gateway network. Notably, the authors control many variables in their measurements, including spreading factor, channel selection, bandwidth selection, and modulation. Another significant work [58] reports very complex results from outdoor measurements of SNR in the campus use case (a single-gateway network). The results from [57,58] are valuable to the scientific community and provide a bright idea about the LoRaWAN technology and its usage in outdoor environment for private use cases. Moreover, the paper [57] presents the approach of using different channels of the 868 MHz band.

When we consider Europe, LoRaWAN operates in the unlicensed sub-GHz band, which for most European countries is set by the standard to 868 MHz [10] under CEPT Rec. 70-03 frequency band regulation [31]. The LoRaWAN specification recommends only three default channels: 868.1 MHz, 868.3 MHz, and 868.5 MHz [10]. In spite of that, they belong to the most frequently used channels in the unlicensed 868 MHz band (863–870 MHz) with a high probability of collision and high level of radio noise. There are several works focusing on collisions in the 868 MHz band, i.e., [9,59,60].

The paper [9] shows decreasing network performance, which comes with the growing number of communicating devices, i.e., decreasing number of received packets, decreasing packet delivery success ratio, and decreasing maximal throughput, to mention only a few. Moreover, the paper [59] shows the growing probability of collisions and packet loss, which comes with the increasing number of communicating nodes operating with different spreading factors. Further, the paper [60] summarizes the relations between the increasing number of communicating devices and the probability of channel occurrence, and the probability of collision. Furthermore, the number of wireless devices is growing in the 868 MHz band every day, which increases the noise background. These are, for example, fire alarm systems, intruder alarm systems, automation systems, access and remote control systems, smart meters, telemetry networks, automotive systems, and many others. The frequency band of 868 MHz is a free-licensed band, and we cannot completely evade the possibility of collision or a higher noise level. The paper [61] summarizes the level of interference experiences for selected channels of the 868 MHz band in different areas: shopping area, business park, hospital complex, industrial area, and residential area. Moreover, the same authors also published the paper [62], which focuses on the impact of interferences on the LoRaWAN and SigFox technologies. The interferences significantly impact the service quality and network coverage. For this reason, the three recommended channels of LoRaWAN will not be sufficient in future.

As one can see from the discussion above, none of the previous works has offered a comparison of the different LoRaWAN deployment options (i.e., private versus public). Meanwhile, this decision is critical and has to be often made by the application developers and service providers. Therefore, to bridge this gap, in the following we discuss the different aspects of the two network deployment options along the three tracks: the communication performance, the security, and the costs. We hope that these results will equip an interested reader with clear understanding of advantages and disadvantages of the two approaches, and assist him or her when deciding whether to go for a private or a public LoRaWAN network.

3. Experimental Environment

Our experimental environment is located in Brno, Czech Republic, at the Faculty of Electrical Engineering and Communication Technologies of the Brno University of Technology. The location is covered simultaneously by two LoRaWAN networks—a public and a private one, which we discuss in detail in the following subsections. In the last subsection, we also provide details about the devices we used in our tests.

3.1. Private Lorawan

The private network includes one single gateway with LORIOT cloud server. Specifically, we use the Lorank 8+ gateway with the following properties:

- Transmit power up to +27 dBm (500 mW, the power was always based on the selected channel and allowed value from the regulation recommendation [31]).
- Received signal sensitivity up to −138 dBm.
- Five dBi antenna.
- Communication range up to 25 km.

- Up to eight simultaneous receiving channels.
- Up to 60 thousand nodes.
- Whole gateway covered in an IP67 case.

Figure 3 shows the different parts of the university campus. Each letter indicates one part of the building. The gateway was positioned to cover both the building and part of the city in the E-part of the building. Further, the campus building is one of the highest points in the city. The Lorank 8+ gateway was placed on the roof of the E-part of the building of our campus with the coordinates of the site 49.2269133° N, 16.5752194° E. The E-part of the building provides a power panel for outdoor gateways and metal pillars for deployment. Using the 3D preview of the selected area, it can be observed that from the roof of the E-part of the building, which is marked in the picture (black dot), it is possible to observe most of the buildings in the city of Brno in the line-of-sight (see Figure 4). From the selection of multiple positions, this position seemed the most strategic given the above-mentioned parameters.

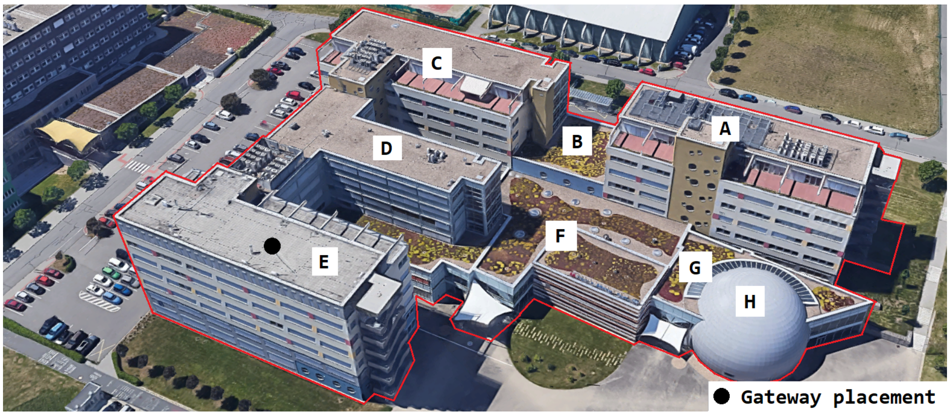


Figure 3. Location of our private one-gateway LoRaWAN experimental network with view of the individual buildings of the Electrical faculty (A–H are the names of the buildings).

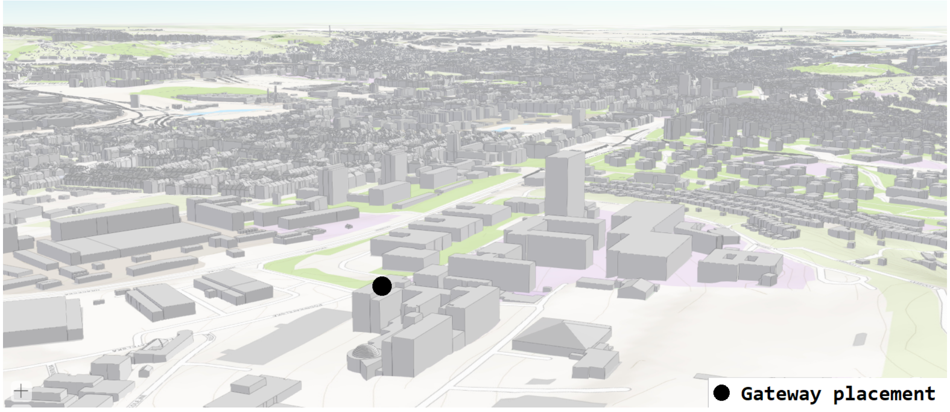


Figure 4. Location of our private one-gateway LoRaWAN experimental network with view of the city of Brno (website: http://webmaps.kambrno.cz/ (accessed on 15 February 2022)).

The gateway is connected via a basic commercial switch through the 100 MB/s Ethernet to the campus network. The optical connection was chosen to protect network equipment on campus from lightning damage. For this reason, however, Ethernet-to-optic media converter must be used at the gateway side and optic-to-Ethernet media converter on the campus side of the network. The LORIOT cloud itself is not operated locally on campus, but is run directly on LORIOT's servers, for which gateway access is through the Internet . The complete network topology is displayed in Figure 5.

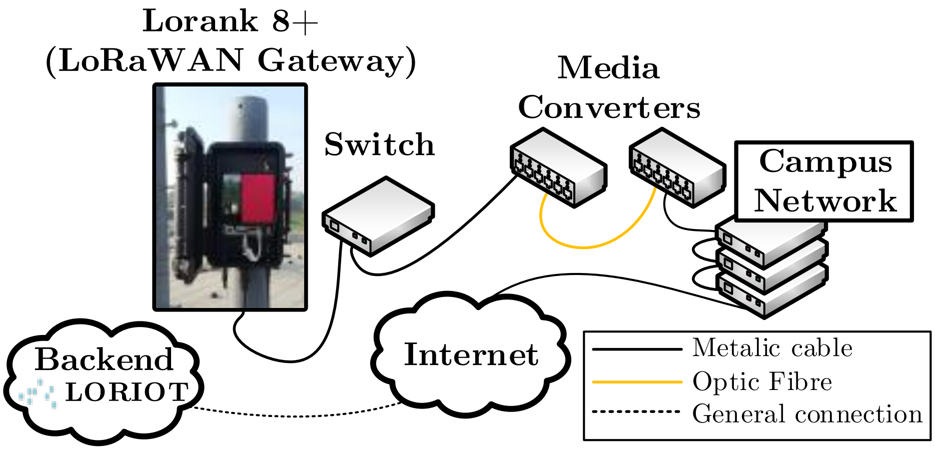


Figure 5. Topology of our LoRaWAN experimental single-gateway network.

3.2. Public Lorawan

To represent the public network, the LoRaWAN network of the Czech national operator ČRa (České Radiokomunikace) was selected (the coverage is displayed in Figure 6). The estimated coverage is based on the theoretical range of 8 km per gateway [58] (the availability was verified in a calibration test in front of the campus building). Therefore, our selected location should be decently covered by the national LoRaWAN operator with multiple nearby gateways. A total of 10 ČRa gateways are located within a radius of 16 km from the university campus. Even though there are several public LoRaWAN providers in the Czech Republic, the selected national operator is the only one covering the whole Czech Republic with hundreds of deployed base stations (WAN area). The other operators mostly provide only local services and their network covers only selected locations (LAN/MAN areas).

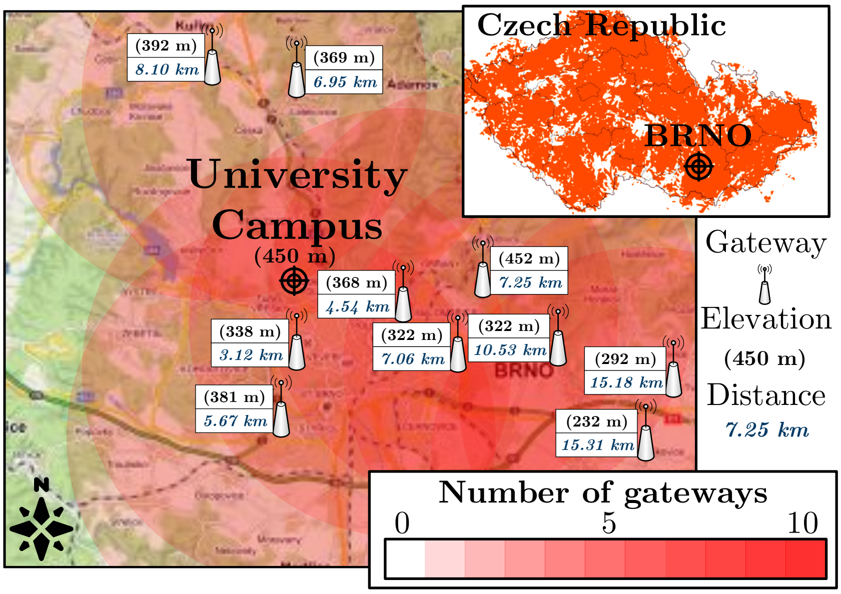


Figure 6. Coverage map of the public LoRaWAN network in the Czech Republic (upper-right corner) and coverage estimation of the nearest public network gateways in the selected location.

3.3. Test Device

For our measurements we used a certified LoRaWAN Field Test Device from Adeunis RF (ARF8123AA), with the following parameters [63]:

- Static node (no movement during measurement).
- Transmit power of 14 dBm (25 mW).

- Spreading factor 12.
- ABP activation (OTAA was not supported by public network operator that time), fixed data rate (adaptive data rate was not supported by public network that time).
- Sensitivity up to −140 dBm, 0 dBi wire antenna (Thermolast K TC7AA).
- Communication range up to 15 km.
- Device temperature limits −30 to +70 °C.

Table 2. Frequency plan for experimental measurements (both public and private networks).

Channels, f [MHz]	868.1 *	868.3 *	868.5 *	867.1
Channels (cont-d), f (MHz)	867.3	867.5	867.7	867.9
BW (KHz)	125			
MOD/SF	LoRa with Multi-SF			

* Default LoRaWAN channels from the newest specification [10].

To ensure fairness, the frequency plan was chosen based on the public operator's plan to provide identical conditions for both networks (see Table 2). To minimize the possibility of internetwork collisions, measurements were conducted in different time slots.

4. Experimental and Analytical Results

This section contains the main contribution of this paper—the results demonstrating the performance and comparing the two LoRaWAN deployment alternatives along the three tracks (each presents as a separate sub-chapter):

- **Performance evaluation**—provides an evaluation of the performance of the public and the private networks. First, we report the results of the outdoor measurements to confirm our claim about the importance of channel selection and its impact on the network parameters (signal strength, signal-to-noise ratio, and loss rate). Further, we provide extensive experimental measurement results for indoor scenario, coverage, penetration, and loss rate, which should give a sufficient overview of the LoRaWAN behavior in the indoor environment.
- **Security evaluation**—gives accurate information about the recent changes in the LoRaWAN protocol based on the newest documentation. We look at the basics of information security parameters, such as authentication, encryption, and data integrity, but also at key establishment and key update. We also discuss possible vulnerabilities and compare the older with the newest version of the LoRaWAN protocol. Finally, we summarize the differences regarding security in private and public networks.
- **Deployment ease evaluation**—introduces the deployment difficulties, a methodology for the deployment of the public or private network, and evaluates the possible expenses in the context of private and public networks.

4.1. Performance Evaluation

4.1.1. Impact of Channel Selection on Network Performance

We measured in front of the building H (approx. 35 m in front of the building H and 60 m from the building E). We selected two frequency plans (see Table 2): (i) the default LoRaWAN channel frequency plan (i.e., the three default LoRaWAN channels in the 868 MHz sub-band); and (ii) the extended channel frequency plan (in the 867 MHz sub-band, including additional channels). The results are displayed in Table 3 (LR = loss rate).

Table 3. Effect of the plan on performance (arithmetic means).

Scenario	RSSI (dBm)	SNR (dB)	LR (%)
Public—default plan (i)	−125	−18.36	43
Public—default plan (ii)	−97	−2.05	3
Private—default plan (i)	−96	0.01	21
Private—extended plan (ii)	−70	14.90	1

Each value represents an arithmetic mean of 100 messages, which were transmitted over the day for each scenario for the public and private network. The default channel settings showed a higher loss rate (40% higher in the public and 20% higher in the private network). The noise level, when using the default channels, was >14 dB higher than that for the extended frequency plan (the RSSI difference was >26 dB). The measurement sufficiently proves our claim that it is possible to at least partially evade interferences by choosing the right channels to extend the frequency plan. The growing number of devices will, in the future, create an environment with increased noise. Therefore, the LoRaWAN standard will need to evolve together with extending the recommended frequency plan, and give a methodology for choosing the right channels. Therefore, the private network has an advantage (given that these are updated regularly) over the public network as there might be a fully customized frequency plan that allows minimizing the interferences with other systems. Notably, the smaller scale of these networks supports using the different frequency plans in different regions.

4.1.2. Indoor Coverage and Signal Propagation

We measured the public and private network performance in the campus building (see Figure 3). Specifically, we estimated the RSSI, which provides information about signal propagation, coverage, sensitivity, and attenuation of materials. Each value is an arithmetic mean of 20 measurements. These values were obtained for each building part and the floor. Together, they were used to create a heat map of the RSSI (the outdoor calibration values are in Table 3—scenario (ii), private −84 dBm and public −108 dBm).

Figures 7 and 8 provide results for both networks on the seventh floor. The public network RSSI ranged from −97 to −119 dBm. The private network RSSI ranged from −70 to −107 dBm with expected best results in the building E (the building with our gateway on the roof). The mean loss rate was <0.1% for both types of network; this allows using both deployments in critical applications requiring >99.9 availability [64]. However, we observed a higher loss rate (7%) under the gateway (approx. 3 meters under a gateway with the reinforced concrete roof in between, the building E—the place with highest RSSI −70 dBm, see Figure 7). Although the private network offers higher RSSI than the public network, the public operator offers sufficient service to cover indoor conditions in this case. Based on the authors' market knowledge, the 868 MHz traffic will probably become denser in the future due to the growing number of sensors. Therefore, we can expect that the selected channels in the frequency plan will gain a higher noise level and the −119 dBm might become a border value for the sensitivity because the interferences might cause a signal strength degradation of over 20 dB for the LoRaWAN technology [62].

Figures 9 and 10 provide results for both networks on the fifth floor. The private network signal strength was in the range of −86 to −115 dBm with a strength loss of >10 dB in most of the building, except for the building A, where the degradation was minimal due to the line-of-sight between the building and the gateway. The loss rate in the private network grows to 1%. Moreover, the higher loss rate under the gateway in the building E was not observed. On the other hand, the public network signal strength ranged from −98 to −119 dBm. The min/max values are the same as on the previous floor, but the heat-map shows a rapid decrease of the mean RSSI (Figure 10). Further, the average loss rate on the fifth floor grew to 7% in the public network, which allows using it in non-critical indications, metering, and other applications requiring (>90%) availability. On this floor, the private network starts to show a slight advantage.

Figures 11 and 12 provide results for both networks on the third floor. The signal strength for the private network was in the range of −97 to −115 dBm. The signal strength dropped again by about 5 to 10 dB and the loss rate increased to 4%. However, the network parameters were stable, and the communication service was available throughout the whole building. An availability of 96% allows using it in most of the metering applications which require (>90%) availability [64]. Further, the range of RSSI for public networks was in the range of −116 dBm to no signal (N/O). The signal strength also decreased by another 10 dB. Compared with the calibration value, the attenuation is already more than 30 dB, which can be considered as a deep(er) indoor condition. The public service was already unavailable in some parts of the university complex (buildings A, B, and C). In other parts, the service was on the border of the measuring device's sensitivity. The heat map shows cold signal places throughout the whole building. Further, the average loss rate on this floor increased to 10% for the public network. This is the border value for most of the current applications [64].

Figures 13 and 14 provide results for both networks on the first floor. We experienced very deteriorated communication conditions. The building C is in the basement (below ground level). Other floors are above ground. For this reason, the building C shows the worst results. The private network RSSI ranged from −113 to −117 dBm (with no signal in the upper-right corner of the building C—marked as N/O). In the other parts of the campus, the RSSI values ranged from −89 to −115 dBm. The parameters were stable, and the loss rate increased to 5%, which still allows using it in most of the metering applications requiring (>90%) availability [64]. However, the public service was unavailable in the building C, and most of the other parts were on the border of sensitivity, close to −120 dBm. The loss rate grew to 12%, which is unacceptable for most of the current communication applications. The lowest floor, where very deep indoor conditions were experienced, shows the most significant differences between the private and the public network. Both networks show significantly decreased service quality.

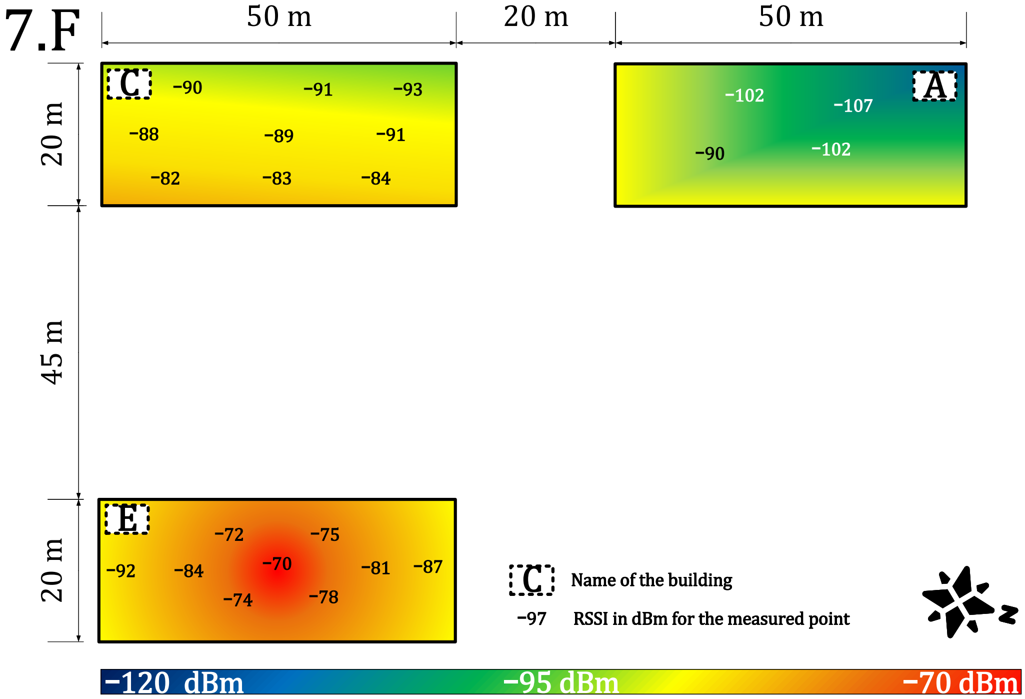


Figure 7. Private network coverage and signal propagation on the seventh floor.

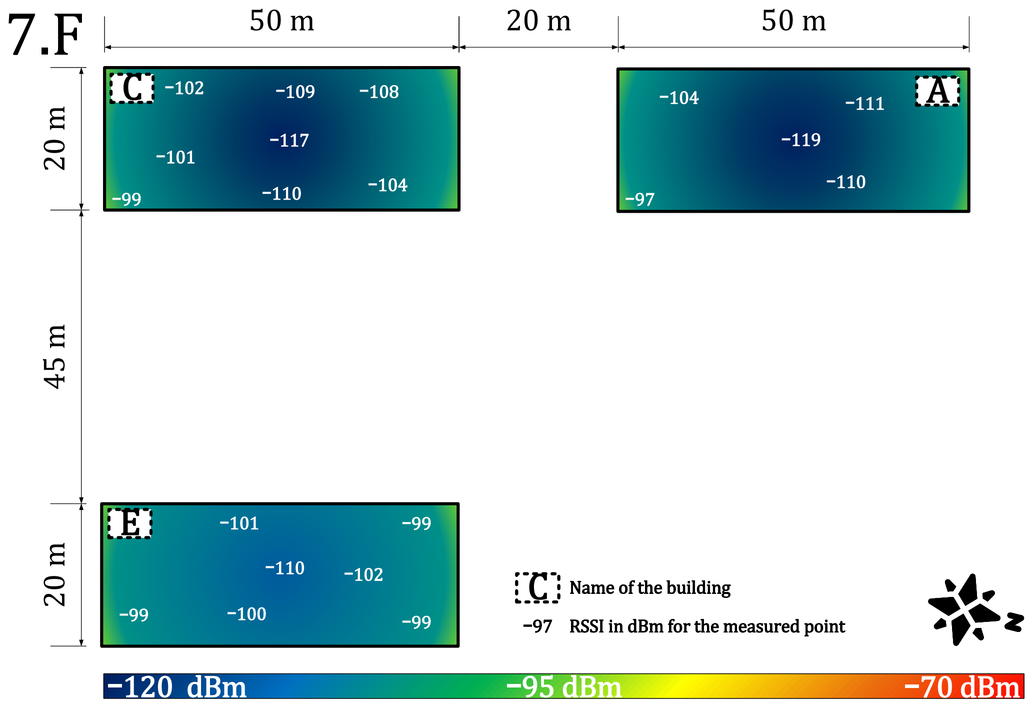


Figure 8. Public network coverage and signal propagation on the seventh floor.

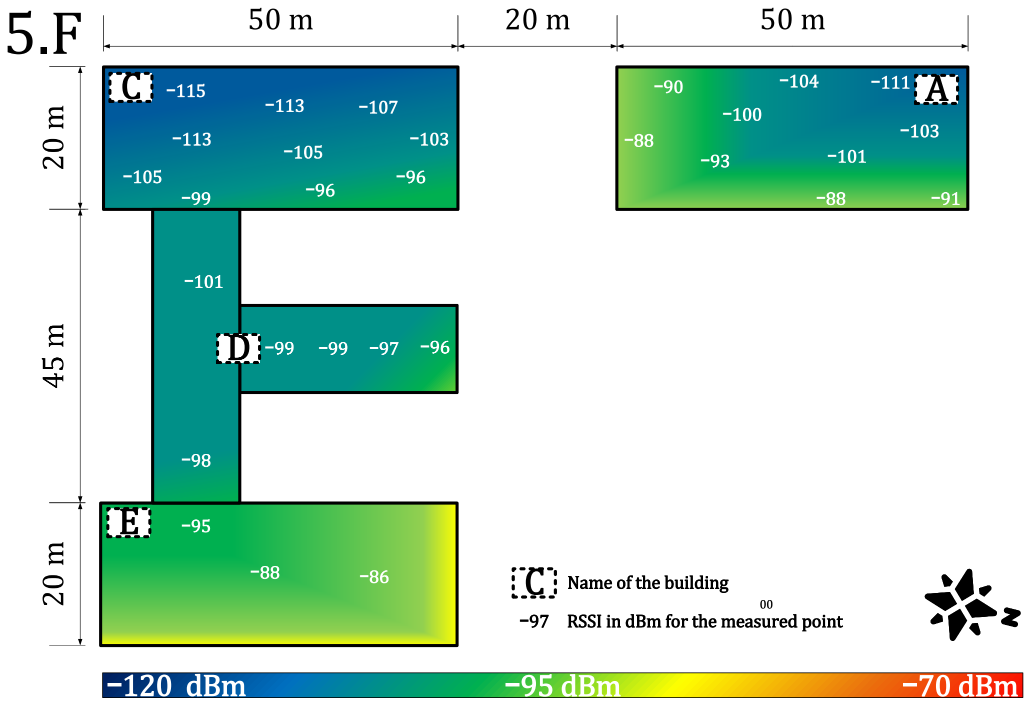


Figure 9. Private network coverage and signal propagation on the fifth floor.

