UWB Security and Enhancements

K. Reaz¹, Lea Muth¹, Thibaud Ardoin¹, Gerhard Wunder¹, Marian Margraf¹, Mahsa Kholghi¹, Kai Jansen¹, Christian Zenger¹, Julian Schmidt¹, Enrico Köppe¹, Zoran Utkovski¹, Igor Bjelakovic¹, Mathis Schmieder¹, and Olaf Dressel¹

¹Affiliation not available

March 19, 2024
UWB Security and Enhancements

Release 1.0

Freie Universität Berlin\(^1\), PHYSEC GmbH\(^2\), NC Systems GmbH\(^3\), Fraunhofer Heinrich-Hertz Institut\(^4\), Bundesdruckerei GmbH\(^5\)

March 13, 2024

1 Khan Reaz, Lea Muth, Thibaud Ardoin, Gerhard Wunder, Marian Margraf
2 Mahsa Kholghi, Kai Jansen, Christian Zenger
3 Julian Schmidt, Enrico Köppe
4 Zoran Utkovski, Igor Bjelakovic, Mathis Schmieder
5 Olaf Dressel

Abstract

Ultra-Wideband (UWB) technology re-emerges as a groundbreaking ranging technology with its precise micro-location capabilities and robustness. However, the security aspects of UWB technology demand thorough scrutiny due to its widespread use in both consumer and industrial sectors. This white paper highlights the security dimensions of UWB technology, focusing in particular on the intricacies of device fingerprinting for authentication, examined through the lens of state-of-the-art machine learning techniques. Furthermore, we explore various potential enhancements to the UWB standard that could realize a sovereign UWB data network. We argue that UWB data communication holds significant potential in healthcare and ultra-secure environments, where the use of the common unlicensed 2.4 GHz band-centric wireless technology is limited or prohibited. A sovereign UWB network could serve as an alternative, providing secure localization and short-range data communication in such environments.

Contents

1 Introduction 2

2 Known Attack Vectors 2
  2.1 Ghost Peak ................................................................. 2
  2.2 Cicada ................................................................. 3
  2.3 Cicada++ ............................................................. 3
  2.4 Early Detect/Late Commit Attack ........................................ 4
  2.5 Adaptive Injection Attack ................................................ 4
  2.6 Relay Attack .......................................................... 5
  2.7 Distance Enlargement Attack .......................................... 5
  2.8 Mix-Down Attack ...................................................... 6
  2.9 Strech-and-Advance Attack .......................................... 6
  2.10 Signal Jamming ...................................................... 6

3 Extending UWB Security by Physical Layer Information 8
  3.1 Device Fingerprinting from Channel Impulse Response .................. 8
  3.2 Sovereign UWB Data Network ........................................ 10
  3.3 Countermeasures to Secure ToA-based Ranging ....................... 11
  3.4 Spatial Characterization Through Secrecy Maps ..................... 11

4 Conclusion 13
1 Introduction

The unprecedented resurgence of Ultra-Wideband (UWB) technology in consumer electronic devices is attributed to its unparalleled accuracy in indoor tracking, minimal interference with other wireless technologies, and low cost. As outlined by the FiRa Consortium [5], UWB possesses huge potential to become the de facto standard for providing precision secure ranging and proximity authentication. Among its many potential use cases, UWB’s distinctive features are particularly well-suited to the requirements of hospital settings, focusing on ensuring patient safety, operational efficiency, and the dependability of medical equipment and communications. One exemplary application is asset tracking and access control. Keeping track of medical equipment, such as portable monitors, infusion pumps, wheelchairs, and other valuable assets, is crucial in hospitals or nursing homes. In this system, UWB tags are affixed to different pieces of equipment. These tags communicate with UWB anchors installed throughout the facility, providing precise location data for each tagged item. This information is then integrated into the hospital’s digital management system. Beyond asset tracking and access control, the data exchange capability of UWB technology presents an attractive opportunity. This involves interconnecting potential equipment in a peer-to-peer and peer-to-mesh topology, allowing them to exchange small amount of data.

Standards such as the one from FiRa, Car Connectivity Consortium (CCC), and Omlox primarily consider the secure ranging aspect of the UWB technology but leave out its data communication capabilities. A large volume of current UWB related literature is primarily focusing on achieving ranging accuracy, faster refresh rate, while being efficient for a mobile tag. The data communication aspects of the UWB nodes, however, remain less explored or simply ignored. From our perspective, data communication over the UWB interface has potential in healthcare sectors, special industrial facilities, and ultra-secure governmental premises, where the security guarantee provided by UWB technology may outweigh its energy aspects. In these locations, the use of common unlicensed 2.4/Sub-GHz band-centric wireless technology is restrictive. UWB could serve as an alternative, offering secure localization and short-range data communication in such environments.

