Fira | The Power to Be Precise

Introduction to Impulse Radio UWB Seamless Access Systems

Hans-Juergen Pirch, HID Global
Frank Leong, NXP Semiconductors

Abstract

In this paper we present an overview on the development and standardization of ultra-wideband systems, technical aspects of the IEEE 802.15.4 standard, and improvements made by the 802.15.4z amendment. We also explain the basic workings of a physical access system, the desired seamless access experience and how ultra-wideband technology can enable it. In addition, we briefly compare ultra-wideband to facial recognition access systems. We conclude by mentioning how ultra-wideband technology may extend to other related applications.

1) Introduction

1.1   Scope

Impulse Radio Ultra-Wideband (IR-UWB) systems have received significant media attention throughout 2019. This is due to announcements from high profile companies that they are either investing in, or have already released this technology in their new products. Some examples of this are Apple's iPhone 11 and the Car Connectivity Consortium press release.[1] In this paper we provide an overview of this technology and illustrate one of the most popular use-cases, seamless access, in more detail.

---

[1] *https://carconnectivity.org/press-release/car-connectivity-consortium-unveils-new-features-for-digital-key-specification/*
https://www.cnet.com/news/apple-built-uwb-into-the-iphone-11-heres-what-you-need-to-know-faq/

1.2   A Brief History

UWB stands for ultra-wideband and this general term applies to any radio communication system that employs a wide bandwidth, typically defined as either a 10 dB bandwidth greater than 20% of the center frequency or greater than 500 MHz in absolute terms [Itur06]. Most of the recent research and work in this field relates to IR-UWB systems in particular, meaning systems that employ very short duration / high bandwidth pulses for their communication. This paper primarily refers to such systems, so the term UWB is often used synonymously with IR-UWB, even if not explicitly stated.

UWB systems are not new. Rather, they are the oldest form of radio communication. In 1887 Heinrich Hertz built the first experimental spark-gap transmitter to prove Maxwell's prediction of electromagnetic waves [Huur03]. Guglielmo Marconi later used impulse transmissions in his telegraph systems, including the famous transatlantic transmissions in 1901.

Approximately fifty years after Marconi's inventions, impulse radio transmissions gained some traction in radar applications, primarily for military purposes [Neko05].

In the early 1990s Robert Scholtz and Moe Win started to collaborate at the University of Southern California, providing the basis for UWB wireless networks. They were the first to demonstrate superiority of UWB in multipath environments due to its resilience to fading and interference.[2]

As interest in the commercialization of UWB increased, an extensive study was conducted by the U.S. Federal Communications Commission (FCC), which led to the authorization of the commercial use of UWB for selected applications in February 2002 [Neko05]. The amount of bandwidth for development of commercial UWB technology was unprecedented and represents the widest band available for license free radio use today (7.5 GHz of useable spectrum bandwidth). The radiated power of such systems was strictly limited to prevent interference with other technologies.

1.3   Standardization

In addition to regulatory bodies such as the FCC and ETSI, other standard setting organizations like the Institute of Electrical and Electronics Engineers (IEEE) became involved in UWB systems early on.

Early commercial UWB efforts were focused on high data rate communications, using Orthogonal Frequency-Division Multiplexing (OFDM) and Direct Sequence Spread Spectrum (DSSS). Only later did the focus shift to ranging and geolocation, and in 2004 the IEEE established the 802.15.4a task group to develop a standard for such applications including an associated UWB physical layer (PHY). An updated version of this PHY is included in [Ieee15]. The IEEE is currently developing a security extension for IR-UWB systems in the form of the 802.15.4z amendment, thereby further improving the current specification in multiple aspects, some of which we will discuss in this paper.

Building on this standardization activity, other bodies, such as the FiRa Consortium, have taken the IEEE 802.15.4 PHY and MAC specifications as the basis for further extensions. These include the specification of an application layer and service-specific protocols to support a variety of vertical market applications, thus creating standards for end-to-end, interoperable UWB systems.

[2] *https://ethw.org/Robert_A._Scholtz, https://ethw.org/Moe_Z._Win*

2) Radio Channel

2.1   Frequency Bands

The FCC authorizes the commercial use of UWB devices in the frequency band from 3.1 GHz to 10.6 GHz with a very restricted Equivalent Isotropic Radiated Power (EIRP) of -41.3 dBm/MHz [Fccx02] [Fccx05]. [Ieee15] divides this spectrum further into individual channels as shown in Figure 1 below.
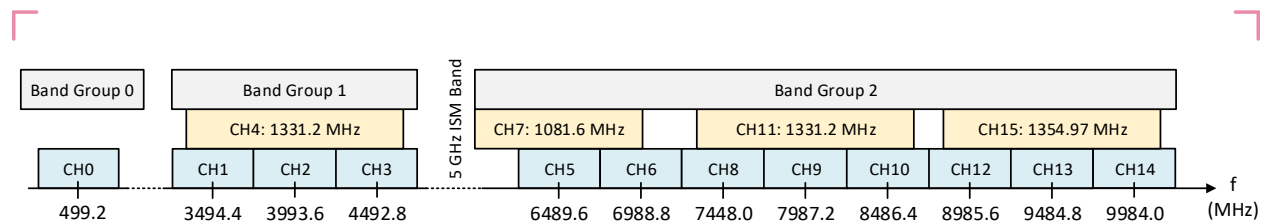

Figure 1: IEEE 802.15.4-2015 - HRP PHY band allocation (blue channels have 499.2 MHz bandwidth, others as noted)

The frequency band is divided into three separate groups:

• Band Group 0: sub-gigahertz channel

• Band Group 1: low-band HRP UWB channels

• Band Group 2: high-band HRP UWB channels

From Figure 1 it can be seen that not all of the FCC authorized bandwidth has been assigned to channels within [Ieee15]. The frequency gap between Band Group 1 and Band Group 2 was introduced in order to avoid interference between UWB and technologies in the 5 GHz ISM band (e.g., WiFi).