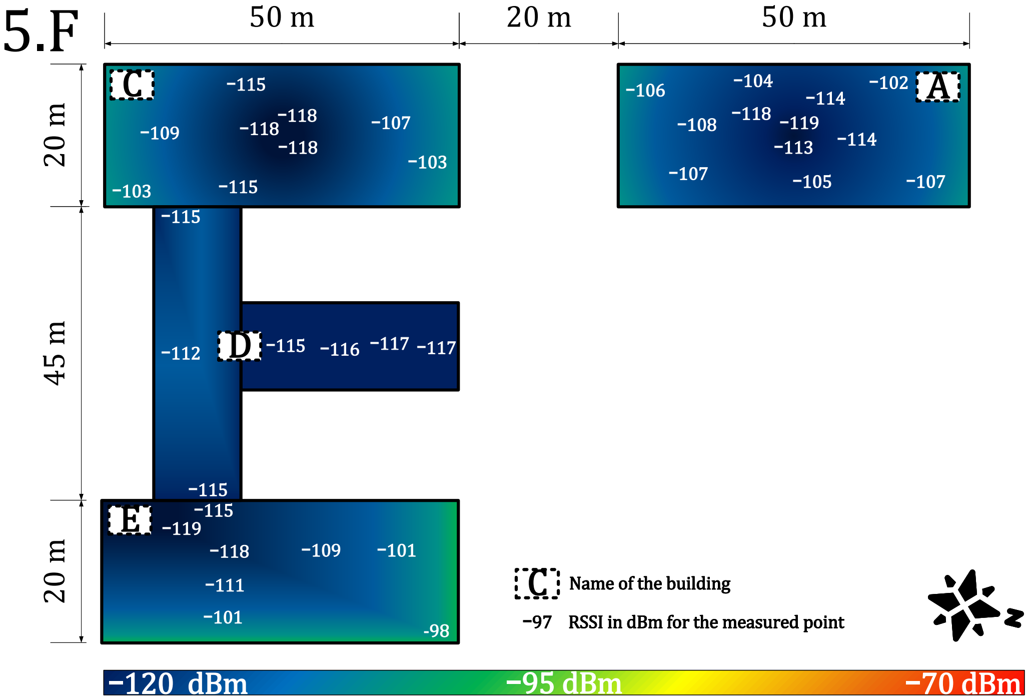


Figure 10. Public network coverage and signal propagation on the fifth floor.

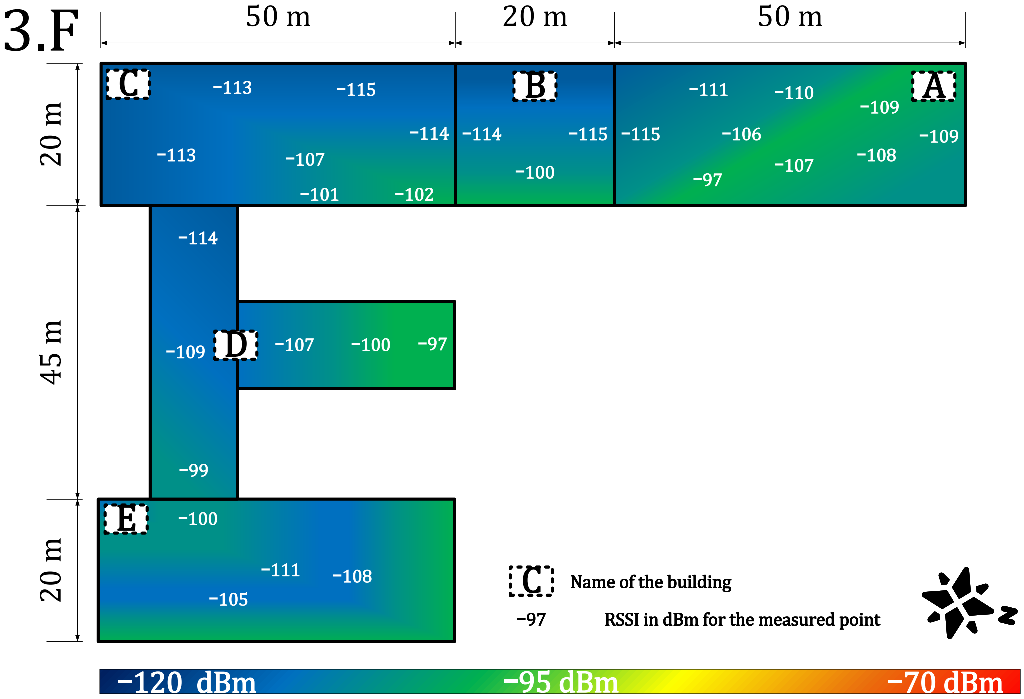


Figure 11. Private network coverage and signal propagation on the third floor.

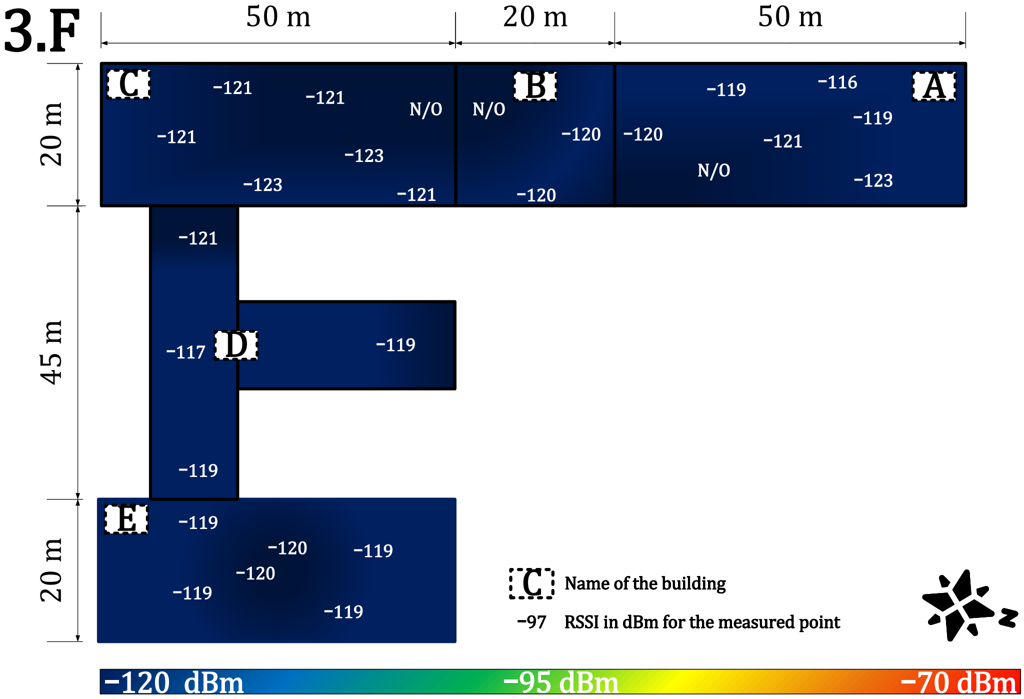


Figure 12. Public network coverage and signal propagation on the third floor.

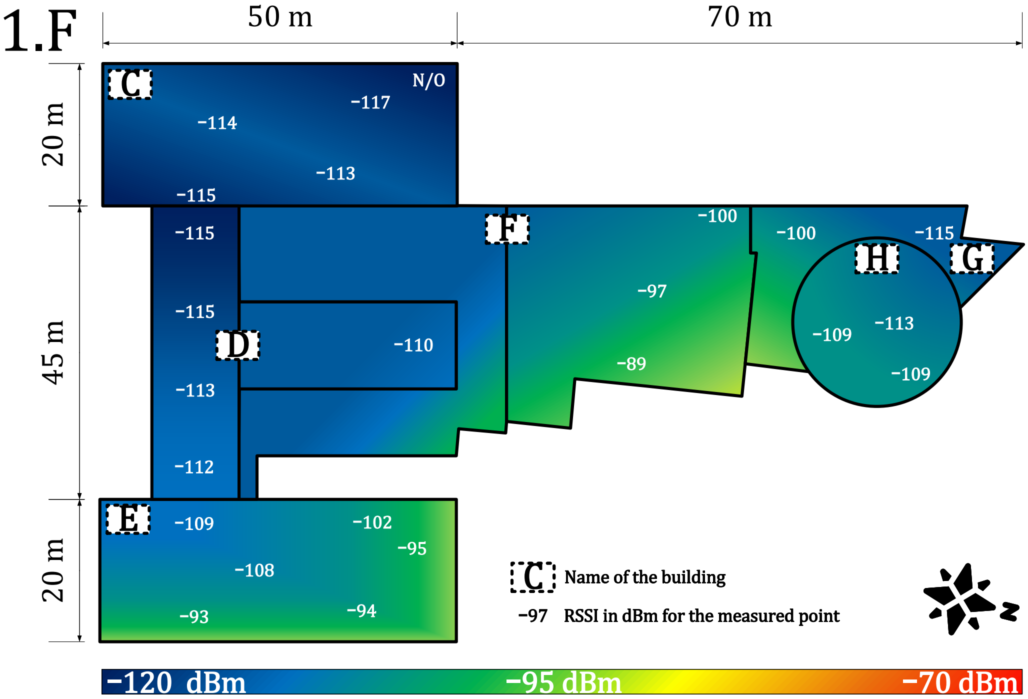


Figure 13. Private network coverage and signal propagation on the first floor.

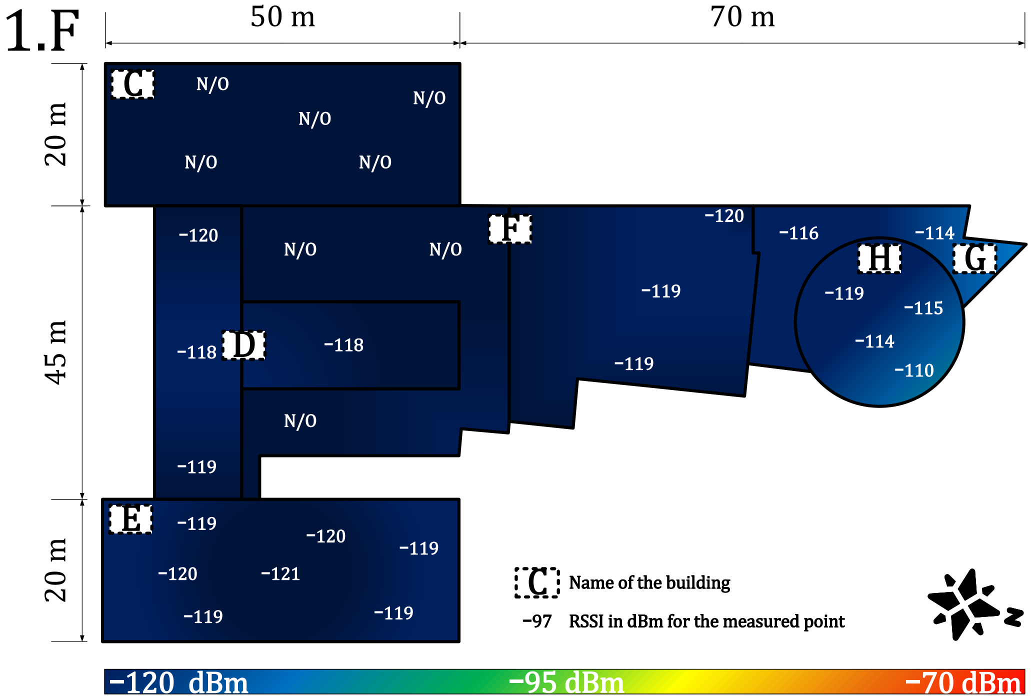


Figure 14. Public network coverage and signal propagation on the first floor.

The presented results illustratively demonstrate the specifics of the public network's coverage. The deep middle of the buildings is mostly poorly covered, while the edges feature a higher RSSI benefiting from multiple gateways located around. Meanwhile, our results show that it is possible to cover the whole complex by one single private gateway. For use cases with a higher number of end-nodes, the multiple-gateway solution should be used, i.e., we could add another gateway to the building A or C to improve the network parameters. This shows another advantage of the private network. We can add more gateways to boost the performance where and when needed. Unfortunately, this level of flexibility is hard to achieve when being served by a public network.

4.2. Security Evaluation

This section reports the comprehensive security analysis of LoRaWAN and names several benefits of private LoRaWAN deployments. We focus on the basics of security properties and vulnerabilities, and we also mention several improvements in related works. Notably, we analyze how LoRaWAN specification 1.1 (released in October 2017) and the most recent specification 1.0.4(2020) address the security issues present in the previous specification (1.0).

The following LoRaWAN specifications are currently available: 1.0 (2015 [65]), 1.0.1 (2016 [66]), 1.0.2 (2016 [67]), 1.1 (2017 [10]), 1.0.3 (2018 [68]), and 1.0.4 (2020 [69]).

Version 1.0.1 brings many corrections and clarifications to the definitions of the previous specification. Version 1.0.2 separates regional parameters from the link-layer specification. Subsequently, version 1.1 was released, which addresses additional roaming features and security improvements. Consequently, since the industry did not move to version 1.1 and is still building the 1.0 series of infrastructure and products, the LoRa Alliance has created version 1.0.4, which is currently the latest version of the 1.0 series, into which some features from 1.1 are imported. From a security perspective, versions 1.0.1, 1.0.2, and 1.0.3 are almost identical. This is worth noting that since the public networks have been (i) deployed earlier, and (ii) have to host the older sensors, they often base on the older versions of LoRaWAN specification.

The LoRaWAN security design is mainly based on symmetric cryptography. The specifications 1.0 [65] to 1.0.3 [68] define the following main security procedures:

Key establishment: The LoRaWAN specification 1.0 offers two approaches to establish keys. The first approach is the OTAA (join procedure). The end-device and the NS (or a JS) generate the AppSKey and NwkSKey keys from the same preshared AppKey. The second approach is the ABP activation. The device address (DevAddr), network session key (NwkSKey), and application session key (AppSKey) parameters are configured at production time. OTAA is considered more secure than ABP, but it still has several security issues.

Authentication: Each node has a 64-bit globally unique identifier called device identifier (DevEUI) and a unique 128-bit AES key (called AppKey) that are set by vendors or application providers. The application identifier (AppEUI) uniquely identifies the application. The OTAA proves that both the end-device and the NS (or a JS) have the knowledge of the preshared AppKey key. The end-device sends the join request message with AppEUI, DevEUI, and DevNonce and adds the message integrity code (MIC) computed by AppKey. The NS checks the MIC and generates keys for data encryption and data integrity. The server responds to the end-device by the join accept message with the MIC. The mutual authentication is ensured by the knowledge of the AppKey on both sides.

Key update: Session keys can be updated several times, but the preshared master key AppKey cannot be updated.

Encryption: Data encryption is ensured by the 128-bit AES encryption in the CTR mode. Application payloads are encrypted by the end-to-end shared key AppSKey, which is known only to the end-device and the AS. Nevertheless, the NS also knows the AppSKey and can decrypt the messages. Therefore, the NS has to be trustworthy.

Data integrity: Data integrity is ensured by the 32-bit message integrity code (MIC) produced by the CMAC function using the 128-bit AES encryption. The 4-byte MIC is calculated from a MAC payload and the NwkSKey key shared between the NS and the end-device. This code is added after the MAC payload. To avoid a packet replay attack, a frame counter is used (16 bits). However, the payload could be flipped due to the AES-CTR mode not providing data authentication.

4.2.1. Vulnerabilities

There are several imperfections and security issues of the LoRaWAN technology (specification 1.0.x):

- The preshared key AppKey cannot be updated. The key update problem is discussed in [70].
- The keys are persistently stored on a LoRaWAN device and could be subject to physical attacks. Using a tamper-resistant storage (i.e., secure element, HSM) improves the security of the stored key, but it also increases the costs.
- The paper [71] demonstrates that LoRaWAN transmissions are prone to jamming attacks.
- The paper [72] shows that the OTAA approach enables attackers to conduct a replay attack.
- The operator's NS knows the application keys and can decrypt the end-to-end communication, as noted in [73] (fixed in 1.0.4).
- The paper [74] shows potential vulnerabilities to denial of service (DoS) attacks during the join procedure.

4.2.2. The State-of-the-Art Improvements

In the following, we analyze the recent works and improvements to the LoRaWAN security approaches.

Kim and Song [70] propose a dual key-based activation scheme. Their proposal resolves the problem of key updates by using a dual key setup. Keys, that users share with the NS and the AS, are recomputed from previous keys and nonces by the AES encryption function. The proposal addresses such security requirements as authentication, message integrity, data confidentiality, and replay attack prevention. End node authentication is achieved by using the shared key with the NS and checking the CMAC value in the join phase.

The public key infrastructure of LoRaWAN has several security issues related to key management and the join phase. For example, the paper [72] demonstrates that attackers may misuse the OTAA for a replay attack. The paper presents this attack and offers the countermeasure by adding a masking token. Kim and Song [73] present a secure D2D link establishment scheme that consists of the SecureD2DReq, and SecureD2DAns messages exchanged between end nodes and the NS. The NS delivers security parameters to both nodes, so that both D2D nodes can securely establish cryptographic keys for protecting the D2D communication. A minor disadvantage is that the NS knows the encryption keys that are used between the nodes. In consequence, the NS has to be a trusted party. The work [75] presents a reputation system in order to select trustworthy nodes as proxies that are involved in the key derivation phase in order to improve the key robustness.

4.2.3. Security Improvements in LoRaWAN ™ 1.1 Specification

The specification 1.1 [10] released in 2017 and LoRaWAN™ Backend Interfaces 1.0 Specification [17] enhance the security in several ways and reflect many security issues discovered in the previous version of LoRaWAN standard. The security improvements and differences are as follows:

Key establishment: The LoRaWAN specification 1.1 offers a preshared symmetric key approach and OTAA and ABP procedures to derive session keys. However, LoRaWAN 1.1 adds another AES-128 root key, called NwkKey, which is used to derive the FNwkSIntKey, SNwkSIntKey, and NwkSEncKey session keys. This key may be shared with a network operator in order to manage the join procedure and to derive network session keys. The other root key, AppKey, is used for the derivation of the AppSKey session key. The security improvement is that users do not need to share AppKey with the network operator. AppKey and the derived AppSKey can be used solely for end-to-end encryption. Nevertheless, the devices (defined by LoraWAN 1.1) that communicate with NS (defined by LoraWAN 1.0.x) must only use NwkKey to derive all keys in order to preserve backward compatibility. Using the security elements and HSM to store the shared keys is still not possible.

Authentication: The version 1.1 improves OTAA (join procedure) by modifying JoinAccept MIC in order to prevent the replay attack. Further, all nonces are not random numbers but counters. Newly, OTAA is managed solely by the JS (not NS), which has to know both shared root keys. The mutual authentication is still based on the secrets shared between the devices and the JS. The knowledge of secrets is proved by computing and checking the CMAC functions (MIC).

Key update: Devices supporting LoRaWAN 1.1 can update session keys and reset counters by the rejoin procedure. The size of counters is increased from 16 bits to 32 bits. Nevertheless, the root keys (AppKey, NwkKey) cannot be updated as in 1.0 to 1.0.3.

Encryption: Data encryption is ensured by the 128-bit AES encryption in the counter with CBC-MAC (CCM) mode (not only CTR as in 1.0). Newly, the NS is not able to decrypt application data without AppSKey.

Data integrity: The version 1.1 defines the CCM authenticated encryption mode that provides data integrity. The data integrity of uplink frames is newly ensured by two CMAC functions with two keys (SNwkSIntKey, FNwkSIntKey). MIC is composed of 2B-cmacS and 2B-cmacF, but the length remains the same (4 B).

A comparison of the security aspects of both the LoRaWAN 1.0 standard and the new LoRaWAN 1.1 standard is displayed in Table 4.

The main improvement of the version 1.1 is in defining another key solely for the network level. This enables an enhancement of security for users and developers in public networks. In this way, users who do not use the operator's JS can encrypt data at the application layer without being worried about the operator listening. Nevertheless, some security associations between servers are still outside the scope of the LoRaWAN specifications.

Table 4. Differences in security parameters for LoRaWAN 1.0.x and LoRaWAN 1.1.x.

Security Procedure	LoRaWAN 1.0.x	LoRaWAN 1.1.x
Key establishment	OTAA/ABP	Added the second root key and enhanced key derivation
Authentication	64 b/128 b keys	Improved anti-replay technique
Key update	Only session key	Session key enhanced by the rejoin procedure
Encryption	AES_{CTR}-128	AES_{CCM}-128 and enhanced data confidentiality at the application layer
Data integrity	32 b MIC	Provided by AES-CCM (2CMAC functions)

Data obtained from the standard specification [9–58,65,67].

4.2.4. Security Improvements in LoRaWAN ™ 1.0.4 Specification

Version 1.0.4 brought several improvements from version 1.1. Specifically, the security procedures require the 32-bit frame counter size being stored in persistent memory, such as NVRAM, so that the value remains stored with the rest of the security context during the reboot for the ABP device. As a result, the counter value will not be reset, thus preventing possible threats, and the behavior of DevNonce was changed so that the DevNonce values of the device monotonically increase so that the work of a JS is much easier, and it is possible to monitor DevNonce to prevent replay attacks that are possible when using the same DevNonce.

4.2.5. Security Comparison of Private and Public Network

Due to several security imperfections in the public networks and basic specifications (mainly in 1.0 series), we assume that employing a private network may provide higher security than a public one under certain conditions. The main security benefit of using the private network is that keys are controlled and created by the end-users themselves. There is no possible danger caused by exposing encrypted data to a public operator. The specification 1.1 fixes this issue, but the problem remains if the operator employs the 1.0 series network server. Further, the developers can improve the security in their own private networks by adding security features and procedures presented in the state-of-the-art works, such as device-to-device encryption, reputation approaches, or by solving security associations between servers.

At the same time, the larger public networks have one benefit—they can offer higher availability benefiting from multiconnectivity and presence of multiple gateways, and thus are more resistant to some kinds of attack, such as replay and denial of service attacks. A private network topology with a low number of gateways can be overwhelmed by a large amount of malicious or repeated messages. In these situations, robust public networks could be more stable and reliable.

4.3. Deployment Ease Evaluation

This section contains two main parts: (1) costs evaluation, which provides a clear idea of the expected expenses for both public and private networks, and (2) methodology, which discusses the series of steps and operations for deploying the private or public network.

4.3.1. Deployment Costs Evaluation

This section briefly speculates on the costs of the private and the public network. However, an accurate analysis is strongly affected by the business practices and costs in each region and thus is beyond the scope of this paper. We include this analysis to support the evaluation of private and public networks; and to show the main differences in the nature of the costs they inquire. Moreover, this section might also serve for future estimation in specific use cases by application developers.

The costs of technology and solution are based on two types of costs: (i) CAPEX (capital expenditures); and (ii) OPEX (operating expense). The list of items which form the CAPEX costs is displayed in Table 5. Together, these items make up the total CAPEX costs:

$$\begin{aligned}\sum C_{\text{capex}} &= C_{\text{prop}} + C_{\text{sus}} + C_{\text{bld}} + \\ &+ C_{\text{res}} + C_{\text{cap-oth}} - C_{\text{dis}} - C_{\text{sell}}.\end{aligned} \tag{2}$$

Table 5. The list of components of CAPEX costs.

Parameter	Description
C_{prop}	From the end-user perspective, in the case of public network, the propriety costs are mainly composed of the costs of the end-devices. However, the private networks must also include other costs, i.e., gateways, racks, cables, antennas, feeders, software customized solutions, and others. Moreover, the costs for network optimization must include covering the places with a higher noise level (for an estimation of a precise simulation model needs to be made). If a larger private network is considered, it might also be necessary to include core infrastructure building costs if needed.
C_{sus}	Sustainability needs to be included if the horizon of the considered application is beyond the device's lifetime (i.e., devices with a 15-year lifetime will be used in applications with a horizon of 30 years).
C_{bld}	If a large-scale private network is considered, there might also be additive costs for renting roofs or buildings for gateways. However, this item considers only the buying price for the buildings, where the fees (if any) are included in the similar item for the OPEX costs.
C_{res}	The LoRaWAN technology is still quite new on the market, and most of the end-devices are of basic character. More specific applications could require research of the end-devices, which will also impact the final CAPEX costs.
$C_{\text{cap-oth}}$	There might be other additional costs not mentioned above, i.e., high-level design (HLD), low-level design (LLD), detailed-level design (DLD), installation and deployment costs, device configuration, supplies or network optimization costs (work).
C_{dis}	There will be a certain discount on the price of the devices (item C_{prop}) based on the seller and amount of devices.
C_{sell}	If the time difference between the application horizon and the device lifetime is >0, there is a possibility of selling the network equipment, which slightly lowers the CAPEX costs (i.e., the devices with a 15-year lifetime will be used in an application with a horizon of 5 years).

The CAPEX of a private network highly depends on the size of the network. Based on our experiences, the CAPEX costs of private network are considered to be higher than public network costs due to the high C_{prop} and $C_{\text{cap-oth}}$.

The list of items which form the OPEX is displayed in Table 6.

Together these items result in the total OPEX costs:

$$\begin{aligned}\sum C_{\text{opex}} = t \cdot (C_{\text{fee}} + C_{\text{enr}} + C_{\text{rent1}} + \\ + C_{\text{rent2}} + C_{\text{ope-oth}}),\end{aligned} \tag{3}$$

where t is the application horizon in years. The OPEX of both networks highly depends on the size of the network. Moreover, the OPEX costs of a private network are considered to be lower than the public network costs, because most of the applications, such as smart grid, smart city, smart home, and others, are considered to be included in the functional user's infrastructure without any need to build new ones. However, the OPEX costs of the private network will markedly increase if no infrastructure is provided.

Table 6. The list of items constituting OPEX.

Parameter	Description
C_{fee}	In the public network, there will be regular fees based on the number of devices and the number of messages. Though the private network has no device or message fees, the fee for the back-end (LoRaWAN server) needs to be considered. Moreover, the gateways need to be connected via a transport technology such as cellular or Ethernet. For this reason, there might be additional costs for transport services (connecting the gateways). Further, this item also includes regular fees such as software licenses, software updates, and paid support.
C_{enr}	The price for energy consumption. The public network mostly contains only end-devices which are often powered by batteries (devices powered by power network should be included here). However, the private network's energy consumption costs must include the cooling system energy costs as well as main servers, gateways, and other devices used for the LoRaWAN infrastructure. Moreover, this part should also include battery exchange, which occurs in the use cases with a higher frequency of messages, where batteries last only several years.
C_{rent1}	These are the rents for roofs or pillars for antennas, which are necessary in the private networks (large-scale private applications only).
C_{rent2}	Second renting part, where rented parts of the infrastructure might be included (again, mostly in the large-scale private applications only).
$C_{\text{ope-oth}}$	Other operational costs such as material costs, insurance, surveillance, training, taxes, salaries, depreciation, and others.

Note: All the costs must be computed for one whole year.

