The Power to Be Precise

UWB Secure Ranging in FiRa

FiRa™ Consortium | August 2022

Table of Contents

1 Abstract 3
2 Introduction to Ultra-Wideband (UWB) Ranging 4
2.1 Link-Budget Optimized Ranging 4
2.2 Secure Ranging 5
2.3 Secure Receiver Characteristics 6
3 Attack Scenarios 7
4 FiRa Standardization and Certification Programs 8
4.1 UWB PHY Technical Requirements 8
4.2 UWB MAC Technical Requirements 8
4.3 Secure UWB Service API 9
5 UWB Modem Implementation Considerations 10
6 Conclusions 13
7 References 13

FiRa Consortium
Security Working Group

Authors List:
Giridhar Mandyam (Qualcomm)
Xiliang Luo (Apple)
Eric Perraud (Qorvo)

Acknowledgement List:
Rias Al-Kadi (NXP)
Hugues de Perthuis (NXP)
Fabien Courtiade (Qorvo)
Darren Krahn (Google)
Brian Redding (Qualcomm)

MITIGATIONS FOR ULTRA-WIDEBAND SECURE RANGING ATTACKS

1 Abstract

Secure ranging is the process of precise detection of the relative location of a radio transmitter with respect to the receiver, with protection against “distance shortening” attacks. If the distance between the transmitter and receiver is within a pre-specified limit, then some form of authorization, usually in the form of physical access such as unlocking a door, may be given to the transmitting device.

Ultra-Wideband (UWB) radio technology has seen increased adoption in secure ranging due to the ability to form an accurate Time-of-Flight (ToF) estimation and therein relative position determination. Several attacks are possible on UWB systems, which take advantage of the regularity inherent in the transmitted waveform. FiRa™ has considered theoretical and reported attacks (see [1]-[3]). FiRa standardization, through technical specifications and the associated certification program, is notably ensuring that such attacks would be difficult to carry out against FiRa-compliant products.

This paper introduces an overview of some well-known attack methods applied to UWB ranging and their technical prerequisites. It also describes how FiRa is mitigating these attacks along with UWB design considerations.

2 Introduction to Ultra-Wideband Ranging

Thanks to its ultra-wide bandwidth, Impulse Radio UWB (IR-UWB) is an ideal RF waveform to enable accurate distance measurement (ranging) between devices. For applications that focus more on ranging accuracy, receivers can be implemented such that the best ranging accuracy performance can be achieved under typical noise or interference scenarios. This category of ranging is also referred to as link-budget optimized ranging. Meanwhile, in those applications that rely on physical ranging to enable various secure applications, it is required that the ranging result always provides an upper bound on the actual physical distance, a.k.a. distance-bounding. Both types of ranging are enabled by the scrambled timestamp sequence (STS) signal, which is a particular physical signal carrying cryptographically encrypted bits as specified by FiRa [4]. Moreover, these two categories of ranging methods could differ in how confidentiality of the keys used during ranging and filtering are applied.

2.1 Link-Budget Optimized Ranging

Under typical noise or interference conditions, the ranging problem can be thought of as a standard parameter estimation one. Receivers could be designed to provide the best ranging accuracy under specific system models in the sense of minimum variance or minimum mean-square error (MSE). For example, a maximum-likelihood principle can be applied to obtain the range estimator that is able to achieve the Cramer-Rao bound asymptotically.

2.2 Secure Ranging

In secure ranging, we need to ensure the robustness against feasible distance decreasing attacks. Specifically, a secure ranging receiver needs to ensure the probability that Ymea is less than Xphy is small enough, where Xphy denotes the actual physical distance between device A and device B and Ymea denotes the measured distance. Note that, during each ranging event, whenever Ymea becomes less than Xphy, we call it a false acceptance.

