INTEGRATING LOCALIZATION INTO WIRELESS COMMUNICATION OF IEEE 802.15.4 TIME SLOTTED CHANNEL HOPPING NETWORKS

Grega Morano

Doctoral Dissertation
Jožef Stefan International Postgraduate School
Ljubljana, Slovenia

Supervisor: Assoc. Prof. Dr. Andrej Hrovat, Jožef Stefan Institute and Jožef Stefan International Postgraduate School, Ljubljana, Slovenia
Co-Supervisor: Prof. Dr. Tomaž Javornik, Jožef Stefan Institute and Jožef Stefan International Postgraduate School, Ljubljana, Slovenia

Evaluation Board:
Prof. Dr. Aleš Švigelj, Chair, Jožef Stefan Institute and Jožef Stefan International Postgraduate School, Ljubljana, Slovenia
Prof. Dr. Boštjan Batagelj, Member, Faculty of Electrical Engineering, University of Ljubljana, Slovenia
Prof. Dr. Gordana Gardašević, Member, Faculty of Electrical Engineering, University of Banja Luka, Bosnia and Herzegovina

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
JOŽEF STEFAN INTERNATIONAL POSTGRADUATE SCHOOL



Grega Morano

INTEGRATING LOCALIZATION INTO WIRELESS COMMUNICATION OF IEEE 802.15.4 TIME SLOTTED CHANNEL HOPPING NETWORKS

Doctoral Dissertation

UMESTITEV LOKALIZACIJE V BREZŽIČNO KOMUNIKACIJO OMREŽIJ IEEE 802.15.4 S ČASOVNIM PREKLAPLJANJEM MED KANALI

Doktorska disertacija

Supervisor: Assoc. Prof. Dr. Andrej Hrovat

Co-Supervisor: Prof. Dr. Tomaž Javornik

Ljubljana, Slovenia, January 2026

To my parents

Acknowledgments

Over the course of this research, many people contributed their time, expertise, and support, and I would like to thank them sincerely.

First and foremost, I would like to express gratitude to my supervisor Prof. Dr. Andrej Hrovat and co-supervisor Prof. Dr. Tomaž Javornik for their guidance, assistance and invaluable support during my doctoral studies. Your insightful questions and perspectives strengthened this thesis and helped refine my critical thinking and advance my academic growth.

I would like to thank the members of the dissertation committee, Prof. Dr. Aleš Švigelj, Prof. Dr. Boštjan Batagelj and Prof. Dr. Gordana Gardašević for their insightful comments and suggestions that improved the quality of this thesis.

I would also like to thank to the Department of Communication Systems at the Jožef Stefan Institute, especially Prof. Dr. Mihael Mohorčič, for the wonderful collaboration during my studies, and to my colleagues and fellow researchers from the Communication Technology laboratory for creating a supportive and stimulating research environment. I am especially grateful to Aleš Simončič and Dr. Teodora Kocevska, for their assistance, encouragement, and the many conversations that helped me see problems more clearly. Thank you for the wonderful years we spent together.

Finally, I am deeply thankful to my family and friends for their unwavering support and encouragement throughout the completion of this thesis, and for reminding me to celebrate the small wins along the way.

Abstract

The evolution of wireless networks toward large-scale, heterogeneous Internet of Things (IoT) systems has created a need for communication infrastructures that not only support data exchange but also perceive and interpret the surrounding environment. Integrated Sensing and Communication (ISAC) has emerged as a key paradigm, aiming to unify wireless communication and radio sensing within a common framework. While ISAC is gaining attention in high-throughput and complex telecommunication systems, its application in low-power, constrained IoT networks remains an open research challenge. Limited resources, stringent energy constraints, and the use of low-cost hardware make the seamless integration of sensing functions alongside communication particularly demanding. This dissertation addresses the challenges of constrained IoT protocols by developing methods to implement accurate and energy-efficient localization and sensing capabilities into the IEEE 802.15.4 standard and its Time Slotted Channel Hopping (TSCH) protocol.

The first part of the dissertation demonstrates how the Phase-Based Ranging (PBR) method can be integrated into TSCH communication, enabling distance estimation with each packet exchange. The use of compressed sampling technique reduces measurement overhead while maintaining sub-meter accuracy. The second part extends the integration paradigm to Angle-of-Arrival (AoA) estimation by embedding a phase measurement process into the TSCH slot, enabling sequential phase sampling across multiple antennas. Carrier Frequency Offset (CFO) distortions are mitigated with a two-stage calibration procedure, enabled by a newly developed CFO estimation algorithm. With the developed channel sampling methods, a hybrid localization framework that combines distance and angle estimation is proposed. Leveraging the hierarchical topology of TSCH networks, the designed system enables simultaneous communication and localization with a single anchor device, without disrupting network operation. The fourth part addresses a central ISAC challenge: mutual interference between communication and sensing during concurrent operation in shared spectrum. The proposed one-way channel reconstruction algorithm improves distance estimation in multipath environments, outperforming existing algorithms at low Signal-to-Noise Ratio (SNR) conditions.

The developed methods are implemented on low-cost IoT platforms and validated through extensive experimental campaigns. The results confirm that sub-meter localization accuracy can be achieved with minimal modifications to the communication protocol. Open-source software implementations and publicly available measurement datasets support reproducibility and promote further development of ISAC systems. The provided resources establish a benchmark for future studies, enabling consistent comparison and advancement of localization algorithms under realistic scenarios. The dissertation demonstrates that accurate localization and sensing can be achieved within existing IoT systems, laying the foundation for a new generation of energy-efficient, self-aware networks that combine connectivity and localization within a unified ISAC framework.

Povzetek

Razvoj brezžičnih omrežij v obsežne in heterogene sisteme interneta stvari (ang. Internet of Things, IoT) izkazuje potrebo po komunikacijskih infrastrukturah, ki so sposobne tako izmenjave podatkov kot tudi zaznavanja in razumevanja okolice. Integrirano zaznavanje in komunikacija (ang. Integrated Sensing and Communication, ISAC) se je pojavilo kot obetaven pristop, katerega cilj je združiti brezžično komunikacijo in radarsko zaznavanje v enoten sistem. Čeprav ISAC v zadnjih letih priteguje veliko pozornosti v visokozmogljivih in kompleksnih telekomunikacijskih sistemih, njegova uvedba v nizkoenergijskih omrežjih IoT ostaja odprt raziskovalni izziv. Omejeni računski in energijski viri ter uporaba cenovno ugodne in strojno omejene opreme močno otežujejo izvedbo sočasne lokalizacije in komunikacije. Disertacija obravnava izzive z razvojem metod za uvedbo natančnih in energijsko učinkovitih funkcij lokalizacije in zaznavanja v standard IEEE 802.15.4 in njegov protokol preskakovanja kanala s časovno režo (ang. Time Slotted Channel Hopping, TSCH).

Prvi del disertacije obravnava umestitev metode merjenja razdalje na osnovi faze (ang. Phase-Based Ranging, PBR) v komunikacijski protokol TSCH. Predlagani pristop omogoča oceno razdalje ob vsakem poslanem paketu. Z uporabo tehnik stisnjenega vzorčenja se bistveno zmanjša število potrebnih meritev, pri čemer se ohrani natančnost določanja razdalje pod enim metrom. V drugem delu disertacija predlaga integracijo ocene kota prihoda signala (ang. angle-of-arrival, AoA) z vpeljavo postopkov merjenja faze v časovne reže protokola TSCH. Vpliv napak zaradi odmika nosilne frekvence (ang. Carrier Frequency Offset, CFO) je zmanjšan z dvostopenjskim postopkom kalibracije, ki temelji na novo razvitem algoritmu za ocenjevanje CFO. Na podlagi razvitih metod vzorčenja kanala je zasnovana hibridna lokalizacijska shema, ki združuje ocenjevanje razdalje in kota prihoda signala. Z izkoriščanjem topologije omrežij TSCH predlagani sistem omogoča sočasno komunikacijo in lokalizacijo z uporabo ene same sidrne naprave, ne da bi pri tem posegal v delovanje komunikacijskega dela omrežja. Četrti del naslavlja osrednji izziv koncepta ISAC, in sicer medsebojno interferenco med komunikacijo in zaznavanjem pri sočasnem delovanju v istem spektru. Predlagani algoritem za rekonstrukcijo kanala izboljša točnost ocenjevanja razdalje v primerjavi z obstoječimi pristopi in izkazuje zaneslivejše delovanje v večpotnih okoljih z nizkim razmerjem signal-šum (ang. Signal-to-Noise Ratio, SNR).

Razvite metode so implementirane na cenovno ugodnih IoT platformah, njihovo delovanje pa je ovrednoteno z obsežnimi meritvami v realnih okoljih. Rezultati potrjujejo, da je z IoT platformami mogoče doseči natančnost lokalizacije boljšo od enega metra, ob zgolj minimalnih posegih v obstoječ komunikacijski protokol. Odprtokodne programske implementacije in javno dostopni merilni nabori podatkov, nastali v okviru disertacije, zagotavljajo ponovljivost in spodbujajo nadaljnji razvoj sistemov ISAC. Vzpostavljeni viri predstavljajo izhodišče za prihodnje raziskave, saj omogočajo dosledno primerjavo in nadaljnje izboljševanje lokalizacijkih algoritmov v realnih scenarijih. Rezultati disertacije dokazujejo, da je znotraj obstoječih sistemov IoT mogoče zagotoviti natančno lokalizacijo in zaznavanje, kar postavlja temelj za razvoj nove generacije energijsko učinkovitih in samozavednih omrežij IoT, ki v enotnem okviru ISAC združujejo povezljivost in lokalizacijo.

Contents

Abbreviations **xv**

1 Introduction **1**
1.1 Wireless Localization . . . 2
1.2 Integrated Sensing and Communication . . . 4
1.3 Enabling IoT Technologies . . . 5
1.4 Constrained IoT Protocols . . . 7
1.5 Motivation . . . 9
1.6 Aims and Objectives . . . 10
1.7 Hypothesis . . . 11
1.8 Scientific Contributions . . . 12
1.9 Dissertation Structure . . . 13

2 Integration of Phase-based Distance Estimation into TSCH Communication **15**
2.1 Introduction . . . 17
2.2 Related Work . . . 18
2.3 Challenges of Including Phase Measurements into TSCH Communication . . . 19
2.4 Proposed Implementation of Phase Measurement Process . . . 21
2.5 Validation of Proposed Implementations . . . 22
2.6 Conclusion . . . 25

3 Integration of Angle-of-Arrival Estimation into TSCH Communication **29**
3.1 Introduction . . . 31
3.2 AoA Integration . . . 32
3.3 Measurement Impairment Mitigation . . . 33
3.4 Validation Procedure . . . 35
3.5 Conclusion . . . 37

4 Hybrid Localization with TSCH Communication **39**
4.1 Introduction . . . 41
4.2 Related Work . . . 43
4.3 Localization in TSCH . . . 45
4.4 Integration of Localization Functionality . . . 47
4.5 Experimental Setup . . . 49
4.6 Experimental Results and Analysis . . . 51
4.7 Conclusions . . . 55

5 One-way Channel Reconstruction for Robust Phase-based Distance Estimation **59**
5.1 Introduction . . . 61
5.2 Phase-Based Ranging . . . 63

5.3 Robust OWCFR Reconstruction 67
5.4 Computational Complexity 70
5.5 Evaluation of the Proposed Method 71
5.6 Discussion 75
5.7 Conclusion 76

6 Conclusions and Future Work **79**
6.1 Summary of Contributions 79
6.2 Future Work 80

References **83**

Bibliography **91**

Biography **95**

Abbreviations

2D	Two Dimension
3GPP	Third Generation Partnership Project
5G	Fifth Generation Wireless Systems
6G	Sixth Generation Wireless Systems
AoA	Angle-of-Arrival
AoD	Angle-of-Departure
BE	Beacon Enabled
BLE	Bluetooth Low Energy
CCC	Car Connectivity Consortium
CFO	Carrier Frequency Offset
CIR	Channel Impulse Response
CW	Continuous Wave
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSI	Channel State Information
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Techniques
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
GNSS	Global Navigation Satellite System
IoT	Internet of Things
IIoT	Industrial Internet of Things
IMU	Inertial Measurement Unit
IR	Infrared
ISAC	Integrated Sensing and Communication
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union

IETF	Internet Engineering Task Force
LoS	Line-of-Sight
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Medium Access Control
MCPD	Multi-Carrier Phase Difference
MUSIC	MUltiple SIgnal Classification
NBE	Non-Beacon Enabled
OS	Operating System
OSI	Open Systems Interconnection
OWCFR	One-Way Channel Frequency Response
PHY	Physical
PBR	Phase-Based Ranging
PMP	Phase Measurement Process
RF	Radio Frequency
RPL	Routing Protocol for Low-Power and Lossy Networks
RSSI	Received Signal Strength Indicator
RTT	Round-Trip Time
SAGE	Apace-Alternating Generalized Expectation-maximization
SFO	Sampling Frequency Offset
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
TDMA	Time Division Multiple Access
ToF	Time-of-Flight
TSCH	Time Slotted Channel Hopping
TWCFR	Two-Way Channel Frequency Response
UWB	Ultra-Wideband
VLP	Visible Light Positioning
WSN	Wireless Sensor Network

Chapter 1

Introduction

The Internet of Things (IoT) extends connectivity beyond people and computers to billions of devices, sensors, and machines, creating a network where the physical world and digital intelligence continuously interact. Everyday objects can capture data from their surroundings through sensing and measurement equipment, and the IoT provides the communication means to exchange information and deliver commands back to devices. In this way, the IoT transforms ordinary environments into adaptive systems that can continuously monitor and control their operations. Connectivity lays the foundation for context-aware, responsive infrastructures, capable of evolving into autonomous systems that support novel scientific, industrial, and societal applications [1]. Early IoT solutions were primarily focused on connecting devices and enabling basic communication, but today the greater challenge lies in interpreting the massive streams of data generated by these networks [2], [3]. Transforming raw measurements into meaningful knowledge depends not only on the type of data collected, but also on the location from which it originates. Knowing the value of a temperature reading, the status of a machine, or the presence of an asset is far more useful when its location is also known. Localization provides important spatial context, turning isolated data points into structured information that can reveal patterns, capture dynamics, and support intelligent decision-making [4].

On a factory floor, for example, linking machine status with exact location helps maintenance teams identify failing equipment immediately and prevent costly downtime. Combining sensor readings with position allows factory managers to spot bottlenecks in production lines and optimize workflow. In agriculture, knowing the precise position of livestock or crop monitoring sensors helps farmers optimize field management, reduce resource waste, and respond quickly to emerging conditions. Localization therefore emerges as a natural complement to communication and makes IoT systems truly actionable. Far from being just an add-on, localization functionality further empowers IoT systems by enabling advanced applications, such as coordination of mobile devices, tracking of valuable assets, and delivery of context-aware services that adapt to the position of users and machines [4]. In logistics and smart warehouses, precise location estimation enables automated inventory management with collaborative robots and real-time route optimization. In healthcare, patient monitoring combined with localization supports fall detection, emergency response, and tracking of vital equipment inside hospitals. Localization facilitates smart homes by enabling context-aware automation and intelligent interaction with the environment, such as smart machines for household chores, touchless home appliances, or adaptive lighting and heating solutions that follow the movements of residents. An illustrative example of an indoor environment enriched by localization is presented in Figure 1.1. Whether identifying the source of an environmental reading, coordinating fleets of connected machines, or enabling personalized user services, location awareness transforms IoT from a network

of devices into a coherent system that reflects and responds to the real world [5].

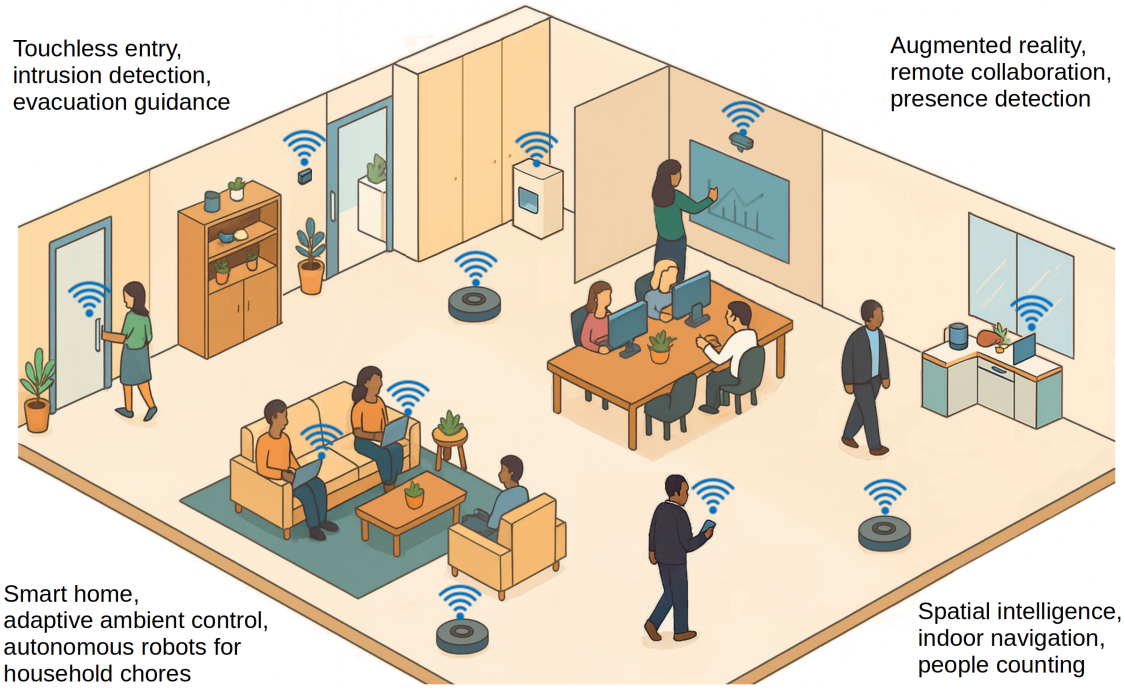


Figure 1.1: Illustration of an indoor smart environment where IoT connectivity and localization enable a broad range of context-aware services.

1.1 Wireless Localization

Localization is the process of determining the position of an object or node, referred to as the target, within a defined coordinate system or environment. Localization assigns each target a placement in physical space and encompasses the models, principles, and methods for obtaining position and spatial relationships. Different localization schemes can be categorized along six complementary dimensions: interaction, reference frame, architecture, collaboration, methodology and technology, as shown in Figure 1.2. In terms of node interaction, active localization schemes require the target to carry dedicated equipment and participate in the process, while in passive localization, the target carries no equipment and its position is inferred indirectly through environmental sensing. Regarding the reference frame, anchor-based (or absolute) localization schemes rely on dedicated devices called anchors with known coordinates that provide a frame of reference, allowing positions to be mapped to global coordinates. Anchor-free schemes establish a relative coordinate system among nodes, preserving spatial geometry without global alignment. Based on architectural design, localization schemes can be divided into centralized approaches, where a central station collects raw or preprocessed measurements and computes positions for all targets, and distributed approaches, where localization computations are performed locally at the nodes. From the perspective of collaboration, non-cooperative approaches treat each target independently, while cooperative localization allows multiple targets to share information and jointly estimate their positions, improving accuracy and robustness at the cost of additional communication and complexity. In terms of methodology, range-free localization schemes rely on indirectly observed features from a target and map them to a position using a pre-learned model. They can be further grouped

into proximity-based methods such as fingerprinting, connectivity-based methods such as hop-counting, and landmark-based methods such as pattern matching. Range-based (or geometric) localization schemes derive positions from physical measurements of distances and angles between nodes, offering higher accuracy at the expense of complexity. These schemes include lateration, which uses distances to compute positions, angulation, which relies on measured angles, and hybrid approaches that combine both distance and angle information. The choice of localization schemes in IoT applications depends on the specific requirements of the system and the constraints of the environment. No single scheme is universally optimal, and practical deployments often seek a balance among dimensions to match the needs of the intended application.

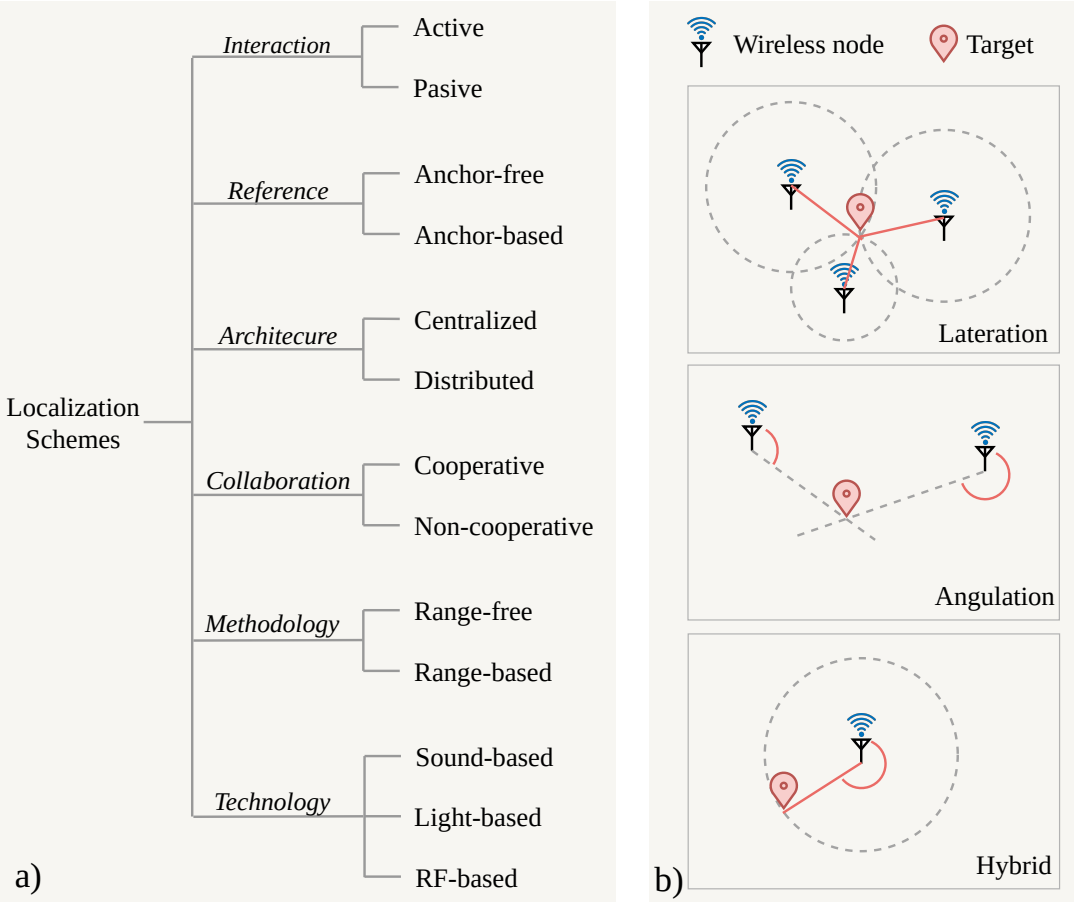


Figure 1.2: a) Classification of localization schemes in IoT networks. b) Examples of rage-based localization schemes that determine the target position using distance and/or angle measurements.

Lastly, localization also depends on measurements that describe and capture how the target interacts with its surroundings, which introduces a sixth dimension of classification based on the underlying technology used to sense the environment. IoT solutions employ various sensing modalities that are utilized for localization, including ultrasound and acoustic positioning, Infrared (IR), image-based localization, Visible Light Positioning (VLP), Global Navigation Satellite System (GNSS) and Inertial Measurement Unit (IMU) [4]–[7]. These technologies differ in accuracy, range, and scalability, but all require additional hardware to be added to existing infrastructure, increasing the cost, design complexity, and energy consumption of IoT devices. A more effective and scalable alternative is to

exploit the Radio Frequency (RF) technologies already embedded in IoT networks, reusing the same wireless signals that devices already exchange during communication. Since radio propagation is governed by geometry and the environment, the received RF signals encode information about distance, direction, and surrounding objects. Thus, the communication signal can also serve as a sensing modality, enabling localization through the existing communication infrastructure. From this perspective, localization emerges as a native capability of the communication system, which constitutes the central premise of the Integrated Sensing and Communication (ISAC) paradigm.

1.2 Integrated Sensing and Communication

In wireless systems, communication and sensing have evolved along parallel but separate paths, even though both rely on electromagnetic wave propagation. They are typically designed and evaluated using different performance metrics: communication focuses on reliable and efficient data exchange, while sensing aims to interpret the physical environment. However, recent technological trends are blurring this boundary, motivating the concept of ISAC [8]–[10]. The unified use of radio signals for both sensing and communication within a single framework offers several advantages:

- A single combined system that reuses the antennas, RF front-ends and signal processing units reduces the cost and size of devices and enables easier deployment and maintenance [11], [12].
- With the exponential growth of wireless devices and the increasing bandwidth requirements, spectrum scarcity has become a pressing issue. ISAC addresses the problem by enabling simultaneous sensing and communication over the same spectral resources, optimizing the use of the spectrum [11], [13].
- The synergy between the two systems enables mutual assistance, as sensing can provide improved safety, enhanced beam alignment and interference mitigation for communication, while communication can assist sensing by enabling information exchange between devices [14], [15].

The realization of ISAC requires selecting an appropriate integration strategy, typically classified into three levels of integration: coexistence, cooperation, and co-design [13]. In the coexistence model, communication and sensing functions operate independently while sharing the same spectral resources. In cooperation, the two systems exchange information to optimize their respective operations. The most integrated form is co-design, where communication and sensing share not only spectrum, but also waveforms, hardware components, and signal processing techniques. Within this class, a further categorization is made based on design priority [10]: (i) communication-centric, where sensing is added to existing communication systems without compromising data transmission, (ii) radar-centric, where communication capabilities are embedded into radar platforms, (iii) and joint design, where both functions are developed from the ground up as part of a unified system.

Despite the benefits of ISAC, its widespread adoption is limited by multiple challenges, particularly in meeting the stringent and often conflicting performance requirements of sensing and communication tasks. Interference management is a key issue, as simultaneous operation can cause severe self-interference, requiring advanced mitigation techniques such as adaptive beamforming, full-duplex isolation or time-slotted scheduling [9]. New signal processing algorithms must be co-developed and optimized to ensure robust dual functionality [16]. Resource allocation is another major challenge, where the trade-offs between sensing accuracy and communication throughput need to be dynamically balanced by

intelligent, context-aware strategies [17]. ISAC systems must also address practical hardware limitations, including synchronization errors, non-ideal RF components, and limited dynamic range, all of which can degrade sensing accuracy and communication reliability if not properly managed [18]. Furthermore, the new functionalities of ISAC systems raise security and privacy concerns, since pervasive sensing could allow unauthorized tracking or surveillance [19]. Finally, the lack of standardization and interoperability frameworks remains a major obstacle [20]. Coordinated efforts from academia, industry and regulators are needed to define standardized ISAC protocols that enable broad deployment across heterogeneous platforms [18].

Prominent standardization bodies have already acknowledged the growing importance of ISAC and have taken active steps to address these challenges through dedicated working groups and technical initiatives. The Radiocommunication Sector of International Telecommunication Union (ITU) has included ISAC as one of the six core usage scenarios in the "IMT-2030 Framework" [21]. The published recommendations outline the objectives for the future development of Fifth Generation Wireless Systems (5G) and Sixth Generation Wireless Systems (6G), highlighting the role of ISAC in the development of advanced sensing services. In parallel, Third Generation Partnership Project (3GPP) has begun formalizing ISAC standards in Release 19. Technical specification 22.137 defines use cases and service requirements to enable sensing functions in mobile networks [22]. Similarly, European Telecommunications Standards Institute (ETSI) has launched the Industry Specification Group on ISAC, which recently published a deliverable listing 18 advanced ISAC use cases, deployment scenarios, and key performance indicators to guide subsequent 3GPP and ITU work [23].

While mobile telecommunication standardization provides an important baseline for wide-area ISAC, many sensing driven applications are implemented in practice within IoT deployments that rely on short-range connectivity stacks rather than cellular access. Indoor positioning, device-to-device ranging, and proximity services are therefore shaped not only by the evolution of 5G and 6G, but also by the measurement primitives provided by widely deployed IoT standards. Although short range technologies have historically been designed primarily for connectivity, recent amendments increasingly incorporate localization relevant measurements and procedures, enabling ISAC-style operation within existing IoT technologies.

1.3 Enabling IoT Technologies

The choice of wireless technology in an IoT network depends on application requirements such as data rate, energy budget, device cost, and deployment density. The same constraints also determine which localization techniques are feasible, since achievable accuracy depends on factors such as available bandwidth, timing support, antenna configuration, and deployment topology. As a result, different technologies tend to rely on different measurement principles for localization. Several mainstream IoT connectivity stacks have already begun introducing various procedures and localization-relevant measurements as part of their protocol specifications.

Wi-Fi communication technology, based on the IEEE 802.11 standard, is widely adopted in environments requiring broadband connectivity and Internet access, such as enterprise networks, residential deployments, and public infrastructure. High data rates, broad ecosystem support, and scalable deployments make Wi-Fi suitable for applications where energy consumption is not the primary constraint. Alongside connectivity evolution, IEEE 802.11 has progressively incorporated measurement capabilities that support localization. Early deployments exposed Received Signal Strength Indicator (RSSI) values,

providing the most basic means for localization [24], [25]. The IEEE 802.11az amendment introduced Round-Trip Time (RTT) techniques for Time-of-Flight (ToF) measurement, providing the foundation for range-based indoor positioning [26], [27]. In parallel, the IEEE 802.11ac amendment included Channel State Information (CSI) estimation techniques, which have since become the basis of many fine-grained localization schemes. With the release of IEEE 802.11bf in early 2025, measurement methods, CSI reporting, and procedures supporting sensing tasks have been standardized, enabling seamless integration of localization capabilities into future Wi-Fi systems [28].

Ultra-Wideband (UWB) communication uses very short duration pulses over a wide bandwidth. Although UWB throughput does not reach the levels of Wi-Fi, UWB capacity is sufficient for many IoT functions such as sensor messaging, control signaling, and secure access exchanges. Historically, UWB has been attractive for high-precision localization, rather than its communication capabilities, as its wide bandwidth provides fine temporal resolution, enabling accurate ToF estimation and detailed Channel Impulse Response (CIR) characterization [29], [30]. IEEE 802.15.4a established UWB as a Physical (PHY) layer option for low data rate communication with inherent ranging support in 2007 [31]. The IEEE 802.15.4z amendment, released in 2020, further improved RTT techniques for ToF estimation with improvements in accuracy, robustness and measurement security [32]. In parallel, industry organizations including the FiRa Consortium, the UWB Alliance, and the Car Connectivity Consortium (CCC) have promoted interoperability by defining application layer profiles and certification programs that complement IEEE specifications [33]. Commercial adoption in consumer devices has followed, including Apple's U1 chip and Samsung Galaxy SmartTag, reflecting the growing demand for high-accuracy, short-range localization in IoT ecosystems.

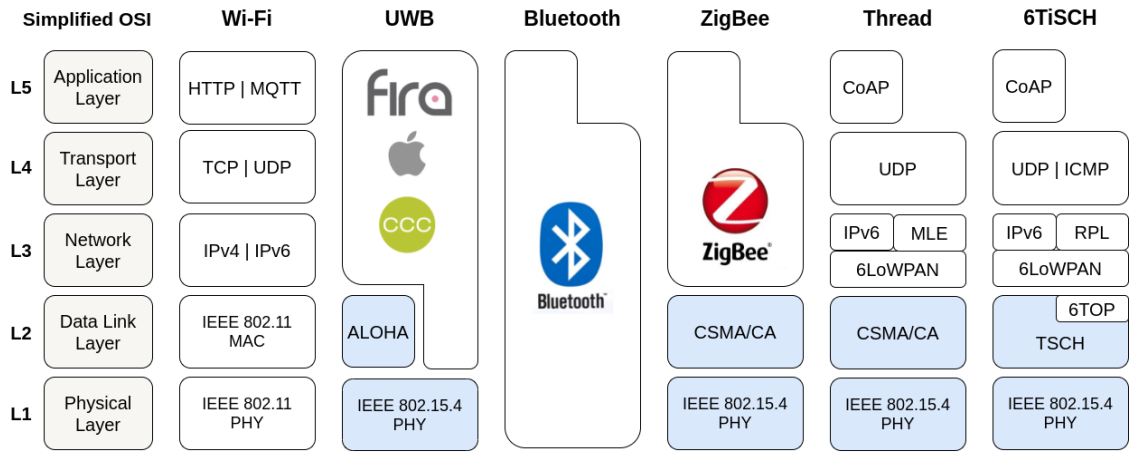


Figure 1.3: Network stacks architecture examples for common wireless IoT communication protocols.

Bluetooth is a short-range wireless technology that has become ubiquitous in consumer electronics. Bluetooth Classic has been widely used for audio and peripheral connectivity, while Bluetooth Low Energy (BLE) expanded Bluetooth adoption toward low-power IoT devices that require moderate data rates and direct integration with mobile platforms, including medical, fitness and wearable systems. Localization support has evolved gradually within the Bluetooth ecosystem. Early deployments relied on RSSI for proximity detection [34], enabling simple presence and coarse location services in commercial products such as iBeacon and Chipolo. Bluetooth 5.1 introduced direction-finding capabilities based on Angle-of-Arrival (AoA) and Angle-of-Departure (AoD) techniques, enabling substantially

improved spatial awareness when antenna arrays are available [35], [36]. In September 2024, Bluetooth 6.0 introduced Phase-Based Ranging (PBR) and RTT techniques for accurate distance estimation, bringing high-accuracy ranging capability into the mainstream Bluetooth protocol [37], [38].

Together, Wi-Fi, UWB, and BLE demonstrate a clear standardization trend toward integrating localization oriented measurements into mainstream connectivity stacks. In contrast, many practical IoT deployments in smart buildings, agriculture, and industrial monitoring rely on other resource-constrained mesh protocols, where the radio interface exposes only a limited set of wireless channel observables. As a result, localization is rarely treated as a native capability and is often delegated to higher network layers. Nevertheless, such deployments frequently require localization functionality during operation, motivating the integration of sensing into constrained IoT protocols.

1.4 Constrained IoT Protocols

Constrained IoT protocols are designed for networks consisting of devices with limited power, processing capabilities, and communication capacity. Protocols such as ZigBee, Thread, ISA 100.11a, WirelessHART, and 6TiSCH provide energy-efficient, low-data-rate connectivity that enables large-scale deployments of battery-powered nodes [39]. Their robustness and operational simplicity make these stacks suitable for smart homes, building automation, and industrial monitoring, where devices are expected to operate for years with minimal maintenance [40]. At the core of these protocols is the IEEE 802.15.4 standard, which defines the operation of Low-Rate Wireless Personal Area Networks (LR-WPANs) and specifies the PHY and Medium Access Control (MAC) layers of the Open Systems Interconnection (OSI) model, as presented in Figure 1.3. Since its first release in 2003, IEEE 802.15.4 has served as the foundation for Wireless Sensor Networks (WSNs) and Industrial Internet of Things (IIoT) systems [41].

The IEEE 802.15.4 PHY supports operation in multiple Industrial, Scientific and Medical (ISM) bands, including 868 MHz, 915 MHz, and 2.4 GHz, with additional bands introduced through amendments. The PHY layer specifies modulation, packet transmission and reception, receiver processing, and transceiver state control. The MAC layer defines frame formats and channel access mechanisms, offering operating modes to adapt to different application needs. The original IEEE 802.15.4 specification introduced two operating modes [42]. Non-Beacon Enabled (NBE) mode relies on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and is commonly used in networks, where tight synchronization is not required. Conversely, Beacon Enabled (BE) mode introduces a coordinator managed superframe structure with a beacon for time reference. The superframe includes a contention access period that uses CSMA/CA, a period based on Time Division Multiple Access (TDMA), and an inactive period that allows devices to sleep and conserve energy. Nonetheless, NBE and BE modes have key limitations: they cannot guarantee a bounded delay, their reliability is constrained by the inefficiency of CSMA/CA under contention, and they lack protection against interference and fading [43].

To address deterministic communication requirements, the IEEE 802.15.4e amendment from 2012 introduced five additional channel access modes, with Time Slotted Channel Hopping (TSCH) emerging as the most significant advancement [43], [44]. TSCH combines time-slotted access with frequency channel hopping. Time is divided into slots that are organized in a repeating slotframe, as shown in Figure 1.4. Transmissions are scheduled under network-wide synchronization, which enables predictable latency and avoids contention. Channel hopping across different frequencies improves resilience against interference and multipath fading, increasing reliability in challenging environments. With concepts origi-

nating from industrial protocols such as WirelessHART and ISA 100.11a [45], [46], TSCH brings deterministic, energy-efficient, and robust communication to IEEE 802.15.4-based networks, making it a cornerstone for IIoT [41], [47].

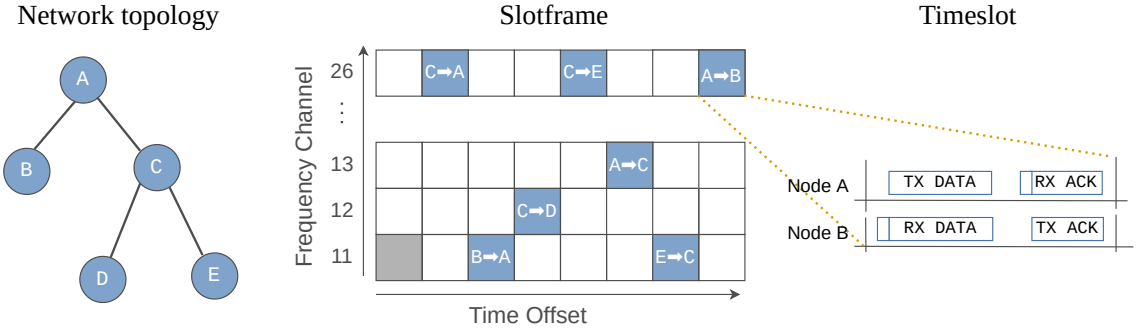


Figure 1.4: An example TSCH link schedule of a synchronized network. Timeslots define transmission and reception periods and are organized into slotframes that repeat over time.

Above the IEEE 802.15.4 PHY and MAC layers, different ecosystems define the remaining layers of the communication stack and provide interoperability through profiles and certification programs. The ZigBee stack is specified and maintained by the Connectivity Standards Alliance, which defines the network and application layer specifications on top of IEEE 802.15.4. ZigBee is commonly used in smart home and building automation systems that require mature device profiles and broad interoperability across vendors [48]. Thread targets similar application domains but adopts an IP-based architecture and provides natural integration with existing Internet services. The protocol stack is maintained by Thread Group and relies on IPv6 connectivity enabled by 6LoWPAN, which allows IPv6 operation over IEEE 802.15.4 CSMA/CA links [49]. In industrial monitoring and control, where predictable performance and high reliability are essential, 6TiSCH is a representative solution, standardized within the group of protocols defined by the Internet Engineering Task Force (IETF) [50]. 6TiSCH combines an IPv6 stack with IEEE 802.15.4 TSCH, enabling deterministic scheduling and improved robustness compared with CSMA/CA operation, and adopts Routing Protocol for Low-Power and Lossy Networks (RPL) to enable multi-hop forwarding.

Despite the widespread adoption of IEEE 802.15.4 in constrained IoT protocols, integration of localization alongside communication remains limited. LR-WPANs stacks based on IEEE 802.15.4 typically treat localization as an application layer feature, rather than as a radio capability exposed through standardized PHY and MAC primitives. Most work focuses on the RSSI technique, which is attractive due to its universal availability across all IEEE 802.15.4 radios [51]–[54]. In practice, multipath propagation and temporal signal variability substantially distort RSSI, often resulting in positioning errors on the order of several meters, which restricts its applicability to coarse proximity detection. Another research direction has investigated ToF estimation using transmitted packets [55]–[57]. These approaches have demonstrated higher accuracy than RSSI, but low-cost hardware is unable to sample time with high precision, and narrowband IEEE 802.15.4 physical layers do not provide sufficient temporal resolution for precise ranging. Although IEEE 802.15.4 specifies procedures for ToF and CIR measurements, these were designed primarily for UWB physical layers, where wide bandwidth enables accurate timing and detailed characterization of the channel. Narrowband IEEE 802.15.4 variants cannot achieve comparable measurement quality, leaving a gap between standardized measurement concepts and practical localization performance in constrained mesh deployments.

Recent advances in low-cost radio transceivers have enabled access to phase measurements of received signals, which has stimulated increased interest in phase-based localization. Studies in [58]–[61] employ PBR and report improved ranging and localization accuracy compared with RSSI and narrowband timing-based approaches. However, many proposed designs treat sensing as the dominant task and do not explicitly account for the impact on communication. In several cases, sensing procedures require long measurement intervals that interrupt or delay regular data traffic, increasing latency and reducing network responsiveness. Furthermore, many prototypes assume deployment scenarios where nodes primarily perform localization, which does not reflect typical constrained mesh operation where communication remains the primary objective. Finally, direction finding based on phase interferometry and antenna arrays has received limited attention in the context of IEEE 802.15.4 compliant devices, despite the potential of such methods for providing localization information under narrowband constraints.

1.5 Motivation

The evolution of wireless technologies has been characterized by the gradual convergence of communication and localization. In short-range IoT ecosystems, standards such as Wi-Fi, UWB, and BLE already expose physical layer measurements and procedures that enable accurate positioning, while constrained IEEE 802.15.4 based mesh networks continue to offer only limited localization capabilities. To address the current gap between localization accuracy and communication efficiency in narrowband IEEE 802.15.4 networks, the goal of this dissertation is to enable the seamless integration of localization into IEEE 802.15.4 compliant systems while preserving the primary communication function. Such integration eliminates the need for parallel localization infrastructure, reduces deployment costs, and makes localization available as a baseline capability, allowing IEEE 802.15.4 networks to evolve toward a dual-purpose solution aligned with the broader ISAC vision.

The main challenge with existing approaches is the rigid separation between communication and sensing phases, where accurate localization requires interruption or delay of data exchange, causing latency and limiting responsiveness in real-world deployments. Furthermore, many designs do not explicitly account for the networks structure, which constrains how localization can be performed in practice. In contrast, this work aims to develop a communication-centric ISAC approach that treats sensing as a parallel and lightweight process that can operate alongside existing communication. Among IEEE 802.15.4 operating modes, TSCH is a particularly suitable candidate, as it offers deterministic scheduling, strict time synchronization, and channel hopping, which provide natural opportunities for synchronous channel measurements and frequency diversity resilient to multipath fading. These features allow robust localization to be embedded directly into the TSCH protocol without fundamentally changing its communication behavior.

Network structure further constrains localization strategy. In many TSCH deployments, routing is provided by RPL, which commonly produces a tree-structured topology, where traffic flows between child nodes and parent nodes toward the root and back. Such traffic patterns limit availability of direct measurements between arbitrary node pairs, complicating lateration and angulation schemes that assume flexible pairwise ranging. A practical alternative is a hybrid localization scheme with a single reference node, typically the root or a designated parent, which directly addresses child nodes and estimates distance and angle. Such design remains compatible with existing TSCH operation and routing patterns, while enabling accurate position estimation without disruptive protocol changes.

Beyond protocol integration, a central challenge in ISAC systems is mutual interference

between communication and sensing when both functions share spectrum and operate concurrently. This challenge is especially pronounced in the crowded 2.4 GHz ISM band, where IEEE 802.15.4 networks coexist with other common IoT technologies, and where in-band interference is common in real deployments. Since such interference directly corrupts sensing observables, localization performance depends on robust signal processing methods that remain reliable under noise, interference, and measurement distortions.

1.6 Aims and Objectives

The aim of this research is to develop and validate methods that enable the integration of sensing and communication functionalities in low-power IoT networks based on the IEEE 802.15.4 standard with the TSCH protocol. By establishing a framework that enables simultaneous data transmission, sensing and localization, the thesis supports the ISAC concept through a communication-centric design. The main objectives are the design and implementation of techniques that embed distance and angle estimation into the existing TSCH communication protocol, and the development of robust signal processing methods that maintain localization accuracy under multipath and noise. The proposed unified localization framework should provide accurate position estimation with minimal changes to the protocol and network structure and should ensure reliable operation in indoor environments under realistic interference conditions.

First, the most suitable channel metrics and estimation techniques for accurate localization on narrowband devices with limited resources will be identified through a theoretical study of existing research. To enable ranging between two devices, a lightweight channel sampling procedure will be designed and integrated into the TSCH protocol, providing distance estimation with each transmitted data packet. Compressed sampling techniques that reduce energy consumption and communication interference while maintaining the desired level of ranging accuracy will be investigated. Furthermore, the integration of direction estimation techniques that provide AoA estimation alongside TSCH data exchange will be explored. An investigation of dedicated calibration steps to reduce errors caused by frequency mismatches will enable accurate angle estimation resilient to low-cost hardware imperfections. The developed channel sampling concepts will then be combined into a hybrid localization framework that can be embedded within the TSCH protocol structure, ensuring compatibility with existing communication functions. The goal is to allow position estimation using only one anchor node, exploiting the communication hierarchy in TSCH networks and providing localization functionality. Finally, signal processing algorithms that remain reliable under noise and in-band interference will be developed, which are essential for concurrent ISAC operation.

Practical validation is a crucial part of system design, ensuring that theoretical concepts hold under real-world conditions. Although simulation studies provide valuable insights, they cannot fully capture the complexity of physical environments. The validation of the proposed methods with real-world prototypes on low-cost hardware will allow exploration of interference effects, synchronization errors, and radio non-idealities on system performance. Results from measurement campaigns and simulations will support efforts to improve the current state-of-the-art algorithms for robust localization in indoor environments. Additionally, the developed ISAC system will offer a platform to evaluate and compare communication and localization performance in realistic environments, serving as a benchmark for future research. The thesis aims to establish an open and reproducible experimental foundation for future ISAC studies by making all custom modifications to the IEEE 802.15.4 standard, newly created radio drivers, obtained datasets, and proposed algorithm implementations publicly available on dedicated online platforms.