In Europe, further restrictions apply to Band Group 1, such that a device using those channels needs to implement a Low Duty Cycle (LDC) mitigation technique as well as Detect And Avoid (DAA) mechanism [Etsi16]. These additional restrictions make the use of Band Group 2 channels more attractive for globally deployed UWB devices.

2.2   Pulse Shape

In order to match the UWB signal to the 500 MHz bandwidth of [Ieee15], the pulse shape needs to be chosen carefully to ensure compliance to the [Ieee15] specified transmit spectrum mask and avoid distortion of adjacent channels. Additionally, stringent regulatory transmit limits must be respected. Figure 2 shows the [Ieee15] Root Raised Cosine (RRC) HRP UWB reference pulse with a center frequency that corresponds to channel 9, as well as an upconverted 8th order Butterworth low pass pulse with a -3 dB bandwidth of 500 MHz and a center frequency that corresponds to channel 5. Both of these pulses would meet the requirements specified in [Ieee15] to be used for IR-UWB radios.
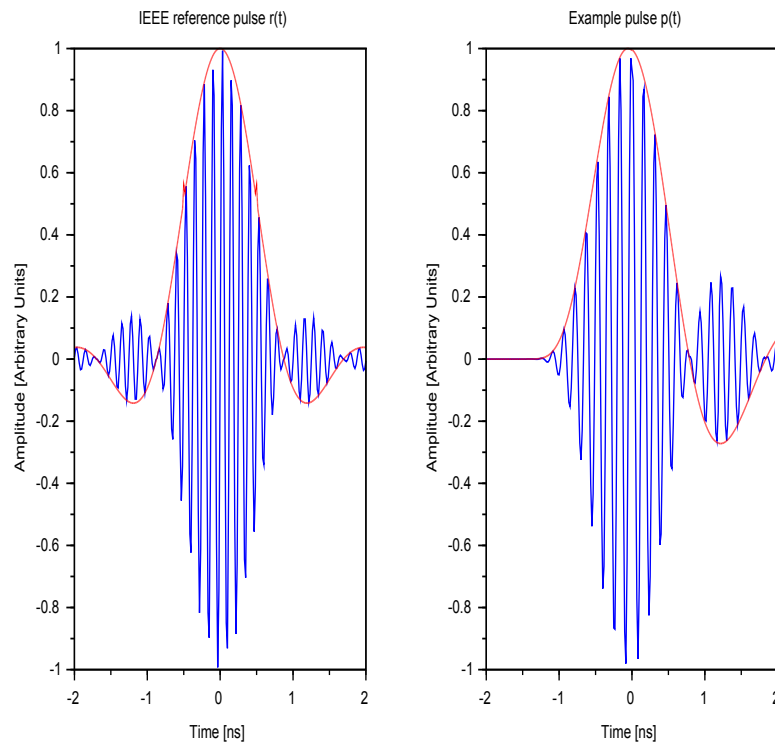
Figure 2: [Ieee15] reference pulse for channel 9 and example pulse for channel 5

2.3   Channel Characteristics

The ultimate performance limit of a communication system is determined by the channel it operates in. In order to effectively predict performance, a realistic channel model is essential [Moli05]. Channel models are typically developed by combining practical measurements in relevant environments and simulation [MCE+06] [KWA+07].

Commercial UWB systems are intended to be used in complex environments such as residential, office or industrial indoor areas. In these environments, signal reflection and diffraction play a significant role. The signal received by an antenna is the sum of the attenuated, delayed and possibly overlapping versions of the transmitted signal and may vary over time (due to movement of receiver/transmitter or change in environment). These different versions of the transmitted signal are typically referred to as multipath components (MPCs).

The large bandwidth of UWB systems ensures a high level of resilience to frequency-selective fading, which is an effect that limits performance in narrow-band technologies [WiSc93]. Furthermore, many of the multipath components are resolvable due to the short pulse durations/high bandwidth involved [Moli09].

For the design of a receiver it is important to understand the number of MPCs that are necessary to capture a certain amount of energy. In previously mentioned environments this can be a challenge, especially in Non-Line-of-Sight (NLOS) scenarios where the 100 strongest MPCs may carry as little as 30% of the total energy [KWA+07].

Furthermore, for ranging applications it is essential to identify the first path, as it is most representative of the distance between transmitter and receiver. In NLOS scenarios especially, this may not be the strongest of the MPCs [Moli09] as illustrated in Figure 3, which represents an additional challenge for the receiver (first path detection).
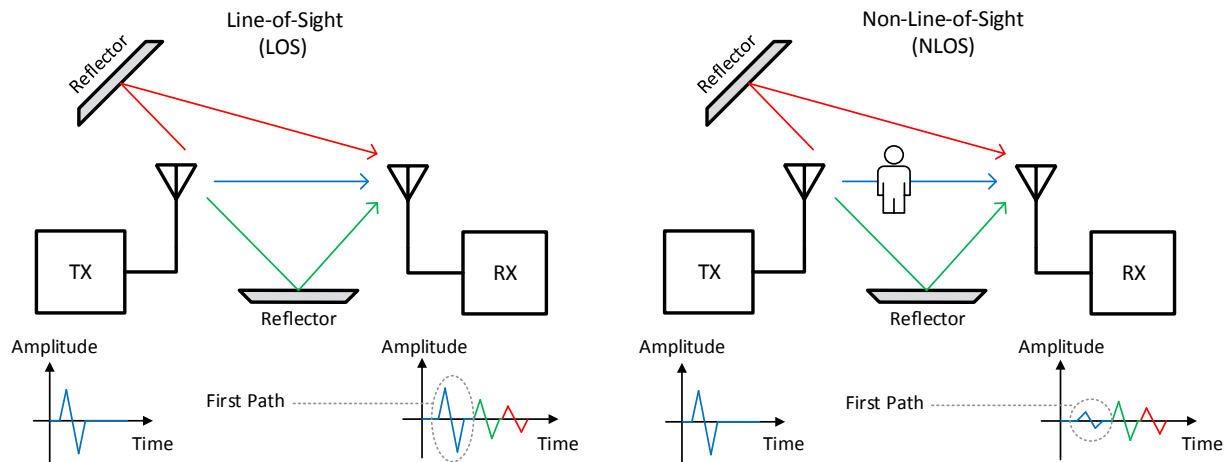