For each practical application, a specific Critical Search Window (CSW) can be defined and consists of a set of timing/distance candidates earlier/shorter than the physical first path. An effective distance-decreasing attack is realized only when one timing/distance candidate within the CSW is recognized and reported. Accordingly, one effective false acceptance event is counted only when the measured/reported distance lies in the CSW (i.e., Ymea $\in$ CSW). Thus, the Effective False Acceptance rate (EFA), EFA $\triangleq$ Prob (Ymea $\in$ CSW), is used to measure the security level. Let α specify the target EFA. A secure ranging receiver needs to be able to ensure Pr (Ymea $\in$ CSW) $\leq \alpha$ in the presence of various attacks as illustrated in Figure 1.

In Figure 1, an example of secure ranging is depicted where device A is the door key and device B is the door lock. Whenever the distance to A measured by B becomes less than 2 meters, B will open. For this protocol to be safe, B needs to ensure that no attacker can reduce the measured distance at B below 2 meters when A is farther away (e.g., more than 20 meters away).

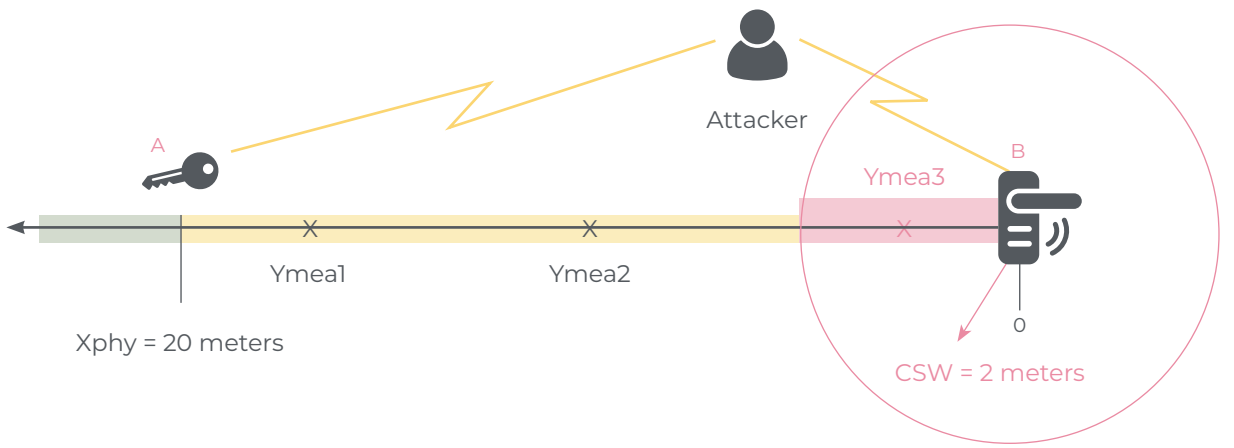

Figure 1

Secure ranging example: Only Ymea3 is counted as EFA since it lies in CSW. The probability of Ymea3 shall be guaranteed small enough. Both Ymea1 and Ymea2 will not sacrifice security since they are outside the CSW.

2.3 Secure Receiver Characteristics

As discussed in previous sections, a secure ranging receiver needs to guarantee that the EFA is lower than a specified target under arbitrary feasible STS attacks. Given that the focus here is on the secure ranging enabled by the STS signal at the physical layer, it is assumed that the attacker has no knowledge about the parameters used to seed the STS pseudo random generator. Other than this, no further constraints are put on the attacker's capabilities. The attacker can only learn the history STS information by listening to the legitimate STS transmission.

