UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband

Mridula Singh, Patrick Leu, AbdelRahman Abdou, Srdjan Capkun
Dept. of Computer Science
ETH Zurich
{firstname.lastname}@inf.ethz.ch

Abstract

Mobile autonomous systems, robots, and cyber-physical systems rely on accurate positioning information. To conduct distance-measurement, two devices exchange signals and, knowing these signals propagate at the speed of light, the time of arrival is used for distance estimations. Existing distance-measurement techniques are incapable of protecting against adversarial distance enlargement—a highly devastating tactic in which the adversary reissues a delayed version of the signals transmitted between devices, after distorting the authentic signal to prevent the receiver from identifying it. The adversary need not break crypto, nor compromise any upper-layer security protocols for mounting this attack. No known solution currently exists to protect against distance enlargement. We present *Ultra-Wideband Enlargement Detection* (UWB-ED), a new modulation technique to detect distance enlargement attacks, and securely verify distances between two mutually trusted devices. We analyze UWB-ED under an adversary that injects signals to block/modify authentic signals. We show how UWB-ED is a good candidate for 802.15.4z Low Rate Pulse and the 5G standard.

1 Introduction

Ranging and positioning information is often necessary for mobile autonomous systems, robots and cyber-physical systems to operate successfully. These systems are used in security and safety critical applications. Drones are becoming more popular for transportation and rescue [24], and autonomous systems are being increasingly tested and integrated as part of the ecosystem. The 5G community emphasizes the importance of designing the wireless protocols for the safety of the autonomous vehicles [33]. A stringent requirement for these systems is to avoid crashing into, *e.g.,* buildings, pedestrians, properties, or each other [25]. For example, keeping drones and autonomous vehicles on their intended paths
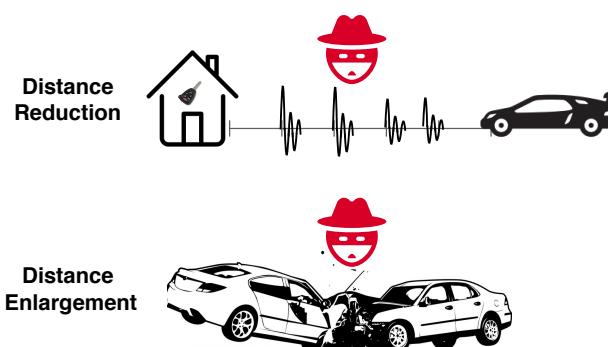
Figure 1: Ranging systems are vulnerable to distance reduction and enlargement attacks.

and preventing their collision can be achieved only if they are able to calculate their relative positions accurately and securely. Figure 1 shows that an adversary can manipulate the perceived distance between two mutually trusted devices by the distance reduction and enlargement attacks.

Conventional ranging systems, such as GPS and WiFi Positioning Systems (WPS) [34], are useful for benign environments and coarse-granular geolocation. However, they provide insufficient precision for accurate distance estimations (*e.g., cm*-level granularity), suffer availability constraints (*e.g.,* indoors, outdoors), and are relatively slow to calculate locations for fast and mobile autonomous systems. More importantly, the aforementioned ranging systems are susceptible to various spoofing attacks [4, 14, 28].

Two-way time-of-flight (ToF)-based ranging systems (which map ToF to distance as signals propagate at the speed of light) have the potential to conduct accurate, fast, and secure distance measurements. Examples include high precision Ultra-wide Band (UWB) ranging systems, some of which are now available off-the-shelf [1, 9, 13, 35]. Numerous previous efforts were directed towards protecting these systems from distance-reduction attacks, *e.g.,* for access control. These mainly rely on the principle that propagation speeds

are bounded by the physical characteristics of the media, and cannot be sped-up. For example, distance bounding protocols return an upper bound on the measured distance, armed by the fact that an adversary would not succeed in guessing (secret) bit level information [5, 6]. Other techniques are based on tailoring modulations to prevent distance-reduction attacks at the physical layer [26]. None of these approaches prevent distance enlargement attacks.

Distance enlargement attacks can deviate vehicles from their intended paths, or cause physical collisions. Existing protection approaches rely on dense, and often fixed, verification infrastructures, *e.g.,* towers. These may not exist, and often do not; installing them in outdoor settings is a costly affair, and not necessarily feasible (*e.g.,* in drone-based military missions behind enemy lines). Distance enlargement is a more devastating attack than distance shortening because an adversary in the communication range only needs to annihilate (cancel) [23] or distort the authentic signals to prevent the receiver from identifying them and using their time-of-arrival (ToA) for ranging. The adversary then simply replays a delayed version of the authentic signals, which it has already received by positioning itself in the vicinity of the sender or the receiver. The adversary need not guess these signals, nor compromise any upper-layer protocols to do that. The amount of delay corresponds to the adversary-intended distance to enlarge. In a collision-avoidance system of automobiles or self-driving cars for example, a few meters ($\sim$ a few nanoseconds) could be catastrophic.

We present *Ultra-Wideband Enlargement Detection* (UWB-ED)—the first known modulation technique to detect distance enlargement attacks against UWB ranging based on ToF. UWB-ED relies on the interleaving of pulses of different phases and empty pulse slots (*i.e.,* on-off keying). Unable to perfectly guess the phase, this leaves the adversary with a 50% chance of annihilating pulses (similarly for amplification). As a result, some of the affected (authentic) pulses will be amplified, while others will be annihilated. Unaffected pulses will remain intact, while positions that originally had no pulses may now have adversary-injected ones. The technique presented herein gets the receiver to seek evidence indicating whether such a deformed trail of pulses in the transmission was indeed authentic, albeit corrupt.

Similar to Singh *et al.* [26] (which addresses distance-reduction attacks), we leverage a randomized permutation of pulses. However, unlike [26], we cannot simply look for whether these are out of order, and ignore them if so because that is precisely the adversary's objective in distance-enlargement: misleading the receiver to ignore the authentic signals. Instead, UWB-ED checks the *energy distribution* of pulses: comparing the aggregate energies of a subset of pulses at the positions where high energy was expected (as per the sender-receiver secret pulse-permutation agreement), with others where low energy was expected. To subvert this, the adversary would be forced to inject excessive energy throughout the whole transmission, which could then be detected using standard DoS/jamming-detection techniques.

We derive the probability that an adversary succeeds in a distance-enlargement attack against UWB-ED. This is also useful in setting input parameters, *e.g.,* balancing an application's security requirements and ranging rate, while accounting for channel conditions. For example, we show how proper parameterization of UWB-ED limits an adversary's success probability in enlarging distances to $< 0.16 \times 10^{-3}$.

In summary, the paper's contributions are twofold.

- UWB-ED—a novel, readily-deployable modulation technique for detecting distance enlargement attacks against UWB ToF ranging systems, requiring absolutely no verification infrastructure, and making no impractical assumptions limiting adversarial capabilities.

- Analytical evaluation to UWB-ED, where the probability of adversarial success is derived as a function of input parameters and channel conditions. This evaluation is also validated using simulations.

The sequel is organized as follows. Sections 2 and 3 provide background and detail the threat model. The new distance enlargement detection technique is explained in Section 4, and evaluated in 5. Section 6 complements with a related discussion, and 7 is related work. Section 8 concludes.

2 Background and Motivation

A device's position can be estimated using the distances between itself and other landmarks with known locations; or it could be expressed using a coordinate system, *e.g.,* in a Cartesian plane. The distance between two devices can be measured using radio signal properties, such as received signal strength [3], phase [30], or the signal's propagation time including ToF and ToA [15]. Reduction or enlargement of the calculated distances can lead to wrong positioning.

Adversarial distance reduction has been analyzed in previous literature [31], but limited work was performed on enlargement attacks. Preventing enlargement is achieved when a node is inside a polygon determined by an infrastructure of devices/towers, where verifiable multilateration [31] is applied. Enlargement attacks are harder to detect without an infrastructure. Signal strength-based systems do not provide strong security guarantees during high variations of signal strengths in some channel conditions. For distance reduction attacks, the adversary can amplify a degraded signal but for enlargement, degradation is in the adversary's favor.

One-way ToF systems, such as GPS, can be spoofed to reduce/enlarge distances [4, 14]. Two-way ToF, such as UWB, provides secure upper bound by using distance bounding along with secure modulation techniques [5, 6, 26]. This provides strong guarantees against reduction attacks, but is still susceptible to enlargement attacks.

2.1 UWB

IEEE 802.15.4a and IEEE 802.15.4f have standardized impulse radio UWB as the most prominent technique for precision ranging. IEEE 802.15.4z [2] is in the process of standardizing UWB to prevent attacks on the ranging systems. Off-the-shelf UWB ranging systems were recently developed [1, 9, 13, 35], and the research community/industry has expressed tremendous interest in these systems (*e.g.,* for autonomous vehicles). Because current standards do not prevent enlargement attacks, it is important to mitigate them before standards are deployed in practice.

Symbol Structure. UWB systems operate over wide segments of licensed spectrum. They have to be compliant with stringent regulatory constraints. Firstly, the power spectral density should not exceed -41.3dBm/MHz, averaged over a time interval of 1ms. Secondly, the power measured in a 50MHz-bandwidth around the peak frequency is limited to 0dBm. Due to these constraints, the power per pulse is limited. To support longer distances, the energy of multiple pulses is aggregated to construct meaningful information. Figure 3 shows On-Off-keying (OOK) modulation, as used in IEEE 802.15.4f-based UWB ranging systems. Each symbol has two pulses and two empty slots. The symbol length is represented as T_b and the spacing between consecutive pulses is T_s. Information bits are encoded in the position of the pulse.

Symbol Detection. Figure 2 shows a conventional non-coherent energy detector (ED) receiver [32]. The energy detector receiver is consist of square-law device to compute instantaneous received signal power and an energy integrator. For the received signal $r(t)$, the output of the receiver can be expressed as:

$$E(k) = \int_{T_s*k}^{T_s*k+T_I} [r(t)]^2 dt \qquad (1)$$

where $T_s * k$ is the integration start time, T_I the integration window size, and T_s the spacing between consecutive pulses.