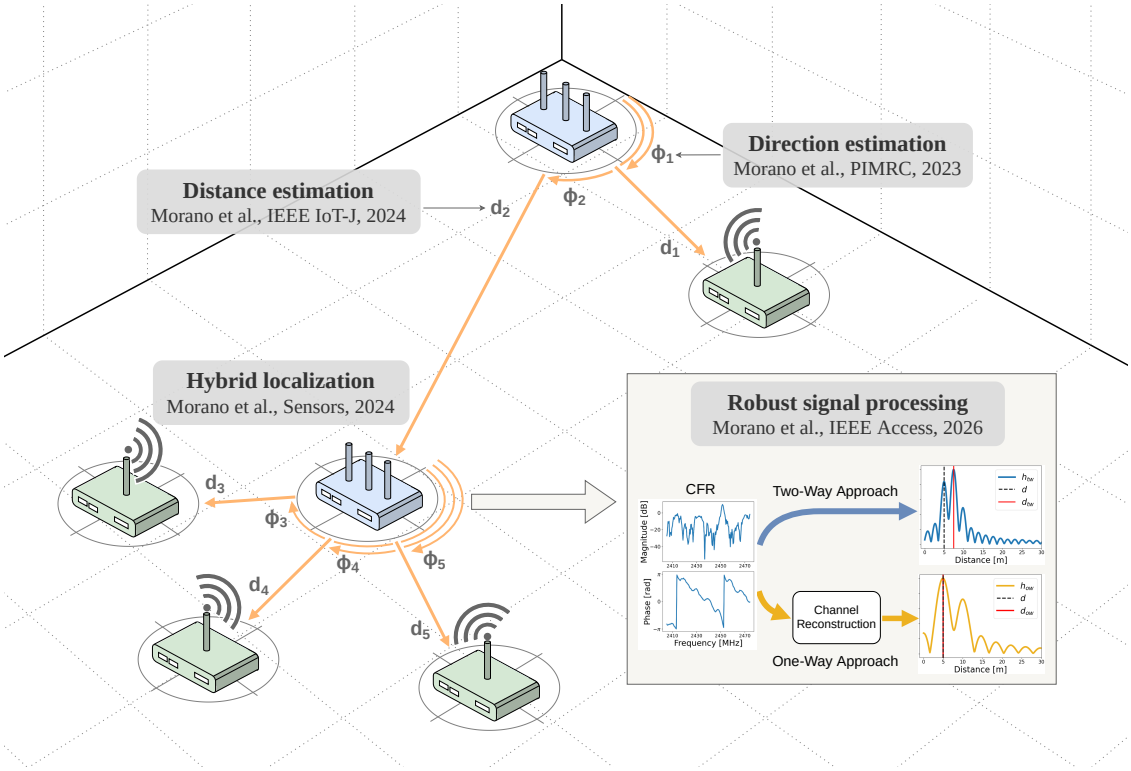


Figure 1.5: Thesis structure overview and main objectives. Four research papers are presented, each targeting a component required for integrating localization into wireless communication of IEEE 802.15.4 TSCH.

1.7 Hypothesis

Localization in wireless networks is a mature research area, yet important challenges remain in making localization methods practical for constrained IoT systems and reliable in complex indoor environments. Addressing these challenges requires integration of sensing into existing communication protocols and refinement of localization algorithms through advanced signal processing supported by real world validation. With the described set objectives, the thesis investigates the following hypotheses:

H1 **The IEEE 802.15.4 standard and TSCH MAC mode can be enhanced with integrated localization functionality.** Localization can be achieved with minimal impact on communication latency, interference, and energy consumption.

H2 **The low-cost hardware impairments that degrade measurement accuracy can be mitigated through sampling design and calibration procedures.** Relevant hardware impairments include initial phase offsets, synchronization error between devices, and carrier frequency offset effects.

H3 **A hybrid localization scheme can achieve sub-meter localization error in indoor environments.** A hybrid localization scheme combining estimated range and direction of arrival is suitable for TSCH networks.

H4 **State-of-the-art localization algorithms can be improved for indoor environments with advanced signal processing methods.** Algorithms designed to tolerate in-band interference and noise can improve robustness of ranging and localization under realistic ISAC deployment conditions.

1.8 Scientific Contributions

The contribution of this work lies in demonstrating how localization can be seamlessly embedded into the TSCH protocol, bridging the gap between constrained IoT networks with ongoing evolution of ISAC in modern wireless standards. The main contributions of the thesis are:

C1 Development of communication-centric ISAC approach for IEEE 802.15.4 TSCH networks exploiting phase measurements. The contribution supports empirical validation of ISAC concepts on constrained platforms and provides evidence relevant to future standardization of ISAC-enabled IoT systems. This contribution is composed of three parts:

- **C1.1** Development and integration of novel phase-based distance estimation method into the TSCH communication protocol.
- **C1.2** Integration of AoA estimation functionality for single RF chain devices into the TSCH communication protocol.
- **C1.3** Implementation of a novel hybrid localization scheme based on estimated distance and angle that is integrated alongside TSCH communication.

C2 Improvements to core algorithms for distance and angle estimation. The developed localization approaches mitigate hardware imperfections, noise, and interference effects, and refine state-of-the-art algorithms for robust operation under realistic deployment conditions.

C3 System-level ISAC prototypes on constrained platforms. The thesis implements a practical, system-level ISAC solutions on resource-constrained hardware. The prototypes address a key research gap, where most existing ISAC work remains theoretical and lacks empirical validation under realistic hardware limitations. The contribution is composed of three parts:

- **C3.1** Implementation of ISAC prototype based on the VESNA platform [62] equipped with an AT86RF233 radio, enabling phase-based distance estimation alongside communication.
- **C3.2** Design of ISAC prototype based on the OpenMote-B platform [39] equipped with an AT86RF215 radio and a 12-element antenna array, enabling AoA estimation integrated with communication.
- **C3.3** Development of ISAC prototype based on the VESNA platform equipped with an AT86RF215 radio and an 8-element antenna array, implementing a hybrid localization scheme within the communication framework.

C4 Empirical evaluation in simulations and real-world environments. Through experimental evaluation, the thesis reveals performance limitations and challenges in indoor environments, describing valuable findings for improvement of current signal processing and localization algorithms. In addition, the establishment of a reproducible methodology and experimental results serve as a benchmark for the research community and facilitate further comparative studies.

C5 Publicly available real-world datasets and open-source software release. The thesis generates diverse, publicly available datasets for localization in low-power networks, an important resource for the growing machine learning and signal processing community where access to real-world data remains a bottleneck. In addition, the

created software is released as an open-source solution that enables reproducibility, adaptation, and further development by other researchers and developers.

By providing a functional prototype, open-source tools and data for community engagement, this research will not only advance the state-of-the-art, but also support broader community engagement and innovation in the field.

1.9 Dissertation Structure

The overreaching themes and objectives introduced above are central to the individual papers in this cumulative thesis, each contributing to the integration of localization functionality into the IEEE 802.15.4 TSCH networks and the broader ISAC vision, where regular communication also supports sensing and localization. After the introductory remarks and motivation in Chapter 1, an integration of phase-based distance estimation technique into the TSCH protocol is described in Chapter 2. Following, Chapter 3 describes the integration of AoA estimation technique into the TSCH protocol. A hybrid localization scheme for TSCH-based network is presented in Chapter 4, demonstrating its seamless integration into the protocol. Chapter 5 introduces improvements to the distance estimation algorithm, enhancing its robustness to interference and noise. Finally, Chapter 6 concludes the thesis with final remarks and gives directions for future work. The thesis structure is depicted in Figure 1.6, highlighting the thesis flow with corresponding papers.

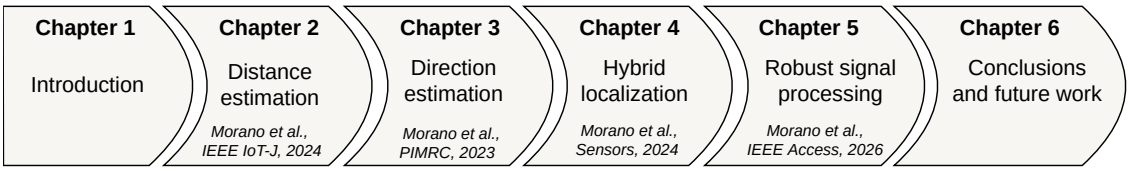


Figure 1.6: Conceptual structure of the thesis.

Chapter 2

Integration of Phase-based Distance Estimation into TSCH Communication

Distance estimation is a fundamental building block of many localization schemes, serving as the first step toward enabling positioning, navigation, and sensing services. In RF systems, distance can be estimated by analyzing different metrics of the received wireless signal. RSSI-based techniques are straightforward and already supported by the IEEE 802.15.4 standard, but their accuracy is severely limited by noise, interference, and multipath propagation, especially in dynamic indoor environments [63]. In contrast, ToF measurements can provide higher accuracy but require nanosecond timing resolution, which is difficult to achieve with narrowband IEEE 802.15.4 radios. Phase-based ranging emerges as an attractive alternative [61], [64]. With the Multi-Carrier Phase Difference (MCPD) technique the distance between two devices can be obtained with high accuracy while avoiding the strict timing requirements of ToF estimation [65].

The paper presented in this chapter exploits the advantages of MCPD and explores its seamless integration into the IEEE 802.15.4 TSCH protocol. We developed two novel methods of embedding phase measurements directly into the TSCH timeslot: phase measurement after acknowledgment and phase measurement after data packet, addressing hypotheses **H1**. The methods enable devices to estimate distance with every exchanged packet, transforming standard TSCH communication into a dual-purpose operation and delivering the contribution **C1.1**. The paper also highlights the impact of hardware impairments such as initial phase offsets, measurement delay mismatches, and synchronization errors, addressing aspects of hypothesis **H2**. Building on insights and findings from related works, we designed a lightweight channel sampling procedure to mitigate these impairments. Additionally, we applied compressed sampling techniques based on Golomb ruler design, which reduced the number of required phase measurements from hundreds to only 15 while preserving the accuracy of distance estimation. The applied compressed sampling shortened the channel sensing process and minimized its impact on communication.

We implemented the proposed solutions into the Contiki-NG stack running on low-cost VESNA devices equipped with AT86RF233 transceivers, resulting in a system-level ISAC prototype which represents contribution **C3.1**. To validate the design, we carried out extensive empirical evaluations in diverse environments, including outdoor Line-of-Sight (LoS) and challenging indoor multipath scenarios, delivering contribution **C4**. We compared the achieved ranging accuracy with two modern distance estimation algorithms adapted to support the proposed compressed sampling technique. We further enhanced robustness by applying a median filter over five consecutive measurements, which reduced

outliers caused by multipath propagation. The modified Fast Fourier Transform (FFT)-based algorithm consistently achieved median errors around 0.26 m indoors and 0.05 m outdoors.

An analysis of communication performance under the integrated design showed that phase measurement after data packet offered better responsiveness and reduced overhead compared to the phase measurement after acknowledgment method. In both cases, throughput was reduced due to the extended timeslot duration (20 ms instead of 10 ms), but the trade-off remains acceptable for TSCH systems, which prioritize reliability and deterministic scheduling over high data rates. The use of the proposed frequency set for ranging reduced the probability of interference with communication, as only two communication channels were directly affected by continuous wave transmissions used for sensing. We also analyzed the energy consumption of the added phase measurement routine. The process consumed approximately the same energy as the transmission of one maximum-size packet, which is lower than previous PBR systems that required up to 200 phase samples. This makes the proposed approach well-suited for energy-constrained IoT deployments.

The results demonstrate the feasibility of integrating phase-based ranging into TSCH with acceptable trade-offs in throughput and energy consumption, achieving sub-meter distance estimation accuracy in real-world conditions, confirming the aforementioned hypotheses. In line with the principles of open science, we release the measurement datasets and the software implementation as an open-source solution to the community, representing contribution **C5**. The proposed solution opens the way for cost-effective IoT systems that provide connectivity and localization using the same hardware.

Publication included in this chapter:

G. Morano, K. Guan, A. Hrovat, and T. Javornik, **"Phase-Based Distance Estimation Integrated With IEEE 802.15.4 TSCH Communication"**, *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11 460–11 470, Apr. 2024, ISSN: 2327-4662. DOI: 10.1109/JIOT.2023.3330933

Created open-access resources:

Measurement dataset
G. Morano, A. Hrovat, and T. Javornik, *IEEE 802.15.4 TSCH dataset for phase-based distance estimation*, Zenodo, Dec. 20, 2022. DOI: 10.5281/zenodo.7464319

Software implementation
Contiki-NG contributors, *Contiki-NG OS for Next Generation IoT Devices*, GitHub repository, 2023. [Online]. Available: https://github.com/9morano/contiki-ng/tree/vesna-pmp

11460 IEEE INTERNET OF THINGS JOURNAL, VOL. 11, NO. 7, 1 APRIL 2024

Phase-Based Distance Estimation Integrated With IEEE 802.15.4 TSCH Communication

Grega Morano, *Graduate Student Member, IEEE*, Ke Guan, *Senior Member, IEEE*, Andrej Hrovat, *Member, IEEE*, and Tomaž Javornik, *Member, IEEE*

***Abstract*—Localization and sensing inputs are enabling new and improved Internet of Things (IoT) applications and have been studied extensively over the past decade. Unfortunately, many solutions focus primarily on improving localization performance, which in turn reduces communication capabilities. Driven by the integrated sensing and communication (ISAC) aspects, we investigate how localization functionality can be seamlessly integrated into an IEEE 802.15.4 time-slotted channel hopping communication protocol. We present two new methods of phase-based ranging that estimate the distance between two devices with each transmitted data packet. We further analyze the effects of introduced changes on communication, their power consumption, and ranging operability. We improve the state-of-the-art algorithm of phase-based distance estimation by reducing the number of phase samples required, without reducing its accuracy and sensitivity while increasing the energy efficiency.**

***Index Terms*—AT86RF233, IEEE 802.15.4, integrated sensing and communication (ISAC), Internet of Things (IoT), phase-based ranging, time-slotted channel hopping (TSCH).**

I. Introduction

CURRENT paradigms for the Internet of Things (IoT) and the sixth-generation mobile communication networks (6G) emphasize multifunctional networks that alongside communication support also sensing and localization functions [1]. Integrated sensing and communication (ISAC) approaches [2] explore how these functions can be combined into a single integrated system, improving spectral efficiency and providing beneficial mutual assistance. A single combined system also reduces the cost and size of hardware equipment and enables easier network deployment and maintenance, which is especially desirable for large IoT setups. The advantages presented have brought great attention to ISAC and have driven research in multifunctional network design. Classification of such systems recognizes many different approaches [2], [3], including the realization where sensing and communication are co-designed with the aim of meeting the performance requirements of both functions.

The choice of wireless technologies for an IoT network depends on the application use cases and their requirements. LoRaWAN and NB-IoT are suitable for long-range communication and low-power devices in applications like smart cities or agriculture [4]. In contrast, Bluetooth is well suited for short-range communication between devices in close proximity, as often used in wearables and home automation [5]. IEEE 802.11 (Wi-Fi) provides high data rates for applications requiring fast data transmissions, such as video streaming or real-time monitoring, while the IEEE 802.15.4 standard defines a set of PHY and MAC protocols designed for low data-rate personal area networks. One of the representatives of the IEEE 802.15.4 standard is the time-slotted channel hopping (TSCH) protocol, introduced in the 2015 revision [6], which significantly improves the packet delivery rate by using the channel hopping technique. It offers high reliability, low or at least predictable delay, and low power consumption, which is perfect for critical low-power applications and the Industrial IoT (IIoT) [7].

Since most of the IoT services are used to monitor the environment, supplementary sensing inputs are beneficial and of great interest, making the ISAC approach the desired feature. The increasing demand for real-time ranging and localization capabilities is enabling new and improved IoT applications, such as asset tracking, indoor navigation, parking management, assisted living, worker safety, smart inventory, warehouse management, etc. Bluetooth 5.1 has already recognized the benefits of adding a sensing function to communications and introduced a packet extension in 2019, that can be used for localization purposes. Similarly, IEEE 802.11az addressed the localization demands by introducing enhancements for indoor positioning in 2022. IEEE 801.15.4a included another PHY mode in 2007, called ultra-wideband (UWB), whose large bandwidth enables high-precision localization. In 2020, IEEE 802.15.4z approved an amendment to the UWB PHY mode that improves the accuracy of localization. The TSCH mode, however, still does not provide sufficient channel sensing functionality, which was the main motivation for this study.

Distance estimation between two devices, which is the first step in many localization approaches, can be achieved with observable parameters that can be extracted from radio communication, including the intensity of the signal, its

Manuscript received 9 June 2023; revised 5 October 2023; accepted 31 October 2023. Date of publication 8 November 2023; date of current version 26 March 2024. This work was supported by the Slovenian Research Agency under Grant P2-0016, Grant J2-2507, Grant J2-4461, and Grant BI-BA/19-20-045. *(Corresponding author: Grega Morano.)*

Grega Morano, Andrej Hrovat, and Tomaž Javornik are with the Department of Communication Systems, Jožef Stefan Institute, 1000 Ljubljana, Slovenia, and also with Jožef Stefan International Postgraduate School, 1000 Ljubljana, Slovenia (e-mail: grega.morano@ijs.si; andrej.hrovat@ijs.si; tomaz.javornik@ijs.si).

Ke Guan is with the State Key Laboratory of Advanced Rail Autonomous Operation, Beijing Jiaotong University, Beijing 10004, China, and also with the Department of Communication Systems, Jožef Stefan Institute, 1000 Ljubljana, Slovenia (e-mail: ke.guan.bjtu@qq.com).

Digital Object Identifier 10.1109/JIOT.2023.3330933

© 2023 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

frequency and phase, and the timing of packet transmission. The IEEE 802.15.4 standard already defines the function of measuring the received signal strength indicator (RSSI) of a received frame and calculating its link quality index (LQI). Based on the attenuation of the received signal, the distance to the transmitter can be estimated. Since signal strength metrics are easily obtained after each received packet, their use is generally straightforward to implement and widely accepted [8]. Many RSSI-based localization systems also rely on the fingerprinting technique [9], and with the advent of novel machine learning (ML) approaches, the accuracy of such systems is constantly improving [10]. Unfortunately, RSSI measurements are highly susceptible to noise and signal interference and are particularly unreliable in rapidly changing environments, making them unsuitable for high-accuracy solutions. Studies, such as [8] and [11], which investigated RSSI-based localization with different wireless technologies, have also shown that RSSI measurements made with other technologies (WiFi and Bluetooth) outperform those made with ZigBee technology, which is made upon IEEE 802.15.4 standard.

The time it takes for a packet to travel from source to destination, known as Time of Flight (ToF), can be used to estimate the range between devices. In the context of narrowband IEEE 802.15.4, Lanzisera et al. [12], [13] have demonstrated the use of a two-way ranging technique, that can estimate the distance between devices with an accuracy of 1–3 m. Bedford and Kennedy [14] looked at ZigBee modules for ToF-based distance measurement in underground tunnels. However, relying on ToF might be problematic because the propagation speed of electromagnetic waves is very high while the distances are relatively short. Even minor measurement errors lead to significant distance errors (1-m accuracy requires a time resolution of about 3 ns). This is especially observed in narrowband communication, in contrast to UWB technology, whose wide bandwidth allows subnanosecond resolution [15].

The challenges of the packet travel time measurements can be mitigated by measuring the phase angle of a radio wave. By measuring the phase difference between the received and transmitted signals, it is possible to estimate the distance between the transmitter and receiver. To avoid initial phase offsets and precise clock synchronization between devices, the active reflector (AR) [16] method can be used, where the devices exchange the continuous-wave (CW) signal and measure the phase angle both ways with respect to each other. The method is also referred to as two-way phase measurement (PM) [17]. To reduce the impact of a multipath environment, devices exchange CW signals over multiple carrier frequencies, expanding the used bandwidth and improving the overall accuracy and resolution of the ranging system.

The IEEE 802.15.4 TSCH protocol natively supports only the RSSI metric, which is extracted during regular data transmission and thus does not affect the main function of the network, i.e., communication between devices. Extraction of other metrics is not supported by the TSCH protocol, and while other solutions primarily aim to improve localization performance, they in turn reduce communication performance. In this article, we propose an improvement to the TSCH protocol that allows the distance estimation between two devices without compromising the ongoing communication. The phase-ranging approach is seamlessly integrated into TSCH, and whenever a data packet is sent, the distance between the receiver and the transmitter is estimated. The solution, therefore, provides two functions using the same hardware and can be realized with commercial off-the-shelf devices, which are cost efficient and well suited for IoT setups.

The contributions of this study are summarized as follows.

1) Development and integration of novel phase-based distance estimation method into the TSCH communication protocol.
2) Adaptation and optimization of the state-of-the-art distance estimation algorithm.
3) Implementation and evaluation of the proposed approach in three use-case scenarios.

The remainder of this article is structured as follows. In Section II, we present related work that addresses the inclusion of PM in a communication protocol. In Section III, we discuss the challenges of implementing PMs in the communication protocol, and then propose two novel implementations in Section IV. In Section V, we present the experimental setup to test the new methods and evaluate their impact on communication, its ranging errors, and energy consumption. Finally, we draw the conclusions in Section VI.

II. Related Work

The literature presents many solutions addressing specific issues related to phase-based distance estimation, however, a comprehensive solution that encompasses the ISAC aspects of integrating localization into IEEE 802.15.4 communication is lacking. This section explores the related work in the field, presenting the various solutions proposed for individual problems.

In 2012, Atmel (now Microchip) equipped its IEEE 802.15.4 compliant radios (e.g., AT86RF233) with a PM unit (PMU) that provides a function to measure the phase of the incoming signal [18]. Pelka et al. [19] were the first to use the radio to experimentally demonstrate how a distance between two nodes can be estimated from a slope of the measured phase angle. They created an error model and evaluated how the PM is affected by the clock drift of the device, errors in changing the carrier frequency, and the noise generated when sampling the interfered carrier. Using the simple slope extraction approach and phase angle measurements of only two frequencies, they estimated the distance between the devices with the accuracy of 0.02 m in the best case. However, they were only able to estimate the distance in the maximum unambiguous range (UR) of 2 m, since a large frequency step was used.

Oshiga et al. [20] proposed to create a large set of phase differences from a small number of measured phase angles, which are sampled at predefined frequencies determined by the Golomb ruler technique. The efficient slope sampling ranging (ESSR) algorithm was proposed to compare the phase differences with a precomputed set of phase slopes and to estimate the distance between two devices. The multiple

computed distances were then used for the localization of a device. von Zengen et al. [21] presented a real-valued distance estimation (RDE) algorithm that calculates the distance between two devices using autocorrelation and fast Fourier transform (FFT). They presented the InPhase system which sampled 200 frequencies in steps of 0.5 MHz and achieved an accuracy of 0.3 m with the UR of 300 m. In a later paper [22], Schröder et al. proposed a complex-valued distance estimation (CDE) algorithm that first computes a complex signal from the measured phases and then applies it to the FFT. To reduce the computational complexity, they proposed to use a smaller bin count and later interpolate the FFT result, while preserving the accuracy of the distance estimation. They showed that the CDE algorithm outperforms the RDE and ESSR algorithms, achieving an accuracy of 0.15 m with the UR of 300 m.

However, none of the proposed methods conforms with the IEEE 802.15.4 communication standard. The RDE and CDE algorithms for example require a large number of measured phase angle samples. To obtain the PM at each frequency in the 2.4-GHz band, the authors proposed to interrupt the communication between two nodes for a certain period of time and measure the phase angles. During this time, the devices are in the "atom routine" and are not available for communication. The network downtime may result in unreliable communication, which is not desirable for time-critical applications. In addition, the measured data from one device has to be sent to the other device after the measurement is complete, which places an additional burden on the communication service and its data throughput.

Bluetooth technology, on the other hand, has already introduced positioning information in Bluetooth Core Specification 5.1, namely, the constant tone extension (CTE). A sequence of modulated ones is appended to the end of a packet, which appears as an unmodulated carrier and is primarily used for the measurement of the Angle of Arrival (AoA) and the Angle of Departure (AoD). Zand et al. [17] used the CTE of a packet for a multicarrier phase-based ranging solution compatible with the BLE standard, including connection-oriented and connectionless modes of operation. They analyzed the effects of phase sampling intervals between the initiator and reflector, which affect the ranging error. To reduce phase noise and ranging accuracy, which accumulates with time between two phase samples, they proposed a new packet structure called constant tone prefix (CTP), which is prefixed to the response packet. The same authors also introduced one-to-many and many-to-many phase-based ranging, which provides simultaneous distance estimation for all participating devices in a large-scale Bluetooth network [23]. Although some parallels can be drawn, the proposed methods do not comply with the IEEE 802.15.4 communication standard, which uses different packet structures, modulation, message exchange procedures, etc.

III. Challenges of Including Phase Measurements Into TSCH Communication

The integration of phase-based distance estimation functionality into the TSCH protocol requires a detailed analysis of PM, that have to be considered during the implementation of the solution into the TSCH protocol. In this section, we outline the challenges of phase-based distance estimation and present a comprehensive method for PM that incorporates insights from various research studies.

A. Measuring Phase Angle

A device can measure the phase angle of an incoming CW signal by comparing the signal's waveform with its local reference. The phase shift between the reference signal and the received signal is proportional to both frequency f and distance d, i.e.,

$$\phi(f,d) = \frac{2\pi d}{c}\cdot f + (2\pi N) \ + \phi_{\text{off}} \tag{1}$$

where c is the speed of light, and an integer N represents the cyclic nature of the phase angle as it rotates with period 2π. Since the clock source of the receiver is not synchronized with the transmitters, an additional phase offset ϕ_{off} is induced during the measurement. To remove the influence of the unsynchronized clocks, Kluge and Sachse [16] proposed the AR technique, which measures the phase of the communication channel in both directions. First, the device called the initiator transmits the local oscillator signal, i.e., a constant tone, and the second device, called the reflector, performs the PM. In the next step, the reflector transmits the constant tone with its local oscillator frequency back to the initiator, which performs the measurement. When the initiator later obtains the measured phase from the reflector, it can merge the two measurements and remove the additional phase offset term

$$\phi_{\text{AR}}(f,d) \ = \phi_I(f,d) - \phi_R(f,d) = \frac{4\pi d}{c}\cdot f + (2\pi N). \tag{2}$$

The same technique also removes an additional phase term that is generated by the local oscillator, which introduces a random initial phase shift when the hardware resets to a new frequency [19].

To eliminate the cycle ambiguity, the PM is obtained from two different frequencies with a frequency step of $\Delta f = f_{k+1} - f_k$, so that the phase difference becomes

$$\Delta\phi = \phi_{\text{AR}}(f_{k+1},d) - \phi_{\text{AR}}(f_k,d)). \tag{3}$$

By combining (2) and (3) and solving them for d, the distance estimate becomes

$$d = \frac{c}{4\pi}\cdot\frac{\Delta\phi}{\Delta f} + \left(\frac{c}{2\Delta f}N\right) \tag{4}$$

and the UR is now equal to $c/(2\Delta f)$. For example, a frequency step of 5 MHz would result in a maximum distinguishable range of 30 m. To achieve high UR resolution, the frequency step should be smaller.

PMs are sensitive to external disturbances and interference. As radio frequency signals bounce off surrounding objects in the environment, the receiver obtains several copies of the signal, each resulting in a different phase shift. Since apparent multipath components in the system can be affected by changing the carrier frequency, multiple tones in the range

of $\{f_1, \ldots, f_K\}$ can be used, so that the phase difference after phase unwrapping becomes

$$\Delta\phi = \frac{4\pi d}{c} \cdot (f_K - f_1) = \frac{4\pi d}{c} \cdot \Delta f \cdot K \tag{5}$$

and the estimated distance can be expressed as

$$d = \frac{c}{4\pi} \cdot \frac{\phi_{\mathrm{AR}}(f_K) - \phi_{\mathrm{AR}}(f_1)}{\Delta f \cdot K}. \tag{6}$$

Combining multiple tones increases the effective bandwidth by a factor of K without decreasing the maximum UR, resulting in higher resolution and accuracy of sensing.

B. Sampling Frequency Selection

The IEEE 802.15.4-2015 standard defines 16 channels in 2.4-GHz ISM band, separated by 5 MHz. Combining the PMs with this configuration would produce a wide bandwidth ($K \cdot \Delta f = 80$ MHz). But based on real-world measurements, 16 phase samples are not sufficient for the desired resolution due to possible interference and multipath effects. In addition, by using $\Delta f = 5$ MHz, the maximum UR becomes 30 m, which is not enough for outdoor scenarios.

The InPhase system used $K = 200$ samples with the step of 0.5 MHz which results in a UR of 300 m [22]. However, the time to measure phases on 200 frequencies does not fit into the tightly scheduled TSCH timeslot. As reported, in their setup the measurement on one frequency takes up to 244 us, resulting in an interval of 48.8 ms for all tones, which is almost five times larger than the typical timeslot duration of 10 ms. To minimize intrusiveness to the communication protocol, the number of taken samples should be reduced. In addition, even though the authors reported no drop in Wi-Fi performance, sweeping with the constant tone over the entire ISM band causes additional, unwanted interference for communication. Therefore, we seek for a tradeoff between a number of sampled phases and the resolution of the ranging system and its UR.

Equation (4) shows that the distance is proportional to the phase slope, or in other words to the ratio between phase difference and frequency step. By following the Golomb ruler technique, a large set of phase differences can be created from a small number of measured phases. For instance, by taking K PMs $\Phi = \{\Delta\phi_1, \ldots, \Delta\phi_K\}$ on selected frequencies, the original set can be uniquely expanded into a new set of phase differences $\Delta\Phi$

$$\Delta\Phi = \{\Delta\phi_2 - \Delta\phi_1, \ldots, \Delta\phi_K - \Delta\phi_1, \ldots, \Delta\phi_K - \Delta\phi_{K-1}\} \tag{7}$$

and their related expanded frequency steps $\Delta F = \{\Delta f_1, \ldots, \Delta f_M\}$, with the power of $M = K[(K-1)/2]$ [20]. Described superresolution technique with proposed optimized sampling was proposed in [24] by Oshiga et al. and well studied on phase ranging problem in [20]. In later, the authors proposed to sample $K = 15$ frequencies which result in $M = 105$ unique phase difference samples. This approach systematically reduces the number of frequencies sampled, thereby reducing measurement delay and power consumption, which is beneficial for a low-power network such as TSCH.

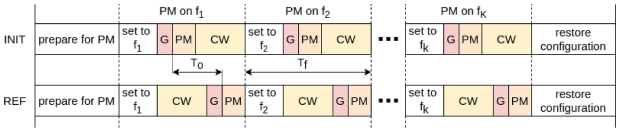


Fig. 1. Proposed PM process between initiator (INIT) and reflector (REF). PM: phase measurement, CW: continuous-wave transmission, and G: guard interval.

C. Sampling Time and Clock Synchronization

As studied in [17], the PM (and hence the estimated distance) is strongly dependent on the time offsets between the sampling periods. The distance error is sensitive to the initiator end reflector measurement difference delay (T_o), and to the delay between the measurement of two different frequencies (T_f). Since the crystal oscillator used for the system clock and frequency generation is imperfect (drift given in ppm), the sampled phase includes two additional errors. The first is the consequence of a slightly different generated frequency, which results in a different phase rotation for the same distance. The second error is due to the sampling time difference of the measurement by the initiator and reflector, which is caused by the system clock drift. Since the crystals are imperfect and cause a clock deviation during T_o, this leads to an additional phase shift in the phase samples [17].

The described errors in the distance estimates could be compensated if the crystal drifts are known. Since each device has its own crystal, determining all drifts is a difficult task, especially with a large number of devices in WSNs. To avoid this, we observed that the PM of the initiator and reflector should be performed in the shortest possible interval. We propose to obtain the data on selected frequency by measuring the reflectors and initiators phase successively. Furthermore, to avoid crystal offsets measurements and corrections we propose to measure phases from all of the required frequencies sequentially. Fig. 1 depicts the proposed PM process.

Since PM is not part of the normal radio operation during communication, the devices first prepare for the measurement by storing all the register values of the radio and configuring the PMU. The process is exactly the same for both devices, so we assume that the preparation takes the same amount of time. After configuration, the devices start with the PM by setting the local oscillator to a desired frequency (f_1). The reflector then waits for a predefined guard time before measuring the phase, and then transmits a CW. The initiator starts transmitting CW and then waits for a guard time before the measuring phase. This method ensures that both nodes measure phase while a CW transmission is in progress. The process is repeated for K different frequencies, and at the end, the nodes reconfigure the radio using the stored register values so that they can proceed with the communication.

D. Constant Tone Generation

The PM requires that a transmitter sends an unmodulated CW at a constant frequency. For example, Ayyalasomayajula et al. [25] extended the data packet with a stream of 1 or 0 bits that produce a constant tone

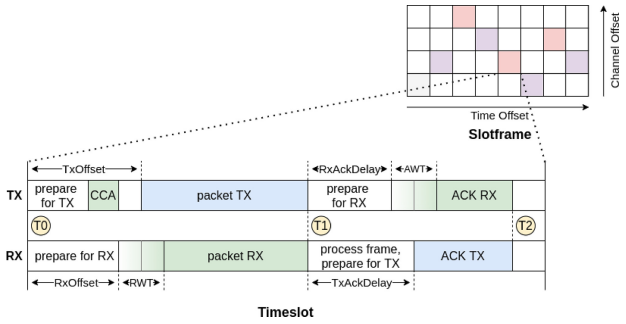


Fig. 2. TSCH default timeslot as part of a slotframe for transmission (TX) and reception (RX) routine (the size of the blocks is not in scale).

due to the GSK modulation used. Unlike Bluetooth, the IEEE 802.15.4 standard defines the use of offset quadrature phase-shift keying (O-QPSK) for the 2.4-GHz band, so a similar approach cannot be used. However, most radios on the market are capable of transmitting an unmodulated carrier, by emptying the frame buffer and configuring the modulation data source to utilize continuous zero or one chip, creating CW. Since this is not a part of the radio's operation during data transmission, the time needed to prepare the radio for CW should be considered when implementing the new approach in the communication timing scheme.

The IEEE 802.15.4 standard also defines the use of TSCH in sub-GHz bands where either OFDM or FSK modulations can be used. While this study focuses on the 2.4-GHz band, a similar approach could be implemented in these scenarios.

E. Synchronization of the Measured Samples

Another requirement for successful measurement of the AR phase is synchronization between the devices; both devices should start the PM process at the same time. Here, we rely on the IEEE 802.15.4 TSCH standard, which by definition builds a globally synchronized network. The communication time is divided into timeslots, typically 10 ms long, which is sufficient to accommodate a data packet transmission and reception, an acknowledgment (ACK) exchange, and all the necessary guard times for packet processing and radio module preparation. Multiple timeslots form a slotframe, a structure that repeats over time as presented in Fig. 2. Each timeslot is uniquely identified by its absolute sequence number (ASN), a counter that is incremented at each timeslot. Every node knows the current ASN in the network and therefore knows exactly when to wake up from the low-power operation and prepare for the communication.

Since the nodes exhibit system clock drift due to inaccurate crystal oscillators, it is essential that the nodes periodically correct the drift to their time source. The TSCH utilizes synchronization through pairwise communication: a node synchronizes when it receives a packet or an ACK from its time source neighbor [26]. In the first case, the node timestamps the reception of a packet and calculates the time difference from the expected time. The node then increases or decreases the duration of the current timeslot to compensate for the drift error. In the latter case, the time source calculates the time delta of the reception of a packet sent by the node. The time delta is then included in the ACK so that the node can readjust its current timeslot and compensate for the drift error. Additionally, adaptive time synchronization can be used, where the node learns the relative drift from past synchronizations [27].

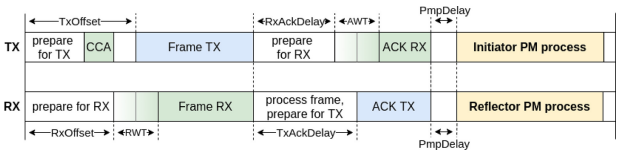


Fig. 3. Extended timeslot including PM after acknowledgment (the size of the blocks is not in scale).

To ensure the tight timings within the timeslot itself, the TSCH standard specifies a timing template with corresponding delays, as presented in Fig. 2. The delays are inputted into timer counters, and their interrupts are utilized for accurate timing operations.

IV. Proposed Implementation of Phase Measurement Process

The timeslot shown in Fig. 2 is tightly packed with transmission and reception processes, and adding the PM process will extend its typical duration of 10 ms recommended in the IEEE802.15.4 standard. Longer timeslots are already included in the Contiki-NG stack to support the slower radios [26]. There is no header-based signaling of timeslot duration within a transmitted frame, so all participating nodes should be configured in advance and consistently for the network to work properly.

For the devices to start the PM process at the same time, there are at least three points in time within the timeslot where synchronization is guaranteed: at the beginning of the timeslot (time T0), after the exchange of the data frame (time T1), and after the exchange of the ACK packet (time T2). We consider the time points T1 and T2 to investigate two noninvasive implementations of the proposed method for effective measurement of the phase angle: 1) PM after acknowledgment and 2) PM after the data packet.

A. Phase Measurement After Acknowledgment

Inspired by the example of Bluetooth CTE, PM can be seamlessly integrated into the communication protocol by expanding the communication window and adding PM after the ACK packet is exchanged between devices.

As shown in Fig. 3, we define a new short timing delay `PmpDelay` that is added to ensure the devices start the measurement process synchronously. Afterward, the devices start with the PM process as described in Section III. When the devices obtain the data from all 15 predefined frequencies, they store the measurement along with the ASN, which is later used to combine the samples into the phase differences ϕ_{AR}.

Since the measurement is done only after ACK packets, devices measure the phase of the communication link on every unicast packet. Broadcast packets, which do not require an

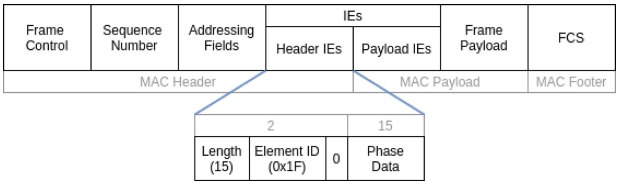


Fig. 4. Enhanced acknowledge frame and added information element structure (the size of the blocks is not in scale).

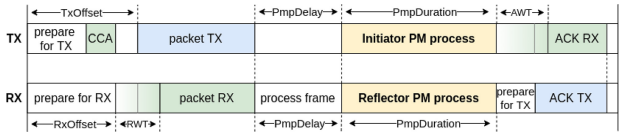


Fig. 5. Extended timeslot including PM after data packet.

ACK, are not in our interest because their destination node address is not known. This also helps preserve privacy, because the exact time of PM measurement is not known for a listener outside of the network.

The data obtained by the reflector must be returned to the initiator for the ϕ_{AR} calculation. This can be done within another data packet, but the solution therefore relies on the upper layers (i.e., the application layer), not just on the MAC layer of our interest. Additional feedback data packets increase communication traffic and thus decrease network throughput, since this solution requires the exchange of two data packets for a single distance estimate. With the aforementioned drawbacks in mind, we introduce a new, more efficient approach that addresses the stated problems.

B. Phase Measurement After Data Packet

Each unicast packet in the TSCH network must be acknowledged by the receiver. This feature can be used to send the feedback data to the initiator. The reflector could first obtain the information about the channel and return it back to the transmitter by adding the measured data to the ACK packet. The PM can be encapsulated in the packet using an information element (IE), as they provide an adjustable container for additional data to be exchanged between the devices [6]. There are two different types of IEs: 1) a Header IE, which is a part of the MAC header and is not encrypted and 2) Payload IE, which is a part of the payload and therefore could be encrypted. As defined in the IEEE 802.15.4-2015 standard, the IE is structured with an identification field, a length field, and a content field [6].

In the proposed implementation, we are using Header IEs to return the phase information measured with the receiver. We defined a new Element ID 0x1F with the name *PM*. Its length is set to 15, since we are measuring $K = 15$ samples of phases. The structure of the new enhanced acknowledge frame is presented in Fig. 4. When TSCH uses encryption, the measured data can be returned to the initiator by using Payload IE which further decreases the possibility of unwanted attacks.

Fig. 5 depicts the proposed implementation, where the participating devices first exchange the data packet, then measure the phase and afterward send the ACK packet. The PM procedure cannot be done immediately after frame transmission/reception because the received frame is still in the radios buffer, and the PM setup would discard its content. Therefore, the frame is first obtained and processed. If the ACK is required, the PM process is started. To ensure that the devices start the PM process synchronously, we defined new timeslot timings. The `PmpDelay` value is the same on both devices and should last approximately the same as previously defined `TxAckDelay` (time needed to process the data packet). The new value of `PmpDuration` is equal to PM procedure duration.

The proposed implementation is more intrusive to the TSCH protocol, as less data space is available in the ACK packet, and more changes are introduced at the network stack compared to the PM after acknowledgment implementation. However, in this approach, the data is exchanged between the devices without additional traffic. The PMs from both devices are available at the initiator after each packet is sent, which results in high responsiveness and a high refresh rate since a device can induce more PMs of a link by sending more packets to a targeted device.

V. Validation of Proposed Implementations

To evaluate the proposed modifications of the TSCH protocol we test them in real-world scenarios by implementing them in the Contiki-NG [28] and its protocol stack. We used VESNA [29] wireless sensor nodes equipped with AT86RF233 transceivers [18]. The radio datasheet contains little information on PMU setup, but a more detailed description of the operation can be found in [30].

The used frequency set was generated with the Golomb ruler proposed in [20] and results in: $f_{\mathrm{Golom}} = \{2400.5, 2406, 2407.5, 2408, 2412.5, 2423, 2431, 2447.5, 2452, 2460.5, 2463, 2466.5, 2476.5, 2479.5, 2480.5\}$ MHz. The duration of the PM process for a single frequency is equal to $T_f = 420$ us. Measurements at 15 frequencies, together with the time needed for radio preparation and reconfiguration last for 7.9 ms, thus `PmpDuration` time was set to 8000 us. Since the `PmpDelay` should be approximately the same as the previous `RxAckDelay`, we used the same value, which was in our case set to 2000 us. In both proposed implementations, the timeslot duration was extended from the default 10 to 20 ms to accommodate the PM process.

A. Effects on Communication

The introduced distance estimation techniques shorten the time available for communication which affects the throughput of the network. The number of packets per second (pps) that can be exchanged between two devices correlates with the number of available timeslots per second. The latter is determined by the timeslot duration, size of the slotframe, and its schedule, which are not defined in the IEEE 802.15.4 TSCH standard and are left open to higher levels and implementers, who can adjust their network setup according to the desired requirements and application use cases. To quantify the impact of the proposed TSCH modification on the communication, first, an ideal TSCH network scenario is modeled, in which a

TABLE I
PROPOSED METHODS IMPACTS ON COMMUNICATION

	throughput [pps]	protocol changes	high level application
default TSCH	100	/	/
PM after ACK	25	`PmpDelay`	packet exchange handler
PM after data	50	`PmpDelay`, `PmpDuration`, additional IE	/

node can utilize all of the timeslots in a slotframe to exchange packets with its neighbor. This schedule would result in a throughput of 100 pps for the typical timeslot duration of 10 ms. In the case where TSCH implements PM after data, less time is available for communication as the timeslot is extended to 20 ms, and the pps ratio drops to 50, reducing the network throughput by a factor of 2. In the case where TSCH implements PM after acknowledgment, the pps ratio drops to 25 because, in addition to extending the timeslot duration, the measurements from the reflector must be sent back to the initiator with an additional data packet that would otherwise be available for application data exchange. The communication load in the network is thus increased, since an additional timeslot is consumed for each measurement feedback, which reduces the overall network throughput by a factor of 4.

The PM after acknowledgment method is also more complex to implement than the PM after data method because it requires a higher layer application, which includes a packet exchange handler to ensure that measurements are efficiently exchanged and later correctly combined using ASN. The PM after data method, on the other hand, returns the measurement from the reflector within the ACK packet to the initiator, so no handler application is required. The MAC layer can compute the ϕ_{AR}, and higher layers can query it after each packet sent. The PM after data method however introduces more changes to the TSCH protocol, because it consumes additional IE of the ACK packet, and defines new timeslot timings for the in-slot synchronization, which are not required for the PM after acknowledgment method. Table I summarizes the impacts of the proposed methods on the TSCH communication.

The throughput effects could be reduced by shortening the entire PM process, for which a faster signal's phase acquisition is needed. Although the AT86RF233 samples the phase with the interval of 8 us, the radio only supports the serial peripheral interface (SPI) speed of 8 MHz, which is not sufficient for a fast data acquisition. Furthermore, the time needed to configure the radio for CW and to reconfigure it to measure the phase is relatively high, due to low SPI speeds and slow PLL settling times. If the PM would be natively supported by the hardware (similar to the Bluetooth implementations), the PM process could be shortened, reducing the effects on the network throughput.

It is important to note, that the primary goal of IEEE 802.15.4 and TSCH is not to provide a high throughput, but rather to ensure reliable and energy-efficient communication in low-rate applications. A tradeoff between throughput and the function of range estimation should be considered regarding the desired application use case, and all devices in the network should be configured the same prior the deployment.