In this document, we take a closer look at where UWB technology stands today, especially in terms of security, and pointed out what’s missing in the current standards. We have suggested several improvements to make UWB more secure and useful. For instance, we are bringing in machine learning to help recognize devices more accurately with the physical layer information, which omits the necessity of out-of-band or certificate based authentication. We have also designed a new Medium Access Control (MAC) protocol for UWB devices to communicate with each other in a mesh network, making the network more flexible, resilient and scalable. Additionally, we have introduced the concept of Secrecy Maps, a tool that makes it possible to determine the data leakage quantitatively in a statistical manner and visualize it spatially under different channel conditions. In this sense, Secrecy Maps can serve both as a basis for immediate countermeasures in the event of security deficits, and as a basis for network planning. Together, our proposed enhancements are aimed to solidify UWB as a secure, reliable technology.

Acknowledgment: This work is part of “Sicherheitsarchitektur für eine UWB-basierte IoT-Anwendungsplattform (UltraSec)” project, funded by the German Federal Ministry of Education and Research (BMBF).

2 Known Attack Vectors

2.1 Ghost Peak

The Ghost Peak attack reported in [15] exposes a critical vulnerability in UWB-ranging systems, particularly in HRP UWB implementations, by exploiting the physical layer’s security limitations. There are two variants of the attack: either the Initiator or the Responder can be attacked. The authors include an extensive experimental
2.2 Cicada evaluation, demonstrating the attack’s effectiveness on real devices. The attack caused distance reductions ranging from approximately 2 meters to over 12 meters, with varying success rates depending on the specific device pairing and attack configuration.

**Attack mechanism:** The Ghost Peak attack employs a *selective overshadowing technique*. This involves transmitting signal pulses at specific power levels to overshadow legitimate signals partially. The attacker sends these pulses at a higher power to overshadow the legitimate signal, creating a scenario where the noise is misclassified as an early copy of the signal. The power of the transmitted signal is carefully adjusted based on the relative distance between devices. The power is lowered to avoid being detected as jamming, especially when the attacker’s device is far from the victim’s device. The attack specifically targets packets in Double-Sided Two-Way Ranging (DS-TWR) systems, which are commonly used in HRP UWB configurations. This method involves manipulating the timing of packet reception to reduce the measured distance.

**Countermeasures:** The suggested countermeasures include advanced signal analysis techniques and reducing the maximum accepted difference between Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) signal paths [15].

2.2 Cicada

Fig. 2: Cicada Attack - Overlay of the original signal and the imitated, cicada-shaped signal (Source: [18]).

The Cicada attack [18] is a specific type of security threat targeting UWB systems. The attack is a proximity-shortening attack designed to manipulate the distance measurements that are critical to the functionality of UWB technology. UWB systems use Time-of-Flight (ToF) measurements to determine the distance between individual devices by measuring the duration of signal transmissions between devices. The Cicada attack can be challenging to detect as it does not necessarily affect the regular function of the UWB system but merely corrupts the distance measurements.

**Attack mechanism:** Under the Cicada attack, a series of additional pulses imitating the rhythm of Cicada sounds are transmitted and superimposed onto the legitimate UWB signal. The additional signals interfere with the receiver’s ability to measure the arrival time of the legitimate signal accurately. As a result of this interference, the receiver miscalculates the ToF, underestimating the actual distance between the transmitter and receiver.

**Countermeasures:** The authors [18] propose the abandonment of fine synchronization, where the estimation of ToA is based solely on the strongest multipath component. The use of a time-hopping preamble is suggested to avoid the periodicity exploited by the Cicada attack. According to the authors, the periodicity of the Cicada signal could also be detected and filtered out using the Fourier transform.

2.3 Cicada++

Fig. 3: Cicada Attack++: The benign transmitter sends a signal (top). The adversary sends random pulses at a multiple of the PRF of the legitimate STS (bottom) (Source: [25]).
The Cicada++ attack [25], based on the principles of the original Cicada attack, is an advanced and more sophisticated method of compromising UWB systems. While the Cicada attack focuses on interfering with UWB signals to alter distance measurements, Cicada++ takes this a step further with more refined techniques.

**Attack mechanism:** Injecting more complex pulse patterns that are multiple times stronger than the legitimate signal and sending them at a fraction of the repetition frequency effectively mimics the legitimate signals to fool the system into estimating it as the highest correlation peak. This is achieved through better synchronization with the legitimate UWB signal compared to the original Cicada attack.

**Countermeasures:** The authors point out that the system can increase its robustness against attacks such as Cicada++ by cleverly adjusting the receiver’s parameters, such as the maximum peak-to-early peak ratio and the peak-to-average power ratio [25].

