Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: Ranging Integrity with HRP STS

Date Submitted: May 2023

Source: Xiliang Luo, Vinod Kristem, Moche Cohen (Apple)

Address: One Apple Park Way, Cupertino, CA 95104, USA

E-Mails: xiliang_luo@apple.com

Abstract: More results about the ranging integrity with the STS waveform.

Purpose: Highlight that STS waveform also enables quantifiable ranging integrity.

PAR Scope

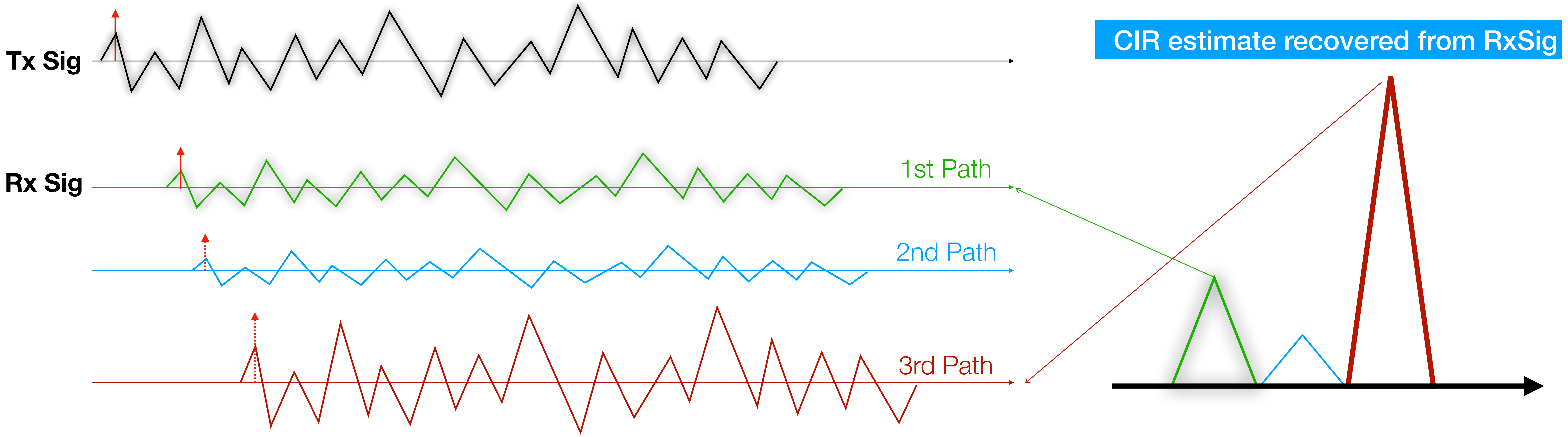
PAR Objective	Proposed Solution (how addressed)
Safeguards so that the high throughput data use cases will not cause significant disruption to low duty-cycle ranging use cases	
Interference mitigation techniques to support higher density and higher traffic use cases	
Other coexistence improvement	
Backward compatibility with enhanced ranging capable devices (ERDEVs)	
Improved link budget and/or reduced air-time	
Additional channels and operating frequencies	
Improvements to accuracy / precision / reliability and interoperability for high-integrity ranging	Ranging integrity with STS waveform: clarifications
Reduced complexity and power consumption	
Hybrid operation with narrowband signaling to assist UWB	
Enhanced native discovery and connection setup mechanisms	
Sensing capabilities to support presence detection and environment mapping	
Low-power low-latency streaming	
Higher data-rate streaming allowing at least 50 Mbit/s of throughput	
Support for peer-to-peer, peer-to-multi-peer, and station-to-infrastructure protocols	
Infrastructure synchronization mechanisms	