These receivers perform squaring and integration, making phase information irrelevant for pulse detection. In the case of multi-pulse per symbol, the energies of multiple pulses are aggregated. For the orthogonal hypothesis tests H_1 and H_0 for bit 1 and 0 respectively, the decision of the ED receiver is made in favor of the positions with higher energy.

$$b(i) = \begin{cases} 0 & E_{H_0}(i) \geq E_{H_1}(i) \\ 1 & E_{H_0}(i) < E_{H_1}(i) \end{cases} \qquad (2)$$

2.2 Distance-Enlargement Attack

In contrast to reduction attacks, to enlarge the distance, the adversary need not predict the authentic signal. Instead, it replays the authentic signal by replaying an amplified version of
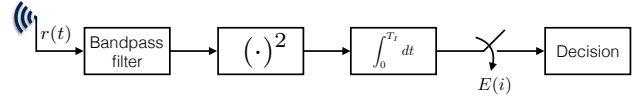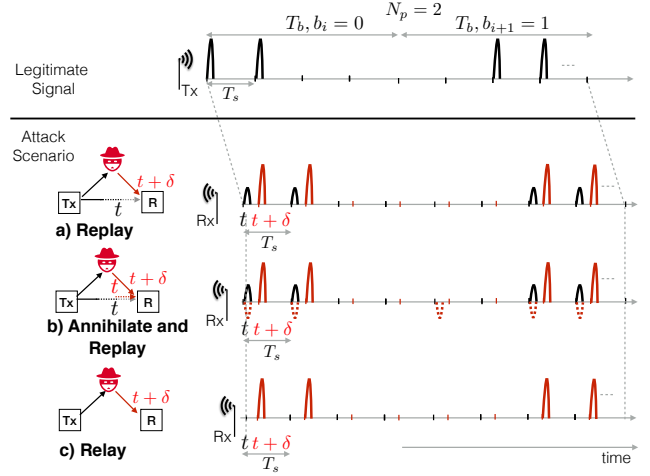

Figure 2: Non-coherent energy detector receiver.

Figure 3: Various attack scenarios on UWB. Black and red colors represent authentic and adversary signals respectively. Dotted red represent adversarial signal-annihilation attempts.

it after some delay. The receiver gets both, authentic and adversary's signal superimposed. Because these authentic signals also reach the receiver, the adversary cannot control how the receiver processes them. None of the existing ranging systems is secure against enlargement attack- be it UWB -802.15.4z, WiFi- 802.11, or GPS. Signal replay is a typical strategy to mount distance enlargement attacks. Other enlargement attacks, such as jamming, alters the output of the receiver's automatic gain control (AGC), and are likely to expose the adversary [22, 27]. Complementing signal replay by signal annihilation prevents the receiver from detecting the authentic signal. Annihilation is possible due to the predictable symbol structure.

In Fig. 3, the devices know each other's communication range, and could verify that they are within that range, *e.g.,* using secure ranging (see Fig. 4). For short LoS distances, a symbol length of $N_p = 1$ (*i.e.,* one pulse-per-symbol) could suffice. Longer distances are attained by longer symbols ($N_p = 2$ in Fig. 3). Pulses are separated by time T_s, which should be more than the channel's delay spread. The length of the symbol (T_b) is determined by the number of pulses per symbol, and the interval between two consecutive pulses ($N_p \cdot T_s$). Figure 3 also shows instances of replay attacks on these symbols. When an adversary replays authentic signals after some delay (δ), both authentic and replayed signals are received. To deceive the receiver, the adversary needs to annihilate authentic signals.
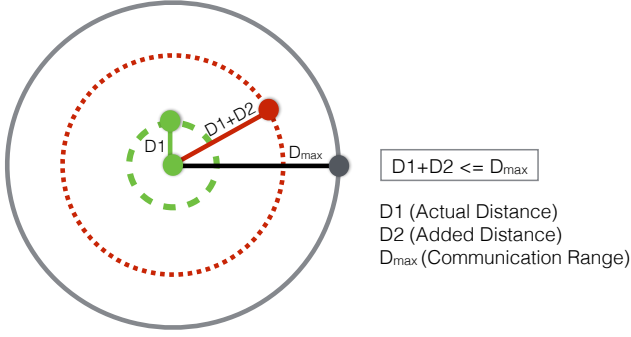
Figure 4: If $D1 + D2 > D_{max}$, the devices realize they are outside each other's communication range without the need to run distance-enlargement detection protocol.

In Fig. 3a, an authentic signal reaches the receiver at time t, and the adversary's signal at $t + \delta$. If the receiver backtracks in time (searching for earlier-received signals), the authentic signal will be encountered. Figure 3b shows how the predictability of the symbol structure enables an adversary to annihilate its pulses (by emitting a reciprocal pulse phase), preventing the receives from detecting it. Figure 3c shows the case when nodes are not in the communication range (or signal is attenuated by channel condition); the receiver does not get authentic signals, just adversary-relayed (and delayed) signals.

3 Threat Model

We focus on the scenario where there are two devices in a wireless network that are interested to securely measure the physical distance between them, and protect the measurements from a third-party adversary. The devices know their maximum communication range. The adversary's objective is to enlarge the distance that the devices measure. The adversary cannot directly block or modify messages on the channel (*cf.* Dolev-Yao's adversary [10]); it can rather inject signals, and through such injection it can block/modify the authentic signals. If successful, this injection can lead to jamming, signal annihilation, and/or content modification. This model captures the capabilities of man-in-the-middle (MITM) attacks in wireless settings, and is typical in previous literature [7, 12]. The model also fits well with our target application scenario: the communicating devices are typically mobile and move (drive or fly) in formation. In such scenarios, it is unlikely that an adversary prevents the signals of one device from reaching the other by physical obstacles, and is thus limited to injecting signals.

We assume the adversary is able to communicate and listen on any channel the devices use. However, because the devices are communicating over UWB, the adversary is unable to deterministically annihilate pulses without knowing their phase (positive or negative). Existing hardware is not fast enough to enable the adversary to sample a pulse's phase and react by injecting the reciprocal pulse promptly due to the very narrow UWB pulse width of ≈ 2 *ns*. We therefore assume that the adversary will not be able to deterministically annihilate pulses from the channel, only with some probability < 1. It succeeds in annihilating pulses if it guesses the phase of the pulse correctly. We over-approximate the adversary by providing the capability to synchronize attack signal with the authentic transmission. Signal synchronization is a hard problem, but an adversary can achieve it by using stable clock and distance information.

We assume the adversary knows the actual physical distance between the two devices at any point in time. The adversary can calculate this using several means, *e.g.,* by eavesdropping on unencrypted position announcements the devices make. The adversary can also position itself along the direct path between the two devices, measure the distance between itself and each from that position, and add both distances. To measure these distances, the adversary's device can perform two-way ranging with each device independently, pretending to be the other device; or even without such impersonation, it could perform one-way ranging after synchronizing its clock with each device separately.

We assume the devices themselves are not compromised; the adversary cannot attach a physical cable to their interfaces, nor hijack their firmware. However, the adversary can have multiple network cards and antennas, and is not energy-bounded. It can be stationary or mobile.

UWB-ED (Section 4) involves transmitting, between the victim devices, a code of n pulses, α of which are data-representing, and the remaining β are absent of energy, where $n = \alpha + \beta$. We assume the adversary knows the values of α and β, but not the positions of these pulses in the transmission. (Their positions are determined by both devices pseudo-randomly in each transmission.) The adversary can learn these parameters by remaining passive in the vicinity of the victim devices, silently observing their transmissions.

Finally, we assume that it is not in the adversary's interest to prevent the devices from communicating, *e.g.,* by shielding them, or jamming the channel.

4 UWB-ED Design

UWB-ED consists of two phases conducted between both devices: Distance Commitment and Distance Verification. Figure 5 shows a timing diagram of both phases. In the first, the devices measure the distance between them using a two-way ranging protocol. The distance measured in this phase (t_{tof}^c) should not exceed the supported communication range (t_{tof}^{max}). In the distance verification phase, the devices measure their distance by exchanging verification codes (generated using a special UWB-ED modulation). To detect enlargement attacks, devices look for distorted traces of that code. The
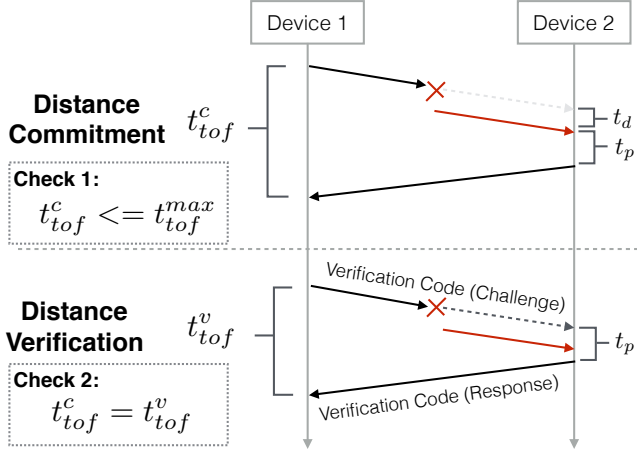
Figure 5: Timing diagram of UWB-ED operation. See inline (Section 4) for notation.
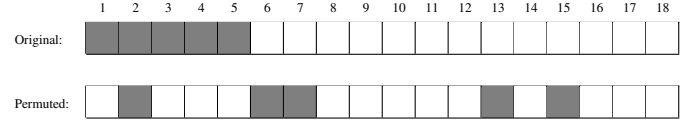

Figure 6: An example verification code with a randomly-looking pulse reordering, where $\alpha = 5$, $\beta = 13$, and the code contains $n = \alpha + \beta = 18$ pulses. Upon receiving the permuted code pulses as per the secret agreement between the sender and receiver, the receiver knows that Bin_α will contain the received energies at the positions (gray) $\{2, 6, 7, 13, 15\}$, which are the expected high-energy pulses. Bin_β will contain the rest: $\{1, 3, 4, 5, 8, 9, 10, 11, 12, 14, 16, 17, 18\}$.

attack is detected when such traces are found, $t_{tof}^c > t_{tof}^{max}$, or when $t_{tof}^c \neq t_{tof}^v$ (Fig. 5). By enlarging distance in the commitment phase, the adversary increases t_{tof}^c by t_d, but fails to enlarge the distance in the verification phase. Annihilation attempts on the challenge frame are shown, but the adversary can also attack responses from both devices.