The whole costs of the application might be computed as follows:

$$\sum C = C_{\text{capex}} + C_{\text{opex}}. \tag{4}$$

4.3.2. Methodology of Deployment

The public and the private network should follow a certain methodology for deployment. However, our experiences show that these methodologies slightly differ from each other. This chapter introduces a summary of deployment methodology for both private and public networks based on our best practice.

- **Decision- making**

1. Estimate the size of the network (geographic area, number of gateways for a private case, number of nodes, density of nodes), desired service parameters (availability, throughput, type of communication, latency, communication frequency), and desired additional services (such as localization service presence).
2. Determine the possible future growth of the network or the network requirements. In addition, determine the possible future growth of the environment (i.e., new shopping areas, industrial complexes, and other noise-generating elements).
3. Analyze the feasibility of handling these requirements and future needs by LoRaWAN accounting for frequency regulations and technology limitations (check the availability of desired devices for the selected application). Decide whether the LoRaWAN technology is suitable for the selected use case. If possible, make a cost-efficiency analysis for LoRaWAN and other technologies (include the cost of development if end-devices are not available).
4. Use tester device(s) to characterize the signal quality of the public service from the most remote and difficult points (ask for an exact frequency plan of the network service provider). Discuss the possibilities of service-level agreement (SLA) with the public operator. Based on the results, selected parameters, and cost-efficiency, decide whether to go for either the private or the public network.

- **Private Network**

1. Estimation of the network coverage should be computed via simulation tools, i.e., Radio Mobile. This software uses the Irregular Terrain Model (ITS) based on the Longley–Rice model, which is a method for predicting the attenuation of radio signals for a telecommunication link in the frequency range of 20 MHz to 20 GHz. Based on the results, the position of the gateways should be established with reference to the simulation and also the node density. However, the best position may not be always available, and the location of already owned infrastructure should also be considered).
2. Make a noise analysis and select a frequency plan. Deploy the gateways based on the estimated plan.
3. Select power levels and data rates (if adaptive data rate is not in use) for the nodes. Use the tester device to characterize the quality of the signal from the most remote and difficult points.
4. Optimize the network by replacing or adding gateways and device antennas.
5. Deploy the first devices and test the long-term parameters of the network by monitoring the main parameters, i.e., availability and latency.
6. Scale the network up by continuously monitoring the main metrics.
7. The network parameters will change continuously over time, and the network needs to be continuously optimized to preserve the required parameters.

- **Public Network**

1. To ensure the performance metrics, agree with the public operator on the parameters via SLA.
2. Select power levels and data rates (if adaptive data rate is not in use) for the nodes.
3. Deploy the first devices and test the long-term parameters of the network by monitoring the main parameters, i.e., availability or latency.
4. Scale the network up by continuously monitoring the main parameters
5. The network parameters will change continuously over time, and it is necessary to continuously control the SLA from the operator.

4.4. Results Discussion

The private approach has a slight advantage over the public approach, because of the possibility of customizing the frequency plan and many other variables. Moreover, our results show a clear advantage of the private network's performance for an end-user, whose devices are located in a reasonably small geographical area, with respect to coverage (indoor), signal strength, signal propagation, or loss rate. However, the private network will need to increase the number of gateways to provide sufficient communication performance for an increased number of devices or for mobile devices. We provided a methodology for estimating the expenses which impact both of the LoRaWAN approaches. However, these need to be brought into a real-case context. Meanwhile, security-wise, the private approach offers, again, a slight advantage and a higher level of security, mostly thanks to the private key management without a third party and the possibility of improving the internal security mechanisms.

5. Conclusions and Future Work

This article clarifies the differences between the private and the public deployments of the LoRaWAN technology by providing theoretical and experimental results. We expect that both types of LoRaWAN deployments will need to face the inevitable issues of growing of the background noise level caused by the increasing number of devices in the unlicensed band. The results presented in this study demonstrate the importance of frequency resource usage optimization.

The number of the gateways and their optimization in the context of both private and public network is another issue of the utmost importance, requiring further research. Notably, in the current study we focused on the uplink-only traffic, which is specific for sensor devices. Meanwhile, the downlink traffic (relevant, e.g., for actuator devices) introduces a number of novel challenges and optimization dimensions, which can also affect the interplay between public and private deployments. One of the notable issues here is the half-duplex nature of many commercial gateways and uplink–downlink interference.

In addition, in the paper, we approached and discussed the security aspects and cost structures for both private and public networks. We identified the different trade-offs between the parameters and performance metrics, and showed that under particular implications either of the approaches may outperform its counterpart. This justifies the need for further research to enable development of more accurate and easy-to-use models, which can be used to plan and assess the deployment of LoRaWAN networks. This is the challenge we aim to approach in our further studies.

Author Contributions: Conceptualization, R.F., K.M., J.P., A.P. and J.M.; methodology, R.F. and K.M.; software, R.F.; validation, R.F., K.M., J.P., A.P. and J.M.; formal analysis, R.F., K.M., J.P., A.P. and J.M.; investigation, R.F., K.M., J.P., A.P. and J.M.; resources, R.F., K.M. and J.P.; data curation, R.F., K.M., J.P., A.P. and J.M.; writing—original draft preparation, R.F., K.M., J.P., A.P. and J.M.; writing—review and editing, R.F., K.M., J.P., A.P. and J.M.; visualization, R.F., K.M., J.P., A.P. and J.M.; supervision, J.M.; project administration, R.F.; funding acquisition, R.F. and J.M. All authors have read and agreed to the published version of the manuscript.

Funding: The research of this paper is a part of the project no. TK02030013 funded by Technology Agency of the Czech Republic. The research of K. Mikhaylov has been supported by the Academy of Finland 6Genesis Flagship (decision 318927), MRAT-SafeDrone (decision 341111) and RoboMesh (decision 336060) projects.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are available on demand via corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Le, N.T.; Hossain, M.A.; Islam, A.; Kim, D.; Choi, Y.; Jang, Y.M. Survey of Promising Technologies for 5G Networks. *Mob. Inf. Syst.* **2016**, *2016*, 2676589. https://doi.org/10.1155/2016/2676589.
2. IoT Connections Outlook, Broadband IoT Set to Overtake 2G and 3G. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook (accessed on 8 February 2022).
3. Chen, X.Y.; Jin, Z.G. Research on Key Technology and Applications for Internet of Things. *Phys. Procedia* **2012**, *33*, 561–566.
4. Goudos, S.K.; Dallas, P.I.; Chatziefthymiou, S.; Kyriazakos, S. A Survey of IoT Key Enabling and Future Technologies: 5G, Mobile IoT, Sematic Web and Applications. *Wirel. Pers. Commun.* **2017**, *97*, 1645–1675.
5. Poorter, E.D.; Hoebeke, J.; Strobbe, M.; Moerman, I.; Latré, S.; Weyn, M.; Lannoo, B. Sub-GHz LPWAN Network Coexistence, Management and Virtualization: An Overview and Open Research Challenges. *Wirel. Pers. Commun.* **2017**, *95*, 187–213.
6. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67.
7. Goursaud, C.; Gorce, J. Dedicated networks for IoT: PHY/MAC state of the art and challenges. *EAI Endorsed Trans. Internet Things* **2015**, *15*, 1–11.
8. Yang, W.; Wang, M.; Zhang, J.; Zou, J.; Hua, M.; Xia, T.; You, X. Narrowband Wireless Access for Low-Power Massive Internet of Things: A Bandwidth Perspective. *IEEE Wirel. Commun.* **2017**, *24*, 138–145.
9. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melià-Saguí, J.; Watteyne, I.T. Understanding the limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40.
10. LoRa Alliance. *LoRaWAN™ 1.1 Specification*; Technical Specification; [Final Release, October]; 2017. Available online: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 (accessed on 8 February 2022).
11. Therdpong, D.; Pana, U. WUTTIDITTACHOTTI, Pongpisit. A Study of 5G Network Performance: A Pilot Field Trial at the Main Skytrain Stations in Bangkok. In Proceedings of the 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST), Yogyakarta, Indonesia, 29–30 June 2021; pp. 191–195.
12. Gbadamosi, S.A.; Hancke, G.P.; Abu-Mahfouz, A.M. Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks. *IEEE Access* **2020**, *8*, 188641–188672. http://dx.doi.org/10.1109/ACCESS.2020.3030653.
13. Sinha, R.S.; Wei, Y.; Hwang, S.-H. A survey on LPWA technology: Lora and Nb-IOT. *ICT Express* **2017**, *3*, 14–21.

14. AlarmNet. Network Overview. Technical Report, 2005. Available online: http://library.ademconet.com/MWT/fs2/7810IR/AlarmNet-network-overview.pdf (accessed on 8 February 2022).
15. Seller, O.B.A.; Sornin, N. Low Power Long Range Transmitter. E.U. Patent EP 2763321 A1, 5 February 2013.
16. Hornbuckle, C.A. Fractional-N synthesized chirp generator. U.S. Patent US 7791415 B2, 18 May 2007.
17. LoRa Alliance. *LoRaWAN™ Backend Interfaces 1.0 Specification*; Technical Specification; [Final Release, October]; 2017. Available online: https://lora-alliance.org/wp-content/uploads/2020/11/lorawantm-backend-interfaces-v1.0.pdf (accessed on 8 February 2022).
18. Pekar, A.; Mocnej, J.; Seah, W.K.; Zolotova, I. Application domain-based overview of IOT network traffic characteristics. *ACM Comput. Surv.* **2021**, *53*, 1–33.
19. Osorio, A.; Calle, M.; Soto, J.D.; Candelo-Becerra, J.E. Routing in LoRaWAN: Overview and Challenges. *IEEE Commun. Mag.* **2020**, *58*, 72–76. https://doi.org/10.1109/MCOM.001.2000053.
20. Haxhibeqiri, J.; Poorter, E.D.; Moerman, I.; Hoebeke, J. A survey of Lorawan for IOT: From technology to application. *Sensors* **2018**, *18*, 3995.
21. Citoni, B.; Fioranelli, F.; Imran, M.A.; Abbasi, Q.H. Internet of Things and LoRaWAN-Enabled Future Smart Farming. *IEEE Internet Things Mag.* **2019**, *2*, 14–19. https://doi.org/10.1109/IOTM.0001.1900043.
22. Pinto-Erazo, A.M.; Suárez-Zambrano, L.E.; Mediavilla-Valverde, M.M.; Andrade-Guevara, R.E. Introductory analysis of Lora/Lorawan Technology in Ecuador. *Commun. Smart Technol. Innov. Soc.* **2021**, 547–557. https://doi.org/10.1007/978-981-16-4126-8_49.
23. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7.
24. Kajati, E.; Papcun, P.; Liu, C.; Zhong, R.Y.; Koziorek, J.; Zolotova, I. Cloud based cyber-physical systems: Network Evaluation Study. *Adv. Eng. Inf.* **2019**, *42*, 100988.
25. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.-P.; Chehab, A. Lorawan security survey: Issues, threats and possible mitigation techniques. *Internet Things* **2020**, *12*, 100303.
26. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873.
27. Andreev, S.; Galinina, O.; Pyateav, 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.
28. Knyazev, N.S.; Chechetkin, V.A.; Letavin, D.A. Comparative analysis of standards for Low-power Wide-area Network. In Proceedings of the 2017 IEEE Systems of Signal Synchronization, Generating and Processing in Telecommunications, Kazan, Russia, 3–4 July 2017; pp. 1–4.
29. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035.
30. Silva, J.C.; Rodrigues, J.J.P.C.; Alberti, A.M.; Solic, P.; Aquino, A.L.L. LoRaWAN-A Low Power WAN Protocol for Internet of Things: A Review and Opportunities. In Proceedings of the 2017 2nd International Multidisciplinary Conference on Computer and Energy Science, Split, Croatia, 12–14 July 2017; pp. 1–6.
31. CEPT-Electronic Communications Committee. *Recommendation 70–03 Relating to the Use of Short Range Devices (SRD)*; Technical Recommendation/Regulation; Denmark, Copenhagen [Version from October 2017]; 2017. Available online: https://docdb.cept.org/download/25c41779-cd6e/Rec7003e.pdf (accessed on 8 February 2022).
32. Vangelista, L.; Zanella, A.; Zorzi, M. Long-range IoT technologies: The dawn of LoRa™. In *Proceedings of the Future Access Enablers for Ubiquitous and Intelligent Infrastructures, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Atanasovski V., Leon-Garcia A., Eds.; Springer: Cham, Switzerland, 2015; Volume 159, pp. 51–58.
33. Bardyn, J.; Melly, T.; Seller, O.; Sornin, N. IoT: The era of LPWAN is starting now. In Proceedings of the 2016 IEEE 42nd European Solid-State Circuits Conference, Lausanne, Switzerland, 12–15 September 2016; pp. 25–30.
34. Semtech Corporation. AN1200.22: LoRa™ Modulation Basics. Application note. 2015 [Revision 2, May]. Available online: https://www.frugalprototype.com/wp-content/uploads/2016/08/an1200.22.pdf (accessed on 8 February 2022).
35. Vejlgaard, B.; Lauridsen, M.; Nguyen, H.C.; Mogensen, I.K.P.E.; Søreosen, M. Coverage and Capacity Analysis of Sigfox, LoRa, GPRS, and NB-IoT. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference, Sydney, NSW, Australia, 4–7 June 2017; pp. 1–5.
36. Seye, M.R.; Gueye, B.; Diallo, M. An evaluation of LoRa coverage in Dakar Peninsula. In Proceedings of the 2017 IEEE 8th Annual Information Technology, Electronics and Mobile Communication Conference, Vancouver, BC, Canada, 3–5 October 2017; pp. 478–482.
37. Petajajarvi, J.; Mikhaylov, K.; Roivainen, A.; Hanninen, T.; Pettissalo, M. On the Coverage of LPWANs: Range Evaluation and Channel Attenuation Model for LoRa Technology. In Proceedings of the 2015 IEEE 14th International conference on ITS Telecommunications, Copenhagen, Denmark, 2–4 December 2015; pp. 1–6.
38. Aref, M.; Sikora, A. Free space measurements with Semtech LoRa technology. In Proceedings of the 2014 IEEE 2nd Inernational Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Odessa, UKraine, 11–12 September 2014; pp. 19–23.

39. Barriquello, C.H.; Bernardon, D.P.; Canha, L.N.; Silva, F.E.S.; Porto, D.S.; Ramos, M.J.S. Performance assessment of a low power wide area network in rural smart grids. In Proceedings of the 2017 IEEE 52nd International Universities Power Engineering Conference, Heraklion, Greece, 28–31 August 2017; pp. 1–4.
40. Casals, L.; Mir, B.; Vidal, R.; Gomez, C. Modeling the energy performance of LoRaWAN. *Sensors* **2017**, *17*, 2364.
41. Lauridsen, M.; Nguyen, H.; Vejlgaard, B.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M. Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² Area. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference, Sydney, NSW, Australia, 4–7 June 2017; pp. 1–5.
42. Petajajarvi, J.; Mikhaylov, K.; Pettissalo, M.; Janhunen, J.; Iinatti, J. Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1–21.
43. Patel, D.; Won, M. Experimental Study on Low Power Wide Area Networks (LPWAN) for Mobile Internet of Things. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference, Sydney, NSW, Australia, 4–7 June 2017; pp. 1–5.
44. Petrić, T.; Goessens, c.; Nuaymi, L.; Toutain, L.; Pelov, A. Measurements, performance and analysis of LoRa FABIAN, a real-world implementation of LPWAN. In Proceedings of the 2016 IEEE 27th Annual International Personal, Indoor, and Mobile Radio Communications, Valencia, Spain, 4–8 September 2016; pp. 1–7.
45. Almuhaya, M.A.; Jabbar, W.A.; Sulaiman, N.; Abdulmalek, S. A survey on Lorawan technology: Recent trends, opportunities, simulation tools and future directions. *Electronics* **2022**, *11*, 164.
46. Goldoni, E.; Savazzi, P.; Favalli, L.; Vizziello, A. Correlation between weather and signal strength in Lorawan Networks: An extensive dataset. *Comput. Netw.* **2022**, *202*, 108627.
47. Masek, P.; Stusek, M.; Svertoka, E.; Pospisil, J.; Burget, R.; Lohan, E.S.; Marghescu, I.; Hosek, J.; Ometov, A. Measurements of LoRaWAN Technology in Urban Scenarios: A Data Descriptor. *Data* **2021**, *6*, 62.
48. Centelles, R.P.; Freitag, F.; Meseguer, R.; Navarro, L. Beyond the Star of Stars: An Introduction to Multihop and Mesh for LoRa and LoRaWAN. *IEEE Pervasive Comput.* **2021**, *20*, 63–72. https://doi.org/10.1109/MPRV.2021.3063443.
49. Mocnej, J.; Pekar, A.; Seah, W.K.G.; Papcun, P.; Kajati, E.; Cupkova, D.; Koziorek, J.; Zolotova, I. Quality-enabled decentralized IOT architecture with efficient resources utilization. *Robot. Comput.-Integr. Manuf.* **2021**, *67*, 102001.
50. Leenders, G.; Callebaut, G.; Ottoy, G.; der Perre, L.V.; Strycker, L.D. Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT. *IEEE Commun. Mag.* **2021**, *59*, 98–104. https://doi.org/10.1109/MCOM.008.2100382.
51. Navarro-Ortiz, J.; Sendra, S.; Ameigeiras, P.; Lopez-Soler, J.M. Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 60–67. https://doi.org/10.1109/MCOM.2018.1700625.
52. Kulkarni, P.; Pradeep, B.; Raza, U.; Alsaedi, S.; Almadhaani, R. LoRaWAN in Licensed Access Spectrum? A Techno-Economic Perspective. *IEEE Internet Things Mag.* **2020**, *3*, 70–75. https://doi.org/10.1109/IOTM.0001.2000043.
53. Neumann, P.; Montavont, J.; Noële, T. Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study. In Proceedings of the 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications, New York, NY, USA, 17–19 October 2016; pp. 1–8.
54. Gregora, L.; Vojtech, L.; Neruda, M. Indoor signal propagation of LoRa technology. In Proceedings of the 2016 IEEE 17th International Conference on Mechatronics-Mechatronika, Prague, Czech Republic, 7–9 December 2016; pp. 1–4.
55. Haxhibeqiri, J.; Karaagac, A.; Abeele, F.V.; Joseph, W.; Moerman, I.; Hoebeke, J. LoRa indoor coverage and performance in an industrial environment: Case study. In Proceedings of the 2017 IEEE 22nd International Conference on Emerging Technologies and Factory Automation, Limassol, Cyprus, 12–15 September 2017; pp. 1–8.
56. Ayele, E.D.; Hakkenberg, C.; Meijers, J.P.; Zhang, K.; Meratnia, N.; Havinga, P.J.M. Performance analysis of LoRa radio for an indoor IoT applications. In Proceedings of the 2017 International Conference on Internet of Things for the Global Community, Funchal, Portugal, 10–13 July 2017; pp. 1–8.
57. Petajajarvi, J.; Mikhaylov, K.; Hamalainen, M.; Iinatti, J. Evaluation of LoRa LPWAN Technology for Indoor Remote Health and Wellbeing Monitoring. *Int. J. Wirel. Inf. Netw.* **2017**, *24*, 153–165.
58. Loriot, M.; Aljer, A.; Shahrour, I. Analysis of the use of LoRaWan technology in a Large-Scale Smart City Demonstrator. In Proceedings of the 2017 IEEE Sensors Networks Smart and Emerging Technologies, Beiriut, Lebanon, 12–14 September 2017; pp. 1–4.
59. Ferre, G. Collision and Packet Loss Analysis in a LoRaWAN Network. In Proceedings of the 2017 IEEE 25th European Signal Processing Conference, Kos, Greece, 28 August–2 September 2017; pp. 2586–2590.
60. Krupka, L.; Vojtech, L.; Neruda, M. The Issue of LPWAN Technology Coexistence in IoT Environment. In Proceedings of the 2016 IEEE 17th International Conference on Mechatronics-Mechatronika, Prague, Czech Republic, 7–9 December 2016; pp. 1–8.
61. Lauridsen, M.; Vejlgaard, B.; Kovacs, I.Z.; Nguyen, H.; Mogensen, P. Interference Measurements in the European 868 MHz ISM Band with Focus on LoRa and SigFox. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
62. Vejlgaard, B.; Lauridsen, M.; Nguyen, H.; Kovacs, I.Z.; Mogensen, P.; Sorensen, M. Interference Impact on Coverage and Capacity for Low Power Wide Area IoT Networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference, San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
63. Adeunis. Field Test Device: LoRaWAN Europe EU863-870. Technical Documentation (Version V1.2.1), 2017. Available online: https://www.adeunis.com/en/produit/ftd-868-915-2/ (accessed on 8 February 2022).

64. Korowajczuk, L. *LTE, WiMAX and WLAN Network Design, Optimization and Performance Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2011; pp. 187–190.
65. LoRa Alliance. *LoRaWAN™ 1.0 Specification*; Technical Specification; [Final Release, January]; 2015. Available online: https://lora-alliance.org/wp-content/uploads/2020/11/2015_-_lorawan_specification_1r0_611_1.pdf (accessed on 8 February 2022).
66. LoRa Alliance. LoRaWAN™ 1.0.1 Specification. Technical Specification; [Final Release, February]; 2016. Available online: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-1/ (accessed on 8 February 2022).
67. LoRa Alliance. LoRaWAN™ 1.0.2 Specification. Technical Specification; [Final Release, July]; 2016. Available online: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-2/ (accessed on 8 February 2022).
68. LoRa Alliance. LoRaWAN™ 1.0.3 Specification. Technical Specification; [Final Release, July]; 2018. Available online: https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-3/ (accessed on 8 February 2022).
69. LoRa Alliance. LoRaWAN™ 1.0.4 Specification. Technical Specification; [Final Release, October]; 2020. Available online: https://lora-alliance.org/resource_hub/lorawan-104-specification-package/ (accessed on 8 February 2022).
70. Kim, J.; Song, J.S. A Dual Key-Based Activation Scheme for Secure LoRaWAN. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 6590713.
71. Aras, E.; Ramachandran, G.S.; Lawrence, P.; Hughes, D. Exploring the Security Vulnerabilities of LoRa. In Proceedings of the 2017 IEEE 3rd International Conference on Cybernetics, Exeter, UK, 21–23 June 2017; pp. 1–6.
72. Na, S.J.; Shin, D.Y.H.W.S.; Kim, K. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 IEEE International Conference on Information Networking, Da Nang, Vietnam, 11–13 January 2017; pp. 718–720.
73. Kim, J.; Song, J. A Secure Device-to-Device Link Establishment Scheme for LoRaWAN. *IEEE Sens.* **2018**, *18*, 2153–2160.
74. Tomasin, S.; Zulian, S.; Vangelista, L. Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference Workshops, San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
75. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Enhancing the security of the IoT LoraWAN architecture. In Proceedings of the 2016 IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks, Paris, France, 22–25 November 2016; pp. 1–7.

sensors

MDPI

Article

Exploring LoRaWAN Traffic: In-Depth Analysis of IoT Network Communications

Ales Povalac [1,*], Jan Kral [1], Holger Arthaber [2], Ondrej Kolar [1] and Marek Novak [1]

[1] Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 61600 Brno, Czech Republic; jan.kral@vut.cz (J.K.); ondrej.kolar@vut.cz (O.K.); xnovak0m@vut.cz (M.N.)

[2] Institute of Electrodynamics, Microwave and Circuit Engineering, TU Wien, Gusshausstrasse 25/354, 1040 Vienna, Austria; holger.arthaber@tuwien.ac.at

* Correspondence: povalac@vut.cz

Abstract: In the past decade, Long-Range Wire-Area Network (LoRaWAN) has emerged as one of the most widely adopted Low Power Wide Area Network (LPWAN) standards. Significant efforts have been devoted to optimizing the operation of this network. However, research in this domain heavily relies on simulations and demands high-quality real-world traffic data. To address this need, we monitored and analyzed LoRaWAN traffic in four European cities, making the obtained data and post-processing scripts publicly available. For monitoring purposes, we developed an open-source sniffer capable of capturing all LoRaWAN communication within the EU868 band. Our analysis discovered significant issues in current LoRaWAN deployments, including violations of fundamental security principles, such as the use of default and exposed encryption keys, potential breaches of spectrum regulations including duty cycle violations, SyncWord issues, and misaligned Class-B beacons. This misalignment can render Class-B unusable, as the beacons cannot be validated. Furthermore, we enhanced Wireshark's LoRaWAN protocol dissector to accurately decode recorded traffic. Additionally, we proposed the passive reception of Class-B beacons as an alternative timebase source for devices operating within LoRaWAN coverage under the assumption that the issue of misaligned beacons can be addressed or mitigated in the future. The identified issues and the published dataset can serve as valuable resources for researchers simulating real-world traffic and for the LoRaWAN Alliance to enhance the standard to facilitate more reliable Class-B communication.

Keywords: IoT; LoRa; LoRaWAN; Class-B; dataset; network sniffer; traffic monitoring; time synchronization

check for updates

Citation: Povalac, A.; Kral, J.; Arthaber, H.; Kolar, O.; Novak, M. Exploring LoRaWAN Traffic: In-Depth Analysis of IoT Network Communications. *Sensors* **2023**, *23*, 7333. https://doi.org/10.3390/s23177333

Academic Editor: Gianluigi Ferrari

Received: 29 June 2023
Revised: 21 July 2023
Accepted: 17 August 2023
Published: 22 August 2023

1. Introduction

The Internet of Things (IoT) has revolutionized the way we interact with our environment, enabling a wide range of applications from smart cities to industrial automation. Low Power Wide Area Networks (LPWANs) have emerged as key technology for IoT, providing a balance between low power consumption and long-range communication.

Long-Range Wire-Area Network (LoRaWAN), a popular LPWAN technology, is based on the Long-Range (LoRa) physical layer and provides features such as adaptive data rates, bidirectional communication, and various device classes, making it suitable for different use cases. Given the limited Radio Frequency (RF) power of 25 mW, LoRaWAN facilitates a communication distance of up to 5 km in urban areas [1]. These diverse capabilities have led to widespread adoption across various industries, establishing it as a vital component in the growing IoT ecosystem [2,3].

The LoRa Physical (PHY) layer employs a unique modulation technique known as Chirp Spread Spectrum (CSS). CSS facilitates long-range communication and robustness against narrow-band interference by spreading the information signal over a wider bandwidth [4]. Above this, the LoRaWAN Medium Access Control (MAC) layer provides a standardized protocol for IoT devices [5].