Introduction to Ranging with STS

Ranging and CIR Estimation

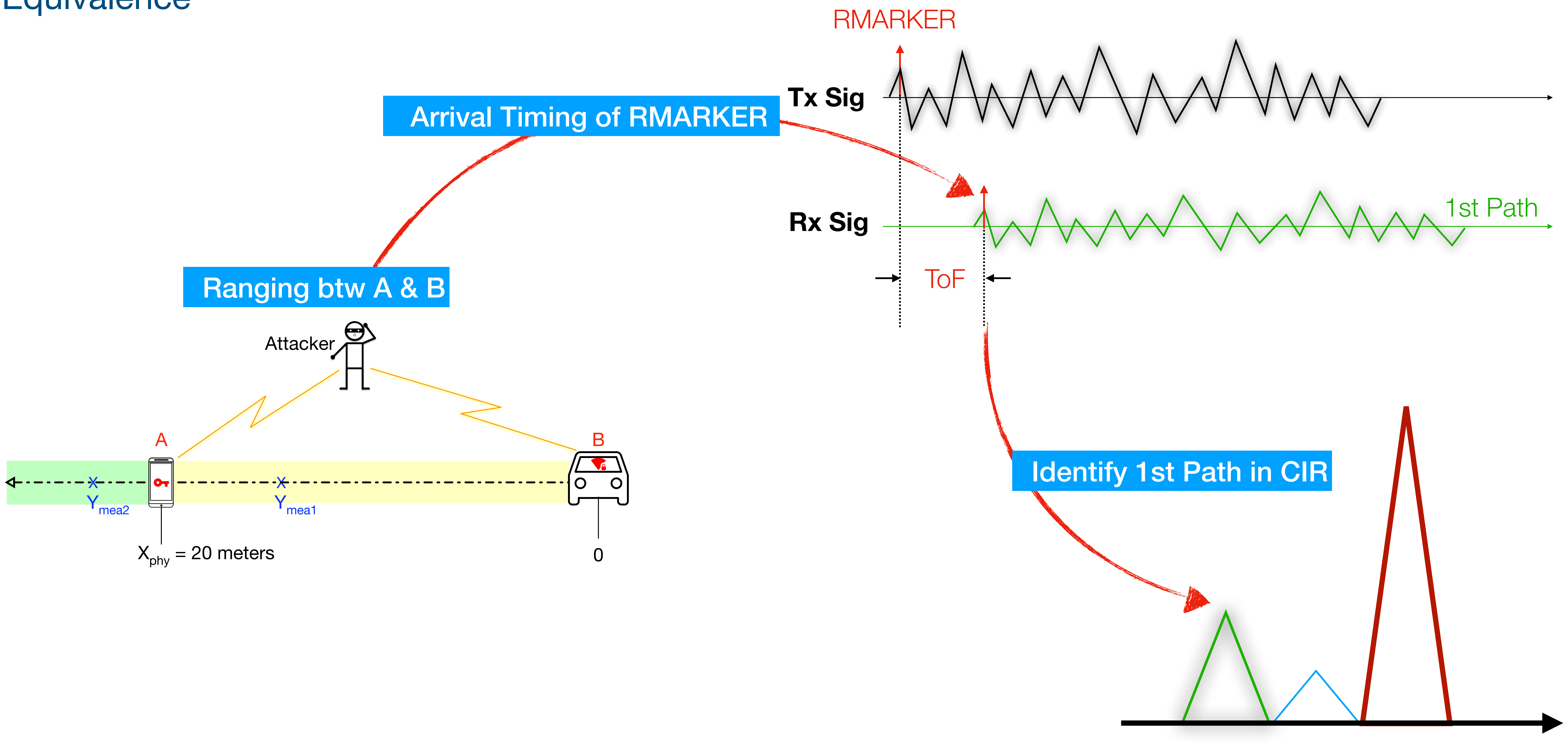
First-Path Arrival Timing at Receiver

- Receiver needs to figure out **the arrival timing of the RMARKER in the received STS packet**
  - Record the timestamps for the arrival timing of the RMARKER in the received packet and the departure timing of the RMARKER in the transmitted packet
  - The round-trip times and the reply times are derived with the recorded timestamps
- The **first path in the estimated channel impulse response (CIR)** at the receiver is mapped to the arrival timing of the RMARKER



