Security Analysis of Ranging Protocols: UWB and Bluetooth Channel Sounding

Sultan Qasim Khan

May 21, 2025 – Escar USA

Together we're creating a more secure digital future

About me

- Hardware and Embedded Systems (HES) practice lead for North America at NCC Group
- Based in Waterloo, Ontario, Canada
- Creator of Sniffle and Sniffle Relay
- Wireless communications aficionado
- Car enthusiast

What are ranging protocols?

- Ranging protocols are radio protocols defining procedures to estimate or measure distance between devices.
- Commonly used for many applications:
  - Automotive passive entry and passive start (PEPS)
  - Building access control
  - Asset tracking and locating items
  - Indoor location systems
  - Collision avoidance in machinery

How do ranging protocols work?

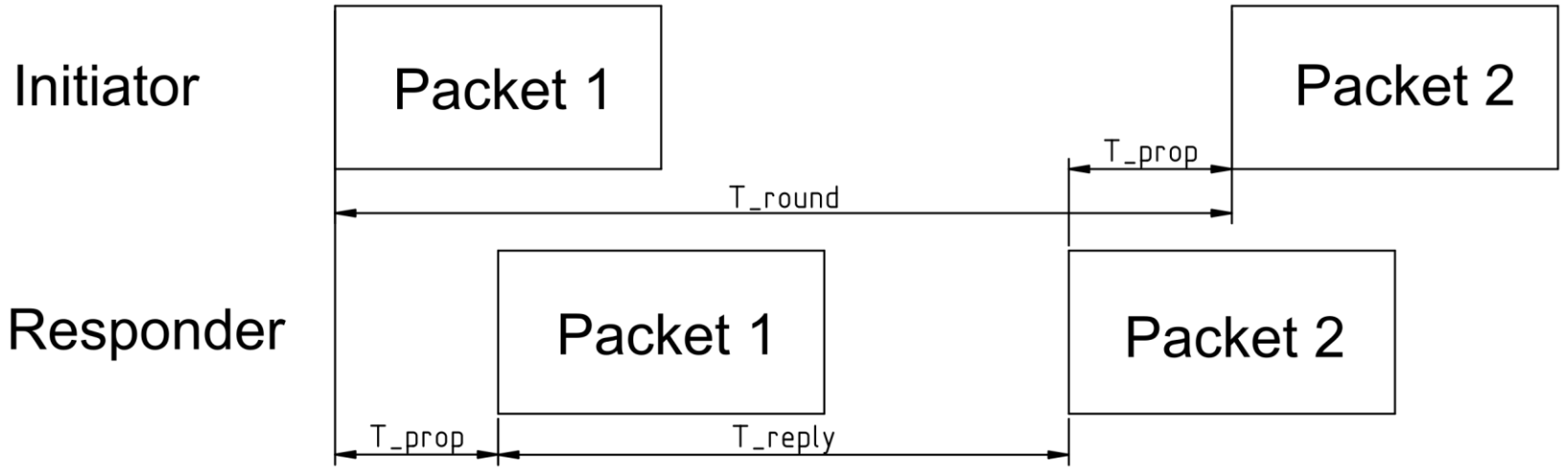
- Several possible approaches, and some protocols combine them
- Signal path loss (RSSI-based ranging)
- Message response timing
- Phase shift in “reflected” tones
  - “Reflected” tones are actively transmitted by devices at a known phase offset from received tones
- Triangulation using angle of arrival
  - Based on phase difference between multiple antennas

Path loss manipulation

- Relay or amplify message to reduce perceived distance
- Attenuate signals to increase perceived distance
- Quite simple to carry out, even unintentionally
  - Human bodies usually attenuate signals passing through
  - Clothing and objects may attenuate or reflect signals
  - Reflective RF dishes can focus (i.e., passively amplify) received signals
- While path loss ranging simple to implement, path loss is not a reliable or accurate measure of distance