Under a specific operating scenario, a particular tradeoff between the detection rate (Pd) and the effective false acceptance rate (Pfa) can be realized for each given receiver by adjusting the corresponding detection threshold or criterion (a.k.a. receiver operating characteristic (ROC) [5]). Note that the detection rate Pd refers to the probability of successfully detecting the timing candidate corresponding to the true physical path. In Figure 2, some exemplary tradeoffs between Pd and Pfa are demonstrated. One secure ranging receiver can ensure that the given secure level is met under all kinds of feasible attacks. On the other hand, if the receiver is not securely implemented, it is likely to violate the specified security level, e.g., α in Figure 2, under some attacking schemes, e.g., Attack Type-2 in Figure 2. Note that Attack Type-1 and Attack Type-2 in Figure 2 can refer to any possible attacking strategies. For example, Attack Type-1 could denote the attack that simply injects random and uncorrelated interference to the channel. On the other hand, Attack Type-2 could denote the attack that adapts the interfering signal according to the knowledge learned from past STS pulses. Note that these types of attacks can be considered "black box" attacks in which the attacker has no apriori knowledge of the transmitted waveform. Attackers with "white box" knowledge (i.e., detailed information about the hardware or software in the receiver) can carry out more sophisticated attacks.

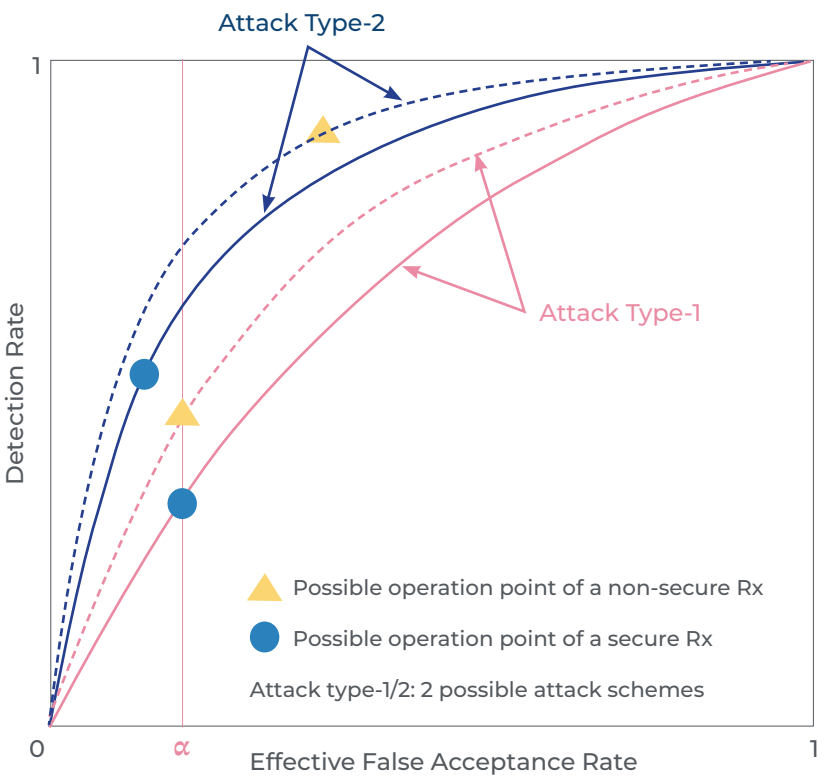

Figure 2

Tradeoff between detection rate and effective false acceptance rate for a secure Rx vs a non-secure Rx

3 Attack Scenarios

The paper by M. Singh et al [3] describes four attacks on High-Rate Pulse (HRP) receivers that could result in incorrect distance measurements due to inaccurate peak correlation on the incoming signal. The first attack is known as Cicada and was introduced in an earlier paper [2]. This attack is meant to exploit the frequency selectivity of typical wireless channels, in which the line-of-sight path (which arrives earliest) may not necessarily be the strongest signal reflection. In Cicada, the attacker transmits a signal comprised of uniformly spaced (in time) pulses which are meant to overlap the desired signal preamble in such a way as to result in the receiver mis-detecting the earliest arriving signal and therefore inaccurately estimating the distance between the desired transmitter and receiver. The attack described in [3] leverages Cicada to produce a new attack known as Cicada++. In the new attack, the attacker injects uniformly spaced pulses time-synchronized to the desired signal but at a fraction of the desired signal repetition frequency. Moreover, the attacker pulses are transmitted at a higher power than the desired signal pulses. If successfully executed, this can result in inaccurate detection of the earliest arriving path at the receiver and potential peak detection of the signal at a time aligned with the attacker repetition frequency.