Figure 3: Simplified example of multipath components in LOS and NLOS scenario

3) Ranging/Receiver

Systems such as Global Positioning System (GPS) rely on One Way Ranging (OWR), whereby multiple satellites (representing fixed nodes referred to as anchors) regularly transmit synchronized sets of radio packets, which allow a receiver unit (representing the mobile node referred to as tag) to calculate its position via Tag-Side Time-Difference of Arrival (TS-TDOA) evaluation. The reverse, commonly applied with IEEE 802.15.4 LRP UWB based systems, would also be possible: the tag transmits a radio packet, and the synchronized anchors calculate the tag's position via Anchor-Side Time-Difference of Arrival (AS-TDOA) evaluation. Depending on specific application requirements, both methods can be used with the IEEE 802.15.4 HRP UWB PHY.

Basic Time-of-Flight (TOF) Two Way Ranging (TWR) consists of two (radio) packets being exchanged. This is called Single Sided Two Way Ranging (SS-TWR). In the diagram below, the actual time differences are drawn. The estimated / measured time differences are denoted as their actual counterparts with an additional subscript "m". An SS-TWR TOF estimate can be calculated as follows.

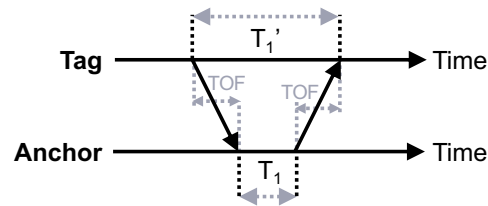$$TOF_{est,ss} = \frac{1}{2} \cdot (T'_{1,m} - T_{1,m}).$$

Figure 4: Single Sided Two Way Ranging (SS-TWR)

A more advanced TOF ranging method, called Double Sided Two Way Ranging (DS-TWR), allows implicit correction of errors due to clock offsets. A method for calculating a DS-TWR TOF estimate is given below.

$$TOF_{est,ds} = \frac{1}{2} \cdot \frac{T'_{1,m} \cdot T'_{2,m} - T_{1,m} \cdot T_{2,m}}{T'_{1,m} + T'_{2,m} + T_{1,m} + T_{2,m}}.$$

In this case, if we denote the normalized local clock frequencies by f1 and f2 (nominally both equal to 1 in the case of ideal clocks), the estimate will depend on clock offsets as follows.

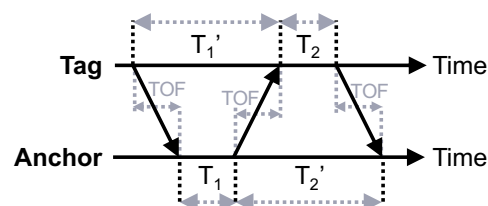$$TOF_{est,ds} = \frac{f_1 \cdot f_2}{f_1 + f_2} \cdot TOF.$$

Figure 5: Double Sided Two Way Ranging (DS-TWR)

In case of UWB, correction of clock errors is also possible for SS-TWR, as state-of-the-art receivers are able to accurately determine clock offsets between the transmitters of incoming packets and the local clock used for reception.

Another central factor in determining the performance of a TOF ranging system is the capability of a receiver to accurately determine the Time of Arrival (TOA) of an incoming (radio) packet, particularly the TOA associated with the direct or Line-of-Sight (LOS) path. Determination of the LOS TOA may be challenging, especially when the LOS path is obscured (e.g. by human body attenuation, see Figure 3) while a strong reflected path is present at the same time. A receiver needs to provide high dynamic range to be able to successfully detect the LOS TOA in such scenarios. The key metric used to express the receiver's dynamic range is the largest ratio between reflected path strength and direct path strength for which the direct path is still reliably detected.

For the IEEE 802.15.4 HRP UWB PHY, high dynamic range can be obtained by correlation. The Channel Impulse Response (CIR) is determined/estimated by a correlator, acting as a de-convolution operator on a known pulse pattern (preamble) associated with the incoming radio packet.