Distance Commitment Phase. The devices measure secure upper bound by using distance bounding along with secure modulation techniques [5, 6, 26]. This provides strong guarantees against reduction attacks but is susceptible to enlargement attacks. The distance committed in this phase should not exceed the communication range (*i.e.,* an enlargement attack is detected when $t_{tof}^c > t_{tof}^{max}$). This check ensures that the nodes can communicate without a relay. An adversary enlarging distance by more than the communication range is also exposed using this check.

Distance Verification Phase. In this phase, the committed distance is verified, *i.e.,* an enlargement attack is detected when $t_{tof}^c \neq t_{tof}^v$. To achieve this, the devices measure their distance using round-trip time-of-flight, with both challenge and response messages protected using specially crafted *verification codes* (*i.e.,* special UWB-ED modulation). In this exchange, the sender initiates the distance verification phase by transmitting a verification code; the receiver tries to detect the presence of that code, or traces thereof, in the transmission, despite the adversary's efforts to *trail-hide* its existence from the channel (Section 2.2). The verification code and its check is applied to both time-of-flight messages. Both devices first agree on the code's structure as follows.

4.1 Modulation/Verification Code Structure

Code length. The code consists of n positions, α of which have energy, and the remaining $\beta = n - \alpha$ are empty, *i.e.,* absent of pulses (conceptually similar to OOK modulation,

where $\alpha = \beta$). The code length affects the performance and security of the presented modulation technique. Larger α and β values improve the security by reducing the probability of adversarial success in mounting undetectable distance-enlargement attack. However, increasing the code length reduces the frequency of conducting two-way ranging. Additionally, the Federal Communications Commission (FCC) imposes restrictions on the number of pulses with energy, effectively limiting α per unit of time. As such, β could be independently increased to compensate for the loss of code length. Setting these parameters is discussed in Section 5.

Pulse phase. The sender uses a random-phase for the α pulses it transmits. Each phase is equally likely. The phase will be irrelevant for the receiver because ED receivers are agnostic to the phase, as explained in Section 2.1. The sender need not share this information with the receiver since the receiver measures the energy, not the polarity of the pulse.

Pulse permutation. The sender and receiver secretly agree on a random permutation of the n positions, obtained from a uniform distribution. Figure 6 shows an example before and after the permutation. The verification code can thus be considered a sequence of $\{-1, 0, 1\}$ pulses, where $\{-1, 1\}$ represent the phase, and $\{0\}$ pulse absence.

Spacing between pulses. The time between two consecutive pulses, T_s, is normally lower bounded by the delay spread of the channel. We submit that T_s should be such that $T_s > 2d/\mathbf{c}$, where d is the distance between the two devices. If the adversary replays the authentic signal delayed by more than the equivalent RTT, the attack will be detected by the mismatch between the measured RTT and the one equivalent to the committed distance. To avoid being detected, the adversary would thus replay its delayed version of a pulse within the T_s time window. As such, authentic pulse i will not overlap with the adversary's delayed version of pulse $i-1$, or any further adversary pulses $i-2$, $i-3$, *etc.*

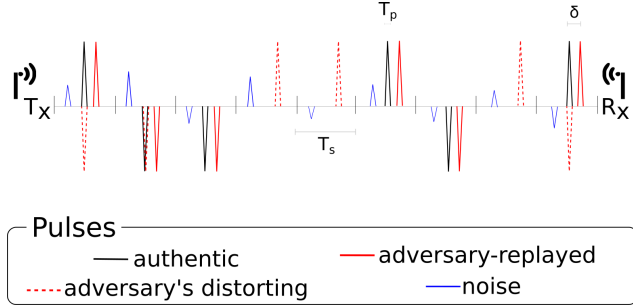An example code structure, and adversarial attempts to corrupt and replay it, is shown in Fig. 7.

Figure 7: An example verification code of n slots (9 of which are shown), the spacing T_s between consecutive pulses is $1\mu s$ and pulse width T_p is $2ns$. An adversary transmits a pulse to distort the legitimate pulse (dashed red). The adversary also replays the authentic signal with the delay δ (solid red). Best viewed in color.

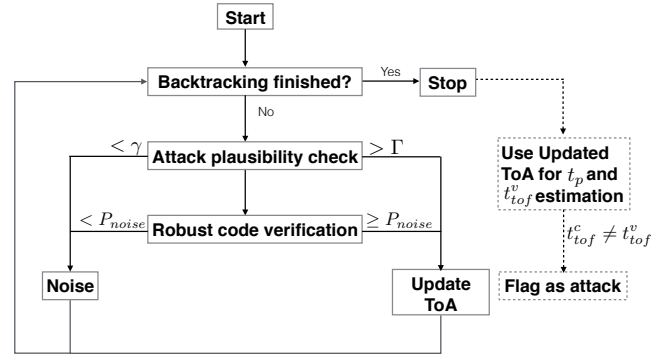
Figure 8: The receiver backtracks to detect enlargement attacks. An event is flagged as an attack when the aggregate energy is higher than Γ (*e.g.,* DoS, jamming), *i.e.,* the data looks more similar to a verification code than noise. The last flagged position is used for the ToF estimation.

4.2 Verification Code Identification

Upon receiving a transmission, the receiver starts processing the code associated with the highest preamble's peak. The code associated with a peak is the train of T_s-spaced pulses that start at a fixed time interval (*e.g.,* agreed upon between the sender and receiver) after the peak. This peak however may not be authentic, and could be the adversary's replayed version. The receiver thus backtracks at fixed time steps corresponding to the pulse width T_p (*e.g.,* 2 *ns*), trying to identify if another version of the code (or a possible distorted imprint of it) was present in the transmission at an earlier time. The receiver does not need to backtrack further beyond some time T_0, knowing the maximum communication range. If the last distance verification occurred recently, the verified range could be used (in combination with the devices' upper bound motion speeds) to reduce the backtracking time.

Backtracking requires the receiver to record transmissions. If an earlier version of the code is found (and their difference exceeds the receiver's standard precision, *e.g.,* ± 10 *cm* for DecaWave [9]), it is used for ToF estimation.

As shown in Fig. 8, the receiver performs Attack Plausibility check and Robust Code Verification to detect attacks until the maximum backtracking time is reached. For each code, the receiver does not look for an exact match of the transmitted pulses in their positions simply because that could be easily bypassed with minimal adversarial efforts (as explained in Section 2.2). Instead, the receiver proceeds as follows. Knowing the mapping of the pulse positions, the receiver distributes the received powers of each pulse among two bins, Bin_α and Bin_β. The former will have the values of the received power (*e.g.,* in Watts) of the energy-present pulse positions, the latter energy-absent positions (Fig. 6).

Attack Plausibility check. For each candidate verification code obtained during backtracking, the overall received signal power (the aggregate of Bin_α and Bin_β) is measured, and

compared to a predefined threshold, γ. This threshold is based on the receiver's noise figure. If the aggregate exceeds γ, a potential verification code has been found. Otherwise it gets discarded as noise. The aggregate energy is then compared to another threshold, Γ. This is calculated based on the overall aggregate energy the receiver expects to receive based on the measured distance in the commitment phase, following the path loss model. Artificial distance enlargement caused by the adversary in the commitment phase lowers the receiver's calculated Γ (because of the higher path loss), thus increases the likelihood of the actual received aggregate to exceed Γ. If the aggregate exceeds Γ, an adversary may possibly be injecting energy into the channel to distort the authentic code. If the verification code is neither discarded as noise ($< \gamma$) nor exceeds Γ, the receiver proceeds to the Robust Code Verification check.

Robust Code Verification. Now the receiver checks the verification code content. If the receiver simply flags the presence of one or more pulses (above noise) in Bin_β as an attack, false positives increase because such pulses could occur for many legitimate reasons (*e.g.,* noise spikes, reflections, interfering transmissions, antenna orientation, or multipath).[1] Instead, the receiver performs a sequence of binary hypothesis tests on random pulse samples. It tests if the candidate code is more similar to an authentic code than noise. It chooses $r \leq \alpha$ random pulses from the α in Bin_α (where r is the number of pulses per symbol), aggregates their received powers and compares that to the aggregate of another r pulses randomly chosen from the β in Bin_β. If the aggregate of those selected from Bin_α is larger, the receiver identifies this as a candidate authentic code, and records its ToA. Finally, the distance is calculated based on the recorded ToA of the most recently

---

[1]If the receiver instead interprets a pulse in Bin_β as an indication that the code is not authentic and continues backtracking, it may very well skip the authentic code thus helping the adversary.

received code, and a mismatch with the committed distance is flagged as an attack.

A candidate verification code could be again noise, which has slipped the Attack Plausibility check perhaps due to some sporadic noise spikes in the transmission. Noise has a probability of $\leq P_{\text{noise}}$ to satisfy the Robust Code Verification check, where P_{noise} is derived as (32) in Section 5.1.4. As such, the receiver estimates the probability that the above condition is satisfied. This is done by repeating the random sampling υ times, and checking if the ratio of the number of times the condition is satisfied to υ exceeds P_{noise}. This would indicate the code is not noise, and is either authentic or adversary-replayed. Regardless, the receiver uses the ToA of the most recent code found.