Another attack described is the ED/LC (early detect/late commit) attack [1]. In this attack, the attacker detects the entirety of a transmitted symbol using the initial part of that symbol (early detect). It then reproduces the detected symbol in a transmitted waveform with a small enough time offset so that the receiver's early path detection is delayed as well – resulting in a measurement inaccuracy. Singh et al propose the Adaptive Injection attack, which is more selective than the ED/LC approach. In this attack, the attacker acts as a relay of the desired signal and can receive the desired signal but does not have to transmit it.

In this manner, the attacker can selectively replace parts of the desired signal in the transmitted waveform, such as with a reduced frequency attack pulse train. This allows the attacker to have more control over the detected peak position.

All four of these attacks require the attacker to stage HRP transmitters in the location where the attack target is located. In this regard, none of these attacks is easily scalable as they require the placement of transmitters in the vicinity of every single HRP receiver that is subject to the attack. Note that co-location adds complexity to these types of attacks; if the target is of sufficiently high value (e.g., access to a secure facility) then co-location may not present a significant obstacle. Moreover, given that all these attacks involve the attacker sending transmitted waveforms, it is critical for the attackers to only transmit when a desired signal is present. In addition, attacks such as ED/LC and Adaptive Injection require detection of the incoming waveform which may not always be feasible given the relative location of the attacker equipment with respect to the transmitter of the desired signal. Particularly for the Adaptive Injection attack, the attacker should be able to effectively block the desired transmitted signal – which requires undetected co-location with the target receiver. Nevertheless, even if such attacks are not easily scalable, they can be attractive depending on the value of the target and therefore should be considered in the design of a secure ranging system.

4 FiRa Standardization and Certification Programs

FiRa standards, along with associated interoperability validation, provide an integral baseline set of specifications that allow for development of a secure UWB ranging system. In particular, three FiRa specifications are discussed in this section along with their roles in establishing secure ranging: the UWB PHY Technical Requirements [4], the UWB MAC Technical Requirements [7], and the Secure UWB Service (SUS) API (Application Programming Interface) [8]. These specifications also have a minimum required conformance level testing that FiRa administers along with interoperability testing.

4.1 UWB PHY Technical Requirements

Although the IEEE 802.15.4 standard already defines the necessary physical layer requirements for UWB that could be used for secure ranging, FiRa defines a profile of this specification which allows vendors to clearly target the minimum necessary functionality to achieve secure ranging. The critical over-the-air data encoding and transmission starts with the scrambled timestamp (STS) sequence. The FiRa UWB PHY specification provides the necessary PHY Protocol Data Units (PPDU) that are required to support STS encoding. As per further discussion in Section 5 of [4], the STS payload is a securitized data block that is essential to provide resiliency to UWB attacks. The corresponding STS conformance procedures are described in Section 5.4 of [8].

4.2 UWB MAC Technical Requirements

The FiRa UWB MAC Technical Requirements documents describe the format of the different frames exchanged between the UWB devices. From security point of view, the following items are the most relevant:

- **Synchronization of the devices via a shared monotonic counter (STSindex)**
- **Generation of the STS**
- **Encryption and authentication of the frames**

A session key shared between both sides of the ranging session is derived into multiple keys and initialization vectors (including the initial value of the STSindex). STSindex is used to synchronize both sides of the transaction and as part of the counters used for STS generation and payload encryption. By keeping track of its value, replay attacks are prevented. Each of the derived keys is dedicated to a specific purpose (e.g., encryption and authentication of the frame, generation of the STS, confidentiality of the STSindex). Encryption, authentication, and key derivation rely on NIST-approved standards.