### 2.4 Early Detect/Late Commit Attack

Flury et al. and Singh et al. described an “Early Detection/Late Commit”-attack (ED/LC-attack) against UWB systems that utilizes distance bounding for secure distance measurement in order to determine the estimated distance by the time of arrival of a packet [9, 25]. An attacker can launch an ED/LC-attack to perform distance bounding. This attack exploits the predictability of the (internal) signal structure of a symbol, whereby the attacker learns the values of the packet/symbol early and transmits them late in order to deceive the receivers about the arrival time of the signal.

**Attack mechanism:** In the early detection phase, the attacker identifies the entire symbol using only the initial part. In the late commit phase, the attacker forges the symbol such that the small initial part of the symbol is non-committal. In contrast, the last part of the symbol is sufficient to generate correct data during demodulation in the receiver. This enables an attacker to initiate the transmission of a symbol prior to knowing what exact data the sender’s symbol encapsulates, thereby advancing the measured arrival time of the symbol by a desired time.

**Countermeasures:** The two papers discuss countermeasures against the ED/LC-attack. In the context of secure ranging using the IEEE 802.15.4z HRP mode, Singh et al. proposed to develop HRP-capable receivers that can accurately detect the first occurrence of the STS while also being resistant to external interference and multipath fading [25]. Critical components of this approach include peak detection thresholds, noise level estimation, and leading edge detection to ensure accurate ToA measurements and reduce the risk of ED/LC attacks. Flury et al. suggested to reduce the payload symbol duration since the distance-reducing attack cannot reduce the distance by more than one symbol duration [9].

### 2.5 Adaptive Injection Attack

Singh et al. presented the Adaptive Injection Attack as a method that introduces fine-grained control over the position of the injected peak, in which an attacker controls the position of an injected peak a few nanoseconds earlier in the signal to manipulate the range estimation. This attack relies on the attacker’s ability to relay or block the legitimate signal and adjust the power and timing of the transmitted signal to create a spike in the receiver’s signal processing that misrepresents the actual distance. This attack introduces a significant challenge to securing UWB ToF distance measurements, especially in systems such as IEEE 802.15.4z HRP UWB that rely on the integrity of these measurements for applications such as secure ranging and positioning [25].

**Attack mechanism:** An attacker initially monitors the target receiver to understand its signal processing behavior and any protective measures. Based on this understanding, the attacker starts to inject signals into the receiver’s signal path. Those signals are designed to interfere with the receiver’s regular processing. If the receiver adapts its processing to counter the interference, the attacker adapts by changing the characteristics of the injected signals.

**Countermeasures:** Singh et al. suggested the backward search time window technique, requiring the receiver to carefully manage the backward search time window to account for peaks that could represent the direct path signal. Furthermore, they suggested leading edge detection, whereby the receiver design must provide accurate detection of the leading edge of the Scramble Timestamp Sequence (STS) [25].
2.6 Relay Attack

A Relay Attack [11, 10, 24] is a type of security breach targeting communication systems, especially those relying on proximity security measures, such as passive keyless entry and start systems (PKES) in modern cars or contactless card readers. In this attack, the attacker uses devices that relay signals between a target system and the key or card. The attack makes the target system believe that the key/card is physically closer than it actually is, enabling the attacker to unlock and gain access to the target system without physical access to the key/card. This kind of attack is effective even if the key/card is located far away from the target system and does not require the key/card’s encryption or authentication mechanisms to be compromised. Relay attacks can be carried out with relatively inexpensive and straightforward equipment and make PKES systems vulnerable regardless of their cryptographic strength.

**Attack mechanism:** The attack is typically carried out using two devices, one located close to the legitimate key or card (transmitter) and the other near the target system (receiver). The sender device intercepts the signal from the key/card and forwards it to the receiver device, which then transmits it to the target system. The target system receives the forwarded signal and assumes that the key or card is nearby, granting access or authorization.

**Countermeasures:** Francillon et al. [10] proposed shielding the key/card and removing its battery to deactivate wireless communication. Furthermore, they suggested software or hardware changes as well as the use of signal strength or multi-channel communication. In addition, they proposed a new PKES system based on radio frequency distance limitation to verify the physical proximity of the key to the car securely. Singh et al. [24] presented the “UWB with Pulse Reordering” (UWB-PR) method to secure distance measurements in UWB systems against relay and physical layer attacks. They introduce the UWB-PR modulation scheme, securing distance measurement without performance degradation by applying pulse reordering and cryptographic pulse fading. Their approach prevents attackers from manipulating the measured distance by confusing the pulse train associated with each bit, thus increasing the security of UWB systems against such attacks.

2.7 Distance Enlargement Attack

In the Distance Enlargement attack [23], an attacker delays authentic signals exchanged between devices in a positioning system and replays them. By doing so, the receiver cannot recognize the authentic signal and, hence, cannot use its arrival time for distance measurement. In order to perform this attack, the attacker does not need to break any cryptographic security or compromise the upper-layer protocols.

**Attack mechanism:** The attack is carried out by first intercepting or receiving the authentic signals transmitted between the devices. The attacker distorts the authentic signals to prevent the receiver from identifying them and using their ToA for accurate ranging. After manipulating the original signals, the attacker replays these signals with a delay added. The added delay is proportional to the additional distance the attacker wants to fabricate.

**Countermeasures:** Singh et al. presented a novel approach, called Ultra-Wideband Enlargement Detection (UWB-ED), to counteract distance-enlargement attacks [23]. This technique is based on the encapsulation of pulses with different phases and the inclusion of blank pulse slots. This approach makes it difficult for an attacker to predict the pulse phase, reducing the likelihood of successful signal cancellation or manipulation.
2.8 Mix-Down Attack

The Mixed-Down (MD) attack [2] is a novel threat to UWB and targets the Single-Sided Two-Way Ranging (SS-TWR) of the present standard. The attack exploits flaws in the transmitter clock synchronization to produce an error and, therefore, to manipulate the distance measurements between two UWB devices and reduce the measured distance.

**Fig. 5: Mix-Down Attack** - The attacker intercepts the responder’s signal. Instead of returning the signal directly to the initiator, the attacker applies a mix-down process that shifts the frequency of the response signal (Source: [2]).

**Attack mechanism:** The attacker’s device intercepts the responder’s reply and modifies the frequency of the signal to represent the required clock drift. This mix-down process is demonstrated by converting a high-frequency wave into a low-frequency wave. The attacker then transmits the modified signal to the initiator again. The purpose of this manipulation is to simulate a condition in which the receiver’s clock does not run faster but slower, effectively causing a negative clock drift. Resulting in the initiator observing a reduced round-trip time of the signal and, therefore, measuring a shorter distance than the actual distance between the devices.

**Countermeasures:** As a countermeasure, Singh et al. suggested using a Double-Sided Two-Way Ranging as a configuration within the standard instead of Single-Sided Two-way Ranging [23].

2.9 Strech-and-Advance Attack

For the sake of completeness, the following theoretical attack upon the draft of the new 802.15.4.ab standard is also included. The Strech-and-Advance attack (S&A) is a potential attack for which no hardware implementation yet exists.

**Attack mechanism:** During this theoretical attack, a manipulated distance message will be injected, which appears to come from a legitimate sender with a slowed clock. This manipulation causes the message to be stretched in time and received earlier than legitimate signals, misleading the receiver into assuming a reduced distance between the respective devices. Thus, the attacker gains enough time to capture and replay unknown parts of the message, ensuring that the receiver recognizes the manipulated message as a legitimate one. As a result, the measured distance is reduced, and the integrity of the UWB distance measurement is undermined.

**Countermeasures:** A proposed countermeasure to mitigate the S&A attack by [23] is to ensure consistent clock drift estimates between two devices. Usually, the clock drift of one device, being measured by another, leads to a corresponding adjustment in the reporting. Meanwhile, the S&A attack leads to a significant deviation in this process. By establishing a specific bit error rate threshold, the countermeasure can effectively prevent the S&A attack. This method thus ensures that any attack to reduce the S&A distance reduction attack is limited to an arbitrarily low probability of success.

2.10 Signal Jamming

UWB is considered highly resistant to jamming due to its very short pulses spread across a wide spectrum of frequencies. The utilization of UWB technology [17] further enhances its robustness, making it a preferred
choice in various military systems as an effective countermeasure against jamming.

To assess the jamming resistance claim, we conducted tests on a Qorvo’s 3001CDK development kit [19], which is capable of operating on channel 5 and 9 of UWB, and offers a choice of 32 different preamble codes. Essentially, it should be possible to demonstrate our test with any other standardized UWB module.

**Experiment Procedure:** The evaluation board was configured with specific parameters for the channel, including encryption using STS (Scrambled Timestamp Sequence). Notably, the attacker was assumed to possess no prior knowledge about the channel, apart from knowing which channel communication was ongoing. The objective was to observe the effect of varying distances and the density of devices on the success of the jamming attack. It is crucial to note that jamming packets were continuously sent without any delay, simulating a scenario where the channel is constantly disturbed. Despite not having access to the key used for STS communications, the attacker aimed to interfere with authenticated signals. Initially, the transmitter and receiver are positioned in 1 meter apart. Subsequently, we systematically increase the number of jammers and the distance between the jammer and the receiver in the subsequent scenarios.

![Impact of Jammer Density on Loss](image)

**Fig. 6:** Effect of jammer Devices Quantity on Receiver Packet Loss

**Results:** Figure 6 demonstrates that utilizing 5 jammers significantly increases packet loss compared to employing only 1 jamming device. However, the disparity between employing 5 and 10 jammers is no longer recognizable. This observation provides valuable insight into the impact of the number of jamming devices employed.

![Packets Loss Across Varying Distances](image)

**Fig. 7:** Both figures illustrate packet loss at various distances.

Now, we focus on examining the effects of varying distances on jamming and packet loss. Figure 7 shows a distinct and significant rise in packet loss occurring once the distance reaches 8 meters. At this point, approximately 70% of transmitted packets fail to reach their destination. Consequently, the re-transmission process introduces delays in communication.

Our experiments demonstrate that jamming the UWB signals is indeed possible. The success of this attack lies in interference pulses disrupting the preamble field of the legitimate packet, making it difficult for the receiver to accurately detect the correct preamble for synchronization or localization, potentially causing dropouts of packets.
Such jamming attacks can have a significant impact, especially in critical scenarios like ranging applications. For example, if the attacker jams the channel by 90%, it could lead to inaccurate ranging measurements and system response delays. This underscores the importance of robust security measures in UWB communication systems to mitigate the potential risks posed by jamming attacks.

3 Extending UWB Security by Physical Layer Information

3.1 Device Fingerprinting from Channel Impulse Response

Radio Frequency Fingerprinting (RFF) is a type of signal intelligence applied within the radio frequency domain. It involves a technique that identifies a unique signature from the hardware transmitting the signal. This unique identification results from the unintentional variations introduced during the fabrication process of different physical components resulting in slight changes in the signal’s waveform without altering the intended transmitted data. Precisely, we use the following definition of the fingerprint [30]:

- **Differentiable**: Each device has a unique fingerprint that can be distinguished from those of other devices.
- **Relative stability**: The unique feature should remain as stable as possible over time, despite environmental changes.
- **Hardware**: The sole independent source of the fingerprint is the condition of the hardware. Any other impact on the waveform, such as interference, temperature, time, position, orientation, or implementation, is considered a bias.

Once RFF features are extracted from the signal, they can be used as a unique identifier for a particular device. Since this fingerprint is rooted in the hardware, and derived from the raw signal shape, it is inherently challenging to mask or spoof. Therefore, RFF has the potential to become a key element of physical layer security, offering a robust method for **Device Authentication**.

Most studies demonstrating successful device classification via RFF focus on commonly utilized radio technologies, such as Wi-Fi, 5G, or Bluetooth [13]. To the best of our knowledge, there has been no research conducted on RFF for UWB signals thus far. Two technical aspects could add challenges to the RFF detection in the case of UWB signal. First, UWB technology transmits pulses, resulting in shorter duty cycles compared to the continuous transmission seen in other technologies. This leads to fewer available features in the signal for fingerprint detection. Second, the main advantage of UWB technology is its position sensitivity, rendering it advantageous for numerous applications. Nevertheless, this characteristic can introduce strong variations in the signal when the position changes, which ultimately hampers the learning of consistent features across diverse environments or locations. Figure 8 illustrates how changing the position of one device has a more significant impact on the signal than swapping devices.

![Fig. 8: Signal amplitude shape according to position and device.](image-url)
3.1 Device Fingerprinting from Channel Impulse Response

Addressing potential measurement biases is crucial, despite the theoretical concept of fingerprint. Unintended biases may lead machine learning models to differentiate devices based on incidental factors rather than genuine hardware signatures — a phenomenon referred to as the Clever Hans effect. Unfortunately, current scientific literature on RFF often overlooks this concern, with only a few works presenting compelling evidence of mitigating biased correlations associated with detection. In order to minimize the bias due to position change during the data acquisition process, we utilized a 3D printed mount. The Channel Impulse Response (CIR) of the signal is then measured with two UWB development boards (Qorvo’s 3001CDK) — the receiver and the emitter — in a fixed position facing each other. The mount is then gradually rotated in a clockwise manner to generate CIR data across different positions in the environment.

We consider the following three evaluation scenarios to clearly demonstrate how well the learning process can generalize its feature extraction:

- **Scenario 1:** The fingerprint authentication is conducted between two fixed nodes (typically known as anchors) within a UWB network, where both the positions and identities of the nodes are known. The constructed model is fine-tuned based on this information.
- **Scenario 2:** The fingerprint authentication is performed between a fixed node and a tag node moving around the environment. The tag’s identity is known, and the feature extraction is fine-tuned specially for this tag.
- **Scenario 3:** The fingerprint authentication is carried out between a fixed node and an unknown tag in an unknown position. Initially, the network generates a trusted feature embedding of that tag to serve as an ID. Future feature embeddings can then be compared to this anchor to re-identify the tag.

Ideally, algorithms designed for RFF should be lightweight enough to facilitate real-time identification. However, achieving accurate RFF necessitates striking a balance between computational efficiency, and the algorithm’s overall performance. Here, we introduce two approaches that address the trade-offs along this spectrum:

**Convolution Neural Network:** A classical method highlighted in the literature [6, 1] for dealing with signal data and identifying different sources in RFF is the use of 1-dimensional Convolution Neural Network (CNN) to predict the source device. With this specific feature extraction, we can build a small classifier model of 10k parameters that can run on a low resourced device. The performances of such a CNN model can be found in Table 1. Noticeably, in scenario 1, the results have 100% success in classification. However, when we introduce positional variation, as seen in scenarios 2 and 3, the performances come closer to random. This indicates an over-fitting to the positional dependency of the training data and poor ability to generalize across different environments.

**Transformer:** In order to extract more potent features from the signal, we opted for a vision Transformer (ViT) [29, 7], using spectrograms of the signal as input. This model has been trained using a contrastive learning method [31], a paradigm of deep-learning that project the data into a high-dimensional latent space to capture only the relevant details necessary for the problem. Inspired by the work performed on biometrical identification such as facial recognition [21], this method is well-suited to the re-identification problem. The technique aims to achieve more generalization as the model is explicitly trained to ignore the positional information. In this setup we managed to improve the results for the second and third evaluation scenarios, indicating a better generalization of the desired feature extraction.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>CNN (10k)</th>
<th>ViT (2Mio)</th>
<th>Random projection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Classification</td>
<td>Re-ID</td>
<td>Classification</td>
</tr>
<tr>
<td>Scenario 1</td>
<td>100%</td>
<td>77%</td>
<td>100%</td>
</tr>
<tr>
<td>Scenario 2</td>
<td>15%</td>
<td>26%</td>
<td>39%</td>
</tr>
<tr>
<td>Scenario 3</td>
<td>11%</td>
<td>23%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Table 1: Performances for RFF.

The reported metrics are F1-score for Classification and F1-score for the Re-Identification task.

**Results:** The primary metric reported in our study is the F1-score for classification. It is a measure of the accuracy that a classifier can obtain in the latent space of the models. It displays the capacity of the model to shape a separable representations, but is not the method used in practice. Therefore, we introduce a second metric, the F1-score for re-identification. It consists in creating anchor vectors that represent each identity in the latent space that we compare to the query vectors to match the corresponding ID. This way we can also identify devices that
have never been seen during the training process. Note that these metrics are raw 1-shot result to give an idea of the performances. In practice, the accuracy could be improved by collecting multiple signal samples per device for identification purposes. The key insight gleaned from our work is the recognition of the challenges associated with implementing fingerprinting for UWB signals. Simpler solutions, though viable, lack robustness and require fine-tuning in specific settings. Their effectiveness is significantly influenced by the stability of the environment, particularly in networks where fixed devices consistently interact with each other. In contrast, more sophisticated learning strategies, such as those we offer, provide improved device discrimination when data is collected under controlled conditions.

3.2 Sovereign UWB Data Network

**Network Architecture:** We propose an architecture, depicted in Fig. 9 for a UWB data network, which diverges from the traditional anchor and tags concept by attributing devices based on their capability and availability. **LeaderNodes** are critical components that maintain constant operation; they are always-on and equipped with multiple network interfaces, which enable them to oversee packet forwarding and network synchronization. **FullNodes** support the network with the added potential of being promoted to LeaderNode status. **HalfNodes**, which are less frequently active, utilize UWB interfaces for packet forwarding but do not have the capacity to become a leader. **LeafNodes**, with their limited resources, perform only ranging functions and do not forward packets or assume leadership roles. **BorderNodes** stand out with their ethernet connections, always active to ensure the connection between the mesh network and external zones such as the RemoteZone and servers. We define the **HomeZone** as the first point of contact for an Authenticated User and their Smart Devices with a UWB interface.

**Medium Access Control Protocol:** Even though the UWB PHY layer supports data communication, building a standalone UWB data network is challenging due to the absence of a standardized Medium Access Control (MAC) layer protocol for applications beyond ranging. Typically, two approaches are taken to design a MAC protocol for wireless technologies: (1) Spectrum sensing-based, and (2) Time-slot-based. All commercially available wireless technologies are narrowband compared to the vast bandwidth present in UWB technology. The impulse-like nature of UWB signals (i.e., short duty cycle) poses challenges in implementing popular sensing-based MAC protocols, such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), thus rendering them unsuitable for use. In order to enable the UWB devices to form a data network, a UWB MAC stack has been developed. A key

![Fig. 9: Architecture of an Ultra Secure UWB data network](image-url)
feature of this stack is the use of a superframe structure. The superframe (100ms) is divided into time slots using Time Division Multiple Access (TDMA). This organized structure of the superframe ensures that devices have designated time slots for communication, reducing the likelihood of collisions. Each time slot serves a specific purpose and is allocated for a particular task.

In a zone, a LeaderNode periodically broadcasts superframes. Within one superframe, the LeaderNode provides synchronization information, helping all devices in the zone maintain a common time reference. This synchronization is crucial for accurate ranging and coordination within the UWB network. The information within the beacons also provides the position and mesh topology of the corresponding LeaderNode. Following the beacon slots, ranging slots are used by the other nodes for localization (e.g., through two-way ranging) and data exchange between a LeaderNode and another node. The last block of slots is reserved for data exchange between LeaderNodes with each node having its own collision-free data exchange slot.

**UWB Mesh Networking:** In our proposed UWB mesh network architecture, nodes are connected either directly to a node or indirectly through other mesh nodes. This allows each node to communicate directly with its neighbors and relay messages for other nodes, extending the network’s reach (automatic routing). The mesh network is resilient to node failures; if a node becomes unreachable, the network dynamically reroute traffic through alternative paths (self-healing). Adding more LeaderNodes/FullNodes easily scales the mesh network; new nodes can join, and existing nodes will adapt the routing accordingly (scalability). Smart devices with UWB capability are handled differently in the UWB mesh network due to their mobility. They primarily connect only during their ranging slot intervals (listening to beacon slots as required), operating in an energy-efficient manner. Consequently, mesh messages are exchanged within the ranging slots through the surrounding LeaderNode.

**Payload Accommodation:** IPv6 represents the latest version of the Internet Protocol (IP), the core technology behind the Internet. The transition from IPv4 to IPv6 is primarily driven by the need to address the limitations of IPv4, notably its limited address space, that is insufficient for the rapidly expanding number of devices connecting to the internet. IPv6, with its 128-bit address space, can support a virtually unlimited number of devices, ensuring global connectivity for billions of new devices. Beyond the expanded address space, IPv6 introduces enhancements in routing and network autoconfiguration, reduces the need for network address translation (NAT), which can complicate internet communication and hinder the performance of low-latency applications. IPv6 also includes improved security protocols as part of its core specifications, offering built-in support for IPsec for more secure communications. Clearly, UWB devices must be able to handle IPv6 packets to remain as a future-proof technology. However, the direct integration of IPv6 packets, which are 1280 bytes in size, into UWB’s 127-byte frames is impractical due to size constraints. The 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) provides an essential solution in this challenge. One of its primary advantages is the ability to transmit IPv6 packets over low-power, low-bandwidth wireless networks, enabling devices with limited processing capabilities to connect directly to the internet. Additionally, 6LoWPAN’s efficient use of IP-based communication reduces the need for complex protocol translations, simplifying network architecture and lowering operational costs. Consequently, integrating a 6LoWPAN adaptation layer into the UWB standard is necessary to compress the 40-byte IPv6 header to a minimum of 3 bytes.

### 3.3 Countermeasures to Secure ToA-based Ranging

As highlighted in the previous section, UWB devices are vulnerable to Time of Arrival (ToA) manipulation attacks in various ways. A robust countermeasure can be implemented by any node within the UWB system to enhance the security against ToA manipulation. This involves using the UWB PHY synchronization header to accurately timestamp the ToA for critical messages such as the Ranging Initiation Message, Ranging Response Message, and Ranging Final Message. When a UWB node receives these messages, it conducts a comparative analysis between the ToA calculated from the STS and the ToA derived from the UWB PHY header. A significant discrepancy between these two ToA values can serve as a red flag, prompting the UWB node to invalidate the ToA and, consequently terminate the ranging process.

### 3.4 Spatial Characterization Through Secrecy Maps

In the wireless radio access scenario, the knowledge of the local geometry provides context information for the probabilistic secrecy characterization. In particular, the probabilistic characterization necessitates prior knowledge of the distribution of large-scale channel gains between arbitrary locations in the radio access network. Second order statistics of channels between arbitrary locations and a fixed location in the radio access networks can
be obtained from so-called radio maps, whose construction and estimation has been a popular research topic in machine learning in recent years [20]. Based on this, we propose the use of any-to-any (A2A) radio maps that provide means for characterization of the wireless environment from the perspective of the adopted security metric (e.g., semantic security), by associating security levels to the communication links. This characterization results in so-called secrecy maps [27] that may be considered as a generalization of the concept of radio maps for physical layer security. The specified security levels are based on mathematically provable security guarantees for certain channel models, with semantic security ([12, 4]) serving as the security metric. In this sense, the secrecy maps can describe the leakage of information into the environment or into certain spatial regions based on a concrete description of the communication medium. The flexibility of this approach has already been demonstrated by using it in the context of indoor and outdoor communication in traditional wireless networks ([27, 28]), as well as in the case of sub-THz wireless communication [22]. In addition, variants of radio maps are already being discussed in the realm of UWB and used to solve specific localization problems (cf. for example [16, 14] and references therein). Achievable communication rates for certain UWB multipath fading channel models have been identified in [26, 3]. These results can serve as a starting point for construction of any-to-any radio maps which can then be augmented by security aspects. The basis for this will be a mathematical derivation of security guarantees for such types of channel models with respect to semantic security metric. The construction of secrecy maps can be based on either ray tracing simulators, such as NVIDIA-Sionna, in which a virtual replica of the environment and the radio channel is created, or real channel measurements for specific spatial regions can provide the necessary data for the construction of secrecy maps. To illustrate the concept, in Fig. 10 we depict (qualitatively) a secrecy map generated based on measurements in an indoor scenario (uplink). For each different position of the transmitter, we plot the resulting secrecy level of the transmitter-receiver communication link, with semantic security serving as a metric. The secrecy characterization is performed in a statistical sense, meaning that the security level can be guaranteed with a pre-defined probability.

Fig. 10: Qualitative depiction of a statistical secrecy characterization in an indoor environment (uplink scenario). Different colors encode different security levels. On the right-hand side we illustrate the effect of (gradually) switching on additional access points on the secrecy characterization (improvement of the secrecy outlook).

Implications on System Design: Given the stochastic nature of UWB channels/networks, it is possible then to quantify confidence levels for meeting the application-dictated security and reliability requirements. In addition, the secrecy maps provide information on which spatial regions would be particularly advantageous for potential eavesdroppers, i.e. they visualize regions in which leakage is particularly high. For users or areas with a security deficit, certain measures can be taken to improve the security outlook including the following techniques which have been discussed in connection with traditional wireless communication: utilization of additional access points, “friendly” jamming of spatial regions particularly attractive for potential eavesdroppers to deteriorate eavesdropper’s communication link, among others. Given this background, the secrecy characterization of the environment would act as an enabler for the integration of physical-layer security in the radio access system design. Being contextual, i.e. location specific, the secrecy characterization provides relation to the concept of spatial availability of services in the spirit of the framework in [8]. Central to this approach is the definition of a quantity to measure the spatial availability of a wireless link for a service-relevant confidence level. From a system perspective, this framework relates traditional radio link key performance indicators (KPIs) to service-level KPIs, by providing insight on the availability and reliability of wireless links. In this context, the security levels obtained through the spatial characterization can be associated with quality-of-service (QoS) levels, which in practice can be related to a prescribed set of modulation and coding schemes (MCS) as in, e.g., legacy communication systems (LTE, 5G-NR). As a result, the concept has implications...
for system aspects such as resource allocation and link adaptation. On a more general note, one can foresee a framework where users can "negotiate" and "buy" security levels based on their requirements and the cost, making information security a potential profit point for operators. As different services might have in general entirely different Quality-of-Service (QoS) requirements and security levels, it can be expected that the servitization of information security would present security as a new type of service (e.g., like voice and data).

4 Conclusion

This paper comprehensively highlighted the existence and emergence of various attacks on UWB technology, emphasizing the imperative need for enhanced security measures. To strengthen the security aspect of UWB, we proposed a novel machine learning based approach to device fingerprinting utilizing CIR information for robust device authentication. This offers an alternative to the traditional authentication methods. The results demonstrate the effectiveness of our proposed methods in extracting and identifying unique device fingerprints across three distinct scenarios. Furthermore, we explored the concept of sovereign UWB data network, envisioning its potential application in healthcare and secure environments where conventional wireless technologies may be limited or prohibited. We outlined a UWB mesh network architecture that encompasses a wide range of devices based on their capability and availability, and developed a TDMA based MAC protocol, keeping in mind the limited payload capacity of UWB’s physical layer. Moreover, we have investigated the potential of the secrecy map to further improve the security of UWB systems. Finally, we advocated that the integration of the proposed enhancements into UWB standard would significantly contribute to strengthening the security posture of UWB and foster its wider adoption across various applications.
References


[21] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. 2015. 3.1


[31] Ye Yuan, Wuyang Chen, Yang Yang, and Zhangyang Wang. In defense of the triplet loss again: Learning robust person re-identification with fast approximated triplet loss and label distillation, 2019. 3.1