4.3 Setting the Energy Thresholds.

Setting the upper-bound threshold, Γ. To set Γ, the receiver relies on the committed (unverified) distance between itself and the sender. This dictates the path loss—the amount of power loss per pulse as pulses propagate the medium. Larger committed distance causes the receiver to expect less power, thus setting a lower Γ. Thus, by increasing the committed distance, the adversary helps divulge its malice.

The path loss function $f()$ for outdoor UWB LoS is [20]:

$$f(d) = PL_0 + 10 \cdot n \cdot log\left(\frac{d}{d_0}\right) \quad (3)$$

where d is the distance in meters, and PL_0 is a constant representing the path loss at the reference distance d_0. For UWB LoS channel model, these constants are set to [20]:

$$f(d) = -46.3 - 20 \, log(d) - log\left(\frac{6.5}{5}\right) \quad (4)$$

This is calculated in the standard signal ratio unit, dB, where:

$$\text{Power ratio (in } dB) = 10 \, log \, (\text{ratio}) \quad (5)$$

The path loss function thus expresses the power loss as

$$f(d) = 10 \, log\left(\frac{(\lambda_b)^2}{(\lambda_{\text{sent}})^2}\right) \quad (6)$$

or

$$\frac{(\lambda_b)^2}{(\lambda_{\text{sent}})^2} = 10^{f(x)/10} \quad (7)$$

where $(\lambda_b)^2$ is the pulse instantaneous power the receiver *expects*, and $(\lambda_{\text{sent}})^2$ is that the sender has actually sent, *e.g.,* both in Watt. Knowing the constant pulse power of the sender, then the pulse power is expected to be received as:

$$(\lambda_b)^2 = (\lambda_{\text{sent}})^2 \, 10^{f(x)/10} \quad (8)$$

The receiver then calculates Γ as follows:

$$\Gamma = \alpha \, (\lambda_b + N)^2 + \beta \, (N)^2 \quad (9)$$

where d is the (unverified) distance in meters between the sender and receiver obtained at commit stage, either true or artificially enlarged in case of an attack. N is an instantiation of zero-mean Gaussian noise at the receiver, *i.e.,* the noise present in the receiver's channel and cannot be removed [19].

There are other factors that contribute to the degradation of power. These factors could cause further power loss E, typically up to $E = -8 \, dB$ more [17, 21]. If the receiver sets Γ as that after the expected further degradation (*i.e.,* too small Γ value), false positives may increase because such additional signal-degradation factors may or may not occur— if they do not, the receiver would then falsely assume such relatively "too high" aggregate energy is due to an attempted attack. Accordingly, the receiver sets Γ based only on the (almost certain) path loss deterioration. Any further power loss would then be added benefit to the adversary, as it allows the adversary to inject more pulses into the channel to corrupt the authentic code without exceeding Γ.

Setting the lower-bound threshold, γ. If the aggregate energy is $< \gamma$, it would be either due to noise or a substantial deterioration of the authentic signal where no meaningful information could be recovered during the Robust Code Verification. Too high γ leads to false negatives; too low triggers Robust Code Verification even for noise. For critical applications seeking to prevent false negatives, γ could be set conservatively based on the receiver's noise variance σ_N^2:

$$\gamma = (\alpha + \beta) \cdot \sigma_N^2 \quad (10)$$

4.4 Attack Resilience

Here we explain how UWB-ED resists standard enlargement attacks. More complex attacks are discussed in Section 6.

4.4.1 Detecting Signal Replay

An adversary that simply replays authentic pulses does not win because the receiver backtracks to detect earlier copies of the code. UWB-ED provides resilience to benign signal distortion, *e.g.,* due to channel conditions or antenna orientation, because the receiver looks for similarities between the code and the received signal (versus exact data match), allowing for a higher bit error rate. In general, poor channel conditions (low SNR) can be compensated for by increasing the symbol length, r, minimizing the bit error rate.

4.4.2 Complicating Signal Annihilation

The unpredictability of the pulse phase means an adversary must either wait to detect it and immediately inject the reciprocal pulse for annihilation, or inject a random-phased pulse hoping it is the reciprocal. The former is infeasible in practice for UWB (see Section 3). The latter results in amplifying or annihilating the authentic pulse, each with a 50% chance. Amplification is unfortunate to the adversary, as the adversary
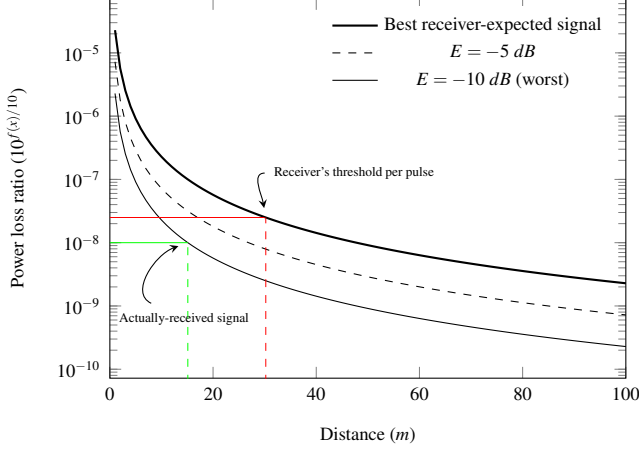
Figure 9: The best expected signal power as calculated by the receiver using the path loss function in (4), the signal at $E = -5$ db of further power loss, and at $E = -10$ db (worst expected). If the distance is $D_1 = 15.11$ m (green line), and the adversary doubles it, *i.e.,* by adding $D_2 = 15.11$ m to make it $D_1 + D_2 = 30.22$ m (red line), the receiver will set the threshold following the fake distance, at $10^{f(D_1+D_2)/10} = 10^{-7.6}$. The adversary's room is the difference between the red and green lines on the *y*-axis. At $D_2 = 32.68$ m, the adversary has no room. Best viewed in color.

now needs to compensate with an equivalent amplitude, A. Amplification doubles the amplitude. The estimated energy of the pulses will thus amount to $\sim A^2$, and the adversary-contributed amplification to $\sim (2A)^2$.

Since the result is indeterministic for the adversary, it leads us to the next discussion: how successful would the adversary be in "contaminating the evidence" that an authentic verification code existed, and how much energy room does the adversary have to do that before exceeding Γ?

4.4.3 Mitigating Evidence Contamination

To hide the authentic code, the adversary tries to inject energy into the channel, hoping it annihilates as many of Bin_α pulses as possible. We thus calculate the room available to the adversary here, and use that to derive the probability of adversarial success in distance enlargement in Section 5.

Figure 9 shows the path loss function in (7) as used by the receiver to detect the threshold Γ, as well as the worst receiver-expected signal after additional deterioration. The receiver sets the threshold based on the best expected signal. The room available for the adversary to add energy depends on the actual signal received. The most favorable situation to the adversary is when the received signal power is the worst (lowest E), which allows the adversary to inject pulses without exceeding Γ. For example, in Fig. 9, if the actual distance between the sender and receiver is $D_1 = 15.11$ m (green line), and the
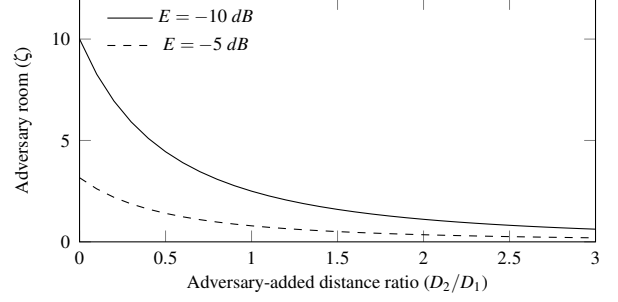

Figure 10: Adversary's room to add energy, ζ in (12), against the ratio of the adversary-added to true distance (D_2/D_1); E represents additional signal degradation beyond path loss.

adversary is trying to add $D_2 = 32.68$ m to make the distance $D_1 + D_2 = 47.79$ m (red line), the receiver will set Γ using the fake distance, $D_1 + D_2$. At such a relatively large added distance, D_2, the received pulse power is unlikely to fall below $f(D_1) + E = 10^{-8}(\lambda_{\text{sent}})^2$ at, *e.g.,* $E = -10$ dB. The room available to the adversary to inject energy becomes too small, significantly reducing its chances of success.

The room-per-pulse, R, available to the adversary to enlarge the distance thus lies in-between the received signal and Γ, and is calculated in dB as:

$$R = f(D_1 + D_2) - (f(D_1) + E) \tag{11}$$

where E represents other channel degrading factors, and the distances D_1 and D_2 (in meters) are respectively the true distance between both devices, and the extra distance the adversary intends to add. This room is thus expressed as:

$$\zeta = 10^{R/10} \tag{12}$$

Figure 10 plots ζ at various distance ratios D_2/D_1.

Recall that the adversary may succeed to annihilate some of the pulses falling in Bin_α. But since Bin_β in the authentic code have nothing but noise, adding pulses into those will result in an increase in the overall aggregate energy. As such, this available energy room in (11) by itself does not give a perfect indication to the adversary's chances of success.