Depending on the protection level required by the application, 128- or 256-bits session keys can be used, and the rotation rate of some of the derived keys can be adapted.

The FiRa UWB MAC Technical Requirements provide two methods for STS sequence generation: static and dynamic.

In Static STS, cryptographic materials are reused from round to round. Hence no security claims are made for this mode. Pseudo random STS are used here only to protect distance measurements from interference and are used for link-optimized ranging. In other words, static STS is intended to improve measurement accuracy but provides no inherent security.

In Dynamic STS, cryptographic materials are used to generate STS and protect frames change on a per slot basis, following the STSindex counter – which makes it difficult for a third-party to predict the sequence, or replay it later.

This is described in detail in Section 6.4 of [6], and corresponding conformance validation procedures are provided in Sections 3.20 and 4.20 of [9].

4.3 Secure UWB Service API

The FiRa Secure UWB Service (SUS) API specification provides a method for a discrete UWB subsystem to retrieve short term (the duration of a ranging session) critical key material from a secure element. This keying material (the URSK, i.e., UWB Ranging session key) is leveraged as base key material from which all dynamic STS keying is derived. The secure element (SE) is high security assurance, tamper-resistant discrete hardware on which sensitive key derivation, based on long-term secrets, can take place. The UWB subsystem communicates with a secure element via the Secure Channel Protocol (SCP) [10]. SCP is a general-purpose protocol targeted to establish an encrypted tunnel through which all communication between an SE and an Off-Card Entity (OCE) can take place.

Given that the URSK is sent via an encrypted tunnel to the UWB modem, all STS key derivation can take place within the security facilities in the UWB modem itself (e.g., in the UWB modem's root-of-trust). The URSK is retrieved from the SE as part of an overall Ranging Data Set (RDS), by using a command/response protocol via the SCP tunnel (see Figure 3).