For the basic IEEE 802.15.4 HRP UWB PHY, the preamble symbols have perfect periodic autocorrelation properties, allowing (in principle, for a radio channel length shorter than the preamble symbol) determination of the CIR via direct correlation, whilst the preamble symbols are sufficiently long, so as not to cause spectral peaks, which would degrade the allowable transmitted integrated band power. Within the upcoming 802.15.4z amendment, the Scrambled Timestamp Sequence (STS) field is additionally available. The STS is not limited to the preamble symbol length and is not predictable provided the RNG seed is not revealed or otherwise known to adversaries, but may require some Digital Side Lobe Suppression (DSLS) being applied in the receiver to correct for added peaks in the ranging ambiguity function (i.e., artifacts in the autocorrelation of the STS). As the STS is not periodic, it does not cause periodicity-related peaking in the transmit spectrum.
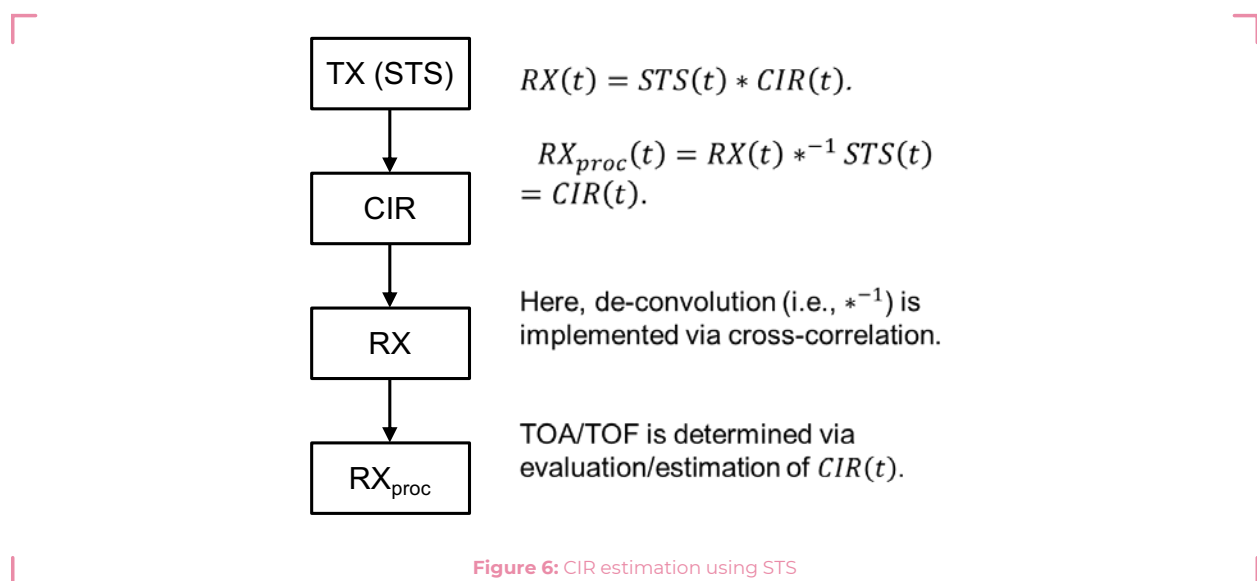
TX (STS) → CIR → RX → RX$_{proc}$

$$RX(t) = STS(t) * CIR(t).$$

$$RX_{proc}(t) = RX(t) *^{-1} STS(t) = CIR(t).$$

Here, de-convolution (i.e., $*^{-1}$) is implemented via cross-correlation.

TOA/TOF is determined via evaluation/estimation of $CIR(t)$.

Figure 6: CIR estimation using STS

As shown in January 2019[3], improvement of the receiver's dynamic range is possible by increasing the number of threshold decision events. This may be done by increasing the number of pulses being transmitted, i.e., raising the mean Pulse Repetition Frequency (PRF), which is done in the 802.15.4z HRP UWB HPRF mode.

4) PHY Layer Security

Whilst IR-UWB provides ranging estimates suitable for low-latency localization applications, concerns have been raised regarding the level of security provided by the basic IEEE 802.15.4 HRP UWB PHY, related to the periodic preamble correlation pattern that can be used in a typical receiver implementation [PFP+11]. Furthermore, in non-secure ranging and localization applications, the use of the periodic preamble for range estimation may introduce measurement artifacts under specific multipath channel conditions.

[3] https://mentor.ieee.org/802.15/dcn/19/15-19-0053-01-004z-selecting-parameter-sets-in-the-revised-hrp-uwb-phy.pptx

The periodic nature of the basic IEEE 802.15.4 HRP UWB PHY preamble allows an attack, in which a delayed version of one or more preamble symbols is (partially) injected. This can "wrap around" and be interpreted as a first path associated with the next preamble symbol, while containing insufficient energy to significantly affect reception (authentication) of payload data. This scenario is referred to as "preamble injection attack" and is illustrated in Figure 7. Note that when the original packet contains a large number of preamble symbols, this type of attack may succeed even if the adversary's delayed fake signal contains no more than one pulse per preamble symbol.
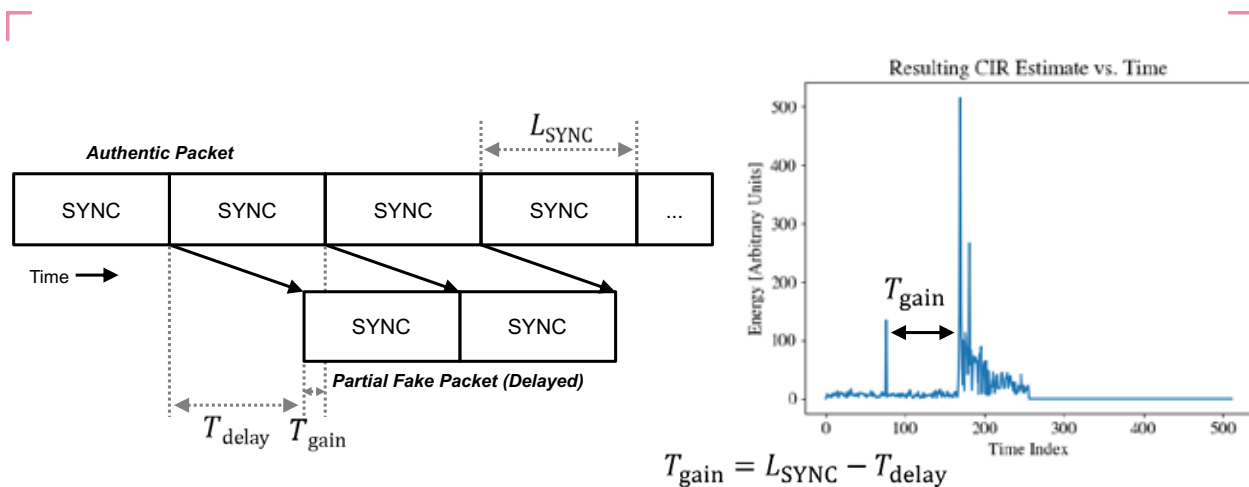