TABLE II
PARAMETERS OF THE EXPERIMENTS

	d_{min} [m]	d_{max} [m]	No. of results	No. of discarded ESSR	No. of discarded iCDE
office	0.5	5.0	3120	660	603
hallway	2.0	20.0	3103	540	1206
park	5.0	100.0	2580	186	547

In addition to the affected throughput, it would seem that the transmission of CW employed for channel estimation may affect the usual TSCH communication with additional interference. However, all of the nodes in the network are configured upfront, and even if two devices start the timeslot operations at the same time (at different channels within the slotframe), the communication part of the timeslot will not be affected by the PM part. On the contrary, the communication in other TSCH networks in the vicinity can be affected by introduced ranging, as the networks are not synchronized. With the proposed frequency set, only channels 22 and 26 are directly interfered with the CW transmission. In case the packet exchange happens on those channels while the channel is jammed, TSCH will detect the possible failed attempt and retransmit the packet on a different channel.

B. Ranging Performance

In order to demonstrate the viability of the proposed method for ranging, we carried out a measurement campaign during which the devices utilized the PM after data packet implementation. Comparable outcomes can be achieved using the PM after acknowledgment, as the PM results remain consistent regardless of whether they are sampled before or after the acknowledgment. Measurements were made in three different scenarios: 1) outdoors in a park; 2) indoors in an office (5 m × 5 m), and indoors in a hallway (3 m × 40 m). The outdoor scenario was selected as the reference environment with low multipath effects, while the indoor scenarios represent a test environment with possible multipath components and additional IEEE 802.11 interference.

In each scenario, two VESNA devices were placed on a stand 1.6 m above the floor with clear line-of-sight conditions. The initiator node was connected to a computer to calculate the distance estimates from measured phases. The actual distance between the nodes was measured by laser ranger with an accuracy of ±1.5 mm. The minimal (d_{min}) and maximal (d_{max}) tested distance of separate experimental scenario are shown in Table II. The table also presents the number of obtained measurements per scenario and the number of discarded measurements from different algorithms.

To estimate the distance between the devices, the obtained data was feed to two algorithms: 1) the ESSR algorithm presented in [20] and 2) the iCDE algorithm presented in [22], which we further adopted to our data collection method. By default, the ESSR algorithm uses only 15 samples of measured phases and compares them with a precomputed set of slopes. The algorithm outputs a vector of residues and the peak

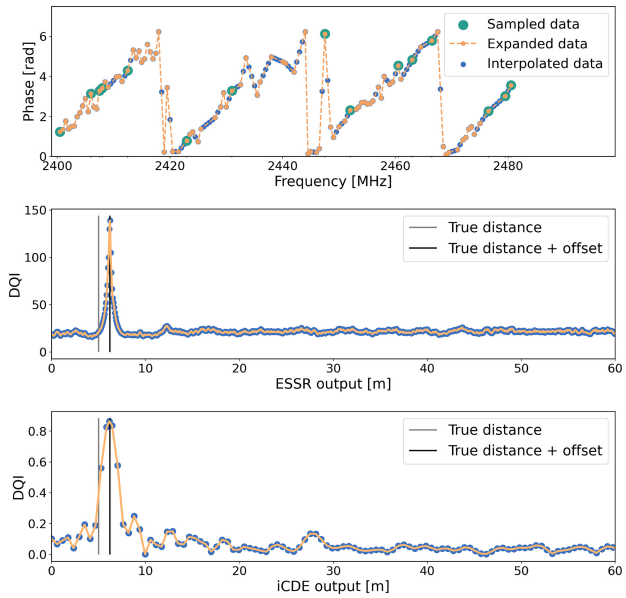


Fig. 6. Example of phase angle measurements at 5 m with corresponding expanded and interpolated data (top), the output from the ESSR algorithm (middle), and the output of the iCDE algorithm for the same phase angle measurements (bottom).

value corresponds to the estimated distance. The number of precomputed slopes determines the accuracy of the algorithm and the maximum UR. To be comparable to the results in [22], we used 4096 different slope samples with a maximum range of 300 m, resulting in a minimum distinguishable distance of 0.0732 m. The same configuration was used for all three scenarios.

iCDE algorithm first computes a complex signal from the measured phases which is then applied to the FFT. By searching for the peak value of the FFT output, the distance can be estimated. The number of used FFT bins is related to a minimal distinguishable distance within the range of the selected maximum range. Schröder et al. [22] showed that the number of used FFT bins can be reduced from 4096 to 512 while preserving the accuracy in the UR of 300 m, if the output vector of the FFT is interpolated with polynomial interpolation. The iCDE algorithm, however, requires a larger set of input samples to achieve desired accuracy and sensitivity, thus obtained 15 samples are not enough. As presented with (7), by using phase samples measured at frequencies designed with a Golomb ruler, we can uniquely expand the measured $K = 15$ samples into sets of $M = 105$ samples. Yet, the frequency step of an expanded set of measurements is not equal for each measurement, as seen in Fig. 6. To achieve the same sample rate Δf of 0.5 MHz in the whole used spectrum of 80 MHz, we propose to extend the data with linear interpolation. An expanded set of 160 measurements, created from 15 samples can now be fed into the iCDE algorithm.

Both algorithms provide a distance quality indicator (DQI) for each estimated distance, which can be used to rule out erroneous measurements by discarding the ones with a DQI value below a predefined threshold. Using the Youden index, as proposed in the [21], we found that the threshold in our

TABLE III
MEASUREMENT ERRORS

		min [m]	max [m]	med [m]	MAE [m]	σ [m]
Office	ESSR	-0.989	137.548	0.359	2.127	14.459
	iCDE	-0.707	6.445	**0.254**	**0.527**	**0.950**
Hallway	ESSR	-2.951	110.337	0.259	1.457	9.676
	iCDE	-2.477	1.918	**0.235**	**0.545**	**0.381**
Park	ESSR	-19.962	88.503	0.068	1.470	9.106
	iCDE	-0.339	0.358	**0.065**	**0.088**	**0.083**

system was 36 for ESSR and 0.41 for iCDE algorithm, resulting in 15.7% and 26.7% of the measurements being discarded, respectively. Each measurement result contains an additional offset due to the radio signal paths on the circuit board and the antenna. In our case, we measured an offset of 1.1 m, and all measurement results were corrected accordingly. Table III shows the measurement errors from all three scenarios, where the minimum and maximal estimated distance error returned by the algorithms are denoted as min and max consequently. The final median (med), mean absolute error (MAE), and standard deviation (σ) values are calculated as the median of the individual values per tested distance, respectively.

Results in Table III show that the office scenario has the highest σ and the highest MAE, while the results of the park scenario can be considered as optimal with respect to the radio channel conditions for the measurements. In addition, indoor scenarios may suffer from interference, as 17 Wi-Fi access points were in operation during the measurement campaign, which was not present outdoors. The results are confirming the conclusion drawn in the [22], where iCDE yields the best results. Our proposed modified version of iCDE, where only 15 PMs are needed, is comparable to the original iCDE algorithm and also outperforms the ESSR algorithm. In addition, iCDE requires less computational resources making it the preferred choice for an embedded device.

The better distance estimation performance of the iCDE algorithm can be attributed to better detection of erroneous measurements with DQI value. Upon further examination of the measurement results, we found that both algorithms frequently reported wrong distance estimates at certain locations, due to the influence of multipath propagation and signal reflections from the floor or walls of the building. While iCDE successfully rejects most of the wrong measurements, ESSR fails to detect them, resulting in higher MAE and σ. This is also confirmed by the reported number of discarded measurements. With the result investigation we also observed, that by using only the DQI value, all outliers in the results cannot be detected. In the case of a mismatch in the measurement process (e.g., erroneous expansion of the measured phases due to noise, the PM measurement is not correctly synchronized, a device misses the time slot, etc.), both algorithms still provide a distance estimate. This value is random and ranges from 0 to 300 m, which has a large impact on the statistics of the measured data. Since the proposed method makes a

TABLE IV
MEASUREMENT ERRORS WITH FIVE SUCCESSIVE MEASUREMENTS

		min [m]	max [m]	med [m]	MAE [m]	σ [m]
Office	ESSR*	0.090	0.505	0.341	0.327	0.070
	iCDE*	0.116	0.465	**0.255**	**0.316**	**0.041**
Hallway	ESSR*	-0.044	0.479	**0.174**	**0.245**	0.084
	iCDE*	-0.022	0.267	0.217	0.393	**0.061**
Park	ESSR*	-0.108	0.134	0.061	0.054	0.061
	iCDE*	-0.060	0.078	**0.048**	**0.053**	**0.033**

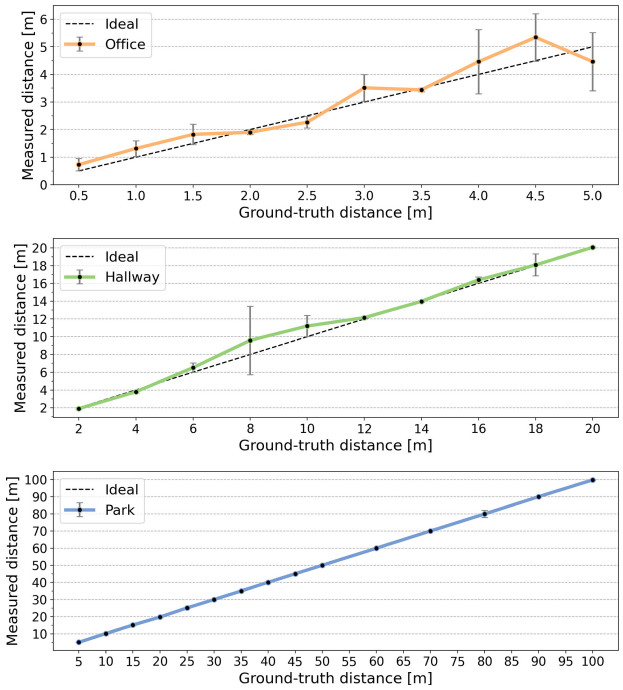


Fig. 7. iCDE* distance estimation results displaying median value and mean absolute error.

distance estimate after each packet is sent, the update rate of the measurement can be high and depends on the interval of sending a data packet to a particular device. This feature offers an option of utilizing additional simple filtering, by using the median of five consecutive measurements as the final distance estimation result. The new measurement results using the iCDE algorithm for different scenarios are plotted in Fig. 7. As can be seen from the measurement errors listed in Table IV (the additional filtering is marked with the asterisk symbol *), the accuracy and sensitivity of the system are greatly improved.

C. Energy Consumption

IEEE 802.15.4 TSCH is intended for use in low-power applications where device energy consumption is of great importance. To analyze the impact of the introduced ranging implementations on energy consumption, we measured the current consumption of the radio using the onboard shunt resistor and shunt amplifier. We used the maximum packet

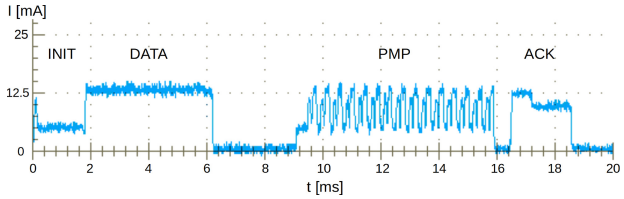


Fig. 8. Radio's power consumption during transmission routine measured with the onboard shunt resistor. INIT: initialization, DATA: transmission of a data packet, PMP: PM process, and ACK: acknowledgment.

size and presented only the transmission routine since the PM process in the reception routine is similar. In addition, only PM after data packet is presented as the energy consumption of the PM after acknowledgment method is the same. Fig. 8 shows the measured current consumption in a transmission timeslot, where four states of the radio can be identified: 1) initialization of the radio; 2) data transmission; 3) PM process; and 4) acknowledge reception. During the PM process, the current consumption changes rapidly as the radio consumes 10.0 mA in the receive mode, 12.8 mA in the transmit mode, and 5.2 mA when powered on [18]. Considering the time required for each state, the radio consumes an average of 179.2 uWs during the PM process, which is roughly the same as the radio's power consumption during the maximum length packet transmission (179.9 uWs). Compared with the previously proposed phase-based ranging solutions in [21] and [22], our implementation consumes less energy, as it is sampling phase angles on only 15 different frequencies instead of 200.

VI. CONCLUSION

In this article, we introduced two new methods of phase-based distance estimation that are compatible with the IEEE 802.15.4 TSCH protocol. By seamlessly adding a PM process in the timeslot, the proposed method is able to estimate the distance between two devices after each data packet is sent. The acquisition rate of the distance estimations can be high, and we suggest using five consecutive measurements to filter out possible outliers. Although the timeslot is extended by 10 ms and the energy consumption increases, in return, we can estimate a distance with a median error of 0.26 m and an accuracy of 0.31 m for indoor scenarios and a median error of 0.05 m and an accuracy of 0.05 m for outdoor scenarios. The proposed improvement of the iCDE algorithm, where only 15 samples are obtained instead of 200, further improves the time efficiency and reduces the energy consumption of the distance estimation technique. The implementation of the proposed methods on low-cost off-the-shelf devices offers a cost-effective solution for IoT networks, where localization functionality is required alongside responsive and reliable communication capabilities of the TSCH network.

REFERENCES

[1] C. De Lima et al., "Convergent communication, sensing and localization in 6G systems: An overview of technologies, opportunities and challenges," *IEEE Access*, vol. 9, pp. 26902–26925, 2021.

[2] J. Wang, N. Varshney, C. Gentile, S. Blandino, J. Chuang, and N. Golmie, "Integrated sensing and communication: Enabling techniques, applications, tools and data sets, standardization, and future directions," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23416–23440, Dec. 2022.

[3] J. A. Zhang et al., "Enabling joint communication and radar sensing in mobile networks—A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 306–345, 1st Quart., 2022.

[4] R. Marini, K. Mikhaylov, G. Pasolini, and C. Buratti, "Low-power wide-area networks: Comparison of LoRaWAN and NB-IoT performance," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21051–21063, Nov. 2022.

[5] S. J. Danbatta and A. Varol, "Comparison of ZigBee, Z-wave, Wi-Fi, and Bluetooth wireless technologies used in home automation," in *Proc. 7th Int. Symp. Digit. Forensics Security (ISDFS)*, 2019, pp. 1–5.

[6] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Standard 802.15.4-2015 (Revision of IEEE Standard 802.15.4-2011), 2016.

[7] M. Lekic, G. Gardasevic, and M. Mladen, "Experimental evaluation of multi-PHY 6TiSCH networks," *ITU J. Future Evolv. Technol.*, vol. 3, no. 2, pp. 470–482, 2022.

[8] S. Sadowski, P. Spachos, and K. N. Plataniotis, "Memoryless techniques and wireless technologies for indoor localization with the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10996–11005, Nov. 2020.

[9] V. Bianchi, P. Ciampolini, and I. De Munari, "RSSI-based indoor localization and identification for ZigBee wireless sensor networks in smart homes," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 2, pp. 566–575, Feb. 2019.

[10] M. T. Hoang, B. Yuen, X. Dong, T. Lu, R. Westendorp, and K. Reddy, "Recurrent neural networks for accurate RSSI indoor localization," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10639–10651, Dec. 2019.

[11] S. Sadowski and P. Spachos, "RSSI-based indoor localization with the Internet of Things," *IEEE Access*, vol. 6, pp. 30149–30161, 2018.

[12] S. Lanzisera, D. Zats, and K. S. J. Pister, "Radio frequency time-of-flight distance measurement for low-cost wireless sensor localization," *IEEE Sensors J.*, vol. 11, no. 3, pp. 837–845, Mar. 2011.

[13] S. Lanzisera, D. T. Lin, and K. S. J. Pister, "RF time of flight ranging for wireless sensor network localization," in *Proc. Int. Workshop Intell. Solut. Embed. Syst.*, 2006, pp. 1–12.

[14] M. D. Bedford and G. A. Kennedy, "Evaluation of ZigBee (IEEE 802.15.4) time-of-flight-based distance measurement for application in emergency underground navigation," *IEEE Trans. Antennas Propag.*, vol. 60, no. 5, pp. 2502–2510, May 2012.

[15] L. Flueratoru, S. Wehrli, M. Magno, E. S. Lohan, and D. Niculescu, "High-accuracy ranging and localization with ultrawideband communications for energy-constrained devices," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7463–7480, May 2022.

[16] W. Kluge and E. Sachse, "System, method, and circuit for distance measurement between two nodes of a radio network," U.S. Patent 8 644 768B2, 2014.

[17] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE)," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–8.

[18] "Microchip technology," Data Sheet AT86RF233, Microchip Technol. Inc., Chandler, AZ, USA, 2014. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8351-MCU_Wireless-AT86RF233_Datasheet.pdf

[19] M. Pelka, C. Bollmeyer, and H. Hellbrück, "Accurate radio distance estimation by phase measurements with multiple frequencies," in *Proc. Int. Conf. Indoor Position. Indoor Navig. (IPIN)*, 2014, pp. 142–151.

[20] O. Oshiga, A. Ghods, S. Severi, and G. Abreu, "Efficient slope sampling ranging and trilateration techniques for wireless localization," in *Proc. IEEE Workshop Position., Navig. Commun. (WPNC)*, 2015, p. 6.

[21] G. von Zengen, Y. Schröder, S. Rottmann, F. Büsching, and L. C. Wolf, "No-cost distance estimation using standard WSN radios," in *Proc. 35th IEEE Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2016, pp. 1–9.

[22] Y. Schröder, D. Reimers, and L. Wolf, "Accurate and precise distance estimation from phase-based ranging data," in *Proc. Int. Conf. Indoor Position. Indoor Navig. (IPIN)*, 2018, pp. 1–8.

[23] P. Zand, A. Duzen, J. Romme, J. Govers, C. Bachmann, and K. Philips, "A high-accuracy concurrent phase-based ranging for large-scale dense BLE network," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, 2019, pp. 1–7.

[24] O. Oshiga, S. Severi, and G. T. F. De Abreu, "Superresolution multipoint ranging with optimized sampling via orthogonally designed Golomb rulers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 267–282, Jan. 2016.

[25] R. Ayyalasomayajula, D. Vasisht, and D. Bharadia, "BLoc: CSI-based accurate localization for BLE tags," in *Proc. 14th Int. Conf. Emerg. Netw. Exp. Technol.*, 2018, pp. 126–138.

[26] S. Duquennoy, A. Elsts, B. A. Nahas, and G. Oikonomo, "TSCH and 6TiSCH for Contiki: Challenges, design and evaluation," in *Proc. 13th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, 2017, pp. 11–18.

[27] T. Chang, T. Watteyne, K. Pister, and Q. Wang, "Adaptive synchronization in multi-hop TSCH networks," *Comput. Netw.*, vol. 76, pp. 165–176, Jan. 2015.

[28] "Contiki-NG, the OS for next generation IoT devices." [Online]. Available: https://www.contiki-ng.org/

[29] "LOG-a-TEC by SensorLab." [Online]. Available: https://log-a-tec.eu/

[30] Y. Schröder and L. Wolf, "InPhase: Phase-based ranging and localization," *ACM Trans. Sens. Netw.*, vol. 18, no. 2, pp. 1–39, Jan. 2022.



Grega Morano (Graduate Student Member, IEEE) received the M.Sc. degree in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 2021. He is currently pursuing the Ph.D. degree in information and communication technologies with Jožef Stefan International Postgraduate School, Ljubljana.

He currently works as a Research Assistant with the Department of Communication Systems, Jožef Stefan Institute, Ljubljana. Among his research interests are IoT communication protocols, integrated sensing and communication, wireless sensor networks, and wireless experimental testbeds.



Ke Guan (Senior Member, IEEE) received the B.E. and Ph.D. degrees from Beijing Jiaotong University, Beijing, China, in 2006 and 2014, respectively.

He is a Full Professor with the State Key Laboratory of Advanced Rail Autonomous Operation and the School of Electronics and Information Engineering, Beijing Jiaotong University. He is with the Department of Communication Systems at the Jožef Stefan Institute, Ljubljana, Slovenia. In 2015, he was awarded a Humboldt Research Fellowship for Postdoctoral Researchers. In 2009, he was a Visiting Scholar with the Universidad Politécnica de Madrid, Madrid, Spain. From 2011 to 2013, he was a Research Scholar with the Institut für Nachrichtentechnik, Technische Universität Braunschweig, Braunschweig, Germany. From September 2013 to January 2014, he was invited to conduct joint research with the Universidad Politécnica de Madrid. He has authored/coauthored two books and one book chapter, more than 200 journal and conference papers, and four patents. His current research interests include measurements and modeling of wireless propagation channels, high-speed railway communications, vehicle-to-x channel characterization, and indoor channel characterization for high-speed short-range systems including future terahertz communication systems.

Dr. Guan is the pole leader of the European Railway Research Network of Excellence (EURNEX). He was the recipient of the 2014 International Union of Radio Science Young Scientist Award. His papers received ten Best Paper Awards, including the IEEE Vehicular Technology Society Neal Shepherd Memorial Best Propagation Paper Award in 2019 and 2022. He is an Editor of *IEEE Vehicular Technology Magazine*, IEEE ACCESS, *IET Microwave, Antenna and Propagation*, and *Physical Communication*, and a Guest Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *IEEE Communications Magazine*. He serves as a Publicity Chair for PIMRC 2016, the Publicity Co-Chair for ITST 2018, the Track Co-Chair for EuCNC, the International Liaison of EUSIPCO 2019, the Session Convener for EuCAP 2015–2022, and a TPC Member for many IEEE conferences, such as Globecom, ICC, and VTC. He has been a delegate in 3GPP and a member of the IC1004 and CA15104 initiatives.



Andrej Hrovat (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 2004 and 2008, respectively, and the Ph.D. degree from Jožef Stefan International Postgraduate School, Ljubljana, in 2011.

He has been with the Department of Communication Systems, Jožef Stefan Institute, Ljubljana, since 2004, where he is a Senior Research Fellow. He is an Associate Professor with Jožef Stefan International Postgraduate School. He works on several projects connected with professional mobile communication systems, 2/3/4G, WiFi and WiMAX technologies, satellite and sensor networks, including several COST actions, Framework Program projects, H2020 projects, European Space Agency projects, and numerous national research and application projects. He is the author or coauthor of more than 80 peer-reviewed journal and conference papers. His research and working experience are in the field of telecommunications, focusing on development and performance analysis for fixed and mobile systems, including terrestrial, stratospheric, and satellite systems, and radio-channel modeling for fixed and mobile narrowband and broadband radio communication systems.

Dr. Hrovat serves as a journal editorial board member and a guest editor, and a reviewer for several international impact-factor journals, and is a TCP member for various international conferences and workshops.



Tomaž Javornik (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 1987, 1990, and 1993, respectively.

He is a Scientific Counsellor with the Communication Systems Department, Jožef Stefan Institute, Ljubljana, and an Assistant Professor with Jožef Stefan International Postgraduate School, Ljubljana. He participated in several COST and Framework Programme projects. He has coauthored more than 100 refereed journal and conference papers and several books and book chapters in the field of mobile and wireless communications. He holds two international patents. His research experience is in the field of telecommunications, focusing on the development and performance analysis of fixed and mobile systems, radio-channel measurements, modeling and simulations and in indoor localization.

Dr. Javornik serves as a TPC member or a reviewer for several IEEE conferences and journals.

Chapter 3

Integration of Angle-of-Arrival Estimation into TSCH Communication

Direction estimation based on the AoA technique complements distance estimation by providing angular information fundamental for wireless localization, allowing devices to determine orientation and relative position from the received signal. A device equipped with multiple spatially separated antennas exhibits phase differences between antenna elements, which depend on the direction of the incoming signal. The phase information enables estimation of the AoA using algorithms such as MUltiple SIgnal Classification (MUSIC), Apace-Alternating Generalized Expectation-maximization (SAGE) or Estimation of Signal Parameters via Rotational Invariance Techniques (ESPRIT) [67]. In advanced wireless architectures, the spatial distribution of antennas is achieved with multiple parallel RF chains that enable simultaneous phase measurements and deliver high localization accuracy. The use of multiple radios introduces high hardware cost, energy consumption, and implementation complexity, making such architectures impractical for IoT platforms. For constrained devices, a more suitable solution is to employ an antenna switching network that connects a single RF chain to several spatially distributed antennas. However, sequential sampling of antennas introduces sensitivity to Carrier Frequency Offset (CFO), requiring careful design of the switch sequence and sampling intervals to preserve the accuracy of AoA estimation [36].

Despite the challenges of sequential antenna sampling, we investigate how AoA estimation can be seamlessly integrated into the IEEE 802.15.4 TSCH protocol by leveraging the lightweight single RF chain architecture, addressing hypothesis **H1**. In the paper presented in this chapter, we introduce a modification of the TSCH timeslot structure that incorporates a dedicated Phase Measurement Process (PMP), enabling the device to gather phase samples while switching across an antenna array within the predefined measurement intervals. The proposed mechanism enables AoA estimation with each received packet, transforming the communication network into a dual-purpose system, and delivering contribution **C1.2**. Although the extension reduces throughput by 20%, the key communication properties of TSCH remain intact, confirming that AoA estimation can be integrated with minimal trade-offs.

We developed a signal model to characterize how CFO and Sampling Frequency Offset (SFO) affect AoA accuracy and to enable full exploitation of sequential phase measurements. With low-cost IoT hardware, maintaining identical transmit and receive frequencies is challenging, and even small CFO values lead to large cumulative phase errors. We introduced additional reference measurement slots in PMP, that are used to estimate CFO

and calibrate phase measurements before AoA processing, addressing hypothesis **H2**. We tested different CFO estimation algorithms, including the common linear and Moose methods as well as the proposed FFT based approach. Through extensive simulations, we found that the FFT-based method delivered greater robustness to noise and accuracy across a broad CFO range. We further proposed a two-stage CFO calibration scheme: a coarse estimate from the reference samples, followed by a fine estimate using antenna switching samples. The calibration process improved robustness and enhanced angle estimation accuracy across different operating conditions, representing contribution **C2**.

For experimental validation, we selected OpenMote-B platforms with AT86RF215 radio because their accurate phase measurement capability and Continuous Wave (CW) operation align with the requirements of the proposed system. We developed radio drivers to implement the proposed solution in Contiki-NG Operating System (OS), which were later accepted into the official distribution (release 5.1), providing contribution **C5**. For the antenna array, we employed an in-lab developed circular design [36], combined with an RF switch for sequential sampling. The implementation represents contribution **C3.2**, a practical ISAC prototype built on constrained IoT hardware.

The proposed approach was validated through a measurement campaign conducted in an indoor hallway under LoS conditions. During the experiments, the nodes exchanged packets over 16 frequency channels defined in IEEE 802.15.4, estimating AoA from each transmission. The measurement analysis revealed that multipath propagation distorts real-world AoA estimation and produces frequency-dependent spurious results, representing contribution **C4**. To mitigate multipath effects, we leveraged the channel hopping feature of TSCH, aggregating measurements from different frequency channels and combining them using the median of successive estimates to suppress errors. With 16 successive AoA estimates under a Round Robin switching scheme, the mean absolute error was consistently below 1.7°, with the standard deviation typically below 1°. The results confirm that accurate AoA estimation can be achieved on constrained IoT platforms with acceptable communication trade-offs, supporting hypotheses **H1** and **H2**. The measurement datasets and the software implementation are available as an open-source solution, promoting reproducibility and further research, providing contribution **C5**.

Publication included in this chapter:

G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, **"Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol"**, in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2023, pp. 1–7. DOI: 10.1109/PIMRC56721.2023.10293886

Created open-access resources:

Measurement dataset

G. Morano, A. Simončič, T. Javornik, and A. Hrovat, *Phase Measurements for AoA Estimation in IEEE 802.15.4 TSCH-based Networks*, Zenodo, Oct. 29, 2025. DOI: 10.5281/zenodo.17476028

Software implementation

Contiki-NG contributors, *Contiki-NG OS for Next Generation IoT Devices*, GitHub repository, 2023. [Online]. Available: https://github.com/9morano/contiki-ng/tree/openmote-aoa

Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol

Grega Morano*†, Aleš Simončič*†, Teodora Kocevska*†, Tomaž Javornik*†, Andrej Hrovat*†
*Department of Communication Systems, Institute "Jožef Stefan", Ljubljana, Slovenia
†Jožef Stefan International Postgraduate School (IPS), Ljubljana, Slovenia.
Emails: {grega.morano,ales.simoncic}@ijs.si, kocevska46@gmail.com, {tomaz.javornik,andrej.hrovat}@ijs.si

***Abstract*—Wireless localization and sensing functions play a crucial role in facilitating collaboration and interaction between people and machines in Industry 5.0. Driven by the Integrated Sensing and Communication (ISAC) paradigm, we modify the Time Slotted Channel Hopping (TSCH) protocol to support Angle of Arrival (AoA) estimation, enabling joint localization and communication functionalities. The TSCH timeslot is extended allowing the AoA to be estimated with each received packet. In order to improve the accuracy of the AoA estimates and enable estimation even at high Carrier Frequency Offset (CFO), we propose a two-stage CFO calibration method. The operation of the proposed solution is validated in an indoor scenario utilizing low-cost off-the-shelf components. By utilizing 16 successive AoA estimates with a Round Robin antenna switching pattern, the standard deviation and the mean absolute error are on average below 1.7°.**

***Index Terms*—Angle of Arrival (AoA), IEEE 802.15.4, Time Slotted Channel Hopping (TSCH), Integrated Sensing and Communication (ISAC), Industrial Internet of Things (IIoT), industry 5.0**

I. Introduction

Future industry [1] will rely heavily on advances in wireless technologies [2]. At the same time, the industry requirements [3] will be one of the key drivers for the development of next-generation wireless technologies [4]. Wireless systems have to be intelligent and adaptable to provide ultra-reliable, low-latency communications for a wide range of use cases across a variety of emerging vertical industries. Therefore, the adoption of advanced technologies [5], such as digital twin, terahertz, visible light, industrial massive MIMO, reconfigurable intelligent surfaces, and localization is needed for enhancing the performance of industrial wireless communications and design of the wireless network that connects people and robots in the mixed real-physical and virtualized-digital world and supports advanced manufacturing in Industry 5.0.

Angle of Arrival (AoA) estimation [6] is foreseen to be significant for improved communication and localization of nodes in the Industrial Internet of Things (IIoT) [7]. The research on indoor localization has been active for many years [8]. The developments towards Industry 5.0 motivated the research in high-accuracy and low-cost localization for industrial applications [9]. The industrial environment presents a particular challenge for accurate localization due to the electromagnetic effects of industrial equipment, the harsh propagation environment resulting in multipath propagation, and the presence of people. Therefore, novel solutions are needed for precise and seamless localization in dynamic industrial environments.

The localization and sensing functionalities are envisioned to be integrated with the communication in the future wireless systems [10], to optimize the overall system performance and to enable new applications; a paradigm referred to as integrated communication and sensing (ISAC). Reported studies have been investigating solutions that allow devices to communicate and sense over a common waveform, a single hardware platform, a signal processing framework, and/or a network infrastructure.

One of the communication protocols specifically designed to address the unique challenges and requirements of industrial-grade applications is the Time Slotted Channel Hopping (TSCH) protocol defined in the IEEE 802.15.4-2015 standard [11]. It is designed to be robust to interference and adapt to changing environmental conditions through a channel hopping mechanism that alleviates the effects of multipath propagation by changing the communication carrier frequency with each transmission. Features such as time synchronization, determinism, energy efficiency, and scalability make TSCH well-suited for demanding industrial applications where predictable and reliable wireless communications are essential. Adding extra functionality of AoA estimation, which can be used for localization, would further improve usability and meet some of the requirements of Industry 5.0.

To integrate AoA into a wireless protocol, the receiver must know the transmitted symbols in advance to measure the phase of the signals that contain the angle of arrival information. Prior to the integration of the AoA function into wireless protocols, the well-known sequence of preamble [12] or pilot signals [13] were used to estimate the AoA. The proposed AoA integration in the TSCH protocol follows a similar implementation to the AoA integration in the Bluetooth Low Energy (BLE) standard [14], where the constant tone extension (CTE) is appended to a data packets to transmit the unmodulated signal or preform the AoA estimation.

Motivated by the possibility of incorporating localization functionality into the TSCH communication protocol, in this paper, we focus on integrating accurate AoA estimation into the communication. To further improve the accuracy of AoA, we have developed a measurement calibration technique. The proposed approach is validated by measurements performed in a real-world indoor environment. The contributions of this

study are summarized as follows.

- Integration of AoA estimation functionality for single RX chain devices into the TSCH communication protocol;
- Two-step approach for channel frequency offset (CFO) estimation and calibration;
- Validation of the proposed approach in an indoor environment using off-the-shelf radio transceivers with single RX chain and a proprietary antenna array.

The remainder of this paper is structured as follows. In Section II we introduce and describe in detail the integration of AoA into the TSCH protocol. The phase measurement procedure with switching antennas and the CFO estimation and calibration approach are explained in Section III. Section IV covers the real-world validation procedure, including the measurement setup and discussion of the results. Finally, concluding remarks are drawn and directions for future work are suggested in Section V.

II. AoA integration

The integration of AoA functionality into the TSCH protocol requires a detailed analysis of the requirements for AoA estimations that have to be considered when implementing the solution into the TSCH protocol. The proposed generic solution, applicable to any analog radio, has been modified for currently available low-cost off-the-shelf radios.

A. Estimating the angle of arrival

The AoA can be estimated using multiple antennas separated by a distance that is less than half of a signal's wavelength. When the receiver (RX) is placed in the far field of the transmitter (TX), the distance of signal travelling to the individual antennas differs by Δd which can be translated into the phase difference $\Delta\phi = 2\pi\frac{\Delta d}{\lambda}$. The phase difference is then used to estimate the AoA and is usually the input of the high-resolution AoA algorithms [15]. In this paper, we have validated the accuracy of AoA estimation using the MUltiple SIgnal Classification (MUSIC) algorithm [16], which is renowned for its resilience to noise and is, therefore, suitable for industrial applications.

B. Antenna array and switching pattern

Obtaining the phases from different antennas depends on the architecture of the receiver and antenna setup. The radios that support IEEE 802.15.4 are typically designed to be low cost, low power, and low complexity, resulting in the implementation of a single radio frequency signal chain. Therefore, to integrate the AoA into the TSCH protocol, we propose to use an antenna switching circuit to acquire the phase samples from multiple antennas, which provides a low-cost, and low-power solution with fast switching times.

In the paper two different switching patterns are analyzed: (i) Round Robin (RR) and (ii) Return-To-First (RTF). The first approach provides more samples per antenna, while the second provides additional samples on a reference antenna that can be used to calibrate the measurements. The scheme of switching patterns for a single cycle is shown in Table I,

TABLE I
SELECTED SWITCHING PATTERNS

Round Robin	a_0, a_1, a_2, a_3, ..., a_{N-1}
Return-To-First	a_0, a_1, a_0, a_2, ..., a_0, a_{N-1}

where a_n represents the antenna element in the N element antenna array so that $n \in [0, N)$.

To validate the AoA solution integrated into the TSCH protocol, we used the 12-element uniform circular array (UCA) antenna array from [17]. It was designed for the 2.4 GHz frequency band, making it compatible with the IEEE 802.15.4 standard in 2.4 GHz ISM band. Its validation with BLE technology provided promising results for AoA estimation.

C. Radio transceivers

Different radios designed for the IEEE 802.15.4 standard exist, which supports fast frequency synthetization required by TSCH protocol. However, to our knowledge, only two of them provide a function of measuring the phase of the received signal. In 2012, Atmel (now Microchip) released a radio AT86RF233 [18] that offered an extended feature called Phase Measurement Unit (PMU) that can sample the phase angle of the incoming signal. After additional configuration of the radio, the measurement is available to the user with an update interval of 8 us. An improved version of the radio called AT86RF215 [19] was released in 2015, which, in addition to phase measurement, provides an options of sampling the IQ values of the signal, measuring the carrier frequency deviation, and calculating the quality factor of the phase measurement. Unlike the AT86RF233 radio, the AT86RF215 also provides support for synchronization. The value of the 1 MHz counter is accessible in the radio's register and all measured values are updated after the counter transits from 7 to 0, resulting in an update interval of 8 us. Both radios also support the transmission of continuous wave (CW) signals, which are required for the proposed method.

D. TSCH protocol modification

The time for communication in the TSCH protocol is divided into timeslots that coordinate the intervals for packet preparation, payload reception/transmission, and acknowledgement exchange, as shown in Figure 1. To add an AoA estimation function to the protocol, we propose to extend the timeslot with an additional procedure referred to as phase measurement process (PMP).

The structure of the PMP is determined by the desired number of samples collected and the sampling rate of the radio. Although the radios used in this study require 8 us to sample a phase, the time required to switch between antennas has to be considered because changing the signal path during the measurement will corrupt the signal. Therefore, we construct a 16 us long sampling slot in which the radio first measures the phase and then immediately selects the following antenna. This method ensures that the antenna is not changed

during the measurements, as one measurement is discarded while waiting for the 16 us period to end.

The number of samples obtained per antenna determines the accuracy of the MUSIC algorithm. As shown in [17], the higher the number of samples per antenna, the better the root mean square error (RMSE) of the estimated AoA. As a tradeoff between the time allocated for sensing and the time available for communication, we decided to create 90 slots for phase measurements, which result in duration of 1440 us. To account for the additional time required for radio preparation, we defined the length of the PMP to 2 ms. The introduced sensing method therefore reduces the throughput of the network by a factor of 0.2, since the time available for communication is reduced.

90 slots for phase measurements were selected to accommodate sufficient amount of samples per antenna and to allow different types of switching patterns with various number of antenna elements. In case of antenna array with 12 elements applying RR or RTF switching pattern, the number of samples per antenna is 7 and 4 respectively.

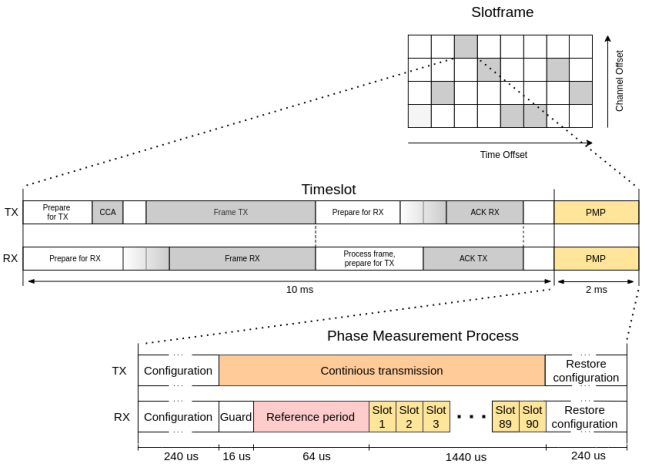


Fig. 1. Phase measurement process integrated into TSCH protocol

As shown in the following chapter, the measured phase deviates from the actual value due to induced phase offsets that lead to impairments of the result. To estimate the impairments, we added a reference period in which 8 phase samples are to be obtained on a single antenna. Since antenna switching is not considered, the sampling rate is equal to 8 us and the reference period lasts 64 us.

Phase measurement is currently not part of the normal radio operation during communications, so an additional 240 us is provided for radio preparation at the beginning of the PMP and another 240 us dedicated for restoring the initial configuration at the end of the PMP. After configuration, the PMP differs between the transmitter and receiver; TX immediately begins transmitting the continuous wave signal for 1520 us, while the receiver first waits for a guard period of 16 us before starting phase measurements.

The chosen timings were determined by measuring the time required for individual operation, and thus enable the support for both Atmel's radios. In case of native hardware support for phase measurement and faster sampling times, the PMP could be shorten to minimize the effect taken on the communication.

III. Measurement Impairment Mitigation

Noise due to hardware limitation and other sources introduced in measured samples, affects the accuracy of the AoA estimate. With a detailed analysis of phase sampling with switching antenna arrays, we first investigate the sources of measurement error and then present a method for calibration.

A. Phase measurement with switching antenna

To measure the phase angle of a signal, the transmitter emits an unmodulated continuous wave signal $s_{tx}(t)$. In a heterodyne receiver, the received signal $s_{rx}(t)$ is first down-converted to the intermediate frequency f_{if} by mixing the signal with the local oscillator signal $s_{lo}(t)$ tuned to the desired receiving frequency f_{rx}, such that $f_{if} = f_{tx} - f_{rx}$. Afterwards, the higher frequency components are filtered out and the signal results in $s_{if}(t)$, as depicted in Figure 2. The phase of the incoming signal is measured by comparing the signal $s_{if}(t)$ with a local reference signal $s_s(t)$ with sampling frequency f_s. As explained in [20], this process is performed within the PMU as follows:

$$\begin{aligned}\phi_n &= \left(2\pi f_{if} t - 2\pi f_{tx}\left(\frac{d_n}{c}\right) + \varphi_{tx} - \varphi_{rx}\right) \\ &\quad - (2\pi f_s t + \varphi_s) \\ &= \underbrace{2\pi(f_{if} - f_s)t}_{time} - \underbrace{2\pi f_{tx}\left(\frac{d_n}{c}\right)}_{space} + \underbrace{\varphi_{tx} - \varphi_{rx} - \varphi_s}_{initial}, \end{aligned} \quad (1)$$

where ϕ_{tx}, ϕ_{rx} and ϕ_s are the random initial phases of the transmitted signal, local oscillator signal, and reference signal, respectively, and d_n is the distance between the TX and the n-th antenna, and c is the speed of light. The equation presents the structure of the measured phase, which consists of time-dependent, space-dependent, and initial phase offset terms. The space-dependent term contains the AoA information, while the other terms represent the possible impairments in the measurement.

The phase difference $\Delta\phi$ between the antennas is needed for AoA estimation. Subtracting the phase obtained at the n-th antenna from the phase at the reference antenna yields:

$$\Delta\phi' = \phi_0 - \phi_n = 2\pi f_{tx}\frac{n\Delta d}{c} \quad (2)$$

where Δd is the additional distance traveled by the signal compared to the reference antenna. The subtraction cancels out the unknown initial phase offsets since neither the receiver nor the transmitter restarts during the measurement process and initial offsets stay the same. Since a single RX chain with an RF switch is used to capture the phases from different antennas, the time at which the sample was made must be considered. Even if the source signal is constant over time, there is still a phase progression, and (2) no longer holds. The

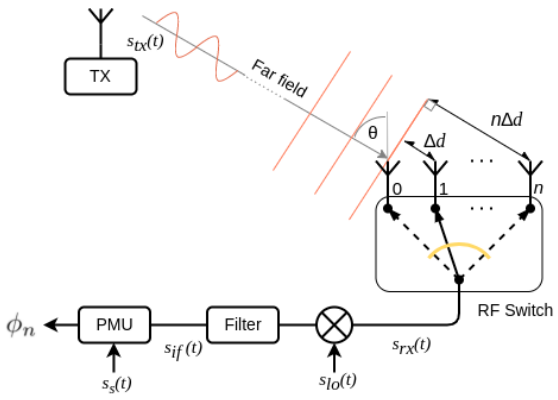


Fig. 2. Receiver architecture

phase difference of two successive samples is therefore equal to:

$$\Delta\phi = 2\pi(f_{off})T_s + 2\pi f_{tx}\frac{\Delta d}{c} = \Delta\phi_{CFO} + 2\pi f_{tx}\frac{\Delta d}{c}, \quad (3)$$

where T_s is the sampling interval between two measurements at different antennas, and $f_{off} = f_{tx} - f_{rx} - f_s$ represents the frequency offset, which includes both the Carrier Frequency Offset (CFO) and Sampling Frequency Offset (SFO). Since both contribute to the same frequency offset, we model them under the single abbreviation CFO. Achieving the same transmitting and receiving frequencies using real hardware is a difficult task [21], especially with low-cost hardware used in IoT devices. Therefore, the measured phase deviates from its true value as the sampling interval increases. Accumulated phase offset, caused by the CFO, affects the accuracy of the AoA estimation, thus we present an algorithm to compensate for it.

B. CFO estimation and calibration

CFO estimation is a well-known problem in communication systems and the solutions presented are mostly optimized for time efficiency and low computational complexity, allowing a wide estimation range [12], [22]. However, for AoA, high accuracy is required along with noise insensitivity and sufficient measurement range. Since the signal in the PMU is undersampled at a sampling frequency of $f_s = f_{if}/8$, the phase in the CFO case experiences a linear increase that affects the estimated AoA. The angle estimation error for a CFO of 200 Hz considering no noise, the RR switching pattern and the use of the antenna array described in II-B results in an error of 0.7°using the MUSIC algorithm. Therefore, it is necessary to estimate the CFO and compensate for it prior the AoA calculation.

To select the most appropriate method for CFO calibration, we first analyzed and compared three widely used methods for CFO estimation for different signal-to-noise ratios (SNR) and CFO values. The straightforward linear method [23] is used to estimate CFO by calculating the slope of the line fitted to the phase samples using the least square algorithm, which has an upper-frequency limit of $f_s/2$. Since the acquired phase samples fall in the range of 2π, phase unwrapping is required, which becomes a challenging task in the presence of noise.

Another commonly used method for CFO estimation is the Moose algorithm [12], [24], which is based on the assumption that phase samples begin to repeat after half the acquisition time. The Moose method has an upper frequency limit of $\frac{1}{T_a}$, where T_a is the acquisition time.

The third method, referred as the FFT method, utilizes the fast Fourier transform (FFT) [25]–[27] on the I/Q components derived from the phase samples. In the case of undersampling ($f_s = f_{if}/8$), the I/Q components have a sinusoidal shape whose frequency equals to the CFO. Although the resulting FFT spectrum has an upper-frequency limit of $f_s/2$, the FFT method itself, used to correct the phase samples due to the CFO and not to estimate the true CFO frequency, does not have this limitation due to the mirroring of frequencies around multiples of f_s as a consequence of sampling the signal and equality:

$$\Delta\phi_{CFO} = 2\pi(f_{off})T_s = 2\pi(f_{off} \pm k\ f_s)T_s \quad (4)$$

where k is an arbitrary integer. To further improve the resolution of the FFT method, we symmetrically zero-padded the I/Q samples at both ends, resulting in a final data length of 4096. To improve the accuracy of the estimated CFO, a parabolic interpolation of the FFT result is performed [28]. This approach circumvents the lower frequency limit of f_s/N, where N is the number of available phase samples.