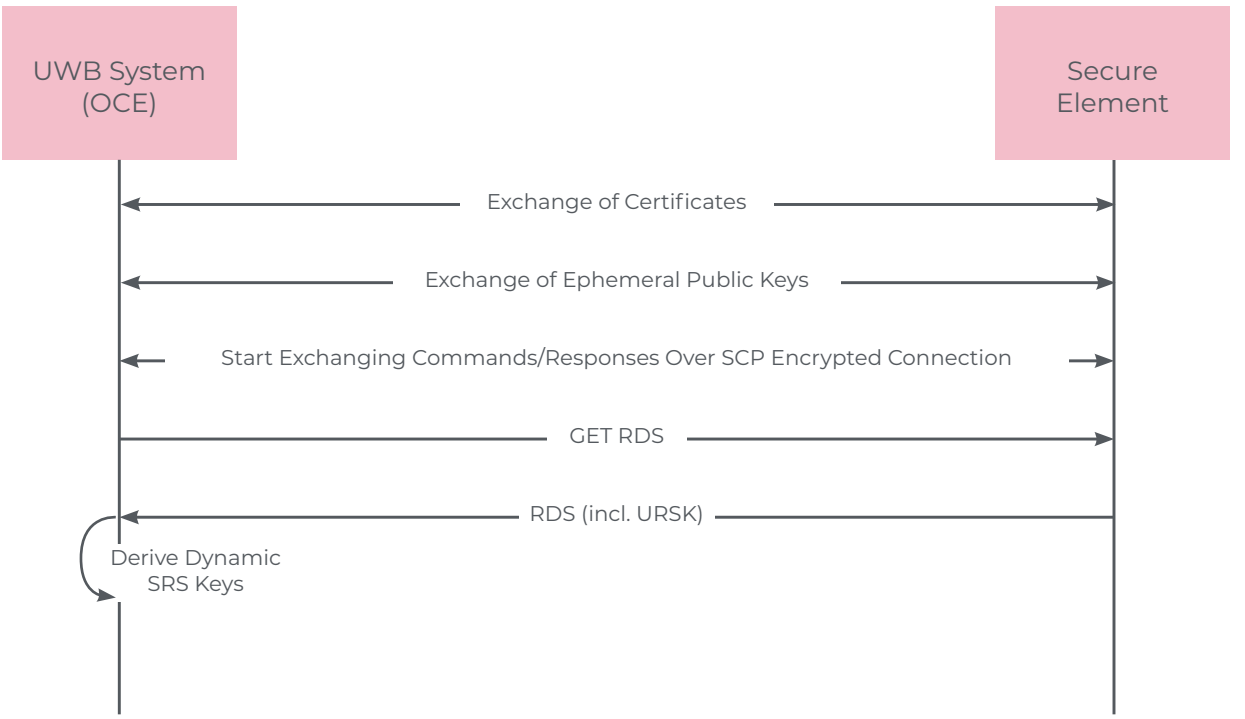

Figure 3

SUS API Message Exchange

5 UWB Modem Implementation Considerations

Secure ranging is done with a few UWB messages being exchanged between an initiator and a responder. The responder is usually the device which authorizes the wireless transaction to be performed (typically lock or unlock a door). The initiator is usually the user's mobile phone which hosts a virtual key application. It is shown in Figure 4, where the ranging flow is a Dual-Side Two-Way-Ranging (DS-TWR) flow. The blue arrows are UWB frames which are used as ranging signals. The receiver device uses the secure timestamp (STS) pattern to securely timestamp the Time-of-Arrival (TOA) of the messages. The black arrow only carries a Measurement Report which is composed of T_{reply2} and T_{round1}.

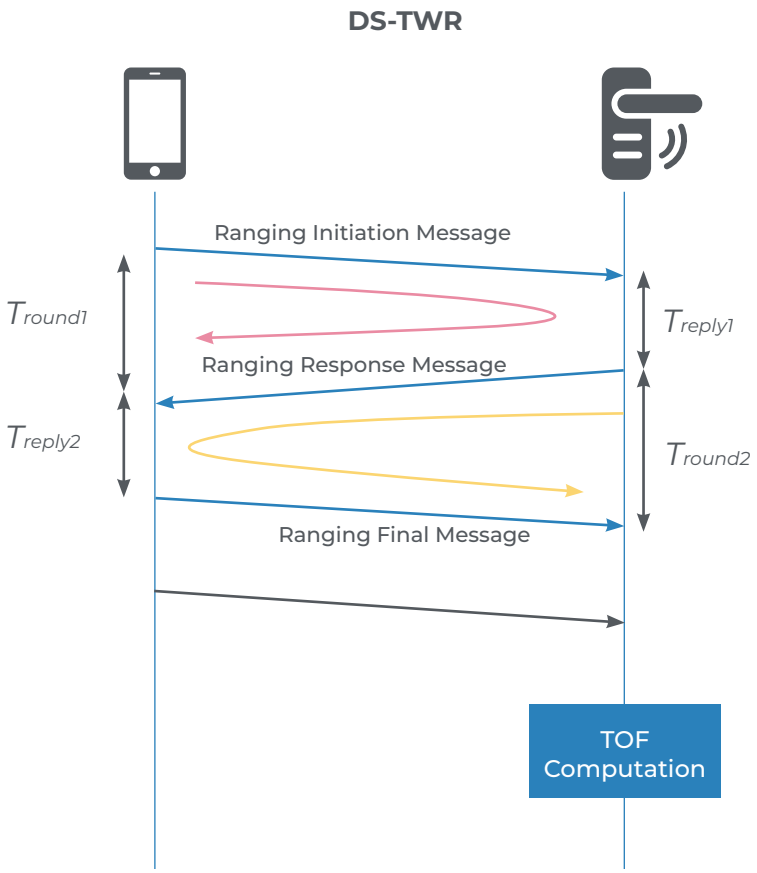

Figure 4
Dual-Side Two-Way-Ranging (DS-TWR) Call Flow

The Time-of-Flight (TOF) between the initiator and the responder is computed by the responder and it is given by Equation 1:

$$DS\text{-}TWR\ TOF = \frac{(T_{\_round1} * T_{\_round2} - T_{\_reply1} * T_{\_reply2})}{(T_{\_round1} + T_{\_round2} + T_{\_reply1} + T_{\_reply2})}$$

Equation 1

If an attacker is close to the receiver (i.e., at a distance such that the attack signal is strong enough to create STS correlation peaks higher than the noise level at the STS correlator output), its attack signal may shift the TOA of The Ranging Initiation Message (RIM) or the TOA of the Ranging Final Message (RFM). It shall be noted that the time of transmission of a Ranging Response Message (RRM) does not depend on the TOA of the RIM, because a FiRa device must transmit at the beginning of its time slot. If the attacker succeeds to shifting the TOA of the RIM, it changes the T_{reply1} value in the above formula. If the attacker succeeds in shifting the TOA of the RFM, it changes the T_{round2} value in the above formula.

The MAC stack on the responder can implement a simple countermeasure. It may also do a Single-Side Two-Way-Ranging (SS-TWR) with the RRM and the RFM (it is the yellow arrow) or with the RIM and the RRM (it is the red arrow). The SS-TWR TOFs are computed by Equation 2 and Equation 3.

$$SS\text{-}TWR\ TOF\ 2 = \frac{(T_{\_round2} - T_{\_reply2})}{2}$$

Equation 2

$$SS\text{-}TWR\ TOF\ 1 = \frac{(T_{\_round1} - T_{\_reply1})}{2}$$

Equation 3

With the Measurement Report Message (MRM), the responder MAC stack has all the information it needs to compute the SS-TWR TOFs and DS-TWR TOF.

If the attacker succeeds in shifting the TOA of the RIM, it can alter the DS-TWR TOF; but the SS-TWR TOF2 is not altered. If the attacker succeeds in shifting the TOA of the RFM, it alters the DS-TWR TOF but not the SS-TWR1. By comparing the TOF values, the responder can easily detect that the legitimate signal is overlapped with an attack signal which attempts to shift the TOA of the received ranging messages.

If the attacker succeeds in shifting the TOA of the RRM by dt, both SS-TWR TOF and DS-TWR TOF are shifted by dt/2. In this case, the responder can't detect that an attacker is altering the ranging. But it is not a real concern because the attacker must be physically close to the initiator and not to the responder (i.e., at a distance such the attack signal is strong enough to create STS correlation peaks higher than the noise level).

There is a second countermeasure which either the responder or the initiator MAC stack can easily implement. The UWB PHY Synch header can also be used to timestamp the TOA of RIM, RRM or RFM. When RIM or RRM or RFM is received, the MAC stack can compare the TOA computed with the STS pattern (TOA_{sts}) and the TOA computed with the UWB PHY header (TOA_{sync}). If they diverge, the UWB stack can reject the TOA and abort the ranging.