Ranging → ToF → RMARKER → CIR

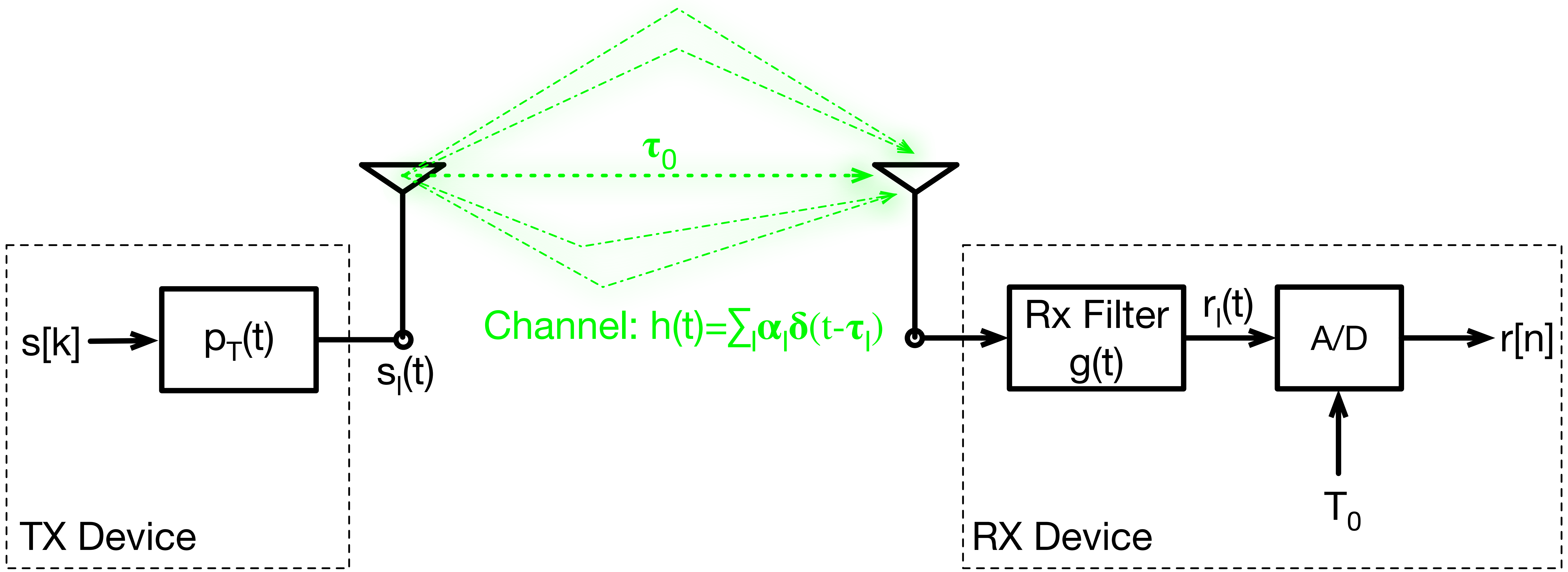
Equivalence



Secure Ranging: **Definition** and **Attacks**

System Model

From TX to RX



STS waveform: $s_l(t) = \sum_{k=0}^{Q-1} s[k]p_T(t - k \cdot L\mathrm{T_c})$

$\mathrm{T_c}$: chip duration (about 2ns)

$L = 4$ or 8: spreading factor in 4z HRP

$$r_l(t) = \sum_{k=0}^{Q-1} s[k]q_R(t - k \cdot L\mathrm{T_c}) + w(t)$$

$$q_R(t) := p_T(t) * h(t) * g(t) = \sum_l \alpha_l q_r(t - \tau_l)$$

$$r[n] := r_l(nT_0) = \sum_{k=0}^{Q-1} s[k]q_R[n - kM] + w[n]$$

Secure Ranging

Definition

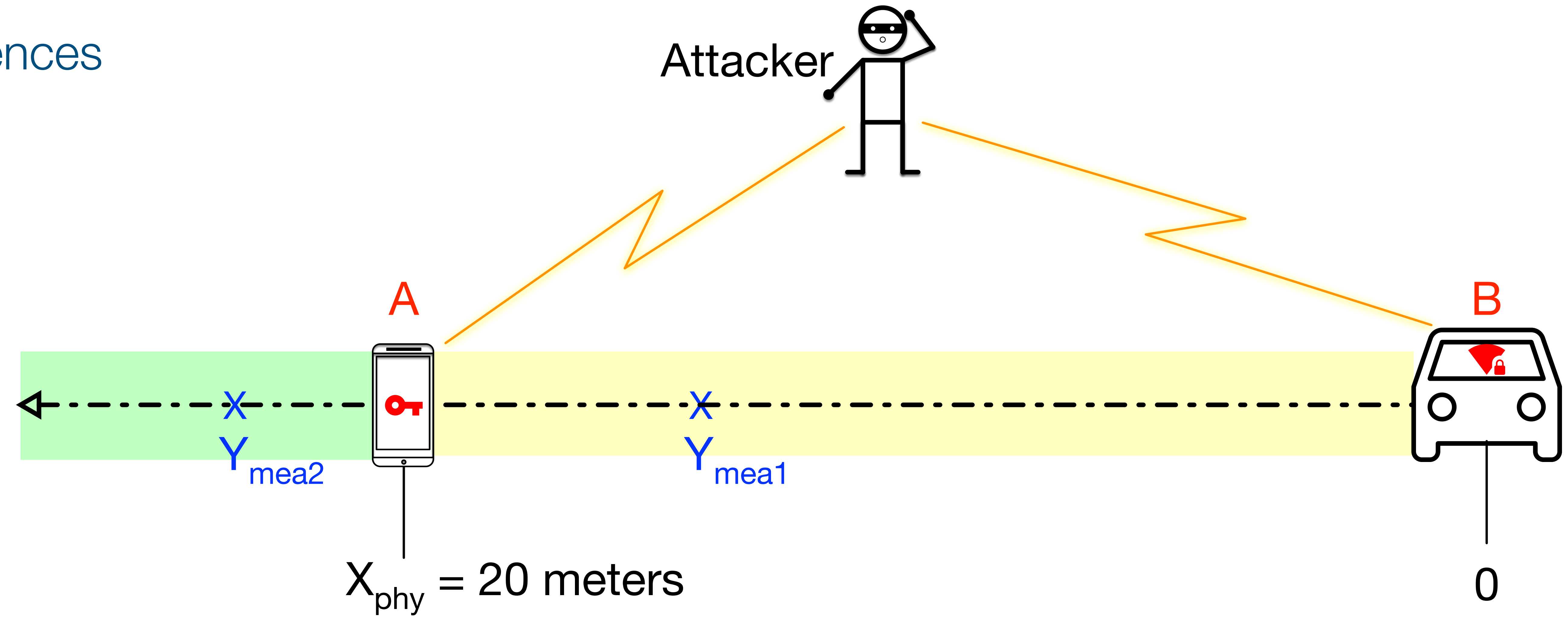
The ranging receiver at the RXD **is secure only if** it **ensures** that a given timing estimate η is accepted with a probability no more than a prescribed value whenever it is earlier than $\tau_0 - \Delta$, i.e.,

$$\Pr(\text{Accept } \eta \,|\, \eta < \tau_0 - \Delta) \leq \rho$$

where

- τ_0 is the true timing of the first path
- Δ is a constant representing the amount of allowed implementation headroom
- ρ is the prescribed upper bound on the false acceptance rate
- the probability is with respect to all random STS sequences

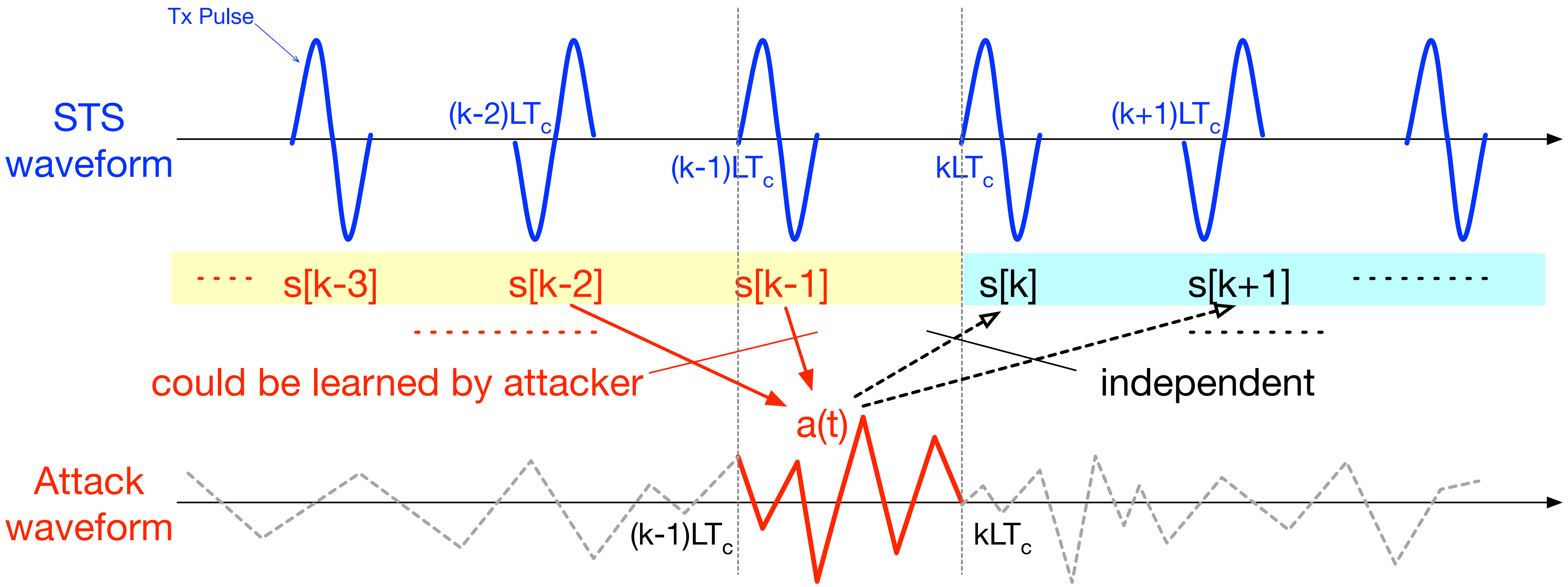
This security guarantee also applies to the cases where arbitrary feasible attacks try to advance the timing estimate by manipulating the STS ranging waveform from the TXD.



Feasible Attack

Definition

- An attack to the STS ranging waveform **is feasible only if** this attack does not utilize any non-causal information from the cryptographic STS sequence at any time
  - In other words, $\forall k$, at any time within the interval $((k-1)L\mathrm{T}_c, kL\mathrm{T}_c)$, a feasible attack to the STS waveform can only learn information about $\{s[n] \,|\, n \leq k-1\}$ and is unable to make any inferences about $\{s[n] \,|\, n \geq k\}$
- Let $a(t)$ represents the time-domain attack waveform generated by an attacker
  - The attack to the STS waveform **is feasible only if** $a(t)$ is independent of $\{s[n] \,|\, n \geq k\}$, $\forall t < kL\mathrm{T}_c$ and $\forall k$

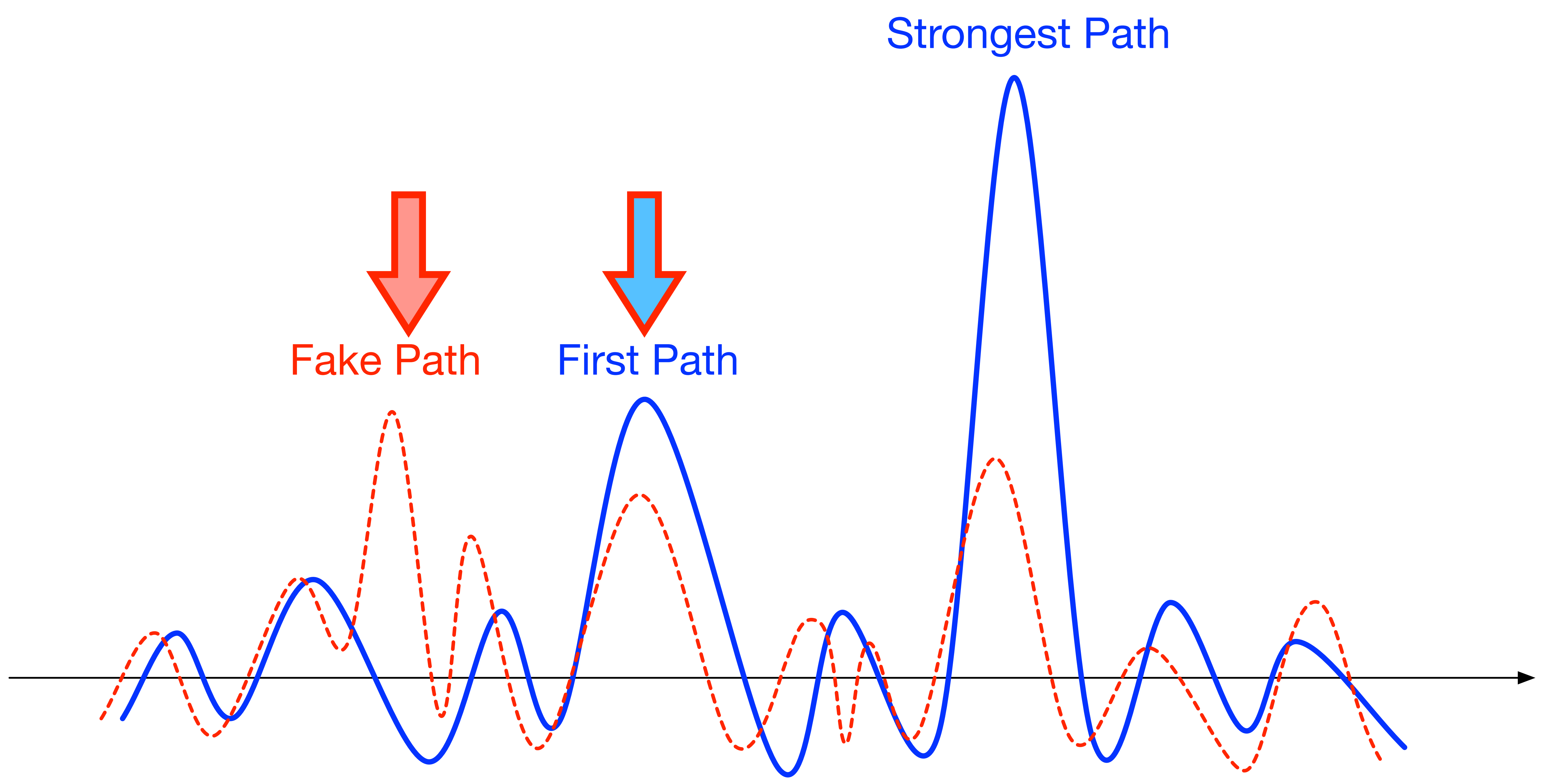


A Reference STS Receiver with **Proved Security**

STS Receiver

Hypothesis Detection

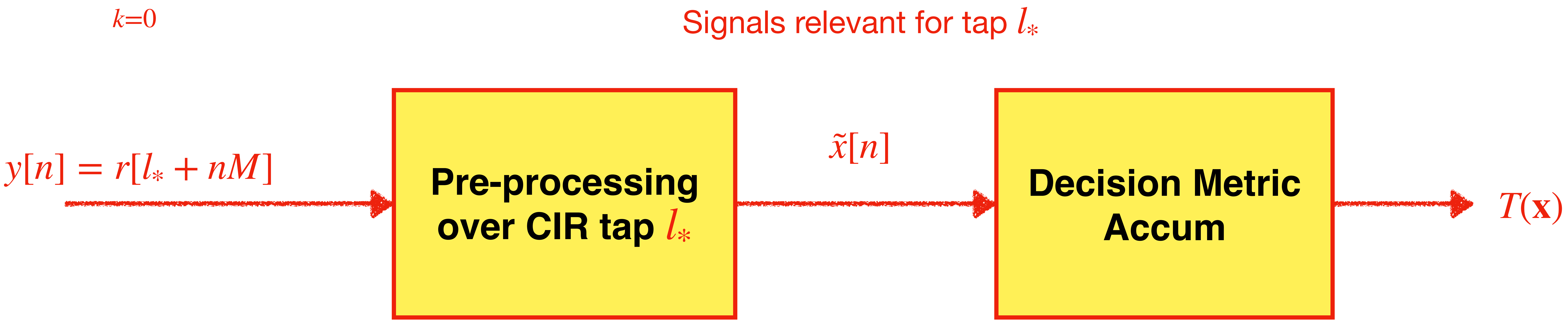
- After observing the STS signal
  - RXD first obtains **an estimate of the CIR**
    - either with the SYNC or with the STS
  - then the RXD identifies a particular tap as **a first path candidate**
  - the next task is to **either accept** it as a true physical path **or reject** it
- In the case of attack
  - there could be **fake peaks in the estimated CIR** that are earlier than the true first path
  - a secure STS receiver need to reject any fake peak earlier than the true first path reliably
- **Two hypotheses** when validating a particular CIR tap l_*:
  - $\mathscr{H}_0$: tap l_* does not corresponds to any true physical path
  - $\mathscr{H}_1$: tap l_* is a real physical path



A Reference STS Receiver

High Level View

$$r[n] := r_l(nT_0) = \sum_{k=0}^{Q-1} s[k]q_R[n - kM] + w[n]$$



Proof of Security

Tap l_* Earlier than True 1st Path

- When the **CIR tap l_* is earlier than the first path**, the received signal under $\mathscr{H}_0$ becomes
  - $y[n] = \dot{w}[n] + y_{\text{legit}}[n]$

  where
  - $y_{\text{legit}} := \sum_{\zeta>0} q_R[l_* + \zeta M] s[n-\zeta]$, $\dot{w}[n]$ models both the adversarial attack and the additive noise
  - feasible attack: the received waveform from the attacker at time n, i.e., $\dot{w}[n]$, is independent to the STS sequence starting from time n, i.e., $\{s[k] \,|\, k \geq n\}$

When validating a CIR tap l_* that is earlier than the true physical first path, the false acceptance rate of the reference STS receiver is upper bounded as

$$\Pr(\text{Accept } l_*) = \Pr(T(\mathbf{x}) \geq \gamma) \leq \exp\left(-\frac{\gamma^2}{2}\right)$$

Meanwhile, the upper bound is valid under arbitrary feasible attacks.

Detection Performance

Tap l_* Corresponding to True 1st Path

- When the **CIR tap l_* corresponds to the true first path**, we have
  - $\tilde{x}[n] = q_R[l_*]s[n] + \tilde{w}[n]$

  where $\tilde{w}[n]$ models both the additive noise and the interference. Then we can also have
  - $x[n] = \mathbb{Q}\left(\hbar s[n] + \bar{w}[n]\right) = \mathrm{E}[x[n]\,|\,s[n]] + e[n] := \mathbb{M}(s[n]) + e[n]$

  where $\mathbb{M}(s[n])$ is the conditional mean estimate of $x[n]$ and $e[n]$stands for the estimation error with a zero mean

Assume the estimation error $e[n]$ is uncorrelated with $s[n]$ conditioned on the past samples $\{x[k]\}_{k<n}$ and the past STS $\{s[k]\}_{k<n}$. When validating a CIR tap l_* corresponding to a true physical path, the miss rate of the reference receiver can be upper bounded as

$$\Pr(\text{Reject } l_*) = \Pr(T(\mathbf{x}) < \gamma) \leq \exp\left(-\frac{Q\left(\bar{C} - \gamma/\sqrt{Q}\right)^2}{2}\right)$$

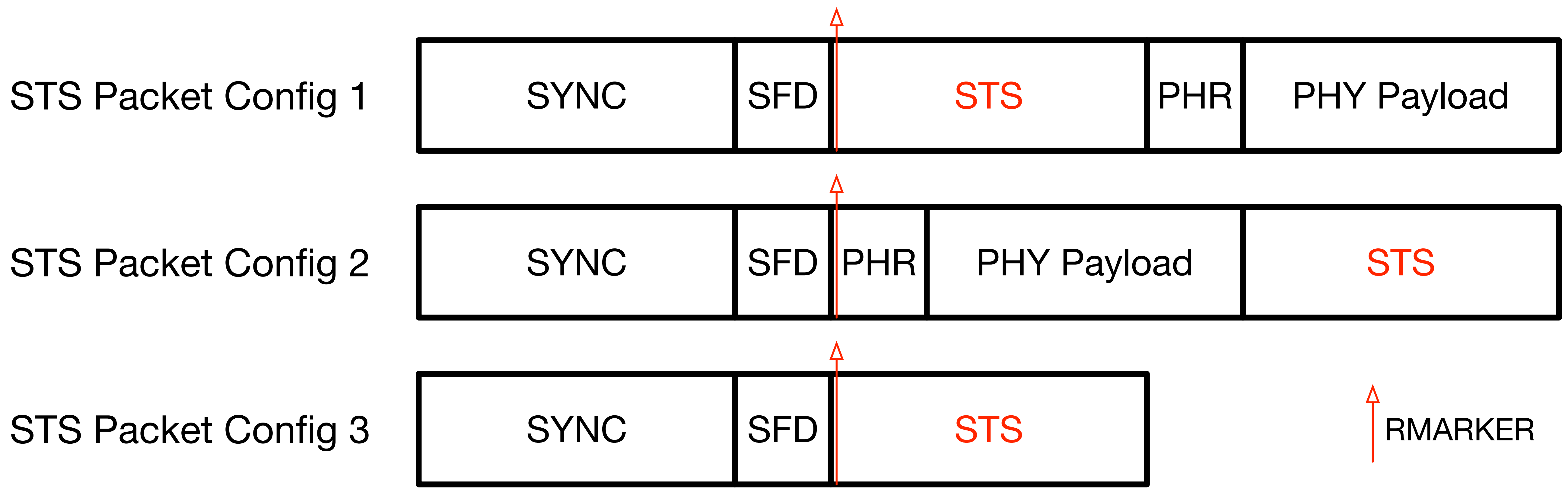
where $C_n := \mathrm{E}[\mathbb{M}(s[n])s[n]]$, $\bar{C} := \sum_{n=0}^{Q-1} C_n/Q$, and $\bar{C}$ or Q is large enough such that $\bar{C} > \gamma/\sqrt{Q}$.

Backup Slides

IEEE 802.15.4z HRP UWB

STS and RMARKER

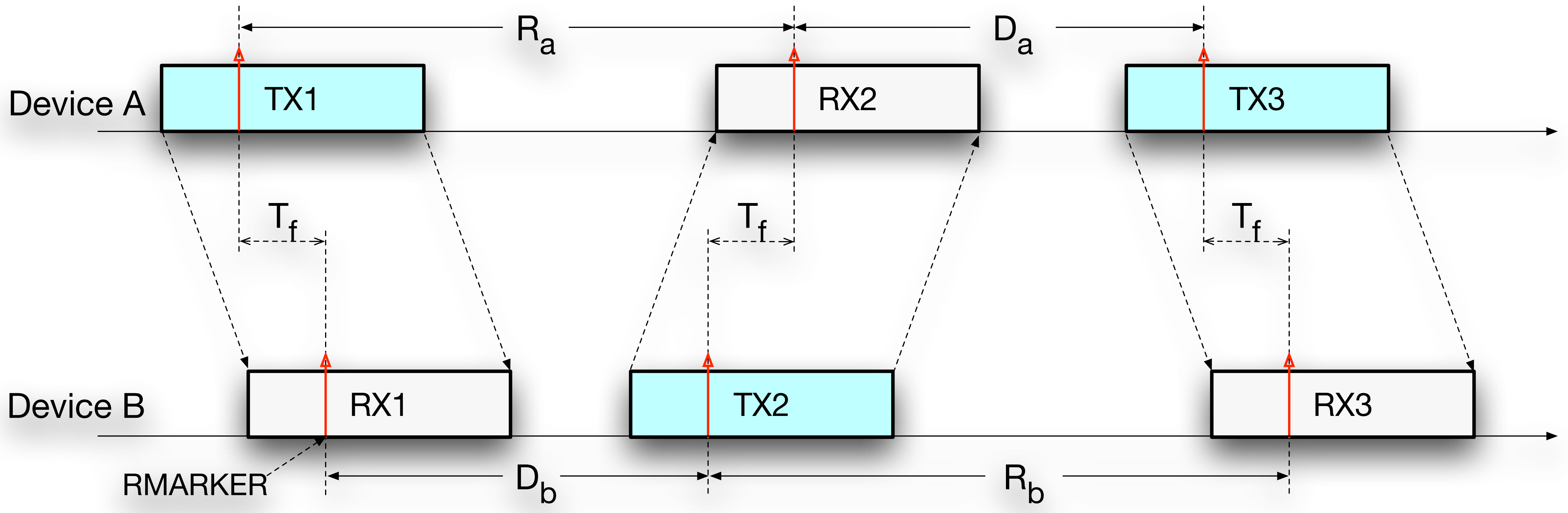
- **SYNC** (Synchronization):
  - initial packet acquisition, timing and frequency synchronization, and channel estimation
  - SYNC portion includes a repetition of a ternary preamble code that exhibits an ideal auto-correlation function
- **STS** (Scrambled Timestamp Sequence):
  - the STS portion consists of a sequence of uniformly spaced pulses with pseudo-random polarities that are generated by applying the AES-128 engine in counter mode
- **RMARKER** (Ranging Marker):
  - the time when the peak of the (hypothetical) pulse associated with the first chip following the SFD is at the local antenna
  - all reported times during ranging are measured relative to the RMARKER.



Double-Sided Two-Way Ranging

DS-TWR

- **With respect to the RMARKERs**, both Device A and B measure the following times
  - **Round-trip** times:
    - $\hat{R}_a = k_a R_a$ (packet TX1)
    - $\hat{R}_b = k_b R_b$ (packet TX2)
  - **Reply** times:
    - $\hat{D}_a = k_a D_a$ (packet TX2)
    - $\hat{D}_b = k_b D_b$ (packet TX1)



- **IEEE formula** to obtain the ToF estimate

$$\hat{T}_f = \frac{\hat{R}_a \cdot \hat{R}_b - \hat{D}_a \cdot \hat{D}_b}{\hat{R}_a + \hat{R}_b + \hat{D}_a + \hat{D}_b}.$$

- The **relative error** in the ToF estimate

$$\frac{\hat{T}_f - T_f}{T_f} \approx \frac{(k_a - 1) + (k_b - 1)}{2}.$$

✓ Device A clock frequency to ideal clock ratio: k_a

✓ Device B clock frequency to ideal clock ratio: k_b

✓ Ground-truth times: R_a, R_b, D_a, D_b
  - $R_a = D_b + 2T_f$
  - $R_b = D_a + 2T_f$