V-Range: Enabling Secure Ranging in 5G Wireless Networks

V-Range: Enabling Secure Ranging in 5G Wireless Networks

Mridula Singh[1], Marc Röschlin[1], Aanjhan Ranganathan[2], and Srdjan Capkun[1]

[1]Dept. of Computer Science, ETH Zurich
[2]Khoury College of Computer Sciences, Northeastern University

Abstract

A number of safety- and security-critical applications such as asset tracking, smart ecosystem, autonomous vehicles, driver assistance functions, etc. are expected to benefit from the position information available through 5G. Driven by the aim to support such a wide-array of location-aware services and applications, the current release of 5G seeks to explore ranging and positioning [12] as an integral part of 5G technology. In recent years, many attacks on positioning and ranging systems have been demonstrated, and hence it is important to build 5G systems that are resilient to distance and location manipulation attacks. No existing proposal either by 3GPP or the research community addresses the challenges of secure position estimation in 5G. In this paper, we develop V-Range, the first secure ranging system that is fully compatible with 5G standards and can be implemented directly on top of existing 5G-NR transceivers. We design V-Range, a system capable of executing ranging operations resilient to both distance enlargement and reduction attacks, including a novel carrier-frequency offset attack where an adversary can undermine the distance calculation by manipulating the *carrier-frequency offset estimation*, a key component responsible for detecting data in 5G-NR receivers. We experimentally verify that V-Range achieves high precision, low-latency, and can operate in both the sub-6GHz and mm-wave bands intended for 5G. Our results show that an attacker cannot reduce or increase the distance by more than the imprecision of the system, without being detected with high probability.

1 Introduction

5G is the next-generation cellular networking technology designed to increase data speeds while realizing a flexible wireless communication infrastructure. The advent of autonomous machines such as self-driving cars, smart ecosystems (e.g., smart homes, cities, and factories), and the Internet of Things has led to a rapid increase in data processing and communication requirements, which will soon exceed the capabilities 4G and all other predecessors of 5G. Besides low latency and improved configurability, 5G is supposed to offer high-precision indoor and outdoor location and positioning services. 3GPP, the standards organization responsible for the development of the 5G New Radio (5G-NR) architecture, intends to enable and improve state-of-the art positioning techniques that make use of the high bandwidth and the network architecture of 5G [1, 12]. In fact, the availability of larger bandwidth in millimeter wave frequencies makes 5G a perfect fit for high-accuracy positioning of end-devices. Several applications, including asset tracking, unmanned aerial vehicles, autonomous navigation, automated supply chains in manufacturing industry, etc., are expected to benefit from both absolute and relative positioning.

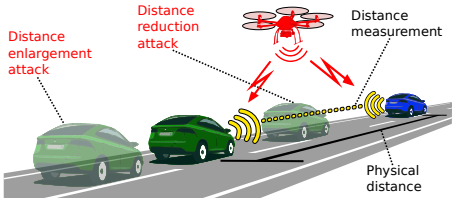

Figure 1: Example scenario. Distance reduction can result in unexpected emergency braking and evasive maneuvers. Distance enlargement can even lead to a collision.

One of the main use cases for 5G-enabled positioning is Vehicle-to-Vehicle (V2V) and Vehicle-to-Anything (V2X) communication, as depicted in Figure 1. The precise distance measurements that 5G provides will increase the contextual awareness of every individual road user and improve road safety as a whole [15, 23]. However, location information that can be obtained through positioning and ranging are not only expected to augment services running on top of the 5G infrastructure, but also target use cases within the architecture of 5G itself, such as localization during emergency calls. 3GPP and other standardization bodies are thus actively working with industry and academia partners to define the performance require-

*mridula.singh@inf.ethz.ch
†marc.roeschlin@inf.ethz.ch
‡aanjhan@northeastern.edu
§srdjan.capkun@inf.ethz.ch

ments for 5G positioning systems. Even though 3GPP has put forward a plan to introduce positioning and ranging into 5G, the current release evaluates different potential solutions mainly from the perspective of system performance [21, 45]. Many of the presented use cases for 5G positioning reside in a security- or safety-critical context, and therefore, it is crucial to devise a localization and ranging mechanism that is both precise and secure, i.e., it must not be subverted by adversarial interference.

Designing a secure localization mechanism based on radio frequency transmission is an intricate task. Establishing location typically requires estimating the physical distance between two or more entities. The majority of existing radio frequency-based distance measurement techniques have shown to be vulnerable to distance modification attacks [26, 30, 38, 39, 42, 43]. For example, researchers have repeatedly demonstrated the vulnerability of passive keyless entry systems in automobiles to relay attacks [25]. Although the key was several tens of meters away from the car, it was possible to open the car and drive away by relaying the radio frequency signals between the car and the key. The described scenario is an instance of a distance reduction attack. Distance enlargement can be more devastating, especially in autonomous cyber-physical systems such as vehicle platoons and adaptive cruise control (see Fig. 1) [46, 48].

Secure distance measurement based on ultra-wideband radio (UWB) has shown to be a promising technology that can thwart some of these attacks. UWB-enabled ranging is described in the recent IEEE 802.15.4z standard [14] and has led to a number of commercial deployments [7, 10]. While insights from UWB ranging can be used as a stepping stone, there are several challenges that need to be addressed to realize a secure positioning system in 5G networks. For example, unlike UWB, 5G uses OFDM symbols at the physical layer, which makes 5G based ranging vulnerable to distance manipulation attacks. Furthermore, 5G uses coherent receivers i.e., the received signal must be phase synchronized with a reference for proper decoding; thereby posing additional challenges in the receiver design.

In this work, we make the following contributions: We design the first secure ranging system for 5G-NR radio architecture and demonstrate that our system is secure against both distance reduction and enlargement attacks. We enumerate the challenges that need to be addressed in order to enable secure positioning in 5G. We design a solution that can be integrated into the 5G-NR radio architecture and therefore does not affect or deviate from existing standards and proposals. We build a proof-of-concept for sub-6GHz and mm-wave modes of 5G communication and evaluate their performance and security guarantees. We identify a novel *carrier-frequency offset attack* that specifically affects 5G-NR based systems and show that our proposed design is resilient to such an attack. The V-Range system uses shortened OFDM symbols in which energy is aggregated over a short time period. By applying proper data and sample level integrity checks, a V-Range receiver can ensure that distance estimation is correct. The short effective symbol length and added integrity checks at the receiver make all known reduction and enlargement attacks impracticable. Our security analysis confirms that V-Range constitutes a highly secure ranging system. When using 16-QAM modulation, the success probability of a reduction attack is 10^{-7}, and an enlargement attack can be carried out with a likelihood lower than 10^{-5}. The probabilities we derive in this work are computed *per* ranging operation and consider the case where an attacker can modify the measurement by more than the imprecision of the system, i.e., 3m for sub-6Ghz and 60cm for mm-wave band. In addition to secure and precise ranging, our solution can perform a (two-way) time of flight measurement in 83 μs, allowing for a high refresh rate and high temporal resolution in a scenario with many involved devices.

2 Background and Related Work

2.1 5G New Radio (5G-NR)

5G has a dynamic Time Division Duplex (TDD) frame structure; the frames are divided into subframes and slots. Slots are either dedicated entirely to the uplink or downlink channel, or be configured to allow both uplink and downlink. Every symbol in a slot can also be configured in a variety of ways based on the application. For device-to-device communication (e.g., vehicle-to-vehicle communication), or in the absence of a base station, the device initiating the communication within a slot is considered to transmit on the downlink channel and any other (responding) device on the uplink channel. This allows two devices to use the same slot [22].

Every slot consists of 14 orthogonal frequency-division multiplexing (OFDM) symbols. However, 5G-NR standard allows accommodating more symbols using slot aggregation. The OFDM is a digital multi-carrier modulation scheme that makes use of a large number of closely-spaced orthogonal subcarriers transmitted in parallel. The symbol length (T_{sym}) depends on the bandwidth of the subcarriers, and not on the total bandwidth of the system. For example, an OFDM symbol in 5G-NR can have a minimum symbol length of 2.08 μs (at subcarrier bandwidth of 480 kHz), irrespective of the total bandwidth allocated to the system. Devices operating in sub-6GHz frequency bands support subcarrier spacing of up to 60 kHz, and mm-wave devices support much higher subcarrier bandwidth, up to 480 kHz.

2.2 Positioning with 5G-NR

Several public and private companies, including hardware and equipment manufacturers, space agencies, and mobile network operators, are pushing for the delivery of higher accuracy and precision by cellular location services to enable a new generation of commercially motivated location-based services.

As a result, 3GPP and other standardization bodies are taking a fresh look at the application space and performance requirements for cellular positioning in their upcoming

releases. Compared to earlier cellular communication standards, 5G-NR's flexible design, wider bandwidth, mmWAve frequency bands, massive MIMO capabilities make it ideal for realizing high precision, low-latency ranging systems [50]. 3GPP is already exploring the feasibility of using different distance measurement techniques such as round trip time, time of arrival, angle of arrival, and carrier-phase based techniques [12, 17] and designing new signals to support the various ranging techniques. 3GPP is currently focused on ensuring seamless availability of 5G-NR-based positioning to a multitude of applications such as asset tracking, smart cities, healthcare, UAVs, augmented reality, and many more. In the transportation sector, the ranging system is expected to support traffic management and collision prevention with several field tests already ongoing to explore capabilities of 5G enabled vehicle-to-everything communication and ranging [23].

2.3 Ranging Systems

Numerous ranging techniques that use radio communication signals have been developed in the recent years. Broadly, there are two types of radio frequency ranging systems. One set of ranging systems compute distances by measuring one or more physical properties (e.g., amplitude, phase and frequency) of the signal such as received signal strength [18], multicarrier phase ranging [49], frequency modulated continuous wave radars etc.. These systems although simple to implement, are more susceptible to channel interference effects and require extensive error correction. Alternatively, ranging systems can compute distance based on measuring round-trip time of flight [20], time of arrival [31], and time difference of arrival of the radio frequency signals. The total time a signal traveled from one device to the other is directly proportional to the distance, as radio waves are assumed to propagate at the constant speed of light. Hence, to measure distance, the receiver only has to determine the point in time at which the signal arrived. This operation is called *leading edge detection* and works by continuously sampling the incoming signal and performing a *search* on the acquired samples to determine the beginning of the signal. Leading edge detection is challenging as the signal can be affected by multipaths, fading and attenuation while on its way to the receiver.

Distance Manipulation Attacks: Ranging systems that do not specifically provision against adversarial influence are susceptible to distance manipulation attacks. An external attacker can reduce or enlarge the distance measured by benign devices. The system based on signal properties such as received signal strength and signal phase are vulnerable to relay attacks, e.g., relay attack on keyless entry systems in Automobiles [42]. For example, in a RSSI-based ranging system, an attacker can manipulate the estimated distance by simply amplifying and forwarding the radio frequency signals. Similarly, an attacker can shift the frequency or delay the phase to cause distance modification in systems that rely on frequency and phase estimations for ranging. In general, we can conclude that ranging systems that rely on physical-layer signal characteristics are easily vulnerable to distance manipulation attacks.