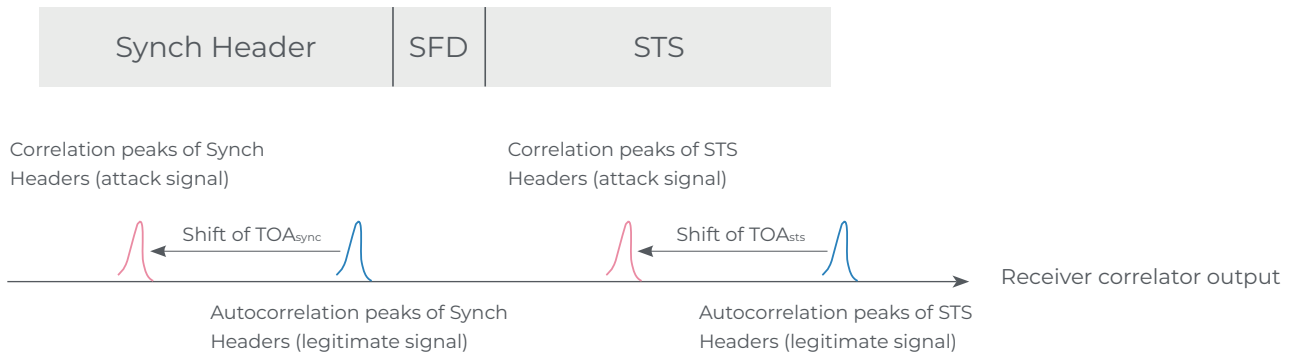

Figure 5

STS Correlation At Receiver

The UWB PHY Synch header is a known pattern (or the set of patterns is very limited). Therefore, an attacker may determine an attack pattern over the PHY Synch header so that it controls the TOA_{synch} shift. But since the STS pattern is a-priori unknown by the attacker (with Dynamic STS), the attacker can't control the TOA_{sts} shift for this attack. The attacker could intercept the UWB message, analyze the STS pattern and attempt multiple attack patterns so that the TOA_{sts} shift (when it succeeds) matches with the targeted TOA_{synch} shift. Then it can replay the legitimate UWB signal overlapped by the attack signal. However, any UWB receiver expects the UWB signal within a 10µs window. Therefore, such a complex attack must be carried out in less than 10 µs, which is unrealistic (see Figure 5).

Both countermeasures (compare DS-TWR TOF with SS-TWR TOF and compare TOA on STS pattern and on PHY Synch pattern) can of course be combined to increase the likelihood to detect a physical layer attack.

6 Conclusions

Accurate distance measurement is possible using IR-UWB, and security features defined in the FiRa specifications allows for resiliency against attacks that seek to corrupt the distance measurement as determined at the two endpoints of any ranging session. By ensuring that the critical part of the UWB over-the-air transmission payload is protected using dynamic key material, a FiRa-compliant UWB implementation can provide the essential components for a secure ranging solution. In addition, proper UWB receiver design can ensure that such an implementation can provide security assurances that simpler modem algorithmic design would not. FiRa conformance specifications and interoperability testing programs also form an integral part in inspiring confidence in FiRa-compliant products. FiRa specifications support a scalable security architecture based on use case needs. Some use cases require no or low security while other use cases require a higher level of security. The FiRa specifications support different security levels, but even the lower levels of security will provide resilience against the types of attacks described in this paper.

7 References

[1] M. Flury et al. “Effectiveness of Distance-Decreasing Attacks against Impulse Radio Ranging”. Proceedings of the Third ACM Conference on Wireless Network Security. 2010. pp. 117-128.

[2] M. Poturalski et al. “Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures”. IEEE Transactions on *Wireless Communications*. Vol. 10. No. 4. 2011. pp. 1334-1344.

[3] M. Singh et al. “Security Analysis of IEEE 802.15.4z/HRP UWB Time-of-Flight Distance Measurement”. *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. June 2021. pp. 227-237.

[4] FiRa Consortium UWB PHY Technical Requirements, version 1.3.0.

[5] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Upper Saddle River, NJ, USA: Prentice Hall, 1998.

[6] FiRa Consortium MAC Technical Requirements, version 1.3.0.

[7] FiRa Secure UWB Service API, version 1.0.0.

[8] FiRa Consortium UWB PHY Conformance Test Specification, version 1.1.0.

[9] FiRa Consortium MAC Conformance Test Specification, version 1.1.0.

[10] Global Platform Technology. Secure Channel Protocol 11. Version 1.2. July 2018. https://globalplatform.org/wp-content/uploads/2017/09/GPC_2_3_F_SCP11_v1.2_PublicRelease.pdf.

The Power to Be Precise