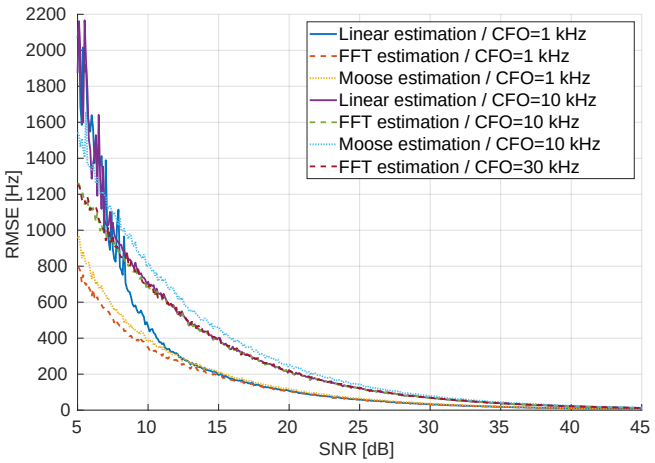


Fig. 3. RMSE of the different CFO estimation methods at different SNR levels for the reference period. For each SNR, the RMSE is calculated based on 1000 CFO estimates with a different noise.

To assess the precision of the CFO estimates, we performed simulations using the presented methods, as depicted in Figure 3. The RMSE of the CFO estimates was calculated from 1000 iterations with different signal-to-noise ratios (SNR). We first compared the behaviour of the CFO estimation methods by adding 1 kHz CFO to 8 phase samples. Although the differences between methods are small when the SNR is 15dB, the FFT method exhibits the smallest error below this value,

demonstrating its robustness to noise. The Moose and FFT methods offer a distinct advantage over the linear method by eliminating the need for phase wrapping. By adding 10 kHz to the samples,the methods incur a larger error compared to a 1 kHz CFO using the same number of samples as shown in Figure 3. We also performed a comprehensive comparison of all methods for CFO frequencies ranging from 10 kHz to 50 kHz. At lower SNR values, the error of the linear and Moose methods increases rapidly with increasing CFO. Conversely, the FFT method showed a relatively consistent error near the 10 kHz curve, indicating its reduced reliance on the CFO value.

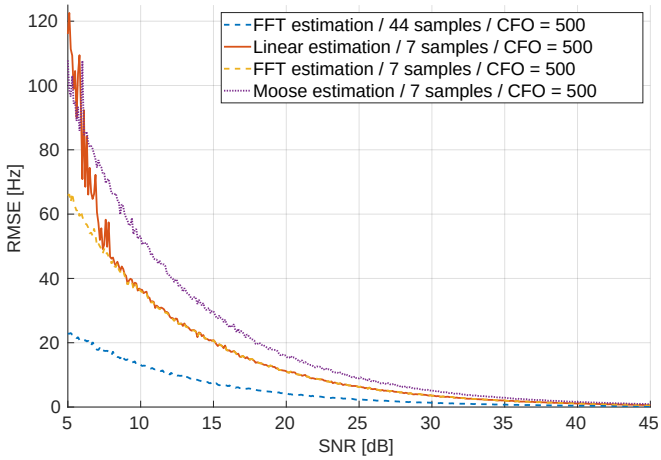


Fig. 4. RMSE of the different CFO estimation methods at different SNR values for samples obtained in sample slots. For each SNR, the RMSE is calculated based on 1000 CFO estimates with a different noise.

Presented methods can be applied for CFO estimation in the reference period, but due to the limited number of available samples, their accuracy is limited. To achieve higher accuracy, without extending the reference period to more than 8 samples, we propose a two-step CFO estimation. A course estimate of the CFO can be made using the reference samples, followed by a fine estimate using the samples from the sample slots. For the fine estimation, we can obtain 7 samples per antenna for the RR switching pattern with a sampling period of 192 μs. Alternatively, we can obtain 44 samples for the RTF switching pattern with a sampling period of 32 μs, as presented in Section II.

Figure 4 shows three CFO estimation methods used for CFO fine estimation with 7 available samples. The simulation setup was the same as in Figure 3, except that we added 500 Hz CFO to the phase samples. For SNR values above 8 dB, the Moose method performs worse, while the linear and FFT methods perform similarly. We also analyzed the accuracy of the FFT method for the RTF switching pattern, where 44 samples are available. It is evident that the RTF method provides higher CFO estimation accuracy.

More accurate CFO estimation using phase samples from sample slots is accompanied by a reduced upper-frequency limit for the linear and Moose methods. We propose to use the FFT method for course and fine CFO estimation because it is robust to noise, has no frequency constraints, and the CFO value has a minimal impact on its estimation.

IV. Validation procedure

To evaluate the proposed method, we conducted a measurement campaign in an indoor scenario using off-the-shelf devices. The measurements were performed under line-of-sight conditions in a 3 m $\times$ 40 m hallway in the "Jožef Stefan" Institute. The radio nodes are mounted on a stand, 1.6 m above the floor, separated by 3.5 m. We used OpenMoteB [29] devices with AT86RF215 radios connected to a computer performing the calculations. The radio drivers were developed to incorporate PMU and the protocol stack of the Contiki-NG operating system was modified to include the PMP. The code is openly available on GitHub [30]. A dipole antenna was used at the transmitter site and a circular antenna array was used at the receiver site [17]. To obtain measurements for different angles, the transmitter was stationary and the receiver antenna was rotated on its axis. The nodes exchanged packets on all available IEEE 802.15.4 channels, to initiate the measurements.



Fig. 5. Measurement setup in the "Jožef Stefan" Institute's hallway.

A. Evaluation of AoA estimation

We performed two sets of measurements for the two different switching patterns: RTF and RR. We gathered measurements for 12 angles ranging from 30° to 360°. The total number of measurements obtained is 8300 and 7873 for RTF and RR, respectively. Errors in the measurements may occur when the devices are not synchronized. The erroneous measurements were discarded by using the Quality Factor (QF) feature provided by the AT86RF215 radio. The inverse mean deviation of the measured phases within the PMU period is estimated and for measured phases with a QF below a

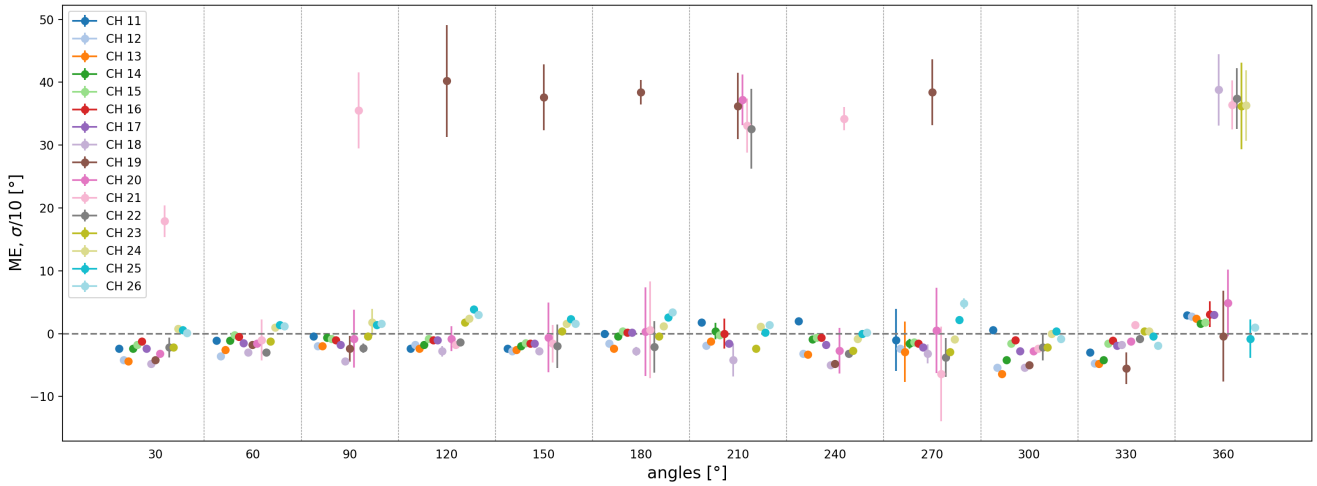


Fig. 6. Mean error (ME) and standard deviation σ (scaled by a factor of 10) of the estimated AoA per channel, for RR switching pattern.

TABLE II
MEASUREMENT RESULTS FOR RR AND RTF SWITCHING PATTERNS. MAE: MEAN ABSOLUTE ERROR, STD: STANDARD DEVIATION.

Estimated angle		30°	60°	90°	120°	150°	180°	210°	240°	270°	300°	330°	360°
RTF 8 packets	MAE [°]	1.95	7.27	1.59	0.92	0.7	2.25	1.86	5.08	3.64	4.14	12.42	8.95
	STD [°]	8.17	27.58	4.85	0.82	0.91	1.22	2.26	12.3	7.97	11.31	17.75	17.04
RR 8 packets	MAE [°]	2.22	1.2	0.99	1.06	1.65	0.77	1.13	1.87	1.83	1.97	2.25	5.56
	STD [°]	0.88	0.66	1.04	0.92	0.59	1.71	2.66	0.92	1.15	0.67	0.88	7.69
RTF 16 packets	MAE [°]	1.01	1.69	0.76	0.78	0.61	2.16	1.57	2.77	2.84	1.17	6.29	4.45
	STD [°]	1.16	6.73	1.04	**0.64**	0.77	0.77	2.03	1.51	1.33	1.54	11.28	8.23
RR 16 packets	MAE [°]	2.24	1.15	0.95	0.92	1.67	0.54	0.64	1.78	1.81	1.99	2.1	3.55
	STD [°]	**0.74**	**0.52**	**0.97**	0.7	**0.36**	**0.68**	**0.72**	**0.83**	**0.76**	**0.56**	**0.67**	**3.97**

threshold set to 100, the measurement is discarded. A total of 82 and 76 measurements were discarded for the RTF and RR sets, respectively.

The mean error of the angle estimation for a specific channel and its standard deviation are shown in Figure 6, where RR switching pattern was used. It is noted that some of the channels (e.g., channel 19) frequently report incorrect estimation due to multi-path propagation present in indoor scenarios. The MUSIC spectrum contains two peaks in these measurements, and the peak search algorithm returns the multipath component as the result, which is not the actual AoA. To avoid any special filtering solutions, we propose to obtain the angle estimation from multiple channels and use the median of the estimates as the final result. In Table II, two scenarios are presented where either 8 or 16 consecutive measurements were taken as the final result. The frequency channels, from which the measurement was taken, was pseudo-random, since the data were gathered sequentially while the devices were exchanging packets.

The accuracy of AoA estimation is improved for a larger number of consecutive packets, but the time between two estimations is longer. Although RTF provides more samples for CFO estimation, we can estimate CFO with the RR switching pattern and two-step CFO estimation. The results show that the resolution and accuracy are better when the RR pattern is used, mostly because of the larger number of samples per antenna available for the MUSIC algorithm. The standard deviation for RR with 16 consecutive packets is less than 1° for all angles, with an exception at angle 360°. In additional analysis of the data at this angle, we found, that communication often occurs on channels with multipath components.

B. Evaluation of CFO calibration

To validate the CFO calibration method, we manually changed the frequency of the receiving node to induce the custom CFO. We collected 460 measurements using the RR switching pattern with the nodes placed at an angle of 340°. The median of the angle estimates is given in Table III. The first row shows the results of AoA estimation without CFO

calibration (abbreviated as CC), while the second row shows the results when CFO calibration is considered. The results highlight the importance of CFO calibration. The estimated angles without the CFO calibration are completely wrong and even random, while the results with the CFO calibration show the accuracy of the angle within one degree.

TABLE III
COMPARISON OF AOA ESTIMATION AT AN ANGLE OF 340° WITHOUT (W/O) AND WITH (W/) CFO CALIBRATION.

CFO [kHz]	1	10	30	60	100
median AoA w/o CC [°]	342.8	97.7	155.1	324.7	127.2
median AoA w/ CC [°]	340.2	340.1	340.2	340.2	341.0

V. CONCLUSION

In this paper, we present a design of PMP and its integration into the TSCH protocol to enable AoA functionality alongside communication. We propose a two-step CFO calibration approach with FFT method to improve the AoA estimation. The operability of the proposed method was validated by a measurement campaign in an indoor scenario. Leveraging the channel hopping of the TSCH protocol, a sequence of 8 or 16 measurements was used, and the median value was taken as the AoA estimate to mitigate multipath effects. The RR switching pattern with 16 successive samples achieved a standard deviation below 1° for all angles except 360°. In the future work, the presented solution will be tested with other AoA estimation algorithms and different antenna arrays, which will offer new possibilities for sensing and localization applications in industrial environments.

REFERENCES

[1] A. Adel, "Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas," *Journal of Cloud Computing*, vol. 11, no. 1, pp. 1–15, 2022.

[2] Y. Ghildiyal, R. Singh, A. Alkhayyat, A. Gehlot, P. Malik, R. Sharma, S. V. Akram, and L. M. Alkwai, "An imperative role of 6G communication with perspective of industry 4.0: Challenges and research directions," *Sustainable Energy Technologies and Assessments*, vol. 56, p. 103047, 2023.

[3] P. K. R. Maddikunta, Q.-V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, "Industry 5.0: A survey on enabling technologies and potential applications," *Journal of Industrial Information Integration*, vol. 26, p. 100257, 2022.

[4] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6G technologies: Key drivers, core requirements, system architectures, and enabling technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 18–27, 2019.

[5] W. Xian, K. Yu, F. Han, L. Fang, D. He, and Q.-L. Han, "Advanced manufacturing in industry 5.0: A survey of key enabling technologies and future trends," *IEEE Transactions on Industrial Informatics*, pp. 1–15, 2023.

[6] A. Zandamela, A. Chiumento, N. Marchetti, and A. Narbudowicz, "Angle of arrival estimation via small iot devices: Miniaturized arrays vs. mimo antennas," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 146–152, 2022.

[7] S. Hayward, K. van Lopik, C. Hinde, and A. West, "A survey of indoor location technologies, techniques and applications in industry," *Internet of Things*, vol. 20, p. 100608, 2022.

[8] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[9] A. Karaagac, J. Haxhibeqiri, M. Ridolfi, W. Joseph, I. Moerman, and J. Hoebeke, "Evaluation of accurate indoor localization systems in industrial environments," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017, pp. 1–8.

[10] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, 2022.

[11] "IEEE Standard for Low-Rate Wireless Networks," pp. 1–709.

[12] "TyrLoc: A Low-cost Multi-technology MIMO Localization System with A Single RF Chain."

[13] Y. Zhao, W. Zhao, G. Wang, B. Ai, H. H. Putra, and B. Juliyanto, "AoA-based channel estimation for massive MIMO OFDM communication systems on high speed rails," *China Communications*, vol. 17, no. 3, pp. 90–100, Mar. 2020, conference Name: China Communications.

[14] B. SIG, "Bluetooth Core Specification, V 5.1," Bluetooth SIG, Tech. Rep. 5.1, 2019.

[15] Z. Chen, G. Gokeda, and Y. Yu, *Introduction to Direction-of-arrival Estimation*. Artech House, 2010, google-Books-ID: IsZQmAEACAAJ.

[16] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, Mar. 1986, conference Name: IEEE Transactions on Antennas and Propagation.

[17] A. Simončič, T. Javornik, A. Sešek, and A. Hrovat, "Direction of arrival estimation for BLE: Antenna array design and evaluation," *AEU - International Journal of Electronics and Communications*, p. 154722, May 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1434841123001966

[18] "AT86RF233." [Online]. Available: https://www.microchip.com/en-us/product/AT86RF233

[19] "AT86RF215." [Online]. Available: https://www.microchip.com/en-us/product/AT86RF215

[20] M. Gunia, A. Zinke, N. Joram, and F. Ellinger, "Setting up a phase-based positioning system using off-the-shelf components," in *2017 14th Workshop on Positioning, Navigation and Communications (WPNC)*, pp. 1–6.

[21] A. Mohammadian and C. Tellambura, "RF Impairments in Wireless Transceivers: Phase Noise, CFO, and IQ Imbalance – A Survey," *IEEE Access*, vol. 9, pp. 111 718–111 791, 2021, conference Name: IEEE Access.

[22] R. Ayeswarya and N. A. Prabha, "A Comprehensive Review: Techniques of CFO Estimation and Mitigation in OFDM," vol. 13, no. 16, 2018.

[23] H. Ye, B. Yang, Z. Long, and C. Dai, "A Method of Indoor Positioning by Signal Fitting and PDDA Algorithm using BLE AOA Device," *IEEE Sensors Journal*, vol. PP, pp. 1–1, Jan. 2022.

[24] P. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Transactions on Communications*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994, conference Name: IEEE Transactions on Communications.

[25] M. S. A. Raboh, H. M. Zakaria, and M. M. E. Bahy, "Carrier Frequency Offset (CFO) Estimation Methods, A Comparative Study."

[26] J. Meng, H. Wang, P. Ye, L. Guo, Y. Zhao, W. Wei, and H. Zeng, "Carrier Frequency Offset Estimation Based on Twice FFT Matrix Algorithm," in *2019 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, May 2019, pp. 1–6, iSSN: 2642-2077.

[27] Y. Wang, L. Li, R. Li, T. Fu, x. Fu, and x. Tianhui, "An Improvement Method of Frequency Offset Estimation Performance in Communication System Carrier Synchronization," in *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Oct. 2016, pp. 454–458.

[28] J. O. Smith, *Spectral Audio Signal Processing*. W3K, 2011, google-Books-ID: NXRMcgAACAAJ.

[29] FIT IoT-LAB. FIT IoT-LAB. [Online]. Available: https://iot-lab.github.io/docs/boards/openmoteb/

[30] G. Morano, "Contiki-NG: The OS for Next Generation IoT Devices," Dec. 2022, original-date: 2022-12-12T10:03:45Z. [Online]. Available: https://github.com/9morano/contiki-ng

Chapter 4

Hybrid Localization with TSCH Communication

Standalone distance or angle estimations provide valuable information about spatial relationships and relative positioning but face practical limitations when used for localization in real IoT deployments. Distance-based methods typically use lateration scheme, requiring at least three anchors with known positions to localize a node in Two Dimension (2D). Ensuring overlapping coverage with anchor positions imposes substantial deployment constraints that demand careful planning for each setup and lead to higher costs. Similarly, angulation methods that rely on AoA information require at least two reference nodes for 2D localization. Moreover, each anchor node must be equipped with an antenna array, which is expensive and often infeasible for small, low-power IoT devices. A hybrid localization approach that combines distance and angle estimation enables 2D localization with only a single anchor node, reducing the need for dense anchor deployment. The hybrid scheme is especially attractive for constrained IoT scenarios, where a single node equipped with an antenna array can localize nearby simple, low-cost tags. Reducing dependency on multiple anchors lowers costs, simplifies network planning, reduces backhaul and power requirements, and makes the system more practical for real-world IoT deployments.

Hybrid localization also aligns with the native topology of TSCH systems, which commonly employ the RPL routing protocol. RPL organizes the network into a tree-like structure where a root node serves as the gateway, and data traffic primarily flows between parents and their children, with limited peer-to-peer exchange. This hierarchical organization makes the implementation of lateration or angulation challenging, as they require arbitrary inter-node measurements that disrupt the communication structure. In addition, the schemes depend on measurement exchanges with several anchors, increasing airtime, collision probability, and energy consumption. In contrast, the hybrid approach can leverage the parent node as a sensing anchor, equipped with an antenna array, to localize its children. Localization can be achieved with a single channel probing, preserving battery life and reducing channel occupancy and latency, which are critical in dense IoT deployments. Such design leverages the inherent network structure and enables accurate and efficient localization with minimal overhead, demonstrating the principles of communication-centric ISAC design.

Recognizing the advantages, we integrate the hybrid localization scheme into the IEEE 802.15.4 TSCH protocol, extending network functionality with joint sensing and communication capabilities and addressing hypothesis **H1**. In the paper presented in this chapter, we extend our previous work by modifying the TSCH timeslot to include a dedicated phase measurement process, enabling nodes to estimate both the angle and the distance to their neighbors alongside the regular packet exchanges. The estimates are

used to determine a location of a device with each transmitted packet, without requiring substantial protocol modifications or disrupting the network structure, representing a communication-centric ISAC design and contributing to **C1.3**.

The operation of the proposed approach was demonstrated through a system-level prototype implemented on the VESNA micro-controller platform, forming contribution **C3.3**. We developed an extension shield built around the AT86RF215 radio and a RF switch that can accommodate an antenna array with up to eight elements. The board design ensures that all traces from the RF switch to the antenna connectors are of equal length and that each path contributes equally to the overall phase delay, preventing errors in AoA estimation. The developed radio drivers and proposed hybrid localization approach were implemented in the Contiki-NG OS. During the measurement campaign, six devices placed in an empty office formed the IEEE 802.15.4 TSCH network, and the root node, placed in the center of the room, attempted to determine the positions of child nodes alongside communication.

The empirical validation of the hybrid scheme through an extensive experimental campaign and result analysis represent contribution **C4**. The MUSIC algorithm was used for angle estimation and an FFT-based algorithm for ranging. While single measurements exhibited errors of 6 m, applying median filtering across 16 successive estimates improved robustness to multipath, lowering the maximum error to below 0.65 m. As the acquisition time for 16 measurements was 1.92 s, which is impractical for mobile device scenarios, we investigated the trade-off between refresh rate and accuracy. We proposed using only five successive measurements, reducing the acquisition time to 0.6 s while keeping the maximum error below 2 m and the average localization error at 0.37 m. The results demonstrate that sub-meter localization accuracy is achievable in real-world TSCH networks, confirming hypotheses **H1** and **H3**.

Finally, we released the datasets as well as the Contiki-NG software implementation to the community, supporting future research and providing contribution **C5**. The comprehensive solution establishes a practical foundation for hybrid localization in IEEE 802.15.4 TSCH networks and paves the way for future ISAC applications in resource-constrained IoT systems.

Publication included in this chapter:

G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, **"Distance- and Angle-Based Hybrid Localization Integrated in the IEEE 802.15.4 TSCH Communication Protocol"**, *Sensors*, vol. 24, no. 12, p. 3925, Jan. 2024, ISSN: 1424-8220. DOI: 10.3390/s24123925

Created open-access resources:

Measurement dataset

G. Morano, A. Simončič, T. Javornik, and A. Hrovat, *Distance and Angle Measurements for Hybrid Localization in IEEE 802.15.4 TSCH Networks*, Zenodo, Oct. 30, 2025. DOI: 10.5281/zenodo.17481601

Software implementation

Contiki-NG contributors, *Contiki-NG OS for Next Generation IoT Devices*, GitHub repository, 2023. [Online]. Available: https://github.com/9morano/contiki-ng/tree/vesna-atasw

sensors

MDPI

Article

Distance- and Angle-Based Hybrid Localization Integrated in the IEEE 802.15.4 TSCH Communication Protocol

Grega Morano [1,2,*], Aleš Simončič [1,2], Teodora Kocevska [1], Tomaž Javornik [1,2] and Andrej Hrovat [1,2]

[1] Jožef Stefan Institute, Jamova cesta 39, 1000 Ljubljana, Slovenia; ales.simoncic@ijs.si (A.S.); teodora.kocevska@ijs.si (T.K.); tomaz.javornik@ijs.si (T.J.); andrej.hrovat@ijs.si (A.H.)
[2] Jožef Stefan International Postgraduate School, Jamova cesta 39, 1000 Ljubljana, Slovenia
* Correspondence: grega.morano@ijs.si

Abstract: Accurate localization of devices within Internet of Things (IoT) networks is driven by the emergence of novel applications that require context awareness to improve operational efficiency, resource management, automation, and safety in industry and smart cities. With the Integrated Localization and Communication (ILAC) functionality, IoT devices can simultaneously exchange data and determine their position in space, resulting in maximized resource utilization with reduced deployment and operational costs. Localization capability in challenging scenarios, including harsh environments with complex geometry and obstacles, can be provided with robust, reliable, and energy-efficient communication protocols able to combat impairments caused by interference and multipath, such as the IEEE 802.15.4 Time-Slotted Channel Hopping (TSCH) protocol. This paper presents an enhancement of the TSCH protocol that integrates localization functionality along with communication, improving the protocol's operational capabilities and setting a baseline for monitoring, automation, and interaction within IoT setups in physical environments. A novel approach is proposed to incorporate a hybrid localization by integrating Direction of Arrival (DoA) estimation and Multi-Carrier Phase Difference (MCPD) ranging methods for providing DoA and distance estimates with each transmitted packet. With the proposed enhancement, a single node can determine the location of its neighboring nodes without significantly affecting the reliability of communication and the efficiency of the network. The feasibility and effectiveness of the proposed approach are validated in a real scenario in an office building using low-cost proprietary devices, and the software incorporating the solution is provided. The experimental evaluation results show that a node positioned in the center of the room successfully estimates both the DoA and the distance to each neighboring node. The proposed hybrid localization algorithm demonstrates an accuracy of a few tens of centimeters in a two-dimensional space.

Keywords: integrated localization and communication (ILAC); hybrid localization; direction of arrival (DoA); multi-carrier phase difference (MCPD); IEEE 802.15.4; time-slotted channel hopping (TSCH); AT86RF215

check for updates

Citation: Morano, G.; Simončič, A.; Kocevska, T.; Javornik, T.; Hrovat, A. Distance- and Angle-Based Hybrid Localization Integrated in the IEEE 802.15.4 TSCH Communication Protocol. *Sensors* **2024**, *24*, 3925. https://doi.org/10.3390/s24123925

Academic Editor: Davy P. Gaillot

Received: 26 April 2024
Revised: 13 June 2024
Accepted: 14 June 2024
Published: 17 June 2024

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

1. Introduction

The emergence of context-aware applications in industry and smart cities requires localization functionalities in Internet of Things (IoT) wireless communications to improve operational efficiency, safety, user experience, and resource management. In industrial applications, localization is crucial for tracking assets, managing inventory efficiently, and optimizing logistics by precisely locating equipment and goods in real time [1,2]. Smart cities benefit from localization through improved public safety and traffic management systems, where the precise location of vehicles and pedestrians can significantly improve routing efficiency and emergency response [3]. In smart homes, localization functions enable more sophisticated control and automation, adjusting lighting, heating, or security systems based on the presence and movements of occupants. In consumer applications,

Sensors **2024**, *24*, 3925

such as indoor navigation in museums, malls, or airports, localization can significantly improve the user experience by providing more accurate and reliable directions [4]. Localization with wireless systems can be achieved by observing the communication channel's characteristics during packet exchange; thus, the same hardware can be used for dual purposes [5]. Integrated Localization and Communication (ILAC) [6,7] enables IoT devices to simultaneously exchange data and determine and report their position in space, maximizing resource utilization while reducing deployment and operation costs.

In challenging scenarios with many obstacles and complex propagation, IoT protocols that can mitigate interference and multipath fading and ensure that consistent data transmission are promising enough to provide localization functionality. IEEE 802.15.4 Time-Slotted Channel Hopping (TSCH) [8] is particularly suitable due to its use of the channel hopping technique, which can efficiently mitigate the issues of interference and multipath fading by changing the transmission frequency in a pseudo-random manner [9]. Low power consumption and high reliability make the protocol suitable for critical IoT applications in harsh environments. Integrating accurate localization functionality into TSCH will further enhance the effectiveness and operational capabilities of the protocol and open up new possibilities for automation, monitoring, and interaction within physical environments. The integration design has to ensure that communication reliability and network efficiency are not adversely affected by the additional localization capabilities.

Localization based on channel metrics from wireless systems, where the location of a target device is determined based on its interaction with devices with known locations referred to as anchors, has been used for indoor environments where satellite-based localization systems optimized for outdoor environments do not operate [1,10]. The location can be determined with the fingerprinting technique or by using more advanced and accurate geometric methods based on a separate or joint use of distance and angle estimations. Lateration is a common two-dimensional (2D) localization method that uses distance estimation from the target to at least three anchor devices. The distance between devices can be estimated through various techniques that include Received Signal Strength Indicator (RSSI), Time of Arrival (ToA) and Phase-Based Ranging (PBR). While RSSI-based methods estimate distance by measuring signal attenuation, they often suffer from significant inaccuracies due to multipath fading, interference, and varying environmental conditions [11]. ToA-based methods, which calculate the distance by measuring the travel time of signals, also face challenges, such as the need for precise synchronization and the impact of signal reflections. PBR can provide more accurate distance estimation than techniques based on RSSI and ToA, even in rich multipath environments [12]. A technique called Multi-Carrier Phase Difference (MCPD) ranging uses the phase difference of a received signal at multiple frequencies to estimate the distance with high precision [13].

Another common 2D localization method is angulation, which uses the angle measurements related to the direction of the received or transmitted signals [14]. Direction of Arrival (DoA) estimation with rotary antennas involves using a rotating directional antenna to measure signal strength at different angles, identifying the direction from which the signal is strongest or most consistent [15]. However, rotary antennas are impractical to implement due to their mechanical complexity and slow response time. Instead, phase interferometry is often employed, where multiple antennas spaced by a distance shorter than half of a signal's wavelength are formed into an antenna array. As a signal phase propagates in space, its variations in the phase measured across antenna elements of the array can be used to estimate the direction with high-resolution DoA algorithms, such as MUltiple SIgnal Classification (MUSIC) or the Estimation of Signal Parameters via Rotational Invariance Technique (ESPRIT) [14]. Recent advancements in DoA estimation explore full-hardware approaches that reduce the computational overhead of classical algorithms and offer angle estimation response in real time [16].

The hybrid localization method combines the lateration and angulation methods, where the 2D location of a target device can be estimated with only a single anchor node, which is beneficial for systems with a single receiver or access point. Even if the goal is not

Sensors **2024**, *24*, 3925

to minimize the number of anchor devices, the hybrid localization method can be beneficial, as fusing measurements from multiple anchors can greatly improve the accuracy of the localization system [1]. A straightforward approach to achieve hybrid localization is to combine the ToA and DoA estimates. Wi-Fi networks offer great opportunities for hybrid localization because they provide Channel State Information (CSI) that can be extracted alongside communication. CSI contains the amplitude and phase information of the signal transmitted at multiple subcarriers between different antenna elements, which can be used to extract both DoA and ToA estimates [17,18]. Several hybrid localization solutions have been proposed for ultra-wideband (UWB) technology. When an antenna array is employed at the receiver, the 2D MUSIC algorithm can be used for joint estimation of DoA and ToA [19].

An efficient approach for integrating localization functionality in IEEE 802.15.4 TSCH networks has not yet been proposed in the literature. The level of accuracy required for current and future IoT applications cannot be achieved with the available localization techniques that rely on either RSSI [20] or ToA-based [21] lateration. The proposed modifications in solutions using PBR for lateration [22] disrupt the normal operation of the communication process and lead to increased complexity and reduced network performance. Angulation and hybrid localization techniques have not yet been considered for implementation in the protocol. In this study, we propose a method for integrating hybrid localization into the IEEE 802.15.4 TSCH protocol, designed to minimize disruptions to the communication network. The approach ensures that devices can perform localization alongside communication without requiring any special network deployment changes. Our solution builds on previous research, where we developed methods for integrating MCPD distance estimation [23] and DoA estimation [24] into the TSCH protocol. We synthesize findings and insights obtained to introduce a comprehensive hybrid localization solution within the TSCH protocol. We discuss the requirements necessary for successful angle and distance estimation and introduce a scheme that operates concurrently with communication. With the proposed enhancement, a node can transmit a packet to a target device and estimate both the DoA and the distance to the receiving node, which can be used for localization. We validate our proposed localization method in a real-world setting using low-cost proprietary devices. The main contributions of the paper are as follows:

- Proposing a novel approach for hybrid localization based on distance and angle that is integrated alongside TSCH communication.
- Demonstrating the feasibility and effectiveness of our approach in a real-world scenario using low-cost proprietary devices.
- Providing software incorporating our approach that can be of service in future research.

The remainder of this paper is organized as follows. The integration of localization functionality alongside communication in various IoT wireless technologies is reviewed in Section 2. Section 3 discusses the requirements for localization with the TSCH protocol and provides a theoretical background on distance and DoA estimation. The proposed modification of the TSCH protocol is presented in Section 4. The focus in Section 5 is on describing the details of our proprietary system. Section 6 presents and discusses the experimental evaluation results. Section 7 concludes the paper and outlines future work.

2. Related Work

Acquiring location estimation alongside communication has become an extremely useful and desired feature of wireless networks. Various wireless technologies have recognized the need for precise localization and have started integrating localization techniques into the protocol specifications, as summarized in Table 1. This section overviews the recent advancements in ILAC for the most commonly used technologies in IoT setups.

The Wi-Fi communication technology specified in IEEE 802.11 is widely adopted for high-speed data transmission in various IoT applications when power consumption is not a limiting factor within the system. Wi-Fi technology is increasingly utilized for

Sensors **2024**, *24*, 3925

indoor localization solutions mainly based on CSI [25]. The detailed information about channel conditions between the transmitter and receiver, including data on amplitude and phase for each subcarrier, makes CSI-based localization a cost-effective solution for indoor positioning systems [26]. Machine learning (ML) approaches have been proven to be effective for fingerprinting-based localization in scenarios where a large amount of channel measurement data is available for building the ML models [27]. Recognizing the need for wireless localization, the IEEE 802.11az-2022 amendment greatly enhanced localization performance by leveraging the mmWave spectrum and dedicated beamforming techniques [28]. The Wi-Fi standard continues to evolve to incorporate enhanced sensing capabilities with Integrated Sensing and Communication (ISAC) aspects through the development of the IEEE 802.11bf amendment [29].

Providing accurate location and timing information was within the focus of UWB technology for low data rate communication, introduced in 2007 by standard IEEE 802.15.4a [30]. Short-duration pulses and wide bandwidth provide good temporal resolution for accurate ToA and Channel Impulse Response (CIR) estimates [31,32]. The IEEE 802.15.4z UWB physical (PHY) enhancements, released in 2020, include additional improvements for higher accuracy as well as secure localization and ranging in multipath environments [33,34]. Recent research has focused on enhancing UWB-based localization systems by integrating advanced signal processing algorithms and ML techniques [35].

Bluetooth Low Energy (BLE) is widely adopted in IoT devices due to its low power consumption, high data rate connectivity, and compatibility with smartphones and wearables. BLE supports basic localization functionalities using RSSI measurements, allowing fingerprint-based and proximity-based localization [36,37]. A significant advance in BLE's capabilities for localization services was introduced with the release of Bluetooth 5.1, which enables devices to estimate the DoA and determine the angle from which a signal arrives at a receiver [38,39]. Recent developments in BLE standardization aim to further enhance the accuracy of localization by adding the channel sounding feature alongside the communication protocol [12]. This feature uses PBR to analyze the phase information of the radio signal and thus enables precise distance estimation between devices, even in challenging multipath environments.

Conversely, for IoT scenarios that require low power and low data rate connectivity with a potentially large number of devices in a relatively large area, various alternative IoT protocols are employed, such as ZigBee, Thread, 6LoWPAN, and Wireless HART. These protocols are based on the IEEE 802.15.4 standard and its TSCH protocol, added in the 2016 amendment [8]. There have been several studies on applying the IEEE 802.15.4 standard and related IoT technologies for localization, primarily using the RSSI metric for proximity-based and fingerprint-based localization methods [20,40]. Although the accuracy of RSSI-based localization systems is continuously improving with the development of ML algorithms [41], the main drawback remains. The high sensitivity of the RSSI metric to environmental changes [11] makes the localization system unreliable and case-specific to the particular scenario. Some IEEE 802.15.4 compliant radios available on the market provide a feature that triggers an interrupt signal at the start of the detected data packet. This ability was exploited for ToA-based ranging that is compatible with the IEEE 802.15.4 standard, achieving distance estimation accuracy at a range of several meters [21,42].

Recent advancements in radio design have introduced the option of measuring the phase of received signals, motivating research into PBR. With the use of the MCPD method [43], also referred to as Active Reflector (AR) [22], the presented solutions achieved even greater accuracy in ranging and localization compared to other methods [22,43,44]. Nevertheless, there has been little consideration of how the PBR process affects the overall communication process. Communication is often interrupted or delayed for longer periods to allow devices to measure the signal's phase. Additionally, these solutions focus on specific use-case scenarios, where nodes are used only for localization and do not adequately cover the more typical network deployments destined for communication.

Sensors **2024**, *24*, 3925

Table 1. Localization techniques for different wireless technologies.

Technology	Communication				Localization		
	Range	**Throughput**	**Power Usage**	**Radio Signal**	**Metric**	**Advantages**	**Disadvantages**
Wi-Fi [29]	15–100 m	54 Mbps–9.8 Gbps	High	OFDM	RSSI [26,27]	Simple to implement; Widely available	Prone to multipath effects, noise, and environmental changes; Low accuracy
					CSI [25,26,45]	More robust to noise and multipath; High accuracy	Not widely available on of-the-shelf devices; Complex processing algorithms
UWB [46]	10–100 m	6.8–460 Mbps	Low	PPM	ToA (TDoA) [31,33,47]	Immune to interference; Less susceptible to multipath effects; High accuracy	Shorter range; Requires wide bandwidth; Need for synchronization between multiple anchors
BLE 5.1 [48]	10–200 m	125–2000 kbps	Low	GFSK	RSSI [36,37]	Simple to implement; Readily available on consumer devices	Prone to multipath effects, noise, and environmental changes; Low accuracy
					DoA [38,39]	High accuracy; Less susceptible to multipath effects; Requires fewer anchors for localization	Requires switch antenna array; Complex processing algorithms for higher resolution
					PBR [12,13]	High accuracy; Less susceptible to multipath effects	Complex processing algorithms; Longer time for sampling at multiple frequencies
IEEE 802.15.4 [8]	100 m	250 kbps	Low	O-QPSK	RSSI [20,40]	Simple to implement; Metrics available alongside communication	Prone to multipath effects, noise, and environmental changes; Low accuracy
Proposed					PBR, DoA	High accuracy; Less susceptible to multipath effects; Single anchor node required for localization	Requires switch antenna array; Longer time for sampling at multiple frequencies; Complex processing algorithms

3. Localization in TSCH

In TSCH networks, the Routing Protocol for Low-Power and Lossy Networks (RPL) is usually deployed, which creates a destination-oriented directed acyclic graph (DODAG) topology [9], as shown in Figure 1. In this configuration, one node is a dedicated DODAG root, while others are parent and child nodes. The packets in the network generally traverse from the child nodes to the parent nodes and eventually reach the root node, which then forwards them down to the destination device. This poses a challenge for localization because any two arbitrary devices cannot exchange messages directly in the default configuration and, therefore, cannot effectively measure the characteristics of the communication channel between them. Therefore, integrating lateration or angulation methods into the TSCH protocol is difficult to realize without extensive communication protocol and network structure changes. One of the possible solutions is the use of hybrid localization with a single node, where the root or parent node undertakes the localization of other devices. The root/parent node can address its child nodes arbitrarily, send packets to them, and measure the properties of the communication link. To implement hybrid localization with a single node, both the angle of arrival and the distance to the device of interest are required.

Sensors **2024**, *24*, 3925

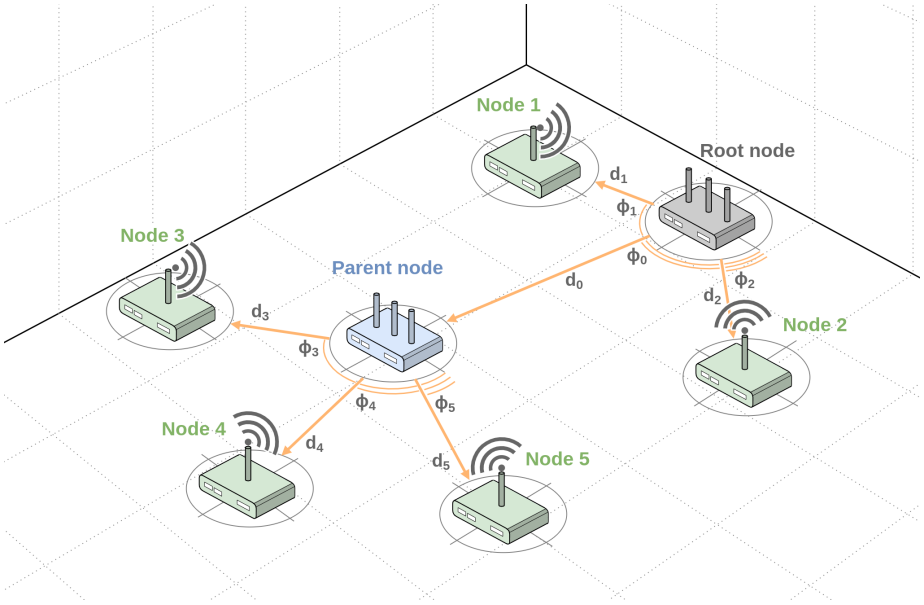


Figure 1. Topology of the destination-oriented directed acyclic graph (DODAG) network with the proposed method of hybrid localization, where a single node referred to as the root/parent node can determine the location of its child nodes.

3.1. Estimation of Direction of Arrival

The phase difference in the incoming signal at multiple antennas, separated by a distance shorter than half the wavelength of the signal, can be used to estimate the direction from which a signal is received [24]. High-resolution algorithms can be applied at the receiver to analyze how the phase of the signal changes across the antenna array and to determine the angle at which the signal arrives [49]. In this study, we validated the effectiveness of the MUSIC algorithm, which is considered adequate for real scenarios due to its resilience to noise.

The phase measurement for different antennas in systems with a single radio frequency (RF) chain, such as the radios that support IEEE 802.15.4, is commonly approached with an antenna switching circuit. It allows the device to switch between antennas and sample the phase with various switching patterns, providing application-oriented features. In this study, the Round Robin switching pattern was used, as it provides the most phase samples per antenna, which benefits the MUSIC algorithm. Although switching antenna arrays are suitable for developing a cost-effective and energy-efficient solution, they introduce a time delay between the measurements from each antenna, which can lead to large errors in the case where the Carrier Frequency Offset (CFO) between the devices is not compensated.

3.2. Estimation of Distance between Two Devices

A distance between devices can be determined using phase differences across multiple frequencies, which can be measured using the MCPD method. In this method, one of the devices acts as the initiator, and the other acts as the reflector. To eliminate initial unknown offsets in the phase of the generated signal, the devices alternately measure the phases: first, the initiator transmits a continuous wave (CW), and the reflector measures the phase of the received signal, whereupon the roles are reversed. To increase the maximum unambiguous range (UR) and spatial resolution, the devices extend the apparent bandwidth by repeating the phase measurements at several frequencies and later construct the phase response from them. The frequency step between the frequencies determines the UR, while the total bandwidth used determines the resolution of the system.

The method of obtaining phase samples can be either uniform [22] or non-uniform [50], and it can include weighting of the phase samples [51]. After acquiring the phase response of a link, spectral analysis techniques can be employed to estimate the distance between

Sensors **2024**, *24*, 3925

the devices. Among the various algorithms available, such as slope-based [52], Fast Fourier Transform (FFT)-based [53], MUSIC-based [43], and ML-based [54], we use the FFT-based interpolated Complex-valued Distance Estimation (iCDE) algorithm [55] in this study due to its robustness to noise and ability to mitigate multipath effects.

4. Integration of Localization Functionality

Integrating localization functions into the TSCH protocol requires a thorough analysis of DoA and MCPD estimation requirements for effective implementation. A novel comprehensive hybrid localization solution using the TSCH protocol is developed considering the findings from our proposed methods for TSCH protocol enhancement with MCPD distance estimation [23] and DoA estimation [24]. The approach was selected to evaluate the hybrid localization performance by solely modifying the PHY and Medium Access Control (MAC) layers of the IEEE 802.15.4 standard. Although altering the upper layers of the communication protocol might present numerous potential enhancements and performance optimization, these are beyond the scope of this study.

4.1. Design Considerations

The main objective of the proposed localization process is to minimize its impact on communication while ensuring that the required changes in the communication protocol remain minimal. A short interruption of the communication process is introduced for the devices to measure the communication channel characteristics in a Phase Measurement Process (PMP) procedure. A single angle and distance to the neighbor estimate are obtained to minimize the impact on communication, although multiple estimates are feasible.

Simultaneous initiation of the measurement is needed for an appropriate channel estimation. The globally synchronized network inherently provided by the TSCH protocol is used to satisfy the synchronization requirement. The protocol utilizes a slotframe in which the communication time is divided into timeslots that coordinate the intervals for the preparation of packets, the reception/transmission of user data, and the exchange of acknowledgment. To add localization functionality to the protocol, we propose to extend the timeslot with an additional interval that allocates the required time for PMP, as shown in Figure 2. The newly defined TSCH timeslot timings enable both devices to simultaneously start with the channel measurement. Leveraging the TSCH protocol further, PMP is positioned immediately following the data packet exchange, allowing the measured phase information to be returned to the initiator as an information element within the acknowledgment exchange.

For DoA estimation, the PMP allocates 90 slots where a device can select the desired antenna element and sample the phase of the signal. This allocation is determined as a trade-off between the sensing time and the communication time to provide sufficient samples per antenna, enabling various switching patterns with different numbers of antenna elements [24]. Since a single RX chain with an RF switch is used to capture phases from different antennas, the phase measurement accuracy decreases with the increasing sampling time interval due to the CFO. The cumulative phase offsets induced by the CFO significantly affect the accuracy of the DoA estimation. A reference period is added to the PMP to address this, where eight samples can be obtained from a single antenna. The reference period can be used for CFO estimation so that calibration can be used to compensate for the phase offsets [24], enhancing the overall accuracy of the DoA estimates.