LoRaWAN features three distinct device classes—A, B, and C—addressing different application requirements and power constraints [5]. Class-A devices offer the highest energy efficiency, suitable for applications with infrequent communication needs, with brief receive windows after each transmission. Class-B devices provide predictable downlink communication latency by synchronizing with network beacons and enabling scheduled receive slots, maintaining moderate power consumption. Class-C devices prioritize downlink latency over power efficiency, offering continuous receive windows for near real-time communication. End devices use a random access transmission method (ALOHA), which allows them communication without the need for pairing with a specific gateway.

Given the complexity and diverse operating conditions of LoRaWAN, it is essential to gain insight into its actual internal functionality in real deployments using tools for network communication analysis. To address this need, we developed a dedicated hardware sniffer—a specialized device designed to capture and decode wireless traffic. In the context of LoRaWAN, this sniffer can be used to collect a dataset and subsequently investigate various aspects of the network, such as signal strength, coverage, data rates, and communication protocols. These insights can help identify potential issues, evaluate network deployments, and optimize configurations for better performance. To provide the greatest flexibility in analyzing the recorded packets, we selected Wireshark—a widely recognized open-source network protocol analyzer.

Our research is guided by several key questions related to the dataset. Firstly, we aim to determine which information can be extracted from captured real-world traffic within a LoRaWAN network, with particular attention to downlink traffic and Class-B beacons. Furthermore, we investigate how Class-B beacons and their optional extensions are used in actual installations. It is also crucial to assess whether security and spectrum regulations are followed in current LoRaWAN deployments. Another key aspect of our research is to examine the accuracy and reliability of time synchronization in LoRaWAN, notably regarding the Class-B beacons, and their susceptibility to interference and misconfiguration. Finally, we explore the potential for new applications of Class-B beacons.

Contribution of This Work

We collected and analyzed a large dataset [6] of real-world LoRaWAN traffic from four European locations. Unlike previous datasets [7–10], our collection includes uplink, downlink, and Class-B traffic. In the Results and Discussion section, we present an analysis that encompasses the Class-B beacons and highlights potential issues of LoRaWAN deployments.

To obtain this dataset, we used a custom LoRaWAN hardware sniffer. Both the hardware and software sources of this device are available online [11]. Recognizing the outdated LoRaWAN protocol support in Wireshark, we enhanced its capabilities for decoding real-world traffic. These improvements are incorporated into the Wireshark development branch and are now publicly accessible.

Furthermore, we proposed an innovative approach of using Class-B beacons as a timebase source in urban environments. This method offers several advantages over alternative time sources such as Global Navigation Satellite System (GNSS), DCF77, and Network Time Protocol (NTP), including better indoor reception, smaller and more cost-effective antennas, and independence from internet connectivity.

Hence, the main contributions of this work are as follows:

- it describes a novel LoRaWAN sniffer with open hardware design files and software framework that allows capturing all LoRaWAN traffic and its examination in Wireshark;
- it provides a large public dataset with real-world traffic captured in multiple locations;
- it analyzes the unencrypted part of captured packets, providing insights into network operators, end device manufacturers, and LoRaWAN feature support;
- it provides an analysis of Class-B beacons regarding precise timing and gateway localization;

- it points out to several identified issues, like invalid Class-B beacons, compromised encryption keys, and invalid LoRaWAN traffic;
- it proposes the novel use of Class-B beacons as a timebase source.

2. Related Research

The IoT research community recognizes the significance of real-world, quantitative data for studying the network environments and deployments. Several LoRaWAN datasets have been made available [7–10]. Bhatia et al. [7] gathered uplink packets from gateways in the dense urban environment of London (UK). They included packet header information and PHY layer properties reported by the gateways, making the dataset one of the largest and most extensive [12]. Aernouts et al. [8] collected data focused on fingerprint localization in Antwerp (Belgium). Their dataset contains a large volume of traces with known end device position.

Blenn et al. [9] presented an analysis of The Things Network (TTN), obtaining a dataset of packets through the TTN Application Programming Interface (API) using a known default network key. However, their findings were constrained to TTN uplink traffic due to its API limitations. Presently, the acquisition of such dataset is no longer feasible due to the evolution of the TTN backend.

Choi et al. [10] developed LoRadar, a passive packet monitoring tool, and conducted an analysis of traffic within an anonymized city-wide area. Their study closely resembles our research. However, they were limited to monitoring uplink sessions due to hardware constraints. To the best of our knowledge, no previous study has attempted to capture both uplink and downlink simultaneously.

An overview of the existing sniffers is provided in [13]. These sniffers are limited to a single RF channel [14] or employ one multichannel concentrator [9,10]. They are either based on a gateway (concentrator type) [9,10] or developed using the GNU radio (SDR-type) [15]. Software-Defined Radios (SDRs) were deemed unsuitable due to high Signal-to-Noise Ratio (SNR) requirements [15–17]. Recently, an SDR-based demodulator competitive in SNR requirements was made available [18]. However, it still demodulates one frequency and Spreading Factor (SF) per block, requiring over 100 differently configured LoRa demodulator blocks for the intended sniffer functionality, which is computationally demanding.

Other papers focus on simulating various LoRaWAN issues (overview in [19]) and the deployment of custom experimental setups (controlled environments of nodes and one or multiple gateways) [20,21]. Our work focuses on passive monitoring of real-world traffic, similar to [10], but also includes an important study of downlink messages and Class-B beacons.

Time synchronization in LoRaWAN has been analyzed in several studies, such as [22,23]. Ramirez et al. [22] achieved an excellent time error below 10 µs using a custom protocol in a Class-A network. Rizzi et al. [23] employed a posteriori synchronization, enabling time sync with an uncertainty in the order of tens of milliseconds. No studies have suggested passive listening to Class-B beacons for time synchronization.

3. Sniffer Design

The sniffer is based on commercially available modules, and its software is customized for capturing network traffic. It operates autonomously when connected to a power source, storing the collected records locally and simultaneously transmitting them to a server over the Long Term Evolution (LTE) modem.

To overcome the limitations of currently available devices, our new sniffer needs to capture all LoRaWAN traffic according to the EU868 frequency plan, including the RX2 channel [24]. This necessitates supporting both uplink and downlink reception, which differ in the chirp signal polarity at the physical LoRa layer. Additionally, we aimed to receive Class-B beacons transmitted on RX2 channel with a non-inverted chirp signal. The combinations of these parameters are summarized in Table 1.

Table 1. LoRaWAN EU868 frequency plan with possible combinations of LoRa parameters [24–26].

Transmission Kind	Frequency (MHz)	Spreading Factor	Uplink Signal Polarity	Downlink Signal Polarity
RX1 channel 1	$868.5 - 0.4 = 868.1$	SF7–SF12	non-inverted	inverted
RX1 channel 2	$868.5 - 0.2 = 868.3$	SF7–SF12	non-inverted	inverted
RX1 channel 3	868.5	SF7–SF12	non-inverted	inverted
RX1 channel 4	$867.5 - 0.4 = 867.1$	SF7–SF12	non-inverted	inverted
RX1 channel 5	$867.5 - 0.2 = 867.3$	SF7–SF12	non-inverted	inverted
RX1 channel 6	867.5	SF7–SF12	non-inverted	inverted
RX1 channel 7	$867.5 + 0.2 = 867.7$	SF7–SF12	non-inverted	inverted
RX1 channel 8	$867.5 + 0.4 = 867.9$	SF7–SF12	non-inverted	inverted
RX2	869.525	SF7–SF12 [1]	–	inverted
Class-B beacon [2]	869.525	SF9	–	non-inverted

[1] SF12 for the LoRaWAN standard, SF9 for The Things Network [26]. The sniffer supports all spreading factors.
[2] Class-B beacons use implicit header mode with specific settings [24].

The sniffer is based on the industry-standard IMST iC880A LoRaWAN concentrator [27], a hardware device designed for receiving and processing LoRa signals in LoRaWAN network gateways. The module is equipped with a Semtech SX1301 digital baseband chip [28] and two Semtech SX1257 RF front end chips [29], providing up to 10 programmable parallel demodulation paths. It supports multiple LoRaWAN channels in the 868 MHz frequency band, enabling the simultaneous reception of data from multiple end devices. Additionally, the module is also capable of performing time-stamping of incoming packets, which is essential for precise time synchronization.

The main baseband chip SX1301 provides eight LoRa demodulators with automatic SF selection on IF0–IF7 signal paths. Moreover, an additional LoRa demodulator with fixed parameters and implicit header mode support, referenced as a SingleSF modem, is available on the IF8 signal path.

There are several limitations introduced by the chipset. In the LoRa physical layer, the modulated signal is represented by a chirp, which is a sinusoidal waveform whose frequency increases or decreases linearly over time [4]. The SX1301 demodulator can only detect chirps with one of two different polarities, each representing its inverse. Each LoRa demodulator needs to know the polarity of a LoRa chirp signal in advance. As a result, at least two iC880A concentrator modules need to be used for a simultaneous reception of uplink and downlink transmission, each configured to demodulate a different chirp signal polarity (GW #1 and GW #2).

The IF0–IF7 LoRa channels may be connected individually to radio front ends, referenced as Radio A or Radio B [27,28]. However, the useful bandwidth of SX1257 radios is approximately only 925 kHz [30], assuming typical 125 kHz channels in the EU868 band [24]. This bandwidth is sufficient for the simultaneous reception of all RX1 channels using both front ends. Nevertheless, the RX2 channel operates at a significantly different frequency, making it impossible to receive using the typical configuration. This is not an issue for a standard concentrator, as it only transmits on RX2 without receiving. However, for a sniffer, complete data reception is desired. To overcome this limitation, a third iC880A concentrator must be added to the sniffer system (GW #3). This concentrator enables reception in the RX2 downlink with one of its eight LoRa demodulators. Figure 1 illustrates the relationship between channels, bands, and radio front ends.

Another goal of the sniffer is to receive Class-B beacons. These beacons are transmitted on the RX2 frequency with specific parameters involving the implicit LoRa header [24]. Demodulation of the header is supported by the SingleSF modem on the IF8 signal path. An implicit header refers to a packet format where the length of the packet is not explicitly included in the packet header. Instead, the packet length is assumed to be fixed and known in advance. This reception is handled by the third concentrator module (GW #3).

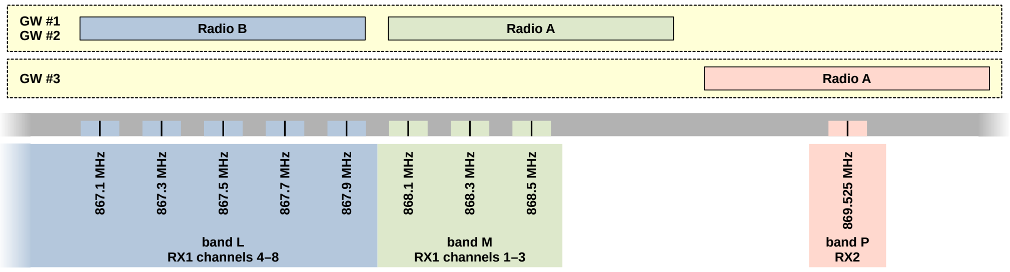


Figure 1. LoRaWAN EU868 channels and sniffer front ends.

3.1. Sniffer Hardware Overview

Figure 2 shows the block diagram of our LoRaWAN sniffer. Initially, the radio signal is received by an Ultra-High Frequency (UHF) omnidirectional antenna with a gain of 2 dBi and vertical polarization. This signal is subsequently filtered by a narrow bandpass filter, amplified by a Low Noise Amplifier (LNA), and then distributed to the inputs of three iC880A modules via a power splitter. Table 2 outlines the function of each iC880A module.

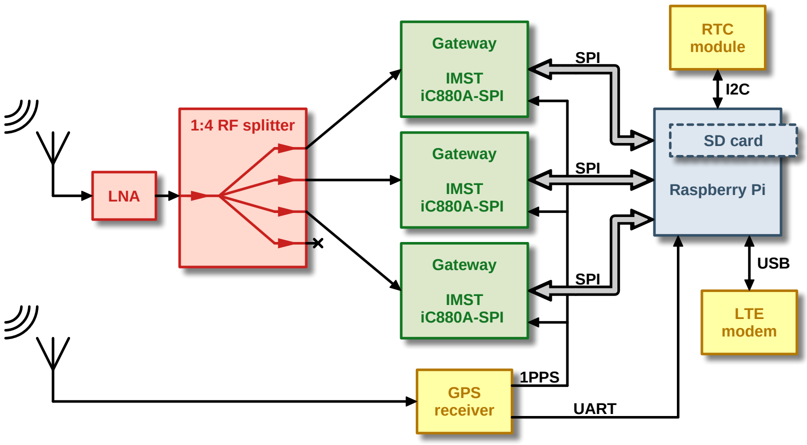


Figure 2. Block diagram of the developed LoRaWAN sniffer.

Table 2. Roles of iC880A modules in the LoRaWAN sniffer.

Concentrator	Receives on	IF0–IF7 Paths	IF8 Path
GW #1	RX1 channel 1–8	downlink	–
GW #2	RX1 channel 1–8	uplink	–
GW #3	RX2	downlink (IF0 only)	Class-B beacon

A Raspberry Pi minicomputer serves as the central processing unit, which communicates with the iC880A modules through its integrated Serial Peripheral Interfaces (SPIs). In addition, it obtains the current time from a GNSS receiver module for accurate timestamping of the received packets. For this purpose, a 1 pps signal is distributed from the GNSS module to all iC880A concentrators. The Raspberry Pi also has a Real Time Circuit (RTC) connected to its I^{2}C interface and an LTE modem connected via USB for remote management and sending the measured data to the server. An external 24 V adapter powers the whole device. Figure 3 shows the photo of the sniffer internal hardware. Complete schematics and hardware design files are available online [11].

From a mechanical perspective, the complete LoRaWAN sniffer is enclosed in an IP68-rated aluminum box, enabling safe outdoor installations. To accommodate the sniffer's requirement for GNSS-based time synchronization and LTE communication, an additional plastic container conceals the GNSS and LTE antennas, eliminating the need for waterproof external antennas. The two containers are securely bonded together and all openings are sealed to maintain watertight integrity.

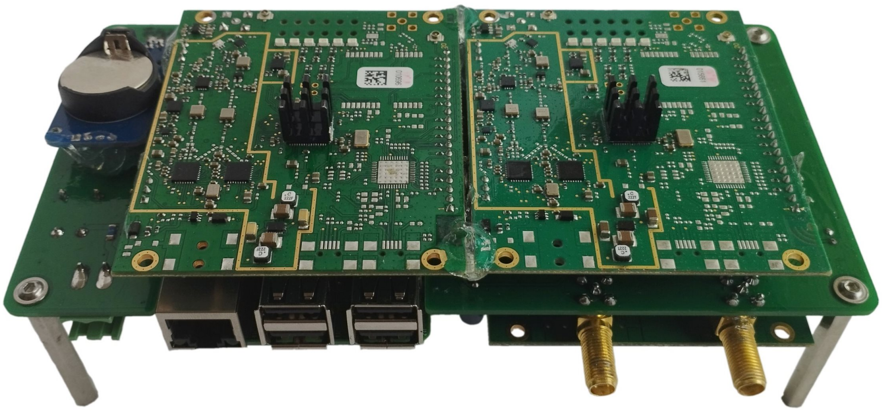


Figure 3. Photo of the LoRaWAN sniffer internal hardware.

3.2. Sniffer Software Overview

The software relies on adapted open-source utilities supplied by Semtech, specifically `libloragw` from the `lora_gateway` repository [30] and `lora_pkt_fwd` from the `packet_forwarder` repository [31]. The LoRa gateway library manages SPI communication between the host computer and the SX1301 baseband chip. The packet forwarder employs the gateway library to receive packets, incorporate detailed data, and transmit the packet via a standardized UDP socket.

It was necessary to add support for handling multiple SPIs, switching chirp signal polarity, receiving packets without a valid Cyclic Redundancy Check (CRC), and decoding the Class-B beacon implicit header. As a result, the packet forwarder was modified to parse configuration JavaScript Object Notation (JSON) files and pass the relevant settings to the library, enhancing its versatility and adaptability. The complete software framework is available online [11].

3.3. Data Processing

To address the limitations of original Wireshark LoRa encapsulation, we developed an updated version of the LoRaTap header to efficiently manage the additional PHY layer information, such as frequency channel, signal level, timestamp, and other relevant details [32]. The sniffer's JSON output produced by the packet forwarder utility can be converted to the `pcap` format by conversion utility [11].

We also significantly updated the Wireshark LoRaWAN dissector. Key enhancements include the addition of a LoRaWAN Class-B beacon dissector, *Join Accept* decryption, support for MAC commands from the LoRaWAN v1.0.4 specification [5], and various improvements to enable successful decoding of real-world traffic captured by the sniffer. These modifications are integrated into the development branch for future official release and are currently available through the Wireshark automated builds [33].

3.4. Analysis and Decryption

Subsequent data processing can be performed manually in Wireshark or through automated scripts in Wireshark's console version, TShark. We employed an automated approach for the quantitative analysis of captured packets. Data post-processing from the TShark utility is executed with Python scripts, while final statistical and visual processing is carried out in MATLAB. The scripts are available online [11].

LoRaWAN packets are usually partially encrypted, with the keys generally unknown to a sniffer device. However, there are several properties of LoRaWAN communication that can be analyzed without knowing the decryption keys. The following fields of a LoRaWAN packet are not encrypted:

- Message Header (MHDR): Contains information about the message type (MType) and LoRaWAN version.
- Device Address (DevAddr): A unique 32-bit identifier for the end device within a specific network.
- Frame Control (FCtrl): Contains information about the Adaptive Data Rate (ADR), Frame Options Length, and other control flags.
- Frame Counter (FCnt): A 16-bit counter value that increments with each uplink frame to prevent replay attacks.
- Frame Options (FOpts): Contains optional MAC commands.
- Frame Port (FPort): Indicates the port number for application-specific or MAC layer communication.

The application payload (FRMPayload) and Message Integrity Check (MIC) are encrypted for both uplink and downlink packets, requiring the corresponding keys for decryption and verification [5].

LoRaWAN activation processes include the Over-the-Air Activation (OTAA) and Activation By Personalization (ABP). OTAA involves an end device transmitting a *Join Request*, encrypted with a pre-shared Application Key (AppKey). The network server verifies the request, generates session keys, namely the Network Session Key (NwkSKey) for the MIC and the Application Session Key (AppSKey) for the payload, and responds with a *Join Accept* message, which includes the assigned Device Address (DevAddr). Given the necessary keys, Wireshark can decrypt the join process packets, allowing for a more comprehensive analysis.

ABP, on the other hand, involves pre-configuring the end device with session keys (NwkSKey and AppSKey) and a DevAddr, enabling immediate communication without a join procedure. While this approach simplifies the process, it may increase security risks due to prolonged use of the same keys.

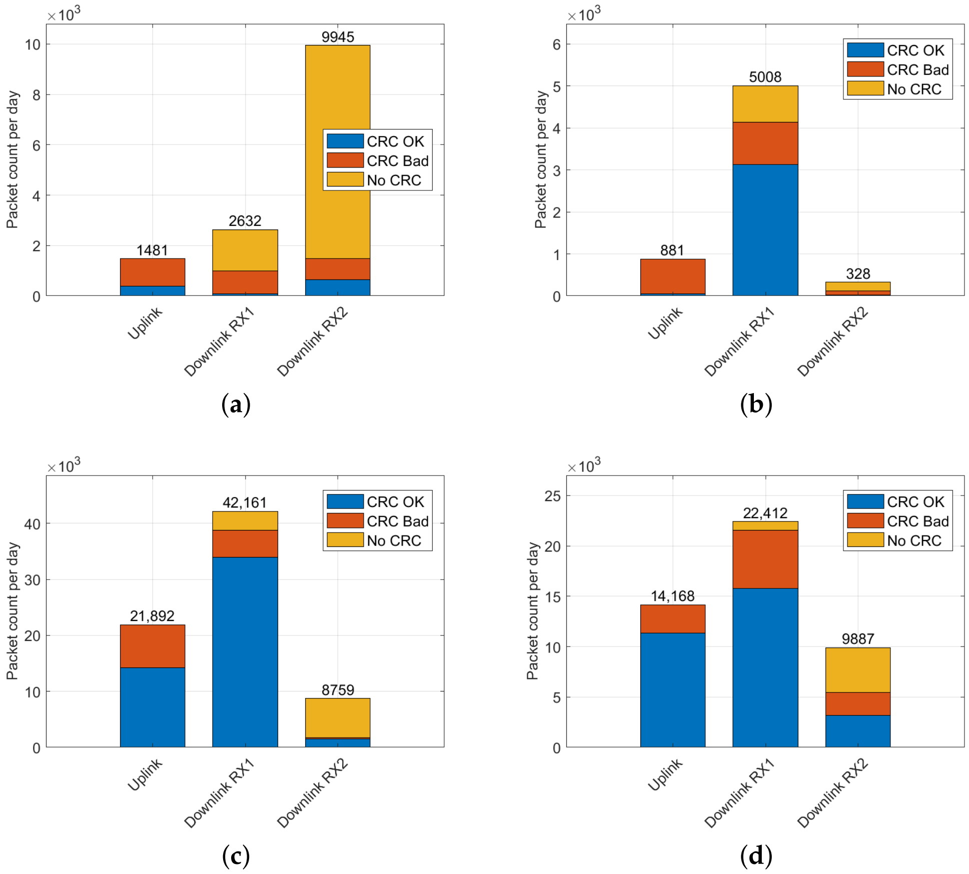
4. Results and Discussion

Data from the LoRaWAN networks were collected in four cities: Liege (Belgium), Graz (Austria), Vienna (Austria), and Brno (Czechia). These cities were chosen for data gathering due to various factors, such as their central European location, their prominence as major urban areas with well-established LoRaWAN networks, and the intention to capture a diverse range of city environments for data collection. Table 3 provides a summary of the characteristics and details associated with each capture.

Table 3. Dataset details.

Location	Geographic Coordinates	Sniffer Placement	Capture Interval	Days	Average Packets per Day	Valid LoRaWAN Packets per Day
Liege (Belgium)	50.66445° N 5.59276° E	Roof of a residential building in a suburb area; limited view.	25 August 2022– –19 September 2022	17.8	14,088	6609
Graz (Austria)	47.07049° N 15.44506° E	Enclosed balcony of a historical building in the city center; indoor.	26 October 2022– –29 November 2022	26.3	6225	3215
Vienna (Austria)	48.19666° N 16.37101° E	Roof of a university building in the city center; clear view.	1 December 2022– –4 January 2023	34.1	72,892	58,330
Brno (Czechia)	49.22685° N 16.57536° E	Roof of a university building in a suburb area; clear view.	16 February 2023– –30 March 2023	42.0	46,467	30,937

Ideal placement of the sniffer in Vienna and Brno is evident in the distribution of the number of packets received in uplink, downlink, and independent downlink (RX2), as depicted in Figure 4. To account for varying time periods across the datasets, packet counts in all histograms were normalized to display the number of packets per day.



(**a**) (**b**) (**c**) (**d**)

Figure 4. Distribution of LoRaWAN packets for individual receive chains for packets with valid, invalid, and missing CRC in: (**a**) Liege dataset; (**b**) Graz dataset; (**c**) Vienna dataset; (**d**) Brno dataset.

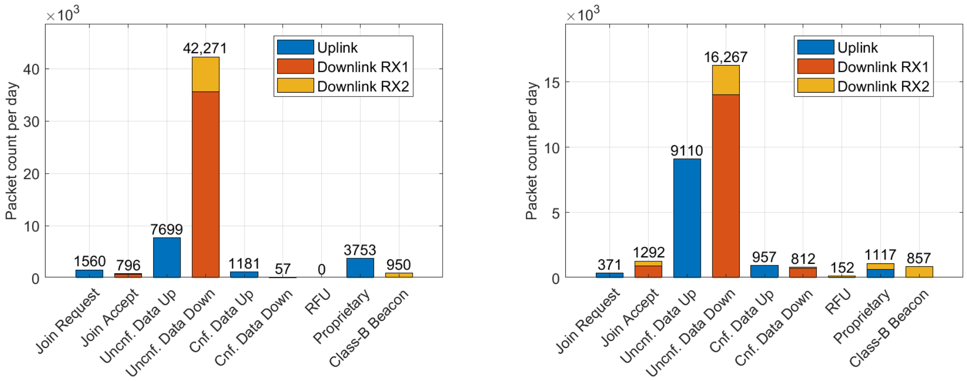
In Liege, the site is primarily characterized by the downlink traffic—unconfirmed data without a checksum, particularly on the RX2 channel. The Graz data also suggest a suboptimal sniffer placement, as the sniffer predominantly captured downlink signals from gateways (better positioned than nodes). Consequently, most of the received uplink traffic was discarded due to wrong checksums, as shown in Figure 4.

4.1. Selected Results of Data Post-Processing

Despite optimal sniffer placement in Vienna and Brno, a higher number of packets was received in the downlink compared to the uplink. The distribution of valid LoRaWAN message types is depicted in Figure 5. To determine the validity of real LoRaWAN messages, the CRC verification was applied at the physical LoRa packet level, and packet headers were checked for errors. Payload checksums were verified for the Class-B beacons.

Suboptimal placement in Liege and Graz resulted in the reception of predominantly downlink packets. Class-B beacons were observed in Brno, Liege, and Vienna. In some instances, particularly in Liege, these beacons also conveyed additional information regarding the geographic position of the gateway.

The Vienna dataset can be considered a representative source of data. The histograms in Figure 6 demonstrate the identified transmission parameters. Spreading factors SF7 and SF12 are dominant, with a coding rate of 4/5 required by the standard [24]. Channels are occupied almost uniformly (except for the 867.5 MHz frequency), and most packets are relatively short, with lengths of 12–19 bytes in the downlink and 20–40 bytes in the uplink. The Received Signal Strength Indicator (RSSI) and the SNR confirm the superior placement of gateways compared to nodes in terms of radio coverage.



(**a**) (**b**)

Figure 5. LoRaWAN message types: Join Request, Join Accept, Unconfirmed/Confirmed Data Up/Down, RFU, Proprietary, and Class-B Beacon in: (**a**) Vienna dataset; (**b**) Brno dataset.

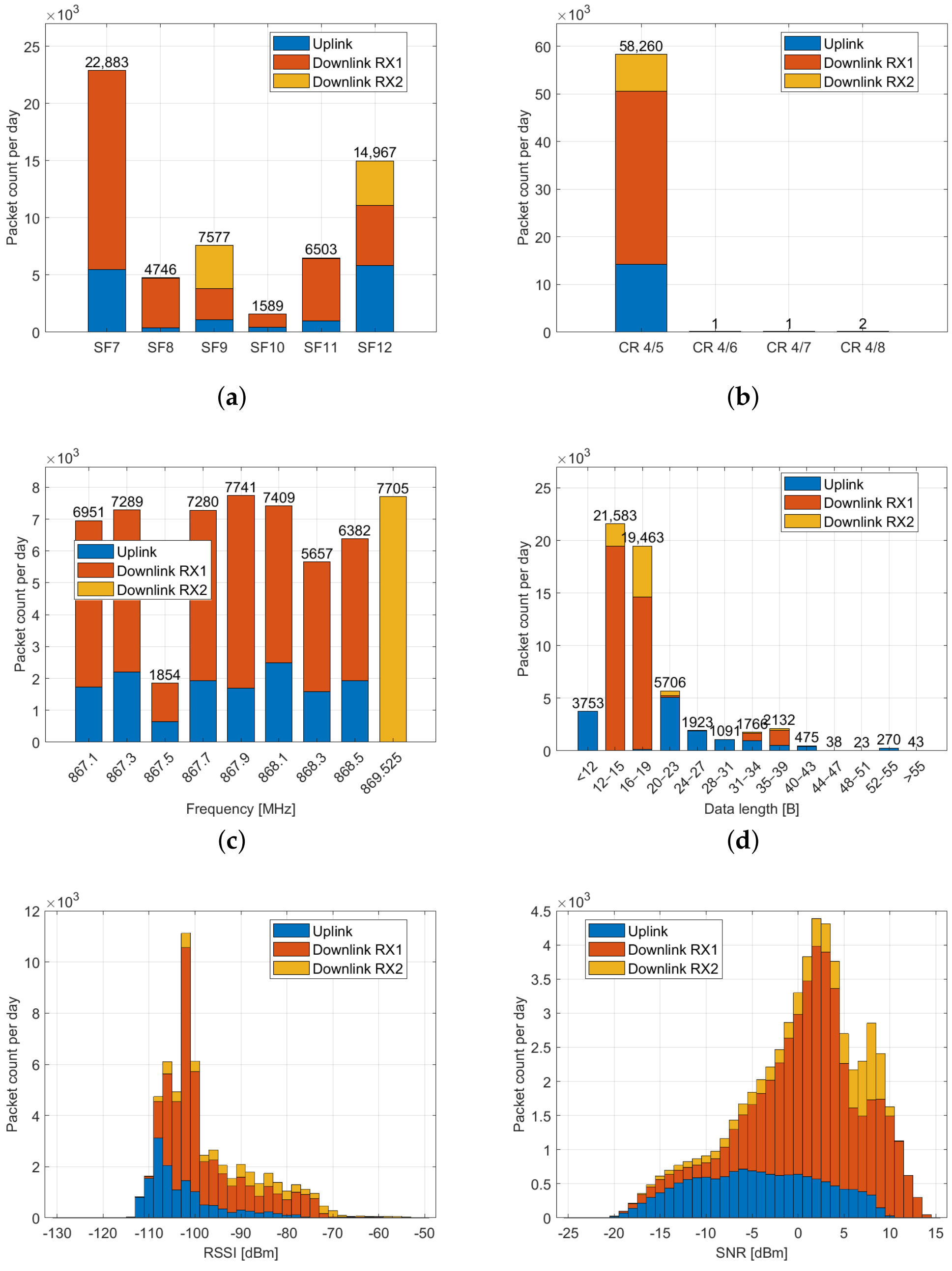
Table 4 shows the percentage of traffic with declared Adaptive Data Rate (ADR) support from end devices (extracted from uplink frames) and network servers (from downlink frames), declared end device Class-B support, and the percentage of downlink messages containing valid payload CRC.

Table 4. Support for ADR and Class-B features along with the occurrence of payload CRC in downlink messages found in captured LoRaWAN messages.

Location	Gateway Packets with ADR Support	End Device Packets with ADR Support	End Device Packets with Class-B Support	Downlink Messages with Payload CRC
Liege (Belgium)	3.9%	79.8%	2.3%	1.2%
Graz (Austria)	99.7%	57.4%	34.1%	99.7%
Vienna (Austria)	79.2%	83.6%	1.4%	81.9%
Brno (Czechia)	96.6%	86.6%	0.0%	99.3%

ADR is a feature that optimizes the data rate, transmission power, and airtime for end devices based on their connectivity conditions [5]. In uplink frames, the ADR flag set by the end device indicates its support for the ADR feature and requests the network server to manage its data rate and transmission power settings. When the ADR bit is set in a downlink frame, it informs the end device that the network server can send ADR commands. The ClassB flag in the uplink packet header indicates to the network server that the end device activated Class-B mode and is ready to receive scheduled downlink pings.

In accordance with the LoRaWAN standard, uplink and downlink packets are distinguished by the presence of payload CRC. While payload CRC is mandatory in the uplink packets, the standard does not require it in the downlink, allowing for reduced airtime and associated duty cycle for gateway transmissions [5]. However, the observed data indicate that, aside from the Liege site, payload CRC is appended in the downlink by the majority of LoRaWAN gateways.



(**a**) (**b**) (**c**) (**d**) (**e**) (**f**)

Figure 6. Parameters of captured LoRaWAN messages in the Vienna dataset: (**a**) Spreading factor; (**b**) Coding ratio; (**c**) Channel occupation; (**d**) Payload length; (**e**) Received Signal Strength Indicator (RSSI); (**f**) Signal-to-Noise Ratio (SNR).

4.2. Network Operators

The DevAddr field serves as an identifier for the end device within the LoRaWAN network [5,34]. It is transmitted unencrypted in both the uplink and downlink. To determine the network operator, we cross-referenced the prefix of DevAddr with the LoRa Alliance list [35]. The corresponding findings are presented in Table 5, which highlights significant traffic (over 400 packets per day) from various locations. Identifying the source gateway from a captured downlink packet is infeasible without access to the network server because it lacks explicit gateway-related information.

Table 5. Major network operators identified from the captured LoRaWAN traffic.

Network Operator	Liege Packets per Day	Liege % of Total	Graz Packets per Day	Graz % of Total	Vienna Packets per Day	Vienna % of Total	Brno Packets per Day	Brno % of Total
Private/experimental nodes	1312	21.6	3152	99.1	33,886	66.1	19,759	72.8
Minol ZENNER Connect	–	–	–	–	6138	12.0	–	–
The Things Network	59	1.0	9	0.3	4600	9.0	2194	8.1
Proximus	2751	45.3	–	–	4158	8.1	–	–
Actility	972	16.0	–	–	–	–	–	–
KPN	757	12.5	–	–	–	–	–	–
Orbiwise	–	–	–	–	412	0.8	–	–
Other/unassigned	218	3.6	19	0.6	2070	4.0	5193	19.1

4.3. End Device Manufacturers

In addition to analyzing the network operators, we also examined the end device manufacturers by analyzing the Device Extended Unique Identifier (DevEUI) field in the *Join Request* messages. The DevEUI is a globally unique number assigned to a LoRaWAN device and complies with the 64-bit Extended Unique Identifier (EUI-64) format [5].

To identify the manufacturers of end devices within the captured dataset, we cross-referenced the DevEUIs with the IEEE EUI-64 address space [36]. Table 6 presents the results of this analysis, highlighting the major traffic (over 10 join packets per day) from different manufacturers.

Table 6. Major end device manufacturers identified from the captured LoRaWAN traffic.

End Device Manufacturer	Liege Packets per Day	Liege % of Total	Graz Packets per Day	Graz % of Total	Vienna Packets per Day	Vienna % of Total	Brno Packets per Day	Brno % of Total
DZG Metering	–	–	–	–	603	38.6	–	–
RisingHF	–	–	–	–	–	–	288	77.7
Milesight	13	26.2	<1	0.7	106	6.8	7	1.9
Microchip Technology	–	–	–	–	93	6.0	6	1.6
Invoxia	1	1.9	–	–	90	5.8	–	–
Laird Connectivity	–	–	–	–	74	4.7	–	–
Adeunis RF	–	–	–	–	45	2.9	<1	∼0
MClimate	–	–	–	–	2	0.1	42	11.4
Holley Metering	–	–	–	–	30	1.9	–	–
ELSYS	–	–	–	–	23	1.5	–	–
Dragino Technology	–	–	–	–	17	1.1	<1	∼0
Seeed Technology	–	–	–	–	12	0.8	–	–
Viloc	11	21.8	–	–	–	–	–	–
Homerider Systems	10	18.8	5	43.0	1	0.1	–	–
Other/unassigned	16	31.4	9	56.3	893	29.9	65	7.4

4.4. Class-B Beacon Analysis

In a LoRaWAN Class-B network, gateways must be synchronized to broadcast the Class-B beacons. Two possible modes of the transmission exist: tightly synchronized, with gateways synchronized to Global Positioning System (GPS) time with an accuracy better than 1 µs, allowing them to transmit beacons every 128 seconds; and loosely synchronized, where gateways can synchronize with GPS time with an accuracy better than 1 ms but not 1 µs, requiring randomized beacon transmission. Tightly synchronized gateways capitalize on the single-frequency network, while loosely synchronized gateways utilize randomization to counteract beacon interference caused by lower transmit timing accuracy.

To effectively filter the sniffer data, we utilized specific settings for beacon reception at the LoRa physical layer. These settings include an implicit header mode, SF9BW125, CR 4/5, no CRC, a payload length of 17 bytes, a preamble length of 10 symbols, and a non-inverted LoRa signal [24]. The payload comprises a timestamp (representing seconds elapsed since the start of the GPS epoch) and a gateway-specific parameter (e.g., geographic coordinates or network/gateway identification). Each part is protected by an independent CRC checksum.

Significant differences were observed between the various locations included in the dataset. Ideally, 675 beacons per day should be received, considering the beacon interval of 128 s and tightly synchronized gateways without transmitting randomization. As expected due to interference, the actual numbers were lower. However, the data from Vienna and Brno also contained a substantial number of packets violating the LoRaWAN standard, as discussed in later sections.

Table 7 presents an analysis of the captured LoRaWAN Class-B beacons across different locations. All packets included in the table have both of their CRC checksums valid. The timestamp correctness was determined by comparing the precise time of the beacon arrival and the timestamp value contained in its payload. No Class-B beacons were included in the captured data from Graz.

Table 7. Analysis of the captured LoRaWAN Class-B beacons.

	Liege		Graz		Vienna		Brno	
Timestamp	**Packets per Day**	**% of Total**	**Packets per Day**	**% of Total**	**Packets per Day**	**% of Total**	**Packets per Day**	**% of Total**
Correct (includes location)	484	100.0	–	–	383	40.3	–	–
Correct (no location)	–	–	–	–	55	5.8	495	57.7
Incorrect, shifted by 18 s	–	–	–	–	505	53.1	–	–
Incorrect, in UNIX format	–	–	–	–	–	–	361	42.1
Incorrect (other)	–	–	–	–	9	0.9	1	0.1

The locations of Class-B gateways broadcasting their coordinates in the Liege and Vienna datasets, as well as lines connecting each gateway to the respective receiving sniffer, are depicted in Figure 7.

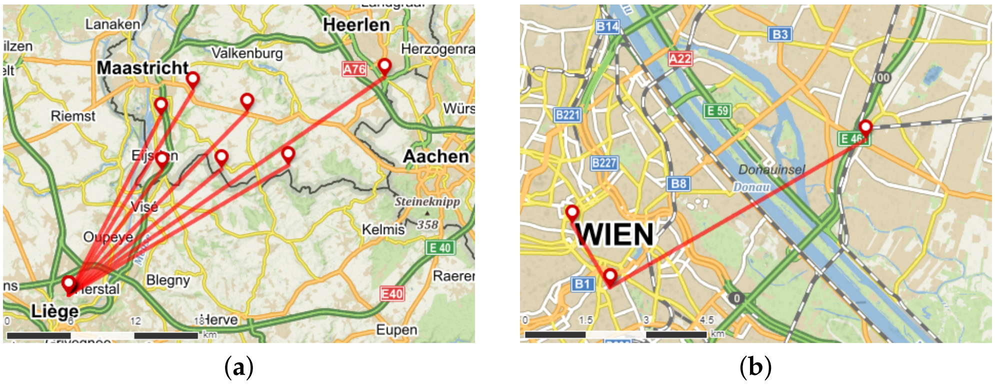


Figure 7. LoRaWAN sniffer placement and identified Class-B gateways beaconing its position in: (**a**) Liege; (**b**) Vienna. Map source: "Mapy.cz".

One of the most crucial pieces of data obtained was the accuracy of the beacon timestamps. Figure 8 displays the difference between the sniffer reference time, synchronized by the 1 pps signal from the GNSS receiver, and the time of the received beacon packet. This difference should ideally represent the beacon signal propagation delay. The time of the received packet is adjusted by 154,143 µs to incorporate the following corrections:

- 1500 µs, the time delay specified in the LoRaWAN standard as $T_{\text{BeaconDelay}}$ [5];
- 152,576 µs, the beacon packet transmission time (calculated from the EU868 beacon channel settings [24] with tool [37]);
- 67 µs, the empirically determined delay, likely due to sniffer signal processing.

For gateways that broadcast their geographic position as part of the beacon payload, we calculated the distance from the sniffer and displayed it as triangular marks in Figure 8. The figure reveals the low jitter in the arrival times of beacons across all sites, enabling the identification of individual gateways based on their distance from the sniffer. In addition to the gateways confirmed through the geographic coordinates, Figure 8 displays the reception of two more gateways in Vienna (at distances of approximately 31 km and 58 km) and a gateway in Brno (at a distance of approximately 90 km). It is important to note that this distance calculation assumes tightly synchronized gateways. Gateways that appear to be significantly distant may be loosely synchronized, transmitting their beacons with a small delay.

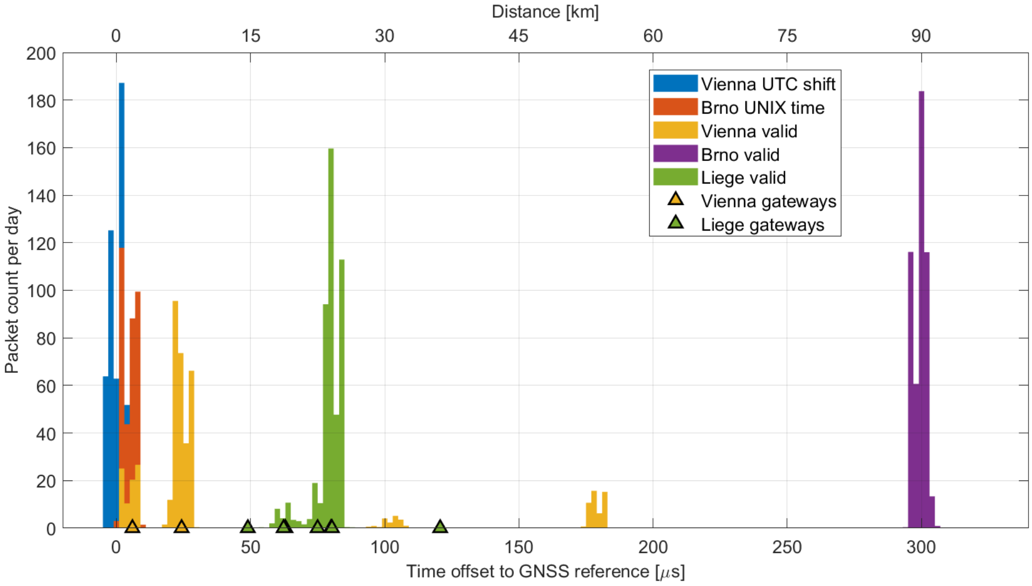


Figure 8. Time offset and corresponding distance between the GNSS reference and the received Class-B beacons.

It is also evident that the beacons with invalid timestamps described earlier are in close proximity to the sniffer. Considering the sniffer's location on university campuses in both Vienna and Brno, these gateways might be experimental and utilized for research and development purposes.

4.4.1. Beacons in the Liege Region

At the Liege location, well-configured gateways were found near the border in the Netherlands, specifically in the Maastricht and Haarlen area. A total of seven gateways with unique coordinates were identified, situated between 15 and 36 km from the sniffer. No gateways lacking the position or with invalid beacon frames were detected.

4.4.2. Beacons in the Vienna Region

Two nearby gateways broadcasting their geographic coordinates were identified. Based on the timing analysis shown in Figure 8, it appears that two additional, more distant gateways also contributed to beacon broadcasting.

However, alongside valid packets, a number of frames transmitted at incorrect times were captured. The vast majority of these erroneous frames were offset by 18 seconds. This offset is likely due to a faulty implementation of the conversion between the GPS time used in Class-B beacons and the commonly used Coordinated Universal Time (UTC). GPS time does not include leap seconds [38,39] and was synchronized to UTC on 5 January 1980. In 2023, the number of leap seconds, i.e., the difference between GPS time and UTC, is precisely 18 s.

Although the majority of recorded beacons were either valid or shifted by 18 seconds, the sniffer also recorded a significant number (0.9%) of packets with different time shifts, as demonstrated in Figure 9. The frames are always shifted by a whole number of seconds, meaning their synchronization within a one-second window is maintained. These packets are likely sent by a malfunctioning gateway, where the system clock is not correct, even though the actual beacon transmission is initiated accurately by the 1 pps signal. Together with the packets shifted by 18 seconds, they pose a significant issue for Class-B synchronization in the Vienna area and are likely to cause random network problems, resulting in LoRaWAN downlink latency degraded to Class-A. In this situation, the Class-B functionality of the end device depends on whether it synchronizes to a correct or invalid signal during the beacon acquisition phase [40].

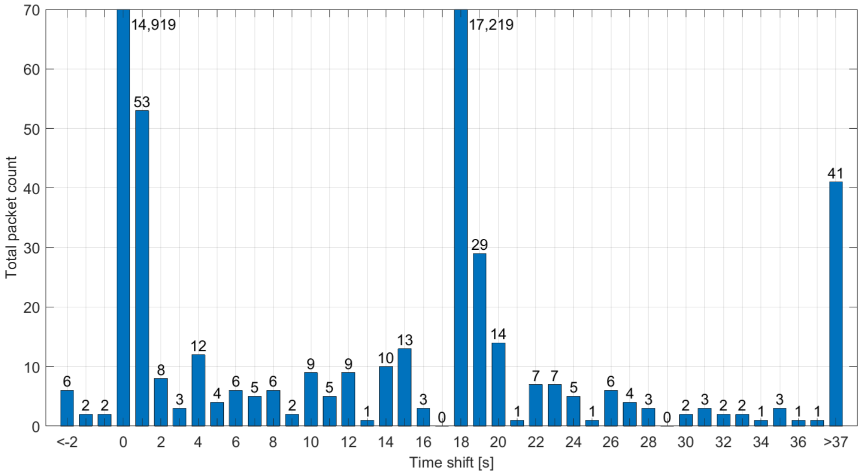


Figure 9. Difference between the actual reception time and the reported time in invalid Class-B beacons from the Vienna dataset.

4.4.3. Beacons in the Brno Region

Two beacon signals were identified in the captured data from Brno. One correct signal was received from a gateway with a time offset corresponding to an approximate distance of 90 km from the sniffer's location. No geographic coordinates that could confirm this distance were found, and approximately 0.1% of the frames were invalid.

Another beacon was identified at a distance of about 2 km. The timing information contained in this beacon was incorrect, shifted by 315,964,782 seconds. This value corresponds to the 315,964,800 s difference between the GPS and UNIX time. By subtracting the 18 leap seconds from this difference, we obtain the observed time shift. In other words, the gateway transmits a UNIX timestamp instead of the GPS time required by the LoRaWAN standard.

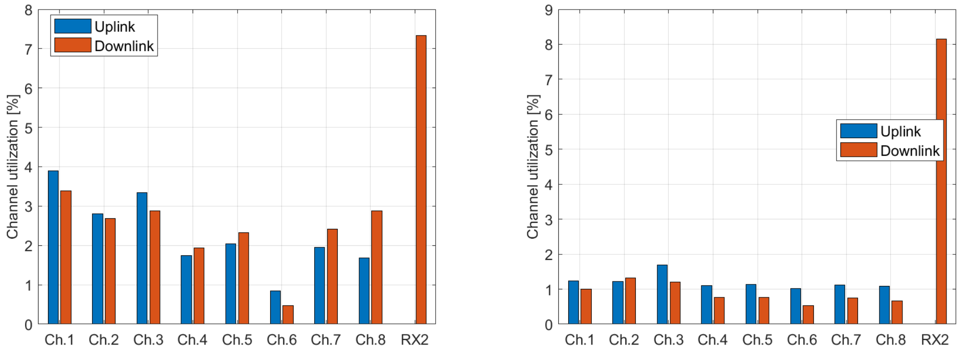
4.5. Channel Occupation and Duty Cycle Violations

LoRaWAN transmissions in the EU868 band must adhere to regulations specified in the ETSI EN 300 220 standard [25]. The duty cycle limitations for end devices and gateways vary depending on the specific frequency sub-bands. However, it should be noted that these duty cycle limitations are only required if the Listen Before Talk (LBT) is not used:

- band L, 865 MHz to 868 MHz, ≤1% duty cycle, includes RX1 channels 4 to 8;
- band M, 868.000 MHz to 868.600 MHz, ≤1% duty cycle, includes RX1 channels 1 to 3;
- band P, 869.400 MHz to 869.650 MHz, ≤10% duty cycle, includes RX2 channel.

The EU868 band is shared with other short-range devices that comply with the regulations, typically employing narrow-band Frequency Shift Keying (FSK) and Amplitude Shift Keying (ASK) modulations. We assessed the shared spectrum usage by calculating the on-air time of each captured packet, a value derived from the spreading factor, bandwidth, coding rate, preamble length, and packet length [37,41].

Furthermore, we computed the total air time for all sites, separately for the uplink and downlink, since different transmit directions utilize inverted, uncorrelated chirps. All captured packets, including those with invalid CRCs, were considered in the calculation to evaluate the total LoRa transmission time on the respective channel. The highest channel occupation was observed at Vienna and Brno, as shown in Figure 10.



(**a**) (**b**)

Figure 10. Channel utilization by LoRaWAN packets in (**a**) Vienna dataset; (**b**) Brno dataset.

Associating a downlink packet with a specific gateway is unfortunately not feasible. Nonetheless, it is possible to calculate the uplink on-air time for individual end devices based on their DevAddr field. The ETSI EN 300 220 duty cycle limits are not applicable to individual LoRaWAN channels; instead, they apply to specified bands that encompass several adjacent channels.

Considering this criterion, we identified a total of eight devices in the Brno dataset that, while adhering to the 1% duty cycle limitation on individual channels, exceed this limitation by several times for the L and M bands (with duty cycles reaching up to 3.9% for the L band and up to 2.6% for the M band). In the Vienna dataset, a single device was discovered to violate the limitation (2.7% duty cycle in the L band). However, it is worth noting that the devices we identified as exceeding the duty cycle limitation could potentially be using the LBT strategy.

4.6. Compromised Encryption Keys

The captured data show that exposed encryption keys are used in existing LoRaWAN networks. Semtech's default key (`2B7E151628AED2A6ABF7158809CF4F3C`) [9] was identified in the Brno dataset. This key is used as the AppKey for the OTAA by RisingHF devices by default, according to the DevEUI identifier. A significant number of data packets (15.5% of all valid packets) from ABP-activated devices in Brno use it as both the NwkSKey and AppSKey. A smaller number of such devices were also discovered in the Vienna dataset (0.2%).

Similarly, the Milesight default key (`5572404C696E6B4C6F52613230313823`) [42] was identified in OTAA-activated devices across Vienna, Brno, and Liege, primarily utilizing TTN. If an eavesdropper intercepts the entire *Join Request–Join Accept* pair, they could derive the NwkSKey and AppSKey, enabling them to decrypt the entire communication of the affected device.

A small number of packets in the Brno and Vienna datasets were also found to use the empty key (`00000000000000000000000000000000`). In these cases, the devices appear to be unconfigured or experimental.

4.7. Limited Front End Image Frequency Rejection

Strong packets can sometimes be received on two different channels with different chirp polarities. This phenomenon arises due to the limited value of the Image Frequency

Rejection Ratio (IMRR) of the radio front ends found in LoRaWAN gateways and the sniffer. An example of this can be identified in packets #306 and #307 in the Brno dataset, with the key characteristics depicted in Figure 11.

```
Frame 306: 62 bytes captured (496 bits)
Epoch Time: 1676538576.498914000 seconds
Src: b8:27:eb:af:ac:00:00:02
Flags: 0x0a, IQ Inverted, Checksum: CRC OK
Frequency: 867300000 Hz
Current RSSI: -112 dBm
SNR: -12.0 dB
Message type: Unconfirmed Data Up
Frame Payload: 0a79b794613ecd1c1d34b251f066
```

```
Frame 307: 62 bytes captured (496 bits)
Epoch Time: 1676538576.498908000 seconds
Src: b8:27:eb:af:ac:00:00:01
Flags: 0x08, Checksum: CRC OK
Frequency: 867700000 Hz
Current RSSI: -59 dBm
SNR: 10.5 dB
Message type: Unconfirmed Data Up
Frame Payload: 0a79b794613ecd1c1d34b251f066
```

Figure 11. Duplicate packets with different chirp polarities in the Brno dataset.

The packets were received almost simultaneously, with a negligible 6 µs difference. Frame #307 is a valid uplink transmission with a signal strength of −59 dBm and a non-inverted chirp. Given a received frequency of 867.7 MHz and a front end center frequency of 867.5 MHz (as shown in Table 1), we can anticipate a mirror signal at 867.3 MHz. This is confirmed by frame #306, which has a signal strength of −112 dBm. The difference of 53 dB corresponds to the IMRR value of the SX1257 front end employed in the sniffer.

Due to the signal spectrum inversion, such invalid packets can be easily identified by the inverted chirp flag, because data marked as uplink in the LoRaWAN header should not be detected by the downlink sniffer. To ensure data accuracy, these packets were filtered out during processing. The described behavior could potentially overshadow a legitimate weak packet at the mirror frequency. However, the likelihood of its occurrence is almost negligible, given the low usage of the channels.

4.8. Invalid LoRaWAN Traffic with Valid Checksum

LoRa packets at the PHY layer contain a Synchronization Word (SyncWord), which serves to differentiate the contents of the following payload. The use of the SyncWord can be confusing due to limited information from the manufacturer.

Semtech recommends only two SyncWord values: 0x12 for private networks, and 0x34 for public/LoRaWAN networks [41,43]. Documents from the LoRaWAN Alliance [24] and certain source codes [30] imply that SyncWord 0x34 is designated for all networks utilizing the LoRaWAN protocol at the MAC layer. This interpretation suggests that both publicly and privately designed networks following the LoRaWAN standard should employ SyncWord 0x34. The private SyncWord 0x12 appears to be reserved for devices utilizing LoRa modulation at the PHY layer without engaging the LoRaWAN MAC layer.

The SyncWord setting is crucial for both modulation and demodulation, as the receiver does not accept packets transmitted with a different SyncWord [44]. This issue is not merely about discarding packets in the case of a mismatch; it arises from the inability to synchronize on the preamble–SyncWord pair [45].

All datasets contain packets with errors that the LoRaWAN dissector cannot decode. The Liege dataset includes a significant number of invalid packets (4.7% of the total). Invalid packets are identified by dissector errors or invalid MAC header entries, which include a non-zero Reserved for Future Use (RFU) field and a Major version that is not equal to R1.

Receiving an invalid LoRaWAN packet can be attributed to a misconfiguration of the LoRa transmitter, which uses a custom payload for packets set with a public SyncWord. The correct approach would be to use a dedicated private SyncWord, which appears to be the issue occurring in the Liege dataset. Another possibility involves accepting invalid packets that are erroneously evaluated as valid due to various factors. This could be attributed to the limited reliability of the 16-bit payload CRC [41], which may occasionally fail to identify packet corruption, or it could be due to the unwanted acceptance of packets with a private SyncWord.

The SyncWord issue was investigated in the InterOP project ATCZ175 [46], and its results indicate a relatively low capability of the gateway to filter packets based on SyncWord. The success rate of receiving a private SyncWord packet when the gateway is set to the public SyncWord depends on the signal strength and the SF used, with the possibility of reaching up to 10%. Consequently, any traffic with a private SyncWord may lead to the observation of invalid packets in sniffer datasets.

4.9. Class-B Beacons as a Timebase Source

Class-B beacons in LoRaWAN networks have the potential to serve as alternative timebase source in urban environments. Beacon receivers typically lock within 128 seconds, providing excellent long-term stability, as their timing is usually derived from a GNSS receiver. According to the LoRaWAN standard, beacon timing is accurate within ±1 µs, while measurements taken by the sniffer without further optimizations revealed an accuracy of ±5 µs. This accuracy is further reduced by the wireless propagation delay—every 300 m of distance represents an additional 1 µs offset.

Compared to GNSS, Class-B beacons can be received indoors, making them suitable for time synchronization in buildings and other structures where GNSS signals are weak or unavailable. Unlike GNSS, Class-B beacons do not require a clear view to the sky, enhancing their reliability in urban environments where tall buildings, trees, or other obstacles might obstruct GNSS signals.

Class-B beacons also offer several benefits compared to the DCF77, a Long-Wave (LW) time signal broadcast from Germany. They exhibit high immunity to noise, making them more reliable in urban environments where specific types of RF interference are common, e.g., the LW interference affecting DCF77 signals. Class-B beacon receivers can use small, cheap antennas, lowering the overall cost and making them more accessible for a wide range of applications. Moreover, Class-B beacons have a similar lock speed to DCF77, with a lock time of up to 128 seconds compared to DCF77's typical lock time of 2–3 minutes [47].

Compared to NTP, Class-B beacons do not require an internet connection for time synchronization, making them suitable for environments with limited or no internet access. This independence from internet connections makes Class-B beacons a compelling alternative for various applications.

To further enhance the lock time, a multichannel (e.g., SDR-based) device may listen for Class-A downlink traffic, which may contain the *DeviceTimeAns* time command in its unencrypted MAC header. Despite the limited accuracy of ±100 ms as defined in [5], this may allow for a coarse lock. The listening device can also derive the time window for Class-B beacon reception from this information, potentially reducing continuous receive time.

However, this proposed time synchronization may encounter difficulties if nearby gateways transmit beacons that violate the LoRaWAN standard. Such issues have already been observed in the Vienna and Brno regions, as previously discussed. Currently, no method exists to verify the authenticity of a received beacon. Moreover, due to the harsh RF environment, beacons may be disrupted by a wide-band UHF interference, resulting in decoding errors and significantly longer lock time.

Despite these challenges, by leveraging the benefits of Class-B beacons, time synchronization in urban environments can be significantly improved. The indoor reception capabilities, noise immunity, cost effectiveness, and independence from satellite availability and internet connections make Class-B beacons an attractive alternative for existing time synchronization methods, provided that the associated disadvantages can be effectively managed.

5. Conclusions

In this study, we created an extensive, publicly available dataset encompassing complete LoRaWAN traffic from four European cities. This dataset enabled rigorous examination of real-world LoRaWAN network functionality. Our analysis revealed security and system challenges, which include:

- invalid Class-B beacon packets, which pose a significant synchronization issue and are likely to cause random Class-B network problems;
- default encryption keys from Semtech and Milesight in existing LoRaWAN installations, which pose a security risk;
- end devices violating the duty cycle limitation for EU868 sub-bands, which could potentially degrade the quality of service for other wireless devices.

We enhanced Wireshark's LoRaWAN protocol dissector to accurately decode recorded traffic, including data and MAC command decryption for packets with known keys. These improvements are now publicly accessible. Additionally, we proposed the use of Class-B beacons as a timebase source in urban environments.

Future research should incorporate datasets from a broader range of locations to enhance understanding of LoRaWAN networks. Additionally, addressing the issues related to invalid Class-B beacons is a critical next step. Class-B devices currently allow the fallback to Class-A when they experience difficulties in tracking the beacon. However, this depends on the specific device implementation, since the documentation only suggests an initial non-specific synchronization [5,40].

Validating received beacons remains a challenge. The beacon payload may contain an optional network/gateway identification. However, to the best of our knowledge, no beacon filtering implementation has been introduced yet. Another approach could involve transmitting the initial synchronization over a secure channel, specifically within a unicast packet with a MIC signature. This method can be employed to acquire the correct Class-B beacon. While a solution that utilizes the *DeviceTimeAns* command to acquire coarse time has been implemented, its use remains optional.

Author Contributions: Conceptualization, A.P. and J.K.; methodology, A.P. and J.K.; software, A.P. and O.K.; validation, A.P., O.K. and M.N.; formal analysis, A.P.; investigation, A.P.; resources, J.K., H.A. and M.N.; data curation, A.P.; writing—original draft preparation, A.P.; writing—review and editing, A.P., J.K. and H.A.; visualization, A.P.; supervision, J.K. and H.A.; project administration, A.P. and J.K.; funding acquisition, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Internal Grant Agency of Brno University of Technology under project no. FEKT-S-23-8191. The dataset was created with the support of the Technology Agency of the Czech Republic under grant agreement no. TK04020173.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are openly available on Zenodo at 10.5281/zenodo.8090619, reference number [6].

Acknowledgments: During the preparation of this work, the authors utilized ChatGPT to help refine language and style. After using this service, the authors reviewed and edited the paper as necessary, and they take full responsibility for the content of the publication.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Semtech. LoRa® and LoRaWAN®: A Technical Overview. Available online: https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf (accessed on 12 July 2023).
2. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 855–873. [CrossRef]
3. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors* **2018**, *18*, 3995. [CrossRef] [PubMed]
4. Semtech. AN1200.22 LoRa™ Modulation Basics. Available online: https://www.semtech.com/products/wireless-rf/lora-connect/sx1276 (accessed on 2 May 2023).
5. LoRa Alliance. TS001-1.0.4 LoRaWAN® L2 1.0.4 Specification. Available online: https://lora-alliance.org/resource_hub/ts001-1-0-4-lorawan-l2-1-0-4-specification/ (accessed on 2 May 2023).
6. Povalac, A.; Kral, J. LoRaWAN Traffic Analysis Dataset. Version 2. Zenodo. 2023. Available online: https://zenodo.org/record/8090619 (accessed on 16 August 2023).
7. Bhatia, L.; Breza, M.; Marfievici, R.; McCann, J.A. LoED: The LoRaWAN at the Edge Dataset: Dataset. In Proceedings of the Third Workshop on Data: Acquisition To Analysis, New York, NY, USA, 16–19 November 2020; DATA '20, pp. 7–8. [CrossRef]
8. Aernouts, M.; Berkvens, R.; Van Vlaenderen, K.; Weyn, M. Sigfox and LoRaWAN Datasets for Fingerprint Localization in Large Urban and Rural Areas. *Data* **2018**, *3*, 13. [CrossRef]
9. Blenn, N.; Kuipers, F. LoRaWAN in the Wild: Measurements from The Things Network. *arXiv* **2017**, arXiv:1706.03086. https://doi.org/10.48550/arXiv.1706.03086.
10. Choi, K.N.; Kolamunna, H.; Uyanwatta, A.; Thilakarathna, K.; Seneviratne, S.; Holz, R.; Hassan, M.; Zomaya, A.Y. LoRadar: LoRa Sensor Network Monitoring through Passive Packet Sniffing. *SIGCOMM Comput. Commun. Rev.* **2020**, *50*, 10–24. [CrossRef]
11. Povalac, A. LoRaWAN Traffic Analysis Tools. Available online: https://github.com/alpov/lorawan-sniffer (accessed on 10 May 2023).
12. Spadaccino, P.; Crinó, F.G.; Cuomo, F. LoRaWAN Behaviour Analysis through Dataset Traffic Investigation. *Sensors* **2022**, *22*, 2470. [CrossRef] [PubMed]
13. Ruotsalainen, H.; Shen, G.; Zhang, J.; Fujdiak, R. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors* **2022**, *22*, 3127. [CrossRef] [PubMed]
14. Broxson, J. Feather TFT LoRa Sniffer. Available online: https://github.com/ImprobableStudios/Feather_TFT_LoRa_Sniffer (accessed on 2 May 2023).
15. Bravo-Montoya, A.F.; Rondón-Sanabria, J.S.; Gaona-García, E.E. Development and Testing of a Real-Time LoRawan Sniffer Based on GNU-Radio. *TecnoLógicas* **2019**, *22*, 130–139. [CrossRef]
16. Robyns, P.; Quax, P.; Lamotte, W.; Thenaers, W. A Multi-Channel Software Decoder for the LoRa Modulation Scheme. In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, Funchal, Portugal, 19–21 March 2018; pp. 41–51. [CrossRef]
17. Marquet, A.; Montavont, N.; Papadopoulos, G.Z. Towards an SDR implementation of LoRa: Reverse-engineering, demodulation strategies and assessment over Rayleigh channel. *Comput. Commun.* **2020**, *153*, 595–605. [CrossRef]
18. Tapparel, J.; Afisiadis, O.; Mayoraz, P.; Balatsoukas-Stimming, A.; Burg, A. An Open-Source LoRa Physical Layer Prototype on GNU Radio. In Proceedings of the 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Atlanta, GA, USA, 26–29 May 2020; pp. 1–5. [CrossRef]
19. Silva, F.S.D.; Neto, E.P.; Oliveira, H.; Rosário, D.; Cerqueira, E.; Both, C.; Zeadally, S.; Neto, A.V. A Survey on Long-Range Wide-Area Network Technology Optimizations. *IEEE Access* **2021**, *9*, 106079–106106. [CrossRef]
20. Marais, J.M.; Malekian, R.; Abu-Mahfouz, A.M. Evaluating the LoRaWAN Protocol Using a Permanent Outdoor Testbed. *IEEE Sens. J.* **2019**, *19*, 4726–4733. [CrossRef]
21. Fujdiak, R.; Mikhaylov, K.; Pospisil, J.; Povalac, A.; Misurec, J. Insights into the Issue of Deploying a Private LoRaWAN. *Sensors* **2022**, *22*, 2024. [CrossRef] [PubMed]
22. Ramirez, C.G.; Dyussenova, A.; Sergeyev, A.; Iannucci, B. LongShoT: Long-Range Synchronization of Time. In Proceedings of the 2019 18th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Montreal, QC, Canada, 16–18 April 2019; pp. 289–300. [CrossRef]
23. Rizzi, M.; Depari, A.; Ferrari, P.; Flammini, A.; Rinaldi, S.; Sisinni, E. Synchronization Uncertainty Versus Power Efficiency in LoRaWAN Networks. *IEEE Trans. Instrum. Meas.* **2019**, *68*, 1101–1111. [CrossRef]
24. LoRa Alliance. RP002-1.0.3 LoRaWAN® Regional Parameters. Available online: https://lora-alliance.org/resource_hub/rp2-1-0-3-lorawan-regional-parameters/ (accessed on 2 May 2023).
25. ETSI EN 300 220-2 V3.2.1: Short Range Devices (SRD) Operating in the Frequency Range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for Access to Radio Spectrum for Non Specific Radio Equipment. Available online: https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf (accessed on 4 May 2023).
26. The Things Network. LoRaWAN Frequency Plans. Available online: https://www.thethingsnetwork.org/docs/lorawan/frequency-plans/ (accessed on 2 May 2023).
27. IMST GmbH. WiMOD iC880A Datasheet. Available online: https://wireless-solutions.de/downloadfile/ic880a-spi-documents/ (accessed on 2 May 2023).

28. Semtech. SX1301: LoRa Core™ Digital Baseband Chip for Outdoor LoRaWAN® Network Macro Gateways. Available online: https://www.semtech.com/products/wireless-rf/lora-core/sx1301 (accessed on 2 May 2023).
29. Semtech. SX1257: LoRa Core™ Low Power Digital I and Q RF Multi-PHY Mode Analog Front End 860-1000MHz. Available online: https://www.semtech.com/products/wireless-rf/lora-core/sx1257 (accessed on 2 May 2023).
30. Semtech. LoRa Gateway Project. Available online: https://github.com/Lora-net/lora_gateway (accessed on 2 May 2023).
31. Semtech. LoRa Network Packet Forwarder Project. Available online: https://github.com/Lora-net/packet_forwarder (accessed on 2 May 2023).
32. De Jong, E. LoRaTap: Encapsulation Format to be Used to Store LoRa Traffic in Pcap Files. Available online: https://github.com/eriknl/LoRaTap (accessed on 2 May 2023).
33. Wireshark. Automated Builds. Available online: https://www.wireshark.org/download/automated/win64/ (accessed on 19 June 2023).
34. LoRa Alliance. TS002-1.1.0 LoRaWAN Backend Interfaces Specification. Available online: https://lora-alliance.org/resource_hub/ts002-110-lorawan-backend-interfaces/ (accessed on 2 May 2023).
35. LoRa Alliance. NetID Allocation. Available online: https://lora-alliance.org/wp-content/uploads/2022/06/LoRa-Alliance-NetID-Allocation-1.pdf (accessed on 2 May 2023).
36. IEEE Standards Association. Guidelines for Use of EUI, OUI, and CID. Available online: https://standards.ieee.org/wp-content/uploads/import/documents/tutorials/eui.pdf (accessed on 3 May 2023).
37. Hu, Y.H. LoRa Air-Time Calculator. Available online: https://github.com/ifTNT/lora-air-time (accessed on 2 May 2023).
38. Lewandowski, W.; Arias, E.F. GNSS times and UTC. *Metrologia* **2011**, *48*, S219. [CrossRef]
39. NIST. Leap Second and UT1-UTC Information. Available online: https://www.nist.gov/pml/time-and-frequency-division/time-realization/leap-seconds (accessed on 2 May 2023).
40. Semtech. An In-Depth Look at LoRaWAN® Class B Devices. Available online: https://lora-developers.semtech.com/uploads/documents/files/LoRaWAN_Class_B_Devices_In_Depth_Downloadable.pdf (accessed on 26 May 2023).
41. Semtech. SX1272: Long Range, Low Power RF Transceiver 860-1000MHz with LoRa® Technology. Available online: https://www.semtech.com/products/wireless-rf/lora-connect/sx1272 (accessed on 2 May 2023).
42. Milesight. 3D ToF People Counting Sensor User Manual. Available online: https://www.milesight.com/static/file/en/download/datasheet/3d-tof/Milesight-3D-ToF-People-Counting-Sensor-User-Manual-en.pdf (accessed on 4 May 2023).
43. Semtech. SX1261: LoRa Connect™ Long Range Low Power LoRa® RF Transceiver +15 dBm, Global Frequency Coverage. Available online: https://www.semtech.com/products/wireless-rf/lora-connect/sx1261 (accessed on 2 May 2023).
44. Haxhibeqiri, J.; Van den Abeele, F.; Moerman, I.; Hoebeke, J. LoRa Scalability: A Simulation Model Based on Interference Measurements. *Sensors* **2017**, *17*, 1193. [CrossRef] [PubMed]
45. Seller, O.B.; Sornin, N. Low Power Long Range Transmitter. Patent US9252834B2, 2 February 2016.
46. ATCZ175 InterOP. Private/Public-Syncword Crosstalk. Available online: https://www.interreg-interop.eu/results/lorawan/privatepublic_syncword_crosstalk/index.html (accessed on 2 May 2023).
47. Engeler, D. Performance analysis and receiver architectures of DCF77 radio-controlled clocks. *IEEE Trans. Ultrason. Ferroelectr. Freq. Control* **2012**, *59*, 869–884. [CrossRef] [PubMed]

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.

A&A 677, A40 (2023)
https://doi.org/10.1051/0004-6361/202346182
© The Authors 2023

Astronomy & Astrophysics

GRBAlpha: The smallest astrophysical space observatory

I. Detector design, system description, and satellite operations

András Pál[1], Masanori Ohno[2], László Mészáros[1], Norbert Werner[3], Jakub Řípa[3], Balázs Csák[1], Marianna Dafčíková[3], Marcel Frajt[4], Yasushi Fukazawa[2], Peter Hanák[5], Ján Hudec[4], Nikola Husáriková[3], Jakub Kapuš[4], Miroslav Kasal[6], Martin Kolář[3], Martin Koleda[7], Robert Laszlo[7], Pavol Lipovský[5], Tsunefumi Mizuno[2], Filip Münz[3], Kazuhiro Nakazawa[8], Maksim Rezenov[4], Miroslav Šmelko[9], Hiromitsu Takahashi[2], Martin Topinka[10], Tomáš Urbanec[6], Jean-Paul Breuer[3], Tamás Bozóki[11], Gergely Dálya[12], Teruaki Enoto[13], Zsolt Frei[14], Gergely Friss[14], Gábor Galgóczi[14,15], Filip Hroch[3], Yuto Ichinohe[16], Kornél Kapás[17,18,15], László L. Kiss[1], Hiroto Matake[2], Hirokazu Odaka[19], Helen Poon[2], Aleš Povalač[6], János Takátsy[14,15], Kento Torigoe[2], Nagomi Uchida[20], and Yuusuke Uchida[21]

[1] Konkoly Observatory, Research Centre for Astronomy and Earth Sciences, Konkoly-Thege M. út 15-17, 1121 Budapest, Hungary
e-mail: apal@szofi.net
[2] Hiroshima University, School of Science, 1-3-1 Kagamiyama, Higashi-Hiroshima, Japan
[3] Department of Theoretical Physics and Astrophysics, Faculty of Science, Masaryk University, Kotlářská 267/2, Brno 611 37, Czech Republic
[4] Spacemanic Ltd, Jablonec 110, 900 86 Jablonec, Slovakia
[5] Faculty of Aeronautics, Technical University of Košice, Rampová 1731/7, 040 01 Košice, Slovakia
[6] Department of Radio Electronics, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technická 3058/10, 616 00 Brno-Královo Pole, Czech Republic
[7] Needronix Ltd, Geologická 1, 821 06 Bratislava, Slovakia
[8] Department of Physics, Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8601, Japan
[9] EDIS vvd., Rampová 7, 041 21 Košice, Slovakia
[10] INAF Istituto di Astrofisica Spaziale e Fisica Cosmica, via Bassini 15, 20133 Milano, Italy
[11] Institute of Earth Physics and Space Science (EPSS), Csatkai E. u. 6-8, 9400 Sopron, Hungary
[12] Department of Physics and Astronomy, Universiteit Gent, Proeftuinstraat 86, 9000 Gent, Belgium
[13] School of Science, Kyoto University, 1 Matsugasakihashigami-cho, Sakyo-ku, Kyoto, Japan
[14] Eötvös Loránd University, Institute for Physics, Pázmány Péter stny. 1/A, Budapest, Hungary
[15] Wigner Research Centre for Physics, Konkoly-Thege Miklós út 29-33, 1121 Budapest, Hungary
[16] Department of Physics, Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo, Japan
[17] Department of Theoretical Physics, Institute of Physics, Budapest University of Technology and Economic, Műegyetem rkp. 3, 1111 Budapest, Hungary
[18] MTA-BME Quantum Dynamics and Correlations Research Group, Budapest University of Technology and Economics, Műegyetem rkp. 3, 1111 Budapest, Hungary
[19] Department of Earth and Space Science, Osaka University, 1-1 Machikaneyamacho, Toyonaka, Osaka, Japan
[20] Institute of Space and Astronautical Science, Japan Aerospace Exploration Agency, 3-1-1 Yoshinodai, Chuo-ku, Sagamihara, Japan
[21] Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, Japan

Received 18 February 2023 / Accepted 27 March 2023

ABSTRACT

Aims. Since it launched on 22 March 2021, the 1U-sized CubeSat GRBAlpha operates and collects scientific data on high-energy transients, making it the smallest astrophysical space observatory to date. GRBAlpha is an in-orbit demonstration of a gamma-ray burst (GRB) detector concept suitably small to fit into a standard 1U volume. As was demonstrated in a companion paper, GRBAlpha adds significant value to the scientific community with accurate characterization of bright GRBs, including the recent outstanding event of GRB 221009A.

Methods. The GRB detector is a $75 \times 75 \times 5$ mm CsI(Tl) scintillator wrapped in a reflective foil (ESR) read out by an array of SiPM detectors, multi-pixel photon counters by Hamamatsu, driven by two separate redundant units. To further protect the scintillator block from sunlight and protect the SiPM detectors from particle radiation, we applied a multi-layer structure of Tedlar wrapping, anodized aluminium casing, and a lead-alloy shielding on one edge of the assembly. The setup allows observations of gamma radiation within the energy range of 70−890 keV with an energy resolution of ∼30%.

Results. Here, we summarize the system design of the GRBAlpha mission, including the electronics and software components of the detector, some aspects of the platform, and the current semi-autonomous operations. In addition, details are given about the raw data products and telemetry in order to encourage the community to expand the receiver network for our initiatives with GRBAlpha and related experiments.

Key words. instrumentation: detectors – space vehicles: instruments – gamma rays: general

1. Introduction

GRBAlpha is an in-orbit demonstration mission of a gamma detector system suitably small to fit into a 1U CubeSat size, having an approximate dimension of 10 × 10 × 11 cm. In this experiment, we validate our concept of employing such small detector systems for extracting astrophysical data related to gamma-ray bursts (GRBs; Pál et al. 2020; Řípa et al. 2022a). One of the most recent findings of GRBAlpha is the characterization of GRB 221009A (Veres et al. 2022; Lesage et al. 2022), an exceptionally bright and long gamma-ray burst reported first by the *Fermi* Gamma-ray Burst Monitor (GBM). We note here that this event was also detected by a series of other instruments, including AGILE/GRID (Piano et al. 2022), AGILE/MCAL (Ursi et al. 2022), BepiColombo/MGNS (Kozyrev et al. 2022), Insight-HXMT & SATech-01/GECAM-C (HEBS; An et al. 2023), INTEGRAL/SPI-ACS (Gotz et al. 2022), Konus-WIND & SRG/ART-XC (Frederiks et al. 2023), MAXI & NICER (Williams et al. 2023), Solar Orbiter/STIX (Xiao et al. 2022), STPSat-6/SIRI-2 (Mitchell et al. 2022), and *XMM-Newton* (Tiengo et al. 2023). As a comparatively small detector, GRBAlpha provided an unsaturated observation (Řípa et al. 2022b), and therefore allowed the scientific community to accurately obtain the peak flux of the event (Řípa et al. 2023).

In this paper, we present a description of the detector subsystem, the satellite platform, the operations scheme and the data downlink management. With its mission concept, involvement of students, and implementation of onboard transponder features the satellite gained the support of the radio amateur community and had an International Amateur Radio Union (IARU) coordination for downlink telemetry frequency in the UHF band[1]. Such a world-wide community can be extremely valuable for GRB astrophysics, due to the low latency of data downlinks for various types of orbits. In order to meet our commitments toward the amateur radio community, an extensive description is included in this paper about the data format related to the telemetry structure and the process required to convert raw data streams into a scientifically relevant format. In order to further extend the available data types for downlink and upgrade the scientific onboard software in accordance, free code points are still available in the data stream to preserve backward compatibility and attain a forward compatibility in the ground segment components.

The structure of the paper is as follows. In Sect. 2, we describe the detector structure used for monitoring GRBs, including the mechanical configuration of the detector, the analog and digital components of the electronics, the onboard digital signal processing (DSP) scheme, and the structure of the data streams provided by the DSP block as it is saved on board and retrieved from the satellite. In Sect. 3, we give the core components of the satellite platform, while in Sect. 4 we present the currently implemented operations scheme, including data formats used for downlink. We give the results from the commissioning of this satellite in Sect. 5, while we give a brief summary and plans about the future onboard payload software upgrade in Sect. 6.

2. Detector structure

In this section, we summarize the design of the satellite main payload (i.e., the scientific detector assembly) and the format of the data provided by (and downloaded from) the detector electronics. The details of the integration of the detector into the satellite platform are described in Sect. 3.

2.1. Scintillator and MPPCs

As stated in Pál et al. (2020), the core of the detector design is a thallium activated cesium-iodine crystal, having a size of 75 × 75 × 5 mm. We applied an enhanced specular reflector (ESR) wrapping around the scintillator, with the exception of a small area of the crystal where the multi-pixel photon counters (MPPCs) or MPPC silicon photomultipliers (SiPMs) are attached. A linear array of 2 × 4 S13360-3050PE MPPCs is mounted on a 60 × 5 mm printed circuit board (PCB). This assembly is then wrapped into a black Tedlar (DuPont TCC15BL3) layer, which prevents stray light leaking from outside both to the detector crystal and the MPPC SiPMs. In addition to the aluminum enclosure, we mounted a lead alloy (PbSb3) shielding at the side of the detector assembly where the MPPCs are located. The steps of the detector assembly are displayed in the panels of Fig. 1.

2.2. Analog and digital electronics

The layout of detector electronics just prior to final integration is exhibited in Fig. 2. To have a greater flexibility in the system design, the analog frontend electronics are mounted on a separate daughterboard. On this board the high-voltage reverse bias supply is controlled via a digital–analog converter (DAC) and provides an adjustable output voltage between 45 and 60 V. Current flowing through the biased MPPCs is proportional to the amount of light detected by the photon counters. After being sensed with an appropriate resistor, the signal is driven into the analog signal chain formed by a preamplifier and the pulse-shaping circuitry. With the appropriately chosen resistor–capacitor (RC) networks, the pulse is widened to have a width that can be fully sampled by the analog–digital converter (ADC) without distorting its characteristics (see Fig. 3 for more details). Further components on the analog daughterboard are an I^{2}C separator for the DAC and an additional power supply that provides the required voltage levels (±5 V) for the amplifiers and the shaping circuitry (see also Torigoe et al. 2019 for further details).

Data acquisition is controlled directly by a field-programmable gate array (FPGA). The real-time processing of the FPGA is ensured by an embedded system-on-a-chip architecture, where both the interface logic toward the 12-bit ADC and the communication lines toward the satellite are attached to a soft microprocessor (soft CPU). This embedded CPU allows high-level programming directly within the FPGA and it is powerful enough to run a FreeRTOS-based operating system at the same time. Communication interfaces connected to the FPGA are a full-duplex universal asynchronous receiver-transmitter (UART) and an inter-integrated circuit (I^{2}C) bus; the primary interface is provided by the UART line, while I^{2}C is used as a cold spare at the present implementation.

The main data acquisition mode supported by the FPGA is a dual-channel histogram accumulator. The waveform of the analog signal chain is continuously sampled with an 1.5 µs period (666kSPS rate) by the ADC attached to the FPGA. During the detection of a burst of optical photons, the digital logic is triggered and provides a number proportional to the energy of the incident gamma photon. The counter associated with the appropriate bin in the active histogram is then increased by one. In

[1] http://www.amsatuk.me.uk/iaru/finished_detail.php?serialnum=745

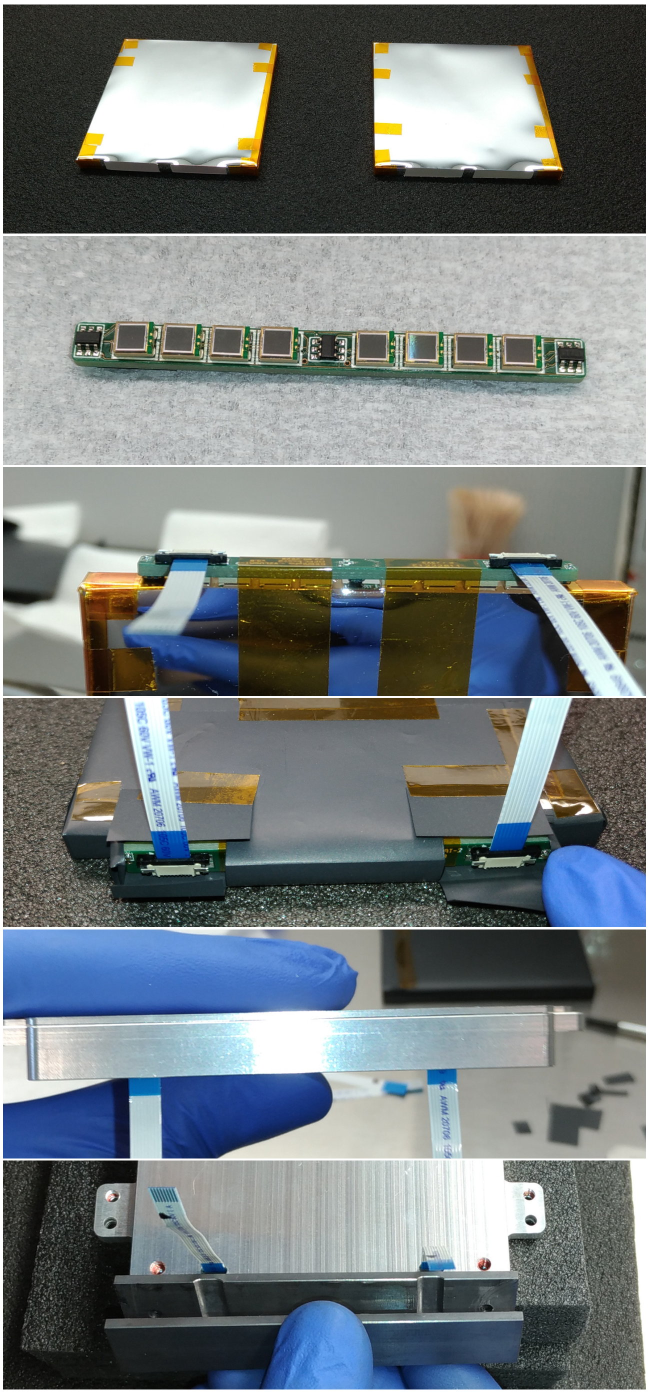


Fig. 1. Structure of the detector shown as a series of photos from the assembly procedure. *Top*: two scintillator crystals, flight model and flight spare, wrapped in ESR foil (with the exception of the positions for the MPPC arrays). *Second*: PCB with two multi-pixel photon counter (MPPC by Hamamatsu) SiPM sensor arrays and thermometers. *Third*: sensor array fixed onto the crystal. *Fourth*: one of the steps used to apply the Tedlar wrapping as a light trap. *Fifth*: enclosure with the flex cables, side view. *Bottom*: mounting the lead shielding at the side of the detector where the MPPC arrays are.

parallel with this accumulation, the passive histogram can be read out and can also be reset after data are read. At the end of the exposure the roles of the two histogram channels are swapped within a single clock cycle, providing a 100% duty cycle for the detector. In practice, the embedded block RAMs associated with both of these (otherwise identical) histograms are 32 bit wide and have a depth of 256. This setup allows a high instrumental resolution for the energy spectra as well as long exposure times without any integer overflow. On the other hand, the data transfer rate between the FPGA and the main microcontroller unit (MCU) allows exposure times as short as 20 ms even at the highest spectral resolution.

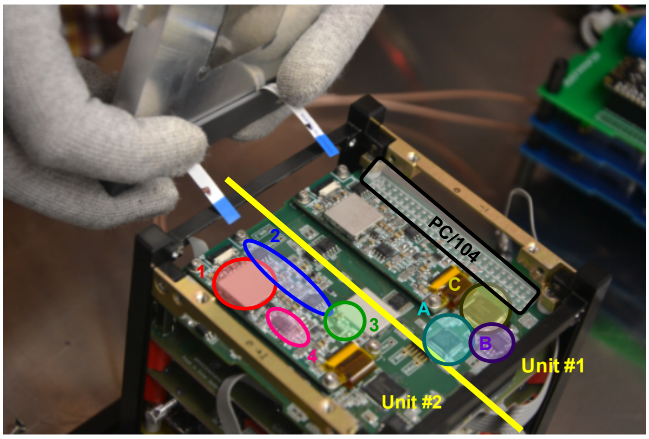


Fig. 2. Payload components of the GRBAlpha nanosatellite. The numbers indicate the daughterboard containing the analog and mixed-signal components for payload unit #2: 1 (red): adjustable high-voltage supply for MPPC reverse biasing, shielded; 2 (blue): Preamplifier and signal shaping circuitry; 3 (green): analog-digital converter; 4 (magenta): High-voltage control logic. The letters indicate the main PC/104 board with the digital control and signal processing parts for payload unit #1: A (cyan): microcontroller unit; B (lilac): FPGA configuration FRAM, also used as a secondary staging area for firmware upgrades; C (yellow): FPGA responsible for the interface between the mixed-signal components on the daughterboard and the MCU. The PC/104 system bus connector can be seen at the top right of the figure. This photo was taken during the integration of the satellite when the scintillator block was attached electrically to the daughterboards using the white-blue flex cables.

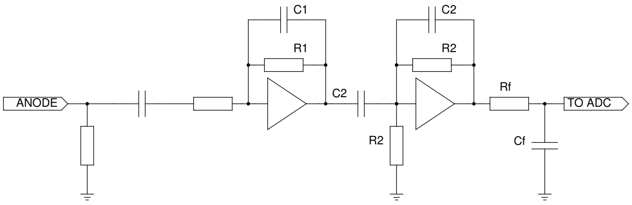


Fig. 3. Block-level schematics of the analog signal chain between the MPPC output and the ADC. This two-stage amplifier is formed by a traditional charge sensitive amplifier with $R_1C_1 = 3.3$ ms decay constant and an RC-CR shaping amplifier $\tau = 2.2$ µs.

In the current implementation, FPGA data acquisition cycles are actively controlled by a MCU. This ARM Cortex-M0 MCU core and the attached peripherals perform further processing and time-tagging of the signal, providing a temporary storage area before downlink and interfacing the detector system to the platform components such as the onboard computer and the radio transceivers.

Before starting routine operations (e.g., after power cycling) the payload enters a bootloader state, and can only be started by sending the appropriate telecommands. This setup, along with the reconfiguration of the FPGA bitstream, allows us smooth and safe system-level operations (as shown in Fig. 4). Moreover, the

Table 1. Self-synchronizing variable-length coding employed in the scientific data streams of GRBAlpha onboard units, and also found in the telemetry format.

Integer range	Bytes	Bit pattern	Overlong range
$0\dots63$	1	00xxxxxx	–
$64\dots2^{12}-1$	2	010xxxxx 1xxxxxxx	$0\dots63$
$2^{12}\dots2^{18}-1$	3	0110xxxx 1xxxxxxx 1xxxxxxx	$0\dots2^{12}-1, 0\dots63$
$2^{18}\dots2^{24}-1$	4	01110xxx 1xxxxxxx 1xxxxxxx 1xxxxxxx	$0\dots2^{18}-1, 0\dots2^{12}-1, 0\dots63$
$2^{24}\dots2^{30}-1$	5	011110xx 1xxxxxxx 1xxxxxxx 1xxxxxxx 1xxxxxxx	$0\dots2^{24}-1,\dots,0\dots63$
Unused code points	1+	011111xx [. . .]	–

Notes. Up to 30-bit integers are currently supported, which also allows integers up to 24-bit length to be encoded in the overlong range. However, 2 bits of code point space are still available for arbitrary future extensions in order to ensure forward compatibility.

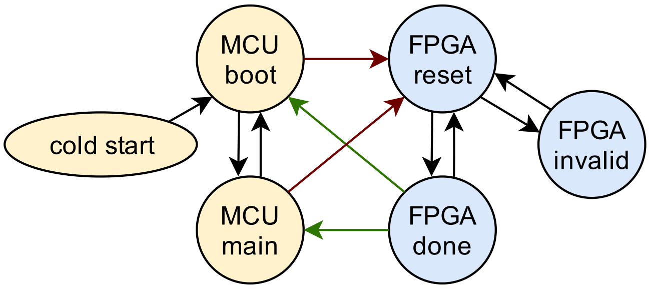


Fig. 4. System-level modes of operations of the GRBAlpha payload. After the cold start, the microcontroller unit enters bootloader mode, but is still able to fully access and control the data acquisition FPGA. Once booted, regular measurements can instantly be started; however, FPGA configuration is still possible at the same time if needed. This setup allows the on-the-fly upgrade of both the MCU software and the FPGA bitstream in a safe manner; both binary images can be uploaded to the staging areas during routine operations. In the diagram, black arrows are state transitions, red arrows denote state changes, while green arrows imply state queries. Neither of the state transitions on the MCU side nor the assertion of FPGA reset state is done automatically by the system; it is only possible by telecommands. Therefore, boot loops are not possible in this setup. If an invalid binary image is uploaded to the MCU, a watchdog reset and/or power cycling will start it again in bootloader mode, allowing the detailed examination of the situation. In the case of a failure in the FPGA bitstream upgrade, the FPGA enters to invalid mode, continuously driving its "configuration done" output low. This is detected by the MCU which can then put it back into reset state for recovery.

system is capable of receiving upgraded firmware images during routine operations including the cases when scientific data acquisition is ongoing.

2.3. Data stream

The onboard storage and telemetry stream both employ a self-synchronizing variable-length code. In addition to the byte stream, the individual code points also form a self-synchronizing pattern at the block level, allowing decoders to unambiguously extract data even from smaller portions. This sequence is optimized for storing spectral count rates with Poisson statistics and finding weak signals above a small background.

The symbols (code points) encoded in the raw byte stream are unsigned integers: the higher the integer number, the greater the number of bytes used to store. On the other hand, this variable length encoding allows the presence of overlong sequences; within an overlong code small numbers are stored in more bytes than the minimum number of bytes needed for storage. Table 1 summarizes the currently employed code space used by the payload storage system and data streams, including the overlong sequences. For instance, the number 42 is small enough to be stored in one byte (`0x2A`), but it is allowed to be stored in two bytes (`0x40 0xAA`), three bytes (`0x60 0x80 0xAA`), or more. Such overlong characters represent block-level synchronization patterns, and its code space also includes metadata about the upcoming block. As listed in Table 1, a maximum of 30-bit numbers are presently supported, but there still is a 2-bit wide unused self-synchronization code point space for further extensions if larger integers and/or other types of data are needed to be transmitted. The rule of thumb is that one byte is needed to store six bits of information, while data equivalent to eight bits are interleaved for block-level synchronization. However, these bits still encode further information regarding the type of the following block (see Table 2 for the currently employed list of synchronization blocks).

3. Satellite platform and system design

The mechanical construction of GRBAlpha follows the standards defined by the CubeSat specifications. A 1 U form factor has a dimension of $100\times100\times113.5$ mm; however, lateral extensions are permitted in the $X\pm$ and $Y\pm$ sides up to 6.5 mm (CubeSat Design Specification 2022). The full GRBAlpha stack is exhibited in Fig. 5 along with the reference frame also involved in the detector modeling. The stack weights 1.2 kg in total and the total amount of available power averaged over one orbit is 1 W.

The primary satellite components found in the 1U-sized stack are connected using the de facto standard PC/104 connector system. This connector system distributes the power from the switchable power supply and wires the three independent internal communication interfaces between the payload electronics, onboard computer, global navigation satellite system (GNSS) receiver, sensor board, radio transceivers, and the power supply. While GRBAlpha is not equipped with an active attitude control system, it has permanent magnets on board as well as patches of magnetically soft material for passive attitude stabilization and attitude information is obtained using MEMS gyroscopes, magnetometers, and sun sensors at the same time.

Radio communication for data downlink incorporates a Gaussian frequency-shift keying (GFSK) modulation with a nominal baud rate of 9600 where individual radio packets (corresponding to one packet on the transport protocol layer) are encapsulated within the High-level Data Link Control (HDLC) framing, in accordance with the specifications defined by the AX.25 link layer. Furthermore, a linear feedback shift register is

Table 2. Data stream synchronization patterns and their respective interpretations for integers encoded in an overlong form.

Integer value or range	Interpretation
2-byte overlong 3 . . . 31	consecutive zeros, number of zeros is the value (i.e., between 3 and 31)
2-byte overlong 32 . . . 39	spectrum, bin mode is the value minus 32 (i.e., between 0 and 7)
2-byte overlong 40	absolute timing, followed by 3 integers: seconds (upper 8 bits and lower 24 bits) and microseconds
2-byte overlong 41	relative timing, followed by a single integer (microseconds, w.r.t. the previous timestamp)
2-byte overlong 42	metadata & housekeeping data: index, exposure time in µs, total count, cutoff value, temperatures
2-byte overlong 42 . . . 47	reserved for future housekeeping information and metadata of satellite platform components
2-byte overlong 48 . . . 63	reserved for future synchronization patterns
3-byte overlong 32 . . . 255	consecutive zeros, number of zeros is the value (i.e., between 32 and 255)
4-byte overlong values	unallocated code points, reserved for future use
5-byte overlong values	unallocated code points, reserved for future use

Notes. All of the overlong code space can also be used for self-synchronization purposes. A portion of the code space is used to encode a longer series of zeros (found in the high-resolution calibration spectra taken in low-background regions), precise absolute timestamps, precise differential timestamps, housekeeping data, metadata associated with the data acquisition parameters, and other types of synchronization patterns.

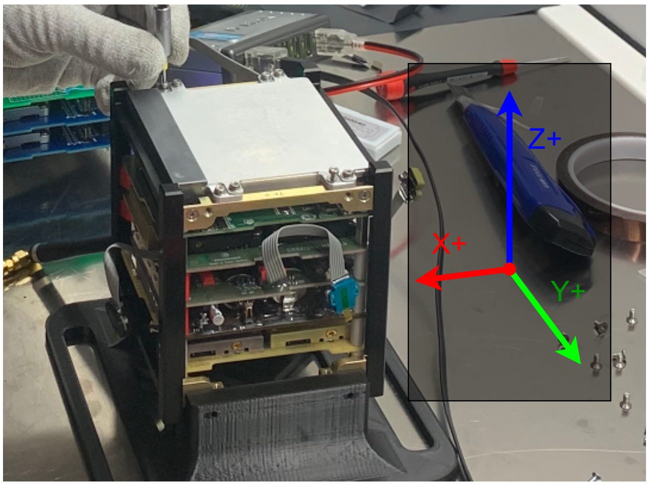


Fig. 5. Stack of GRBAlpha and the reference frame with respect to the satellite. From top to bottom: chasing of the gamma detector, gamma detector payload electronics (see also Fig. 2), onboard computer and GNSS receiver, sensor board, power supply, radio transceivers, and antenna deployer.

applied in addition to the HDLC stream with tap points defined in accordance with the G3RUH packet radio modem design. This is done to further whiten the GFSK radio signal, and to therefore allow many 0 ↔ 1 transitions for asynchronous clock recovery. Telemetry beacons are either HDLC frames or frames with additional headers defined by the AX.25 protocol. Telemetry beacons are then automatically decoded and uploaded to the public dashboard of GRBAlpha[2], while HDLC frames are also diverted to the console during interactive operations (see Sect. 4).

The uncontrolled rotation of GRBAlpha provides a nearly homogeneous temperature distribution within the system. The detector temperature (see Fig. 1, second picture) varies between −5 and +15 °C, while the most exposed parts (e.g., the solar panels) have a temperature between −20 and +25 °C.

4. Operations and data downlink

Using the currently available storage configurations, GRBAlpha is operating in a semi-autonomous mode. Individual observing runs are configured and queued manually during satellite contacts, while data retrieval is either controlled interactively or files (and/or file fragments) are scheduled for further drops above designated stations. The interactive control uses simplex stations; telecommanding is performed via an uplink station in Bankov, near Košice, Slovakia, while telemetry packets are received and forwarded to the console from two receiver stations located at the Piszkéstető Observatory[3,4], Hungary, and in Jablonec[5], Slovakia. Simplex stations eliminate the need of RF power-switching circuitry, greatly simplifying the station design, while two receiver stations provide nearly 100% packet decoding during interactive sessions, compensating for the transmission fading caused by the onboard dipole antenna. During routine operations, the net scientific data downlink daily rate is around ∼200 kB; however, with proper selection of data drops, this daily data volume could go as high as ∼1 MB while still maintaining a positive power balance.

4.1. Onboard storage

GRBAlpha implements two independent forms of onboard data storage schemes. First, the onboard computer allows the storage of arbitrary but small data chunks in a structure known as the DataKeeper (DK). DK is capable of storing chunks received by any node on the satellite, including itself (for collecting platform-specific housekeeping data) and the payload nodes. DK has been designed to work in conjunction with packet radio-based downlink, and the size of the fragments is adjusted in accordance with the maximum individual radio packet size. However, DK relies on the data link layer between the satellite and the ground station(s) during retrieval, and therefore packets that are lost during the transfer need to be requested again if the assembly was not successful. This scheme allows simple operations; however, an excessive number of transactions are needed to compensate for the intrinsic data loss.

In addition to DK, both nodes of the GRB payload units have their own data storage devices, allowing independent (and optionally redundant) data handling. The payload firmware allocates a filesystem distributed along its storage devices; data, including routine measurements, can also be stored in separate files, and during downlink files can be downloaded, either fully or partially. This last option is the preferred one during the

[2] https://dashboard.satnogs.org/d/iXL8Q0lGk/grbalpha

[3] https://network.satnogs.org/stations/2380/

[4] https://ccdsh.konkoly.hu/wiki/SatNOGS_station_2380

[5] https://network.satnogs.org/stations/2138/

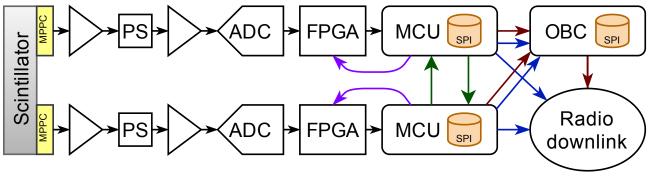


Fig. 6. Scientific data flow within the GRBAlpha payload and platform components. Black arrows show the direction of the signal path originating from the MPPCs attached to the detector. The signal streams processed by the MCU are then being routed into various directions, depending on the currently running data acquisition configuration. Red arrows represent DataKeeper packets while blue arrows represents individual files that are retrieved either directly as file fragments or scrambled for forward error correction. File fragments can also be transferred to DK for employing the DK-based retrieval. Green arrows represent the copying functionality between the two payload nodes. This functionality allows both scientific data transfer between the two nodes (currently only for redundancy at block level) and aiding firmware upgrade by cloning either the main program binary image or the FPGA bitstream image if needed.

extraction of individual GRB events (detected by other missions) where the trigger time is known. The total amount of onboard storage capacity is 2 MB for the DK, while it is 2 × (2 + 64) MB for the GRB payload units. The data storage scheme is displayed in Fig. 6.

4.2. Data downlink

Files storing scientific or auxiliary data are saved in the onboard file system of the payload units. Files are then transferred to ground either via the DataKeeper area of the onboard computer or directly via the radio module. Commonly, these individual files or even portions of these files containing relevant scientific information (e.g., a few dozen minutes of recording before and after a gamma-ray burst) are too large to fit into a single AX.25 radio packet. In this case, the file F is fragmented into smaller chunks (i.e., $F = \{f_0, f_1, \ldots, f_{n-1}\}$, where n is the total number of chunks). These chunks are, in practice, set to $k = 128$ bytes, so $n = \lfloor (S_F + k - 1)/k \rfloor$ where S_F is the size of file F in bytes. Expecting no data loss (or when these file fragments are transferred to DK), the fragments f_i are transferred sequentially without any further processing.

Due to the checksum field embedded in the radio packets, a single packet is either received completely or fully discarded. Therefore, any type of packet radio forward error correction (FEC) should be implemented at a higher level. In order to add such a FEC code at the packet level, the individual fragments are scrambled and converted via a partial Vandermonde transformation over the Galois field $\mathrm{GF}\left(2^{32}\right)$. In our practice, a file fragment f_i is partitioned into a series of 32-bit unsigned integers (i.e., $f_i = \left\{f_i^{(0)}, \ldots, f_i^{(\ell)}, \ldots, f_i^{(L-1)}\right\}$, where ℓ runs from $\ell = 0$ to $L - 1 = 31$ for a 128-byte long fragment). A packet $g_i = \left\{g_i^{(0)}, \ldots, g_i^{(L-1)}\right\}$ sent to the ground is then computed as

$$g_i^{(\ell)} = \sum_{j=0}^{R-1} K_i^j \cdot f_{i+j}^{(\ell)}, \tag{1}$$

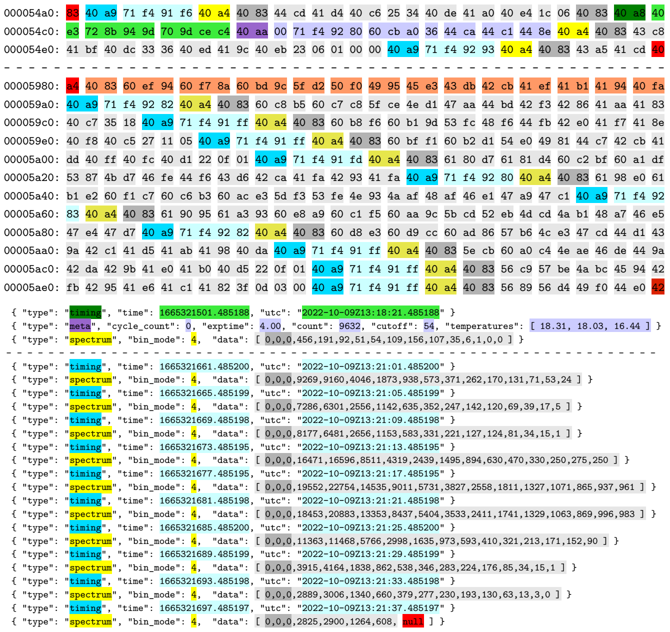
where R is the length defining the partial Vandermonde transformation and K_i is a key associated with this scrambled packet g_i. The multiplication involved in the computation of K^j and during the evaluation of $K^j \cdot f_{i+j}^{(\ell)}$ is defined over the finite field $\mathrm{GF}\left(2^{32}\right)$, and therefore it cannot be implemented as a single binary multiply operation. If $R = 1$, Eq. (1) yields no additional scrambling, and it is equivalent to the sequential file transfer since $K_i^j = K_i^0 = 1$ for all possible values of $K_i \in \mathrm{GF}\left(2^{32}\right)$. On the other hand, if $R = n$ and $K_i = i$, this equation is equivalent to a multiplication of the input vector with the Vandermonde matrix $V_{ij} = K_i^j = i^j$, providing full redundancy during the transfer; receiving n packets in any combination will allow the receiver to assemble the original file. However, letting R be as big as n, the computation of Eq. (1) requires too much computing power; in the practice of GRBAlpha operations we use $R = n$ transfers only for files containing calibration spectra required to characterize detector degradation when the sizes of these files are on the order of a few kilobytes (and not hundreds of kilobytes or megabytes). During a download request, the GRBAlpha payload firmware is also capable of creating a randomized series of i indices in order to further scramble the file transfer. Upon reception of the $g_i^{(\ell)}$ fragments, it is both necessary and sufficient to include the length R, the key K_i, the fragment offset index i, and the total number of fragments n (or, equivalently, the file size) within the same telemetry packet. The net size of the fragment, L is simply taken from the packet size. We found this feature important due to the uncontrolled rotation of the satellite. Specifically, by employing a single receiver station, the transmission could fade as long as five to ten seconds with a period of a few minutes. In this case, adjacent fragments are completely missing from the stream even from comparatively large values of R, and this scenario would make the inversion of the partial Vandermonde matrix impossible.