Figure 7: Resulting channel estimate after preamble injection by adversary; preamble symbols are labeled "SYNC"

Other attacks such as Cicada or Early Detect, Late Commit (EDLC) have been proposed [PFP+11], that target the periodicity and/or predictability of the preamble to achieve a distance reduction in the range measurement, or exploit the length of data symbols such that receivers will accept manipulated measurements – possibly aided by (partial) amplification of the (a priori unpredictable) legitimate data sequences.

The IEEE 802.15.4z amendment provides the HRP UWB PHY with a means to address the points above, by introducing the STS field into the packet.

The STS field consists of a set of pseudo-random Binary Phase Shift Keying (BPSK) modulated pulses, transmitted in one or more segments, which are each bounded by gaps (i.e., time intervals during which the transmitter is silent). The pseudo-randomness of the BPSK modulation sequence is ensured by a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG), also referred to as Deterministic Random Bit Generator (DRBG), as recommended by the National Institute of Standards and Technology (NIST) in [Nist15]. Due to the pseudo-randomness of the sequence, there is no periodicity, allowing reliable, highly accurate, and artifact-free channel estimates to be produced by the receiver.

For efficient decoding of the STS, the receiver needs to have a copy of the sequence locally available before the start of reception. Meeting this requirement, without introducing the means for adversaries to mount replay attacks, is a responsibility that befalls higher layer STS seed management, which is within the scope of other standardization bodies building on top of the IEEE specification such as the FiRa Consortium.

5) Data Communication

5.1   Basic IEEE 802.15.4 Preamble and Data Modulation

The basic IEEE 802.15.4 HRP UWB PHY is essentially a spread-spectrum PHY. Preamble symbols are repeated by the transmitter such that energy can be accumulated in the receiver and data symbols are spread across multiple pulses.

Data bits, as used in the PHY Header (PHR) and the PHY Service Data Unit (PSDU), are encoded using either a SECDED (PHR) or Reed-Solomon (PSDU) code, followed by convolutional encoding, after which the coded bits are mapped via Burst Position Modulation (BPM) and BPSK onto sets of multiple pulses called "bursts". The pulses within a burst are transmitted back-to-back, meaning without gaps on the 499.2 MHz chip grid. The (BPSK) polarities of the pulses, as well as the (BPM) burst timings, are scrambled using a linear feedback shift register (LFSR), in order to whiten the spectrum, so as not to cause spectral peaks which would degrade the allowable transmitted integrated band power. Scrambling also increases orthogonality between different transmitted signals, which may provide benefits in (co-channel) interference scenarios.

5.2   802.15.4z Enhancements to Preamble and Data Modulation

UWB transmissions are, under current FCC [Fccx02] [Fccx05] and ETSI [Etsi16] regulations, limited to an in-band Power Spectral Density (PSD) of -41.3 dBm/MHz, which translates to -14 dBm band power for a "brick-wall spectrum" 500 MHz wide UWB signal. As this power level is very low compared to other radio standards, and certain applications depend on the UWB signals being able to overcome human body attenuation, it is important that the PHY contains no features that further reduce the available link budget.

For the first generation of 802.15.4z based applications, the PHY consists of the basic 64 MHz Pulse Repetition Frequency (PRF) HRP UWB PHY, enhanced by the addition of the STS field in which the PRF is also approximately 64 MHz. The 802.15.4z HRP UWB HPRF modes improve upon this by raising the PRF further and striking a balance between several optimization criteria. These optimization criteria differ from the ones used in defining the basic IEEE 802.15.4 HRP UWB PHY.

First, for the 802.15.4z HRP UWB amendment, a coherent receiver architecture is assumed.