4.5 A Numerical Example

Figure 11 shows an example verification code, expanded from Fig. 6, where the adversary injects $k = 10$ random-phased pulses. For simplicity, the figure assumes $N = 0$. If the distance between the sender and receiver is $D_1 = 4$ m, and the adversary is trying to enlarge it by $D_2 = 4.5$ m to make it $D_1 + D_2 = 8.5$ m, and assuming $(\lambda_{\text{sent}})^2 = 7.6$ μW, then the receiver expects a best case received power of:

$$
\begin{aligned}
(\lambda_b)^2 &= (\lambda_{\text{sent}})^2 \, 10^{f(D_1+D_2)/10} \\
&= 7.67 \times 10^{f(8.5)/10} = 2.4 \; \mu W
\end{aligned}
\tag{13}
$$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Sent (after path loss):	0	-1	0	0	0	-1	1	0	0	0	0	0	1	0	-1	0	0	0	$\Gamma = \alpha\,(\lambda_b)^2 = 12\,\mu W$
Adversary injects:	1	1			-1		1	-1	1			-1	1				-1	-1	$k = 10$ pulses
Receiver gets:	1	0	0	0	-1	-1	2	-1	1	0	0	-1	2	0	-1	0	-1	-1	$\alpha(\lambda_{\text{received}})^2 = 17\,\mu W$

Figure 11: An example of the random-phased Bin_α pulses (dark gray) reordered following the permutation in Fig. 6. After the adversary injects $k = 10$ random-phased pulses at random positions, the receiver will get the summation at each pulse position.

From (10) at $N = 0$ and $\alpha = 5$ (as in Fig. 11), it then calculates the threshold as:

$$\Gamma = \alpha\,(\lambda_b)^2 = 12\,\mu W \tag{14}$$

At $E = -10\,dB$, the actual signals are received as:

$$(\lambda_w)^2 = (\lambda_{\text{sent}})^2\,10^{(f(D_1)+E)/10} \approx 1\,\mu W \tag{15}$$

Now assuming the adversary is $D_3 = 6\,m$ away from the receiver, and uses a random-phased pulse with transmission power of $(\lambda_{\text{sent}}^{\text{adversary}})^2 = 15.77\,\mu W$. At $E = -10\,dB$, the receiver would receive the adversary's signals as:

$$(\lambda')^2 = (\lambda_{\text{sent}}^{\text{adversary}})^2\,10^{(f(D_3)+E)/10} \approx 1\,\mu W \tag{16}$$

So in the best case for the adversary, where the signal is highly deteriorated, the adversary would then have a per-pulse room of $R = 3.45\,dB$ to add energy, which amounts to $7\,\mu W$ more, *i.e.,* up to $\Gamma = 12\mu W$. In Fig. 11, after the adversary injects its $k = 10$ pulses at the example random positions and with the random phases shown, it results in annihilating a single pulse (at position 2), amplifying two pulses (at positions 7 and 13), and adding seven more $1\,\mu W$ pulses for an increase of the overall aggregate to be $17\,\mu W$. This exceeds $\Gamma = 12\,\mu W$, and this attack would thus be detected.

5 Evaluation

We evaluate UWB-ED by deriving the probability of success for an adversary enlarging the distance. We also validate that model using simulations in Section 5.2.

5.1 Probability of a Successful Attack

The adversary hides the authentic code by having the aggregate of the r pulses that the receiver chooses from Bin_β exceed Bin_α. The adversary must also avoid injecting too much energy to not exceed Γ. Not knowing which pulse belongs to which bin, the adversary injects k pulses at random positions thus affecting k of the n pulses in the code.

To that end, the probability of mounting a successful attack, P_{sa}, is the intersection of the probability of two events (the checks in Fig. 8): the aggregate of the energy pulses chosen from Bin_β ($b\beta$) exceeds that of Bin_α ($b\alpha$), and the added energy is $\leq \Gamma$:

$$P_{\text{sa}}(\alpha,\beta,r,\Gamma,k) = P_{b\beta>b\alpha}(\alpha,\beta,r,k) \cap P_{\leq\Gamma}(\alpha,\beta,k) \tag{17}$$

5.1.1 Probability of successfully evading the Robust Code Verification check ($P_{b\beta>b\alpha}$)

To evade this, the adversary must have an energy aggregated from Bin_β exceed Bin_α. When the adversary injects k pulses into the channel, x will fall into Bin_α, and the remaining $k - x$ into Bin_β. $P_{b\beta>b\alpha}$ is then the probability of this distribution occurring multiplied by the probability of the attack succeeding under this distribution, for all possible such distributions $0 \leq x \leq \alpha$ and $0 \leq k - x \leq \beta$. To calculate the probability of the distribution occurring, consider the general case of a bucket containing two types of objects (*e.g.,* colored pearls): I of the first type, and J of the second. If ψ objects are selected at random, the probability that i and j of the ψ are respectively of the first and second type ($i + j = \psi$) is:

$$\frac{\binom{I}{i}\binom{J}{j}}{\binom{I+J}{i+j}} \tag{18}$$

where $\binom{n}{r}$ denotes n choose r and is given by:

$$\binom{n}{r} = \begin{cases} \dfrac{n!}{r!(n-r)!}, & 0 \leq r \leq n \\ 0, & \text{otherwise} \end{cases}$$

Similarly, the probability that x and $k - x$ of the adversary's k pulses respectively affect the α in Bin_α and β in Bin_β is:

$$\frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}}$$

For all possible such distributions, we have:

$$P_{b\beta>b\alpha}(\alpha,\beta,r,k) = \sum_{x=0}^{\alpha}\left(p_{\alpha,\beta,r,k}(x)\cdot\frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}}\right) \tag{19}$$

where $p_{\alpha,\beta,r,k}(x)$ is the probability $b\beta > b\alpha$ given the adversary affected x and $k - x$ pulses in Bin_α and Bin_β respectively.

To derive $p_{\alpha,\beta,r,k}(x)$, we assume for simplicity a unity power-per pulse, *i.e.,* the sender's and the adversary's pulses

reach the receiver after path loss and other factors at a constant energy of $\pm 1\mu W$.[2] This is similar to the example given in Fig. 11. Every adversary-added pulse in Bin$_\beta$ will result in a $1\ \mu W$ of added energy from the receiver's point of view since the receiver's aggregation is agnostic to a pulse's phase. For Bin$_\alpha$, after the adversary affects x pulses, some will be annihilated while others will be amplified. From the receiver's point of view, after the adversary's pulses are injected, Bin$_\alpha$ will have a mix of $2^2 = 4\mu W$ and $0\ \mu W$ (adversary-affected) pulses, as well as the original $1\ \mu W$ unaffected pulses.

More $0\ \mu W$ (annihilated) pulses in Bin$_\alpha$ raises the chances that $b\beta > b\alpha$, which is in the adversary's favor. Since every affected pulse in Bin$_\alpha$ will either result in a $0\ \mu W$ or a $4\ \mu W$ pulse, there are 2^x possible outcomes. Of those, there are $\binom{x}{g}$ ways that g $0\ \mu W$ pulses will occur. The probability that the x adversary-injected pulses that fell in Bin$_\alpha$ result in a annihilation of g pulses is thus $\binom{x}{g}/(2^x)$. For all possible numbers of annihilated pulses $0 \leq g \leq x$, the adversarial success probability in the event that x fell in Bin$_\alpha$ is:

$$p_{\alpha,\beta,r,k}(x) = \sum_{g=0}^{x} \left(p_{\alpha,\beta,r,k,x}(g) \cdot \frac{\binom{x}{g}}{2^x} \right) \tag{20}$$

where $p_{\alpha,\beta,r,k,x}(g)$ is the probability $b\beta > b\alpha$ given g annihilated pulses in Bin$_\alpha$.

When Bin$_\alpha$ has g annihilated ($0\ \mu W$), $x - g$ amplified ($4\ \mu W$), and $\alpha - x$ unaffected pulses ($1\ \mu W$), the probability of $b\beta > b\alpha$ in the event x fell in Bin$_\alpha$, and g of the x pulses were annihilated is the probability that an aggregate of $m - 1$ is chosen from Bin$_\alpha$ and an aggregate of $\geq m$ is chosen from Bin$_\beta$. For each possible $0 \leq y_1, y_2 \leq r$, we have:

$$p_{\alpha,\beta,r,k,x}(g) =$$

$$\sum_{y_1=0}^{r} \sum_{y_2=0}^{r} \left(\frac{\binom{g}{y_1} \binom{x-g}{y_2} \binom{\alpha-x}{r-y_1-y_2}}{\binom{\alpha}{r}} \cdot \sum_{i=m}^{r} \frac{\binom{k-x}{i} \binom{\beta-(k-x)}{r-i}}{\binom{\beta}{r}} \right) \tag{21}$$

where m is:

$$\begin{aligned} m &= 0^2 \times y_1 + 2^2 \times y_2 + 1^2 \times (r - (y_1 + y_2)) + 1 \\ &= r - y_1 + 3y_2 + 1 \end{aligned} \tag{22}$$

At $r = \alpha$ (*i.e.*, selecting all Bin$_\alpha$ pulses) and $\alpha \leq \beta$, we get:

$$p_{\alpha,\beta,r,k,x}(g) = \sum_{i=m'}^{r} \frac{\binom{k-x}{i} \binom{\beta-(k-x)}{r-i}}{\binom{\beta}{r}} \tag{23}$$

where m' is:

$$\begin{aligned} m' &= 2^2 \times (x - g) + 1^2 \times (\alpha - x) + 1 \\ &= 4(x - g) + (\alpha - x) + 1 \end{aligned} \tag{24}$$

Figure 12 plots $P_{b\beta > b\alpha}$, where $\alpha = 50$. From these results, increasing β is not necessarily effective for the Robust Code

---

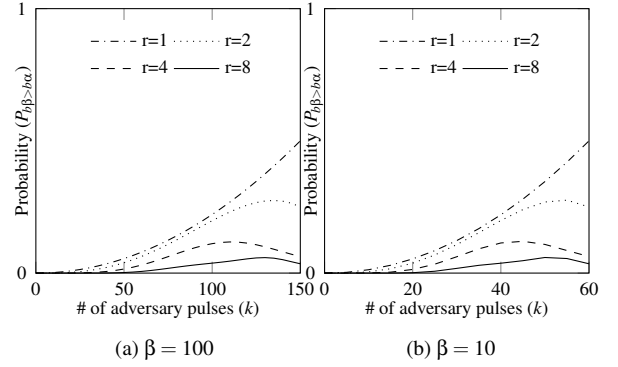[2]Analogous analysis applies for non-constant energy.