Alternatively, the ToF/ToA based ranging system appear to be more secure against amplify and forward relay attacks. However, several demonstrations have indicated that the ToF ranging systems, if not designed to meet certain requirements at both the physical- as well as data-layer, are vulnerable to more sophisticated early detect and late commit attacks (ED/LC) for distance reduction and replay attacks for distance enlargement [24, 38, 39, 44]. Currently, the UWB with the two-way ToF measurement with secure logical layer and physical layer design is the only system that can thwart both reduction and enlargement attack [46, 47] with several ongoing discussion on standardising it. However, there is no indication that 5G-NR is going to implement or incorporate secure UWB ranging into its standards. In fact, several standards committee briefing [12] and academic research [50] indicates direct use of the current 5G-NR physical-layer to build a wide-area positioning infrastructure. Therefore, in this paper we analyse the security guarantees of 5G-NR based ranging system and propose modifications to enable secure ranging and positioning.

3 Attacks on OFDM-based Ranging Systems

The goal of the adversary is to force two benign devices to measure a false distance without physically displacing them. We consider both distance enlargement, and distance reduction attacks as both of them have the potential to cause catastrophic failures in 5G networks. For example, in the case of vehicular platoons, distance enlargement attacks can cause cars to accelerate, and reducing the measured distance will result in the vehicle applying the emergency brakes. Figure 1 shows how an attacker, e.g., a rogue vehicle or a roadside attacker, can modify the measured distance between two cars that rely on 5G for contextual awareness. We assume that the attacker can transmit, eavesdrop, intercept, record, and replay arbitrarily strong radio frequency signals. The described attacker model captures the capabilities of any man-in-the-middle (MITM) attack in a wireless network and is commonly used to assess the security of wireless protocols [19, 29]. In addition to the above, we assume that the attacker has the ability to annihilate (using a reciprocal) or overshadow legitimate signals. However, we assume that the adversary cannot physically tamper the device nor compromise their firmware in any other way. We further assume that the cryptographic primitives used are fully secure and focus on realizing a 5G-NR ranging solution that is secure against physical-layer distance manipulation attacks as these attacks are independent of higher layer cryptographic primitives.

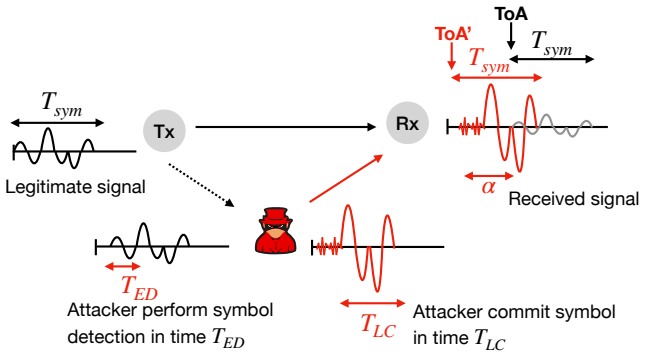

Figure 2: Distance reduction by early detect late commit attack on the longer symbols.

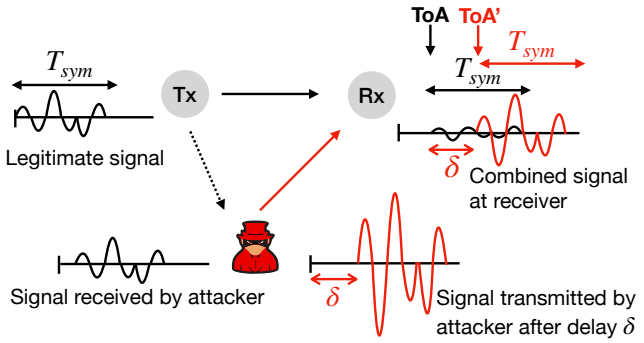

Figure 3: Distance enlargement by symbol overshadowed attack.

receiver design needs to be improved for secure ranging.

3.1 Distance Reduction by Early-Detect & Late-Commit

5G-NR predominantly uses OFDM, and the use of OFDM symbols leads to the possibility of distance reduction by ED/LC attacks [39, 43]. In the early detection phase, the adversary detects a symbol using the initial part, i.e., within $T_{ED} < T_{sym}$. In the late-commit phase, the adversary forges the symbol such that the small initial part of the symbol is noncommittal, whereas the last part of the symbol T_{LC} is sufficient to generate correct data. This way, the attacker can start sending a symbol before knowing what data the symbol encapsulates and advance arrival time of symbol by time α. As an attacker needs to know the initial part of the symbol, the maximum distance reduction is bounded by the symbol length (i.e., $\alpha < T_{sym}$). According to 5G numerology, the minimum length of the OFDM symbol is 2.08 μs and can result in a gain of more than 300 m even if the adversary takes half of the symbol duration to predict [1]. Alternatively, the attacker can exploit the repetitive nature of cyclic prefix and transmit a time-advanced copy creating a signal that arrives earlier than the authentic signals and reducing the measured time-of-flight; thereby successfully executing a distance reduction attack. Such attacks have already been demonstrated [4] and can be considered as a form of late commit attack.

To limit the effect of ED/LC attacks in 5G-NR, the information transmitted as part of the ranging operation has to be encapsulated in short symbols. This reduces the chances for distance manipulation, as symbol length limits the theoretical time a signal can be advanced/delayed by an adversary. This means we need to design and ensure that the 5G-NR symbols are as short as possible while conforming to the properties and requirements set by the 5G numerology. It should be noted that the security of a ranging system also depends on the receiver design. In Section 5, we show that, if the receiver were to perform a standard OFDM demodulation routine and apply FFT over all samples before interpreting them, even shortened OFDM symbols are vulnerable to ED/LC attack. We explain how the

[1] radio waves travel 30 cm in 1 ns

3.2 Distance Enlargement by Overshadowing Symbols

An adversary can enlarge the measured distance by performing a signal overshadow attack, as shown in prior works [44, 51]. In a signal overshadow attack (Figure 3), the attacker transmits a delayed copy (say with a time delay δ) of the legitimate signal with a higher power to completely hide the legitimate signal. Even though a small part of the legitimate signal arrives at the receiver without delay, the high power of the delayed attacker signal forces the receiver to discard the legitimate signal as noise. Therefore, the receiver would use the stronger attacker signal for ToA estimation. Furthermore, since the attacker's signal is a delayed copy of the legitimate signal, it contains the correct data, thus leading to a successful attack.

The attacker succeeds in introducing delay δ if the energy received in time δ is not sufficient for detection and the receiver discards it as noise. OFDM receivers use all $\hat{N}$ samples, transmitted in time T_{sym} to estimate ToF. Even when detecting the OFDM symbol data, all $\hat{N}$ samples are needed, as the energy of each bit is distributed over the $\hat{N}$ samples. By receiving a small part of the symbol, the receiver is incapable of symbol detection. The attacker can choose the value of δ such that it is insignificant for symbol detection, but enough to perform meaningful distance enlargement. We note that the attacker can cause significant distance enlargement in 5G-NR systems with a delay $\delta \ll T_{sym}$. For example, if the 5G-NR system uses symbol length T_{sym} of 16.67 μs (at subcarrier bandwidth of 60 kHz), and the overshadowing signal arrives after a delay of $\delta = .1667\mu s$ (one percent of symbol length), the energy detected at the receiver in time $.1667\mu$ is not sufficient to perform the symbol detection or impulse response estimation, and therefore the receiver uses the higher strength overshadow attack signal for the ToF measurement. With a δ of $.1667\mu s$, an attacker can acheive a distance enlargement of 50 m. By increasing the value of δ, the attacker can easily achieve several hundred meters of distance enlargement. Therefore, inorder to protect against distance enlargement attacks by

overshadowing, it is also essential to implement symbols that have energy aggregated over a short time duration.

3.3 Distance Enlargement by Carrier Frequency Offset Attack

In this section, we introduce a novel attack called *carrier frequency offset attack*. The carrier frequency offset can be viewed as a special case of distance enlargement; an attacker takes advantage of the predictable reference signals and coherent receiver design. In a ToF ranging system, it is crucial that the transmitter and the receiver tune to the same carrier frequency for secure and precise ToF estimation. This assumption also holds for any wireless system requiring integrity of the signal, see, e.g., [19, 29]. Even though the carrier frequency f_c can be precisely and secretly communicated to the devices, due to the mismatch in the transmitter and the receiver frequency oscillator [37], the devices will experience carrier frequency offset (CFO) and phase offsets. The offset is typically corrected with the help of reference signals. For example, the preamble in Ultrawideband high rate pulse mode (UWB-HRP) [3], training sequences in the WiFi [27], and phase tracking reference signals and synchronization signals in 5G [34, 40]. A receiver can estimate the carrier frequency offsets using expected and received reference signal, and adjust the receiver to correct the offsets. The presence of offset results in inter-carrier interference, a decrease in signal amplitude, and phase rotation. The incorrect offset estimation in conventional communication systems leads to high symbol error rate and potentially a denial of service, due to the imbalance in the in-phase and quadrature component of the signal's power distribution. In a ranging system, an incorrect offset estimation results in a time-shift of received signals affecting the measured distance directly. Unfortunately, the use of fixed reference signals for offset estimation also makes coherent receivers, including 5G-NR, vulnerable to distance modification attacks. Instead of correcting the offset, an attacker can use reference signals to increase their offset. The reference signal is predictable; an attacker can modify, annihilate, or delay it. We show an attack on the ranging system by using frequency offset manipulation.

As shown in Figure 4, distance manipulation happens in two steps. First, an attacker performs the overshadowing attack on the reference signal, which are also OFDM symbols. The attacker's hardware oscillator error e'_a is different from the oscillator at the legitimate transmitter e_a, and the attacker signal also has a higher power. The attacker's high power signal affects the frequency offset (Δ) estimation at the receiver – the new estimated offset (Δ') is incorrect to recover legitimate transmission. In the second step, the attacker replays the legitimate signal with a delay δ calculated based on the oscillator error e'_a. As the receiver is tuned to an incorrect offset Δ', it *locks on* to the attacker's replayed signal and decodes the correct data but at a time offset thereby increasing the measured distance. The receiver discards the legitimate signal as noise (strong multi-

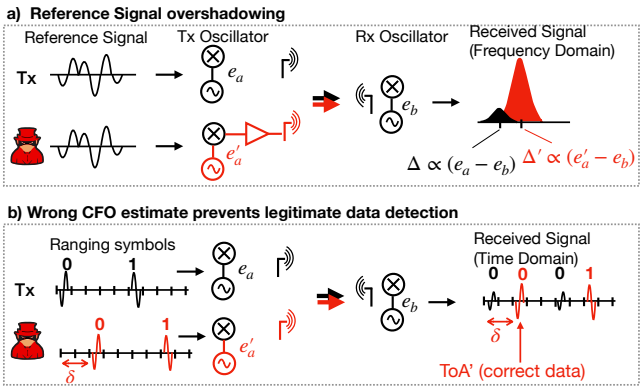

Figure 4: Distance enlargement by manipulating frequency offset estimation.

path) as it does not provide correct data even though it has finite energy. In Figure, the attack is shown using short symbols to emphasize that short symbols are also vulnerable to the offset manipulation attack. Until recently, only ToF measuring systems based around energy detector as receivers are proven to be secure against distance manipulation attacks [46], and issues occurring due to the minor carrier frequency mismatch were not of importance. In Section 6, we show that offset mismatch of 10 KHz is sufficient to prevent data detection [2].

3.4 Mitigating 5G-NR Ranging Attacks

From the above, there are several fundamental requirements for building a secure 5G-NR ranging system. First, the information transmitted as part of a ranging operation needs to be encapsulated within short symbols. This significantly reduces the effects of distance manipulation as symbol length limits the theoretical time a signal can be advanced/delayed by an adversary. However, the shortest symbol duration available in 5G-NR is around 2 μs and can result in several hundred meters of distance manipulation. In other words, it is essential to limit the symbol duration significantly to prevent distance manipulation attacks.

The use of short symbols is insufficient to prevent distance enlargement attacks, as demonstrated by the carrier frequency offset attack, and in order to realize a secure 5G-NR ranging system, it is essential to eliminate the use of predictable reference signals, e.g., for synchronization in coherent receiver designs. The receiver needs to implement integrity checks at both the physical- and data-level to guarantee unmodified delivery of time-critical messages. These checks need to be carefully engineered, guaranteeing security against a variety of communication channel conditions without raising a number of false alarms [33, 47]. The designed system should ensure to the maximum extent possible that the legitimate signal is not discarded as noise since this leads to the enlargement attack

[2] Transceivers operating at 4 GHz and the clock error of 10 ppm expect carrier frequency offset up to $\pm$80 KHz

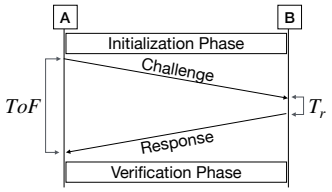

Figure 5: Device A and B run a distance bounding protocol to acquire the time-of-flight (ToF) and measure the distance.

success [46]. In other words, we need integrity and sanity checks that account for anomalies that can result from the legitimate communication channel conditions while detecting all known distance manipulation attacks.

4 V-Range – Secure Ranging in 5G

4.1 System Overview

As shown in Figure 5, V-Range uses time-of-flight (ToF) i.e., a device A measures its distance to another device B based on the time elapsed between transmitting a cryptographically-generated challenge signal and receiving a corresponding response from B. We assume that the logical-layer algorithms and protocols (e.g., distance bounding protocols) used to generate the challenges and responses are secure, i.e., an adversary cannot manipulate distance measurement by simply guessing the challenges or the responses. Distance bounding protocols pre-share a secret in the initialization phase to check the integrity of challenges and responses. Many 5G use-cases already maintain shared secrets between devices. They, therefore, prevent the need for the initialization phase, e.g., communication in vehicular networks must ensure privacy, confidentiality, integrity, and nonrepudiation, irrespective of ranging capabilities [28]. The 5G's flexible slot length allows the transmission of challenge and response of a flexible length. We assume that the ranging devices negotiate the transmission schedules and their slot assignment as part of the standard medium access, i.e., transmitter initiates transmission of ranging signal at a pre-negotiated time. The receiver needs to initiate the signal reception a bit earlier than the pre-negotiated time. This is needed to account for the reference clock mismatch between the two devices. The devices agree in advance which numerology and modulation are to be used during the ranging operation.

Standard 5G symbols transmitted using OFDM are long (i.e., few μs) and, therefore, are vulnerable to distance reduction and enlargement attack. The V-Range transmitter compresses the OFDM symbol length by transmitting the same symbol in all subcarriers; this is in contrast to conventional OFDM, in which each of the subcarriers can carry different data. The results in the aggregation of symbol energy over a short time period (i.e., few ns), making it harder for an attacker to perform early-detect/late-commit distance reduction attack. The short effective symbol length results in increased ranging resolution.

The ToA of these symbols is validated by physical layer

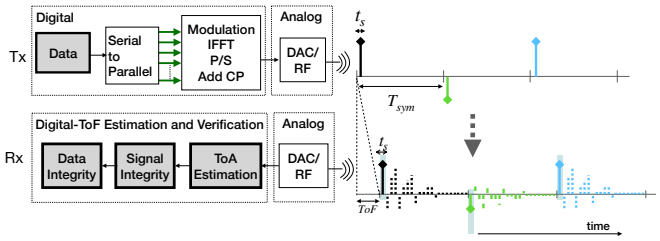

Figure 6: The V-Range system uses shortened OFDM symbols, and the receiver performs integrity checks for ToA estimation and validation.

properties and data at the logical layer. Similar to LTE, 5G uses fixed reference signals to enable phase-tracking, synchronization, and data decoding. An attacker can spoof the reference signals and force *out of turn* transmissions and incorrect decoding of data at the receiver resulting in false distance measurements. In contrast, V-Range does not use any fixed reference signals, and its receiver relies on a custom algorithm for data detection. An attacker can cause distance enlargement attacks by relaying a delayed version of the challenges and responses. Moreover, an attacker can perform signal annihilation to prevent legitimate signal detection at a smart receiver. In V-Range, we implement a signal integrity checker algorithm based on inspecting the energy variance of the received symbols and show that V-Range is capable of detecting such an attempt at distance enlargement attack.

The V-Range system design shown in Figure 6 can be summarized as follows. The device performs the initialization phase and pre-shares data for secure ranging, which is then transmitted by using shortened OFDM symbols. In these symbols of length T_{sym}, energy is aggregated over much smaller part t_s of the symbol. The receiver searches for the ToA of the signal by using granular samples of length t_s. The signal is considered to be a probable leading edge if the average power of these samples is more than the noise threshold (T_{Noise}) and less than threshold (T_{max}). The threshold T_{max} is used to detect the possibility of the receiver's saturation; if an attacker overloads the receiver with too much power (e.g., jamming signal), then the data cannot be recovered. Each receiver can select T_{max} based on its maximum acceptable power (i.e., dynamic range). The signal is used for ranging only after signal integrity (i.e., power distribution) and data integrity validation.

4.2 System Design

Generating short 5G symbols: OFDM achieves high throughput by modulating different data bits over subcarriers, resulting in the energy distribution over the symbol of length T_{sym}, as shown in Figure 7a. However, a secure ranging system does not require high throughput, and our design exploits the same. In contrast to transmitting different data on the subcarriers, V-Range modulates the same data on all subcarriers. This results in a specially shaped symbol with a length same as that

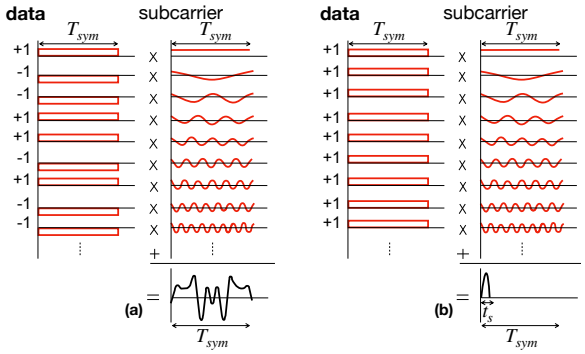

Figure 7: The shortened OFDM symbols are generated by modulating all subcarriers with the same data.

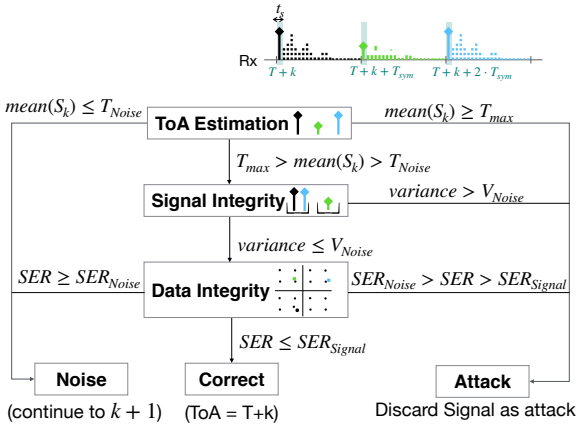

Figure 8: The signal received at estimated ToA is verified using signal and data integrity checks.

of original OFDM but with an energy aggregated over a much smaller part t_s of the symbol, as shown in Figure 7b.

In OFDM, the Inverse Discrete Fourier Transform (IFFT) is applied to subcarriers to generate the time-domain signal. The amplitude of subcarriers is scaled depending on the data modulated on them and then added together. If subcarriers carry different data bits, the energy of the signal is distributed over $\hat{N}$ time samples transmitted in the duration of T_{sym}. When the subcarriers are modulated with the same data (i.e., subcarriers have the same energy), all samples except one cancel each other. The length (T_{sym}) of the symbol is unmodified and the symbol has $\hat{N}$ samples. However, the energy is aggregated over a duration t_s where $t_s << T_{sym}$. At the receiver, the samples within the t_s part of the symbol are sufficient to decode the data. The remaining part of the symbol at the receiver only contains noise as no signal energy was present during transmission. In the following, we express these specialized OFDM symbols mathematically. Each OFDM symbol can be described as a complex valued function $s(t)$ in time domain. The real and imaginary part of $s(t)$ represent in-phase and quadrature component of the signal, also known as I/Q data. An OFDM symbol is then expressed as the aggregation of the contributions of all $\hat{N}$ subcarriers:

$$s(t) = \sum_{k=0}^{\hat{N}-1} X_k \cdot e^{j2\pi kt/T}, \quad \text{where } t \in [-T_g, T_{sym})$$

and X_k is the constellation point encoded on subcarrier $e^{j2\pi kt/T}$. In fact, this is just the IFFT on the complex data elements X_k evaluated over the length of the symbol and the guard interval T_g [36]. If all the data elements are equal, i.e., $X_k \equiv X \in \mathbb{C}$, we simplify this formula to:

$$s(t) = X \cdot \sum_{k=0}^{\hat{N}-1} e^{j2\pi kt/T_{sym}} = X \cdot \sum_{k=0}^{\hat{N}-1} \left(e^{j2\pi t/T_{sym}}\right)^k$$

If $t = p \cdot T_{sym}$ for any integer $p \in \mathbb{Z}$, then $e^{j2\pi t/T_{sym}} = 1$ and thus $s(t) = X \cdot \hat{N}$. Since $t \in [-T_g, T_{sym})$ and $T_g < T_{sym}$, this condition is only satisfied when $p = 0$. In case $e^{j2\pi t/T_{sym}} \neq 1$, the geometric series can be rewritten as:

$$s(t) = X \cdot \frac{1-e^{\rho\hat{N}}}{1-e^{\rho}} = \frac{e^{-\rho\frac{\hat{N}}{2}} - e^{\rho\frac{\hat{N}}{2}}}{e^{-\rho\frac{1}{2}} - e^{\rho\frac{1}{2}}} \cdot \frac{e^{\rho\frac{\hat{N}}{2}}}{e^{\rho\frac{1}{2}}} \cdot \frac{2j}{2j}$$

$$= X \cdot \frac{\sin(\pi\hat{N}t/T_{sym})}{\sin(\pi t/T_{sym})} \cdot e^{j\pi(\hat{N}-1)t/T_{sym}}$$

where we set $\rho = j2\pi t/T_{sym}$. This is known as a (frequency-shifted) Dirichlet kernel or periodic sinc function [35].

The maximum amplitude of the signal is $s(0) = X \cdot \hat{N}$, which is only attained at $t = 0$ where $s(t)$ forms a single narrow peak. Moreover, $s(t)$ has the zeroes $s(\ p \cdot \frac{T_{sym}}{\hat{N}}\ ) = 0$ for any $p \in \mathbb{Z}_{\neq 0}$. The theoretical width of the main "lobe" of the symbol is therefore $t_s = 2\frac{T_{sym}}{\hat{N}}$, i.e., the width scales linearly with the symbol length and is inversely proportional to the number of subcarriers. Figure 7b) shows how $s(t)$ is composed of the different subcarriers. It is apparent that the energy is focused in a single narrow peak. Figure 18 in Appendix depicts over-sampled symbols $s(t)$ from an actual transmission for different subcarrier bandwidths.

The number of unique symbols with such a structure depends on what is encoded as X. Any digital modulation can be used to encode data in X, independent of the number of subcarriers. For example, there exist four unique symbols if 4-QAM is used and sixteen symbols on using 16-QAM. We explore the choice of modulation scheme and the effect on performance and security in Section 6. We also point out that physical channel features, normally a part of OFDM symbols, such as pilot subcarriers and the cyclic prefix required for channel estimation, are not available in our modified symbols. The advantage of these symbols is the fact that they exhibit properties of single carrier symbols even though they are valid multi-carrier OFDM symbols. Due to single carrier properties, there is no inter-carrier interference or phase rotation of each subcarrier, allowing for a simple receiver design that supports secure ranging.

ToA Estimation: The estimation of a symbol's time-of-arrival is key to a precise distance measurement. Assuming that a ranging symbol is transmitted at time T, it arrives at the receiver at time $T + ToF$, where ToF depends on the signal's propagation time between the devices. Recall that unlike standard OFDM, where energy is distributed over the entire symbol duration T_{sym}, the energy of the V-Range OFDM

symbol is concentrated over a much smaller duration. Therefore, the receiver estimates arrival time by using fine-grained samples spaced t_s apart. The receiver starts the search at an offset of k samples and continues until it finds the legitimate symbol (or traces of an attack). As the transmitter sends more than one but n consecutive ranging symbols, the receiver can use all these symbols for ToA estimation and validation. The samples that fall on to the n symbols at offset k are represented as the set S_k and are collected at times $T+k+i\cdot T_{sym}$.

By using these samples, the receiver needs to differentiate between legitimate signal, adversarial signal, multi-path components, and noise. The receiver starts by checking the average power of these samples. If power is less than T_{Noise}, the samples are discarded as noise and receiver continue the search at offset $k = k+1$. If it is more than T_{max}, then the signal is discarded as an attack, and a new ranging operation is initiated. If average power is between thresholds, the offset k is considered as a probable leading edge, and the receiver performs integrity checks for ToA validation.

Signal Integrity Checker: The validity of the physical layer is crucial for secure distance measurement. Even though signal integrity checks can prevent reduction attacks, they are mandatory to avoid distance enlargement attacks. The signal integrity is checked using statistical properties of the signal, such as total power or variance [33, 46]. For the QAM modulated signal, power thresholds are useful for ToA estimation, but variance-based checks are required ToA verification. The power thresholds are not sufficient to differentiate between legitimate and attack signal, as a receiver cannot predict path loss of the channel with certainty. Variance, on the other hand, depends on the receiver's noise profile, i.e., V_{Noise}, and increased variance can indicate the presence of interference or attack signal.

In the absence of an attacker, power distortion can happen due to two reasons: i) inter-symbol interference, and ii) dynamic environment/channel conditions. Inter-symbol interference is the result of the multipath components interfering with subsequent symbols. The V-Range OFDM symbols prevent inter-symbol interference as maximum delay spread is less than $T_{sym}-t_s$; the total time interval during which various multipath components with significant energy arrive at the receiver can only reach up to a few hundred ns [41], while the samples with the transmission energy are spaced in the order of μs. The signal distortion can also occur due to the changing channel condition in the dynamic environment; the signal reflects from nearby objects and buildings, moving vehicles, etc.. In V-Range, all ranging symbols are transmitted within the channel's coherence time, i.e., the channel conditions remain relatively constant for the entire duration of the ranging slot. For example, two energy samples transmitted at time T and $T+T_{sym}$, respectively, which are received at times $T+i$ and $T+T_{sym}+i$, will experience the same channel, i.e., traveled same distance, reflected by the same objects etc. and therefore should experience same power level distortions. Symbols received after the channel coherence time cannot be guaranteed to exhibit similar properties.

The signal integrity check exploits the above property to verify signal integrity. In other words, if the transmitter transmits samples with P power levels (e.g., 16-QAM modulation has three power levels), the receiver should also get these samples with P power levels, as they experience the same channel conditions. Although samples transmitted with the same power can have variance up to V_{Noise} due to the receiver's noise, the receiver can check the power profile of the signal against a series of expected symbols (in our case, it will be the expected challenge/response). If data is not known at the receiver in advance, it can cluster the samples according to their power levels before checking the variance (e.g., by using the algorithm presented in the appendix 8.1)). The receiver computes the variance over the samples transmitted with the same power level, and if it exceeds V_{Noise}, the entire signal is discarded as an instance of attack. If the variance is lower than V_{Noise} for all P power levels, the signal is passed on to the data integrity checker.

Data Integrity Checker After verifying the physical-layer integrity of the ranging symbols, the V-Range receiver checks the correctness of the received data by checking the symbol errors, i.e., the difference between the received symbols and expected symbols. The symbol error rate SER depends on the effects of channel conditions (i.e., SNR) and hardware clock inaccuracies (i.e., carrier frequency offset) on a selected modulation scheme. Some modulation schemes can withstand more diverse channel conditions and higher clock inaccuracies than others. The channel conditions cannot be accurately predicted in advance, and the device can only determine the worst channel condition (i.e., minimum SNR) under which a modulation scheme can operate.

As discussed in Section 3, secure ranging applications cannot use reference signals to correct carrier frequency offset introduced by clock inaccuracies. The carrier frequency offset results in in-phase and quadrature-component imbalance, which can make the recovery of the data infeasible. The V-Range OFDM symbols modulate the same data on all subcarriers; therefore, symbols can be demodulated as single-carrier symbols without considering the rotation of each sub-carrier individually. The V-Range receiver can make use of simpler approaches to estimate frequency and phase offset. For example, the receiver can exhaustively search for these variables to recover the correct data. The exhaustive search can be avoided using optimal techniques, e.g., search for the frequency offset can be avoided if the first and last symbol has a relative rotation within a certain threshold (see Appendix 8.2). The allowed symbol error rate is both a performance and a security parameter. The V-Range system allows symbol errors up to SER_{Signal} to perform under diverse channel conditions with hardware of different capabilities. The signal with error more than SER_{Noise} is considered noise. However, the system can be considered secure only if it is infeasible for an attacker to achieve an error of less than SER_{Signal} or force legitimate signal to have error more than SER_{Noise} without increasing its variance.

5 Security Analysis

We analyze the security of V-Range against distance reduction [25, 26] and enlargement attacks [46, 48], the two kinds of distance manipulation attacks. We specifically focus on physical-layer attacks i.e., the attacks do not require any knowledge of the actual data and therefore are independent of any logical-layer protocol or cryptographic primitive.

5.1 Distance Reduction Attack

In a distance reduction attack, the attacker shortens the distance measured between two legitimate ranging devices. Distance reduction attacks have severe implications, e.g., the attack on modern automobile's passive keyless entry systems has allowed attackers to open and drive the cars [5]. Unlike distance estimation techniques based on signal strength or frequency where the attacker can simply amplify and forward the ranging signal to shorten the distance, in a time-of-flight based distance estimation, an attacker needs to manipulate time-of-arrival estimation. Assuming that the attacker cannot predict challenges and responses, the attacker's only option is to perform physical layer ED/LC attacks.

Early-detect & Late-commit: 5G uses long OFDM symbols (order of μs) to transmit data and therefore is vulnerable to ED/LC attacks. In contrast, V-Range emits only one sample with amplitude greater than zero for every symbol, which concentrates energy within a short duration $t_s \ll T_{sym}$. However, if processed incorrectly at the receiver, short symbol duration alone is not sufficient to guarantee secure time-of-arrival measurement. The 5G receiver design is vulnerable even if short symbols such as those described in Section 4.2 are used. The receiver aggregates energy on a symbol level by performing FFT on all $\hat{N}$ samples collected over symbol duration T_{sym} and obtains data modulated on the sub-carriers:

$$X_k = \sum_{t=0}^{\hat{N}-1} s(t) \cdot e^{-j2\pi kt/T}, \quad \text{where } k = 0,\ldots,\hat{N}-1$$

In V-Range, energy is contained within the first sample $s(0)$, and remaining samples only carry noise, multi-path and channel interference. The output of the 5G receiver after the FFT stage can be expressed as

$$X(k) = s(0) + N_k, \quad \text{where } k = 0,\ldots,\hat{N}-1$$

and N_k represents noise on each sub-carrier. Since added noise can cause distortion preventing the correct assignment of samples to constellation points during de-modulation, 5G and other communication systems have to be designed to tolerate bit errors in order to operate under low SNR conditions. While paramount for reliable communication, symbol-wise aggregation and error tolerance is an attack vector in the context of distance measurement. An attacker can inject energy (on certain sub-carriers) to cause time advancement, and remain undetected if interference is discarded as bit errors.

Distance reduction by $\delta * t_s$ ns is achievable if, after observing sample $s(0)$, an attacker late-commits samples at $t = [1 \;\; \hat{N} - \delta - 1]$ such that samples collected at $t = [-\delta \;\; \hat{N} - \delta - 1]$ result in the correct data. A strategy to achieve time advancement of $\delta = 3$ samples using late commit attack is presented in the Appendix 8.4.

The V-Range receiver, on the other hand, treats each sample independently. The effective symbol duration is $\approx$ 2.5 ns for a system bandwidth of $400MHz$, allowing an attacker to reduce the distance by not more than $75cm$ in an ideal scenario. Similarly, an attacker can achieve distance reduction up to $3m$ when a system uses $100MHz$ bandwidth. However, it is difficult for an attacker to position an adversarial transceiver in line-of-sight of the two devices, especially when one or both of the legitimate devices can move and incur a delay t_d due to the attacker's location. Furthermore, the adversary needs time t_p to process the symbol's initial part and generate a late commit signal. Therefore, the maximum time by which an attacker can advance the signal is bounded by $t_s - t_d - t_p$, where $t_d > 0$ and $t_p > 0$ reducing the effective distance reduction. We conclude that the maximum distance reduction is within the imprecision of the system bandwidth ($t_s \approx 1/\text{system bandwidth}$) and therefore does not allow any meaningful distance reduction. The shortened OFDM symbol to transmit challenge and response in conjunction with the V-Range receiver design prevents all known distance reduction attacks.

5.2 Distance Enlargement Attack

As outlined in section 3, the attacker delays the arrival of the ranging signal at the receiver, thereby causing an increase in the estimated ToF. As the legitimate devices are within communication range, the legitimate signal and attacker's delayed signal arrives at the receiver. Due to the attacker's physical constraints (e.g., attacker hardware delay, attacker position, and being able to transmit signals faster than the speed of light) and laws of physics, the attacker cannot prevent the legitimate ranging signals from arriving at the receiver before the attacker's signal. Alternatively, the attacker can prevent the *reception* by either overshadowing or annihilating the legitimate signal at the receiver. In other words, the distance enlargement attack is successful if the receiver discards the legitimate signals as noise and uses the attacker's delayed version for time-of-flight estimation.

Overshadowing legitimate signal: V-Range aggregates the symbol energy and reduces the effective symbol duration to t_s, and it constrains the choice of delay δ for an attacker. Using $\delta <= t_s$, the distance estimate is within the imprecision of the system. If the attacker's replayed signal does not fall over legitimate signal, i.e., $T_{sym} > \delta > t_s$, the receiver finds traces of the legitimate signal, and use it for the time of arrival estimation. However, if attacker replay signal at delay $\delta = i \cdot T_{sym}$, where i is a positive integer, the attack signal overshadow's subsequent legitimate symbols. In this case, the attacker needs to prevent

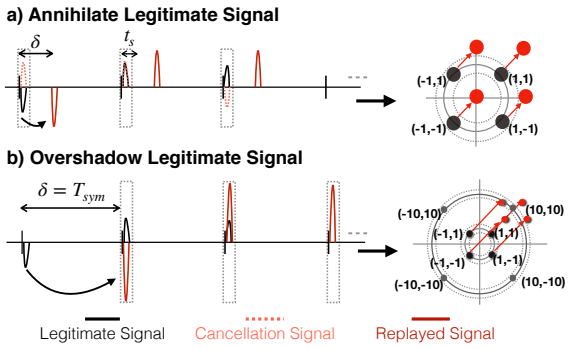

Figure 9: An attacker can perform annihilation or overshadow attack to prevent legitimate signal detection.

Legitimate Signal	1,1	1,-1	-1,1		
Power(Legitimate)	1.41	1.41	1.41	-	**Variance = 0**
Annihilation Signal	1,1	1,1	1,1		
Attack + Legitimate	2,2	0,0	0,2	-	**Incorrect Data**
Power(Legitimate+Attack)	2.8	0	2	-	**Variance = 2.1**
Overshadow Signal	-	10,10	-10,-10	-10,10	
Attack + Legitimate	-	9,9	-11,9	-10,10	**Correct Data**
Power(Legitimate+Attack)	-	12.7	14.2	14.1	**Variance = 0.71**

Table 1: Example. Enlargement attack detection using V-Range; the variance of the received signal increases if an attacker tries to manipulate it. The receivers get a combination of two different phase signals, increasing the variance.

the detection of the only first i symbols. Figure 9 illustrates such an overshadow attack for $i = 1$.

The integrity checks of the V-Range detect even such an attack. In most cases, the receiver decodes correct data as the attack signal is simply the delayed and amplified version of the legitimate signal. However, the combination of delayed high powered attacker signal over legitimate signals change physical layer properties; the legitimate signals behave as high variance noise interference to the attacker's signal. V-Range's signal integrity checker detects attack due to the high signal variance. We show an example scenario in Table 1, and experimental results in the next section.

Annihilating legitimate signal: Another attacker strategy is to prevent the reception of the legitimate signal and then to replay it after delay δ. The success of the legitimate signal annihilation and, therefore, the distance enlargement attack depends on the attacker's ability to guess legitimate signal and transmit a cancellation signal i.e., a signal with the same power as the legitimate signal but with opposite phase. In addition to guessing the correct symbol, the attacker must have complete knowledge of its communication channel (e.g., receiver position, accurate time-of-arrival of the legitimate signal, environmental interference) to execute a successful attack. As discussed in Section 5.1. The attacker's ability to correctly guess the symbol depends on the modulation scheme, higher-order modulation schemes such as 64-QAM has a lower likelihood of successful guessing. Alternatively, the attacker can exploit the early-detect technique used in Section 5.1 to predict the symbol and generate a corresponding cancellation signal. Recall that effective symbol duration t_s is a few nanoseconds, limiting the time to detect and process the legitimate signal and generate the attack signal.

The use of incorrect cancellation signal results in the shifting of the constellation points, as indicated in Figure 9. We show by an example in Table 1 and experiments in Section 6 that such shifts lead to higher symbol error rate and higher signal variance thereby V-Range's integrity checker detects the attempt of signal annihilation with high probability.

Carrier Frequency Offset Attack: An attacker can also spoof the reference signals and force *out of turn* transmissions and incorrect decoding of data at the receiver resulting in false distance measurements. The V-Range design does not use reference signals for offset estimation, V-Range uses shortened OFDM symbols, and apply integrity checks; these choices collectively make the V-Range system secure. The V-Range receiver uses short 5G symbols for offset estimation as well as data detection; therefore, an attacker has to manipulate these symbols directly. Note that the attacker cannot prevent the legitimate signal from arriving at the receiver. An attacker can use a different frequency and phase offset signal, and this attack signal has to fall over the legitimate signal to make it undetectable. The legitimate and attack signals arrive at the receiver with different phases, and the receiver cannot recover data from this distorted signal. However, the V-Range receiver still detects this signal as an attack, as distortion increases the variance of the signal.

The V-Range design prevents all possible distance enlargement attacks as an attacker cannot prevent the detection of a legitimate signal at the receiver without increasing its variance.

6 Implementation and Evaluation

5G features a unified frame structure that supports many different physical layer configurations. The hardware designs of 5G need to be extremely flexible and are expected to use direct RF sampling techniques [16], similar to software-defined radios (SDRs) where the receive and transmit stage can be controlled at the sample level through a digital interface. Consequently, we emulate the 5G-NR physical-layer configurations with the help of SDRs for bandwidths up to 100 MHz. For higher bandwidths, we use a vector signal generator [11] since most existing SDRs currently do not support such high frequencies and bandwidths. Our results are based on two different implementations, a sub-6GHz setup and a mmWave setup, the two frequency ranges 5G operates over. For both frequency bands, we use the maximum allowed subcarrier bandwidth

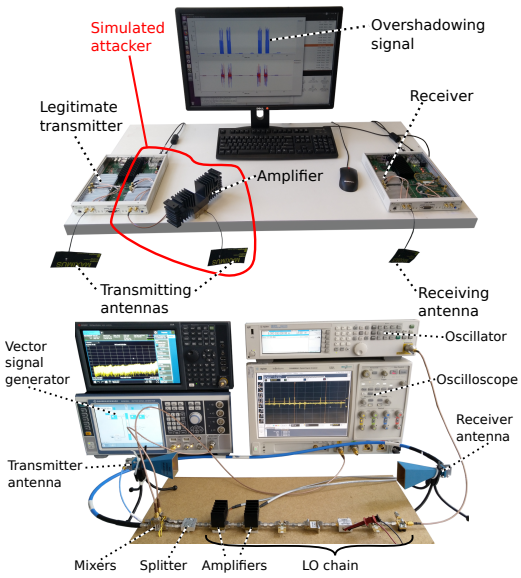

Figure 10: Sub-GHz and mm-wave setup.

(i.e., shortest T_{sym}), as longer T_{sym} only increase latency.

Sub-6GHz setup: We use two USRP-X310 SDRs [9] as shown in Figure 10. Our setup is similar to other experimental studies on 5G [8]. Sub-carrier bandwidth is 60 kHz ($T_{sym} = 16.67\mu s$) and the total number of samples per symbol $\hat{N} = 2048$. With a 60 kHz sub-carrier bandwidth, the narrow peak of the resulting symbol is only $t_s \approx 10ns$ long.

The baseband signal is generated using MATLAB and then up-converted to the center frequency $f_c = 3.4\ GHz$ by the internal mixer of the USRP before signal transmission. Both devices are using their internal clocks, which have an error of $\pm 2.5\ ppm$. The receiver operates at the same center frequency f_c and down-converts the signal without using any offset correction. The received signal is analyzed in MATLAB, which we rely on to implement the signal and data integrity checks.

mm-wave setup: We build a dedicated setup to test the performance of V-Range in the millimeter frequency bands [6]. Figure 10 shows the transmit and receive stage that shares the same local oscillator (LO) chain for signal down- and up-conversion to $f_c = 24.5\ GHz$. The LO chain is shared to reduce the cost and size of the setup. For the mmWave band, we again chose the maximally possible sub-carrier spacing of 480 kHz ($T_{sym} = 2.08\ \mu s$) and $\hat{N} = 256$ (i.e., $t_s \approx 2ns$). The signal is transmitted and received by two identical horn antennas. We use a vector signal generator for the signal generation and an oscilloscope for the recording of the 400 MHz signal. The received signal is processed in MATLAB, similar to the Sub-6GHz setup.

In the security analysis, we will show that distance reduction and enlargement attacks are challenging to carry out against V-Range. We give advantage to the attacker by precisely aligning the attacker's signal with the legitimate signal. Therefore, when simulating an attack, we use two daughterboards of the same USRP to achieve fully synchronized transmission based on the same hardware clock (see Fig. 10). Antennas are placed such that the travel time of the attack and legitimate signal differ at max by 1 ns. We analyze the effect of carrier frequency offset attack using MATLAB simulations as we needed a controlled offset between legitimate and attack signals for analysis.

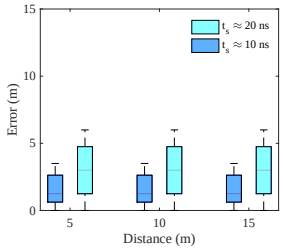

Figure 11: Accuracy of the distance measurement depends on the sample duration t_s

6.1 Parameters and Metrics

The performance of V-Range depends largely on three parameters: (1) maximum expected noise variance, V_{Noise}, (2) maximum allowable symbol error rate of the received signal, SER_{Signal}, and (3) maximum expected symbol error of noise, SER_{Noise}. The threshold V_{Noise} is not channel-dependent and can be pre-estimated from the noise profile of the receiver (e.g., $4.5 \cdot 10^{-7}$ in our sub-6GHz setup). The values for SER_{Noise} and SER_{Signal} is channel dependent. For example, a low value for SER_{Signal} increases false positives in noisy environments i.e., low SNR conditions, and high value for SER_{Signal} allows an attacker to make more incorrect guesses when brute-forcing a challenge and response message. Similarly, SER_{Noise} should be chosen such that V-Range does not classify noisy environments without any legitimate ranging signal as an attack (high false positives). Furthermore, the value of SER_{Noise} should also be chosen based on the modulation scheme, i.e., lower SER_{Noise} value for higher-order modulation (64-QAM). We evaluate the performance and security of V-Range for different values of the above parameters and present our results below. In our experiments, we set the number of symbols $n = 20$ (if not mentioned otherwise), as it keeps the chances of successful brute-force guessing low for all modulation schemes in evaluation. Furthermore, we evaluate the performance of the V-Range design under different SNR conditions. The SNR conditions are realized by varying transmit power and distance between devices.

6.2 Performance Evaluation

We evaluate the performance of V-Range in terms of precision, latency, and the probability of false alarms in a benign setting.

Precision and latency: Figure 11 shows the measurement error for the sub-6Ghz setup obtained under different bandwidth and distance configurations. The results show that measurement

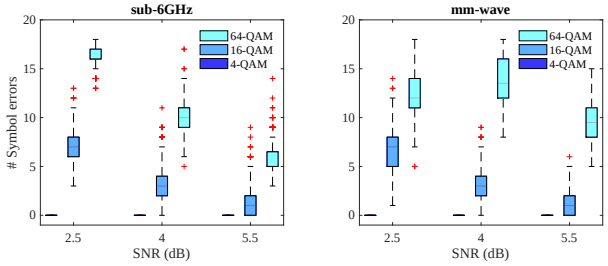

Figure 12: Symbol error rate of the modulation schemes depends on the channel condition (i.e., SNR).

	n = 20			n = 100		
SNR [dB]	**2.5**	**4**	**5.5**	**2.5**	**4**	**5.5**
4-QAM	0	0	0	0	0	0
16-QAM	0.004	0.034	0.054	0	0	0
64-QAM	0.008	0.258	0.371	0	0.001	0.082

Table 2: False positives: variance estimate is imprecise when using high order modulation with a small sample size.

$(SER_{Signal}, SER_{Noise})$	Noise	Legitimate	Attack
4-QAM (0.1, 0.5)	0	1	0
16-QAM (0.3, 0.7)	0	0.913	0.086
64-QAM (0.5, 0.8)	0.0002	0.605	0.394

Table 3: Performance of V-Range at $SNR = 5.5\ dB$.

error depends only on the sample length t_s (i.e., system bandwidth), but is independent of the distances between devices. The shorter sample length t_s (i.e., higher system bandwidth) achieves better precision, e.g., for $t_s \approx 10n$ns, the error is below 3m. For the mm-wave setup with a bandwidth of 400 MHz, the achieved precision is 60 cm. These numbers are in line with what 3GPP expects to be attained by ranging techniques operating in the 5G spectrum [12]. When performing two-way ranging, $2 \cdot n = 40$ symbols are exchanged. Thus, if symbol lengths of 16.67μs (sub-6GHz) and 2.08μs (mm-Wave) are used, the entire ranging operation can be completed in 667μs or 83μs, respectively.

Effect of V_{noise}: The signal integrity checker module monitors the power levels of the received signal and raises the alarm if the variance is higher than V_{noise}. We evaluate the probability of a legitimate signal getting discarded as an attack in Table 2. We observe that, for $n = 20$, 4-QAM and 16-QAM signals have a low probability of being falsely classified as an attack, but 64-QAM signals have a high probability of getting identified as an attack signal. The reason is that 64-QAM sends these symbols with ten different power levels, and the sample size representing each transmit power is small. The low sample size leads to imprecise variance estimation. However, for $n = 100$, the performance of 64-QAM improves, and therefore we conclude that lower modulation schemes should be used when sending fewer symbols.

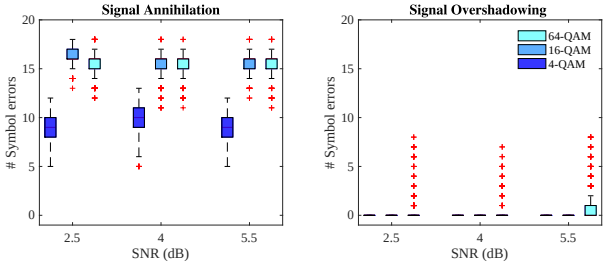

Figure 13: Symbol error rate in the presence of attacker.

	Annihilation			Overshadowing		
SNR [dB]	**2.5**	**4**	**5.5**	**2.5**	**4**	**5.5**
4-QAM	0.835	1	1	1	1	1
16-QAM	0.942	1	1	1	1	1
64-QAM	0.992	0.999	1	0.998	0.997	1

Table 4: Attack detection using integrity check.

Effect of SER_{noise} and SER_{signal}: We evaluate the performance of V-Range under various SNR conditions. Figure 12 shows the observed number of symbol errors over 100,000 challenge messages. The results are similar for the sub-6GHz and mm-wave setups. 4-QAM modulation performs well even under low SNR conditions, and therefore SER_{Signal} can be set to zero. However, higher-order modulation schemes such as 16-QAM and 64-QAM incur symbols errors in low-SNR conditions.

For the V-Range performance presented in Table 3, we choose SER_{Signal} to be about 10% higher than the expected symbol error rate. Even after allowing a high value of SER_{Signal} and SER_{Noise}, the 64-QAM signal has a high probability of being detected as attack or noise. Thus, 64-QAM is not preferred when operating in low SNR conditions.

6.3 Security Evaluation

Distance Reduction Attack: As discussed in Section 5, V-Range is secure against ED/LC distance reduction attacks due to shorter effective symbol length. In our setup, energy is aggregated within 10ns (sub-6GHz) and 2ns (mm-Wave setup). Therefore, the maximum distance an attacker can reduce by performing ED/LC is less than 3 m and 60 cm, respectively. Alternatively, the attacker can guess symbols with a guessing error below SER_{Signal}.

Distance Enlargement Attack: The probability of a successful distance enlargement attack depends on the attacker's ability to prevent detection of the legitimate signal by signal annihilation or overshadowing. In both attack scenarios, the attacker's signal overlaps the legitimate signal; the samples constructed at the receiver contain a combination of legitimate and attack signals. To validate the need for integrity checker modules, we ran 100,000 ranging operations while simulating signal annihilation and overshadow attacks.

The data integrity checker by itself does not help in annihilation and overshadow attack detection. As shown in Figure 13,

symbol error is either too high (i.e., for annihilation attack) or too low (i.e., for overshadowing attack). In a signal annihilation attempt, the signal's symbol error is more than SER_{Noise}. If the receiver only checks data correctness, the legitimate signal will be discarded as noise, and the attacker's replayed signal will be used for distance estimation. In an overshadow attack, the overshadowed signal is a delayed and amplified version of the legitimate signal and resembles the legitimate signal, i.e., symbol error less than SER_{Signal}. Therefore, the receiver will use this delayed attack signal for distance estimation.

However, when the attacker is trying to manipulate data of the legitimate signal, the attacker changes the physical layer properties of the signal, which is detected by the signal integrity checker. The results of the signal integrity checker are shown in Table 4. We observe that an annihilation or overshadow attack is detected with very high probability, i.e., with a false negative rate of less than 10^{-5}, at respective SNR conditions. The probability of attack detection decreases for low SNR conditions, e.g., 2.5 dB. We note that an SNR of 2.5dB is very low, as most wireless receivers require at least 3dB for successful communication.

Carrier Frequency Offset Attack: We perform MATLAB simulations using the 5G toolbox to analyze the carrier frequency offset attack on 4-QAM modulated symbols. The designs under test are OFDM, OFDM shortened symbol with conventional receiver design where OFDM modulated reference signal is used for offset estimation, and V-Range design with the short symbol and integrity checks. We use the simulation to control the frequency offset of the legitimate and attacker signal. All three configurations have almost no bit error in the absence of an attacker. However, when the reference signals are overshadowed (attacker's signal power is 5dB higher than the legitimate signal) with different offset signals, the receiver's offset estimation is incorrect. As shown in Figure 14, both OFDM and shortened OFDM symbols are vulnerable to offset attacks, i.e.,, resulting in higher bit error. The attacker signal that arrives at the receiver after a delay of 100 ns bears the correct data; therefore, the receiver uses this signal for distance estimation. The attack on OFDM and shortened OFDM symbols only differ in the sense that attack signal overlaps with the legitimate signal in OFDM as symbol duration is longer than the delay, and does not overlap in the short OFDM symbol. Therefore, OFDM symbols have incorrect data due to overlap, even when the offset is small.

The attack signal should fall over the legitimate signal to prevent its detection at the V-Range receiver. As shown in Figure 15, the arrival of the legitimate and attack signals with different carrier frequency offsets inhibits the detection of the legitimate signal (higher bit error). Due to the signal integrity checker, V-Range does not discard such a signal as noise. The V-Range receiver detects an increase in variance, which exposes the attack.

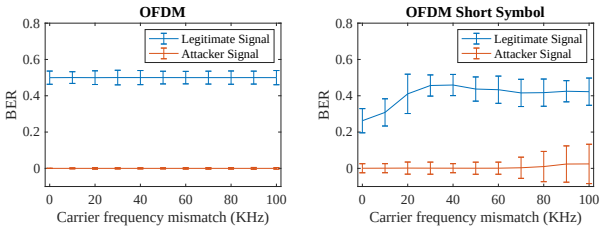

Figure 14: Both OFDM and short symbols are vulnerable to carrier frequency mismatch. The legitimate signal is discarded as noise (higher bit error), and attack signal arriving at the receiver after delay δ with the correct data is used for the distance measurement.

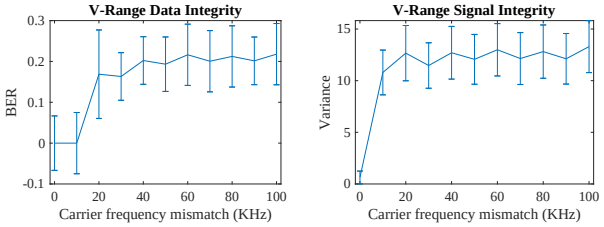

Figure 15: If legitimate and attack signals arrive at the receiver with different carrier frequency offset, bit/symbol error increases. However, the distortion of the signal is detected by the signal integrity check.

7 Discussion

Compatability with LTE, WiFi, and UWB: WiFi and LTE could adopt a design similar to V-Range, but these technologies have certain limitations, such as allocated system bandwidth, access control, and receiver design. The system bandwidth in LTE limits the security guarantees, i.e., longer t_s. V-Range uses the dynamic frame structure provided by 5G; LTE uses a rigid resource grid and does not allow frame aggregation and direct device-to-device communication.

Currently, there are efforts to design a secure ranging system for the WiFi 801.11az standard [2]. 802.11az will support a higher system bandwidth (up to 160 MHz) than its preceding WiFi standards and thus could support V-Range. However, WiFi's carrier-sense multiple access allocation machanism brings a series of challenges that could result in increased false positives (i.e., noise due to packet collision) and higher latency (i.e., longer packet length, random backoff time).

UWB supports very short symbols in the form of pulses and heavily motivated the V-Range design. However, UWB and 5G serve entirely different purposes with different underlying architectures. Even though there exist UWB-based time-of-flight ranging systems—of which few are considered secure—, UWB receivers are generally non-coherent and can only detect the presence of energy on a given channel. Such designs neither support high data rates, nor sophisticated channel access con-

trol mechanisms. V-Range, on the other hand, shows how to use standard modulation schemes for ranging and performs secure ranging using coherent 5G receivers. Coherent receivers bring their own set of pros and cons, e.g., the use of high-order modulation mitigates guessing attacks, but receivers are susceptible to carrier-frequency offset attacks if not handled explicitly.

Key Exchange and Privacy Consideration: Many 5G use cases need to maintain a shared secret for secure communication. The same keys can be used to generate keying material for secure ranging. The 3GPP is designing the SEAL architecture to perform key exchange and secure communication in dynamic scenarios, such as vehicular networks. If a device does not have a shared secret, it can perform key exchange in the initialization and verification phase of the distance bounding protocol.

Peak Power: V-Range uses shortened OFDM symbols, with energy aggregated over one sample duration. The high Peak to Average Power Ratio (PAPR) value of these symbols makes them less robust (i.e., higher SER). The V-Range system is capable of handling symbol errors by using SER thresholds.

Noise, Interference and Jamming: The V-Range system is designed to handle the receiver's noise by choosing values for V_{Noise}, SER_{Signal} and SER_{Noise}. However, interference due to other transmissions needs to be avoided. The physical layer of any ranging system is susceptible to interference, and the same is true for V-Range. The presence of an interference signal leads to denial of service, as it makes it harder to estimate the time of arrival. We assume that the slot assignment of 5G mitigates interference. An attacker can jam the signals to launch a denial of service attack, but jamming does not lead to an incorrect distance measurement.

8 Conclusion

In this paper, we proposed V-Range, the first 5G-compatible secure ranging system that is resilient to both distance reduction and enlargement attacks. We enumerated the challenges that need to be addressed to realize secure positioning in 5G and in the process identified a novel carrier-frequency offset attack that specifically affects 5G systems. The V-Range can be readily deployed over existing 5G standards to achieve high precision ranging on both mmWave and sub-6Ghz frequency bands. We demonstrated that V-Range detected distance manipulation attack with a false negative rate of less than 10^{-5}.

References

[1] 5G; study on scenarios and requirements for next generation access technologies (3gpp tr 38.913 version 14.2.0 release 14).

[2] 802.11az. http://www.ieee802.org/11/Reports/tgaz_update.htm. [Online; Accessed 24. September 2019].

[3] 802.15.4z Task Group. http://www.ieee802.org/15/pub/TG4z.html. [Online; Accessed 17. June 2020].

[4] Cyclic Prefix Replay Attack. https://mentor.ieee.org/802.11/dcn/17/11-17-1122-00-00az-cp-replay-threat-model-for-11az.pptx. [Online; Accessed 24. September 2019].

[5] "mercedes 'relay' box thieves caught on cctv in solihull.". http://www.bbc.com/news/uk-england-birmingham-42132689. [Online; Accessed 15. June 2020].

[6] mm-wave Setup. https://www.highfrequencyelectronics.com/index.php?option=com_content&view=article&id=1994:affordable-solutions-for-testing-28-ghz-5g-devices-with-your-6-ghz-lab-instrumentation&catid=167&Itemid=189. [Online; Accessed 17. June 2020].

[7] NXP Offers UWB Fine-Ranging Chipset for Mobile Devices. https://www.rfidjournal.com/articles/view?18936. [Online; Accessed 29. November 2019].

[8] Open Air Interface. https://www.openairinterface.org. [Online; Accessed 16. October 2019].

[9] USRP X310. https://www.ettus.com/all-products/x310-kit. [Online; Accessed 29. November 2019].

[10] UWB for Secure Ranging-3dB. https://www.3db-access.com/article/15. [Online; Accessed 29. November 2019].

[11] Vector Signal Generator. https://www.rohde-schwarz.com/us/manual/r-s-smu200a-vector-signal-generator-operating-manual-manuals-gb1_78701-28893.html. [Online; Accessed 29. November 2019].

[12] 5g;technical specification group radio access network; study on nr positioning support. 03 2019.

[13] 3GPP. https://www.3gpp.org/ftp/Specs/archive/38_series/38.211/. [Online; Accessed 26. November 2019].

[14] Task Group 4z. IEEE 802.15 WPAN "enhanced impulse radio". http://www.ieee802.org/15/pub/TG4z.html. [Online; Accessed 24. November 2019].

[15] 5G Americas Whitepaper Cellular V2X Communications towards 5G. https://www.5gamericas.org/wp-content/uploads/2019/07/2018_5G_Americas_White_Paper_Cellular_V2X_Communications_Towards_5G__Final_for_Distribution.pdf. [Online; Accessed 16. June 2020].

[16] Sassan Ahmadi. Toward 5 g xilinx solutions and enablers for next-generation wireless systems. 2016.

[17] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang. What will 5g be? *IEEE Journal on Selected Areas in Communications*, 32(6):1065–1082, June 2014.

[18] 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.

[19] 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.

[20] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Proceedings of the Third European Conference on Security and Privacy in Ad-Hoc and Sensor Networks*, ESAS'06, pages 83–97. Springer, 2006.

[21] X. Cui, T. A. Gulliver, H. Song, and J. Li. Real-time positioning based on millimeter wave device to device communications. *IEEE Access*, 4:5520–5530, 2016.

[22] Ericsson. 5G New Radio: Designing for the future. https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2017/designing-for-the-future--the-5g-nr-physical-layer.pdf. [Online; Accessed 16. June 2020].

[23] Hybrid 5G and GPS. https://www.esa.int/Applications/Navigation/ESA_leads_drive_into_our_5G_positioning_future. [Online; Accessed 16. June 2020].

[24] Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Effectiveness of distance-decreasing attacks against impulse radio ranging. In *Proceedings of the Third ACM Conference on Wireless Network Security*, WiSec '10, pages 117–128. ACM, 2010.

[25] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Security Symposium (NDSS)*, 2011.

[26] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones, 2012.

[27] A. Gaber and A. Omar. A study of tdoa estimation using matrix pencil algorithms and ieee 802.11ac. In *2012 Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS)*, pages 1–8, 2012.

[28] Amrita Ghosal and Mauro Conti. Security issues and challenges in v2x: A survey, 03 2019.

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

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

[31] 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.

[32] L. Koschel and A. Kortke. Frequency synchronization and phase offset tracking in a real-time 60-ghz cs-ofdm mimo system. In *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, pages 2281–2286, Sep. 2012.

[33] Patrick Leu, Mridula Singh, Marc Roeschlin, Kenneth G. Paterson, and Srdjan Capkun. Message time of arrival codes: A fundamental primitive for secure distance measurement. 2019.

[34] Xingqin Lin, Jingya Li, Robert Baldemair, Thomas Cheng, Stefan Parkvall, Daniel Larsson, Havish Koorapaty, Mattias Frenne, Sorour Falahati, Asbjörn Grövlen, et al. 5g new radio: Unveiling the essentials of the next generation wireless access technology. *arXiv preprint arXiv:1806.06898*, 2018.

[35] MathWorks. Dirichlet or periodic sinc function. https://ch.mathworks.com/help/signal/ref/diric.html. [Online; Accessed 20. June 2019].

[36] Andreas F Molisch. *Wireless communications*, volume 34. John Wiley & Sons, 2012.

[37] Ali A. Nasir, Salman Durrani, Hani Mehrpouyan, Steven D. Blostein, and Rodney A. Kennedy. Timing and carrier synchronization in wireless communication systems: A survey and classification of research in the last five years. *CoRR*, abs/1507.02032, 2015.

[38] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. Le Boudec. The cicada attack: Degradation and denial of service in ir ranging. In *2010 IEEE International Conference on Ultra-Wideband*, pages 1–4, 2010.

[39] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. Le Boudec. Distance bounding with ieee 802.15.4a: Attacks and countermeasures. *IEEE Transactions on Wireless Communications*, pages 1334–1344, 2011.

[40] Yinan Qi, Mythri Hunukumbure, Hyungju Nam, Hyunil Yoo, and SaiDhiraj Amuru. On the phase tracking reference signal (PT-RS) design for 5g new radio (NR). *CoRR*, abs/1807.07336, 2018.

[41] V. Raghavan, A. Partyka, L. Akhoondzadeh-Asl, M. A. Tassoudji, O. H. Koymen, and J. Sanelli. Millimeter wave channel measurements and implications for phy layer design. *IEEE Transactions on Antennas and Propagation*, 65(12):6521–6533, Dec 2017.

[42] A. Ranganathan and S. Capkun. Are we really close? verifying proximity in wireless systems. *IEEE Security Privacy*, 15(3):52–58, 2017.

[43] Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, and Srdjan Capkun. Physical-layer attacks on chirp-based ranging systems. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, pages 15–26. ACM, 2012.

[44] Kasper Bonne Rasmussen, Srdjan Capkun, and Mario Cagalj. Secnav: secure broadcast localization and time synchronization in wireless networks. In *MobiCom*, 2007.

[45] Ronald Raulefs, Armin Dammann, Thomas Jost, Michael Walter, and Siwei Zhang. The 5g localization waveform. 01 2016.

[46] Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun. Uwb-ed: Distance enlargement attack detection in ultra-wideband. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 73–88, Santa Clara, CA, August 2019. USENIX Association.

[47] Mridula Singh, Patrick Leu, and Srdjan Capkun. UWB with pulse reordering: Securing ranging against relay and physical-layer attacks. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*, 2019.

[48] 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.

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

[50] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson. 5G mmwave positioning for vehicular networks. *IEEE Wireless Communications*, 24(6):80–86, Dec 2017.

[51] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. Hiding in plain signal: Physical signal overshadowing attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 55–72, Santa Clara, CA, August 2019. USENIX Association.

$S_k = Sort(Power(S_k))$;
$B = \{S_k(1)\}$;
$NumBins = 1$;
for *j=2 to N* **do**
  if $(var(B \bigcup S_k(j)) < V_{Noise})$ **then**
    $B = B \bigcup S_k(j)$
  else
    $B = \{S_k(j)\}$;
    $NumBins++$;
  end
end
if $NumBins > P$ **then**
  Abort Ranging
else
  Check data integrity
end

Algorithm 1: Signal-integrity check

	Annihilation			Overshadowing		
SNR [dB]	**2.5**	**4**	**5.5**	**2.5**	**4**	**5.5**
4-QAM	0.82	1	1	1	1	1
16-QAM	0.94	0.98	0.99	0.97	0.99	0.99
64-QAM	0.0002	0.0003	0.069	0.65	0.69	0.71

Table 5: The probability of annihilation and overshadowing attack detection using integrity check without using pre-shared data.

Appendix

8.1 Signal Integrity Check

If ranging data is not pre-shared between entities, such as it is the case in a class of distance bounding protocols, the devices need to rely on message authentication codes to check the validity of the received data. As a consequence, the receiver needs to perform signal integrity check, without any knowledge of the expected data sequence. The only information the receiver has is that the modulation scheme used by the transmitter has a certain number of power levels P the signal is transmitted with (e.g., three power levels in 16-QAM). This information is sufficient to perform an integrity check. In short, the set S_k passes signal integrity check if samples in set S_k can be clustered into P clusters, and each cluster has variance less than V_{Noise}.

The algorithm 1 can be used to implement such an approach. The samples are sorted according to their power; sorting ensures that two consecutive samples have the least variance. The algorithm then assigns the first sample to a bin and continues to add more samples until the variance of the samples in the bin exceeds V_{Noise}. At this point, a new bin is created to assign the remaining samples. Once all samples are assigned to bins, the algorithm counts the number of bins needed to assign all samples. If the number of bins $\leq P$, then the signal is considered correct, and the signal is passed to the data integrity checker. If the number of bins is more than P, then ranging is aborted.

As shown in Table 5, the attack detection probability of this approach is similar to the approach with pre-shared data, for 4-QAM and 16-QAM modulation. However, this algorithm does not perform well for the 64-QAM, the number of bins to samples ratio is too small, i.e., 64-QAM has up to 10 bins for assigning 20 samples. The combination of attack and legitimate signal moves to another bin without affecting its variance. Therefore, the number of bins does not increase.

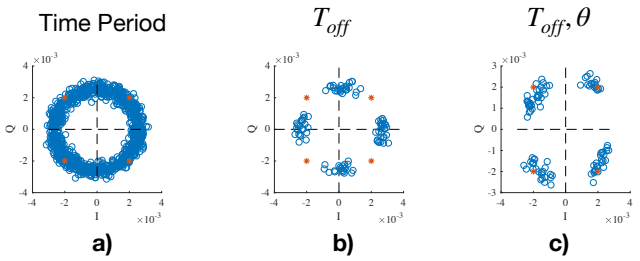

Figure 16: The residual frequency creates the power disbalance in in-phase and quadrature components of the signal. The time T_{off} is the part of the time period (of residual frequency) for which relative phase between the first and last sample is less than ε. The ε accounts for the amount of phase noise handles by the modulation scheme. All samples transmitted within T_{off} can be demodulated by using the same value of θ

8.2 Data Detection

The use of reference signals for fequency offset correction is vulnerable to distance manipulation. Therefore, V-Range does not rely on carrier-frequency estimation during ranging, i.e., the ranging signal has to cope with a certain residual frequency. The effect of frequency offset manifests itself in a rotation of the constellation diagram, as shown in Figure 16a. Although the clock inaccuracy transmitter and receiver experience at a particular time cannot be predetermined, the devices can still estimate the maximum clock inaccuracy (i.e., maximum carrier frequency offset) they can experience. There are several viable approaches to correct frequency and phase offset. For example, the receiver can brute force the constellation to recover the correct data. However, if the first and last symbol of the ranging slot have a relative rotation of less than a certain ε, no exhaustive search for the frequency offset is needed. Figure 16b shows the constellation representation of the symbols transmitted in time T_{off}. The length $T_{off} = \varepsilon/(2\pi\Delta_{max})$, where Δ_{max} is maximum frequency offset between the devices and ε is acceptable relative rotation. As Figure 16c shows, use of correct phase offset (θ) yields the correct symbols. The value of ε and the granularity of θ depends on the choice of modulation scheme and results in the different symbol error rates [32].

The range to exhaustively search for the frequency and phase offset depends on the clock error and modulation scheme, respectively. As shown in Figure 17a, by correcting both frequency and phase offset, we can tolerate a longer sequence of symbols. The symbol error rate depends on channel conditions (i.e., SNR) and modulation scheme. Results are shown for SNR of 5.5dB; 16-QAM exhibits a higher symbol

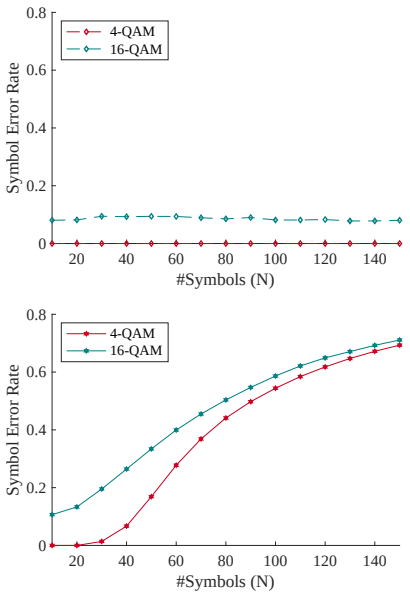

Figure 17: a) By correcting both frequency and phase offset, the device can exchange more symbols for ranging (i.e., longer signal duration T_{len}). The symbol error depends only on the channel condition and modulation scheme. b) When using fewer symbols for the ranging, the symbols can be detected by using the correct phase offset. The symbol error increase when relative rotation ε increases between symbols.

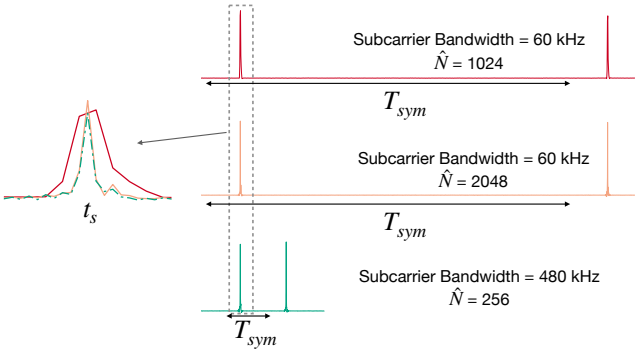

Figure 18: Special OFDM ranging symbols for different subcarrier configurations. Second and third instantiation have higher system bandwidth and thus the lobe is shorter. For the shorter symbols (second and third form above), a multi-path component can be seen.

error than 4-QAM, as it has more constellation points.

Using a shorter ranging slot duration, similar symbol error rates can be achieved by just applying phase offset correction. In such a scenario, the symbol error depends on the clock accuracy of the devices and carrier frequency, along with channel conditions (i.e., SNR) and modulation scheme. As a residual frequency remains in the signal, the relative phase difference between first and last symbol is given by ε. If ε is small, then symbols are detectable using only phase correction. As shown in Figure 17b, the symbol error increases with the number of symbols. This is not surprising as relative rotation ε also increases. The phase offset correction is compulsory for data detection. The frequency offset correction can be made redundant when using only a few symbols and a (very) accurate clock, such as those specified for 5G-based vehicular networks and critical systems).

8.3 Ranging Duration

In a typical communication system, there is always a (small) deviation between the transmitter and receiver's clock signal or local oscillator. The local oscillator plays an important role in generating specific carrier frequency signals and therefore any discrepancy between the transmitter and receiver clocks results in a carrier frequency offset. OFDM systems are sensitive to carrier frequency offsets as it results in phase rotation of the received symbols and therefore potentially incorrect decoding of the data. Typically, carrier frequency offsets is corrected using fixed preambles or pilot sub-carriers. As we have already seen, the use of any fixed reference signals introduces the possibility for an adversary to spoof the reference signals, and thereby manipulate the distance. If the optimization technique addresses this challenge by limiting the symbol duration and therefore the ranging duration, the effect of carrier frequency are minimized. The carrier-frequency offset is higher in the mm-wave (i.e., higher center frequency), so the value of ε increase faster, it is compensated by the shorter symbols in the mm-wave as shown in Figure 19a.

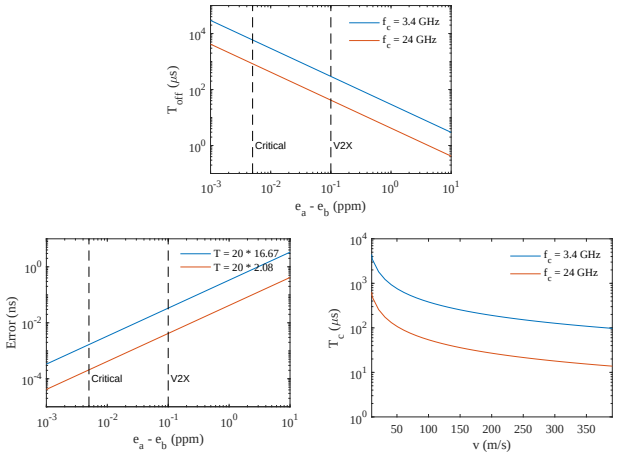

Figure 19: The total length of the signal recoverable at the receiver for the secure distance measurements depends on the hardware capabilities (frequency offset) and channel conditions (coherence time)

w

The frequnecy offset also leads to the sampling rate mismatch between devices. However, the sampling rate mismatch will affect V-Range system when offset between first and last sample used in the ranging slot has error more than $t_s/2$. As shown in Figure 19b, for the mismtach in the first and last sample of 20 symbols is less than 10^{-2} ns for the clock accuracy of .01 ppm.

Another factor that affects the ranging duration is the channel coherence time. A channel's coherence time is the time duration for which the channel conditions remain relatively constant. In V-Range, the ranging symbols are transmitted transmitted within the channel's coherence time as it is a necessary condition to verify the signal's physical-layer integrity at the receiver and thereby detect distance enlargement attacks. Thus, the duration of the V-Range slot should be bounded by clock offset inaccuracies and available channel conditions (coherence time), e.g., $T_{len} = \min(T_{off}, T_c)$, where T_{len} is the ranging duration, T_{off} is the time offset due to clock inaccuracies, and T_c is the channel coherence time.

8.4 ED/LC attack on V-Range Symbol

If used with an FFT-based OFDM receiver, the V-Range symbols are vulnerable to distance reduction by ED/LC. As shown in Figure 21, an attacker can send a late commit signal to achieve an advancement of $\delta = 3$ samples, which translates to 9 m distance reduction even if system bandwidth is set to 100 MHz (a lower bandwidth leads to even greater distance reduction). After observing sample $s(0)$ from the legitimate transmitter, an attacker can define late commit signal for $t = [1 \ \hat{N} - \delta - 1]$ as

$$s'(t) = \begin{cases} s(0), & \text{if } t = 4,8,12,.. \\ -s(0), & \text{if } t = 1,5,9,.. \\ 0, & \text{otherwise} \end{cases}$$

The bit error depends largely on the FFT size ($\hat{N}$), as shown in Figure 20. This is one example strategy an attacker can implement for a late commit attack. Better strategies, e.g., to target particular modulation schemes and FFT window sizes are considered future work.

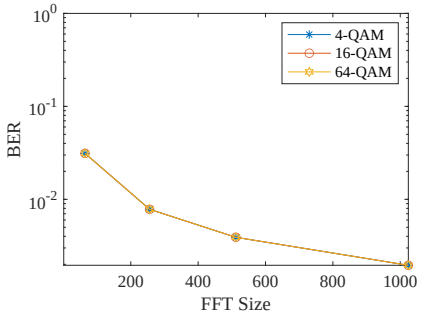

Figure 20: Bit error when attacker perform late commit attack on the V-Range OFDM symbol, and attack signal is procesed by FFT-based receiver.

T_{sym}	Symbol duration
t_s	Sample duration
$\hat{N}$	FFT size
Δ, CFO	Carrier Frequency Offset
T_{Noise}	Noise Threshold
T_{max}	Maximum acceptable power
BER	Bit error rate
SER	Symbol error rate
SER_{Noise}	Symbol error in noise
SER_{Signal}	Allowed symbol errors
V_{Noise}	Receiver's noise variance

Table 6: Parameters and variables

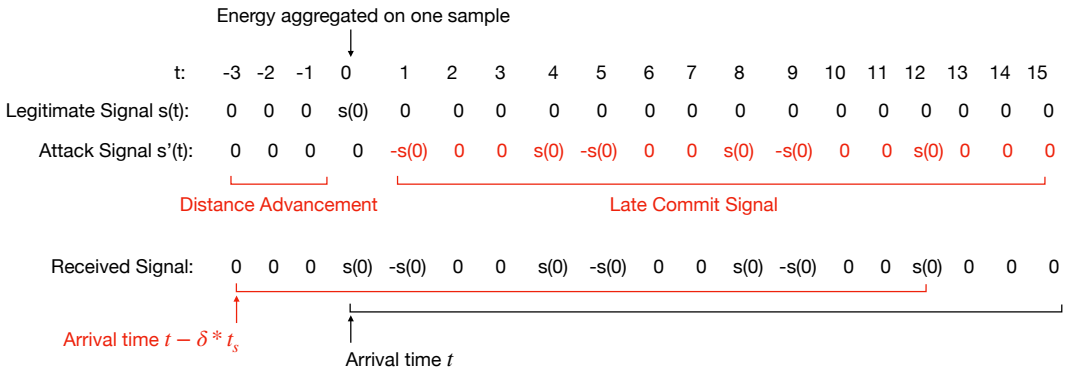

Figure 21: An example of the ED/LC attack on the V-Range symbol when a receiver performs FFT for data detection.