Second, for the HPRF data modulation schemes, a balance is struck between the number of pulses per data bit, airtime per data bit, instantaneous Power Amplifier (PA) peak power, compliance with regulatory peak EIRP limits (i.e., transmit power mask), and expected losses due to inter-symbol interference associated with multipath radio channel conditions. As a result, two new data modulation schemes are defined, with payload data rates of 6.8 Mbit/s (aimed at large number of pulses per data bit) and 27 Mbit/s (aimed at short airtime per data bit). The new data modulation schemes are illustrated below, in Figure 8 and Figure 9, respectively. In both cases, the convolutional encoder output bits (g^0 and g^1) determine the BPSK modulation of the first and second burst within the data symbol, respectively.
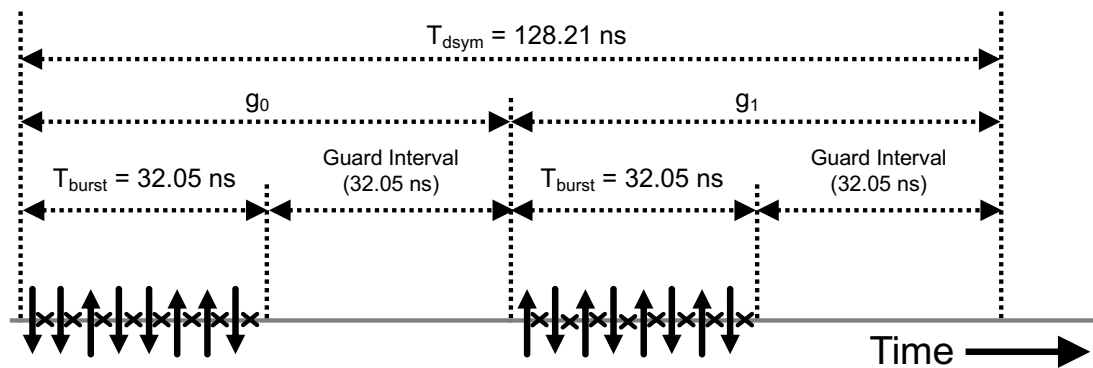
Figure 8: Symbol design for 6.8 Mbit/s payload data rate; guard chips are denoted by "X"
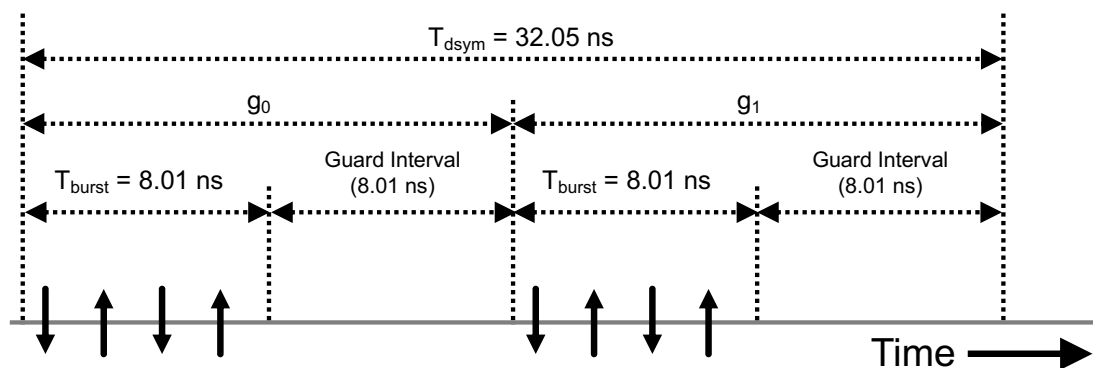

Figure 9: Symbol design for 27 Mbit/s payload data rate

Third, an option is added to use a more advanced K=7 convolutional encoding based Forward Error Correction (FEC) scheme.

Fourth, a different PHR format is defined. For K=3 + RS FEC, each set of two convolutional encoder output bits in the PHR is mapped to two consecutive data symbols (basically symbol repetition after which non-repetitive scrambling is applied), making its data symbol rate half that of the payload. This scheme makes bit errors in the PHR less likely than in the payload, without consuming excessive airtime.

Fifth, the PRF in the STS field is raised to 124.8 MHz (referred to as PRF128). This provides a larger entropy/time ratio and raises the achievable dynamic range in channel estimation.

Sixth, eight new "dense ternary" preamble sequences are defined. These sequences contain proportionally smaller sets of zero-valued elements, raising the PRF compared to the basic IEEE 802.15.4 HRP UWB PHY, and making the PRF more uniform across the packet.

Seventh, binary Start-of-Frame Delimiter (SFD) sequences are used to exploit the capabilities of the coherent receiver architecture, resulting in improved detection performance compared to the basic IEEE 802.15.4 HRP UWB PHY.

6) Application: Seamless Access

6.1   Physical Access Control System

The primary purpose of a physical access control system (PACS) is to authenticate and authorize a person so that he/she can pass through a physical portal. However, the architecture of a PACS may vary significantly based on the application (hotel, residential or office access), technology (door types, interface technologies), and manufacturer. Figure 10 shows a basic system structure as it is typically used in office access applications.
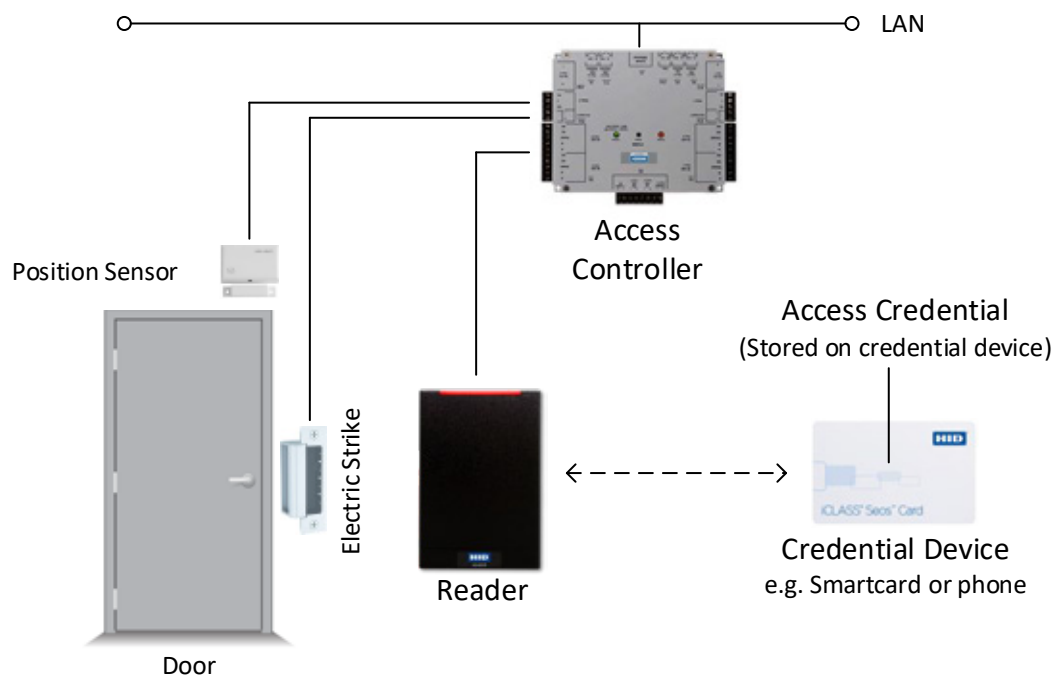

Figure 10: Basic PACS architecture

The following list describes the role of each component within a typical PACS:

- **Access Credential:** Data object, a piece of knowledge (PIN, password) or a facet of a person's physical being (face, fingerprint, etc.) that provides proof of identity.