Figure 12: Probability that the Robust Code Verification check fails to detect the adversary's attack, plotted using (19) in Section 5.1.1, at $\alpha = 50$ and $0 \leq k \leq \alpha + \beta$.

Verification check to detect attacks, since the adversary maintains its success probability by increasing k proportionally; there is a visually similar pattern of adversarial success probability in both Fig. 12a and 12b. As such, the advantage of the empty pulses in Bin$_\beta$ does not quite manifest in the Robust Code Verification check, rather the Attack Plausibility check.

Another observation is that higher r lowers the adversary's success probability. For example at $\beta = 100$ (Fig. 12a), the adversary has a 27% chance at $r = 2$ (which occurs at $k = 135$), versus 5.85% at $r = 8$ (at $k = 130$). In Section 5.1.3, we show that at $r = \alpha$, we get the optimal security results.

5.1.2 Final Probability of Adversary's Success

In (17), the event that the aggregate energy after the adversary's pulses is $\leq \Gamma$ and the event that $b\beta > b\alpha$ are dependent, and thus their intersection is not their product. Recall that in (20), g is the number of annihilated pulses, $x - g$ is the number of amplified pulses in Bin$_\alpha$, and $k - x$ is the number of added pulses in Bin$_\beta$. The aggregate-energy does not exceed Γ when the adversary's pulses satisfy the inequality:

$$\begin{aligned} &(k-x)\,(\lambda' + N)^2 + (x-g)\,(\lambda' + \lambda_w + N)^2 + \\ &(\alpha - x)\,(\lambda_w + N)^2 + (\beta - (k-x) + g)\,(N)^2 \leq \Gamma \end{aligned} \tag{25}$$

where λ' is defined as in (16), and Γ in (10).

If the adversary uses a variable pulse power randomly chosen from a distribution with a mean much different from λ_w, authentic pulses colliding with their reciprocal will not be fully annihilated. The adversary thus sets its power such that its mean at the receiver matches the sender, *i.e.*, $\overline{(\lambda')^2} = (\lambda_w)^2$. Assuming $(\lambda_w)^2 = (\lambda')^2$ in (25), we get:

$$k + 2x - 4d + \alpha \leq \frac{\alpha\,\lambda_b^2 - \varepsilon}{\lambda_w^2} \tag{26}$$

where ε is a representation of noise, and evaluates to:

$$\varepsilon = N\,(\lambda_w\,(2k + 2\alpha - 4g) - \lambda_b(2\alpha))$$

As $\varepsilon \to 0$, (26) becomes:

$$k + 2x - 4d \leq \alpha \left(\frac{\lambda_b^2}{\lambda_w^2} - 1 \right) \quad (27)$$

From (13) and (15), we have:

$$\begin{aligned}
\frac{\lambda_b^2}{\lambda_w^2} &= \frac{(\lambda_{\text{sent}})^2 \, 10^{f(D_1+D_2)/10}}{(\lambda_{\text{sent}})^2 \, 10^{(f(D_1)+E)/10}} \\
&= 10^{(f(D_1+D_2)-(f(D_1)+E))/10} \\
&= \zeta
\end{aligned} \quad (28)$$

where ζ, from (12), represents the room-per-pulse available to the adversary to add energy into the channel.

We now calculate $p_{\alpha,\beta,r,k}(x,\Gamma)$, similar to (20) as:

$$p_{\alpha,\beta,r,k}(x,\Gamma) = \sum_{g=0}^{x} \left(p_{\alpha,\beta,r,k,x,\Gamma}(g) \cdot \frac{\binom{x}{g}}{2^x} \right) \quad (29)$$

such that

$$p_{\alpha,\beta,r,k,x,\Gamma}(g) = \begin{cases} p_{\alpha,\beta,r,k,x}(g), & k+2x-4d \leq \alpha(\zeta-1) \\ 0, & \text{otherwise} \end{cases} \quad (30)$$

Using (29), the final adversarial success probability is:

$$P_{\text{sa}}(\alpha,\beta,r,\Gamma,k) = \sum_{x=0}^{\alpha} \left(p_{\alpha,\beta,r,k}(x,\Gamma) \cdot \frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}} \right) \quad (31)$$

Figures 13a and 13b plot P_{sa} in (31). At $\zeta = 20$, Γ is too high to reduce P_{sa}, but the Robust Code Verification check enables the receiver to limit it to $P_{\text{sa}} < 0.16 \times 10^{-3}$. At $\zeta = 10$, P_{sa} stops growing beyond 0.73×10^{-4}, which limits the adversary's pulses to $k = 495$ for its highest success chance.

Figure 13c shows the effect of β on P_{sa}; P_{sa} is almost constant with β, at around 0.2×10^{-3}, and only starts dropping when β is sufficiently large so that the aggregate energy after the adversary's pulses exceeds Γ. At a certain point, increasing β no longer helps. For example, at $\zeta = 5$ and $\beta \geq 400$, $P_{\text{sa}} \approx 0$. β should thus be set wisely, reflecting the application's sensitivity to distance increases and channel conditions, to avoid increasing transmission lengths unnecessarily.

5.1.3 Symbol length (r)

Figures 13d and 13e plot P_{sa} against the ratio of $r : \alpha$. As shown, longer symbol length (larger r) is better for security; the best results are achieved when the ratio is 1 ($r = \alpha$).

5.1.4 False positives: noise passing Robust Code Verification

Higher-than-usual noise in the channel might satisfy the Robust Code Verification check. Since the receiver backtracks,

it is imperative to calculate the probability, P_{noise}, that noise in the channel satisfies that check. Unlike the adversary's pulses targeted to alter the authentic code, such a candidate trail of noise pulses does not get added to the sender's code because they are at different positions. Without loss of generality, we can separate the noise-intervals in low-energy and high-energy, $e.g.$, across the median of the distribution of N^2. We refer to the number of high-energy intervals as κ. The probability that noise satisfies the Robust Code Verification check is the probability that x of κ pulses fell into Bin_α, by the probability of satisfying the test in that event, $p'_{\alpha,r}(x)$:

$$P_{\text{noise}}(\alpha,\beta,r,\kappa) = \sum_{x=0}^{\alpha} \left(p'_{\alpha,r}(x) \cdot \frac{\binom{\alpha}{x}\binom{\beta}{\kappa-x}}{\binom{\alpha+\beta}{\kappa}} \right) \quad (32)$$

where,

$$p'_{\alpha,r}(x) = \sum_{y=0}^{r} \left(\frac{\binom{\alpha-x}{r-y}\binom{x}{y}}{\binom{\alpha}{r}} \cdot \sum_{i=0}^{y} \frac{\binom{\beta-(\kappa-x)}{r-i}\binom{\kappa-x}{i}}{\binom{\alpha}{r}} \right) \quad (33)$$

This is the probability that an aggregate of y is chosen from Bin_α, and of $\leq y$ from Bin_β. Since we separate along the median, the expected κ is $(\alpha+\beta)/2$. Figure 14 plots P_{noise} against α using (32) at $\kappa = (\alpha+\beta)/2$ and $\beta = 100$. Intuitively (and as the chart confirms), $P_{\text{noise}} \longrightarrow 0.5$ as $\alpha \longrightarrow \infty$.

Since a candidate verification code is discarded as noise if the Robust Code Verification check is satisfied with a probability $< P_{\text{noise}}$ (recall: Fig. 8), the adversary must have a success probability of at least $1 - P_{\text{noise}}$ to hide the authentic code from the receiver. At $r = \alpha$, $P_{\text{noise}}(80, 100, 80, 40) = 0.53$, and the adversary must thus have a success probability of at least 0.47. As this is much higher than the calculated probabilities in Section 5.1.2, the adversary will not be able to disguise authentic code as noise. The value 0.53 is a lower-bound; in practice P_{noise} should be set ≥ 0.53 depending on applications' requirements and channel conditions.

5.2 Validating the Probabilistic Model

The use of prototype implementation using Software Defined Radios (SDRs) and simulations are well-established methods for evaluating wireless systems. Existing SDRs do not support UWB. Therefore, we validate the probabilistic model above with simulations. The channel condition such as noise, multipath effect, and path loss are important factors to consider while designing a wireless system. The IEEE 802.14.4a [18] channel model for different environments is purposefully provided for UWB. The preamble and the verification code are converted into physical layer signals using this model for the outdoor LoS conditions. The model generates the pulse and multipath components to resemble the real world effect of the channel condition. We assume that upper layers, $e.g.$, Medium Access Control (MAC) layer, could decide on when to perform enlargement detection so that it doesn't interfere with

(a) $\beta = 500$; $r = \alpha = 50$. (b) $\beta = 50$; $r = \alpha = 50$. (c) $r = \alpha = 50$. (d) $\alpha = 50$ and $\beta = 500$ (e) $\alpha = 50$ and $\beta = 50$
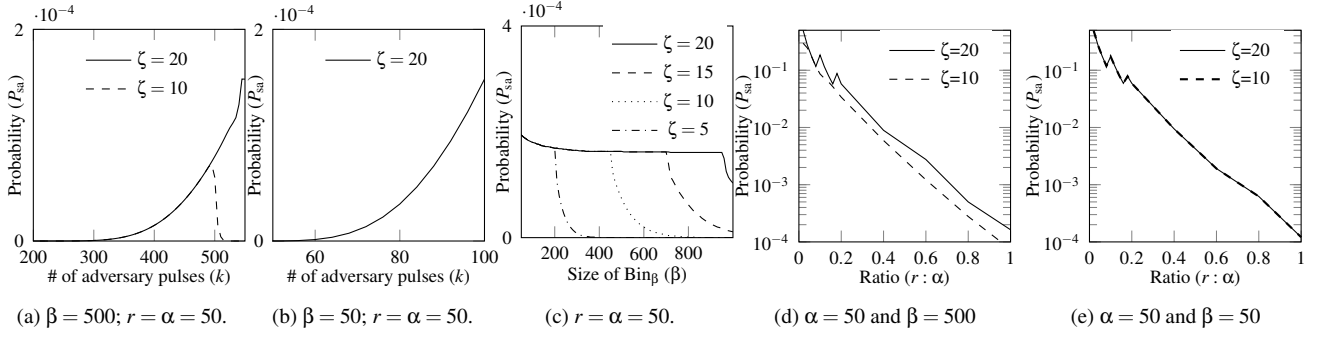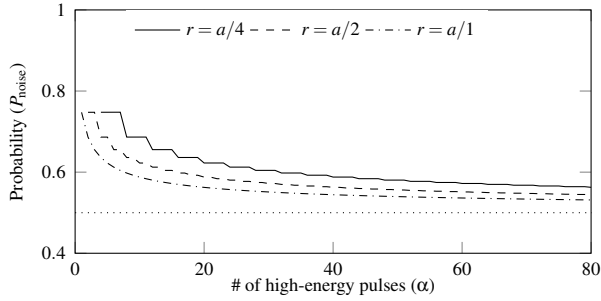
Figure 13: Adversarial success probability in (31).