For example, such a file download can be seen in the SatNOGS observation 7134188[6], where (due to fading) ~840 packets were retrieved out of the nearly ~1000 packets transmitted; however, the above-mentioned scrambling and partial Vandermonde transformation with the length parameter of $R = 8$ was sufficient to easily recover the $n = 600$ fragments. In practice, even a smaller overhead is sufficient for downlink; our experience from many hundreds of such downloads is that the minimum additional redundancy needed is around ~15%, which accounts both for the packet loss due to transmission fading and for the reception of fragments that are not linearly independent over $\mathrm{GF}\left(2^{32}\right)$. This level of redundancy is equivalent to the overhead of an RS(255, 223) Reed-Solomon code. For reference, we give an implementation of the this fragment unpacking, FEC assembly, and scientific data decoding on the project's website[7]. Raw packets retrieved are converted into an intermediate JSON (JavaScript Object Notation) representation (`grbalpha-downlink.sh`), which is then assembled using the FEC method described above (`asmgetf`), and then the assembled scientific streams are decoded into a standardized format (`daq-decode.sh`).

4.3. Data products

By implementing the process of retrieval described in Sect. 4.2, data are available to the community in the format of a JSON representation similar to the listing displayed in Fig. 7. The count spectra in JSON files are also converted to FITS[8] files following the OGIP FITS Standards, which can be used by common

[6] https://network.satnogs.org/observations/7134188/
[7] https://grbalpha.konkoly.hu/static/utils/
[8] https://fits.gsfc.nasa.gov/



```
000054a0: 83 40 a9 71 f4 91 f6 40 a4 40 83 44 cd 41 d4 40 c6 25 34 40 de 41 a0 40 e4 1c 06 40 83 40 a8 40
000054c0: e3 72 8b 94 9d 70 9d ce c4 40 aa 00 71 f4 92 80 60 cb a0 36 44 ca 44 c1 44 8e 40 a4 40 83 43 c8
000054e0: 41 bf 40 dc 33 36 40 ed 41 9c 40 eb 23 06 01 00 00 40 a9 71 f4 92 93 40 a4 40 83 43 a5 41 cd 40
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
00005980: a4 40 83 60 ef 94 60 f7 8a 60 bd 9c 5f d2 50 f0 49 95 45 e3 43 db 42 cb 41 ef 41 b1 41 94 40 fa
000059a0: 40 a9 71 f4 92 82 40 a4 40 83 60 c8 b5 60 c7 c8 5f ce 4e d1 47 aa 44 bd 42 f3 42 86 41 aa 41 83
000059c0: 40 c7 35 18 40 a9 71 f4 91 ff 40 a4 40 83 60 b8 f6 60 b1 9d 53 fc 48 f6 44 fb 42 e0 41 f7 41 8e
000059e0: 40 f8 40 c5 27 11 05 40 a9 71 f4 91 ff 40 a4 40 83 60 bf f1 60 b2 d1 54 e0 49 81 44 c7 42 cb 41
00005a00: dd 40 ff 40 fc 40 d1 22 0f 01 40 a9 71 f4 91 fd 40 a4 40 83 61 80 d7 61 81 d4 60 c2 bf 60 a1 df
00005a20: 53 87 4b d7 46 fe 44 f6 43 d6 42 ca 41 fa 42 93 41 fa 40 a9 71 f4 92 80 40 a4 40 83 61 98 e0 61
00005a40: b1 e2 60 f1 c7 60 c6 b3 60 ac e3 5d f3 53 fe 4e 93 4a af 48 af 46 e1 47 a9 47 c1 40 a9 71 f4 92
00005a60: 83 40 a4 40 83 61 90 95 61 a3 93 60 e8 a9 60 c1 f5 60 aa 9c 5b cd 52 eb 4d cd 4a b1 48 a7 46 e5
00005a80: 47 e4 47 d7 40 a9 71 f4 92 82 40 a4 40 83 60 d8 e3 60 d9 cc 60 ad 86 57 b6 4c e3 47 cd 44 d1 43
00005aa0: 9a 42 c1 41 d5 41 ab 41 98 40 da 40 a9 71 f4 91 ff 40 a4 40 83 5e cb 60 a0 c4 4e ae 46 de 44 9a
00005ac0: 42 da 42 9b 41 e0 41 b0 40 d5 22 0f 01 40 a9 71 f4 91 ff 40 a4 40 83 56 c9 57 be 4a bc 45 94 42
00005ae0: fb 42 95 41 e6 41 c1 41 82 3f 0d 03 00 40 a9 71 f4 91 ff 40 a4 40 83 56 89 56 d4 49 f0 44 e0 42
```

```
{ "type": "timing", "time": 1665321501.485188, "utc": "2022-10-09Z13:18:21.485188" }
{ "type": "meta", "cycle_count": 0, "exptime": 4.00, "count": 9632, "cutoff": 54, "temperatures": [ 18.31, 18.03, 16.44 ] }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,456,191,92,51,54,109,156,107,35,6,1,0,0 ] }
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
{ "type": "timing", "time": 1665321661.485200, "utc": "2022-10-09Z13:21:01.485200" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,9269,9160,4046,1873,938,573,371,262,170,131,71,53,24 ] }
{ "type": "timing", "time": 1665321665.485199, "utc": "2022-10-09Z13:21:05.485199" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,7286,6301,2556,1142,635,352,247,142,120,69,39,17,5 ] }
{ "type": "timing", "time": 1665321669.485198, "utc": "2022-10-09Z13:21:09.485198" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,8177,6481,2656,1153,583,331,221,127,124,81,34,15,1 ] }
{ "type": "timing", "time": 1665321673.485195, "utc": "2022-10-09Z13:21:13.485195" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,16471,16596,8511,4319,2439,1495,894,630,470,330,250,275,250 ] }
{ "type": "timing", "time": 1665321677.485195, "utc": "2022-10-09Z13:21:17.485195" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,19552,22754,14535,9011,5731,3827,2558,1811,1327,1071,865,937,961 ] }
{ "type": "timing", "time": 1665321681.485198, "utc": "2022-10-09Z13:21:21.485198" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,18453,20883,13353,8437,5404,3533,2411,1741,1329,1063,869,996,983 ] }
{ "type": "timing", "time": 1665321685.485200, "utc": "2022-10-09Z13:21:25.485200" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,11363,11468,5766,2998,1635,973,593,410,321,213,171,152,90 ] }
{ "type": "timing", "time": 1665321689.485199, "utc": "2022-10-09Z13:21:29.485199" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,3915,4164,1838,862,538,346,283,224,176,85,34,15,1 ] }
{ "type": "timing", "time": 1665321693.485198, "utc": "2022-10-09Z13:21:33.485198" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,2889,3006,1340,660,379,277,230,193,130,63,13,3,0 ] }
{ "type": "timing", "time": 1665321697.485197, "utc": "2022-10-09Z13:21:37.485197" }
{ "type": "spectrum", "bin_mode": 4,  "data": [ 0,0,0,2825,2900,1264,608, null ] }
```

Fig. 7. Scientific telemetry streams from GRBAlpha in raw format (*upper panel*) and decoded format (*lower panel*, displayed in the form of hierarchical JSON objects and arrays). The corresponding blocks are highlighted accordingly: absolute time instances are highlighted in green, relative time synchronization values are highlighted in blue, data acquisition metadata and housekeeping blocks are purple, spectral measurements are yellow and light gray. Bytes that are out of stream-level synchronization are highlighted with dark red while blocks are out of block-level synchronization are highlighted with orange. The trailing byte is also highlighted as red, denoting a stray byte (however, the full block can also be partially decoded, as it is clear from the JSON form). The data displayed correspond to the second peak of the GRB 221009A event, see also the respective timestamps. Note also that relative timestamps are converted to absolute time instances during the decoding.

spectral analysis tools such as the X-ray spectral fitting package XSPEC[9] (Arnaud 1996). Current and typical data acquisition modes include a 1 s cadence with 4 or 16 energy channels and calibration cycles that are run for 5 × 60 s with full resolution of 256 channels. Within this representation, one JSON record includes the photon counts for each energy bin, and the precise timestamps and settings related to binning are also interleaved. Other settings for the data acquisition, including exposure times, cutoff value settings (for excluding the pedestal before binning), and detector housekeeping data, are interleaved with distinctive JSON object-type fields. Due to the extensible nature of the JSON objects, planned data acquisition modes (e.g., parallel retrieval of data streams, and long exposure and high spectral resolution combined with short cadence and low resolution) can easily be inserted while still being compatible with the current data structure.

5. Commissioning and early scientific results

Along with a few dozen CubeSat-class missions and larger satellites, GRBAlpha was launched on 22 March 2021 via the support of GK Launch Services. During commissioning, we performed all of the relevant platform-side tests of the satellite components and uploaded a revised payload firmware that was developed between the satellite integration and the launch. Following the commissioning phase and the modelling of the detector effective area at various energy ranges (Fig. 8), the satellite started to perform dedicated background monitoring observations. The background level in the form of total counts per second as measured throughout the orbits of GRBAlpha is displayed in Fig. 9. Based on these results, the fraction of time when the satellite is able to detect an average GRB with at least a 5σ significance is ~67%. This is the duty cycle on a 550 km polar orbit and at lower altitudes and smaller inclinations the observing efficiency is expected to be higher. As a representative example, the light curve related to the exceptionally bright event of GRB 230307A is displayed in Fig. 10. The background-subtracted version of this light curve is shown in Dafcikova et al. (2023).

While the initial low-energy threshold of the detectors was in the range of 30 keV after launch, the degradation of the Hamamatsu MPPCs remains at an acceptable level, resulting in a low-energy threshold degradation to 60–70 keV after two years of in-orbit operations. A detailed evaluation of the SiPM detector degradation will be a subject of a forthcoming paper (Takahashi et al., in prep.). In addition, we plan to perform further in-orbit adjustments of the bias voltage settings to optimize the performance at lower energies.

If the satellite is operated continuously, the detection rate is approximately one transient every five days. The number of detected long GRBs is, at the time of writing, significantly higher than the number of short GRBs, which might be the result of the relatively long time bins. The initial length of time bins was four seconds, which was recently changed to one second. Further shortening of the employed bins is expected to increase the detection rate of short GRBs.

6. Summary and future upgrade plans

Since its launch and at the time of writing, GRBAlpha has detected and characterized 23 confirmed GRBs, nine solar flares, two soft gamma repeaters (SGRs), and one X-ray binary outburst, including prominent events like GRB 221009A[10]. In order to further increase and extend the scientific yield, we are planning to continue to tune and optimize the onboard software stack of the system. One of our most important short-term upgrade plans related to the payload software is the inclusion of an onboard trigger system, which would allow autonomous detection of gamma-ray transients by real-time monitoring of the observed count rate. The triggering system would allow independent detection of GRBs and other events without the knowledge of the detection by other missions. Due to the availability of a GNSS receiver, we also plan to connect the GNSS output signals directly to the payload FPGA (Pál et al. 2018) in order to achieve a timing accuracy comparable to the onboard oscillator timing resolution. While an active attitude control is not essential for such a detector type on a small (i.e., transparent) satellite, the knowledge of the attitude is important for the proper interpretation of scientific data. GRBAlpha has on board magnetometers and sun sensors; however, further upgrades are required in order to interleave their corresponding data within the scientific stream. Some of the free code points (see Table 2) are reserved for this purpose. For further missions of similar needs, we developed a procedure involving thermal imaging sensors (Kapás et al. 2021; Takátsy et al. 2022), which is also prepared for in-orbit demonstration (on board a picosatellite platform, see

[9] https://heasarc.gsfc.nasa.gov/xanadu/xspec/

[10] The list of all GRBAlpha detected transients is available at https://monoceros.physics.muni.cz/hea/GRBAlpha/

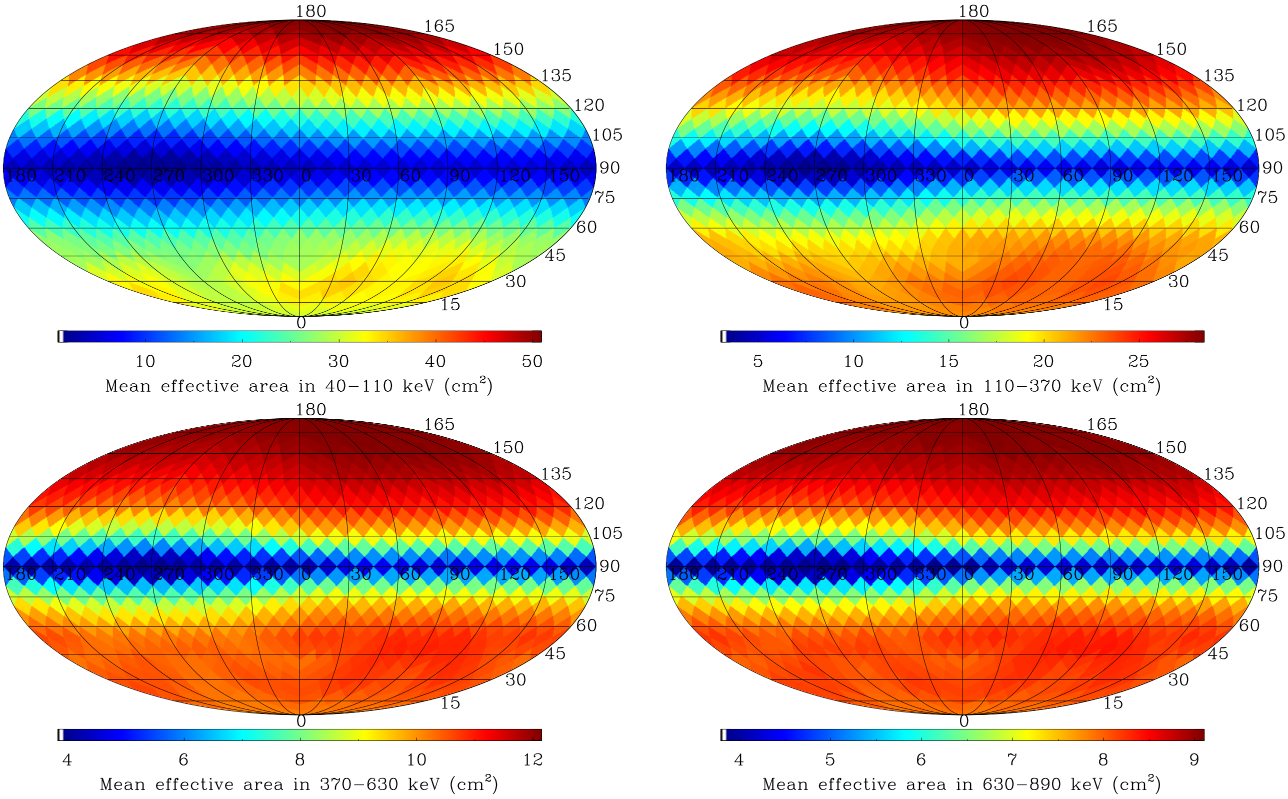


Fig. 8. Expected effective detector area with respect to the direction of the incident gamma radiation for various energy ranges: 40–110 keV (*top left panel*), 110–370 keV (*top right panel*), 370–630 keV (*bottom left panel*) and 630–890 keV (*bottom right panel*). These ϑ (zenith angle, vertical) and φ (azimuth angle, horizontal) plots are displayed in the reference frame of the satellite where $Z+$ axis (i.e., the face of the detector) is equivalent to the $\vartheta = 180°$ angle at the top pole of spherical plots (see also Fig. 5). It is clear that at lower energies, the satellite itself has a transparency around 60–70% while at higher energies it is almost transparent and the structure of the plots is dominated by the geometric cross section of the scintillator crystal.

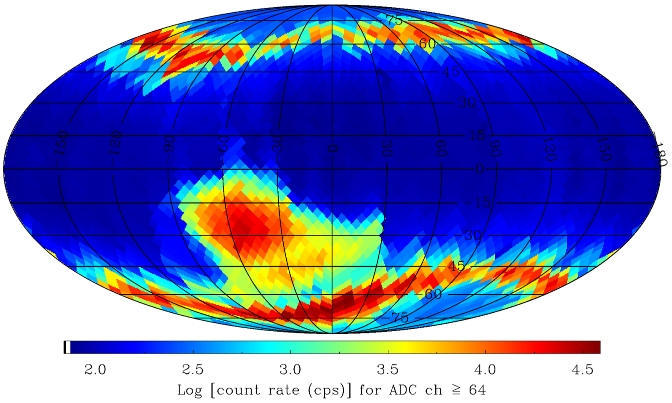


Fig. 9. Particle background, extra-galactic X-ray, and secondary (albedo) X-ray background radiation as measured by the detector system of GRBAlpha. The data plotted here were acquired during the commissioning phase and contain nearly two days of continuous measurements along the orbit of GRBAlpha. The northern and southern polar regions and the South Atlantic Anomaly are clearly visible with the elevated background levels. Otherwise, the background level is around 100 counts s^{-1} in the full spectral range. On this map an equal-area Mollweide geographical projection is used where the prime meridian and the equator cross the center.

Nanosats Database 2022) and scheduled for launch in June 2023. We also plan to extend the radio telemetry beacons with scientific information in parallel with the extension of FEC within the AX.25 frame itself (and not in addition to AX.25, as in the case of FX.25). These extensions will be reduced to special code patterns (like the Manchester code) due to the presence of bit-stuffing in the HDLC framing.

Other nanosatellites that have been developed to detect GRBs and are expected to be launched in the near future include the Educational Irish Research Satellite 1 (EIRSAT-1), which will carry a gamma-ray module (GMOD) that uses SensL B-series SiPM detectors and a CeBr scintillator (Murphy et al. 2021, 2022). A larger and more ambitious nanosatellite mission is NASA's BurstCube, a 6U CubeSat carrying a GRB detector made of four CsI scintillators, each with an effective area of 90 cm^2 (Racusin et al. 2017). Planned nanosatellite constellations include HERMES, which will initially consist of a fleet of 6 3U CubeSats on a low-Earth equatorial orbit. Their detector will use silicon drift detectors to detect both the X-rays from the sky and the optical photons produced in the GAGG scintillator crystals by gamma-rays (Fiore et al. 2020). The Chinese student-led Gamma-Ray Integrated Detectors (GRID) consists of GRB detectors as secondary payloads on larger 6U CubeSats. Six satellites with eight GRID detectors in total have been launched so far, and the plan is to fly the GRB detectors on an additional one to two dozen CubeSats (Wen et al. 2019). One of the most advantageous properties of the employment of a network of satellites is the availability of full-sky coverage, while exhibiting functional redundancy at the same time. The cumulative area can be much larger for a constellation than for an individual satellite. In addition, even simple geometric constraints (e.g., whether the event is being obscured by Earth)

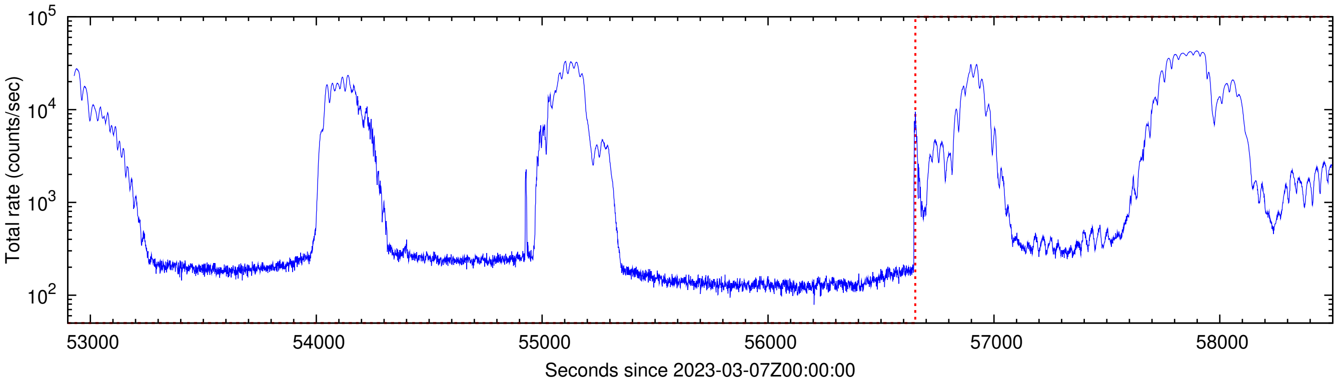


Fig. 10. Light curve observed by and retrieved from GRBAlpha related to the event of GRB 230307A. The trigger is shown with the vertical dashed red line. The total retrieved time span was a complete orbit in this case; therefore, the South Atlantic Anomaly (SAA) and four passages through polar belts are clearly visible (i.e., leaving SAA, entering and leaving the northern and southern polar rings). This prominent event has a comparable amplitude to the increased background level at the polar regions.

and attitude information (e.g., proper compilation of amplitude ratios from distinct detectors being on the same or a different spacecraft) can help the instantaneous localization with the same hardware configuration being tested on GRBAlpha now. Moreover, a timing-based localization is also feasible for such systems, exploiting proper synchronization (Pál et al. 2018; Ohno et al. 2020; Thomas et al. 2023). GRBAlpha itself is a precursor to the CAMELOT constellation. We envision it to contain at least ten 3U CubeSats, each with a geometric detection area eight times larger than that of GRBAlpha (see Werner et al. 2018; Mészáros et al. 2022).

Acknowledgements. We would like to thank our reviewer for the thorough report of our paper and all of the suggestions for improvements. Satellite components and payload development has been supported by the KEP-7/2018 and KEP2/2020 grants of the Hungarian Academy of Sciences and the grant SA-40/2021 of the Eötvös Loránd Research Network, Hungary. We acknowledge the support of the Eötvös Loránd Research Network grant IF-7/2020 for providing financial background for the ground infrastructure. We are grateful to the team developing and operating the SatNOGS network as well as the operators and maintainers of the various stations, especially Brian Yeomans (2433, 2760), David Murphy and the EIRSAT-1 team (2271), Institute for Telecommunication Research, Australia (1382), Utah State University Get Away Special Team (2550) and Small Spacecraft Systems Research Center (SSSRC) at Osaka Metropolitan University (2726). We are also thankful for the many individuals and associations from the radio amateur community providing further housekeeping/telemetry packets received from our satellite. The project has also gained support by the European Union's Horizon 2020 programme under the AHEAD2020 project (grant agreement no. 871158) and by the MUNI Award for Science and Humanities funded by the Grant Agency of Masaryk University. G.D. is supported by the Ghent University Special Research Funds (BOF) project BOF/STA/202009/040 and the Fonds Wetenschappelijk Onderzoek (FWO) iBOF project BOF20/IBF/124. This work was supported by the Internal Grant Agency of Brno University of Technology, project no. FEKT-S-20-6526. This research has been also supported by JSPS and HAS under Japan-Hungary Research Cooperative Program, JSPS KAKENHI Grant Number 17H06362, 19H01908, and 21KK0051.

References

An, Z.-H., Antier, S., Bi, X.-Z., et al. 2023, Nat. Sci. Rev., submitted [arXiv:2303.01203]

Arnaud, K. A. 1996, ASP Conf. Ser., 101, 17

CubeSat Design Specification 2022, CubeSat Design Specification, Revision 14.1, accessed: February 2022 https://static1.squarespace.com/static/5418c831e4b0fa4ecac1bacd/t/62193b7fc9e72e0053f00910/1645820809779/CDS+REV14_1+2022-02-09.pdf

Dafcikova, M., Ripa, J., Pal, A., et al. 2023, GRB Coordinates Network, 33418, 1

Fiore, F., Burderi, L., Lavagna, M., et al. 2020, SPIE Conf. Ser., 11444, 114441R

Frederiks, D., Svinkin, D., Lysenko, A. L., et al. 2023, ApJ, 949, L7

Gotz, D., Mereghetti, S., Savchenko, V., et al. 2022, GRB Coordinates Network, 32660, 1

Kapás, K., Bozóki, T., Dálya, G., et al. 2021, Exp. Astron., 51, 515

Kozyrev, A. S., Golovin, D. V., Litvak, M. L., et al. 2022, GRB Coordinates Network, 32805, 1

Lesage, S., Veres, P., Roberts, O. J., et al. 2022, GRB Coordinates Network, 32642, 1

Mészáros, L., Pál, A., Werner, N., et al. 2022, SPIE Conf. Ser., 12181, 121811L

Mitchell, L. J., Phlips, B. F., & Johnson, W. N. 2022, GRB Coordinates Network, 32746, 1

Murphy, D., Ulyanov, A., McBreen, S., et al. 2021, Exp. Astron., 52, 59

Murphy, D., Ulyanov, A., McBreen, S., et al. 2022, Exp. Astron., 53, 961

Nanosats Database 2022, MRC-100, https://www.nanosats.eu/sat/mrc-100, accessed: December 2022

Ohno, M., Werner, N., Pál, A., et al. 2020, SPIE Conf. Ser., 11454, 114541Z

Pál, A., Mészáros, L., Tarcai, N., et al. 2018, ArXiv e-prints [arXiv:1806.03685]

Pál, A., Ohno, M., Mészáros, L., et al. 2020, SPIE Conf. Ser., 11444, 114444V

Piano, G., Verrecchia, F., Bulgarelli, A., et al. 2022, GRB Coordinates Network, 32657, 1

Racusin, J., Perkins, J. S., Briggs, M. S., et al. 2017, ArXiv e-prints, [arXiv:1708.09292]

Řípa, J., Pál, A., Ohno, M., et al. 2022a, SPIE Conf. Ser., 12181, 121811K

Řípa, J., Pal, A., Werner, N., et al. 2022b, GRB Coordinates Network, 32685, 1

Řípa, J., Takahashi, H., Fukazawa, Y., et al. 2023, A&A, 677, L2

Takátsy, J., Bozóki, T., Dálya, G., et al. 2022, Exp. Astron., 53, 209

Thomas, M., Trenti, M., Sanna, A., et al. 2023, PASA, 40, e008

Tiengo, A., Pintore, F., Vaia, B., et al. 2023, ApJ, 946, L30

Torigoe, K., Fukazawa, Y., Galgóczi, G., et al. 2019, Nucl. Instrum. Methods Phys. Res. A, 924, 316

Ursi, A., Panebianco, G., Pittori, C., et al. 2022, GRB Coordinates Network, 32650, 1

Veres, P., Burns, E., Bissaldi, E., et al. 2022, GRB Coordinates Network, 32636, 1

Wen, J., Long, X., Zheng, X., et al. 2019, Exp. Astron., 48, 77

Werner, N., Řípa, J., Pál, A., et al. 2018, SPIE Conf. Ser., 10699, 106992P

Williams, M. A., Kennea, J. A., Dichiara, S., et al. 2023, ApJ, 946, L24

Xiao, H., Krucker, S., & Daniel, R. 2022, GRB Coordinates Network, 32661, 1