Ping-pong exchange timing

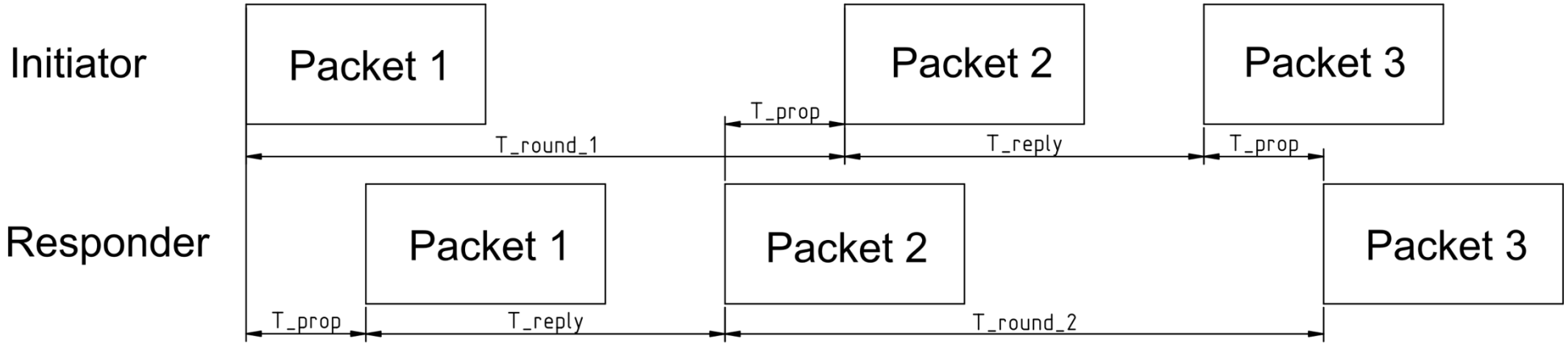
- Known as Single-Sided Two-Way Ranging
- Basis of time-of-flight based ranging methods



$$d = \frac{c}{2}(T_{round} - T_{reply})$$

Double-Sided Two-Way Ranging

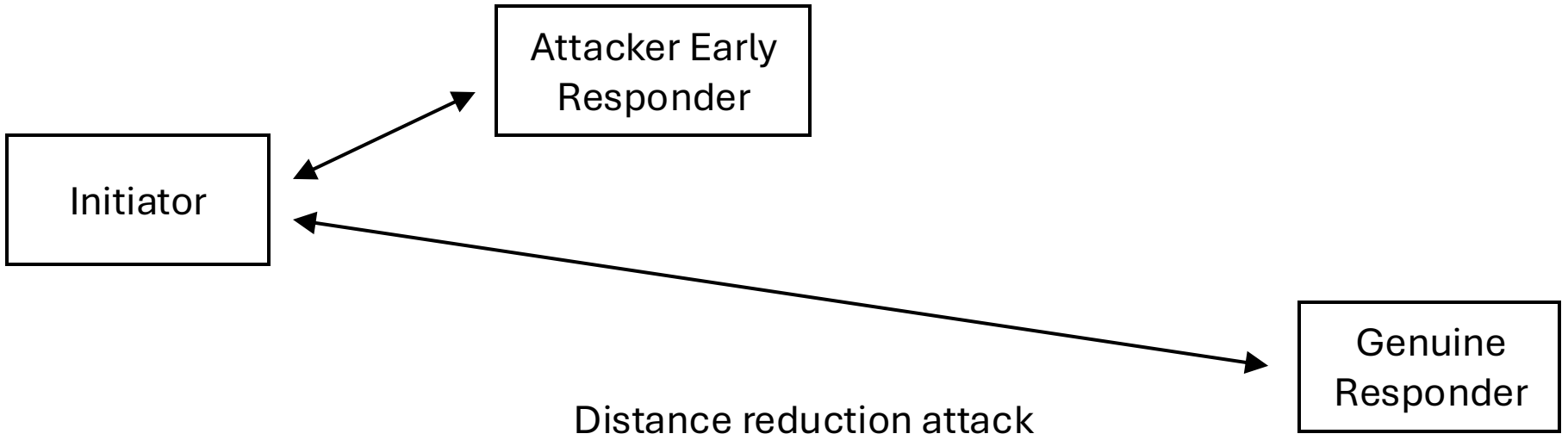
- Commonly, bidirectional ranging operations are performed, and the results are combined
- Large discrepancies between the two ranging operations can be indicative of an attempted attack



$$d = \frac{c}{4}(T_{round\_1} + T_{round\_2} - 2 \cdot T_{reply})$$

Response timing manipulation

- Nearby attacker can respond to ping sooner to reduce perceived distance
- Jam legitimate responses and respond to ping late to increase perceived distance