Figure 14: Probability that noise passes the Robust Code Verification check, calculated using (32); $\kappa = \alpha/2$, $\beta = 100$.

other ranging applications. The simulations account for the noise and interference due to the noise figure of the receiver and multipath components. To verify the simulation setup, we performed a thorough evaluation to cross-check simulation metrics with previous proof-of-concept implementation [26]. Each pulse uses 500 MHz bandwidth, and the sampling time between consecutive pulses is 1 μs. Transmission power is limited to -35 dBm/MHz, well under the limits applied by the FCC/ETSI regulations [11]. The energy is further reduced to adapt to path loss model and extra losses (E; *cf.* Fig. 9).

An adversary is simulated to inject k signals to annihilate or distort the authentic code, and to replay a delayed and amplified versions of the authentic signals. Similar to our assumptions, the adversary in the simulator is capable of annihilating the pulse and its multipath if the phase is guessed correctly; it doubles the amplitude of the pulse otherwise. The time difference between authentic and delayed signals is $\delta = 200ns$ in the simulations (see Fig. 7).

Before demodulation, additive white Gaussian noise (AWGN) is added to the signal. The receiver in Section 2.1 is implemented for code verification; it always locks on to the highest peak, *i.e.,* the peak generated by the adversary due to its replay attack. The communication range is considered 100m, and the backtracking restricted to 660ns.

The goal of our validation is to (1) confirm the probabilistic model's correctness, and (2) analyze the effect of the parameters abstracted from the model, namely noise and the receiver's ability to reconstruct the signal after long distance propagation. In practice, the latter point can be accounted for by increasing the number of pulses ($n = \alpha + \beta$)—see below.

Validating $P_{b\beta > b\alpha}$. Figure 15 shows the validation for $P_{b\beta > b\alpha}$, at a simulated distance between both devices of $d = 10m$. A boxplot is drawn at distinct k, where each scenario is run 10^6 times. The results confirm that abstracting noise from the model does not largely affect its accuracy. Next we show the effect of longer distances on the model.

Validating P_{sa}. Figure 16 shows the validation for P_{sa}, at $r = \alpha$ and $P_{noise} = 0.8$. Results are shown for different k, at distances of 10m and 100m. Each scenario is run 10^6 times, and P_{sa} is calculated as the proportion of these where the adversary succeeded to hide the authentic code. Again the results show comparable patterns between the model and simulations. There is a slight horizontal shift at k due to the abstracted noise. In the simulator, Γ is set as in (9), which may be a bit too high or low depending on actual noise patterns. In Fig. 16a, Γ was relatively low, causing a drop in the simulated P_{sa} at smaller k compared to the model. In Fig. 16b, Γ was relatively high, replicating P_{sa} at higher k.

Another difference between simulations and the model manifests with increasing the distance d between both devices. In practice, in UWB, receivers increase their ability to reconstruct the signals (hence, the SNR) by aggregating over more pulses. We noticed that the model provides such comparable probability patters when we decrease α and β in the model proportionally with increasing d in simulations. For example in Fig. 16b where $d = 100m$, α and β in the simulator had to be increased from 15 and 158 to 50 and 500 respectively ($\sim$ tripled) to account for the increased distance.

Validating the false positives. We also used simulations to confirm that noise would not be falsely mistaken for authentic code upon proper selection of P_{noise} and Γ. For various distances between 10m and 100m, the probability of a false positive was $\sim 1 \times 10^{-6}$, confirming the noise analysis in

(a) {50,50,1} (b) {50,50,2} (c) {50,50,8} (d) {50,150,1} (e) {50,150,2} (f) {50,150,8}
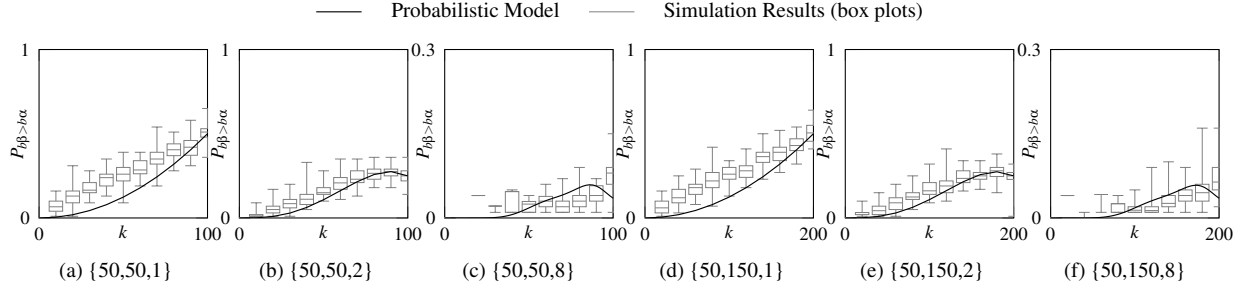
Figure 15: Probability of adversary's failure calculated using (19), and simulations results validating the probabilistic derivations. Each scenario is run with the $\{\alpha, \beta, r\}$ parameters shown in the charts' individual captions.
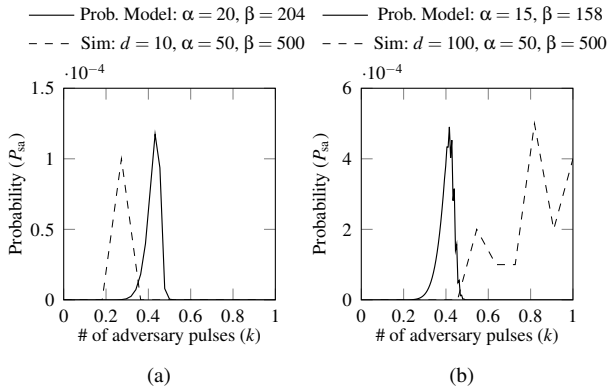

Figure 16: The attack is detected when the aggregate energy is between γ and Γ, but $P_{b\beta>b\alpha}$ is more than P_{noise}. The attack is also detected when energy aggregate is more than Γ; $\zeta = 5$.

Section 5.1.4.

In conclusion, the simulated probabilities follow comparable patterns with the model, and are in the same range. The model derived herein thus serves as a formal means for evaluating the efficacy and suitability of UWB-ED in practice. The results also show that the channel condition, such as path loss, noise, and interference due to multipath components, does not affect the performance and security of the system. An adversary can increase the noise level, which can increase false positives. High false positives may eventually cause DoS (which the adversary can mount anyway by jamming the channel), but the adversary remains unable to enlarge distances.

6 Discussion

Adaptive attacks. An adversary can notice the effect of each of its added pulses on the resultant energy, whether annihilated or amplified. It can then adapt its attack strategy by dynamically deciding k based on the number of pulses it has added/annihilated so far during the transmission. The adversary can then utilize its knowledge of n, α and β in order to, not only decide the optimal value of k statically before the transmission begins, but also adjust their distribution in realtime. This attack does not succeed because the adversary cannot control the resultant pulse phase. Injecting excessive energy in Bin_β exceeds Γ; injecting in Bin_α does not guarantee annihilation because of the unpredictable phase.

Varying energy levels. To achieve perfect signal annihilation, an adversary uses the same amplitude expected at the receiver. Instead of injecting k pulses each with a constant energy of, *e.g.,* $2\mu W$, the adversary can inject one pulse with an energy of, *e.g.,* $2k\mu W$. If all k pulses fell in Bin_β, the aggregate energy would be the same as when that single high-energy pulse also falls in Bin_β. However, intuitively, the adversary is better off injecting multiple pulses with constant energies for two reasons. First, multiple pulses in Bin_β have higher chances of being selected than a single pulse, thus evading the Robust Code Verification check. Second, for those that fall in Bin_α, any leftover energy after annihilating a pulse, regardless of the phase, will be counted towards the overall aggregate, thus hurts the adversary's cause.

Influencing Γ through distance shortening. Instead of enlarging distances directly, the adversary can first mount a distance-reduction attack to trick the devices into using higher Γ (recall: smaller signal attenuation due to shorter path loss leads to higher Γ calibration). It is thus imperative to complement UWB-ED with a distance-reduction detection [5, 6, 26]. Devices should alternate between both techniques; *e.g.,* if distances of d_1 and d_2 are verified using respectively UWB-ED and a distance-reduction detection technique, it should be concluded that the actual distance, d, is in the range $d_1 \leq d \leq d_2$ (d_1 is a lower bound, d_2 an upper).

Influencing the number of pulses, n. An adversary can inject a low stream of noise-like energy, not too high to be detected as jamming. However because Γ is set beforehand, it is not influenced by the adversary. By injecting noise, the adversary actually hurts its own cause as it reduces the amount of energy it can use strategically to prevent code detection.