- **Credential Device:** Stores the access credential in case it is a data object (e.g., smartcard or phone). Often a credential device is referred to as the access credential.

- **Reader:** Retrieves and authenticates the access credential (from the credential device) and sends it to the access controller.

- **Access Controller:** Compares the access credential to an access control list and grants or denies access (controls the door lock). It may also send transaction logs and status information to a database and/or backend system.

In many installations, reader devices may also include the access controller functionality. Such readers are typically referred to as offline or standalone readers. If the unlocking mechanism is included as well, a device is referred to as smart door lock (more typically used in residential applications). Smart door locks especially, are often battery powered, and power consumption (battery lifetime) is a key parameter for them.

6.2   IR-UWB Seamless Access

In the case of physical access, an electronic device needs to authenticate a person, which requires different methodologies than those used for electronic devices authenticating each other. Authentication methods for persons are typically split into three broad categories: "Something you know", "Something you have" and "Something you are" [Schn09] (see also description of access credential above). For a PACS, "Proof of Presence" is as important as the Authentication, when granting access through a particular physical portal at a given moment in time. IR-UWB can provide exactly this information in a secure manner.

Conventionally, an access sequence consists of four parts: Proof of Presence, Intent, Authentication and Authorization. The user approaches the door and presents their access credential / credential device (Proof of Presence & Intent). The reader then checks the validity of the access credential (Authentication) and sends it to the access controller, which grants or denies access (Authorization).

We define seamless access as an experience achieved, where access is granted without intrusive actions to show Intent (e.g., presenting a card, entering a PIN), whilst maintaining the same level of security. The secure and accurate ranging capability of IR-UWB makes it a suitable technology to enable such an experience.

We propose the following sequence for such a scenario:

1.   Out-of-band Authentication (via Bluetooth Low Energy or other RF technology)

2.   Proof of Presence & Intent detection based on secure UWB ranging data

3.   Authorization of access rights

Bluetooth Low Energy (BLE) is used for device discovery and application selection (in case the device hosts multiple UWB applications). A secure communication channel is established between the devices, which is used by the reader to retrieve the access credential. After successful Authentication of the access credential, the reader negotiates the UWB RF parameters and shares a temporary session key (STS seed) with the credential device. At this point the BLE communication channel may be terminated and secure ranging starts. Apart from providing the session key exchange to secure the UWB communications, BLE offers lower energy consumption overhead during the device discovery phase, particularly in scenarios where devices are running multiple BLE applications in parallel. At the start of secure ranging, the two devices are not synchronized and an IR-UWB receiver may consume significant power when active (around 200 mW in first generation IR-UWB ICs). Using BLE for discovery and channel establishment allows the UWB receive time to be minimized.

By acquiring regular UWB ranging information, the reader can determine Proof of Presence and Intent. Depending on various factors like door types, security requirements, etc., the Intent criterion can vary significantly. It can be a simple distance threshold (e.g., user within 1 meter of the door) or a complex algorithm taking into account user trajectory, speed, position and history to determine the Intent to go through a door. Note that IR-UWB in its basic form will only provide distance information. More complex

Intent detection criteria require multiple reader devices working together (e.g., trilateration/multilateration of credential device), or additional features like angle-of-arrival detection within a single device.

When the Proof of Presence and the Intent criteria are met, the reader will release the access credential to the access controller and the access grant/deny decision is made (Authorization). It should be noted, that in the case of standalone readers or smart door locks, Authorization may occur right after the transfer of the access credential, as the reader includes the access controller functionality. In this scenario, the UWB channel would only be established if a user has Authorization to pass through the door. This can significantly reduce energy consumption.

In traditional PACSs, the Intent is actively indicated by the user (e.g., by presenting a card), whilst in seamless access the system needs to infer it. A poorly defined or implemented algorithm can lead to security issues. For example, a simple Intent detection algorithm that opens the door when an authorized user is with 2 meters, may open all doors in a corridor, when said user walks along it without the intention to go through any of them. For high security portals (e.g., door to company server room), traditional technologies may be preferred over seamless access as convenience may have lower priority. However, even in these scenarios, UWB may be considered as a seamless second factor to grant access (e.g., fingerprint paired with UWB device ranging).

6.3   Comparison to Other Seamless Access Technologies

UWB is not the only technology that holds the promise of seamless access. Facial recognition in particular is already used in some PACSs to provide a seamless access experience.

Apart from technical challenges that come with facial recognition (e.g., spoof detection), both types of systems have different advantages.

Facial recognition authenticates the person trying to enter a door directly, whilst UWB access in its basic form verifies only the presence of an enrolled device (whether it is in the hands of an authorized person or not). However, UWB access does have advantages over facial recognition. For example, enrollment procedures already in use for Near Field Communication (NFC) PACSs can readily be adjusted for UWB credentials, whereas the enrollment process for facial recognition systems is more cumbersome, as it involves taking various pictures of the person to be enrolled. Furthermore, there are privacy implications when using facial images.

UWB access and facial recognition are not mutually exclusive. Various multimodal authentication mechanisms exist already [Ushs15], each with its own advantages and drawbacks. We envision that systems may combine both technologies to offer levels of security and/or user experience beyond current systems.

7) Conclusion and Outlook

We have presented the technical basics of IR-UWB, as well as the key building blocks / architecture of a PACS, and how the two can be combined to achieve a seamless access experience.

Deploying such a PACS provides the added opportunity of supporting high precision indoor location services. This would require a backend system, aggregating ranging reports from individual readers, such that the necessary processing can be performed. In situations where access readers are sparsely populated, additional UWB anchors may be required to achieve adequate coverage.

Another application, that is similar to physical access, and may benefit from a UWB seamless experience, is public transportation (e.g., access gates to a subway). A key difference in this scenario is that a financial transaction is involved (fare payment) between the credential device and the reader. Consequently, the communication flow may need to differ from the PACS scenario, to cater for this. For example, the transaction should only happen after Intent is clearly determined as it is part of the Authorization step and it may be performed over the established UWB channel – only once (secure) ranging has determined Intent, the transaction is performed over UWB.

Literature

[Etsi16]   ETSI EN 302 065-1 V2.1.1: "Short Range Devices (SRD) using Ultra Wide Band technology (UWB); Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Part 1: Requirements for Generic UWB applications", ETSI, 2016

[Fccx02]   FCC Code of Federal Regulation Title 47, Part 15 Subpart 250 "Technical requirements for indoor UWB systems", FCC, 2002

[Fccx05]   FCC Code of Federal Regulation Title 47, Part 15 Subpart 517 "Operation of wideband systems within the band 5925-7250 MHz", FCC, 2005

[Huur03]   Huurdeman, Anton A.: "The Worldwide History of Telecommunications", Wiley, 2003

[Ieee15]   IEEE 802.15.4-2015: "IEEE Standard for Low-Rate Wireless Networks", IEEE, 2015

[Itur06]   ITU-R SM.1755-0: "Characteristics of ultra-wideband technology", ITU, 2006

[KWA+07]   Johan Karedal, Shurjeel Wyne, Peter Almers, Fredrik Tufvesson, Andreas F. Molisch: "A Measurement-Based Statistical Model for Industrial Ultra-Wideband Channels", IEEE Transactions on Wireless Communications, 2007

[MCE+06]   Andreas F. Molisch, Dajana Cassioli, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Balakrishnan Kannan, Johan Karedal, Juergen Kunisch, Hans Gregory Schantz, Kazimierz Siwiak, and Moe Z. Win: "A Comprehensive Standardized Model for Ultrawideband Propagation Channels", IEEE Transactions on Antennas and Propagation, 2006

[Moli05]   A.F. Molisch: "Wireless Communications", New York, IEEE Press/Wiley, 2005

[Moli09]   A.F. Molisch: "Ultra-Wide-Band Propagation Channels", Proceedings of the IEEE Vol.97 No.2, 2009

[Neko05]   Nekoogar, Faranak: "Ultra-Wideband Communications: Fundamentals and Applications", Prentice Hall Press, 2005

[Nist15]   NIST Special Publication 800-90A Revision 1: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", NIST, 2015

[PFP+11]   Marcin Poturalski, Manuel Flury, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec: "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures", IEEE Transactions on Wireless Communications, Vol. 10, No. 4, 2011

[Schn09]   Fred B. Schneider: Draft chapters for a textbook on cybersecurity (as yet, untitled: https://www.cs.cornell.edu/fbs/publications/chptr.AuthPeople.pdf), Cornell University, 2009

[Ushs15]   U.S, Department of Homeland Security, Science and Technology: "Access Control Technologies Handbook", System Assessment and Validation for Emergency Responders (SAVER) Program, 2015

[WiSc93]   M. Z. Win and R.A. Scholtz: "Impulse Radio: How it works", IEEE Commun. Lett. Vol.2, 1993

About the Authors

Dipl.-Ing. Hans-Juergen Pirch

CV

Dipl. Ing. Hans-Juergen Pirch studied computer science at the University of Applied Science Mittweida. Since 2005, Mr. Pirch has served in various R&D positions at HID Global, most recently as Engineering Director, Hardware Platforms, with responsibility for developing new platforms and technologies. He also represents HID Global at the FiRa Consortium.

Contact

Hans-Juergen Pirch, HID Global
Waagner-Biro-Strasse 100 (Science Tower)
8010 Graz, Austria
Phone: +43-664-88514692
E-Mail: hpirch@hidglobal.com

Ir. Frank Leong

CV

Frank Leong studied Electrical Engineering at the University of Twente (NL), focusing on Embedded Systems. Since 2007, Mr. Leong has held various R&D roles with NXP Semiconductors. Since 2019, he is in a Product Manager position, responsible for Automotive UWB product definition. Mr. Leong also represents NXP in the IEEE 802.15 work, in the Car Connectivity Consortium DKTG and in the FiRa Consortium.

Contact

Frank Leong, NXP Semiconductors
High Tech Campus 46
5656 AE Eindhoven, The Netherlands
Phone: +31-6-13360727
E-Mail: Frank.Leong@nxp.com

About FiRa Consortium

Headquartered in Beaverton, OR, the FiRa Consortium is a member-driven organization dedicated to the development and widespread adoption of seamless user experiences using the secured fine ranging and positioning capabilities of Ultra-Wideband (UWB) technologies. To learn more about the FiRa Consortium, visit www.firaconsortium.org.