Multi-carrier phase-based ranging

- Initiator and reflector send each other tones and measure received tone phase relative to their local oscillators
- Reflector notifies initiator of phase difference between received and transmitted signals – this is subtracted from the phase difference measured at the initiator
- When plotting frequency vs. phase difference at multiple frequencies, the slope is proportional to the distance between devices

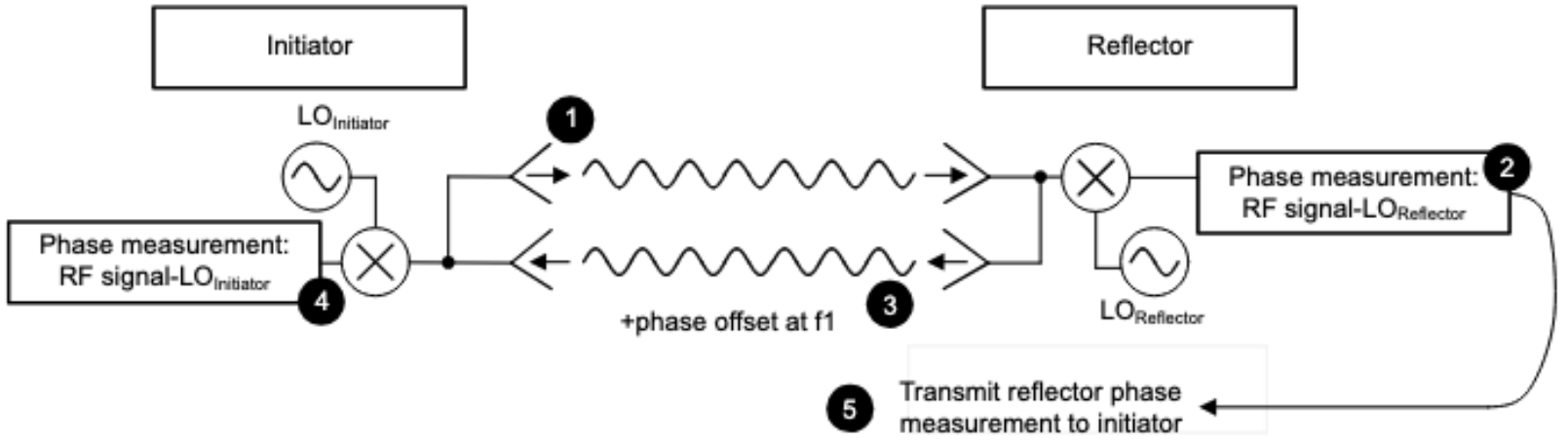
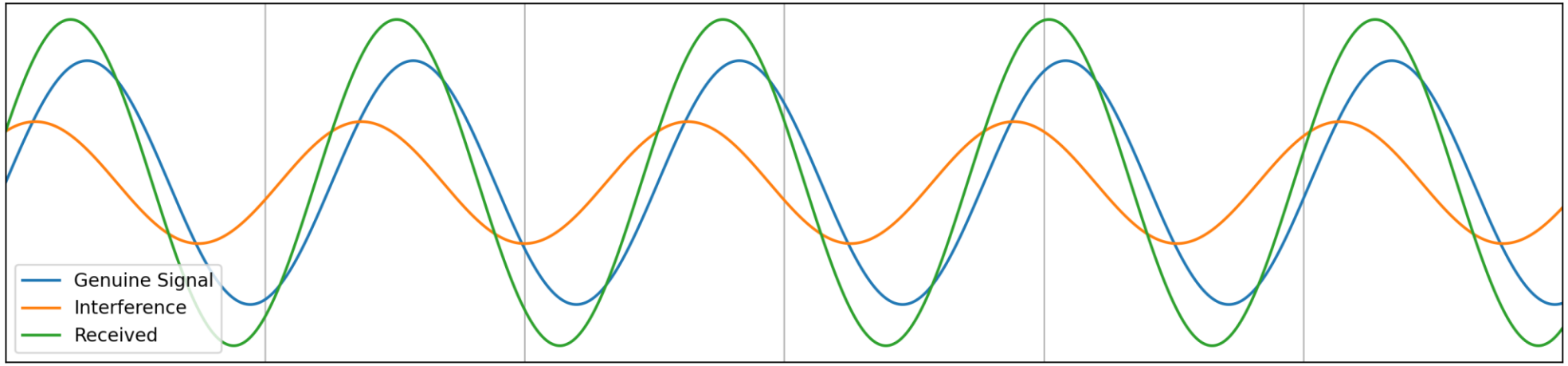


Diagram credit:
Texas Instruments SWRA791

Phase manipulation

- Interference at a matching frequency can alter the received phase
- One can also just transmit arbitrary tones (as phase-based ranging is generally unauthenticated)



Interference altering received signal phase

Secure ranging (distance bounding)

- By combining time-of-flight measurement with cryptography, it is possible to build a system that can theoretically prove that devices are **no more** than some distance apart
- Attackers can still make devices appear further apart than reality through delayed responses
- Basic example – cryptographic challenge/response with response time measurement

Secure ranging protocols

- Most popular secure ranging protocol: 802.15.4z High-Rate Pulse (HRP) Ultra Wide-Band (UWB)
  - Used by AirTags and CCC Digital Key 3.0
- New alternative: Bluetooth Channel Sounding
  - Introduced with Bluetooth Core Specification 6.0
  - Supported by several chips and Android 15, but not yet widely used
  - Likely to gain widespread adoption due to the popularity of Bluetooth
- Other protocols also exist, but are outside the scope of this talk

802.15.4z HRP UWB principles

- Uses UWB pulses with modulation of burst timing and polarity
- Ranging measures propagation time in a ping-pong exchange
- Frames contain a pseudorandom cryptographically generated sequence known as the Scrambled Time Sequence (STS)
  - Generated with an AES-based pseudo-random number generator (PRNG) using negotiated keys and an incrementing counter
  - Frames received with an incorrect STS are rejected

HRP UWB ERDEV physical layer

- UWB uses short pulses with broad spectral content rather than modulating a single carrier frequency
  - Very low power spectral density at any one frequency
  - Pulses can be detected by broadband receivers
- Pulses sent in bursts with a coded ternary sequence
  - Used as DSSS chips
  - Pulse Repetition Frequency (PRF) determines time between pulses
- Burst timing and polarity is modulated
  - Two possible time slots to transmit a burst during one symbol
- Frames consist of preamble, start of frame delimiter (SFD), and STS
  - Frames can also have a payload and associated PHY header

802.15.4z HRP UWB frame format

- Frames consist of:
  - Preamble - sequence of repeated symbols
  - Start of Frame Delimiter (SFD) – fixed sequence of varied symbols
  - Scrambled Time Sequence (STS) – pseudo-random, changes
  - PHY header and payload – optional
- Preamble and SFD are used to synchronize receiver
- STS used to prove authenticity of transmitter
- Frame timestamp may be determined by cross correlating the received STS signal with the expected and selecting the earliest peak – specific approach not well defined by specification

Breaking the theoretically unbreakable

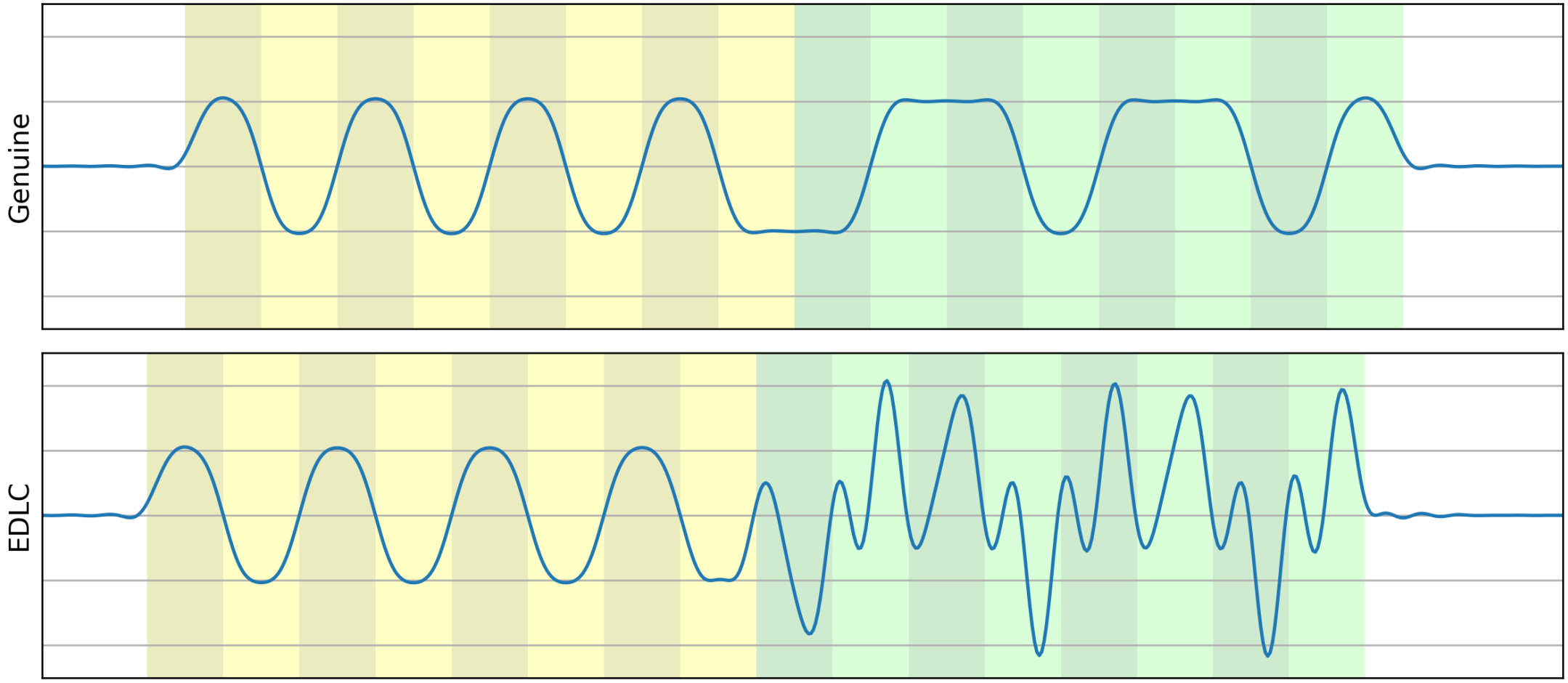
- Secure ranging protocols are theoretically secure at the MAC layer, but confusion at the physical layer may be possible
- Physical layer must handle interference and multi-path signal propagation, but specific rules to handle these securely are not defined by the 802.15.4z specification
- Specially crafted interference can manipulate estimated frame receipt times without altering the perceived value of the STS
- All published attacks against 802.15.4z HRP UWB secure ranging rely on physical layer manipulation

Early Detect Late Commit (EDLC)

- First proposed in 2006 [1], this strategy involves:
  1. Transmitting an ambiguous symbol that will be detected by the receiver early (e.g., runt pulse or weakly modulated signal)
  2. Altering the transmitted signal part way through to commit the symbol to a particular value once the correct value becomes known
- Allows making a receiver's perceived symbol start time earlier without corrupting the perceived value
- Used when the correct value to be transmitted is initially unknown to the attacker, and discovered part way through the attacker's transmission of the ambiguous symbol

[1] Jolyon Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," *Lecture notes in computer science*, pp. 83–97, Jan. 2006, doi: https://doi.org/10.1007/11964254_9.

EDLC example

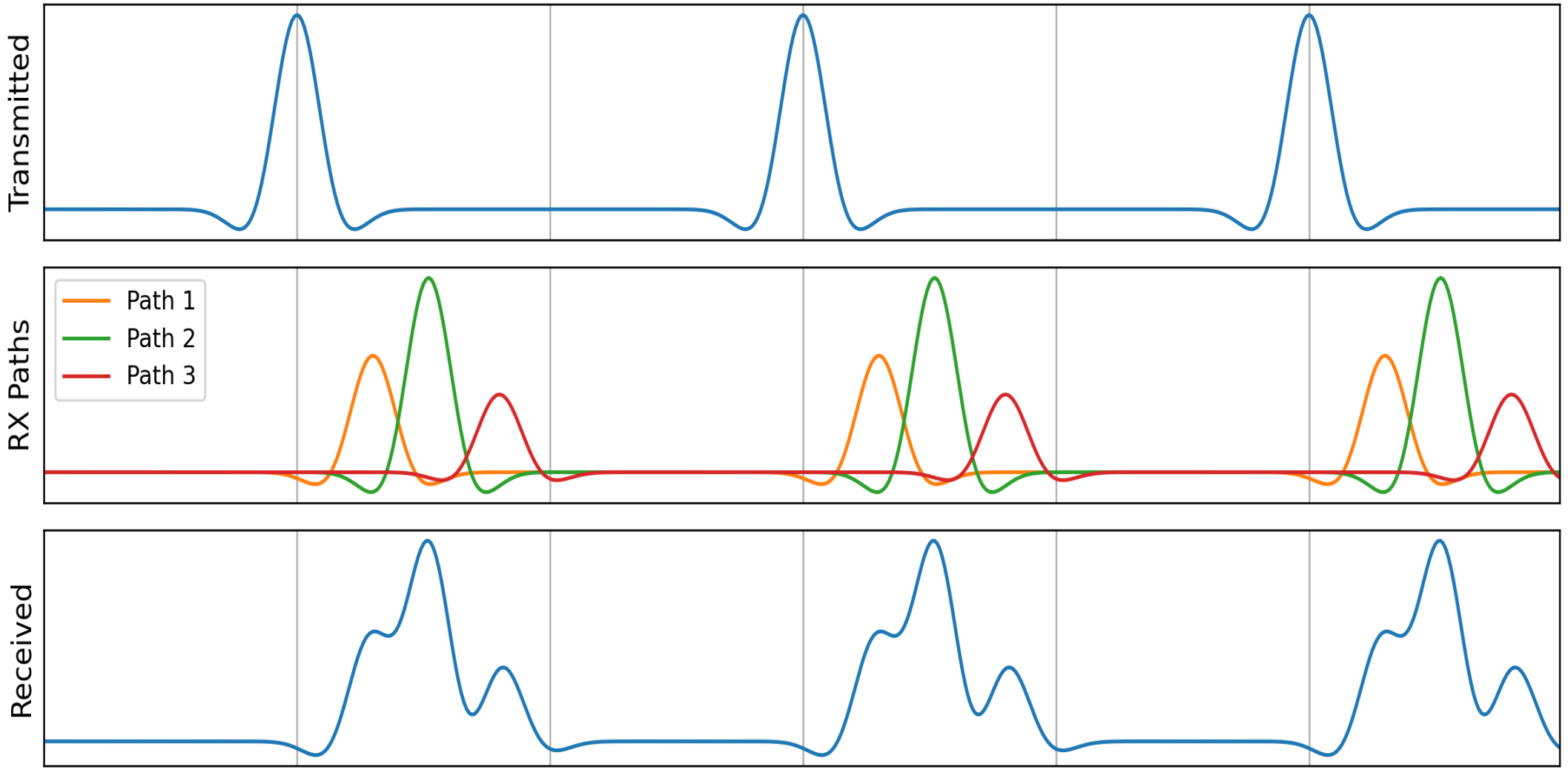


EDLC attack waveform with 8-bit preamble (yellow) and 8-bit data (green)
that advances timing by half a symbol period

Multi-path propagation

- A single transmitted signal can reach a receiver through multiple paths and arrive at different times
- Signals can be reflected or refracted
- Reflected signals can be stronger than the direct path
- Receiver sees a superposition of the signal through all paths
- Different frequencies may be reflected, refracted, and attenuated differently, distorting UWB signals
- The receipt timing of the earliest path can be ambiguous and difficult to determine precisely

Multi-path propagation



Cicada/Cicada++

- Original Cicada attack [2] injects uniformly spaced pulses to disrupt preamble detection in 802.15.4a UWB
  - Injected pulses and genuine pulses both follow multiple paths before reaching the target receiver
  - Injected pulses create weak false peaks in cross correlation with expected preamble, confusing earliest path detection
- Cicada++ attack [3] adapts this to disrupt STS detection in 802.15.4z HRP UWB
  - Uses strong random polarity pulses at a fraction of the PRF of the STS
  - Skipped pulses allow STS value to be perceived correctly, while injected pulses create false early peaks in cross correlation with expected signal

[2] M. Poturalski, M. Flury, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec, "The cicada attack: Degradation and denial of service in IR ranging," *Infoscience (Ecole Polytechnique Fédérale de Lausanne)*, Sep. 2010, doi: https://doi.org/10.1109/icuwb.2010.5616900.
[3] M. Singh, M. Roeschlin, E. Zalzala, P. Leu, and S. Čapkun, "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*, Jun. 2021, doi: https://doi.org/10.1145/3448300.3467831.

Ghost Peak

- Attacker injects UWB ranging responses with a weak preamble (to avoid jamming) and strong random STS (to create false peaks in cross-correlation with expected STS signal) [4]
- Attacker transmission power level is carefully selected such that sufficiently strong false cross-correlation peaks are created but the received STS is still perceived as correct
- False early cross-correlation peaks are sometimes perceived by the radio hardware as the genuine earliest path
- Distance reduction demonstrated to work with approximately 4% reliability against Apple U1 chip used in iPhones and AirTags
  - Reduced perceived distance from 12 m to 0 m in experiments

[4] P. Leu et al., "Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging," arXiv (Cornell University), Jan. 2021, doi: https://doi.org/10.48550/arxiv.2111.05313.

Bluetooth Channel Sounding principles

- Supports two ranging techniques
  - Packet-based (round-trip-time)
  - Tone-based (phase-based ranging)
- Builds on Bluetooth Low Energy and reuses its PHYs
  - Defines 78 channels by reducing channel spacing from 2 MHz to 1 MHz
  - Primary advertising frequencies avoided, leaving 72 channels for use
  - One new PHY mode specific to Channel Sounding using GFSK with bandwidth-symbol time (BT) product of 2.0 instead of 0.5
- Two sides called initiator and reflector

Bluetooth Channel Sounding modes

- Four supported modes for Channel Sounding steps
  - Mode 0: Measures reflector frequency offset. Initiator sends a CS_SYNC packet, reflector sends a CS_SYNC packet and tone T_IP1 later.
  - Mode 1: Measures packet round trip time (RTT). Initiator sends a CS_SYNC packet, reflector sends a CS_SYNC packet T_IP1 later.
  - Mode 2: Measures phase rotation/delta. Initiator sends a tone, reflector sends a tone T_IP2 later.
  - Mode 3: Measures RTT and phase rotation. Initiator sends a CS_SYNC and tone, reflector sends a tone and CS_SYNC T_IP2 later.
- Each Channel Sounding subevent consists of one or more Mode 0 steps and one or more Mode 1/2/3 steps

Bluetooth Channel Sounding security

- Built on exchanging cryptographically generated pseudo-random values (DRBG outputs) based on negotiated keys
  - Channel hop sequence
  - CS_SYNC PDU access address (sync word)
  - CS_SYNC PDU payload (optional)
  - Tone duration (extension slot)
- Each CS_SYNC PDU uses a different access address
  - Different access addresses on every Channel Sounding step
  - Different access addresses for Initiator to Reflector and vice versa
- BLE link layer encryption required to support negotiation of cryptographic materials

BT Channel Sounding packet PHY

- Gaussian Frequency Shift Keying (GFSK) modulation
- Packet consists of:
  - Preamble – 8 or 16-bit sequence of alternating 1s and 0s
  - Access address – 32-bit pseudo-random sequence
  - Trailer – 4 bits (0101 or 1010 depending on last bit of access address)
  - Sounding sequence or random sequence – optional, 32-128 bits
- Packet timestamp determined by cross correlating received access address signal with expected signal and picking the strongest peak (not necessarily the earliest)
  - Defined in Bluetooth Core Specification v6.0, Vol 6, Part H, Section 3.1

BT CS mode 2 step process

1. Initiator sends an unmodulated tone on current channel
2. Responder receives the signal and measures the phase relative to its own local oscillator
3. Responder transmits an unmodulated carrier on same channel
4. Initiator receives the signal and measures the phase relative to its own local oscillator (i.e. what it transmitted earlier)
5. Responder notifies the initiator of the phase offset between what it received and what it transmitted.
6. Initiator computes propagation phase shift by subtracting responder phase shift from measured phase shift

Note: tones contain one bit of data by either transmitting or not transmitting in a time window called the extension slot.

Attacking BT CS mode 2 (phase-based ranging)

- Pseudo-random channel hop sequence can be defeated by listening and responding on all channels
- Phase-based ranging can be manipulated easily
  - Attacker can transmit their own tone with arbitrary phase
  - Phase at receiver can also be altered through interference
- Extension slot carries only one bit of data per step
  - It can be randomly guessed with a feasible likelihood of success
  - Extension slot duration of 10-40 us provides a massive window for EDLC attacks, as signals can travel many kilometres in that time
  - Attacker can also just not transmit during extension slot and let the legitimate signal come through, albeit phase-shifted relative to the attacker signal

Attacking BT CS mode 1 (RTT-based ranging)

- Pseudo-random channel hop sequence can again be defeated by listening and responding on all channels
- Access address is unlikely to be guessed correctly, but it may be possible to manipulate the packet receipt time
  - Cicada++ and Ghost Peak technique with random access address may both be effective against some receivers
  - Specification requiring use of the strongest correlation peak rather than the earliest peak reduces the risk of Cicada and Ghost Peak
  - Performing an EDLC attack on every bit of the access address and payload may also be possible
- More difficult to manipulate than mode 2

Why two different ranging methods?

- Packet-based operation has limited timing precision
  - Typical receiver timestamp precision is 250 ns due to sampling clock rates – light travels 75m in that time
  - Averaging multiple steps can improve precision
- Phase-based ranging more precise but has weaker security
- Combination of the two needed for secure and precise ranging
- How secure is the combination?
  - How are conflicting measurements and measurements of varying accuracy combined?
  - The precise ranging still depends on a less-secure mechanism.

BT CS Normalized Attack Detector Metric (NADM)

- Devices can estimate the likelihood of a distance manipulation attack based on measurements of received signals
- NADM implementation is optional, but required for the highest defined security level (level 4)
- Specifics left open to implementation
- Specification suggests:
  - Analysis of cross correlation between received and expected signals
  - Searching for EDLC glitches in phase-based ranging extension slot
- If implemented, NADM must detect reference attack signals defined by spec with 90% reliability

Other BT CS risks – weak pairing

- Security of Channel Sounding built on encrypted and authenticated communications between devices
  - Channel Sounding requires strong and securely exchanged BLE link layer encryption keys for ranging operations to be secure
- While BLE link layer encryption is mandatory for Channel Sounding, there are situations where encryption may be weak
  - Some devices allow re-pairing if encryption setup fails without requiring physical user confirmation
  - Some devices allow anyone to pair anytime
  - Some devices use “Just Works” pairing that is subject to MITM attacks

Other BT CS risks – capabilities exchange

- While Channel Sounding operations require link layer encryption, the capabilities exchange procedure does not
  - Consists of LL_CS_CAPABILITIES_REQ and LL_CS_CAPABILITIES_RSP
  - Used for devices to inform each other of supported Channel Sounding modes, features, and performance levels
- It may be possible to inject LL_CS_CAPABILITIES_* messages before link layer encryption startup to perform a downgrade attack on Channel Sounding security

Key takeaways

- Theoretically secure distance bounding schemes can be vulnerable in practice due to physical layer manipulation
- Accurately and securely measuring packet timing is difficult with multipath propagation and interference
- Similar physical layer distance manipulation approaches are likely possible for both HRP UWB and BT CS
- Use NADM, many sounding steps, and a combination of sounding modes to improve the security of BT CS
- Beware of capability downgrade attacks in BT CS

Thank you.

Together we're creating a more secure digital future