To estimate distance with MPCD, a sequential phase sampling through the available RF spectrum is required. Although measuring the phase for each communication channel during packet transmission and then combining the measured phases into phase response is theoretically feasible, practical challenges arise due to the significant channel variations between two consecutive packet transmissions. In addition, the time between phase measurements at the initiator and reflector should be minimized to achieve accurate distance estimation [13]. We propose executing the entire RF spectrum sweep sequentially within the shortest possible interval. To minimize the measurement time and avoid com-

Sensors **2024**, *24*, 3925

munication interruptions, a Golomb set of frequencies is used [50]. With this approach, only 15 frequencies are needed for a complete phase response reconstruction, significantly reducing the time compared to other methods that might require up to 160 samples [22]. This is beneficial for introducing localization into communication, as more time can be spent on communication than sensing. The reduced number of frequencies leads to a lower probability of interference with other wireless technologies and more efficient spectrum use. After expanding the measured data [23], the devices can estimate the range with the UR up to 300 m.

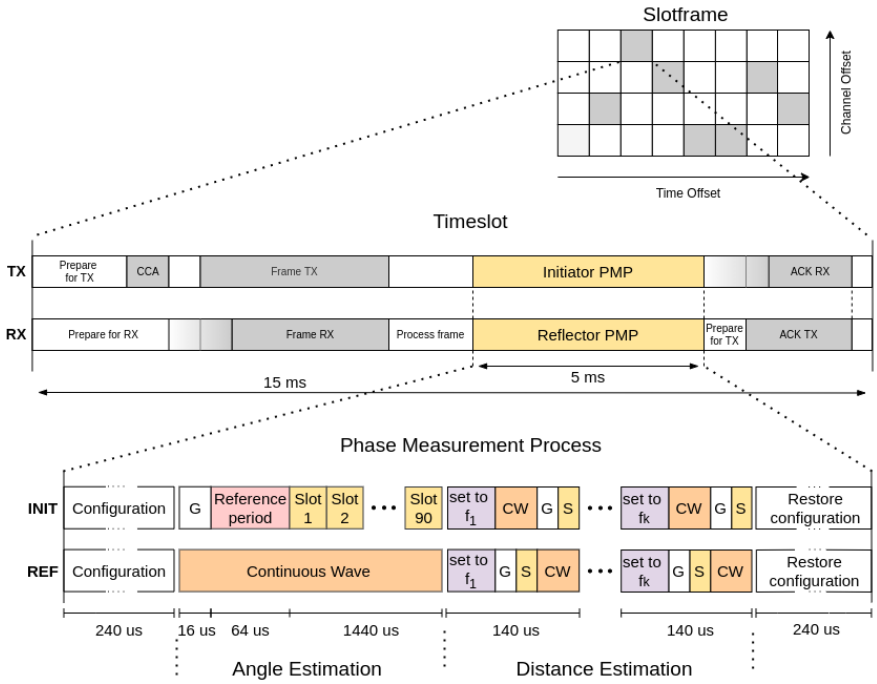


Figure 2. Integration of a phase measurement process into the Time Slotted Channel Hopping (TSCH) timeslot.

In TSCH networks, the communication between a parent node and its neighbor is orchestrated through a schedule known as a slotframe, where each packet exchange occurs in a designated cell. Since the location estimate is obtained with each transmitted packet, the location estimation updates occur at the same rate as packet exchanges. The parent orchestrates multiple devices, and the actual update rate depends on the number of child nodes that the parent has to communicate with. If a new node joins the network, a cell is added to the slotframe, reducing the update rate for all devices. The slotframe is managed by a Scheduling Function (SF), which is not defined in the IEEE 802.15.4 TSCH standard. Nonetheless, the flexibility of the slotframe provides numerous opportunities for improvements in the performance and scalability of the localization system. In case a device requires a faster update rate, more cells can be added to the slotframe for a packet exchange with this device. If a node is recognized as static and does not change its position, the cells can be removed, freeing up space in the slotframe for other devices. The responsiveness and accuracy of the system can be optimized according to the network requirements using a dedicated SF in comprehensive applications.

4.2. Phase Measurement Process

The structure of PMP includes steps for: (1) configuring the radio for phase measurement, (2) estimating the angle, (3) estimating the distance, and (4) restoring the configuration of the radio to continue with the communication. The proposed generic solution, which is applicable to any analog radio, has been modified for the currently available, low-cost, off-the-shelf radios that offer a phase sampling rate of 8 µs [24]. The intervals shown in

Sensors **2024**, *24*, 3925

Figure 2 were selected accordingly, and the timeslot was extended from the default 10 ms to 15 ms.

During the angle estimation, the reflector initiates a CW transmission on the same frequency channel that was used to transmit the data packet. The initiator first waits for a predefined guard period denoted by G in Figure 2 and measures 8 phase samples on the reference antenna for CFO calibration. Then, 90 slots are available for phase measurement with different antenna elements according to the selected switching pattern. To mitigate the phase distortion introduced by altering the signal's path during the measurement, enough time is provided in each slot to sample the phase and to switch to the desired antenna element.

After estimating the angle, the devices start estimating the distance with the MCPD technique. Both devices configure their Phase-Locked Loop (PLL) to a predefined frequency. The initiator then transmits CW, waits for a predefined guard time, and performs a phase sampling denoted as S in Figure 2, while the reflector waits for a guard time interval, samples the phase, and later initiates CW transmission. The process is then repeated at different frequencies until all frequencies in the set are used. The defined PMP scheme with exact intervals enables periodic timer interrupts that ensure the devices remain synchronized, which is crucial for accurate distance estimation.

5. Experimental Setup

To evaluate the performance of the proposed localization in real environments, a test setup shown in Figure 3 was created in an office with low-cost micro-controllers [56]. The IEEE 802.15.4 TSCH network is formed with six devices, and the root node attempts to determine the position of the other five nodes during the communication.

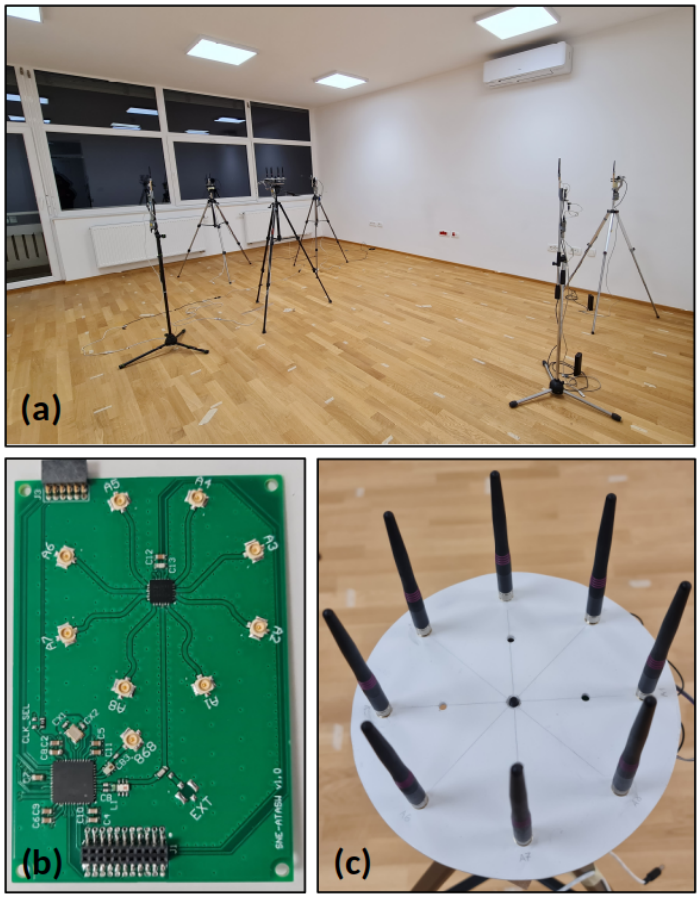


Figure 3. (**a**) Experiment setup. (**b**) Micro-controller equipped with AT86RF215 radio and RF switch. (**c**) Uniform circular antenna array with eight elements.

Sensors **2024**, *24*, 3925

5.1. System Design

The micro-controller devices are built upon the AT86RF215 [57], an IEEE 802.15.4 compliant radio with an option for register-based monitoring of the received signal's phase through the Phase Measurement Unit (PMU). Furthermore, the radio can measure the In-Phase and Quadrature (IQ) components of the received signal, the phase stability or Quality Factor (QF), and the frequency offset [57]. With additional configuration options, the PMU can sample the aforementioned data with a period of 8 µs, which can be accessed via a Serial Peripheral Interface (SPI).

To expand the single RF signal chain of the radio, the platform incorporates an RF switch that can accommodate an antenna array with up to eight elements. The board design ensures that all traces from the RF switch to the antenna connectors are of equal length and that each path contributes equally to the overall phase delay without causing errors in DoA estimation. The co-planar waveguide with a via fence was applied to reduce the cross-talk between the traces. A Uniform Circular Array (UCA) consisting of eight dipole antennas was used for localization, as depicted in Figure 3c. UCA offers an advantage over linear arrays, as it can estimate angles from 0° to 360°. The chosen number of antenna elements is considered as a trade-off between the physical size of the device and its localization performance.

5.2. Radio Configuration

During the normal operation of the radio, the internal baseband core generates and receives the RF signals. The phase of the signal can be measured only after the radio has been configured adequately. A brief description of its configuration for phase measurement is provided for completeness. Additionally, a driver for the AT86RF215 radio within the Contiki-NG operating system [58] has been designed and developed. The driver is available online for future research [59].

The transceiver architecture works as a heterodyne receiver and direct up-conversion transmitter. The received signal is first converted to the intermediate frequency (IF), which can be 0.25 MHz, 0.5 MHz, 1 MHz, or 2 MHz. A band-pass filter with three possible cut-off frequencies can be selected for each IF through the register bits *RFn_RXBWC.BW*. The experimental analysis showed optimal phase measurement performance at an IF of 1 MHz. The initiator and reflector devices must be configured to measure the channel at the same frequency for accurate phase extraction. Since the receiver operates according to the heterodyne architecture, the transmitter must emit a CW at an IF frequency higher than the receiver is listening to. And since the PLL frequency should not be altered when the roles are reversed, the reflector must be configured to use inverted IF by setting the bit *RFn_RXBWC.IFI* to 1. According to the IF configuration, the receiver's sampling frequency is set through *RFn_RXDFE* and must match the IF for optimal operation. The same registers configure the digital post filter for attenuation of out-of-band signals. The gain of the signal must remain the same during phase measurement to avoid phase changes. Thus, the bit *RFn_AGCC.EN* is set to 0 to enable manual control, and the receiver's gain is set to a constant value through the register *RFn_AGCS*. In addition, the energy detection feature is disabled by setting the bit *RFn_EDC* to `0x03`.

The front end of the transmitter is configured with *RFn_PAC* to set the output power, *RFn_TXCUTC* to configure the low-pass cut-off frequency and the ramp-up time of the power amplifier, and *RFn_TXDFE* to configure the digital front end of the transmitter. For *RFn_PAC*, the maximum value is typically selected, while for *RFn_TXCUTC* and *RFn_TXDFE*, the default values can be considered. To enable the transmission of CW, the radio is configured to use the digital-to-analog converter (DAC) overwrite feature, generating a local oscillator carrier signal at the selected frequency. By setting the register *RFn_TXDACI* to `0xFE` and register *RFn_TXDACQ* to `0xBE`, the DAC is overwritten with the maximum I and minimum Q signal magnitude. CW transmission is initiated by disabling the radio's baseband with *RFn_IQIFC1.CHPM* set to 1 and issuing a command to transition the radio into a TX state. When measuring the phase, however, the baseband

Sensors **2024**, *24*, 3925

must be enabled (bit *RFn_IQIFC1.CHPM* set to 0), and the radio must be in the RX state. The PMU must also be configured and enabled. The PMU offers various configuration options: (i) to force the carrier frequency changes to occur at the end of the PMU period if *BBCn_PMUC.CCFTS* set to 1, (ii) to average the measured phase over the entire PMU period using the *BBCn_PMUC.AVG*), and (iii) the phase can be returned with or without normalization using the *BBCn_PMUC.IQSEL*.

5.3. Measurement Scenario

The measurements were performed in an empty office environment with dimensions 5.1 m by 6.5 m. During the measurement campaign, 17 Wi-Fi access points were in operation, and no special consideration was given to the possible interference. The measurement setup shown in Figure 3 includes six devices placed on a stand 1.4 m above the floor. The root node was positioned in the center of the room, with the other devices around for the root node to be a parent for all devices. After initiating the experiment, the root waited for all devices to join the network before transmitting packets to each device at regular intervals. With each received response, the root node forwarded the measured phases to a computer, which calculated the DoA and distance estimates. This simple method was chosen to test localization performance. However, it also offers numerous opportunities for improvement, such as distinguishing between static and mobile nodes, introducing burst packets for mobile nodes for a faster update rate, and dynamically assigning frequency channels for erroneous measurements.

6. Experiment Results and Analysis

The reference point for the estimated angle is positioned in the center of the UCA, while for the distance estimate, the reference point of the measurement is positioned at the first antenna element. For effective localization, this system error is corrected by converting the measured distance to the center of the UCA using the antenna radius and the angle at which the device is positioned. Furthermore, each distance measurement result contains an additional offset due to the radio signal paths on the circuit board and the antenna. In our case, we measured an offset of 2.05 m, and all measurement results were corrected accordingly.

The root node calculates the DoA and the distance to the target node after the transmission of each packet, regardless of whether the phase of the signal was measured accurately. Consequently, the estimations may be incorrect, which is often caused by channel interference or the loss of timeslot synchronization between devices in the network. We used the Quality Indicator (QI) value to identify and eliminate potential outliers. Both the iCDE and MUSIC algorithms generate a pseudo-spectrum as an output function. The peaks in the spectrum indicate the possible distance or angle estimates, and the magnitude of the selected peak represents the QI. The corresponding angle or distance measurements are discarded if the QI value falls below a predefined threshold. The total number of transmitted packets and the number of removed measurements are presented in Table 2.

Table 2. Number of obtained estimations and number of discarded estimations at each node with the use of Quality Indicator (QI).

	No. of Estimates	**No. of Discarded**
Node 1	651	6
Node 2	307	21
Node 3	245	0
Node 4	604	161
Node 5	571	3

However, detecting outliers based on the QI value can be unreliable in environments rich in multipath interference, such as the office environment. Different paths can introduce different phase shifts, resulting in constructive or destructive interference at the receiver.

Sensors **2024**, *24*, 3925

This is particularly evident in DoA estimation, where the device sometimes returns the DoA of the multipath component instead of the line-of-sight path of our interest [24]. The results from multiple frequencies can be used to mitigate the adverse effects of multipath interference, as different frequencies are not equally affected by the multipath effects. Given that devices in the modified TSCH perform DoA estimation at the same frequency at which the packet is transmitted, we can leverage this channel hopping feature. By aggregating the estimated data from multiple successive packets and calculating the median of these measurements, we can effectively filter out measurement outliers, minimizing the impact of multipath variations. In distance estimation processes, multiple frequencies are already employed within each measurement. Since we only sample the phase on 15 frequencies, the resulting phase response is vulnerable to noise. Increasing the number of sampled frequencies would enhance resilience to noise, but this would extend the time needed for obtaining measurements, potentially disrupting ongoing communications. Thus, taking the median of successive distance measurements will also enhance distance estimation accuracy by mitigating the multipath effects and noise.

In the analysis, we considered a single measurement or a median of either 5 or 16 successive measurements as a final result. The effectiveness of location estimates is assessed with Root Mean Square Error (RMSE), which measures the average magnitude of the error between the estimated locations and the true locations. The RMSE gives a clear indication of the accuracy of localization system, but it is highly sensitive to large errors; thus, the Mean Absolute Error (MAE) is also presented, which is less sensitive to outliers and provides a direct average measure of error magnitude. The comparison of localization errors with different numbers of successive measurements is presented in Table 3. Figure 4a shows the comparison of the Cumulative Distribution Function (CDF). It provides insights into the accuracy of the localization system and visually demonstrates the point at which half of the estimated locations fall below the average error, which in all three cases is below 0.41 m.

When only a single measurement is considered as the final result, the maximum error exceeds 6 m. By adopting the median of 16 consecutive measurements to cover all available frequency channels, the maximum error drops to below 0.65 m. The proposed localization system achieves high accuracy using only a single node with a known location, compared to other techniques that require at least three anchors [40]. Acquiring many measurements is time-consuming for mobile device scenarios where a high update rate is essential for accurate device tracking. To quantify the relationship between system accuracy and the time required for final location estimation, we modeled the TSCH network scenario that is available by default in the Contiki-NG operating system. A slotframe with eight timeslots is used with one dedicated cell for packet exchange between devices. With a modified timeslot prolonged to 15 ms, the root can exchange a message with its neighboring node every 120 ms. When the median of 16 estimates is taken as a final result, the location acquisition time equals 1920 ms. As a trade-off between update time and accuracy, we propose to obtain five successive measurements, where the root requires 600 ms for a final location estimate. As shown in Figure 4b, the maximum localization error of the system remains below 2 m, and the average error is 0.37 m.

Table 3. Estimated location errors with different numbers of successive measurements taken as the final result.

	Single		**Successive 5**		**Successive 16**	
	RMSE	**MAE**	**RMSE**	**MAE**	**RMSE**	**MAE**
Node 1	0.374	0.171	0.194	0.112	0.185	0.101
Node 2	2.178	0.824	0.611	0.333	0.452	0.287
Node 3	0.349	0.189	0.278	0.185	0.268	0.183
Node 4	2.506	0.956	0.410	0.267	0.390	0.265
Node 5	1.068	0.486	0.628	0.361	0.583	0.349

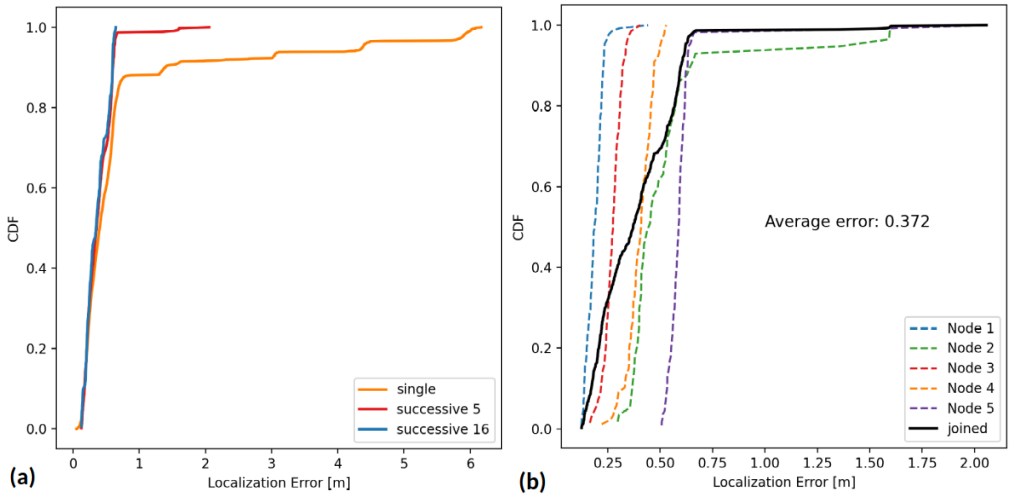


Figure 4. Cumulative Distribution Function (CDF) for estimated location errors. (**a**) Comparison of CDF with a single measurement with 5 and 16 successive measurements. (**b**) CDF for each node's location with 5 successive measurements.

Detailed distance and angle estimation results with a median of five successive measurements are presented in Table 4. The median (MED) error helps to understand the typical error magnitude or accuracy while minimizing the impact of outliers. The standard deviation (STD) provides an understanding of the variability of the estimations around their MED, indicating the precision of estimations. The MAE assesses the average absolute error in the estimations, providing insights into systematic biases. Relatively large errors in the location estimates can be attributed to the inaccurate angle estimations, which can also be observed in Figure 5. Improved angle estimation results can be achieved with a larger number of antenna elements in the UCA and a spatial smoothing technique. In addition, along with tuning of individual dipole antennas to the 2.4 GHz band, the effects of mutual coupling should be considered.

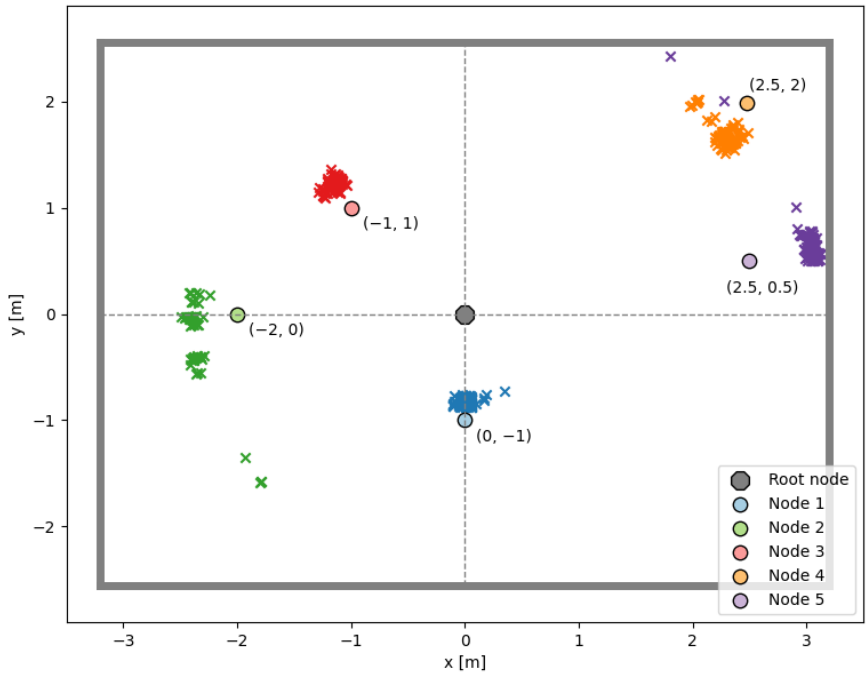


Figure 5. Actual (circles) and estimated (crosses) locations of devices in an office room based on five successive measurements as a final result.

Sensors **2024**, *24*, 3925

Table 4. Detailed distance and angle estimation results per node. A median of five successive measurements has been used as the final estimation result.

	True Distance [m]	Distance Estimates [m]			True Angle [°]	Angle Estimates [°]		
		MED	STD	MAE		MED	STD	MAE
Node 1	1.000	0.818	0.035	0.179	270	272.0	4.10	3.01
Node 2	2.000	2.399	0.041	0.395	180	181.1	10.75	7.47
Node 3	1.500	1.678	0.044	0.178	135	133.8	2.35	2.45
Node 4	3.200	2.836	0.060	0.362	38.6	36.3	2.70	3.09
Node 5	2.540	3.133	0.036	0.587	11.3	11.5	5.03	1.90

The STD of the measured distances is relatively small, which proves the precision of the MCPD distance estimation algorithm, especially after removing the outliers with the median of five successive measurements. The MAE is below 0.6 m with only 15 phase samples, which is comparable to PBR approaches that collected 160 phase samples [22]. The MAE of the estimated distances increases as the devices are positioned closer to the walls due to multipath effects. For example, Nodes 1 and 3, which are only 1 m and 1.5 m away from the root, respectively, show better distance estimation accuracy than other nodes. Algorithms that are less susceptible to noise and multipath effects can be used to improve the accuracy of the estimated distances. In addition, consecutive distance estimations can be made with different antenna elements to exploit the antenna diversity.

The IEEE 802.15.4 standard currently supports RSSI measurement during communication, which can be used to approximate the distance to the source of the transmission. The relationship between RSSI and distance can be modeled using the common free-space path loss (FSPL) formula [60], which describes how the radio signal degrades as it travels through space. This baseline distance estimation solution is compared with the proposed MCPD approach by analyzing an ideal scenario, where the fluctuations in the RSSI due to multipath propagation effects and noise are neglected, and the RSSI is measured with a granularity of 1 dBm [8]. From the FSPL equation, we derive how the small changes in RSSI measurement $\Delta RSSI$ affect the distance estimation error Δd using

$$\Delta d = d \times \frac{\Delta RSSI \ln 10}{20}. \quad (1)$$

A 1 dBm change in the RSSI value results in an approximately 11.5% change in the calculated distance. For example, at the distance of 1 m, the estimation error is within 0.115 m, while for distances above 10m, the estimation error can exceed 1 m. By increasing the distance between the receiver and transmitter, even small fluctuations in RSSI readings lead to high variability in the calculated distance, while variations in the MCPD distance estimation remain low even with the increased distance between the devices [23].

7. Conclusions

In this paper, we propose a hybrid localization approach based on distance and angle estimates integrated with the TSCH protocol, enabling localization functionality alongside communication. The phase measurement process (PMP) is designed, and its integration into the protocol is described. Each packet transmitted includes both DoA and MCPD distance estimates that can be used to localize an unknown device. The channel hopping functionality of the protocol and several successive measurements were considered to mitigate multipath effects and remove outliers. The proposed method was validated based on a measurement campaign in an office environment utilizing low-cost proprietary devices. The results show a few tens of centimeters of accuracy in the investigated indoor scenario. In future work, the presented solution will be tested in various environments, and its scalability will be analyzed by designing a dedicated SF. Additionally, the solution will be extended with antenna diversity for distance estimation, spatial smoothing for DoA estimation, and different spectrum-peak search algorithms to improve performance. With

Sensors **2024**, *24*, 3925

the proposed advancements, we assume that new possibilities will be offered for sensing and localization applications in indoor environments.

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

Funding: This research was funded by the Slovenian Research And Innovation Agency (ARIS), grant numbers J2-4461, J2-3048, P2-0016, and PR-12348.

Data Availability Statement: The driver for the AT86RF215 radio within the Contiki-NG operating system is available online in [59].

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

Abbreviations

The following abbreviations are used in this manuscript:

2D	two-dimensional
AR	Active Reflector
BLE	Bluetooth Low Energy
CDF	Cumulative Distribution Function
CFO	Carrier Frequency Offset
CIR	Channel Impulse Response
CSI	Channel State Information
CW	Continuous Wave
DAC	Digital-to-Analog Converter
DoA	Direction of Arrival
DODAG	Destination-Oriented Directed Acyclic Graph
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Technique
FFT	Fast Fourier Transform
FSPL	free-space path loss
GFSK	Gaussian Frequency Shift Keying
iCDE	interpolated Complex-valued Distance Estimation
ILAC	Integrated Localization and Communication
IoT	Internet of Things
IQ	In-Phase and Quadrature
ISAC	Integrated Sensing and Communication
MAC	Medium Access Layer
MAE	Mean Absolute Error
MCPD	Multi-Carrier Phase Difference
MED	Median
ML	Machine Learning
MUSIC	MUltiple SIgnal Classification
OFDM	Orthogonal Frequency-Division Multiplexing
O-QPSK	Offset Quadrature Phase Shift Keying
PBR	Phase-Based Ranging
PHY	Physical Layer
PLL	Phase-Locked Loop
PMP	Phase Measurement Process
PMU	Phase Measurement Unit
PPM	Pulse Position Modulation
QF	Quality Factor
QI	Quality Indicator
RF	Radio Frequency
RMSE	Root Mean Square Error

RPL	Routing Protocol for Low-Power and Lossy Networks
RSSI	Received Signal Strength Indicator
SPI	Serial Peripheral Interface
STD	Standard Deviation
ToA	Time of Arrival
TSCH	Time-Slotted Channel Hopping
UCA	Uniform Circular Array
UR	Unambiguous Range
UWB	Ultra-Wideband

References

1. Savić, T.; Vilajosana, X.; Watteyne, T. Constrained Localization: A Survey. *IEEE Access* **2022**, *10*, 49297–49321. [CrossRef]
2. Maddikunta, P.K.R.; Pham, Q.V.; Prabadevi, B.; Deepa, N.; Dev, K.; Gadekallu, T.R.; Ruby, R.; Liyanage, M. Industry 5.0: A survey on enabling technologies and potential applications. *J. Ind. Inf. Integr.* **2022**, *26*, 100257. [CrossRef]
3. Simončič, A.; Mohorčič, M.; Mohorčič, M.; Hrovat, A. Non-Intrusive Privacy-Preserving Approach for Presence Monitoring Based on WiFi Probe Requests. *Sensors* **2023**, *23*, 2588. [CrossRef] [PubMed]
4. Bluetooth SIG. Enhancing Bluetooth Location Services with Direction Finding. Available online: https://www.bluetooth.com/bluetooth-resources/enhancing-bluetooth-location-services-with-direction-finding/ (accessed on 26 April 2024).
5. Wang, J.; Varshney, N.; Gentile, C.; Blandino, S.; Chuang, J.; Golmie, N. Integrated Sensing and Communication: Enabling Techniques, Applications, Tools and Data Sets, Standardization, and Future Directions. *IEEE Internet Things J.* **2022**, *9*, 23416–23440. [CrossRef] [PubMed]
6. Kaushik, A.; Singh, R.; Li, M.; Luo, H.; Dayarathna, S.; Senanayake, R.; An, X.; Stirling-Gallacher, R.A.; Shin, W.; Di Renzo, M. Integrated Sensing and Communications for IoT: Synergies with Key 6G Technology Enablers. *arXiv* **2023**, arXiv:2309.13542. [CrossRef]
7. Xiao, Z.; Zeng, Y. An Overview on Integrated Localization and Communication towards 6G. *Sci. China Inf. Sci.* **2022**, *65*, 131301. [CrossRef]
8. *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*; IEEE Standard for Low-Rate Wireless Networks. IEEE Standard: Piscataway, NJ, USA, 2015; pp. 1–709. [CrossRef]
9. Vilajosana, X.; Watteyne, T.; Chang, T.; Vučinić, M.; Duquennoy, S.; Thubert, P. IETF 6TiSCH: A Tutorial. *IEEE Commun. Surv. Tutor.* **2022**, *22*, 595–615. [CrossRef]
10. Adege, A.B.; Lin, H.P.; Tarekegn, G.B.; Jeng, S.S. Applying Deep Neural Network (DNN) for Robust Indoor Localization in Multi-Building Environment. *Appl. Sci.* **2018**, *8*, 1062. [CrossRef]
11. Moradbeikie, A.; Keshavarz, A.; Rostami, H.; Paiva, S.; Lopes, S.I. A Cost-Effective LoRaWAN-based IoT Localization Method Using Fixed Reference Nodes and Dual-Slope Path-Loss Modeling. *Internet Things* **2023**, *24*, 100990. [CrossRef]
12. Jason, H. Bluetooth Channel Sounding—A Step Towards 10-Cm Ranging Accuracy for Secure Access, Digital Key, and Proximity Services. Available online: https://www.bluetooth.com/blog/bluetooth-channel-sounding-a-step-towards-10-cm-ranging-accuracy-for-secure-access-digital-key-and-proximity-services/ (accessed on 24 April 2024).
13. Zand, P.; Romme, J.; Govers, J.; Pasveer, F.; Dolmans, G. A High-Accuracy Phase-Based Ranging Solution with Bluetooth Low Energy (BLE). In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–19 April 2019; pp. 1–8. [CrossRef]
14. Obeidat, H.; Shuaieb, W.; Obeidat, O.; Abd-Alhameed, R. A Review of Indoor Localization Techniques and Wireless Technologies. *Wirel. Pers. Commun.* **2021**, *119*, 289–327. [CrossRef]
15. Shen, L.; Zhang, Q.; Pang, J.; Xu, H.; Li, P.; Xue, D. ANTspin: Efficient Absolute Localization Method of RFID Tags via Spinning Antenna. *Sensors* **2019**, *19*, 2194. [CrossRef]
16. Florio, A.; Avitabile, G.; Talarico, C.; Coviello, G. A Reconfigurable Full-Digital Architecture for Angle of Arrival Estimation. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2024**, *71*, 1443–1455. [CrossRef]
17. Tian, L.P.; Chen, L.Q.; Xu, Z.M.; Chen, Z.D. A Localization and Tracking System Using Single WiFi Link. *Remote Sens.* **2023**, *15*, 2461. [CrossRef]
18. Li, Z.; Tian, Z.; Wang, Z.; Zhang, Z. Multipath-Assisted Indoor Localization Using a Single Receiver. *IEEE Sensors J.* **2021**, *21*, 692–705. [CrossRef]
19. Deng, W.; Li, J.; Tang, Y.; Zhang, X. Low-Complexity Joint Angle of Arrival and Time of Arrival Estimation of Multipath Signal in UWB System. *Sensors* **2023**, *23*, 6363. [CrossRef]
20. Bianchi, V.; Ciampolini, P.; De Munari, I. RSSI-Based Indoor Localization and Identification for ZigBee Wireless Sensor Networks in Smart Homes. *IEEE Trans. Instrum. Meas.* **2019**, *68*, 566–575. [CrossRef]
21. Thorbjornsen, B.; White, N.M.; Brown, A.D.; Reeve, J.S. Radio Frequency (RF) Time-of-Flight Ranging for Wireless Sensor Networks. *Meas. Sci. Technol.* **2010**, *21*, 035202. [CrossRef]
22. Schröder, Y.; Wolf, L. InPhase: Phase-based Ranging and Localization. *ACM Trans. Sens. Netw.* **2022**, *18*, 1–39. [CrossRef]
23. Morano, G.; Guan, K.; Hrovat, A.; Javornik, T. Phase-Based Distance Estimation Integrated with IEEE 802.15.4 TSCH Communication. *IEEE Internet Things J.* **2024**, *11*, 11460–11470. [CrossRef]

24. Morano, G.; Simončič, A.; Kocevska, T.; Javornik, T.; Hrovat, A. Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol. In Proceedings of the 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Toronto, ON, Canada, 5–8 September 2023; pp. 1–7. [CrossRef]
25. Ma, Y.; Zhou, G.; Wang, S. WiFi Sensing with Channel State Information: A Survey. *ACM Comput. Surv.* **2019**, *52*, 1–36. [CrossRef]
26. Dai, J.; Wang, M.; Wu, B.; Shen, J.; Wang, X. A Survey of Latest Wi-Fi Assisted Indoor Positioning on Different Principles. *Sensors* **2023**, *23*, 7961. [CrossRef] [PubMed]
27. Tarekegn, G.; Tai, L.C.; Lin, H.P.; Tesfaw, B.; Juang, R.T.; Hsu, H.C.; Kai-Lun, H.; Singh, K. Applying t-Distributed Stochastic Neighbor Embedding for Improving Fingerprinting-Based Localization System. *IEEE Sens. Lett.* **2023**, *7*, 6005004. [CrossRef]
28. Picazo-Martinez, P.; Barroso-Fernandez, C.; Martin-Perez, J.; Groshev, M.; Oliva, A. IEEE 802.11az Indoor Positioning with mmWave. *IEEE Commun. Mag.* **2023**, 1–7. [CrossRef]
29. Du, R.; Xie, H.; Hu, M.; Narengerile; Xin, Y.; McCann, S.; Montemurro, M.; Han, T.X.; Xu, J. An Overview on IEEE 802.11bf: WLAN Sensing. *arXiv* **2022**, arXiv:2207.04859. [CrossRef]
30. Volpi, A.; Tebaldi, L.; Matrella, G.; Montanari, R.; Bottani, E. Low-Cost UWB Based Real-Time Locating System: Development, Lab Test, Industrial Implementation and Economic Assessment. *Sensors* **2023**, *23*, 1124. [CrossRef] [PubMed]
31. Poulose, A.; Han, D.S. UWB Indoor Localization Using Deep Learning LSTM Networks. *Appl. Sci.* **2020**, *10*, 6290. [CrossRef]
32. Bregar, K.; Hrovat, A.; Mohorčič, M. UWB Radio-Based Motion Detection System for Assisted Living. *Sensors* **2021**, *21*, 3631. [CrossRef] [PubMed]
33. Tiemann, J.; Friedrich, J.; Wietfeld, C. Experimental Evaluation of IEEE 802.15.4z UWB Ranging Performance under Interference. *Sensors* **2022**, *22*, 1643. [CrossRef] [PubMed]
34. Coppens, D.; Shahid, A.; Lemey, S.; Van Herbruggen, B.; Marshall, C.; De Poorter, E. An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions. *IEEE Access* **2022**, *10*, 70219–70241. [CrossRef]
35. Gao, Z.; Jiao, Y.; Yang, W.; Li, X.; Wang, Y. A Method for UWB Localization Based on CNN-SVM and Hybrid Locating Algorithm. *Information* **2023**, *14*, 46. [CrossRef]
36. Bertalanic, B.; Morano, G.; Cerar, G. LOG-a-TEC Testbed Outdoor Localization Using BLE Beacons. In Proceedings of the 2022 International Balkan Conference on Communications and Networking (BalkanCom), IEEE, Sarajevo, Bosnia and Herzegovina, 22–24 August 2022; pp. 115–119. [CrossRef]
37. Milano, F.; Rocha, H.; Laracca, M.; Ferrigno, L.; Espírito Santo, A.; Salvado, J.; Paciello, V. BLE-Based Indoor Localization: Analysis of Some Solutions for Performance Improvement. *Sensors* **2024**, *24*, 376. [CrossRef] [PubMed]
38. Simončič, A.; Javornik, T.; Sešek, A.; Hrovat, A. Direction of Arrival Estimation for BLE: Antenna Array Design and Evaluation. *AEU-Int. J. Electron. Commun.* **2023**, *168*, 154722. [CrossRef]
39. Pau, G.; Arena, F.; Gebremariam, Y.E.; You, I. Bluetooth 5.1: An Analysis of Direction Finding Capability for High-Precision Location Services. *Sensors* **2021**, *21*, 3589. [CrossRef] [PubMed]
40. Fahama, H.S.; Ansari-Asl, K.; Kavian, Y.S.; Soorki, M.N. An Experimental Comparison of RSSI-Based Indoor Localization Techniques Using ZigBee Technology. *IEEE Access* **2023**, *11*, 87985–87996. [CrossRef]
41. Ahmad, R.; Alhasan, W.; Wazirali, R.; Aleisa, N. Optimization Algorithms for Wireless Sensor Networks Node Localization: An Overview. *IEEE Access* **2024**, *12*, 50459–50488. [CrossRef]
42. Bedford, M.D.; Kennedy, G.A. Evaluation of ZigBee (IEEE 802.15.4) Time-of-Flight-Based Distance Measurement for Application in Emergency Underground Navigation. *IEEE Trans. Antennas Propag.* **2012**, *60*, 2502–2510. [CrossRef]
43. Boer, P.; Romme, J.; Govers, J.; Dolmans, G. Performance of High-Accuracy Phase-Based Ranging in Multipath Environments. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5. [CrossRef]
44. Gunia, M.; Zinke, A.; Joram, N.; Ellinger, F. Setting up a Phase-Based Positioning System Using off-the-Shelf Components. In Proceedings of the 2017 14th Workshop on Positioning, Navigation and Communications (WPNC), Bremen, Germany, 25–26 October 2017; pp. 1–6. [CrossRef]
45. Yang, R.; Yang, X.; Wang, J.; Zhou, M.; Tian, Z.; Li, L. Decimeter Level Indoor Localization Using WiFi Channel State Information. *IEEE Sens. J.* **2021**, *22*, 4940–4950. [CrossRef]
46. *IEEE Std 802.15.4z-2020 (Amendment to IEEE Std 802.15.4-2020)*; IEEE Standard for Low-Rate Wireless Networks–Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques. IEEE Standard: Piscataway, NJ, USA, 2020; pp. 1–174. [CrossRef]
47. Chiasson, D.; Lin, Y.; Kok, M.; Shull, P.B. Asynchronous Hyperbolic UWB Source-Localization and Self-Localization for Indoor Tracking and Navigation. *IEEE Internet Things J.* **2023**, *10*, 11655–11668. [CrossRef]
48. Bluetooth SIG. *Bluetooth Core Specification, V 5.1*; Technical Report 5.1; Bluetooth SIG: San Jose, CA, USA, 2019.
49. Chen, Z.D.; Gokeda, G.; Yu, Y. *Introduction to Direction-of-Arrival Estimation*; Artech House Signal Processing Library; Artech House: Norwood, MA, USA, 2010.
50. Oshiga, O.; Ghods, A.; Severi, S.; Abreu, G. Efficient Slope Sampling Ranging and Trilateration Techniques for Wireless Localization. In Proceedings of the 2015 IEEE Workshop on Positioning, Navigation and Communications (WPNC), Dresden, Germany, 13–16 October 2015; p. 6.

51. Wehner, M.; Richter, R.; Zeisberg, S.; Michler, O. High Resolution Approach for Phase Based TOF Ranging Using Compressive Sampling. In Proceedings of the 2011 8th Workshop on Positioning, Navigation and Communication, Dresden, Germany, 7–8 April 2011; pp. 28–32. [CrossRef]
52. Pelka, M.; Bollmeyer, C.; Hellbrück, H. Accurate Radio Distance Estimation by Phase Measurements with Multiple Frequencies. In Proceedings of the 2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Busan, Republic of Korea, 27–30 October 2014; pp. 142–151. [CrossRef]
53. Schröder, Y.; Reimers, D.; Wolf, L. Accurate and Precise Distance Estimation from Phase-Based Ranging Data. In Proceedings of the 2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Nantes, France, 24–27 September 2018; pp. 1–8. [CrossRef]
54. Van Marter, J.P.; Dabak, A.G.; Al-Dhahir, N.; Torlak, M. Support Vector Regression for Bluetooth Ranging in Multipath Environments. *IEEE Internet Things J.* **2023**, *10*, 11533–11546. [CrossRef]
55. Schröder, Y.; Heidorn, D.; Wolf, L. Investigation of Multipath Effects on Phase-based Ranging. In Proceedings of the 2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Pisa, Italy, 30 September–3 October 2019; pp. 1–8. [CrossRef]
56. VESNA Platform. Available online: https://log-a-tec.eu/hw-vesna.html (accessed on 26 April 2024).
57. AT86RF215 Datasheet. Available online: https://www.microchip.com/en-us/product/at86rf215 (accessed on 26 April 2024).
58. Oikonomou, G.; Duquennoy, S.; Elsts, A.; Eriksson, J.; Tanaka, Y.; Tsiftes, N. The Contiki-NG Open Source Operating System for next Generation IoT Devices. *SoftwareX* **2022**, *18*, 101089. [CrossRef]
59. GitHub-Contiki-NG OS. Available online: https://github.com/9morano/contiki-ng/tree/vesna (accessed on 26 April 2024).
60. Molisch, A. *Wireless Communications: From Fundamentals to beyond 5G*; IEEE Press: Piscataway, NJ, USA; Wiley: Hoboken, NJ, USA, 2022.

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.

Chapter 5

One-way Channel Reconstruction for Robust Phase-based Distance Estimation

Throughout experimentation with our working ISAC prototype and various measurement campaigns, we observed deviations in distance measurements. In environments with strong reflections, the estimated distances consistently exceed the true values. This systematic overestimation is inherent to the MCPD technique, which has become a popular candidate for localization with narrowband radios and was recently incorporated into the Bluetooth standard [37]. MCPD eliminates the impact of synchronization errors and initial phase offsets by combining two one-way measurements into a Two-Way Channel Frequency Response (TWCFR) [61]. However, the combination process artificially increases the number of detected multipath components, distorting the LoS component of interest and degrading distance estimation.

The deviation in estimated distances can be mitigated by reconstructing the One-Way Channel Frequency Response (OWCFR) from the TWCFR, as proposed in [16] and [70]. The proposed algorithms perform well in controlled environments, but their application to our measured datasets reveals a critical weakness. Even small measurement deviations cause substantial reconstruction errors and reduce the reliability of the estimated channel. The proposed algorithms are highly sensitive to noise or deviations in the measurements. In practice, such noise arises from in-band interference with TSCH communication or from other coexisting wireless technologies in the crowded 2.4 GHz ISM band. ISAC systems compound the problem by introducing dedicated sensing signals alongside traditional data signals, intensifying self-interference in the network, further degrading phase measurement quality, and exacerbating the limitations of existing channel reconstruction algorithms.

Recognizing the limitations of current reconstruction techniques, we propose a robust one-way channel reconstruction algorithm designed to tolerate noise and distortions common in ISAC environments. In the paper presented in this chapter, we leverage real-world measurements to guide algorithm design and advance state-of-the-art localization algorithms through enhanced signal processing methods, addressing hypothesis **H4**. Specifically, our approach introduces a branch-selective algorithm for OWCFR reconstruction. We develop a peak-driven adaptive windowing method that suppresses noise in the channel impulse response and generates a TWCFR reference for robust branch selection. In addition, we introduce a delay alignment correction that restores the unambiguous range that is otherwise lost during channel reconstruction. These innovations represent a contribution **C2** providing improvements to core algorithms for distance estimation.

We developed a MCPD simulator that replicates real-world operation of the technique

to assess the proposed solution under edge conditions, thereby providing contribution **C4**. In single-path simulations, we demonstrate that the proposed method reduces the operational Signal-to-Noise Ratio (SNR) threshold to below 0 dB across the entire resolvable range, while existing channel reconstruction methods require SNRs above 5 dB and fail beyond one quarter of the unambiguous time window. We further extend the evaluation to multipath scenarios using standardized channel models. The proposed algorithm consistently reconstructs the true one-way channel for SNR values above 5 dB, clearly outperforming existing methods that degrade under the same conditions.

We further validated the interference robustness through extensive real-world experiments with IEEE 802.15.4 TSCH devices, integrated with our distance estimation framework proposed in Chapter 2. Under strong in-band interference conditions with a Signal-to-Interference Ratio (SIR) of –3 dB, our algorithm matches the true LoS distance in more than 99.8% of all measurements, while conventional methods fail due to spurious multipath peaks or unwrap errors. We also demonstrate stable performance under compressed sampling with the Golomb ruler technique, where existing methods fail to reconstruct the channel correctly. The results provide empirical validation across simulations and real deployments, fulfilling **C4**, and confirm that advanced signal processing can improve localization performance in realistic indoor environments, supporting **H4**.

Finally, in line with contribution **C5**, we make real-world datasets publicly available and release the implementation of the proposed algorithm as an open-source solution, ensuring reproducibility and enabling further research in ISAC-based localization.

Publication included in this chapter:

G. Morano, T. Javornik, A. Simončič, A. Švigelj, and A. Hrovat, **"Interference Mitigation in One-Way Channel Reconstruction for Robust Phase-Based Ranging"**, *IEEE Access*, vol. 14, pp. 939–955, 2026, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3649293

Created open-access resources:

Measurement dataset
G. Morano, A. Simončič, and A. Hrovat, *Two-Way Channel Frequency Response Dataset Obtained with MCPD technique*, Zenodo, Jan. 5, 2026. DOI: 10.5281/zenodo.18153931

Software implementation
G. Morano, *Robust Channel Reconstruction Algorithm*, GitHub repository, 2026. [Online]. Available: https://github.com/e6commlab/owcfr-reconstruction

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 December 2025, accepted 23 December 2025, date of publication 29 December 2025,
date of current version 2 January 2026.

Digital Object Identifier 10.1109/ACCESS.2025.3649293

RESEARCH ARTICLE

Interference Mitigation in One-Way Channel Reconstruction for Robust Phase-Based Ranging

GREGA MORANO, (Graduate Student Member, IEEE), TOMAŽ JAVORNIK, (Member, IEEE), ALEŠ SIMONČIČ, (Student Member, IEEE), ALEŠ ŠVIGELJ, (Senior Member, IEEE), AND ANDREJ HROVAT, (Member, IEEE)
Department of Communication Systems, Jožef Stefan Institute, 1000 Ljubljana, Slovenia
Jožef Stefan International Postgraduate School, 1000 Ljubljana, Slovenia

Corresponding author: Grega Morano (grega.morano@ijs.si)

This work was supported by Slovenian Research and Innovation Agency (ARIS) under Grant J2-4461 and Grant P2-0016.

ABSTRACT Under the Integrated Sensing and Communication (ISAC) paradigm, wireless networks are evolving into multifunctional platforms that seamlessly combine data transmission with high-precision ranging for applications such as indoor navigation, asset tracking, and context-aware Internet of Things (IoT). The Multi-Carrier Phase Difference (MCPD) method has emerged as an effective technique for enabling localization in narrowband communication systems by estimating the channel frequency response (CFR) used for distance estimation. Converting the two-way CFR (TWCFR) into a one-way CFR (OWCFR) provides a physically consistent representation of the propagation channel and thus improves the ranging performance. However, existing channel reconstruction (CR) methods rely on noise-sensitive phase unwrapping which degrades in the presence of noise and interference, common in dense IoT deployments and crowded frequency bands. To address these limitations, we propose a noise-resistant OWCFR reconstruction algorithm that utilizes a peak-driven adaptive windowing strategy to generate a reference TWCFR for reliable square-root branch selection and incorporates a delay alignment correction to restore the maximum unambiguous range. Simulation and experimental results using IEEE 802.15.4 time-slotted channel hopping (TSCH) compliant devices demonstrate that the proposed method achieves robust and accurate distance estimation in more than 99.8% of interference scenarios.

INDEX TERMS Bluetooth, channel frequency response (CFR), channel impulse response (CIR), IEEE 802.15.4, localization, multi-carrier phase difference (MCPD), one-way ranging, phase-based ranging (PBR), time slotted channel hopping (TSCH), two-way ranging.

I. INTRODUCTION

Wireless communication systems are rapidly evolving from single-purpose transmission systems to versatile platforms that seamlessly integrate sensing, localization, and information exchange [1]. Adopting the Integrated Sensing and Communication (ISAC) paradigm, wireless networks no longer treat localization as a supplementary feature but embed sensing capabilities alongside conventional data transmission [2]. This evolution is driven by a variety of applications that require indoor positioning and navigation, real-time asset tracking, and secure, location-based access control.

Empowering smart home and Internet of Things (IoT) ecosystems, ISAC combines seamless connectivity with precise localization, enabling context-aware automation and intelligent interaction with the environment, such as collaborative robots for household chores, presence-based ambient control or touchless home appliances [2], [3]. In industrial IoT, factories and warehouses can achieve greater efficiency and safety through systems that combine communication and precise tracking of assets and personnel [4], [5]. Urban infrastructures can benefit from integrated systems that provide both connectivity and situational awareness, improving services such as traffic management,

The associate editor coordinating the review of this manuscript and approving it for publication was Fang Yang.

© 2025 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

crowd management, and public safety in smart cities [6], [7].

Distance estimation between devices is the first and essential step in most localization schemes and can be obtained by measuring physical signal properties such as received signal strength (RSS), time-of-arrival (ToA), or phase of the signal. Practical IoT deployments with low-cost narrowband radios cannot support the wide bandwidth or high sampling rates that conventional ToA techniques require [8], [9]. As a result, IoT systems are often limited to coarse positioning via RSS, which does not provide the accuracy required for indoor navigation, precision asset tracking, and collaborative robotics applications [10]. Phase-based ranging (PBR) overcomes this constraint by estimating distance through phase shifts introduced by the signal propagation path. With the multi-carrier phase difference (MCPD) technique [11], devices can estimate their mutual distance with a decimeter-level accuracy without the need for wide system bandwidth [12], [13]. The potential of PBR has been recognized by several research works that have investigated its incorporation into IoT communication technologies, including Bluetooth [11], [14], IEEE 802.15.4 [15], [16] and RFID [17]. These studies demonstrate that accurate ranging can be achieved with low-cost narrowband devices, enabling localization alongside existing communication. Recently, the Bluetooth Special Interest Group (SIG) included MCPD in the new channel sounding feature of the Bluetooth Core Specification version 6.0, marking the first standardization of PBR within a widely adopted IoT protocol [18], [19].

In a PBR process, the wireless channel is first sampled using the MCPD technique, where two devices estimate the channel frequency response (CFR) by sequentially hopping across multiple frequencies and capturing the phase of the received signal at each step. A key advantage of MCPD is its ability to resolve the initial phase offsets introduced by the phase-locked loops (PLLs) in each device, which would otherwise distort the measurements. Phase mismatches are eliminated by multiplying the measured one-way CFR (OWCFR) from both devices, producing a two-way CFR (TWCFR) that has traditionally served as the basis for range estimation. Due to the harmonic nature of the measured CFR, different spectral analysis techniques can be used to extract the distance.

Early phase-slope methods estimate the range from the slope of the CFR phase [11], [20], but can model only a single propagation path and therefore suffer from bias in multipath conditions. Fourier transform (FT)-based methods address this limitation by transforming the CFR into a channel impulse response (CIR), which reveals the underlying propagation delays of the line-of-sight (LoS) and multipath components (MPCs), enabling robust range estimation. Variants of FT-based methods have been proposed [21], [22], and comparative studies show that FT-based estimators outperform phase-slope methods [19], [23]. Although FT-based estimators are robust at low signal-to-noise ratio (SNR) conditions, their accuracy is limited by the Fourier resolution set by the available bandwidth (BW). In [24] the author proposed an iterative Bayesian refinement approach to improve the separability of closely spaced MPCs.

Subspace-based range estimation methods decompose the measured CFR into signal and noise subspaces and construct a pseudo-spectrum, where distinct peaks appear at the propagation delays corresponding to the true signal paths. As demonstrated in [12], the MUltiple SIgnal Classification (MUSIC) algorithm can achieve super-resolution when spatial smoothing is applied to the CFR to decorrelate closely spaced MPCs. Later work improved the accuracy and performance of the MUSIC framework by incorporating bandwidth extrapolation of the measured CFR, multi-antenna combining and reduced-complexity pseudo-spectrum computation [8]. In [25] the authors introduced a signal-subspace decomposition (SSD) approach with a long-short term memory (LSTM) model that provides improved distance estimation accuracy compared to MUSIC estimators. Data-driven range estimation approaches have also been explored. Support vector regression (SVR) models have been used to map CFR spectral features to distance estimates [26], and deep learning (DL) models have been trained on spatially smoothed CFR representations [9], both outperforming subspace-based range estimation in indoor environments.

In the conventional PBR pipeline, the estimated TWCFR is passed directly to the range estimation block, as shown in Fig. 1. However, the two-way response produced by MCPD represents a squared version of the physical channel, which contains apparent multipath components that distort the delay structure and reduce ranging accuracy [12], [27], [28]. The limitation can be addressed by introducing a channel reconstruction (CR) stage before range estimation. The goal of CR is to recover an OWCFR from the measured TWCFR and improve range estimation performance.

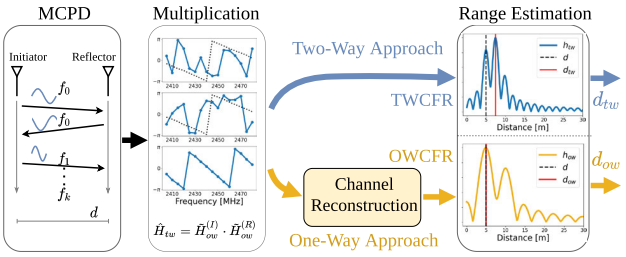


FIGURE 1. Overview of the PBR process. The conventional two-way approach estimates the range directly from the TWCFR, while the one-way approach introduces a CR stage that recovers an OWCFR and improves the ranging performance.

The CR process begins with a square root operation on the TWCFR, which introduces a sign ambiguity that must be resolved. In [29], authors propose to determine the correct sign by comparing the square root TWCFR with the measured OWCFR of one node. The approach relies on maintaining PLL locked when switching between carriers, and requires the time interval between initiator and reflector measurements to remain constant, as any significant timing mismatch can cause a root-flip error. These stringent PLL and

timing requirements inherently limit the applicability of the solution to systems with dedicated hardware.

A more generalized approach was presented in [27], which determines the correct sign by applying phase unwrapping and threshold detection. The proposed approach also extends OWCFR reconstruction to non-contiguous frequency channels, making it applicable to wireless systems operating across multiple bands. However, the method is limited by the accuracy of phase unwrapping, which becomes challenging in the presence of noise in the measured phase. Measurement deviations can confuse the unwrapping algorithm, making the CR method unreliable.

In practical deployments, these deviations arise from hardware fluctuations, sampling techniques, or electromagnetic interference. The 2.4 GHz industrial, scientific, and medical (ISM) band, for example, accommodates numerous wireless technologies, resulting in overlapping transmissions, transient collisions, and variable noise levels. As the number of IoT devices increases [28], the likelihood of spurious emissions and unpredictable interference also increases. ISAC systems compound the problem by introducing dedicated sensing signals alongside traditional data signals, intensifying self-interference in the network, further degrading phase measurement quality, and exacerbating the limitations of OWCFR reconstruction based on phase unwrapping.

In this paper, we propose an enhanced CR algorithm that improves the performance of OWCFR restoration in the presence of noise caused by low SNR values, interference, or compressed sampling techniques. The main contributions of this paper are:

- We develop a branch-selective CR method that switches between square-root TWCFR phase branches using denoised wrap indices to reconstruct a OWCFRthat is consistent with the underlying propagation geometry, while remaining robust to interference and noise.
- We propose a dynamic, peak-driven strategy that identifies dominant CIR peaks and adaptively selects windows around them to generate a noise-reduced reference TWCFR for square-root branch selection.
- We introduce a delay alignment correction to restore the unambiguous range lost during OWCFR reconstruction.
- We validate our approach through simulations and real-world experiments on IEEE 802.15.4 platforms, demonstrating robust performance in multipath and high-interference environments.

The remainder of this paper is organized as follows. Section II presents the PBR and signal model, formalizing the MCPD distance estimation, range estimation, and CR process. This section also introduces the delay alignment correction to recover the full unambiguous range. Section III details our branch-selective OWCFR reconstruction method and the dynamic peak-driven windowing technique. Section IVcompares the computational complexity of the proposed method with baseline CR schemes. Section V outlines the simulation framework and evaluates performance under synthetic channel models. In addition, it describes the collection of real-world data and presents the corresponding experimental results. Section VII provides parameter sensitivity results and discusses the limitations and advantages of the proposed method. Finally, Section VII concludes the paper and discusses directions for future research. The key acronyms and variables used in this paper are summarized in Tables 1 and 2, respectively.

TABLE 1. List of key acronyms.

Acronym	Full Form
MCPD	Multi-Carrier Phase Difference
CFR	Channel Frequency Response
OWCFR	One-Way Channel Frequency Response
TWCFR	Two-Way Channel Frequency Response
CIR	Channel Impulse Response
OWCIR	One-Way Channel Impulse Response
TWCIR	Two-Way Channel Impulse Response
BW	Bandwidth
HPBW	Half-Power Beam Width
UR	Unambiguous Range
UT	Unambiguous Time
FFT	Fast Fourier Transform
iFFT	Inverse Fast Fourier Transform
PLL	Phase-Locked Loop
LoS	Line-of-Sight
MPC	Multipath Component
SNR	Signal-to-Noise Ratio
SIR	Signal-to-Interference Ratio
AWGN	Additive White Gaussian Noise
CR	Channel Reconstruction
CR-DT	Channel Reconstruction with Δt
CR-PU	Channel Reconstruction with Phase Unwrapping
CR-BS	Channel Reconstruction with Branch Selection

Notations: Throughout the paper, $H[\cdot]$ and $h[\cdot]$ denote the discrete CFR and its corresponding time domain CIR, respectively. Subscripts $(\cdot)_{ow}$ and $(\cdot)_{tw}$ indicate one-way and two-way quantities, subscript $(\cdot)_k$ indexes the carrier frequency, while $(\cdot)_l$ and $(\cdot)_m$ label propagation paths. Superscripts $(\cdot)^{(I)}$ and $(\cdot)^{(R)}$ refer to the initiator and reflector nodes, and superscripts such as $(\cdot)^{(DT)}$, $(\cdot)^{(PU)}$ and $(\cdot)^{(BS)}$ distinguish the different reconstruction methods. We use $\angle\cdot$ and $|\cdot|$ for phase and magnitude, $(\cdot)^*$ for complex conjugation, and $\circledast_K$ for circular convolution of length K. Ideal quantities appear without decoration, measured quantities are marked with a tilde $\widetilde{(\cdot)}$, estimated quantities use a hat $\widehat{(\cdot)}$, and filtered quantities use a bar $\overline{(\cdot)}$.

II. PHASE-BASED RANGING

PBR maps phase measurements to a distance estimate between two devices. The pipeline consists of three stages: MCPD acquisition, an optional CR stage, and range estimation. In the conventional two-way approach, the TWCFR from MCPD is passed directly to range estimation, as shown in Fig. 1. In the one-way approach, the additional CR stage

TABLE 2. List of key variables.

Variable	Notation	Description
Ideal OWCFR	H_{ow}	One-way CFR with assumed perfect phase coherency and no noise
Measured OWCFR at initiator	$\widetilde{H}_{ow}^{(I)}$	Phase incoherent one-way CFR measured at initiator node
Measured OWCFR at reflector	$\widetilde{H}_{ow}^{(R)}$	Phase incoherent one-way CFR measured at reflector node
Estimated TWCFR	$\widehat{H}_{tw}$	Two-way CFR obtained by multiplying estimated CFRs from nodes
Noise-reduced TWCFR	$\overline{\widehat{H}}_{tw}$	Windowed two-way CFR with suppressed noise
Square root of the TWCFR	$\widehat{H}_{sqrt}$	Complex square root of the estimated two-way CFR
Estimated OWCFR from CR-DT	$\widehat{H}_{ow}^{(DT)}$	Reconstructed one-way CFR obtained with channel reconstruction method presented in [29]
Estimated OWCFR from CR-PU	$\widehat{H}_{ow}^{(PU)}$	Reconstructed one-way CFR obtained with channel reconstruction method presented in [27]
Estimated OWCFR from CR-BS	$\widehat{H}_{ow}^{(BS)}$	Reconstructed one-way CFR obtained with channel reconstruction method proposed in this paper
UT delay of OWCIR	$T_{0,ow}$	Largest unambiguous time delay that can be estimated from one-way CIR
UT delay of TWCIR	$T_{0,tw}$	Largest unambiguous time delay that can be estimated from two-way CIR

processes the TWCFR to recover an effective OWCFR that more closely follows the true physical channel. The following subsections describe the three stages in more detail.

A. MCPD TECHNIQUE

The MCPD ranging procedure leverages phase measurements across multiple carrier frequencies to estimate the distance between two devices. By adopting an active reflector (AR) technique [20], one device acts as the initiator and the other as the reflector, exchanging continuous wave tones at K frequencies over the available bandwidth (BW), and sampling the in-phase and quadrature (I/Q) components of the received signals. Although early MCPD implementations relied solely on phase measurements, it is now recognized that incorporating amplitude information can further improve distance estimation [12]. The measured OWCFR at the reflector $\widetilde{H}_{ow}^{(R)}$ can be expressed as

$$\widetilde{H}_{ow}^{(R)}[k] = \sum_{l=1}^{L} a_l e^{-j\left(2\pi f_k(\tau_l-\Delta t)-(\phi_k^{(I)}-\phi_k^{(R)})\right)} + \eta_k^{(R)}, \quad (1)$$

and in the measured OWCFR at the initiator $\widetilde{H}_{ow}^{(I)}$ can be expressed as

$$\widetilde{H}_{ow}^{(I)}[k] = \sum_{l=1}^{L} a_l e^{-j\left(2\pi f_k(\tau_l+\Delta t)-(\phi_k^{(R)}-\phi_k^{(I)})\right)} + \eta_k^{(I)}, \quad (2)$$

where f_k is the kth carrier frequency at which the measurement was taken, L is the number of superimposed signal paths, a_l is the amplitude and τ_l is the propagation time of the lth path, Δt is the time difference between the initiator and the reflector, ϕ_k is the initial PLL phase offset of a device, and $\eta_k^{(I)}$ and $\eta_k^{(R)}$ are the assumed additive white Gaussian noise (AWGN) terms for the measurement at kth frequency. Following the MCPD technique, the measured CFR from the reflector is communicated back to the initiator where the two CFRs are multiplied to eliminate the time and phase offsets. The resulting estimated TWCFR $\widehat{H}_{tw}$ for the kth frequency is

$$\widehat{H}_{tw}[k] = \widetilde{H}_{ow}^{(I)}[k] \cdot \widetilde{H}_{ow}^{(R)}[k] = \sum_{m=1}^{M} a_m e^{-j2(2\pi f_k \tau_m)} + \widehat{\eta}_k, \quad (3)$$

where M is the number of newly created signal components, each with the corresponding amplitude a_m and propagation delay τ_m, and $\widehat{\eta}_k$ is the noise component at frequency k, arising from the squared and cross terms of the one-way noise.

B. RANGE ESTIMATION

The range estimation stage converts the measured CFR into an estimate of the propagation distance between the initiator and the reflector. Depending on the processing pipeline, the input to this stage is either the TWCFR produced by MCPD or an OWCFR estimate produced by the CR stage. Several range estimators have been proposed. Subspace-based and data-driven methods can provide enhanced resolution within the same BW, but they depend on design choices such as the assumed number of signal components and model training. In contrast, FT-based analysis applies a deterministic transform to the measured CFR and produces a distance estimate without tuning or training. Although not optimal in terms of absolute ranging accuracy, FT-based range estimation provides a reproducible and transparent baseline suitable for assessing the impact of the CR stage, which is the main focus of this paper.

The FT-based range estimator transforms the obtained CFR into a CIR, identifies the LoS component, and multiplies its propagation delay by the speed of light c_0 to estimate the distance. As the CFR is measured at discrete frequency points, the CIR is obtained using the inverse discrete Fourier transform (iDFT), which is typically implemented by the inverse fast Fourier transform (iFFT) algorithm. The iFFT maps the K collected frequency-domain samples, which are equally spaced with frequency step Δf over a total bandwidth $BW = K\Delta f$, into K time-domain taps ($n = 0, \ldots, K-1$) with:

$$h[n] = \text{iDFT}\{H[k]\} = \sum_{m=1}^{M} \alpha_m \, \delta\big[n - n_m\big] + v[n], \quad (4)$$

where α_m denotes the complex amplitude of the mth path, and n_m is the discrete time index corresponding to the propagation delay τ_m, given by $n_m = \frac{\tau_m}{T_s}$. The time resolution T_s is determined by the measurement BW with $T_s = \frac{1}{BW}$. The term $v[n]$ represents noise in the time domain, obtained as the inverse transform of the frequency-domain noise. The resulting CIR $h[n]$ spans a time window $T_0 =$

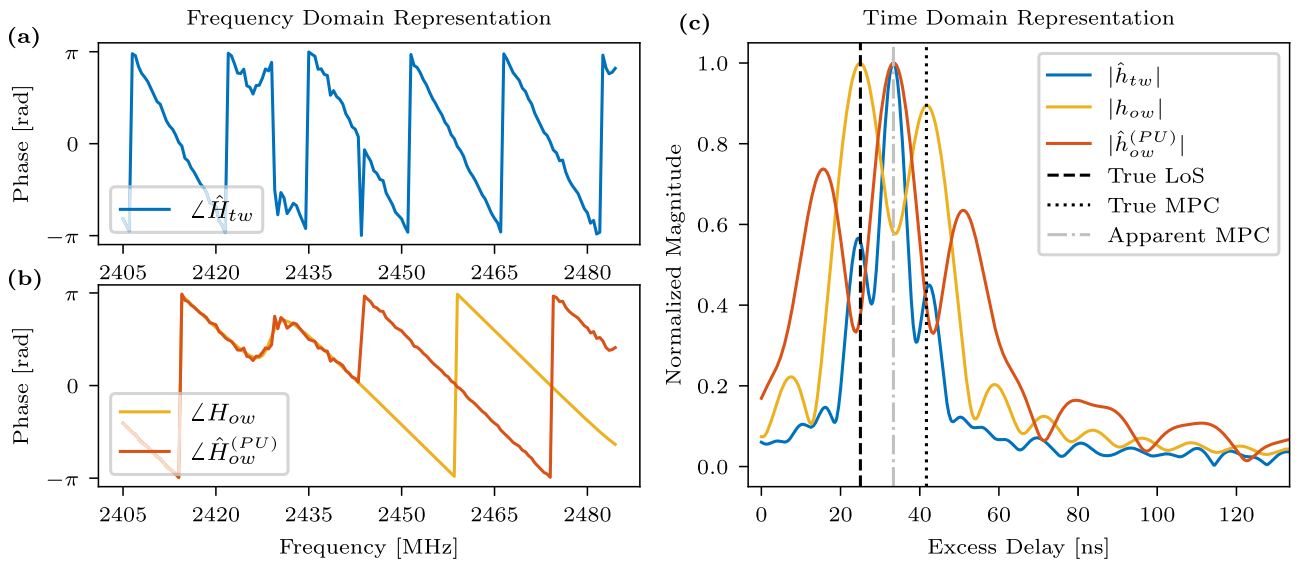


FIGURE 2. An example of a noisy two-tap channel with interference in a single frequency bin at 2442 Mhz. (a) Phase plot of the estimated TWCFR ($\widehat{H}_{tw}$). (b) Phase of the ideal OWCFR (H_{ow}) and the reconstructed OWCFR ($\widehat{H}_{ow}^{(PU)}$) based on CR-PU method, that incorrectly unwraps at 2442 MHz. (c) Corresponding normalized impulse response magnitudes: TWCIR ($\widehat{h}_{tw}$) shows $M = 3$ paths with incorrect delays and magnitudes; the ideal OWCIR (h_{ow}) correctly identifies the LoS path (vertical dashed line) and MPC (vertical dotted line) whereas the one-way reconstruction based on CR-PU ($\widehat{h}_{ow}^{(PU)}$) erroneously restores the CIR.

$K\,T_s$, which defines the maximum unambiguous time (UT) delay and consequently the unambiguous range (UR) over which the MPCs can be distinguished. The CIR appears as a sparse sequence of complex-valued Dirac delta pulses, each corresponding to a propagation path m. Examining the CIR magnitude $|h[n]|$, the height of each peak reflects the amplitude of that path and its position indicates the path delay. The first (and often largest) peak is usually the direct LoS component of interest, while the subsequent smaller peaks arise from reflections and scattering, representing the MPCs.

C. CHANNEL RECONSTRUCTION

The CR stage modifies the output of MCPD before range estimation to align the effective channel representation with the physical one-way propagation. Multiplying the two measured OWCFRs in the MCPD stage mitigates initial phase mismatches and time synchronization effects. In the time domain, multiplication is equivalent to a circular convolution of the two one-way CIRs (OWCIRs):

$$\widehat{h}_{tw}[n] = \widetilde{h}_{ow}^{(I)}[n] \underset{K}{\circledast} \widetilde{h}_{ow}^{(R)}[n]. \tag{5}$$

As a result of the convolution, the two-way CIR (TWCIR) contains an increased number of delay paths M compared to the number of delay paths L in the OWCIR:

$$M = L + \binom{L}{2} = \frac{L(L+1)}{2}, \tag{6}$$

as shown in Fig. 2 (c). The extra taps appear as apparent MPCs, which weaken the true first tap representing the LoS path, making its detection more difficult and reducing ranging accuracy in multipath-rich environments [27]. The introduction of apparent MPCs makes the CIR unusable for sensing applications that require accurate multipath characterization. Furthermore, the multiplication process combines noise from both CFR measurements, increasing the overall noise level in the TWCFR and spreading the channel power over more taps, which reduces their magnitude and can render some undetectable [27].

The CR stage addresses some drawbacks by inserting an intermediate processing block between MCPD and range estimation. The purpose of CR is to reverse the convolution effects and recover a representation that closely resembles the original OWCIR, thereby removing apparent MPCs, restoring the strength of the LoS component, and improving distance estimation. Reconstruction begins by taking the complex square root of the estimated TWCFR and selecting the principal branch, producing $\widehat{H}_{sqrt}$ as follows:

$$\widehat{H}_{sqrt}[k] = b_k \sqrt{\widehat{H}_{tw}[k]}, \quad \text{where } b_k \in \pm 1. \tag{7}$$

The square root operation introduces a sign ambiguity b_k that must be resolved across the carrier frequency index k. When the sequence of signs is recovered correctly, $\widehat{H}_{sqrt}$ coincides with the OWCFR, effectively reconstructing the OWCFR from the TWCFR. Any error in the sequence produces a mismatched OWCFR that generates a CIR unrelated to the true OWCIR and renders the measurement completely unusable.

In [29] the authors propose finding the correct signs b_k by comparing the measured OWCFR of one device with the square root of the TWCFR, evaluating $\Theta[k] = \angle(\widetilde{H}_{ow}^{(I)}[k] \cdot \widehat{H}_{sqrt}^{*}[k])$. Using (2), (3), and (7), we obtain

$$\Theta[k] = 2\pi f_k \Delta t - \Delta\phi_k, \quad \Delta\phi_k = \phi_k^{(R)} - \phi_k^{(I)}. \tag{8}$$

Assuming that the PLL remains locked when switching from frequency index k to $k+1$ so that $\Delta\phi_{k+1} = \Delta\phi_k$, the time difference Δt can be estimated as

$$\widehat{\Delta t} = \frac{\Theta[k+1] - \Theta[k]}{2\pi\,\Delta f}. \tag{9}$$

Since MCPD guarantees that Δt is constant across all carrier frequencies, $\widehat{\Delta t}$ makes a distinct jump at indices k where $\widehat{H}_{sqrt}[k]$ exhibits an incorrect sign. The jump pattern helps resolve the ambiguity in (7) and enables reconstruction of the OWCFR, denoted $\widehat{H}_{ow}^{(DT)}$. Hereafter, we refer to the described reconstruction approach as CR-DT.

However, the CR-DT method can be used only when the PLL remains locked during frequency transitions in the MCPD technique. A more general approach that relaxes the PLL design requirements was presented in [27], which determines the correct sign using phase unwrapping. Specifically, the proposed method analyzes the phase slope of the square root of the TWCFR, $\widehat{H}_{sqrt}$, and identifies the frequency indices where the phase difference between consecutive samples exceeds $\frac{\pi}{2}$. By unwrapping the phase at the detected indices, the method reconstructs the OWCFR, denoted as $\widehat{H}_{ow}^{(PU)}$. Hereafter, we refer to the described CR approach based on phase unwrapping as CR-PU.

D. UNAMBIGUOUS RANGE

Although the effects of CFR multiplication on distance estimation results are well understood [27], its reduction of the maximum UT delay, and therefore the UR of the CIR remain largely unexamined, leaving an important parameter unaddressed by earlier work. For an ideal OWCFR sampled with a frequency step Δf, the FFT-based analysis produces an OWCIR with a period of $T_{0,ow} = KT_s = \frac{1}{\Delta f}$. When two one-way measurements are multiplied to obtain a TWCFR, the corresponding delay-domain operation is a circular convolution of the two impulse responses. The (5) can be rewritten as:

$$\widehat{h}_{tw}[n] = \sum_{p=0}^{K-1} \widetilde{h}_{ow}^{(I)}[p]\,\widetilde{h}_{ow}^{(R)}\big[(n-p) \bmod K\big]. \tag{10}$$

Although convolution increases the time support of the impulse response to twice its original width $2K$, the circular nature (modulo K) folds the indices $n \geq K$ back into the interval $[0, K-1]$. Consequently, the section of $\widehat{h}_{tw}[n]$ that remains alias-free is limited to the first $\frac{K}{2}$ samples, and therefore the maximum UT delay is reduced from $T_{0,ow} = \frac{1}{\Delta f}$ for a one-way measurement to:

$$T_{0,tw} = \frac{K}{2}\,T_s = \frac{1}{2\Delta f}, \tag{11}$$

for a two-way measurement. Any signal propagation component with an excess delay $\tau_m > T_{0,tw}$ is cyclically aliased into the interval $[0, T_{0,tw})$, making the overall interpretation of the impulse response unreliable. Therefore, we recommend using a sufficiently small frequency step during measurements so that practical propagation delays remain below the $T_{0,tw}$ threshold. For example, with $\Delta f = 1\,\text{MHz}$, common in Bluetooth PBR, the two-way unambiguous delay becomes $T_{0,tw} = 500\,\text{ns}$, which corresponds to an unambiguous distance of approximately 150 m.

Taking the square root of the TWCFR and resolving the sign ambiguity in the CR stage does not remove the aliasing caused by the circular convolution of the two one-way impulse responses. In fact, under certain propagation conditions, the reconstructed OWCIR may even be shifted from the first to the second half of the delay window, as illustrated in Fig. 3. To clarify the origin of the CIR shift, we examine the incremental phase of the two-way response from (3), defined as:

$$\Delta\Phi_{tw} = \angle\widehat{H}_{tw}[k+1] - \angle\widehat{H}_{tw}[k] \approx -4\pi\,\Delta f\,\tau. \tag{12}$$

As the time delay (τ) between the transceivers increases, $\Delta\Phi_{tw}$ decreases linearly from 0 to $-\pi$. At certain delay value, denoted τ_{wrap}, the incremental phase reaches $-\pi$ and wraps to $+\pi$. Beyond τ_{wrap} the incremental phase continues to decrease until it reaches 0 again.

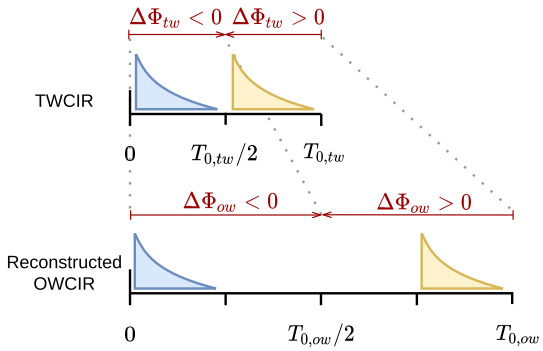


FIGURE 3. OWCIR reconstruction follows the phase slope of the TWCFR $\Delta\Phi_{tw}$. When the average $\Delta\Phi_{tw}$ is negative, the recovered OWCIR maps correctly; when it is positive, the reconstructed OWCIR is shifted by half the delay window ($T_{ow}/2$).

By analyzing the τ_{wrap} for the two-way and one-way channel representations, we can observe that the TWCFR completes a π cycle after only half the delay interval required an ideal OWCFR:

$$-4\pi\,\Delta f\,\tau_{wrap} = -\pi \;\Rightarrow\; \tau_{wrap} = \frac{1}{4\Delta f} = \frac{T_{0,tw}}{2} = \frac{T_{0,ow}}{4}. \tag{13}$$

Since the CR procedure follows the TWCFR phase and interprets $\Delta\Phi_{tw}$ as a one-way phase difference, two distinct reconstructions can occur:

- For channels whose energy is mainly concentrated at delays smaller than τ_{wrap}, the average $\Delta\Phi_{tw}$ is negative, so the recovered OWCIR maps correctly to the interval $[0,\ T_{0,ow}/2]$, where negative phase slopes are expected (Fig. 3 blue shape).
- For channels whose dominant energy lies above τ_{wrap}, the average $\Delta\Phi_{tw}$ appears positive, shifting the reconstructed OWCIR to $[T_{0,ow}/2,\ T_{0,ow}]$ (Fig. 3 yellow

shape). In this case, the estimated propagation delay is systematically greater by $T_{0,ow}/2$.

If left unaddressed, this shift reduces the UT of the reconstructed OWCFR to $T_{0,ow}/4$, further constraining the maximum resolvable range. To compensate for CIR misplacement, we apply a simple alignment correction. For each estimated delay $\hat{\tau}$ obtained from the reconstructed OWCIR we define

$$\hat{\tau}_{corr} = \begin{cases} \hat{\tau}, & \hat{\tau} \le T_{0,ow}/2, \\ \hat{\tau} - T_{0,ow}/2, & \hat{\tau} > T_{0,ow}/2, \end{cases} \tag{14}$$

which maps the corrected delay estimate $\hat{\tau}_{corr}$ back to the physically valid interval $[0, T_{0,ow}/2)$ and restores the full one-way UR.

III. ROBUST OWCFR RECONSTRUCTION

A key weakness in resolving the sign ambiguity in (7) using either CR-DT or CR-PU methods is their sensitivity to measurement deviations. The existing CR methods perform reliably only under high SNR conditions and when the phase slope of the TWCFR is sufficiently small. However, under realistic conditions, several factors introduce or amplify noise in the measured TWCFR, significantly degrading the effectiveness of the CR. First, random fluctuations in hardware and the environment cause unpredictable phase changes, corrupting the measured phase response. Second, in MCPD systems where measurements are taken sequentially at multiple frequencies, external interference at one or more frequencies can produce erroneous phase estimates [28], causing strong deviations in the samples. Third, compressed sampling approaches that extrapolate the TWCFR from fewer samples can introduce additional deviations in the phase [16].

Such deviations in estimated TWCFR can cause incorrect CR for any distance within the UR, as illustrated in Fig. 2, where a single corrupted measurement leads to failure. Larger distances between devices further increase the difficulty in selecting the correct sign b_k, because the phase slope of the TWCFR increases as the range approaches half the UT. For CR-PU, the problem is particularly severe, as the method relies on comparing the phase of two consecutive measurements whose values become nearly π apart near $T_0/2$, leaving no tolerance for small measurement deviations. Any failure in the unwrapping step results in a reconstructed OWCFR that no longer reflects the true channel and becomes unusable for ranging.

To address the identified limitations, we propose a noise resistant CR that resolves the square root ambiguity in (7) using a denoised reference extracted from the estimated TWCFR ($\widehat{H}_{tw}$). The method operates in three steps: 1) peak search, 2) windowing, and 3) square root branch selection, as summarized in Fig. 4. The first two steps generate a noise reduced TWCFR reference $\widehat{\overline{H}}_{tw}$, which is then used in the final step to determine the correct square root branch and obtain the reconstructed OWCFR $\widehat{H}_{ow}^{(BS)}$. Unlike CR-DT, the proposed method does not require the PLL to remain

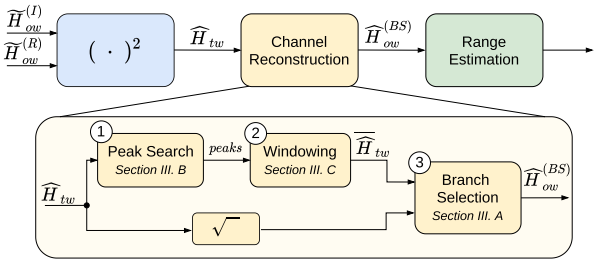


FIGURE 4. The workflow diagram of the proposed CR-BS method.

locked during frequency transitions in MCPD. In addition, the reconstruction is performed on each individual TWCFR measurement without temporal averaging or repeated acquisitions, enabling a single shot operation. Hereafter, we refer to the proposed branch selective reconstruction method as CR-BS. Algorithm 1 summarizes the complete procedure.

A. SQUARE-ROOT BRANCH SELECTION

The core of the proposed CR-BS method is the selection of the correct square root branch in (7) across the carrier index k. Rather than relying on raw phase differences of the estimated TWCFR, which are highly sensitive to noise and interference bursts, the proposed approach anchors all sign transitions to indices where a phase wrap is detected in a noise-reduced TWCFR reference. The reference is constructed through the peak detection and windowing steps introduced later in the section.

The reconstruction begins with the square root of the TWCFR, yielding two possible phase curves by considering the principal branch of the square root $+\sqrt{\widehat{H}_{tw}}$ and its negative branch $-\sqrt{\widehat{H}_{tw}}$, as shown in Fig. 5 (b). The positive branch is selected initially, and its progression is followed until a full phase wrap is detected in the denoised TWCFR reference $\widehat{\overline{H}}_{tw}$. A wrap is declared at carrier index k whenever the difference $|\angle\widehat{\overline{H}}_{tw}[k] - \angle\widehat{\overline{H}}_{tw}[k-1]| \ge \pi$. At each detected wrap index, the opposite branch is selected, and that trajectory is followed until the next wrap. Repeating this process across the carrier index aligns the evolution of the square root with the physical progression of the true one-way channel response and reconstructs the OWCFR $\widehat{H}_{ow}^{(BS)}$. By guiding branch switching with stable wrap points extracted from the denoised reference, the CR-BS produces a consistent OWCFR and avoids erroneous sign flips that affect CR-DT and CR-PU under practical conditions, as illustrated in Fig. 5 (c).

It is important to note that the denoised reference is not used directly to reconstruct the OWCFR. Applying CR-PU or related methods directly to the filtered TWCFR ($\widehat{\overline{H}}_{tw}$) would distort the results, as windowing may suppress parts of the delay profile that belong to the true channel. Instead, the filtered TWCFR is used only to identify reliable wrap indices, while the actual reconstruction is performed on the original estimated TWCFR ($\widehat{H}_{tw}$). Separation ensures that the reconstructed OWCFR preserves the true channel structure when the full square root sequence is stitched together.

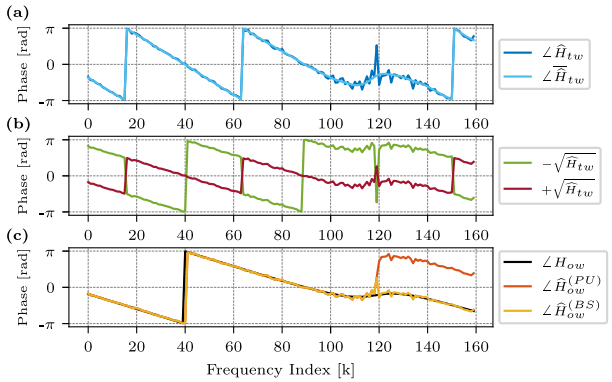


FIGURE 5. (a) Phase of the measured TWCFR $\widehat{H}_{tw}$ and its noise-reduced reference $\overline{\widehat{H}}_{tw}$ used to identify genuine 2π wraps (frequency indexes: 15, 63 and 150). (b) The square root of $\widehat{H}_{tw}$ yields two interleaved phase curves for the positive and negative root branches. (c) CR-BS method begins on the positive root branch and switches the branch at each detected wrap index, ensuring correct one-way phase traversal. The $\widehat{H}_{ow}^{(PU)}$ makes an error at index 119, whereas $\widehat{H}_{ow}^{(BS)}$ correctly follows the ideal OWCFR H_{ow}.

An effective approach to obtain a noise-reduced TWCFR is to transform the estimated channel into the time domain, where the inherent sparsity of the CIR enables easier identification and isolation of signal components. The measured CIR displays distinct peaks corresponding to different signal propagation paths, with noise superimposing additional spurious peaks. To retain only the primary CIR and reduce noise, the true path-induced components are detected and isolated, while the rest of the delay profile is suppressed. In this paper, we propose a windowing technique based on the dynamic identification of CIR peaks and the application of corresponding bandpass windows aligned to the delay of each detected path. Transforming the filtered CIR back into the frequency domain yields a de-noised TWCFR, which serves as a reliable reference for the subsequent branch selection step.

B. PEAK DETECTION

Identifying signal components by detecting peaks in the CIR is challenging in noisy environments, as spurious noise can produce false peaks. To obtain a reference $\overline{\widehat{H}}_{tw}$, we propose defining a fixed amplitude threshold in the CIR and selecting every peak that exceeds this threshold as a signal component. Although a threshold-based approach may occasionally omit very weak multipath arrivals or include a noise artifact, it provides a simple and repeatable procedure for isolating the dominant contributors to the CFR.

The threshold is determined by squaring the absolute CIR to obtain a power delay profile (PDP) and sorting the samples by amplitude to generate an empirical cumulative distribution function (CDF) curve, as shown in Fig. 6. In a typical sparse channel, the curve begins with a long, gently rising tail that represents the noise floor values, followed by a convex increase toward the end of the curve, which corresponds to the peak values from the PDP. In low-noise channels, the knee index of the CDF, i.e. the point of maximum curvature, effectively separates the noise-related values from the steep ascent caused by the peak values. This knee can be identified

Algorithm 1 Channel Reconstruction With Branch Selection

Input: $\widehat{H}_{tw}, P, F$
Output: $\widehat{H}_{ow}^{(BS)}$
Initialization:
$K \leftarrow \texttt{length}(\widehat{H}_{tw})$
peaks $\leftarrow [\,]$
$W \leftarrow \texttt{ones}(K)$
Procedure:
// Step 1: Peak search with threshold
win $\leftarrow \texttt{Hann}(K)$
$\widehat{h}_{tw} \leftarrow \texttt{IFFT}(\widehat{H}_{tw} \cdot \text{win})$
PDP $\leftarrow |\widehat{h}_{tw}|^2$
CDF $\leftarrow \texttt{sort}(\text{PDP})$
dCDF $\leftarrow \texttt{differentiate}(\text{CDF})$
$\text{TH}_P \leftarrow \texttt{max}(\text{dCDF}) \cdot P$
relmax $\leftarrow \texttt{relmax}(\text{PDP})$ // indices of local maxima
for each p**in**relmax **do**
  if $PDP[p] \geq TH_P$ **then**
    append $p$topeaks
  end if
end for
// Step 2: Window segments and product of complements
for each τ_i**in**peaks **do**
  $\Delta_i \leftarrow \texttt{HPBW}(\tau_i) \cdot F$ // Half-power width of peak τ_i
  if $\Delta_i > K$ **then**
    $\Delta_i \leftarrow K$
  end if
  segment $\leftarrow \texttt{Hann}(\Delta_i)$
  $w_i \leftarrow \texttt{zeros}(K)$
  for $l = 0$**to**$\Delta_i - 1$ **do**
    $l_{circ} \leftarrow (l - \lfloor \Delta_i/2 \rfloor + \tau_i) \bmod K$
    $w_i[l_{circ}] \leftarrow$ segment$[l]$
  end for
  $W \leftarrow W \cdot (1 - w_i)$
end for
$W \leftarrow 1 - W$
$\overline{h}_{tw} \leftarrow W \cdot \widehat{h}_{tw}$
$\overline{\widehat{H}}_{tw} \leftarrow \texttt{FFT}(\overline{h}_{tw})$
// Step 3: Branch selection based on $\overline{\widehat{H}}_{tw}$
$\phi \leftarrow \angle \overline{\widehat{H}}_{tw}$
$\widehat{H}_{sqrt} \leftarrow \sqrt{\overline{\widehat{H}}_{tw}}$
$b \leftarrow 1$
for $k = 1$ **to** $K - 1$ **do**
  if $|\phi[k] - \phi[k-1]| > \pi$ **then**
    $b \leftarrow -b$
  end if
  $\widehat{H}_{ow}^{(BS)}[k] \leftarrow b \cdot \widehat{H}_{sqrt}[k]$
end for
return $\widehat{H}_{ow}^{(BS)}$

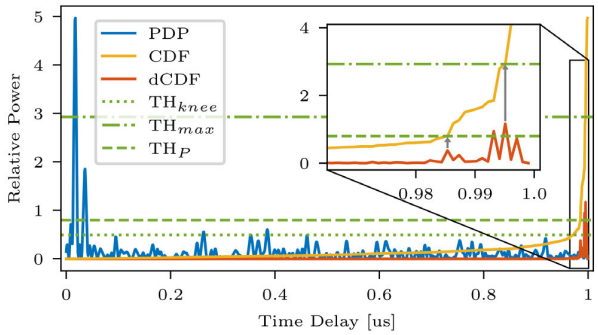


FIGURE 6. The operation of the peak search algorithm in noisy two-tap channel. The PDP is plotted in blue, its CDF in yellow and the derivative of the CDF in red. The threshold obtained with knee method TH_{knee} erroneously classifies noise-related peaks as weak multipath components. The threshold based on the maximum of the CDF derivative TH_{max} recognizes the dominant peak, while the threshold based on a fraction P of the maximum derivative TH_P correctly identifies both signal components and avoids the noise.

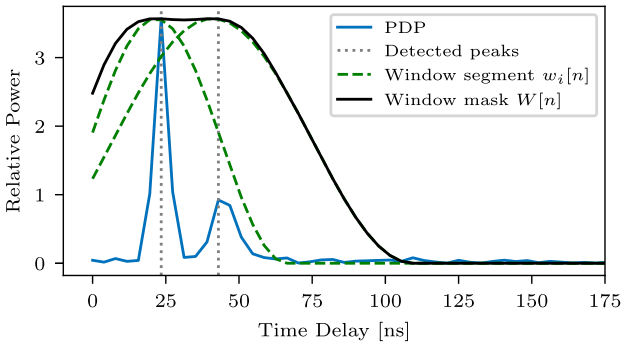


FIGURE 7. The PDP (blue curve) with individual Hann windows w_i (dashed green curve) centered at each detected peak τ_i (dotted gray line). The windows w_i are merged into a single composite window mask W, wrapping around the borders of the PDP. Note that the rightmost window w_i is wider, reflecting the broader HPBW.

using the curvature-based method described in [30] and the threshold (TH_{knee}) is defined as the PDP value at the knee location index. However, as noise variance increases, noise-related peak values raise the tail of the CDF curve, causing the knee detector to frequently misidentify noise peaks as weak multipath components, thereby reducing the robustness of the peak detection process.

To better align threshold selection with the shape of the PDP, we analyze the rate of change in the empirical CDF. Its derivative curve (dCDF) displays distinct spikes, each corresponding to a jump in the CDF caused by high peak values in the PDP. Although the maximum derivative indicates the largest jump in the CDF and thus the strongest peak in the PDP, we instead define the threshold using the index of the first occurrence where the derivative exceeds a fraction P of that maximum. The value of the PDP at this index is taken as the peak search threshold TH_P. The approach ensures that peaks of meaningful magnitude are preserved while ignoring noisy variations, and provides a flexible mechanism to adapt the threshold to different propagation environments. For example, a lower P (e.g., 0.2) will admit more moderate reflections in multipath-rich scenarios, while a higher P (e.g., 0.5) will focus exclusively on the very strong paths common in sparse settings.

C. DYNAMIC WINDOW DESIGN

The purpose of windowing is to isolate the signal's components of interest while attenuating the noise-dominated regions. We observed the following design criteria for effective window design:

- **Sufficient bandpass width**: The window must be wide enough to capture all relevant information from the signal components.
- **Smooth transition**: An abrupt drop from the bandpass to the bandstop (a "sharp window") can introduce undesirable phase distortions. Therefore, a gradual roll-off in the window is essential to minimize unwanted phase shifts.
- **Periodicity**: As the FFT representation of the CIR is inherently periodic, the window must maintain this periodicity. If the detected peak lies near the edge of the CIR, the window should roll over to the other side, ensuring continuity for the iFFT.

Building on the dynamic peak-driven windowing framework, we formalized the construction of individual narrow windows centered on each detected CIR peak and the procedure for combining them into a unified composite filter mask, as shown in Fig. 7. To isolate the spectral contributions of distinct propagation components, a finite-length Hann window $w_i[n]$ is centered at each detected delay τ_i:

$$w_i[n] = \begin{cases} 0.5\left[1 - \cos\left(2\pi \dfrac{n - \left(\tau_i - \frac{\Delta_i}{2}\right)}{\Delta_i - 1}\right)\right], & |n - \tau_i| \le \frac{\Delta_i}{2}, \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

The window span Δ_i is calculated from the half-power beam width (HPBW) of the i-th peak (the difference between the two delay indices where the PDP envelope falls to the half of the peak value) and is scaled by a factor F to capture side lobes and deep fade regions. Isolated propagation paths produce sharp peaks, while densely clustered multipath arrivals produce broader features. Using HPBW to determine the width of each window enables the filter span to adapt intrinsically to the local multipath density.

If any window extends beyond the edges $[0, K]$ of the PDP interval, its samples wrap around modulo K to maintain the inherent periodicity of FFT. The individual window segments $w_i[n]$ are then merged into a single smooth composite mask $W[n]$ through the algebraic sum merge:

$$W[n] = 1 - \prod_{i=1}^{I} (1 - w_i[n]), \tag{16}$$

where I is the total number of detected peaks. This "fuzzy union" operation retains the individual Hann window shapes in regions without overlap and smoothly saturates

towards unity where overlaps occur, resulting in a composite mask that preserves all signal components while effectively suppressing noise.

IV. COMPUTATIONAL COMPLEXITY

PBR is typically implemented on resource constrained IoT devices, where computational load is an important design factor. In this section, we analyze the computational complexity of the proposed CR-BS algorithm and compare it with the CR-DT and CR-PU baseline methods to assess their feasibility on embedded platforms.

The proposed CR-BS consists of three stages, as shown in the diagram in Fig. 4. In the first stage, the TWCFR is windowed, transformed to the time domain, and used to identify signals of interest, where I denotes the number of detected peaks, and $I < K$. In the second stage, the samples around each peak are windowed with the global weighting function W, producing the filtered TWCFR. In the third stage, the denoised TWCFR is used for branch selection, reconstructing the OWCFR. The three steps contribute to the overall time complexity function:

$$T(K, I) = T_{peak}(K) + T_{win}(K, I) + T_{bs}(K). \quad (17)$$

The initial CFR windowing requires $2K$ operations, while the subsequent K point IFFT has a cost of $\frac{3K}{2} \log K$. The computation of the PDP and its CDF involves sorting the K values, contributing another $K \log K$ operations. The CDF differentiation, search for local maxima and amplitude thresholding are performed through linear scans, each requiring K operations. Selecting the valid peaks then requires I comparisons. Hence, the total complexity of the peak search stage is

$$T_{peak}(K) = O(K \log K). \quad (18)$$

For each detected peak τ_i the algorithm generates a window segment of length Δ_i, performs circular indexing to place it on a grid of length K, and updates the global window W via elementwise multiplication. The computational cost for a single peak is therefore $2K + 2\Delta_i$. The cost of constructing a global window over I peaks is $O\big(IK + \sum_{i=1}^{I} \Delta_i\big)$. Since $\Delta_i \leq K$ for all peaks, the total cost is dominated by $O(IK)$. Afterwards, the denoising is performed with multiplication of TWCIR and W which requires K operations, followed by FFT of length K to reconstruct the filtered TWCFR, contributing $\frac{3K}{2} \log K$ operations. The cost function of the windowing stage becomes

$$T_{win}(K, I) = O(IK + K \log K). \quad (19)$$

In branch selection, the computation of the filtered TWCFR phase, the square root operation on the TWCFR, and the phase jump-based branch selection loop each require K operations. Therefore,

$$T_{bs}(K) = O(K). \quad (20)$$

Combining the stages yields

$$T(K, I) = O(IK + K \log K + K). \quad (21)$$

TABLE 3. Asymptotic time complexity of CR algorithms for TWCFR of K carrier frequencies.

Algorithm	Computational Complexity
CR-DT	$O(K)$
CR-PU	$O(K)$
CR-BS	$O(K \log K)$

In the worst case scenario, where half of the points in the PDP are selected as detected peaks and $I = \frac{K}{2}$ the complexity becomes quadratic, $O(K^2)$. However, in typical sparse multipath channels, the number of significant detected peaks I is small and does not increase with K. In this regime, the dominant cost arises from the two FFT operations and the sorting algorithm, giving the final time complexity

$$T(K) = O(K \log K). \quad (22)$$

For comparison, the baseline methods CR-PU and CR-DT have linear complexity in the number of carrier frequencies K. The CR-PU method first applies the square root to the TWCFR and then unwraps the phase across the K carrier frequencies. Both operations require K steps, so the overall complexity is $O(K)$. The CR-DT method applies the square root to the TWCFR, forms a product sequence by combining the square root of the TWCFR with the measured CFR of one device, computes the time difference, detects phase jumps, and constructs and applies the correction mask. Each of the five steps requires K operations, so the complexity of CR-DT also grows linearly with K. The asymptotic time complexity of the three algorithms is summarized in Table 3.

The proposed CR-BS algorithm introduces an additional logarithmic factor in time complexity compared to CR-DT and CR-PU. This additional cost is mainly due to the FFT operations and the sorting step in the peak search stage. Nonetheless, in the complete PBR pipeline, the dominant computational cost often arises in the subsequent range estimation step. In case of FT-based analysis, the input CFR is typically interpolated by zero padding to improve the accuracy of delay estimation, and processed by an iFFT with a size significantly larger than the number of measured carriers K. The computational complexity of such range estimation exceeds the cost of CR-BS, so the additional CR stage has a low impact on overall runtime. The per snapshot cost of CR-BS is therefore within capabilities of resource-constrained IoT and modern embedded platforms that already implement FT-based range estimators. In exchange for the increased computational load, CR-BS provides a significant improvement in robustness of OWCFR reconstruction in the presence of noise and interference, as demonstrated in the following Section V.

V. EVALUATION OF THE PROPOSED METHOD

The evaluation of the proposed algorithm is divided into two parts: simulation-based results and results from real-world deployments. Simulations enable analysis of the

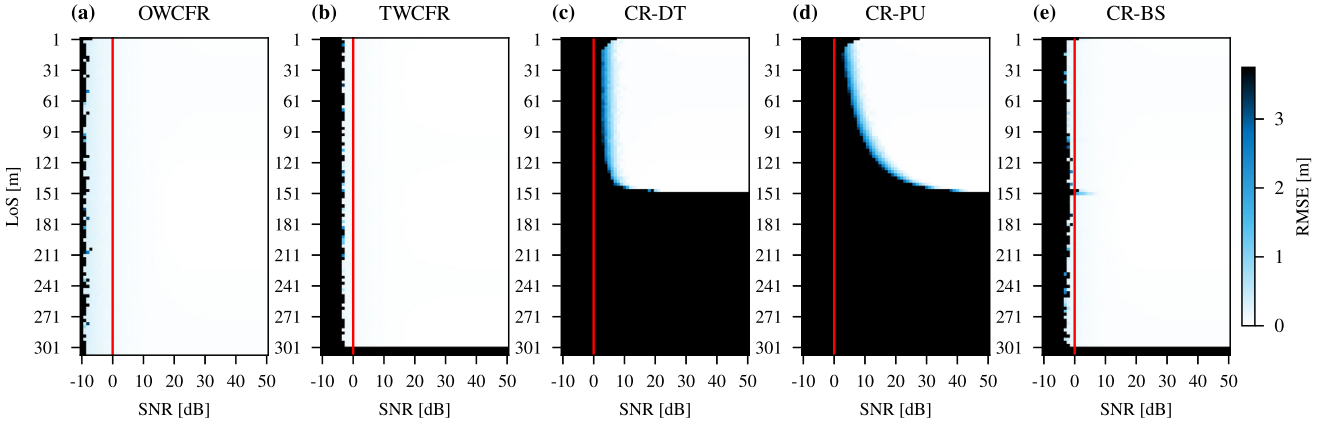


FIGURE 8. RMSE of distance estimation for a single-tap simulation. Plots (a) to (e) present the RMSE obtained when the range estimator uses different CFR inputs, namely: (a) ideal OWCFR (H_{ow}), (b) estimated TWCFR ($\widehat{H}_{tw}$), (c) estimated OWCFR from the CR-DT method ($\widehat{H}_{ow}^{(DT)}$), (d) estimated OWCFR from the CR-PU method ($\widehat{H}_{ow}^{(PU)}$), and (e) estimated OWCFR from the proposed CR-BS method ($\widehat{H}_{ow}^{(BS)}$). For ease of comparison, the 0 dB SNR level is indicated with red vertical line.

algorithm under edge-case conditions, while measurements provide valuable insights into its practical operability. For all experiments, the range estimation stage was carried out with a fixed FT-based procedure. The estimated CFR was zero-padded to 8192 bins, and an iFFT was applied to generate the corresponding CIR. The propagation delay was then extracted as the delay of the maximum peak in the CIR and multiplied by the speed of light to obtain the estimated distance. The unified processing chain allowed for direct comparison of the CR-PU, CR-DT and CR-BS methods without bias from additional range estimator design choices. For the proposed CR-BS algorithm, the following values were used: the peak search parameter P was set to 0.2 and the window factor F to 10, unless stated otherwise.

A. SIMULATION RESULTS

The simulations were performed using a custom-designed simulation framework that emulates the MCPD algorithm. The simulator takes propagation delays and their corresponding amplitudes as input and then synthesizes the CFR measurements of the initiator and reflector over 160 frequency carriers uniformly spaced from 2405 MHz to 2484.5 MHz. AWGN is added according to a specified SNR. The noise power is derived from the average received signal power, computed as the sum of the mean powers received across all propagation paths. For the analysis, ideal synchronization is assumed, meaning that there is no carrier frequency offset or clock drift between devices. Although CFO or clock drift can introduce a linear phase slope across frequencies that affects the absolute range estimate [13], they do not introduce abrupt phase discontinuities that cause failures in CR methods, which are the focus of the analysis.

Firstly, a single propagation path was considered and the distance between the devices was swept from 1 m to 304 m in steps of 3 m. Signal attenuation along this LoS path was modeled using the free-space path loss propagation model. As only a very strong LoS component is expected, the parameter P of the CR-BS algorithm is set to 0.5. Fig. 8 shows the root mean square error (RMSE) of 500 independent distance estimations for SNRs ranging from -10 dB to 50 dB, where the RMSE is capped at 3.75 m as errors above this threshold render the measurement unusable. It can be observed that the distance estimation results depend strongly on the CFR input provided to the range estimation stage.

When the ideal OWCFR is used as input (Figs. 8 (a)), the estimator operates at a lower SNR and maintains higher accuracy. When the estimated TWCFR is used (Figs. 8 (b)), the multiplication step introduces combined noise that increases the lower SNR limit of operation and degrades the accuracy of distance estimates. Although not fully depicted (the distance sweep was limited to 305 m for visual clarity), the ideal OWCFR supports distance estimation up to 600 m, while TWCFR measurements reach a maximum UR of only 300 m. The reduced limit is a side effect of the circular convolution that halves the UT of the two-way measurements. The results of the CR-DT method presented in Fig. 8 (c) show a limited operating region. Reliable distance estimation appears only at sufficiently high SNR (above 5 dB) and the maximum operational range remains below 150 m ($c_0 \frac{T_{0,ow}}{4}$). Outside the reliable region, the CR-DT method does not preserve the true one-way channel representation, leading to large errors in distance estimation. The CR-PU results in Fig. 8(d) show an even more restricted region of correct operation as the distance between devices increases. The increased RMSE can be attributed to the phase unwrapping step, which compares the phase of two consecutive measurements whose values become nearly π apart around the 150 m, leaving no tolerance for small measurement deviations. Fig. 8 (d) presents the results of the proposed CR-BS. The method successfully resolves the range ambiguity for delays above $\frac{T_{0,ow}}{4}$ and reduces the lower limit of operation to SNR below 0 dB. A small degradation appears near 150 m, which is the same effect observed for the CR-DT and CR-PU methods, but the impact on CR-BS is considerably smaller. Notably, although

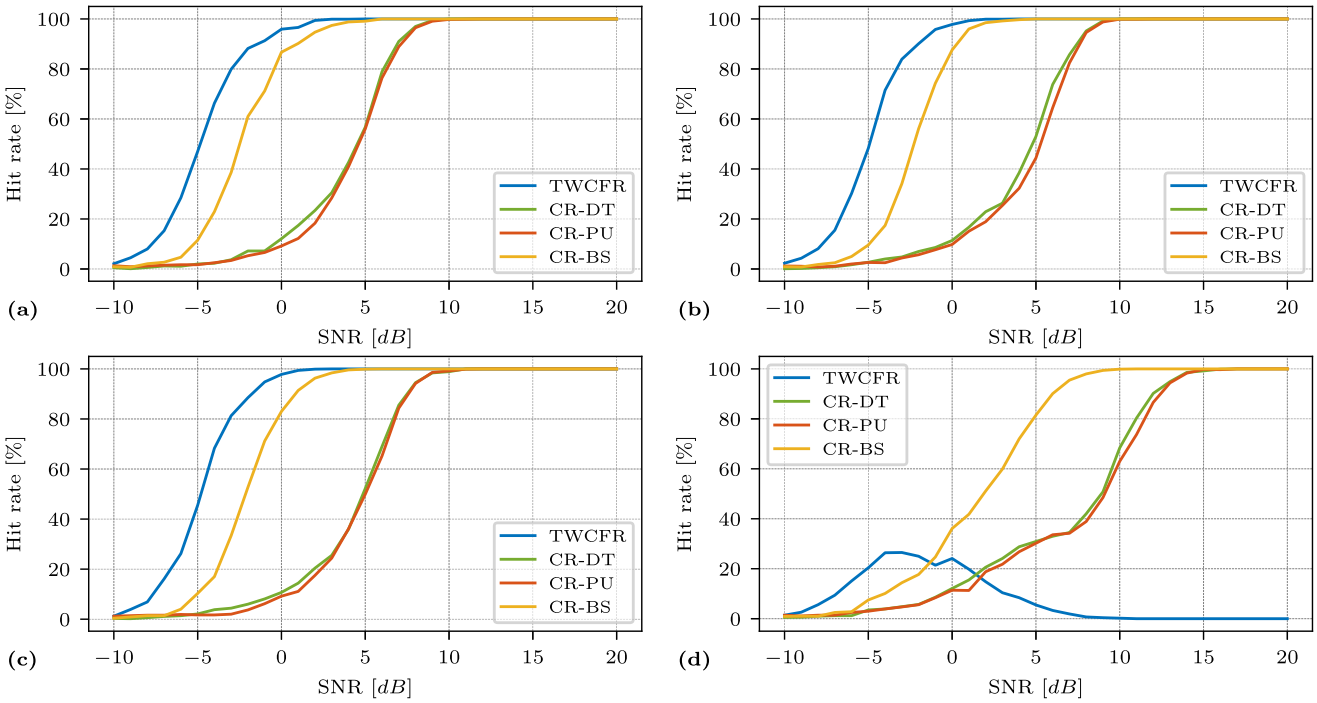


FIGURE 9. The percentage of distance estimates within ±12.5 cm of the true distance (hit rate) with standardized channel models: (a) TGn model B, (b) TGn model C, (c) TGn model D, and (d) TGn model B variant with the increased power of each path in the second cluster by 1.5 dB.

the proposed CR-BS reconstructs a one-way representation of the channel, the UT does not return to the ideal one-way limit and remains the same as that of the two-way channel.

To assess the robustness of the algorithm in more realistic propagation scenarios, we conducted additional simulations using standardized IEEE 802.11 TGn channel models [31]. We considered three LoS channel models: a) Model B (15 ns delay spread, two clusters), for small indoor environments such as offices, b) Model C (30 ns delay spread, two clusters), suited to larger indoor or mixed indoor/outdoor settings such as open-plan offices and hallways, and c) Model D (50 ns delay spread, three clusters), representing spacious environments such as large halls or classrooms, where richer multipath is expected. In addition to the standardized models, we analyzed a modified "high-reflection" variant of Model B, in which the power of every tap in the second cluster was increased by 1.5 dB. The proposed adjustment emulates environments with strong nearby reflectors (e.g., metallic furniture, computer monitors, or industrial equipment) and provides insight into the performance of the algorithm in wireless channels where two propagation paths produce an apparent multipath artifact caused by the multiplication of measured CFRs. AWGN was applied to each channel model over an SNR range of –10 dB to 20 dB in 1 dB increments. At each SNR step, 1000 independent distance estimates were generated from the corresponding CFRs, and the percentage of estimates within 0.25 m of the true distance (hit rate) was calculated. The results are presented in Fig. 9 where subplots (a), (b), and (c) show Models B, C, and D, respectively,

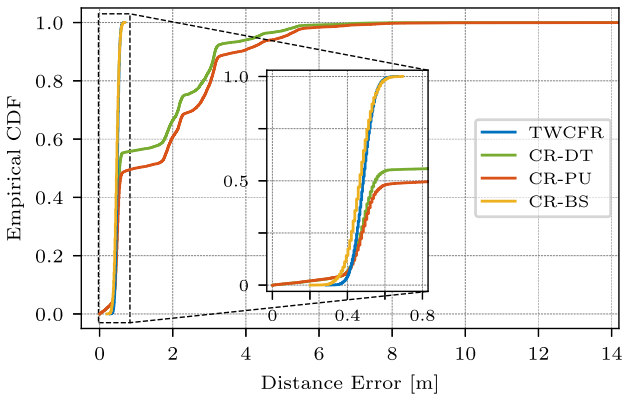


FIGURE 10. CDF of the absolute distance estimation error for the TGn channel model C operating at SNR of 5 dB. The inset provides a magnified view for clarity.

while subplot (d) corresponds to the high-reflection variant of Model B.

When the range estimation stage operates directly on the TWCFR input, the first three scenarios show nearly perfect hit rates for SNR values above 2 dB. However, these high hit rates conceal the fact that the resulting TWCIR contains apparent multipath components, rendering the impulse response unusable for sensing tasks that require an exact channel representation. The limitation becomes evident in the modified Model B scenario (Fig. 9 (d)), where an apparent peak introduced by the two-way operation dominates the true LoS component and causes the range estimator to select an incorrect delay. Consequently, the

hit rate of the TWCFR input drops to zero, revealing a fundamental weakness in relying on two-way measurements in the range estimation stage. In contrast, the CR-DT and CR-PU provide a reconstructed OWCFR to the estimator and succeed in recovering the correct impulse response, but only when the SNR exceeds 15 dB. Below this level, their hit rates fall rapidly. The proposed CR-BS reduces the SNR requirement to below 10 dB and maintains high hit rates even in the presence of considerable noise.

The empirical cumulative distribution of absolute distance errors at an SNR of 5 dB for Model C, based on 10000 trials, is shown in Fig. 10. The zero-padding length for distance estimation was increased from 8192 to 65536 bins so that the CDF appears as a smooth curve rather than a stepped one. When the range estimation stage receives the OWCFR from CR-PU as input, phase unwrapping failures cause approximately half of the estimates to deviate by up to 8 m or more, rendering these measurements unusable. The CR-DT produces a similar distribution, with slightly better performance than CR-PU. The proposed CR-BS reconstruction removes the extreme errors and achieves a tighter error distribution, outperforming the TWCFR in the low SNR regime.

B. MEASUREMENTS WITH INTERFERENCE

The performance of the proposed algorithm was evaluated using real-world channel measurements taken in a conference room (4 m by 6 m) where magnetic boards mounted on the walls provided strong reflective surfaces for multipath components, as shown in Fig. 11. Two proprietary VESNA devices [32], equipped with an AT86RF215 radio supporting IQ sampling, probed the channel under a modified IEEE 802.15.4 Time Slotted Channel Hopping (TSCH) protocol [16] that enables seamless PBR alongside standard communication. Each device captured 160 IQ samples in the frequency range from 2400.5 MHz to 2480.0 MHz.

The transceivers were placed in three LoS configurations, Setup 1, Setup 2 and Setup 3 with separations of 2 m, 3 m and 4 m, respectively. The ground truth distances for all three setups were confirmed using a laser ranger. We obtained 2140 measurements in Setup 1, 2200 measurements in Setup 2 and 2015 measurements in Setup 3. Each distance estimate includes a fixed hardware offset caused by additional propagation paths through the antennas, cables, and circuit board traces. In our deployment, this offset was measured at 1.8 m. The resilience of the algorithm to in-band interference was assessed by injecting additive noise into IEEE 802.15.4 channel 19 (center frequency 2445 MHz and span of 5 MHz) in all three setups, so that the signal-to-interference ratio (SIR) was –3 dB.

Only three CFRs were evaluated in the measurement study: TWCFR and the OWCFRs obtained from the CR-PU and CR-BS methods. The CR-DT method was excluded because the radios used in the experiment do not enable PLL lock. Nonetheless, simulation analysis has already demonstrated that CR-PU performs comparably with CR-DT, so the exclusion of CR-DT does not affect the interpretation of the measurement results.



FIGURE 11. Measurements in a conference room with two magnetic whiteboards.

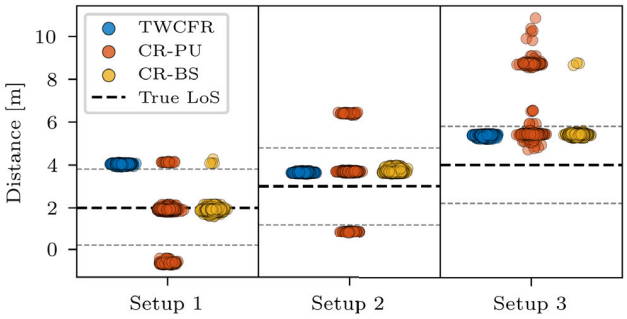


FIGURE 12. Estimated peak locations from real-world measurements with interference on channel 19. Each dot on the plot represents the location of a maximum peak for the estimated CIR.

The distance estimates obtained from different CFR across the setups are shown in Fig. 12. Each dot marks the position of the strongest CIR peak selected as the LoS component. In Setup 1, the TWCFR estimates cluster tightly around 4 m instead of the true 2 m because the multiplication artifact peak in TWCIR outweighs the actual LoS arrival peak and directs the estimator to an incorrect delay. The CR-PU method produces a more dispersed cloud of points that largely lie on the correct distance but occasionally fall below or above it, reflecting phase unwrapping failures caused by in-band interference on channel 19. Note that some of the plotted estimates fall below zero, which results from the hardware offset calibration. In contrast, the OWCFR of the proposed CR-BS method adheres to the 2 m reference line in 99.8 percent of all trials, confirming its ability to reconstruct the channel accurately even in the presence of interference.

An example of impulse responses from measurements in Setup 1 is shown in Fig. 13. The plot illustrates the combination of one-way peaks at 3.7 m and 8.4 m (at 1.9 m and 6.6 m after hardware offset calibration) to create the apparent two-way peak at 5.8 m (at 4 m after calibration). Additionally, the plot demonstrates an occasional distortion of distance estimation due to CR-PU creating a CIR that does not resemble the true channel. These real-world measurement

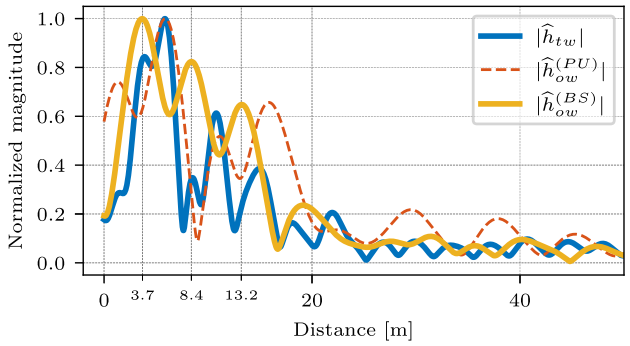


FIGURE 13. Example of CIR estimates from measurements in Setup 1. Since the x-axis is not calibrated for hardware distance offset, the LoS peak is located at 3.7 m instead of 2 m.

results also reveal the fundamental limitation of FT-based range estimation imposed by the 80 MHz measurement bandwidth. Closely spaced MPCs that fall within the $\frac{c_0}{BW}$ resolution merge into a single peak or shift each other through spectral leakage. This systematic error prevents any CR method from achieving perfect accuracy in Setups 2 and 3, where multiple reflections lie near the direct path.

Key error statistics across all three setups are summarized in Table 4. The mean absolute error (MAE) measures the average magnitude of the estimation errors, while the standard deviation (STD) quantifies the spread of those errors around the mean. The hit rate (HR) is the percentage of distance estimates that are within the ± 1.875 m of the true separation. This threshold was chosen to match the resolution of the FT-based range estimator, given by c_0/BW. In Setup 1 the CR-BS delivers highly accurate results, whereas the CR-PU shows high variability, with HR of only 84.5 percent and STD of 0.93 m. In Setup 2 both TWCFR and OWCFR from CR-BS achieve flawless HR with MAE values of 0.65 and 0.69 respectively, reflecting the systematic range estimation error due to bandwidth limitation. The CR-PU remains more erratic with HR of 84.6% and STD of 1.07 m. In Setup 3 the CR-BS again maintains its accuracy with 99.8% HR, while the CR-PU degrades to 78.6%. Overall, CR-BS consistently outperforms baseline methods by combining correct peak recovery with low variance, even under strong interference and across varying propagation channels.

C. MEASUREMENTS WITH COMPRESSED SAMPLING

We further validated the algorithm using a publicly available data set [16] that uses compressed sampling measurements in three real-world deployments: an indoor office, an indoor hallway, and an outdoor park. The measurements were obtained using a modified MCPD scheme, in which the Golomb ruler technique was used to reduce the number of carrier frequencies sampled, thereby decreasing interference with other devices and lowering the energy usage of the devices. After extraction of the samples, the CFR consists of 160 samples with a frequency step of $\Delta f = 0.5$ MHz. Fig. 14 shows the distance estimation results for the three scenarios with the true distance on the x-axis and the distance

TABLE 4. Mean absolute error (MAE), standard deviation (STD), root mean square error (RMSE) and hit rate (HR) counting estimates within ± 1.875 m of the true distance.

		MAE [m]	STD [m]	RMSE [m]	HR [%]
Setup 1	TWCFR	2.054	0.025	2.054	0.0
	CR-PU	0.476	0.931	1.02	84.5
	CR-BS	0.104	0.111	0.143	99.8
Setup 2	TWCFR	0.649	0.017	0.649	100.0
	CR-PU	0.957	1.073	1.16	84.6
	CR-BS	0.695	0.065	0.698	100.0
Setup 3	TWCFR	1.394	0.033	1.394	100.0
	CR-PU	2.136	1.362	2.533	78.6
	CR-BS	1.426	0.132	1.432	99.8

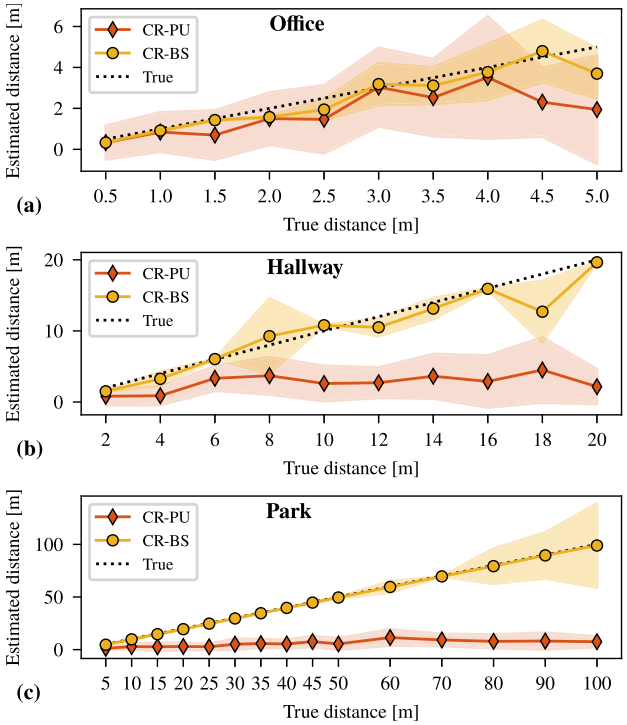


FIGURE 14. Real-world measurement results for: (a) indoor office, (b) indoor hallway and (c) outdoor park. Diamonds and dots denote the median distance estimates when the input for range estimation is obtained from the CR-DT and CR-BS, respectively. The shaded area represents the standard deviation of the measurements.

estimation on the y-axis. Each point in the plot corresponds to the median of the estimated distances, and the spline area around indicates the standard deviation of the estimations.

The compressed sampling technique introduces spikes in the phase response of the TWCFR, as presented in Fig. 15, which completely confuse the CR-PU reconstruction algorithm. As observed in Fig. 14, the algorithm functions only when the distance between devices is short, and otherwise fails to determine the correct distance. In contrast, the proposed CR-BS successfully reconstructs the OWCFR and with it the distance estimation in all three scenarios,

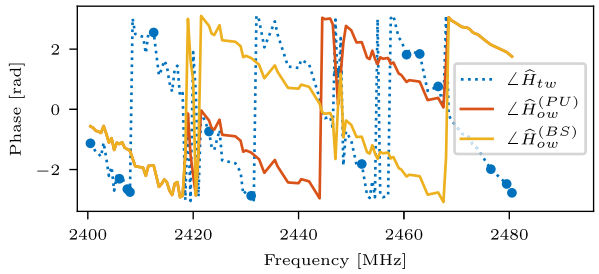


FIGURE 15. Phase of the CFR estimates made using the Golomb ruler technique. The TWCFR is reconstructed by extrapolating 15 measured samples (marked with blue dots) to 160 points, introducing pronounced phase spikes (around 2420 and 2468 MHz) that confuse the phase unwrapping algorithm and render the OWCFR from CR-PU unreliable.

with a noticeably lower standard deviation compared to the CR-PU.

VI. DISCUSSION

To assess the robustness of the proposed peak-driven windowing method, we conducted a detailed parameter sensitivity analysis focusing on the two key design parameters, the peak-selection threshold P and the window-scaling factor F. The evaluation was performed on a modified TGn model B channel. For SNR levels between -4 dB and 14 dB, we generated 1000 independent noisy realizations of the TWCFR. For each realization and every combination of P and F, we obtained the OWCFR from the CR-BS reconstruction, estimated the distance using the FT-based estimator, and recorded the hit rate as the percentage of cases in which the dominant CIR peak was within ± 12.5 cm of the true delay.

The results, corresponding to P values of 0.01, 0.05, 0.1 and 0.5, are shown in the four subplots of Fig. 16 and reveal a clear interaction between the two parameters. When P is set very low, the peak detector accepts even weak noise-induced fluctuations, especially under low SNR conditions. When many peaks are falsely identified as valid signal components, numerous windows are created, collectively passing a significant amount of noise and reducing the hit rate. Increasing the threshold avoids spurious peak detections and improves performance, as only CIR peaks that correspond to actual propagation paths are admitted. For higher thresholds, such as $P = 0.1$ and $P = 0.5$, the algorithm identifies only the strongest components, so the window must be wider to capture the surrounding energy of the multipath features. Consequently, the best results for $P = 0.1$ and $P = 0.5$ are obtained when the window factor is approximately $F = 8$. Once P becomes sufficiently large to reliably exclude noise peaks, further increases of P do not significantly affect the behavior, and the performance curves become visually indistinguishable. Across all threshold levels, a consistent pattern emerges: wider windows allow more noise to pass through, and once F becomes excessively large the filter spans nearly the entire CIR, so performance gradually declines.

The main limitation of the proposed approach is the reliance on accurate peak detection and appropriate

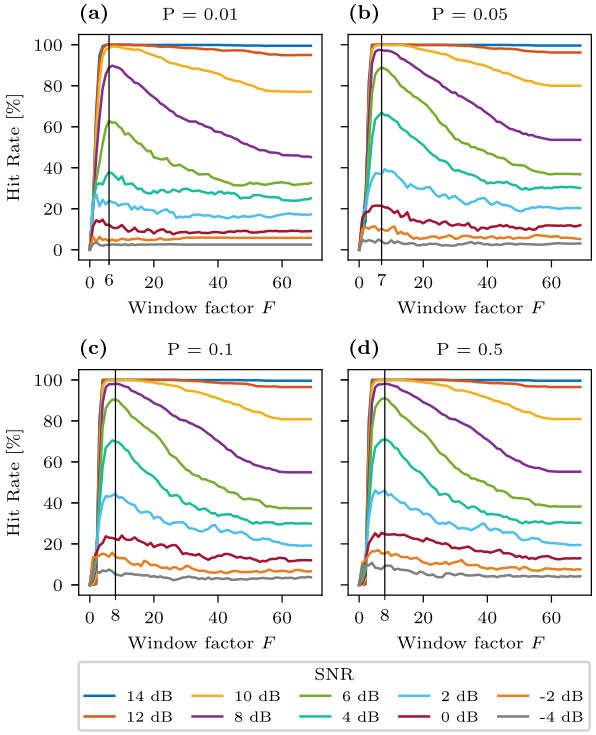


FIGURE 16. Parameter sensitivity of the proposed method for the standardized BN channel model. Each subplot shows the hit rate of CR-BS performance as a function of the window factor F for a peak-selection threshold P: (a) 0.01, (b) 0.05, (c) 0.1 and (d) 0.5. Plot curves represent different SNR levels ranging from -4 dB to 14 dB. Results are obtained from 1000 simulations per SNR value.

windowing. In scenarios with very weak or strongly overlapping MPCs, the thresholding strategy may fail to identify all physically significant peaks, leading to incomplete reconstruction. Similarly, an inappropriate choice of F can either truncate useful signal energy or admit excessive noise, making CR-BS performance sensitive to parameter tuning in channels that deviate from the assumed sparse multipath structure. Nonetheless, the overall study confirms that the proposed CR-BS is highly adaptable and that appropriate adjustment of P and F enables reliable reconstruction even under low SNR conditions.

The simulation and experimental results show that with 80 MHz measurement bandwidth, closely spaced MPCs partially overlap and become distorted through spectral leakage, producing a systematic range error that no CR method can resolve. CR-BS can restore the correct one-way structure at the available delay resolution, but it cannot separate MPCs that fall within the same delay bin or undo the bias caused by clusters that already appear as a single tap in the measured CIR. As a result, CR-BS improves the quality of the input to the range estimator, but the final distance estimate is still constrained by the sounding bandwidth and by the simple maximum peak rule in the FT-based estimator.

Another limitation of the proposed CR-BS method concerns computational complexity and, consequently, energy consumption on constrained IoT devices. As presented

in Section IV, the proposed method imposes additional computational load compared to baseline CR methods. In channels with many significant MPCs, the constant factors in (21) increase, so the energy cost per ranging instance can rise even further. As a trade off, the higher complexity provides improved reconstruction accuracy and ranging performance compared to baseline CR methods, particularly in the presence of strong phase distortions and noise.

At the same time, CR-BS operates on a single snapshot of the TWCFR and does not rely on temporal averaging or tracking. Therefore, the method remains applicable in the presence of non-stationary interference and device mobility, provided that the MCPD frequency sweep is completed within the channel coherence time. Moreover, the algorithm works with the estimated TWCFR and is therefore independent of the underlying physical layer or protocol. Although the experiments are performed with a MCPD implementation in IEEE 802.15.4 TSCH hardware, the method is directly compatible with Bluetooth due to the shared multi-carrier channel sounding procedure, making the approach applicable to other practical PBR solutions.

VII. CONCLUSION

In this work, we propose CR-BS, a branch selective OWCFR reconstruction method that operates on noisy TWCFR measurements and recovers a one-way channel representation consistent with the underlying propagation channel. We also address the implicit misalignment of OWCIR caused by the reconstruction procedure and present a simple delay alignment correction to recover the full unambiguous range. In contrast to the baseline reconstruction schemes CR-PU and CR-DT, the proposed method enables reliable operation at lower SNR and under strong interference. Simulation results for single-tap and standardized multipath channel models demonstrate that our method lowers the operational SNR threshold to below 0 dB for single-path scenarios and below 10 dB in rich multipath, while maintaining the original maximum UR. Real-world measurements using IEEE 802.15.4 TSCH platforms, even under strong in-band interference and compressed sampling, confirm hit rates above 99% and robust one-way channel recovery, demonstrating that CR-BS provides a practical and reliable CR solution for low-cost PBR systems. In future work, we plan to integrate super-resolution range estimation algorithms to mitigate the systematic delay error introduced by bandwidth limitations and to analyze their operation in combination with our proposed OWCFR reconstruction method.

REFERENCES

[1] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022.

[2] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous IoT: Applications, trends, and challenges," *IEEE Netw.*, vol. 35, no. 5, pp. 158–167, Sep. 2021.

[3] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, "A survey of localization systems in Internet of Things," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 761–785, Jun. 2019.

[4] T. Savic, X. Vilajosana, and T. Watteyne, "Constrained localization: A survey," *IEEE Access*, vol. 10, pp. 49297–49321, 2022.

[5] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2568–2599, 3rd Quart., 2019.

[6] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling joint communication and radar sensing in mobile networks—A survey," *IEEE Commun. Surv. Tut.*, vol. 24, no. 1, pp. 306–345, 1st Quart., 2022.

[7] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.

[8] S. N. Shoudha, J. P. Van Marter, S. Helwa, A. G. Dabak, M. Torlak, and N. Al-Dhahir, "Reduced-complexity decimeter-level Bluetooth ranging in multipath environments," *IEEE Access*, vol. 10, pp. 38335–38350, 2022.

[9] Z. Bin Tariq, J. P. Van Marter, A. G. Dabak, N. Al-Dhahir, and M. Torlak, "Reduced complexity deep learning approach for Bluetooth ranging in multipath environments," *IEEE Sensors J.*, vol. 24, no. 19, pp. 31431–31441, Oct. 2024.

[10] A. Moradbeikie, A. Keshavarz, H. Rostami, S. Paiva, and S. I. Lopes, "A cost-effective LoRaWAN-based IoT localization method using fixed reference nodes and dual-slope path-loss modeling," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100990.

[11] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with Bluetooth low energy (BLE)," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.

[12] P. Boer, J. Romme, J. Govers, and G. Dolmans, "Performance of high-accuracy phase-based ranging in multipath environments," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[13] A. Simončič, G. Morano, A. Hrovat, and T. Javornik, "Optimizing frequency switching pattern to reduce asynchronization effect in MCPD ranging systems," *IEEE Access*, vol. 13, pp. 169791–169811, 2025.

[14] P. Zand, A. Duzen, J. Romme, J. Govers, C. Bachmann, and K. Philips, "A high-accuracy concurrent phase-based ranging for large-scale dense BLE network," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–7.

[15] Y. Schröder and L. Wolf, "InPhase: Phase-based ranging and localization," *ACM Trans. Sensor Netw.*, vol. 18, no. 2, pp. 1–39, Jan. 2022.

[16] G. Morano, K. Guan, A. Hrovat, and T. Javornik, "Phase-based distance estimation integrated with IEEE 802.15.4 TSCH communication," *IEEE Internet Things J.*, vol. 11, no. 7, pp. 11460–11470, Apr. 2024.

[17] L. Xie, D. Jiang, X. Fu, and Q. Jiang, "Centimeter-level localization algorithm with RFID passive tags," in *Wireless and Satellite Systems*, M. Jia, Q. Guo, and W. Meng, Eds., Cham, Switzerland: Springer, 2019, pp. 160–170.

[18] (Aug. 2024). *Bluetooth Core Specification*. [Online]. Available: https://www.bluetooth.com/specifications/specs/core-specification-6-0/

[19] M. Nikodem, G. Trajnowicz, G. S. de Blasio, and F. A. Quesada-Arencibia, "Experimental evaluation of multicarrier phase difference localization in Bluetooth low energy," *IEEE Sensors J.*, vol. 25, no. 1, pp. 1548–1560, Jan. 2025.

[20] M. Pelka, C. Bollmeyer, and H. Hellbruck, "Accurate radio distance estimation by phase measurements with multiple frequencies," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Oct. 2014, pp. 142–151.

[21] G. von Zengen, Y. Schroder, S. Rottmann, F. Busching, and L. C. Wolf, "No-cost distance estimation using standard WSN radios," in *Proc. IEEE 35th Annu. IEEE Int. Conf. Comput. Commun.*, Apr. 2016, pp. 1–9.

[22] Y. Schröder, D. Reimers, and L. Wolf, "Accurate and precise distance estimation from phase-based ranging data," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Sep. 2018, pp. 1–8.

[23] M. Gunia, A. Zinke, N. Joram, and F. Ellinger, "Setting up a phase-based positioning system using off-the-shelf components," in *Proc. 14th Workshop Positioning, Navigat. Commun. (WPNC)*, Oct. 2017, pp. 1–6.

[24] J. Mazur, "High-resolution phase-based ranging using inverse Fourier transform in an iterative Bayesian approach," *Sensors*, vol. 24, no. 20, p. 6758, Oct. 2024.

[25] Z. B. Tariq, J. P. Van Marter, A. G. Dabak, N. Al-Dhahir, and M. Torlak, "A data-driven signal subspace approach for indoor Bluetooth ranging," *IEEE J. Indoor Seamless Positioning Navigat.*, vol. 2, pp. 292–303, 2024.
[26] J. P. Van Marter, A. G. Dabak, N. Al-Dhahir, and M. Torlak, "Support vector regression for Bluetooth ranging in multipath environments," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11533–11546, Jul. 2023.
[27] S. Helwa, J. P. Van Marter, S. N. Shoudha, M. Ben-Shachar, Y. Alpert, A. G. Dabak, M. Torlak, and N. Al-Dhahir, "Bridging the performance gap between two-way and one-way CSI-based 5 GHz WiFi ranging," *IEEE Access*, vol. 11, pp. 70023–70039, 2023.
[28] A. Sheikh, J. Romme, J. Govers, A. Farsaei, and C. Bachmann, "Phase-based ranging in narrowband systems with missing/interfered tones," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15171–15185, Sep. 2023.
[29] J. Romme, "Method for distance determination," U.S. Patent 10 928 495 B2, Feb. 23, 2021.
[30] V. Satopaa, J. Albrecht, D. Irwin, and B. Raghavan, "Finding a, 'Kneedle' in a Haystack: Detecting Knee Points in System Behavior," in *Proc. 31st Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2011, pp. 166–171.
[31] V. Erceg, *IEEE P802.11 Wireles LANs, TGn Channel Models*, Standard 802.11-03/940r4, May 2004.
[32] G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Distance- and angle-based hybrid localization integrated in the IEEE 802.15.4 TSCH communication protocol," *Sensors*, vol. 24, no. 12, p. 3925, Jun. 2024.



GREGA MORANO (Graduate Student Member, IEEE) received the M.Sc. degree in electrical engineering from the University Of Ljubljana, in 2021. He is currently pursuing the Ph.D. degree in information and communication technologies with the Jožef Stefan International Postgraduate School.

He is currently a Research Assistant with the Department of Communication Systems, Jožef Stefan Institute, Ljubljana. His research interests include the IoT communication protocols, wireless localization, integrated sensing and communications, embedded systems, wireless sensor networks, and wireless experimental testbeds.



TOMAŽ JAVORNIK (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 1987, 1990, and 1993, respectively.

He is currently a Scientific Counsellor with the Communication Systems Department, Jožef Stefan Institute, Ljubljana, and an Assistant Professor with the Jožef Stefan International Postgraduate School, Ljubljana. He participated in several COST and Framework Program projects. He has co-authored more than 100 refereed journal and conference papers and several books and book chapters in the field of mobile and wireless communications. He holds two international patents. His research experience is in the field of telecommunications, focusing on the development and performance analysis of fixed and mobile systems, radio-channel measurements, modeling and simulations, and in indoor localization. He serves as a TPC member or a reviewer for several IEEE conferences and journals.



ALEŠ SIMONČIČ (Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Ljubljana, in 2019 and 2022, respectively. He is currently pursuing the Ph.D. degree in information and communication technologies with the Jožef Stefan International Postgraduate School.

His master's thesis focused on the estimation of the angle of arrival using BLE technology and antenna arrays. He is also a Young Researcher with the Department of Communication Systems, Jožef Stefan Institute, Ljubljana. His research interests include radio communication systems, particularly protocols, antennas and arrays, direction of arrival estimation methods, embedded systems, and radio environment characterization.



ALEŠ ŠVIGELJ (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 1997, 2000, and 2003 respectively.

He is currently a Senior Research Fellow with the Department of Communication Systems, Jožef Stefan Institute, and a Full Professor with the Jožef Stefan Postgraduate School. He has extensive research in modelling, simulation, and design of advanced telecommunications elements, systems, and services. He has also participated as a coordinator in several national and international projects, including COST projects. He co-authored several books/book chapters and more than 100 peer-reviewed journal and conference papers. His current work focuses on advanced networking technologies for wireless systems.



ANDREJ HROVAT (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Ljubljana, in 2004 and 2008, respectively, and the Ph.D. degree from the Jožef Stefan International Postgraduate School, in 2011.

He has been with the Department of Communication Systems, Jožef Stefan Institute, since 2004. He is currently holding the position of a senior research fellow. He works on several projects connected with professional mobile communication systems, 2G-5G, WiFi, and the IoT technologies, satellite, and sensor networks, including several COST actions, framework program projects, H2020 projects, European space agency (ESA) projects, and numerous national research and application projects. He is the author or co-author of more than 120 peer-reviewed journal and conference papers. His research and working experience are in telecommunications, focusing on development and performance analysis for fixed and mobile systems, including terrestrial, stratospheric, satellite systems, and radio-channel modeling for fixed and mobile narrowband and broadband radio communication systems. He is a TCP member of various international conferences and workshops. He is a reviewer of several international impact-factor journals. He serves on a journal editorial board member and the guest editor.

Chapter 6

Conclusions and Future Work

The integration of sensing and communication marks a fundamental transformation in modern wireless systems. ISAC aims to unify traditionally separate function within a single framework, allowing communication networks to transmit data while simultaneously extracting environmental information such as position, movement, presence, and environmental structure. This convergence has the potential to reshape the IoT ecosystem by transforming communication infrastructures into intelligent, context-aware systems capable of simultaneous connectivity and environmental perception. However, the implementation of ISAC in low-power, narrowband IoT networks remains a challenge. The primary objective of this work was therefore to explore, design, and validate methods that enable seamless integration of localization functionality through distance and angle estimation into IEEE 802.15.4 TSCH communication, thereby establishing a practical foundation for ISAC operation in resource-constrained IoT systems.

6.1 Summary of Contributions

The first part of the research addresses phase-based distance estimation as a fundamental enabler of ISAC localization. Recognizing the limitations of RSSI and ToF techniques on narrowband hardware, the MCPD technique was adopted and integrated into the TSCH communication framework. Two novel methods of phase measurements were introduced to embed the ranging process within the TSCH timeslot structure. The integration enabled distance estimation with each exchanged packet, converting regular communication into a dual-purpose operation, that supports the ISAC vision. A lightweight channel sampling scheme and compressed frequency selection based on Golomb ruler design were developed to reduce the number of measurements while maintaining sub-meter accuracy. The complete system was implemented on the Contiki-NG platform and evaluated on VESNA devices equipped with AT86RF233 radios. Empirical results demonstrated that high-accuracy distance estimation can be achieved with minimal protocol modification and acceptable trade-offs in throughput and energy consumption. This work provided the first demonstration of phase-based ranging integrated into TSCH communication, fulfilling hypotheses **H1** and **H2** and providing contributions **C1.1** and **C3.1**.

The second part of the thesis extended the integration paradigm to AoA estimation, providing direction estimation to complement range-based localization. A phase measurement process was designed and integrated into the TSCH slot, enabling sequential phase sampling across multiple antennas using a single RF chain and an antenna switch. To mitigate distortions caused by CFO and SFO, a two-stage calibration procedure was proposed, consisting of a coarse estimation using reference samples and a fine estimation based on antenna switching data. The complete solution was implemented on OpenMote-B nodes

with AT86RF215 radios and validated through experimental campaigns in indoor environments. The results confirmed that accurate AoA estimation is feasible on constrained IoT hardware with negligible impact on network performance. The presented work validated hypotheses **H1** and **H2**, provided contributions **C1.2**, **C2**, and **C3.2**, and demonstrated that ISAC can be implemented within the operational framework of IEEE 802.15.4 TSCH.

While distance and direction estimation provide valuable sensing information, their combination enables accurate and efficient localization through a hybrid localization framework. The approach, presented in the third part of the thesis, addressed the practical limitations of standalone lateration and angulation methods by enabling 2D localization using only a single anchor node. The design leveraged the inherent hierarchical topology of TSCH networks, where parent–child communication links serve as data channel and sensing opportunity, thereby eliminating the need for inter-node coordination or additional signaling. The proposed system was implemented on a VESNA platform equipped with an AT86RF215 transceiver and an eight-element antenna array. Experimental results demonstrated sub-meter localization accuracy, with an average error of 0.37 m achieved after median filtering over five successive measurements. The approach preserved communication efficiency, required minimal hardware modifications, and maintained compatibility with existing protocol operation. This confirmed hypotheses **H1** and **H3**, delivering contributions **C1.3** and **C3.3**, and established the first practical implementation of hybrid localization within a TSCH-based IoT network.

Given the critical challenges posed by interference and noise in ISAC systems operating within shared and congested frequency bands, the research was advanced to enhance the robustness of the localization algorithms. In the fourth part of this work, a novel one-way channel reconstruction algorithm was proposed to restore the OWCFR from the TWCFR under noise or interference conditions. The developed algorithm introduced branch-selective reconstruction, peak-driven adaptive windowing, and delay alignment correction methods to suppress noise-induced artifacts and maintain correct channel reconstruction. Simulations and real-world experiments demonstrated superior performance compared to existing approaches, achieving reliable operation at SNR below 0 dB and SIR at –3 dB. The study confirmed hypothesis **H4** and represents contribution **C2** by establishing a robust algorithm for reliable phase-based distance estimation under realistic interference scenarios.

The thesis presents a comprehensive and experimentally validated framework for integrating sensing functionalities into TSCH-based IoT communication systems. Through algorithmic design, hardware prototyping, and extensive empirical evaluation, the research identifies key performance limitations and practical challenges in realistic, highly interfered indoor environments. The results informed the refinement of the proposed methods and provided a reproducible basis for further comparative studies, thereby representing contribution **C4**. Additionally, the work follows the principles of open science by publicly releasing of all developed software components and measurement datasets. Together, the resources constitute one of the few openly available solutions for phase-based channel sampling in constrained IoT networks, offering valuable reference data and tools for ongoing studies in localization, signal processing, and machine learning. By enabling reproducibility and supporting the validation of emerging ISAC algorithms, this effort provides contribution **C5** and establishes a foundation for future developments in ISAC research.

6.2 Future Work

The presented work establishes a foundation for integrating sensing and communication in TSCH-based IoT systems and exposes several questions that define key directions for

future investigation. We identify and group them within the three categories, reflecting the need for improved system performance, deeper analysis of design trade-offs between sensing and communication, and improved security in the novel use of existing communication infrastructure.

Improved signal processing and channel sampling

The presented solutions demonstrate the potential and the limitations of phase-based sensing on constrained IoT hardware. Our work identified challenges unique to low-cost platforms, where hardware imperfections significantly affect localization accuracy. The CFO is very common in low-cost hardware and impacts all types of unsynchronized channel sampling. While CFO effects were successfully mitigated in the proposed AoA estimation technique, they remain an open challenge in the distance estimation framework. Furthermore, despite the achieved accuracy, the signal processing algorithms used are still computationally and energy intensive. Therefore, future research should focus on developing more efficient signal processing algorithms that can run directly on low-power embedded platforms without sacrificing accuracy.

Channel sampling represents another major source of energy consumption on constrained devices, emphasizing the need for further optimization. The employed compressed sampling technique based on Golomb rulers significantly reduced the number of measurements required for distance estimation. Similar approaches could be explored for AoA estimation to further reduce acquisition time and power consumption. Additionally, reusing the same channel samples for both distance and angle estimation presents a promising feature for hybrid localization. Designing unified sampling procedures that jointly support MCPD and AoA techniques, especially when multiple antennas are available, could improve sensing efficiency by enabling simultaneous extraction of distance and direction information.

Communication-sensing trade-offs

The available operational prototype enables further investigation of the trade-offs between communication performance and sensing accuracy. In the current hybrid localization design, distance and angle are estimated with every transmitted packet, which may not be efficient for networks with strict latency or throughput constraints. Adaptive approaches could optimize system performance by determining when measurements are required and which parameters to estimate. One possible direction is to integrate sensing control into the TSCH scheduling process [72], allowing higher network layers to allocate measurement opportunities based on node mobility or application demands.

Additionally, IEEE 802.15.4 packet headers could be extended with new configuration fields indicating whether distance, angle, or both should be estimated, along with parameters such as the number of samples, frequency set, or antenna sequence. This flexibility would support real-time optimization of network performance, improved localization accuracy, and enhanced security. Extending these methods beyond TSCH to other IEEE 802.15.4 channel access modes, such as NBE mode with CSMA/CA used in ZigBee and Thread, would further increase applicability but would also require new synchronization mechanisms for channel sensing and likely involve substantial changes to the communication standard.

Security aspects

The integration of localization into communication protocols introduces new procedures and workflows that raise novel security and privacy concerns [73]. Resistance to eavesdropping is crucial so that adversaries cannot infer positions from transmissions. MCPD ranging

provides partial protection because the initial phase offsets introduce randomness in the emitted signal. Since distance estimation depends on measurements from both nodes, the MCPD technique is more secure than AoA estimation, where a nearby receiver can tune to the transmitted CW tone and simply extract the emitter's direction. However, the use of predefined and constant frequency patterns in MCPD still exposes the system to spectral analysis scanning, allowing an observer to identify active nodes or infer relative movement from Doppler analysis.

Replay and relay attacks remain a concern, as captured signals can be retransmitted with modified delay or phase, creating false locations estimations. This issue has already been demonstrated for MCPD-based systems [74]. Spoofing poses another threat, where an attacker forges signals that mimic legitimate transmissions, resulting in manipulated distance or angle estimates. For example in AoA estimation, an attacker equipped with a directional antenna could inject a strong signal component that steers the estimated direction. Jamming also represents a vulnerability, where an adversary transmits strong noise or occupies the defined channels used for ranging, corrupting measurements and preventing localization. Although our evaluation included an interference test for a single channel, future research should assess the resilience of the system when multiple communication channels are simultaneously jammed or distorted. The range of potential attacks demonstrates the need for novel countermeasures, including physical-layer authentication, signal integrity verification, and anomaly detection to improve the resilience and trustworthiness of ISAC systems.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 28, 2010, ISSN: 1389-1286. DOI: 10.1016/j.comnet.2010.05.010.

[2] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: A survey", *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, Aug. 1, 2018, ISSN: 2352-8648. DOI: 10.1016/j.dcan.2017.10.002.

[3] J. Zhang and D. Tao, "Empowering Things With Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things", *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7789–7817, May 2021, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3039359.

[4] F. Zafari, A. Gkelias, and K. K. Leung, "A Survey of Indoor Localization Systems and Technologies", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2568–2599, Aut. 2019, ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2019.2911558.

[5] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, "A Survey of Localization Systems in Internet of Things", *Mobile Networks and Applications*, vol. 24, no. 3, pp. 761–785, Jun. 1, 2019, ISSN: 1572-8153. DOI: 10.1007/s11036-018-1090-3.

[6] T. Savić, X. Vilajosana, and T. Watteyne, "Constrained Localization: A Survey", *IEEE Access*, vol. 10, pp. 49 297–49 321, 2022, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3171859.

[7] S. Ghorpade, M. Zennaro, and B. Chaudhari, "Survey of Localization for Internet of Things Nodes: Approaches, Challenges and Open Issues", *Future Internet*, vol. 13, no. 8, p. 210, Aug. 2021, ISSN: 1999-5903. DOI: 10.3390/fi13080210.

[8] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating Sensing and Communications for Ubiquitous IoT: Applications, Trends, and Challenges", *IEEE Network*, vol. 35, no. 5, pp. 158–167, Sep. 2021, ISSN: 1558-156X. DOI: 10.1109/MNET.010.2100152.

[9] A. Liu, Z. Huang, M. Li, Y. Wan, W. Li, T. X. Han, C. Liu, R. Du, D. K. P. Tan, J. Lu, Y. Shen, F. Colone, and K. Chetty, "A Survey on Fundamental Limits of Integrated Sensing and Communication", *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 994–1034, 2022, ISSN: 1553-877X. DOI: 10.1109/COMST.2022.3149272.

[10] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling Joint Communication and Radar Sensing in Mobile Networks—A Survey", *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 306–345, 2022, ISSN: 1553-877X. DOI: 10.1109/COMST.2021.3122519.

[11] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint Radar and Communication Design: Applications, State-of-the-Art, and the Road Ahead", *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020, ISSN: 1558-0857. DOI: 10.1109/TCOMM.2020.2973976.

[12] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond", *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 6, pp. 1728–1767, Jun. 2022, ISSN: 1558-0008. DOI: 10.1109/JSAC.2022.3156632.

[13] Z. Wei, H. Qu, Y. Wang, X. Yuan, H. Wu, Y. Du, K. Han, N. Zhang, and Z. Feng, "Integrated Sensing and Communication Signals Toward 5G-A and 6G: A Survey", *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11 068–11 092, Jul. 2023, ISSN: 2327-4662. DOI: 10.1109/JIOT.2023.3235618.

[14] T. Wild, V. Braun, and H. Viswanathan, "Joint Design of Communication and Sensing for Beyond 5G and 6G Systems", *IEEE Access*, vol. 9, pp. 30 845–30 857, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3059488.

[15] B. Chang, W. Tang, X. Yan, X. Tong, and Z. Chen, "Integrated Scheduling of Sensing, Communication, and Control for mmWave/THz Communications in Cellular Connected UAV Networks", *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 7, pp. 2103–2113, Jul. 2022, ISSN: 1558-0008. DOI: 10.1109/JSAC.2022.3157366.

[16] S. Helwa, J. P. Van Marter, S. N. Shoudha, M. Ben-Shachar, Y. Alpert, A. G. Dabak, M. Torlak, and N. Al-Dhahir, "Bridging the Performance Gap Between Two-Way and One-Way CSI-Based 5 GHz WiFi Ranging", *IEEE Access*, vol. 11, pp. 70 023–70 039, 2023, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3287850.

[17] S. Lu, F. Liu, Y. Li, K. Zhang, H. Huang, J. Zou, X. Li, Y. Dong, F. Dong, J. Zhu, Y. Xiong, W. Yuan, Y. Cui, and L. Hanzo, "Integrated Sensing and Communications: Recent Advances and Ten Open Challenges", *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 094–19 120, Jun. 2024, ISSN: 2327-4662. DOI: 10.1109/JIOT.2024.3361173.

[18] J. Wang, N. Varshney, C. Gentile, S. Blandino, J. Chuang, and N. Golmie, "Integrated Sensing and Communication: Enabling Techniques, Applications, Tools and Data Sets, Standardization, and Future Directions", *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23 416–23 440, Dec. 2022, ISSN: 2327-4662. DOI: 10.1109/JIOT.2022.3190845.

[19] K. Qu, J. Ye, X. Li, and S. Guo, "Privacy and Security in Ubiquitous Integrated Sensing and Communication: Threats, Challenges and Future Directions", *IEEE Internet of Things Magazine*, vol. 7, no. 4, pp. 52–58, Jul. 2024, ISSN: 2576-3199. DOI: 10.1109/IOTM.001.2300180.

[20] P. S. Farahsari, A. Farahzadi, J. Rezazadeh, and A. Bagheri, "A Survey on Indoor Positioning Systems for IoT-Based Applications", *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7680–7699, May 15, 2022, ISSN: 2327-4662, 2372-2541. DOI: 10.1109/JIOT.2022.3149048.

[21] ITU-R. "Recommendation ITU-R M.2160-0: Framework and overall objectives of the future development of IMT for 2030 and beyond (IMT-2030)," ITU. (Nov. 2023), [Online]. Available: https://www.itu.int:443/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/pages/default.aspx (visited on 04/22/2025).

[22] 3GPP. “TS 22.137: Integrated Sensing and Communication.” (Apr. 2024), [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4198 (visited on 04/23/2025).

[23] E. ISG-ISAC. “Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios.” (), [Online]. Available: https://www.etsi.org/deliver/etsi_gr/ISC/001_099/001/01.01.01_60/gr_ISC001v010101p.pdf (visited on 04/22/2025).

[24] S. Sadowski and P. Spachos, "RSSI-Based Indoor Localization With the Internet of Things", *IEEE Access*, vol. 6, pp. 30 149–30 161, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2843325.

[25] M. Abbas, M. Elhamshary, H. Rizk, M. Torki, and M. Youssef, "WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning", in *2019 IEEE International Conference on Pervasive Computing and Communications (PerCom*, Mar. 2019, pp. 1–10. DOI: 10.1109/PERCOM.2019.8767421.

[26] P. Picazo-Martínez, C. Barroso-Fernández, J. Martín-Pérez, M. Groshev, and A. de la Oliva, "IEEE 802.11az Indoor Positioning with mmWave", *IEEE Communications Magazine*, vol. 62, no. 10, pp. 126–131, Oct. 2024, ISSN: 1558-1896. DOI: 10.1109/MCOM.001.2300454.

[27] J. P. Van Marter, M. Ben-Shachar, Y. Alpert, A. G. Dabak, N. Al-Dhahir, and M. Torlak, "A Multichannel Approach and Testbed for Centimeter-Level WiFi Ranging", *IEEE Journal of Indoor and Seamless Positioning and Navigation*, vol. 2, pp. 76–91, 2024, ISSN: 2832-7322. DOI: 10.1109/JISPIN.2024.3366850.

[28] R. Du, H. Xie, M. Hu, Narengerile, Y. Xin, S. McCann, M. Montemurro, T. X. Han, and J. Xu. “An Overview on IEEE 802.11bf: WLAN Sensing.” arXiv: 2207.04859 [cs]. (Jul. 11, 2022), pre-published.

[29] A. Alarifi, A. Al-Salman, M. Alsaleh, A. Alnafessah, S. Al-Hadhrami, M. A. Al-Ammar, and H. S. Al-Khalifa, "Ultra Wideband Indoor Positioning Technologies: Analysis and Recent Advances", *Sensors*, vol. 16, no. 5, p. 707, 5 May 2016, ISSN: 1424-8220. DOI: 10.3390/s16050707.

[30] K. Bregar and M. Mohorčič, "Improving Indoor Localization Using Convolutional Neural Networks on Computationally Restricted Devices", *IEEE Access*, vol. 6, pp. 17 429–17 441, 2018, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2817800.

[31] J. Zhang, P. V. Orlik, Z. Sahinoglu, A. F. Molisch, and P. Kinney, "UWB Systems for Wireless Sensor Networks", *Proceedings of the IEEE*, vol. 97, no. 2, pp. 313–331, Feb. 2009, ISSN: 1558-2256. DOI: 10.1109/JPROC.2008.2008786.

[32] P. Sedlacek, M. Slanina, and P. Masek, "An Overview of the IEEE 802.15.4z Standard its Comparison and to the Existing UWB Standards", in *2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA)*, Apr. 2019, pp. 1–6. DOI: 10.1109/RADIOELEK.2019.8733537.

[33] D. Coppens, A. Shahid, S. Lemey, B. Van Herbruggen, C. Marshall, and E. De Poorter, "An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions", *IEEE Access*, vol. 10, pp. 70 219–70 241, 2022, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3187410.

[34] M. Nikodem, G. Trajnowicz, G. Salvatore de Blasio, and F. Alexis Quesada-Arencibia, "Experimental Evaluation of Multicarrier Phase Difference Localization in Bluetooth Low Energy", *IEEE Sensors Journal*, vol. 25, no. 1, pp. 1548–1560, Jan. 2025, ISSN: 1558-1748. DOI: 10.1109/JSEN.2024.3495030.

[35] M. Cominelli, P. Patras, and F. Gringoli, "Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System", in *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, ser. WiNTECH '19, New York, NY, USA: Association for Computing Machinery, Oct. 4, 2019, pp. 13–20, ISBN: 978-1-4503-6931-2. DOI: 10.1145/3349623.3355475.

[36] A. Simončič, T. Javornik, A. Sešek, and A. Hrovat, "Direction of arrival estimation for BLE: Antenna array design and evaluation", *AEU - International Journal of Electronics and Communications*, vol. 168, p. 154 722, Aug. 1, 2023, ISSN: 1434-8411. DOI: 10.1016/j.aeue.2023.154722.

[37] "Bluetooth® Channel Sounding," Bluetooth® Technology Website. (Mar. 20, 2025), [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/channel-sounding/ (visited on 04/21/2025).

[38] P. Boer, J. Romme, J. Govers, and G. Dolmans, "Performance of High-Accuracy Phase-Based Ranging in Multipath Environments", in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, May 2020, pp. 1–5. DOI: 10.1109/VTC2020-Spring48590.2020.9128721.

[39] G. Gardašević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, and M. Radonjić, "The IoT Architectural Framework, Design Issues and Application Domains", *Wireless Personal Communications*, vol. 92, no. 1, pp. 127–148, Jan. 1, 2017, ISSN: 1572-834X. DOI: 10.1007/s11277-016-3842-3.

[40] M. Vučinić, T. Chang, B. Škrbić, E. Kočan, M. Pejanović-Djurišić, and T. Watteyne, "Key Performance Indicators of the Reference 6TiSCH Implementation in Internet-of-Things Scenarios", *IEEE Access*, vol. 8, pp. 79 147–79 157, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2990278.

[41] K. EL GHOLAMI, M. Yassine, and F. Imade Fahd Eddine, "The IEEE 802.15.4 Standard in Industrial Applications: A Survey", *Journal of Theoretical and Applied Information Technology*, vol. 99, Aug. 1, 2021.

[42] L. Alkama and L. Bouallouche-Medjkoune, "IEEE 802.15.4 historical revolution versions: A survey", *Computing*, vol. 103, no. 1, pp. 99–131, Jan. 1, 2021, ISSN: 1436-5057. DOI: 10.1007/s00607-020-00844-3.

[43] D. De Guglielmo, S. Brienza, and G. Anastasi, "IEEE 802.15.4e: A survey", *Computer Communications*, vol. 88, pp. 1–24, Aug. 15, 2016, ISSN: 0140-3664. DOI: 10.1016/j.comcom.2016.05.004.

[44] H. Kurunathan, R. Severino, A. Koubaa, and E. Tovar, "IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation", *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1989–2010, Aut. 2018, ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2018.2800898.

[45] D. Chen, M. Nixon, S. Han, A. K. Mok, and X. Zhu, "WirelessHART and IEEE 802.15.4e", in *2014 IEEE International Conference on Industrial Technology (ICIT)*, Feb. 2014, pp. 760–765. DOI: 10.1109/ICIT.2014.6895027.

[46] T. P. Raptis, A. Passarella, and M. Conti, "A Survey on Industrial Internet With ISA100 Wireless", *IEEE Access*, vol. 8, pp. 157 177–157 196, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3019665.

[47] Milica Lekic, Gordana Gardasevic, and Milan Mladen, "Experimental evaluation of multi-PHY 6TiSCH networks", *ITU Journal on Future and Evolving Technologies*, vol. 3, no. 2, pp. 470–482, Sep. 30, 2022, ISSN: 2616-8375. DOI: 10.52953/CGHE6909.

[48] S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay, "Towards the Implementation of IoT for Environmental Condition Monitoring in Homes", *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3846–3853, Oct. 2013, ISSN: 1558-1748. DOI: 10.1109/JSEN.2013.2263379.

[49] R. Herrero, "ThreadThreadArchitecture," in *Fundamentals of IoT Communication Technologies*, R. Herrero, Ed., Cham: Springer International Publishing, 2022, pp. 213–225, ISBN: 978-3-030-70080-5. DOI: 10.1007/978-3-030-70080-5_9.

[50] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, and P. Thubert, "IETF 6TiSCH: A Tutorial", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 595–615, 2020, ISSN: 1553-877X. DOI: 10.1109/COMST.2019.2939407.

[51] V. Bianchi, P. Ciampolini, and I. De Munari, "RSSI-Based Indoor Localization and Identification for ZigBee Wireless Sensor Networks in Smart Homes", *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 2, pp. 566–575, Feb. 2019, ISSN: 1557-9662. DOI: 10.1109/TIM.2018.2851675.

[52] H. S. Fahama, K. Ansari-Asl, Y. S. Kavian, and M. N. Soorki, "An Experimental Comparison of RSSI-Based Indoor Localization Techniques Using ZigBee Technology", *IEEE Access*, vol. 11, pp. 87 985–87 996, 2023, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3305396.

[53] D. Yan, B. Kang, H. Zhong, and R. Wang, "Research on positioning system based on Zigbee communication", in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Oct. 2018, pp. 1027–1030. DOI: 10.1109/IAEAC.2018.8577263.

[54] A. Booranawong, K. Sengchuai, D. Buranapanichkit, N. Jindapetch, and H. Saito, "RSSI-Based Indoor Localization Using Multi-Lateration With Zone Selection and Virtual Position-Based Compensation Methods", *IEEE Access*, vol. 9, pp. 46 223–46 239, 2021, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3068295.

[55] B. Thorbjornsen, N. M. White, A. D. Brown, and J. S. Reeve, "Radio frequency (RF) time-of-flight ranging for wireless sensor networks", *Measurement Science and Technology*, vol. 21, no. 3, p. 035 202, Jan. 2010, ISSN: 0957-0233. DOI: 10.1088/0957-0233/21/3/035202.

[56] S. Lanzisera, D. Zats, and K. S. J. Pister, "Radio Frequency Time-of-Flight Distance Measurement for Low-Cost Wireless Sensor Localization", *IEEE Sensors Journal*, vol. 11, no. 3, pp. 837–845, Mar. 2011, ISSN: 1558-1748. DOI: 10.1109/JSEN.2010.2072496.

[57] M. D. Bedford and G. A. Kennedy, "Evaluation of ZigBee (IEEE 802.15.4) Time-of-Flight-Based Distance Measurement for Application in Emergency Underground Navigation", *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 5, pp. 2502–2510, May 2012, ISSN: 1558-2221. DOI: 10.1109/TAP.2012.2189731.

[58] M. Pelka, C. Bollmeyer, and H. Hellbrück, "Accurate radio distance estimation by phase measurements with multiple frequencies", in *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, Oct. 2014, pp. 142–151. DOI: 10.1109/IPIN.2014.7275478.

[59] G. von Zengen, Y. Schröder, S. Rottmann, F. Büsching, and L. C. Wolf, "No-cost distance estimation using standard WSN radios", in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, Apr. 2016, pp. 1–9. DOI: 10.1109/INFOCOM.2016.7524540.

[60] M. Gunia, A. Zinke, N. Joram, and F. Ellinger, "Setting up a phase-based positioning system using off-the-shelf components", in *2017 14th Workshop on Positioning, Navigation and Communications (WPNC)*, Oct. 2017, pp. 1–6. DOI: 10.1109/WPNC.2017.8250065.

[61] Y. Schröder and L. Wolf, "InPhase: Phase-based Ranging and Localization", *ACM Transactions on Sensor Networks*, vol. 18, no. 2, pp. 1–39, May 31, 2022, ISSN: 1550-4859, 1550-4867. DOI: 10.1145/3494542.

[62] T. Šolc, C. Fortuna, and M. Mohorčič, "Low-Cost Testbed Development and Its Applications in Cognitive Radio Prototyping," in *Cognitive Radio and Networking for Heterogeneous Wireless Networks: Recent Advances and Visions for the Future*, M.-G. Di Benedetto, A. F. Cattoni, J. Fiorina, F. Bader, and L. De Nardis, Eds., Cham: Springer International Publishing, 2015, pp. 361–405, ISBN: 978-3-319-01718-1. DOI: 10.1007/978-3-319-01718-1_13.

[63] A. Moradbeikie, A. Keshavarz, H. Rostami, S. Paiva, and S. I. Lopes, "A cost-effective LoRaWAN-based IoT localization method using fixed reference nodes and dual-slope path-loss modeling", *Internet of Things*, vol. 24, p. 100 990, Dec. 1, 2023, ISSN: 2542-6605. DOI: 10.1016/j.iot.2023.100990.

[64] H. Jason, B. Christian, and H. Li. "Bluetooth Channel Sounding - A Step Towards 10-cm Ranging Accuracy for Secure Access, Digital Key, and Proximity Services," Bluetooth® Technology Website. (Nov. 30, 2023), [Online]. Available: https://www.bluetooth.com/blog/bluetooth-channel-sounding-a-step-towards-10-cm-ranging-accuracy-for-secure-access-digital-key-and-proximity-services/ (visited on 04/24/2024).

[65] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE)", in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2019, pp. 1–8. DOI: 10.1109/WCNC.2019.8885791.

[66] G. Morano, K. Guan, A. Hrovat, and T. Javornik, "Phase-Based Distance Estimation Integrated With IEEE 802.15.4 TSCH Communication", *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11 460–11 470, Apr. 2024, ISSN: 2327-4662. DOI: 10.1109/JIOT.2023.3330933.

[67] H. Obeidat, W. Shuaieb, O. Obeidat, and R. Abd-Alhameed, "A Review of Indoor Localization Techniques and Wireless Technologies", *Wireless Personal Communications*, vol. 119, no. 1, pp. 289–327, Jul. 1, 2021, ISSN: 1572-834X. DOI: 10.1007/s11277-021-08209-5.

[68] G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol", in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2023, pp. 1–7. DOI: 10.1109/PIMRC56721.2023.10293886.

[69] G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Distance- and Angle-Based Hybrid Localization Integrated in the IEEE 802.15.4 TSCH Communication Protocol", *Sensors*, vol. 24, no. 12, p. 3925, Jan. 2024, ISSN: 1424-8220. DOI: 10.3390/s24123925.

[70] J. Romme, "Method for distance determination," U.S. Patent 10928495B2, Feb. 23, 2021. [Online]. Available: https://patents.google.com/patent/US10928495B2/de (visited on 08/01/2025).

[71] G. Morano, T. Javornik, A. Simončič, A. Švigelj, and A. Hrovat, "Interference Mitigation in One-Way Channel Reconstruction for Robust Phase-Based Ranging", *IEEE Access*, vol. 14, pp. 939–955, 2026, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3649293.

[72] A. Elsts, S. Kim, H.-S. Kim, and C. Kim, "An Empirical Survey of Autonomous Scheduling Methods for TSCH", *IEEE Access*, vol. 8, pp. 67 147–67 165, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2980119.

[73] G. Pettorru, V. Pilloni, and M. Martalò, "Trustworthy Localization in IoT Networks: A Survey of Localization Techniques, Threats, and Mitigation", *Sensors*, vol. 24, no. 7, p. 2214, Jan. 2024, ISSN: 1424-8220. DOI: 10.3390/s24072214.

[74] A. Riaz, D. Nash, J. Ngo, C. Juvekar, P. Nadeau, T. Yu, and R. T. Yazicigil, "Security Assessment of Phase-Based Ranging Systems in a Multipath Environment", *ACM Journal on Emerging Technologies in Computing Systems*, p. 3 517 809, Mar. 23, 2022, ISSN: 1550-4832, 1550-4840. DOI: 10.1145/3517809.

Bibliography

Publications Related to the Thesis

Journal Articles

G. Morano, K. Guan, A. Hrovat, and T. Javornik, "Phase-Based Distance Estimation Integrated With IEEE 802.15.4 TSCH Communication", *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 11 460–11 470, Apr. 2024, ISSN: 2327-4662. DOI: 10.1109/JIOT.2023.3330933.

G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Distance- and Angle-Based Hybrid Localization Integrated in the IEEE 802.15.4 TSCH Communication Protocol", *Sensors*, vol. 24, no. 12, p. 3925, Jan. 2024, ISSN: 1424-8220. DOI: 10.3390/s24123925.

G. Morano, T. Javornik, A. Simončič, A. Švigelj, and A. Hrovat, "Interference Mitigation in One-Way Channel Reconstruction for Robust Phase-Based Ranging", *IEEE Access*, vol. 14, pp. 939–955, 2026, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3649293.

Conference Paper

G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol", in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2023, pp. 1–7. DOI: 10.1109/PIMRC56721.2023.10293886.

Technical Documents

G. Morano, A. Simončič, T. Kocevska, T. Javornik, and A. Hrovat, "Angle of Arrival Estimation Using IEEE 802.15.4 TSCH Protocol", in *COST INTERACT 6th MC and 6th Technical Meeting*, Poznań, Poland, Sep. 11, 2023.

G. Morano, K. Guan, A. Hrovat, and T. Javornik, "Phase-based ranging within TSCH communication", in *COST INTERACT 4th MC and 4th Technical Meeting*, Dubrovnik, Croatia, Jan. 23, 2023.

G. Morano, A. Simončič, T. Javornik, and A. Hrovat, "Single access point localization in TSCH network", in *COST INTERACT 7th MC and 7th Technical Meeting*, Lisbon, Portugal, Jan. 22, 2024.

G. Morano, T. Javornik, A. Simončič, A. Švigelj, and A. Hrovat, "Dynamic CIR Noise Suppression for One-Way CFR Reconstruction", in *COST INTERACT 11th MC and 11th Technical Meeting*, Gothenburg, Sweden, Jun. 16, 2025.

Datasets

G. Morano, A. Hrovat, and T. Javornik, *IEEE 802.15.4 TSCH dataset for phase-based distance estimation*, Zenodo, Dec. 20, 2022. DOI: 10.5281/zenodo.7464319.

G. Morano, A. Simončič, T. Javornik, and A. Hrovat, *Phase Measurements for AoA Estimation in IEEE 802.15.4 TSCH-based Networks*, Zenodo, Oct. 29, 2025. DOI: 10.5281/zenodo.17476028.

G. Morano, A. Simončič, T. Javornik, and A. Hrovat, *Distance and Angle Measurements for Hybrid Localization in IEEE 802.15.4 TSCH Networks*, Zenodo, Oct. 30, 2025. DOI: 10.5281/zenodo.17481601.

G. Morano, A. Simončič, and A. Hrovat, *Two-Way Channel Frequency Response Dataset Obtained with MCPD technique*, Zenodo, Jan. 5, 2026. DOI: 10.5281/zenodo.18153931.

Other Publications

Journal Articles

A. Hrovat, A. Simončič, T. Kocevska, G. Morano, A. Švigelj, and T. Javornik, "Integrated Communications and Sensing in Terahertz Band: A Propagation Channel Perspective", *Journal of Communications Software and Systems*, vol. 20, no. 1, pp. 23–37, Jan. 30, 2024, ISSN: 1846-6079. DOI: 10.24138/jcomss-2023-0174.

G. Morano, A. Hrovat, M. Vučnik, J. Puhan, G. Gardašević, D. Vasiljević, and T. Javornik, "Experiment Control and Monitoring System for LOG-a-TEC Testbed", *Sensors*, vol. 21, no. 19, p. 6422, Jan. 2021, ISSN: 1424-8220. DOI: 10.3390/s21196422.

G. Morano, A. Hrovat, A. Švigelj, J. Velkaverh, P. Žnidaršič, and T. Javornik, "Experimental Performance Evaluation of Cooperative Localization in Indoor Environment", *IEEE Sensors Journal*, vol. 25, no. 23, pp. 43 426–43 445, Dec. 2025, ISSN: 1558-1748. DOI: 10.1109/JSEN.2025.3620118.

A. Simončič, G. Morano, A. Hrovat, and T. Javornik, "Optimizing Frequency Switching Pattern to Reduce Asynchronization Effect in MCPD Ranging Systems", *IEEE Access*, vol. 13, pp. 169 791–169 811, 2025, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2025.3614753.

A. Simončič, K. Guan, G. Morano, A. Švigelj, A. Hrovat, T. Kocevska, and T. Javornik, "Experimental Evaluation of Enhanced Antenna Switching for CFO Mitigation in DoA Estimation", *IEEE Open Journal of Antennas and Propagation*, vol. 6, no. 4, pp. 1022–1036, Aug. 2025, ISSN: 2637-6431. DOI: 10.1109/OJAP.2025.3558671.

A. Simončič, G. Morano, A. Hrovat, and T. Javornik, "Mitigating Frequency Dependent Carrier Frequency Offset in Multi-carrier Phase Difference Ranging through Timing Diagram Design", *IEEE Access*, pp. 1–1, 2026, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2026.3665049.

Book Chapters

A. Arous, G. Morano, T. Javornik, Z. Cui, *et al.*, "COST action INTERACT WG2 whitepaper," COST CA20120 INTERACT Working Group 2 (Signal Processing and Localisation), White paper, Oct. 15, 2024. [Online]. Available: https://interactca20120.org/wp-content/uploads/2024/10/WG2_Whitepaper_Final.pdf.

G. Morano, A. Švigelj, A. Hrovat, R. Novak, T. Javornik, G. Morano, A. Švigelj, A. Hrovat, R. Novak, and T. Javornik, "System Architecture for Intelligent Environment-Aware Wireless Communications," in *Advances in Digital Transformation - Rise of Ultra-Smart Fully Automated Cyberspace*, IntechOpen, Dec. 15, 2023, ISBN: 978-0-85466-508-2. DOI: 10.5772/intechopen.1003920.

Conference Papers

B. Bertalanič, G. Morano, and G. Cerar, "LOG-a-TEC Testbed outdoor localization using BLE beacons", in *2022 International Balkan Conference on Communications and Networking (BalkanCom)*, Aug. 2022, pp. 115–119. DOI: 10.1109/BalkanCom55633.2022.9900607.

B. Bertalanič, G. Morano, and G. Cerar, "Lokalizacija na prostem s pomočjo radiofrekvenčnih odtisov tehnologije BLE v testnem omrežjem LOG-a-TEC", in *Proceedings of the 31st International Electrotechnical and Computer Science Conference (ERK)*, A. Žemva and A. Trost, Eds., ser. ISSN 2591-0442, Slovenska sekcija IEEE and Fakulteta za elektrotehniko, Sep. 19, 2022, pp. 50–53. [Online]. Available: https://erk.fe.uni-lj.si/2022/erk22.pdf.

T. Javornik, G. Morano, and A. Hrovat, "Merjenje razdalje na osnovi faze sprejetega signala v napravah IoT", in *27th Seminar on Radio Communications SRK 2026*, Založba Fakultete za elektrotehniko, Univerza v Ljubljani, 2026, str. 74–77, ISBN: 978-961-243-485-4. [Online]. Available: https://srk.fe.uni-lj.si/zborniki/ZBORNIK%20SRK%202026.pdf.

T. Kocevska, M. Murko, A. Simončč, G. Morano, T. Javornik, B. Batageljš, and A. Hrovat, "UWB Channel Impulse Response Alignment Techniques for Accurate Indoor Radio Sensing", in *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sep. 2024, pp. 1–6. DOI: 10.23919/SoftCOM62040.2024.10721882.

T. Mlakar, A. Hrovat, A. Simončič, T. Javornik, and G. Morano, "Ocenjevanje oddaljenosti med napravami s pomočjo faze signala in algoritma MUSIC", in *Proceedings of the 33rd International Electrotechnical and Computer Science Conference (ERK)*, A. Žemva and A. Trost, Eds., ser. ISSN 2591-0442, Slovenska sekcija IEEE and Fakulteta za elektrotehniko, Sep. 26, 2024, pp. 61–65. [Online]. Available: https://erk.fe.uni-lj.si/2024/papers/mlakar(ocenjevanje_oddaljenosti).pdf.

G. Morano, A. Simončič, A. Hrovat, and T. Javornik, "Integrated sensing and communication in TSCH networks", in *26th Seminar on Radio Communications SRK 2024*, T. Mlinar and B. Batagelj, Eds., Založba Fakultete za elektrotehniko, Univerza v Ljubljani, 2024, str. 86–87, ISBN: 978-961-243-461-8. [Online]. Available: https://srk.fe.uni-lj.si/zborniki/ZBORNIK%20SRK2024.pdf.

A. Simončič, A. Hrovat, G. Morano, T. Kocevska, and T. Javornik, "Near-field Beam Steering with Planar Antenna Array", in *2024 7th International Balkan Conference on Communications and Networking (BalkanCom)*, Jun. 2024, pp. 31–36. DOI: 10.1109/BalkanCom61808.2024.10557212.

A. Simončič, G. Morano, A. Švigelj, A. Hrovat, and T. Javornik, "Optimizing Switching Pattern to Reduce CFO Effects in Single RF Chain Direction Finding Systems", in *2024 7th International Balkan Conference on Communications and Networking (BalkanCom)*, Jun. 2024, pp. 113–118. DOI: 10.1109/BalkanCom61808.2024.10557208.

A. Simončič, G. Morano, M. Mohorčič, T. Kocevska, M. Mohorčič, and A. Hrovat, "Validation of solution for people tracking and counting using WiFi network messages", in *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Antwerp, Belgium, 2024, pp 69 (1–4).

Technical Documents

A. Jeknić, K. Guan, A. Švigelj, G. Morano, T. Javornik, A. Hrovat, and T. Kocevska, "Evaluation of Bayesian and non-Bayesian Cooperative Localization Algorithms in the Indoor Environment", in *COST INTEERACT 10th MC and 10th Technical Meeting*, Dublin, Ireland, Jan. 27, 2025.

A. Simončič, K. Guan, A. Švigelj, G. Morano, T. Javornik, A. Hrovat, and T. Kocevska, "Performance evaluation of CFO-resilient switching patterns for accurate DoA estimation", in *COST INTEERACT 8th MC and 8th Technical Meeting*, Helsinki, Finland, Jun. 17, 2024.

M. Murko, A. Simončič, A. Hrovat, T. Kocevska, L. Zmrzlak, T. Mlinar, B. Batagelj, T. Javornik, and G. Morano, "Evaluation of cost-effective UWB technology for accurate indoor CIR measurements", in *COST INTERACT 8th MC and 8th Technical Meeting*, Helsinki, Finland, Jun. 17, 2024.

Datasets

T. Kocevska, A. Simončič, G. Morano, T. Javornik, and A. Hrovat, *Channel Measurements from Sitarjevec Mine for Propagation Modelling in a Cave Environment*, Zenodo, Jul. 24, 2024. DOI: 10.5281/zenodo.12804477.

G. Morano, T. Javornik, G. Gardašević, A. Švigelj, and A. Hrovat, *6TiSCH traces in real-world network deployment*, Zenodo, Dec. 22, 2022. DOI: 10.5281/zenodo.7468518.

G. Morano, B. Bertalanič, A. Hrovat, and A. Švigelj, *Outdoor fingerprint localization with BLE beacons*, Zenodo, Dec. 20, 2022. DOI: 10.5281/zenodo.10077872.

Biography

Grega Morano received his bachelor's (2018) and master's (2021) degree from the Faculty of Electrical Engineering of the University of Ljubljana. He completed the "Electronics" master study programme with the thesis titled "Sistem za spremljanje in nadzor brezžičnega testnega omrežja LOG-a-TEC", for which he received the faculty Prešeren award in 2022.

In 2021, he enrolled in the "Communication and Information Technologies" doctoral study programme at Jožef Stefan International Postgraduate School. At the same time, he joined the Communication Technology Laboratory, Department of Communication Systems (E6) at Jožef Stefan Institute as a research assistant. Under the supervision of assoc. prof. dr. Andrej Hrovat and prof. dr. Tomaž Javornik his research work began with the operation and core maintenance of the LOG-a-TEC 3.0 wireless testbed. From there on, he has been specializing in the field of IoT communication protocols and wireless localization, with a focus on integrated sensing and communication (ISAC). His work involves embedded system design, the development of custom wireless sensor platforms, and the implementation of communication protocols suited for resource-constrained systems. He is experienced in developing and deploying experimental wireless testbeds used for evaluation of wireless system performance in real-world scenarios.

Some of his research milestones toward PhD were presented at national (ERK, SRK) and international conferences (PIMRC, BalkanCom, EuCNC). He attended different international training schools and regularly participated in the H2020 COST Interact meetings and workshops. During his research work he has contributed to several ARIS projects (J2-2507, J2-3048 and J2-4461) and H2020 projects (Fed4FIRE+, Resiloc, UpScale and KReATIVE).