Integrating UWB-ED with 802.15.4z and 5G. The 802.15.4z enhanced impulse radio task group is defining a

series of physical layer improvements to provide secure and precise ranging [2]. Those include additional coding, preambles, and improvement to existing modulations to increase ranging integrity and accuracy. UWB-ED is a potential candidate for enlargement detection in 802.15.4z. It adheres to the low pulse repetition (LRF) mode frequency (1-2 MHz), works with non-coherent receivers, and supports up to 100m.

The 3GPP technical specifications groups are designing the 5G-new radio technology, and it aims to include secure and precise ranging based on wireless signals [16,33]. Properties such as high carrier frequencies, large bandwidths, large antenna arrays, device-to-device communication, and ultra-dense networking will help attain this objective. It is early to say the exact modulation techniques 5G will use for distance measurement, but it is safe to assume that wideband will be used to attain position accuracy; beamforming techniques will achieve long distances. This system is equivalent to setting $r = 1$ herein without restrictions on α, as transmission power restrictions imposed on UWB do not apply to 5G. However, the security of 5G can be increased further, as it allows for the use of beamforming and coherent receivers.

7 Related Work

Detecting enlargement attacks has lately been a prominent research area. Previous literature explored timing acquisition at the preamble, and data ambiguity at payload. Taponecco *et al.* [27] show that the success of enlargement attacks using replay (or overshadowing) depends on the amount of delay the adversary introduces. Such success is harder for controllable attacks, where the adversary is required to position nodes at specific locations. Compagno *et al.* [8] provide a probabilistic model for the success of overshadowing attacks, which captures different channel conditions and leading edge detection techniques for ToA estimation. None of the above efforts considered adversarial signal annihilation.

Tippenhauer *et al.* [29] explored a theoretical approach to detect adversarial signal annihilation for distance enlargement: using a single pulse-per-symbol (consecutive integration windows represent a symbol). They found that modulation with a 2ns slot size, *i.e.,* mostly equivalent to a pulse width, might help detect signal annihilation. This, however limits the ranging technique to short distances. The effect of multipath on that scheme in practice is also unclear, since reflected signals would directly interfere with authentic ones causing distortion (no empty gaps between authentic pulses). In contrast, UWB-ED allows for increased distances by increasing the symbol length, and the sampling time between consecutive pulses is sufficient to handle the multipath effect.

8 Conclusion

We present UWB-ED—the first known technique to detect distance-enlargement attacks against standard UWB ranging systems. UWB-ED is readily deployable for current off-the-shelf receivers, requiring no additional infrastructure. Evaluation is performed by deriving the probability of adversarial success in mounting distance enlargement attacks. Results show that the verification code structure herein prevents signal annihilation. The code also allows the use of longer symbol length at the receiver, which is essential to achieve longer distance in the energy constrained UWB system. UWB-ED is thus a good candidate for enlargement detection in practice (*e.g.,* for 802.15.4z and 5G).

References

[1] 3db. 3db Access AG - 3DB6830 ("proximity based access control"). https://www.3db-access.com/Product.3.html. [Online; Accessed 22. October 2018].

[2] Task Group 4z. IEEE 802.15 WPAN "enhanced impulse radio". http://www.ieee802.org/15/pub/TG4z.html. [Online; Accessed 22. October 2018].

[3] P. Bahl and V. N. Padmanabhan. RADAR: an in-building RF-based user location and tracking system. In *IEEE INFOCOM*, volume 2, pages 775–784, 2000.

[4] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker. The Directional Attack on Wireless Localization -or- How to Spoof Your Location with a Tin Can. In *IEEE GLOBECOM*, pages 1–6, 2009.

[5] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Towards Secure Distance Bounding. Cryptology ePrint Archive, Report 2015/208, 2015. https://eprint.iacr.org/2015/208.

[6] Stefan Brands and David Chaum. Distance-bounding protocols. In *EUROCRYPT*, pages 344–359. Springer, 1994.

[7] M. Cagalj, S. Čapkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J. Hubaux. Integrity (I) codes: message integrity protection and authentication over insecure channels. In *IEEE Symposium on Security and Privacy (S&P)*, pages 15 pp.–294, 2006.

[8] A. Compagno, M. Conti, A. A. D'Amico, G. Dini, P. Perazzo, and L. Taponecco. Modeling Enlargement Attacks Against UWB Distance Bounding Protocols. *IEEE Transactions on Information Forensics and Security*, 11(7):1565–1577, 2016.

[9] DecaWave. DecaWave "dw1000 product description and applications". https://www.decawave.com/products/dw1000. [Online; Accessed 22. October 2018].

[10] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[11] Robert J Fontana and Edward A Richley. Observations on low data rate, short pulse uwb systems. In *IEEE International Conference on Ultra-Wideband (ICUWB)*, pages 334–338, 2007.

[12] Shyamnath Gollakota, Nabeel Ahmed, Nickolai Zeldovich, and Dina Katabi. Secure in-band wireless pairing. In *USENIX Security Symposium*, 2011.

[13] Humatics. Time Domain's PulsON ("p440"). http://www.timedomain.com/products/pulson-440/. [Online; Accessed 23. October 2017].

[14] Todd E. Humphreys. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *Institute of Navigation GNSS (ION GNSS)*, 2008.

[15] Benjamin Kempke, Pat Pannuto, and Prabal Dutta. SurePoint: Exploiting Ultra Wideband Flooding and Diversity to Provide Robust, Scalable, High-Fidelity Indoor Localization. In *ACM SenSys*, pages 318–319, 2016.

[16] Xingqin Lin, Jingya Li, Robert Baldemair, Thomas Cheng, Stefan Parkvall, Daniel Larsson, Havish Koorapaty, Mattias Frenne, Sorour Falahati, Asbjörn Grövlen, and Karl Werner. 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology, 2018.

[17] A. F. Molisch. Ultrawideband propagation channels-theory, measurement, and modeling. *IEEE Transactions on Vehicular Technology*, 54(5):1528–1545, 2005.

[18] A. F. Molisch, D. Cassioli, C. Chong, S. Emami, A. Fort, B. Kannan, J. Karedal, J. Kunisch, H. G. Schantz, K. Siwiak, and M. Z. Win. A Comprehensive Standardized Model for Ultrawideband Propagation Channels. *IEEE Transactions on Antennas and Propagation*, 54(11):3151–3166, 2006.

[19] Andreas F. Molisch. *Wireless Communications*. Wiley Publishing, 2nd edition, 2011.

[20] Andreas F. Molisch, Kannan Balakrishnan, Chia chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal, Juergen Kunisch, Hans Schantz, Ulrich Schuster, and Kai Siwiak. IEEE 802.15.4a channel model - final report. In *Converging: Technology, work and learning. Australian Government Printing Service*. [Online; Accessed 4. November 2018], 2004.

[21] A. Muqaibel, A. Safaai-Jazi, A. Bayram, and S. M. Riad. Ultra wideband material characterization for indoor propagation. In *IEEE Antennas and Propagation Society International Symposium*, volume 4, pages 623–626, 2003.

[22] Pericle Perazzo, Lorenzo Taponecco, Antonio A. D'amico, and Gianluca Dini. Secure Positioning in Wireless Sensor Networks Through Enlargement Miscontrol Detection. *ACM Transactions on Sensor Networks*, 12(4):27:1–27:32, 2016.

[23] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Čapkun. Investigation of Signal and Message Manipulations on the Wireless Channel. In Vijay Atluri and Claudia Diaz, editors, *Computer Security – ESORICS 2011*, pages 40–59. Springer, 2011.

[24] Swiss Post. Drones as transportation vehicle. https://www.post.ch/en/about-us/company/media/press-releases/2017/swiss-post-drone-to-fly-laboratory-samples-for-ticino-hospitals, May 2018.

[25] Mary-Ann Russon. Drones to the rescue! http://www.bbc.com/news/business-43906846, May 2018.

[26] Mridula Singh, Patrick Leu, and Srdjan Čapkun. UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks. In *NDSS*, 2019.

[27] L. Taponecco, P. Perazzo, A. A. D'Amico, and G. Dini. On the Feasibility of Overshadow Enlargement Attack on IEEE 802.15.4a Distance Bounding. *IEEE Communications Letters*, 18(2):257–260, 2014.

[28] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Čapkun. Attacks on Public WLAN-based Positioning. In *ACM/Usenix MobiSys*, 2009.

[29] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, and Srdjan Čapkun. Physical-layer Integrity for Wireless Messages. *Computer Networks*, 109(P1):31–38, 2016.

[30] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In *USENIX NSDI*, pages 165–178, 2016.

[31] S. Čapkun and J. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE Computer and Communications Societies.*, volume 3, pages 1917–1928, 2005.

[32] K. Witrisal, G. Leus, G. J. M. Janssen, M. Pausini, F. Troesch, T. Zasowski, and J. Romme. Noncoherent ultra-wideband systems. *IEEE Signal Processing Magazine*, 26(4):48–66, 2009.

[33] Henk Wymeersch, Gonzalo Seco-Granados, Giuseppe Destino, Davide Dardari, and Fredrik Tufvesson. 5G mmWave Positioning for Vehicular Networks. *Wireless Communications*, 24(6):80–86, 2017.

[34] Paul A Zandbergen. Accuracy of iPhone locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning. *Blackwell Transactions in GIS*, 13(s1), 2009.

[35] Zebra Technologies. "sapphire dart ultra wideband (uwb) real time locating system 2010.". https://www.zebra.com/us/en/solutions/location-solutions/enabling-technologies/dart-uwb.html. [Online; Accessed 22. October 2018].

Errata Slip #5
Proceedings of the 28th USENIX Security Symposium

In the paper "UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband" by Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun, *ETH Zurich* (Wednesday session, "Wireless Security," pp. 73–88 of the Proceedings) the authors have provided an acknowledgment: