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

Mridula Singh
CISPA
Helmholtz Center for Information Security
Saarbrucken, Germany
singh@cispa.de

Marc Roeschlin
Department of Computer Science
ETH Zurich, Switzerland
marc.roeschlin@inf.ethz.ch

Aanjhan Ranganathan
Khoury College of Computer Sciences
Northeastern University, Boston, MA, USA
aanjhan@northeastern.edu

Srdjan Capkun
Department of Computer Science
ETH Zurich, Switzerland
srdjan.capkun@inf.ethz.ch

***Abstract*—A number of safety- and security-critical applications such as asset tracking, smart ecosystems, autonomous vehicles and 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 [1] 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 secure ranging operations resilient to both distance enlargement and reduction attacks. 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.**

I. Introduction

5G is the next-generation cellular networking technology designed to increase data speeds while realizing a flexible wireless communication infrastructure. Besides low latency and improved configure, 5G is expected to offer high-precision indoor and outdoor positioning services. 3GPP, the standards organization responsible for developing the 5G New Radio (5G-NR) architecture, intends to leverage the 5G network architecture and high bandwidth to enable state-of-the-art positioning techniques [2], [1]. The availability of larger bandwidth in millimeter-wave frequencies makes 5G a perfect fit for high-accuracy positioning. Several applications, including asset tracking, indoor navigation, autonomous navigation, supply chains in the manufacturing industry, geofencing, logistics management, personnel management, etc., are expected to benefit from absolute and relative 5G positioning.

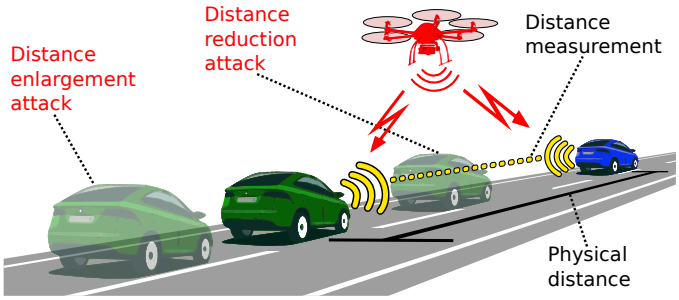

Fig. 1. Example scenario. Distance reduction can result in unexpected emergency braking and evasive maneuvers. Distance enlargement can even lead to a collision.

We note that for several applications that 5G-NR targets, popular positioning systems such as LIDAR or GPS are either unavailable or unreliable (e.g., LIDAR in bad weather or GPS in an indoor setting). In scenarios like vehicle-to-everything (V2X) communication (Fig 1), we expect 5G-NR positioning to complement existing technologies e.g., applications will fuse data from GPS, LIDAR, and 5G-NR to minimize position uncertainty. It is worth pointing out that attacker can manipulate both LIDAR [3] and GPS [4], even when they are fused together [5]. 5G's precise distance measurements, when used with the existing systems such as LIDAR, UWB, and GPS, will increase every individual road user's contextual awareness and improve road safety as a whole [6], [7]. Additionally, the computed location information is expected to augment services running on top of the 5G infrastructure and target applications (e.g., localization during emergency calls) within 5G's architecture itself. 3GPP and other standardization bodies are thus actively working with industry and academic partners to define 5G positioning systems' performance requirements. Even though 3GPP has put forward a plan to introduce positioning into 5G, the current release evaluates potential solutions mainly from the perspective of performance [8], [9]. Many use cases for 5G positioning reside in a security-

Network and Distributed Systems Security (NDSS) Symposium 2022
27 February - 3 March 2022, San Diego, CA, USA
ISBN 1-891562-74-6
https://dx.doi.org/10.14722/ndss.2022.23151
www.ndss-symposium.org

or safety-critical context. Incorrect position estimation would lead to delay in providing emergency services, cause collision between autonomous vehicles and drones (Fig 1), an attacker could get access to private location and services, etc. Therefore, it is crucial to devise a positioning mechanism that is both precise and secure, i.e., it must not be subverted by adversarial interference.

Acquiring the correct position of a device depends on correctly estimating distance with the nearby devices, i.e., User Equipment (UE) and base station in the context of 5G-NR. In the radio-frequency-based ranging system, the device exchanges wireless signals to estimate the physical distance (ranging) between them. Distance estimation is vulnerable to distance manipulation attacks, where an external attacker can prove that these devices are closer or farther than their actual distance [10], [11], [12], [13], [14], [15], [16], [17], leading to an incorrect position estimation [18]. Therefore, correct ranging information is critical in building a secure positioning system.

In this work, we design the first secure ranging system for 5G-NR radio architecture and demonstrate that our system is secure against distance reduction and enlargement attacks. We enumerate the challenges that need to be addressed to enable secure positioning in 5G. Our solution can be integrated into the 5G-NR radio architecture and 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. Furthermore, we identify a novel *carrier-frequency offset attack* that is relevant for 5G-NR based systems and show that our design is resilient to such an attack. Our V-Range system uses shortened orthogonal frequency-division multiplexing (OFDM) symbols in which energy is aggregated over a short time period. A V-Range receiver can ensure that distance estimation is correct by applying proper data and sample-level integrity checks. The short effective symbol length and the added signal and data integrity checks guarantees resilience against all known distance reduction and enlargement attacks. Our security analysis confirms that V-Range constitutes a highly secure ranging system. The success probability of a reduction attack is 10^{-7} and an enlargement attack is $\approx 10^{-5}$ for a 4-QAM (Quadrature Amplitude Modulation) scheme. The probabilities are computed *per* ranging operation and consider the cases where an attacker can modify the measurement by more than the imprecision of the system, i.e., $3\,\mathrm{m}$ for sub-6GHz and $60\,\mathrm{cm}$ for the mm-wave band. We also show that V-Range can perform a (two-way) time of flight measurement in $83\ \mu s$, enabling a high refresh rate and high temporal resolution for high-density application scenarios.

II. Background and Related Work

A. 5G New Radio (5G-NR)

5G has a dynamic Time Division Duplex (TDD) frame structure; slots can be assigned flexibly to uplink or downlink channel. 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 [19].

Every slot consists of 14 OFDM symbols. However, 5G-NR standard allows accommodating more symbols using slot aggregation. The OFDM is a digital multi-carrier modulation scheme that uses closely-spaced orthogonal subcarriers to transmit data 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 $2.08\ \mu s$ (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 $480\ kHz$.

B. Positioning with 5G-NR

The positioning in cellular networks was enabled in the mid-nineties when it was initially introduced to meet regulatory requirements of emergency call positioning. Over time, the ranging techniques, as well as applications space, have developed further. 3GPP proposed LTE Positioning Protocol (LPP) to initiate positioning improvement in long-term evolution (LTE)-advanced system. The LTE supports Enhanced Cell Identity (E-CID), Assisted GNSS (A-GNSS), Observed Time Difference of Arrival (OTDOA), and hybrid localization (A-GNSS + OTDOA) for positioning [20]. OTDOA with Positioning Reference Signal (PRS) is currently used to achieve higher accuracy, coverage, and interference avoidance. There does not exist any evidence that any of these techniques are secure; for example, A-GNSS can be manipulated by replay attack [14], and OTDOA with PRS can be manipulated by overshadowing attack (Section III).

The 5G has currently adopted OTDOA with PRS. However, 3GPP is exploring the feasibility of different distance measurement techniques such as round trip time, time of arrival, angle of arrival, and carrier-phase based techniques [1], [21] and designing new signals to support the various ranging techniques. These new techniques are particularly needed for the wide application space targeted by 5G positioning systems, including asset tracking, smart cities, smart transportation, healthcare, UAVs, geofencing, personnel management, and augmented reality. In the transportation sector, the ranging systems are expected to support traffic management and collision prevention with several field tests already ongoing to explore capabilities of 5G enabled V2X communication and ranging [7]. In healthcare, the 5G positioning should help locate people requesting emergency services, help navigate within hospital buildings, and find medical equipment. These use cases are security and safety-critical; an incorrect distance estimate can lead to loss of money, assets, and human life. Compared to earlier standards, 5G-NR's flexible design, wider bandwidth, mm-wave frequency bands, massive MIMO capabilities make it ideal for these scenarios by realizing high precision, low-latency ranging systems [22]. In fact, standards committee briefings and academic research indicate direct use of OFDM symbols for wide-area positioning infrastructure [1], [22], such as uplink sounding reference signal (UL-SRS) [23]. Therefore, it is necessary to understand attacks possible on

OFDM-based ranging systems and design alternatives that provide secure and precise ranging in order to achieve secure positioning systems.

C. Ranging Systems

Broadly, there are two types of radio frequency-based ranging systems. One set of ranging systems compute distances by measuring one or more physical properties (e.g., amplitude, phase, and frequency) [24], [25]. Although simple to implement, these systems 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 [26], time of arrival [27], 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.

Distance Manipulation Attacks: An external attacker can manipulate distance measurement between benign devices, even when an attacker does not control these benign devices or data exchanged between them. An attacker can directly manipulate signal properties or signal arrival time at the receiver to manipulate distance estimation.

The system based on signal properties such as received signal strength and phase are vulnerable to relay attacks (amplify and forward) [15], e.g., relay attack on keyless entry systems in automobiles [28], [29]. 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. Alternatively, the ToF/ToA based ranging system appears to be more secure against relay attacks [26]. However, several demonstrations have indicated that the ToF ranging systems, if not designed to meet certain physical- and data-layer requirements, are vulnerable to distance manipulation. With the availability of cheap Software Defined Radios (SDR) combined with open-source code, distance manipulation has become far more accessible [30].

Currently, UWB with two-way ToF measurement is the only system that can thwart both reduction and enlargement attack [16], [31]. However, there is no indication that 5G-NR will implement or incorporate secure UWB ranging into its standards. Since recent research and standard briefings indicate the use of OFDM symbols in 5G-NR for ranging (positioning) and ToF measurement is secure against relay attack, we discuss the possibility of manipulating ToA of OFDM symbols in the next section.

III. Attacks on OFDM-based Ranging Systems

The adversary's goal is to force two benign devices to measure a false distance without physically displacing them. We consider both distance enlargement and reduction attacks as both of them have the potential to cause catastrophic failures. We assume that the attacker can transmit, eavesdrop, intercept, record, and replay arbitrarily strong radio frequency signals. The attacker has all the information broadcasted in plain text. The attacker also has the capabilities to synchronize

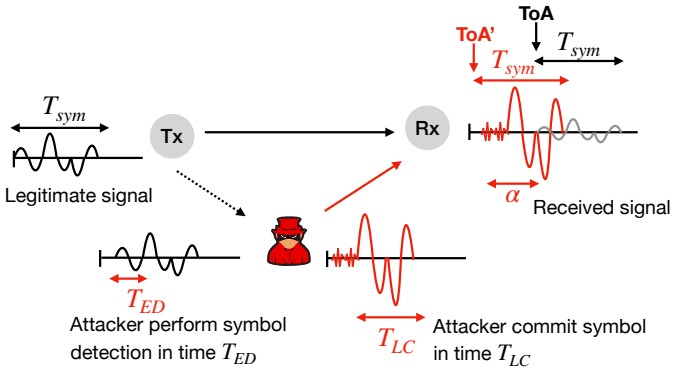

Fig. 2. Distance reduction by early detect late commit attack on the longer symbols.

and listen to the communication going on in the network, e.g., an attacker can have user equipment (UE) capabilities and connect with the base station. 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 [32], [33]. 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 an attacker cannot manipulate data transmitted between them. In the following, we discuss the possibility of manipulating the ToA estimation of the OFDM symbols. The attack we present here applies to LTE, 5G, and other systems that use OFDM symbols for ToA estimation.

A. Distance Reduction by Early Detect Late Commit

There exist the possibility of advancing arrival time of OFDM symbol by ED/LC attacks [11], [12]. 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 the 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 ToF, thereby successfully executing a distance reduction attack. Such attacks have already been demonstrated [34] and can be considered as a form of late commit attack. Therefore, it is essential to design symbols resistant to ED/LC attack while conforming to the properties and requirements set by the 5G numerology. We explore

[1] radio waves travel 30 cm in 1 ns

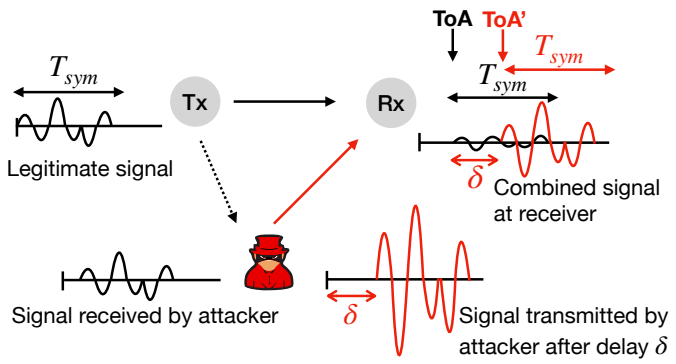

Fig. 3. Distance enlargement: symbol overshadowed attack.

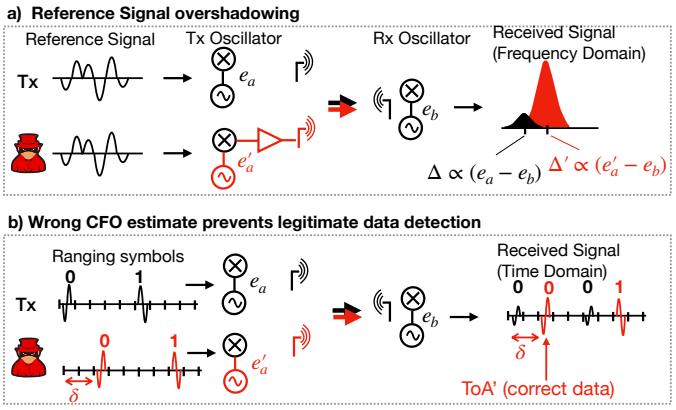

Fig. 4. Distance enlargement by manipulating frequency offset estimation.

ED/LC attacks later in Section V-A and provide a secure receiver design in Section IV-B.

B. Distance Enlargement by Overshadowing Symbols

An adversary can enlarge the measured distance by performing a signal overshadow attack, as shown in prior works [35], [36]. In a signal overshadow attack (Fig 3), the attacker transmits a delayed copy (say with a time delay δ) of the legitimate signal with a higher power to 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 receiver uses samples collected during symbol duration T_{sym} to perform data detection and ToA estimation. In such a receiver design, the attack is successful if a higher power attack signal arrives at the receiver after delay δ, such that energy received in the duration δ is insignificant for ToA estimation 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 $\delta = 0.1667\mu s$ (one percent of symbol length). The energy detected at the receiver during $0.1667\mu s$ is not sufficient to perform the symbol detection or ToA estimation. Therefore, the receiver uses the higher strength attack signal for the ToF measurement, with $\delta = 0.1667\mu s$, an attacker achieve distance enlargement by $\approx$ 50 m. By increasing the value of δ, the attacker can achieve several hundred meters of distance enlargement.

C. Distance Enlargement by Carrier Frequency Offset Attack

In this section, we introduce a novel attack called *carrier frequency offset attack*. This attack 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., [32], [33]. 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, the devices will experience carrier frequency offset (CFO) and phase offsets [37]. The offset is typically corrected with the help of reference signals, e.g., the preamble in ultra-wideband high rate pulse mode (UWB-HRP) [38], training sequences in the WiFi [39], and phase tracking reference signals and synchronization signals in 5G [40], [41]. A receiver can estimate the CFO using the expected and received reference signal and correct the offsets. The presence of offset results in inter-carrier interference, signal attenuation, and phase rotation. The incorrect offset estimation in conventional communication systems leads to a high symbol error rate and potentially a denial of service due to the imbalance in the in-phase and quadrature components 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.

As shown in Fig 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 with a time offset, thereby increasing the measured distance. The receiver discards the legitimate signal as noise (strong multipath) as it does not provide correct data even though it has finite energy. In Fig 4b, the attack is shown using short symbols to emphasize that short symbols are also vulnerable to the offset manipulation attack. Until recently, only energy detector receivers are proven secure against distance enlargement attacks [16], and issues

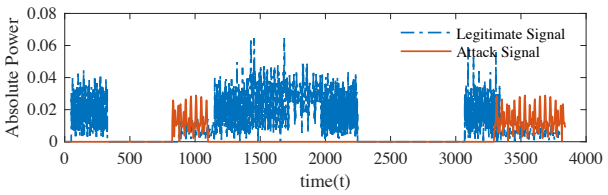

Fig. 5. PRS arrival time manipulation: legitimate signal (in blue) contain PRS signal and information needed for PRS detection, such as cell identity. The attacker is sending PRS signal (in red) with the higher power in advance.

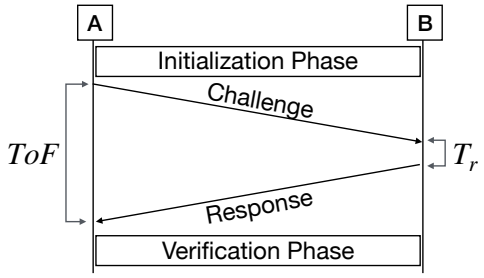

Fig. 6. Device A and B run a distance bounding protocol to acquire the time-of-flight (ToF) and measure the distance.

occurring due to the minor carrier frequency mismatch were not of importance. Any system that uses a coherent receiver, including UWB, LTE, 5G, and WiFi, is vulnerable to distance enlargement by this attack. In Section VI, we show that offset mismatch of 10 kHz is sufficient to prevent data detection [2].

D. Attacks on the PRS (OTDOA)

The LTE/5G's OTDOA is designed to be a broadcast-based service; the Positioning Reference Signal (PRS) is transmitted in the downlink channel. User equipment measures the difference in the arrival time of PRS signal originating from multiple base stations to determine its location. The ToA is estimated by correlating the received signal with a locally generated reference signal. Therefore, all information needed for the local reference generation, such as physical-layer cell identity, number of resource block allocated to PRS, subframe number, and other optional fields, are available to each user [20]. Some of these parameters are communicated in advance by LPP protocol, while others are contained within the subframe containing PRS. The data contained in the LPP protocol or in the subframe is intended for all UE requesting location measurement. Therefore, an attacker can use a UE or open platform like srsLTE to obtain this information and transmit the PRS signal α duration earlier than legitimate PRS to perform distance reduction, as shown in Fig 5. Similarly, an attacker can send it after delay δ for distance enlargement. Mobile phone providers have recently started implementing PRS [42], and it is yet not supported by open-source implementations such as srsLTE [43]. We analyze attacks on the PRS using MATLAB LTE toolbox and software-defined radios USRPs in Section VI-E.

[2]Transceivers operating at 4 GHz and a clock error of 10 ppm expect carrier frequency offset up to ± 80 kHz

IV. V-Range – Secure Ranging in 5G

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.

To realize a secure ranging system, we also need a secure verification process at the receiver. An attacker should not succeed in compromising the ranging signal directly (e.g., ED/LC) or indirectly (e.g., predictable reference signals for offset correction). The receiver needs to implement integrity checks at both the physical and data levels 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 [44], [31]. 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 success [16]. 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.

A. System Overview

As shown in Fig 6, 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 require key exchange between devices, a similar framework can be used to perform the initialization and verification phase of the distance bounding protocol. For example, communication in vehicular networks must ensure privacy, confidentiality, integrity, and nonrepudiation, irrespective of ranging capabilities [45]. 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., the transmitter initiates transmission of the 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 reduc-

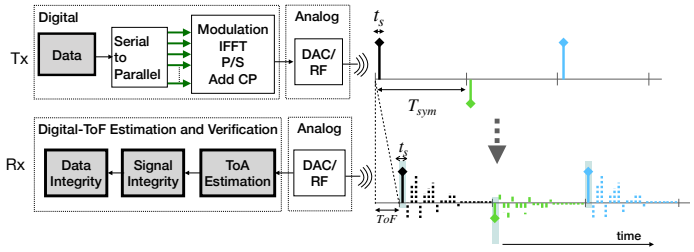

Fig. 7. V-Range uses shortened OFDM symbols and the receiver checks the integrity of ToA estimates.

tion and enlargement attack. The V-Range transmitter compresses the effective OFDM symbol length by transmitting the same data in all subcarriers; this is in contrast to conventional OFDM, in which each of the subcarriers can carry different data. The result is the aggregation of symbol energy over a short time period (i.e., few ns), making it harder for an attacker to perform ED/LC distance reduction attacks. The short effective symbol length also results in increased ranging resolution.

The ToA of these symbols is validated by physical layer properties and data at the logical layer. Similar to LTE, 5G uses fixed reference signals to enable phase-tracking and synchronization. An attacker can spoof these 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 reference signals for the clock offset estimation, 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.

In V-Range, communicating devices perform an initialization phase and pre-share data for secure ranging. The constructed message is converted into a physical layer code using shortened OFDM symbols. These symbols have length T_{sym} within which energy is aggregated over a much smaller part t_s of the symbol. The receiver verifies the ToA of the signal by using granular samples of length t_s, and performs the following integrity checks. The signal is considered a legitimate message for ToA estimation 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.

B. 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

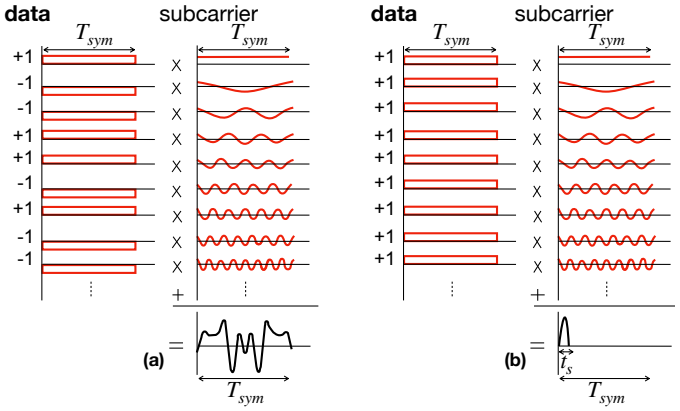

Fig. 8. The shortened OFDM symbols are generated by modulating all subcarriers with the same data.

shown in Fig 8a. However, a secure ranging system does not require high throughput; instead, its primary requirement is to estimate distance precisely. 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 the original OFDM but with energy aggregated over a much smaller part t_s of the symbol, as shown in Fig 8b.

In OFDM, the Inverse Fast Fourier Transform (IFFT) is applied to subcarriers to generate the time-domain signal. The subcarriers' amplitude is scaled depending on the data modulated on them and then added together. If subcarriers carry different data bits, the signal's energy is distributed over $\hat{N}$ time samples transmitted over T_{sym} duration. When the subcarriers are modulated with the same data (i.e., subcarriers have the same energy), all samples except one cancel each other. The symbol's length (T_{sym}) 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 collected within this 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. Below, we formally describe these specialized OFDM symbols. Each OFDM symbol can be described as a complex-valued function $s(t)$ in the time domain. $s(t)$'s real and imaginary parts (I/Q data) represent in-phase and quadrature components. An OFDM symbol is then expressed as the aggregation of the contributions of all $\hat{N}$ subcarriers:

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

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} [46]. 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 $t \in [-T_{\text{g}}, T_{sym})$ and $T_{\text{g}} < T_{sym}$, this

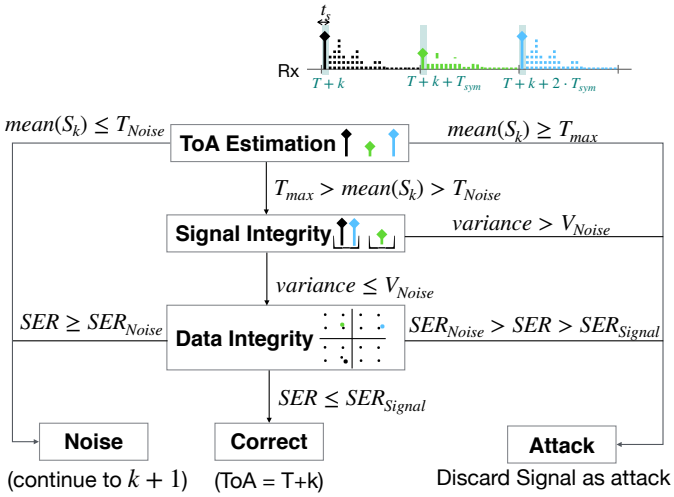

Fig. 9. The signal received at the estimated ToA is verified using signal and data integrity checks. The mean power, variance, and symbol error threshold differentiate between noise, legitimate, and attack signals.

condition is only satisfied when $p = 0$. In case $e^{j2\pi t/T_{sym}} \neq 1$, the geometric series can be rewritten as:

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

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

where we set $\rho = j2\pi t/T_{sym}$. This is known as a (frequency-shifted) Dirichlet kernel or periodic sinc function [47].

The signal's maximum amplitude 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 main "lobe" of the symbol's theoretical width 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. Fig 8b) shows how $s(t)$ is composed of the different subcarriers. It is apparent that the energy is focused on a single narrow peak. Fig 23 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 X. Any digital modulation can be used to encode data in X, independent of the number of subcarriers. We explore the choice of modulation scheme in Section VI to find a performant and secure configuration. We do not need high-order modulation for ranging, as these symbols are intended to be used as reference symbols for ranging. We also point out that physical channel features (e.g., pilot subcarriers and the cyclic prefix required for channel estimation), normally a part of OFDM symbols, are not available in our modified symbols. These symbols' advantage is that they exhibit single carrier symbols' properties even though they are valid multi-carrier OFDM symbols. Due to single carrier properties, there is no inter-carrier interference or subcarrier phase rotation, 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}, V-Range OFDM symbol's energy is concentrated over a much smaller duration. Therefore, the receiver estimates arrival time by using fine-grained samples of duration t_s. The receiver starts the search at an offset of k samples and continues until it finds the legitimate symbol (or attack traces). 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 samples' average power. If power $< T_{Noise}$, the samples are discarded as noise and receiver continue the search at offset $k = k + 1$. If it is $> T_{max}$, 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. The signal integrity is checked using the signal's statistical properties (e.g., total power or variance [16], [44]). For the QAM modulated signal, power thresholds are useful for ToA estimation, but variance-based checks are required for ToA verification. The power thresholds are not sufficient to differentiate between legitimate and attack signals, as a receiver cannot predict the channel's path loss 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 [48], 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 $T + T_{sym}$, 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. The signal transmitted with the same power, if experience the same channel conditions, should have the same received power. Although they can have residual 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 IX-B)). 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 expected power levels, the signal is passed on to the data integrity checker.

Data Integrity Checker After verifying the ranging symbols' physical-layer integrity, the V-Range receiver checks the received data's correctness by checking the symbol errors, i.e., the difference between the received symbols and expected symbols. The symbol error rate SER depends on the channel conditions (i.e., SNR) and hardware clock inaccuracies (i.e., carrier frequency offset). Some modulation schemes withstand 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 III, secure ranging applications cannot use reference signals to correct CFO. The CFO results in in-phase and quadrature-component imbalance, which can make data recovery 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 (Appendix IX-C). The allowed symbol error rate is both a performance and a security parameter. V-Range allows symbol errors up to SER_{Signal} to perform under diverse channel conditions with hardware of different capabilities. The signal with symbol 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.

Resource Allocation: V-Range requires consecutive subcarriers for the short-symbol generation, and these symbols should be transmitted within the channel coherence time. The wider bandwidth and wider sub-carrier bandwidth allocation are favorable to the V-Range design. The wide bandwidth provides better security and accuracy guarantees. 3GPP is discussing to provide wider sub-carrier bandwidth, which would reduce the symbol duration T_{sym}, allowing transmission of more V-Range symbols during the same time. We only need symbol length T_{sym} slightly higher than the delay spread; the channel is underutilized when using narrow subcarrier bandwidth. Like any ToF/ToA based ranging technique (e.g., PRS), V-Range also needs to announce its presence using an upper-layer protocol, and ToF/ToA estimation from multiple stations is needed for the position estimation [18]. The repetition frequency of the V-Range messages and the choice of the distance bounding protocol (e.g., one-to-one, group) depends on the use cases 5G-NR supports.

V. Security Analysis

The V-Range system can be considered as a class of Message Time of Arrival Code (MTAC) [44]—these codes allow the verification of the time of arrival and consist of a tuple of probabilistic polynomial-time algorithms for (1) key-generation, (2) code-generation, and (3) verification. We assume that challenge and response messages are generated using distance bounding protocols, and we focus on the code-generation and verification algorithms. In the code-generation process, the transmitter converts keying material into shortened OFDM symbols. The shortened symbols are comparable to a *sequence of single-pulse bits*, a known MTAC [44], since the energy of the symbol is aggregated in one sample of duration t_s ($\approx$ few ns). The verification function is the combination of signal and data integrity checks; the signal is used for ToA if the mean power of the received signal is above T_{Noise}, its variance is less than V_{Noise} and symbol error is below SER_{Signal}. The signal is otherwise discarded as noise or an attack.

We assume that the attacker is aware of the code-generation and verification functions, and the values that the receiver uses for the different decision parameters, i.e., T_{Noise}, V_{Noise}, SER_{Noise}, and SER_{Signal}. However, as mentioned before, we assume that challenge and response messages (i.e., MTAC's key-generation algorithm) are cryptographically secure, we assume that the attacker cannot predict the data transmitted using shortened OFDM symbols. Due to the attacker's physical constraints and laws of physics (e.g., attacker hardware delay, attacker location, and being able to transmit signals faster than the speed of light), we assume that the attacker cannot prevent the legitimate ranging signals from arriving at the receiver or send it faster. The attacker has access to the samples already emitted by the legitimate transmitter and can precisely align its attack signal with the legitimate transmission. Strictly speaking, when the legitimate transmitter is transmitting the t^{th} sample, the attacker has access to all $t-1$ legitimate samples, where each sample's duration is a few nanoseconds, i.e., $t_s \approx 2.5\,\text{ns}$ and $t_s \approx 10\,\text{ns}$ for a system bandwidth of $400\ MHz$ and $100\ MHz$ respectively.

A. Distance Reduction Attack

In ToA based ranging systems, if the data is unpredictable, the attacker needs to create an illusion of an earlier arrival time by manipulating the symbol structure, i.e., execute an ED/LC attack. The information leaked by the samples already transmitted by the legitimate transmitter is instrumental in such attack strategies. In the following, we show that FFT-based receivers commonly used to reconstruct the data modulated on the subcarriers of OFDM symbols do not provide secure ranging, even when used with our shortened OFDM symbols. We then analyze the security guarantees of V-Range and

highlight the importance of using a combination of secure code generation and verification algorithms.

Early detect Late commit: 5G uses long OFDM symbols (order of μs) to transmit data, and it is therefore vulnerable to ED/LC attacks (Section III). The attacker manipulates the receiver in measuring an earlier arrival time by producing correct data on the samples arriving earlier than the legitimate samples. To reconstruct the data transmitted on the sub-carriers (X_k), an FFT-based receiver uses all $\hat{N}$ samples, i.e., $s(t)$ at $0 \leq t < \hat{N} - 1$.

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

Let us assume we use an FFT-based receiver design with the shortened OFDM symbols i.e., concentrate energy within a short duration $t_s \ll T_{sym}$ by emitting only one sample with amplitude greater than zero for every symbol, as described in Section IV-B. In that case, the attacker will learn about the symbol structure and the data encoded in the symbol after receiving the very first sample of the symbol, i.e., $s(0)$. In order to achieve a distance reduction of α samples duration, the attacker can commit the next $\hat{N} - \alpha$ samples such that when the receiver uses samples $\alpha \leq t < \hat{N} - \alpha$ to perform demodulation, it results in the correct data. We show a simple strategy to generate a late commit signal in Appendix IX-A, and present the result for the bit error rate it achieves for different modulations and FFT sizes.

On the other hand, the V-Range receiver treats each sample independently—the receiver is only interested in sample $s(0)$ and does not combine the samples collected at $t > 0$ for the symbol detection. In order to advance arrival time by α sample duration, attacker needs to early commit the sample $s'(-\alpha)$ at $t = -\alpha$ before the transmission of the legitimate sample $s(0)$ at $t = 0$. As there is no information leakage about $s(0)$ from samples collected at $t \leq -\alpha - 1$, the attack success depends on successful guessing. V-Range performs ToA estimation using n symbols, therefore, the attacker needs to generate the set $\mathbf{S}'(-\alpha) = \{s'_i(-\alpha) | 1 \leq i \leq n\}$ where symbol error is below $\lceil n \cdot SER_{Signal} \rceil$. The probability of generating such a sequence is given by the expression $\sum_{k=0}^{\lceil n \cdot SER_{Signal} \rceil} \binom{n}{k} (1 - 1/M)^k (1/M)^{n-k}$, where $1/M$ is the probability of correctly guessing a symbol. For example, if choosing 4-QAM as the modulation and setting $SER_{Signal} = 0.2$ and $n = 20$, the probability of attack success is 10^{-7}.

B. Distance Enlargement Attack

The algorithms that constitute an MTAC [44] should detect the first instance/path of the legitimate signal (i.e., $\mathbf{S}(0)$), even if an exact copy containing correct data is replayed with delay δ (i.e., $\mathbf{S}'(\delta)$) by an attacker. V-Range meets this requirement by ensuring that the receiver detects the legitimate signal and rejects a (replayed) attack signal. Note that the attacker cannot block the legitimate signal or prevent its detection at the receiver by generating a perfectly reciprocal signal; the duration of these samples ($\approx$ few ns) is too short to detect, process, and generate a reciprocal signal. Therefore, an attacker needs to manipulate the legitimate samples by injecting noise or a structured signal in an attempt to either achieve (partial)

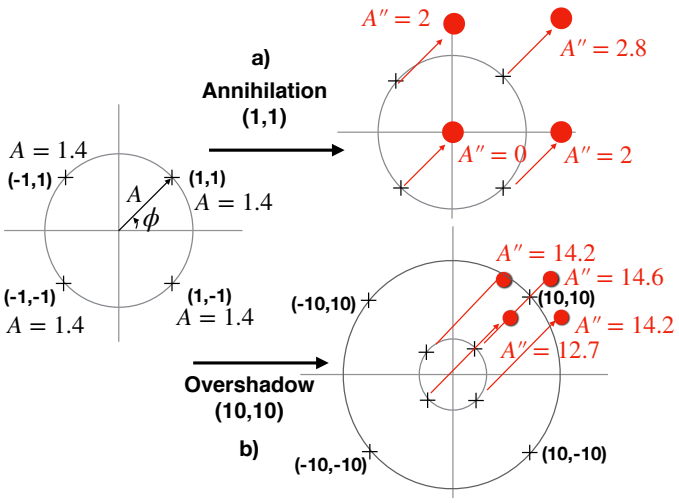

Fig. 10. I/Q constellation in the absence and presence of the attack (annihilation and overshadowing) signal.

annihilation or signal overshadowing where the legitimate signal is drowned by the attacker's transmission. If the attacker chooses to emit a structured signal, it can modify phase and amplitude as well as transmit at different carrier frequency offset(s). The attacker succeeds in distance enlargement if the manipulated signal satisfies one of the following constraints imposed by the V-Range design: (i) the mean power of the received signal is less than T_{Noise}, or (ii) it has a higher bit/symbol error rate without increasing the variance (i.e., symbol error should be more than SER_{Noise} and variance less than V_{Noise}). The following analysis confirms that even a strong attacker capable of determining the expected power of the received signal cannot steer the mean and variance below the expected values (T_{Noise} and V_{Noise}).

As defined in Section IV-B, $s(0)$ is an I/Q sample, the modulation schemes use a set of in-phase (I) and quadrature (Q) inputs to modulate the data. For example, the 4-QAM shown in Fig 10 have four different configuration for (I, Q) values, i.e., $\mathbb{IQ}_4 = \{(I, Q) | I = \pm 1, Q = \pm 1\}$. All 4-QAM modulated symbols are transmitted with the same amplitude ($A = \sqrt{I^2 + Q^2}$) and differ only in the phase ($\phi = tan^{-1}(Q/I)$). High order modulation such as 16-QAM and 64-QAM encode data using different phase as well as different amplitude. In order to perform sample manipulation, an attacker can inject signal $s'(0)$ with in-phase I' and quadrature Q', where amplitude is A' and phase is ϕ'. If both legitimate and attack signal arrive at the receiver at the same time, the resulting in-phase value is $I'' = I + I'$ and quadrature value is $Q'' = j(Q + Q')$, i.e., both amplitude $A'' = \sqrt{(I + I')^2 + (Q + Q')^2}$ and phase $\phi'' = tan^{-1}((Q + Q')/(I + I'))$ of the received signal are affected by the signal injected by the attacker.

Reducing received power: The optimal approach to prevent detection of the received signal is signal annihilation, i.e., by reducing mean power below T_{Noise}. The attacker can choose an arbitrary value for I' and Q', however, perfect cancellation is only possible when $I' = -I$ and $Q' = -Q$, i.e., $A = A'$ and $\phi' = \phi + \pi$. If the I' and Q' values are chosen from the same set of legitimate transmission used for the modulation ($\mathbb{IQ}$), the

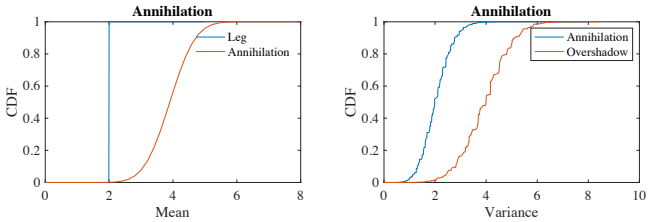

Fig. 11. Mean (a) and Variance (b) of the 4-QAM modulated signal after attack.

probability of successful cancellation increases to $1/M$ (i.e., $M = |\mathbb{IQ}|, M = 4$ for 4-QAM.). As shown by an example in Fig 10 for a 4-QAM signal, if the legitimate signal has amplitude $A = 1.4$, the received signal, after the cancellation attempt, has amplitude $\mathbb{A}'' = \{0, 2, 2.8\}$, with probabilities $p_1 = Pr(A'' = 0) = 0.25$, $p_2 = Pr(A'' = 2) = 0.5$ and $p_3 = Pr(A'' = 2.8) = 0.25$. As we know that each amplitude A''_k occurs with probability p_k, the probability of the occurrence of a $S''(0)$, when each amplitude A''_k occurs exactly x_k times is given by the multinomial distribution

$$Pr = \frac{n!}{x_1! \cdot \ \ldots \ \cdot x_{|\mathbb{A}''|}!} p_1^{x_1} \cdot \ \ldots \ \cdot p_{|\mathbb{A}''|}^{x_{|\mathbb{A}''|}} \text{ where } \sum_{k=1}^{|\mathbb{A}''|} x_k = n \quad (2)$$

This equation provides the probability of each configuration of amplitudes, therefore, the occurrence of different mean power, as shown in Fig 11a for n=20 4-QAM symbols. The probability of reducing received power below the expected power (≈ 2) is $3.3 \cdot 10^{-4}$; in all other scenarios, the presence of attack signal increases received power instead of reducing it. The probability of achieving signal cancellation for all 20 symbols is $9 \cdot 10^{-13}$, i.e., when $A''_k = 0, x_k = n$ in equation 2

Increasing SER without increasing variance: The V-Range receiver discards any signal as noise if the SER is higher than SER_{Noise} *and* the variance of the samples transmitted with the same power is below V_{Noise}. This condition can be satisfied if the attacker steers the signal's phase while keeping the amplitude in check, i.e., the receiver will recover incorrect data due to the incorrect phase estimation. As the attacker cannot manipulate the signal on the fly due to short sample duration ($\approx$ few ns), the attacker needs to inject the signal impacting both amplitude and phase simultaneously. Therefore, an attacker cannot change the phase without manipulating the amplitude of the received signal. As shown by the example in Fig 10a, the amplitude of the legitimate and the attack signals is 1.4 if legitimate and attack signal is chosen from $\mathbb{IQ}_4$, the resulting amplitude $\mathbb{A}'' = \{0, 2, 2.8\}$ due to difference in the phase. Fig 11b shows the distribution of the variance for this $\mathbb{A}''$ for 20 symbols using equation 2. The probability of achieving $V_{Noise} = 0$, as required in the absence of the noise, is $9.5 \cdot 10^{-7}$. On choosing a high variance signal, where an attacker varies both amplitude and phase, the variance is only bound to increase with the higher probability. For example, when the legitimate signal is 4-QAM modulated, and an attacker injects 16-QAM modulated signal, the probability of achieving $V_{Noise} = 0$ reduces to $2.7 \cdot 10^{-12}$. The samples in the set $\mathbf{S}(0)$ are not affected by multipath components, but they experience an AWGN[3] channel. Therefore, the receiver needs to set the value of V_{Noise} based on the expected noise power spectral density and the system's bandwidth. For example, if the receiver sets $V_{Noise} = 0.5$, the probability of achieving variance below V_{Noise} is $3 \cdot 10^{-04}$, assuming that the received signal is only a combination of legitimate and attack signal selected from $\mathbb{IQ}_4$, and probability is obtained using equation 2.

[3]Additive White Gaussian Noise

Overshadowing legitimate signal: An attacker has to perform an overshadow attack by transmitting a high power signal with a delay $\delta = T_{sym} * k$, such that the attack signal overlaps the legitimate signal. Otherwise, the receiver will find traces of the legitimate signal and use it for the ToA estimation. The attack signal is an amplified version of the legitimate signal, i.e., $s'_{i+k}(0) = \mathcal{A} \cdot s_i(0)$, where $\mathcal{A}$ is the amplification factor. Therefore, received signal is the combination of the expected and an amplified signal, i.e., $s''_{i+k}(0) = \mathcal{A} \cdot s_i(0) + s_{i+k}(0))$. This is a special case to increase the SER of the legitimate signal, by hiding it under the high power attack signal. 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 overlapping of the delayed high power attacker signal over the legitimate signal changes the physical layer properties; the legitimate signals behave as high variance noise interference to the attacker's signal. As shown in Fig 10b, the amplitude of the received signal varies due to the phase difference between legitimate and attack signal. The distribution of the variance in Fig 11b shows that the overshadow signal has high variance.

Carrier Frequency Offset Attack: In a traditional OFDM-based system, such as the proposed 5G numerology, 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 (see Section III-C). The V-Range design does not use reference signals for offset estimation, V-Range relies on shortened OFDM symbols, and applies integrity checks; these choices collectively make the V-Range system secure. The V-Range receiver uses short 5G symbols for CFO estimation as well as data detection; therefore, an attacker has to manipulate these symbols directly. An attacker can generate signals with different frequency and phase offset to mount an attack, such that the resulting signal, the combination of legitimate and attack signal, arrives at the receiver with different phases, and the receiver cannot recover data from this distorted signal. However, by crafting an attack signal with varying phase and frequency, the attack adds high variance to the combined signal, making it detectable at the V-Range receiver.

The V-Range design prevents all possible distance enlargement attacks as an attacker needs to generate a signal that overlaps with the legitimate signal. The combination of the legitimate and attack signal induces a detectable change in the physical layer properties of the received signal, i.e., the analysis above highlights that the presence of attack signal increases the mean power and variance. This analysis shows that the V-Range detects the attempt of manipulating the first path/instance of the legitimate signal with high probability. Therefore, V-Rage is the first construct that provides a secure MTAC against both distance reduction and enlargement attack. We further examine the performance and security guarantees of the V-Range using experimental setups.

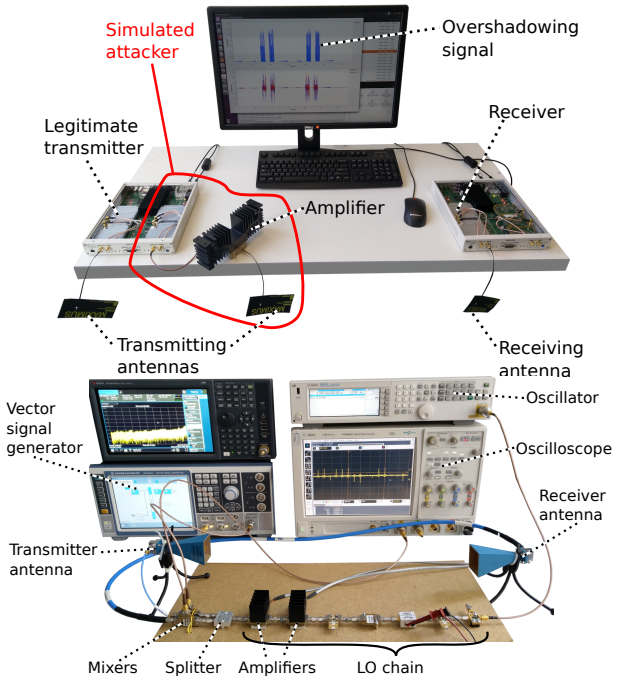

Fig. 12. Sub-GHz and mm-wave setup.

VI. 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 [49], 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 [50] 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 mm-wave setup, the two frequency ranges 5G operates over. For both frequency bands, we use the maximum allowed subcarrier bandwidth (i.e., shortest T_{sym}), as longer T_{sym} only increase latency. We analyze the performance and security of the sub-6GHz and mm-wave band experimental setups.

Sub-6GHz setup: We use two USRP-X310 SDRs [51] as shown in Fig 12. Our setup is similar to other experimental studies on 5G [52]. 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 [53].

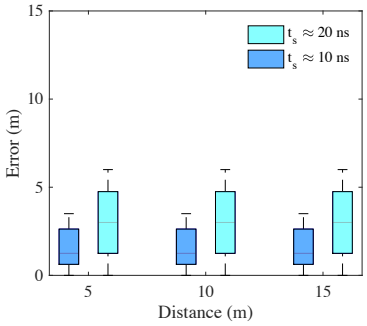

Fig. 13. Accuracy of the distance measurement depends on the sample duration t_s

Fig 12 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 mm-wave 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.

All experiments using these setups were performed in a basement to prevent signal leakage, limiting the communication range (upto $15m$) and the channel conditions between devices. We believe that the ranging distance of up to 15 m is sufficient for many applications targeted by 5G, including geofencing, augmented reality, logistic and personnel management, V2V ranging. In order to validate V-Range performance and security in the varied conditions at the different SNR and channel conditions, we use simulation (Subsection-D).

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 (Fig. 12). Antennas are placed such that the travel time of the attack and legitimate signal differ at max by 1 ns. Since this setup is used only for manipulating ToA estimation, the shorter distance between devices does not limit attacker capabilities. An attacker can choose the time duration to advance or delay the signal's arrival time. For the overshadowing attack, the attack signal is sent after a delay $\delta = T_{sym}$ and it is 20 dB stronger than the legitimate signal.

A. Parameters and Metrics

V-Range's performance depends largely on three parameters: (1) maximum expected noise variance V_{Noise}, (2) receiver signal's maximum allowable symbol error rate SER_{Signal}, and (3) maximum expected symbol error of noise SER_{Noise}. The threshold V_{Noise} is channel-independent and can be pre-estimated from the receiver's noise profile (e.g., $4.5 \cdot 10^{-7}$ in our sub-6GHz setup). SER_{Noise} and SER_{Signal} are channel

TABLE I. FALSE POSITIVES: VARIANCE ESTIMATE IS IMPRECISE WHEN USING HIGH ORDER MODULATION WITH A SMALL SAMPLE SIZE.

	$n = 20$			$n = 100$		
SNR [dB]	**4**	**6**	**8**	**4**	**6**	**8**
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

dependent. For example, a low SER_{Signal} increases false positives in noisy environments and high SER_{Signal} allows an attacker to make more incorrect guesses when brute-forcing a challenge and response message. Similarly, SER_{Noise} should be chosen to prevent V-Range classifying noisy environments without any legitimate ranging signal as an attack (high false positives). Furthermore, SER_{Noise} depends on the modulation scheme, i.e., low SER_{Noise} for higher-order modulation (64-QAM). We evaluate V-Range's performance and security for various 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 V-Range design's performance under different SNR conditions. We vary the transmit power and distance between devices to emulate different SNR conditions.

B. 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: Fig 13 shows the measurement error for the sub-6GHz setup obtained under different bandwidth and distance configurations. The results show that measurement 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 $t_s \approx 10\,\text{ns}$, the error is below 3m. For the $400\,\text{MHz}$ bandwidth mm-wave setup, the achieved precision is $60\,\text{cm}$. These numbers are in line with what 3GPP expects to be attained by ranging techniques operating in the 5G spectrum [1]. When performing two-way ranging, $2 \cdot n = 40$ symbols are exchanged. Thus, if symbol lengths of $16.67\mu s$ (sub-6GHz) and $2.08\mu s$ (mm-wave) are used, the entire ranging operation can be completed in $667\mu s$ or $83\mu s$, respectively.

Effect of V_{Noise}: The signal integrity checker module monitors the received signal's power levels 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 I. We observe that 4-QAM and 16-QAM signals have a low probability of triggering false alarm, but 64-QAM signals have a high probability of getting identified as an attack signal for $n = 20$. 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, the 64-QAM's performance improves for $n = 100$, and therefore we conclude that lower modulation schemes should be used when sending fewer symbols.

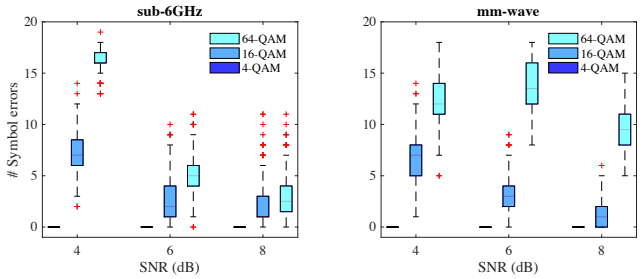

Fig. 14. Symbol error rate of the modulation schemes depends on the channel condition (i.e., SNR).

TABLE II. PERFORMANCE OF V-RANGE AT $SNR = 8\,dB$.

$(SER_{Signal}, SER_{Noise})$	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

Effect of SER_{Noise} and SER_{Signal}: We evaluate V-Range's performance under various SNR conditions. Fig 14 shows the symbol errors over 100,000 challenge messages. The results are similar for the sub-6GHz and mm-wave setups. 4-QAM 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 II, 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.

C. Security Evaluation

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

Distance Enlargement Attack: The distance enlargement attack's success depends on the attacker's ability to prevent the legitimate signal's detection by annihilation or overshadowing. In both attack scenarios, the attacker's signal overlaps the legitimate signal; the samples constructed at the receiver contain both the 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. We did not observe receiver saturation even when the attack signal for symbol overshadowing is $20\ dB$ stronger than the legitimate signal, which validates the use of the receiver's dynamic range as threshold T_{max}.

The data integrity checker alone does not detect annihilation and overshadow attacks as the symbol error is either too high (annihilation attack) or too low (overshadowing attack)(Fig 15). The signal's symbol error $> SER_{Noise}$ in

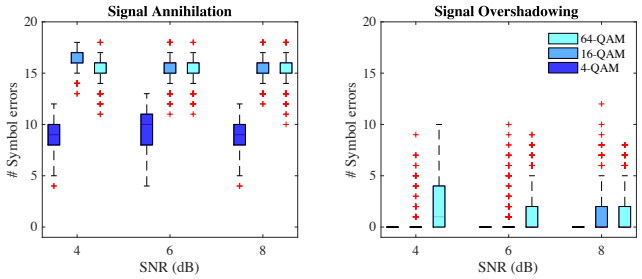

Fig. 15. Symbol error rate in the presence of attacker.

TABLE III. ATTACK DETECTION USING INTEGRITY CHECK.

	Annihilation			Overshadowing		
SNR [dB]	**4**	**6**	**8**	**4**	**6**	**8**
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

an annihilation attack. If the receiver only checks data correctness, the legitimate signal will be discarded as noise and the attacker's 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 (symbol error $< SER_{Signal}$. Therefore, the receiver will use this delayed attack signal for distance estimation.

However, the signal's physical layer properties are changed when attacker manipulates the legitimate signal's data and is detected by the signal integrity checker. The signal integrity checker results are shown in Table III. We observe that an annihilation or overshadow attack is detected with high probability ($4 \cdot 10^{-5}$ false negative rate) at SNR 8 dB. The attack detection probability of the annihilation attack is lower for the low SNR condition.

D. Simulating V-Range in urban scenario

Due to the lack of permission to perform experiments in the open areas. we uses simulations to validate the feasibility of V-Range under different channel conditions. In order to emulate real-world channel conditions, we use MATLAB LTE Toolbox to model the channel scenarios defined in 3GPP TS 36.104 for cellular communication. These channel models are widely used to test the performance of cellular communication systems. We have carefully selected a very representative radio-frequency environment and channel profile that captures most of the intricacies of the wireless channel in an urban area and under moving scenarios, the model generate Rayleigh fading channel with changing delays and doppler shift.

The results show that varying channel conditions have an insignificant effect on the variance (Fig 16a) when all V-Range symbols are transmitted within the channel's coherence time (i.e., all short symbols are affected equally by the multipath components). Therefore, it is possible to determine the variance threshold V_{Noise} in advance to differentiate between legitimate and attack signals. When transmission time is longer than coherence time, we see an increase in variance (Fig 16b). The signal SNR is different under different simulated channels. However, the receiver does not need to change its power

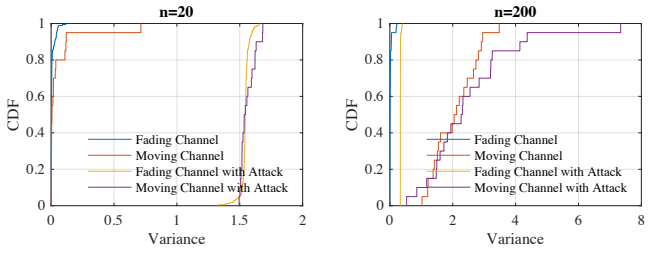

Fig. 16. Variance on different channel conditions.

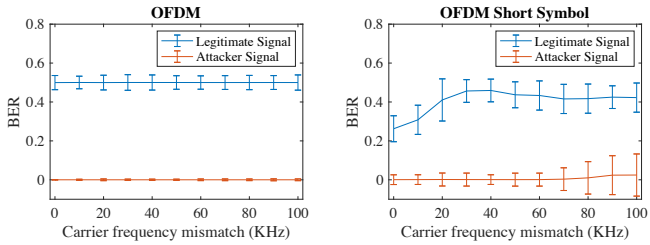

Fig. 17. OFDM and short symbols' vulnerability to carrier frequency mismatch. The attack signal arriving after a delay δ with the correct data is used for the distance measurement and the legitimate signal is discarded as noise due to higher BER.

thresholds T_{Noise} and T_{max} with changing scenarios. A conservative choice of T_{Noise} is always better, as it would trigger the integrity checks for noise, but the receiver would not miss the legitimate signal. Similarly, T_{max} should be lower than the receiver saturation.

Carrier Frequency Offset Attack: We also analyze carrier frequency offset attack (Section III-C) using MATLAB's 5G toolbox on the 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 legitimate and attacker signal's frequency offset. All three configurations have no bit errors in the absence of an attacker. However, when the reference signals are overshadowed (attacker's signal power is 5 dB $>$ the legitimate signal) with different offset signals, the receiver's offset estimation is incorrect. Both OFDM and shortened OFDM symbols are vulnerable to offset attacks resulting in higher bit error rate (BER) (Fig 17). The attacker signal that arrives at the receiver with a 100 ns delay bears the correct data; therefore, the receiver uses this signal for distance estimation. The attack

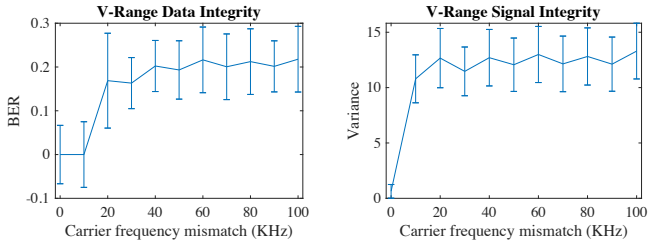

Fig. 18. The bit/symbol error increases as legitimate and attack signals arrive with different carrier frequency offset, . However, the signal integrity checker detects the signal's distortion.

TABLE IV. PRS TIME-OF-ARRIVAL MANIPULATION SUCCESS RATE.

Attack/Legitimate [dB]	**0**	**3**	**6**	**9**	**12**	**15**
$\alpha = 5\ \mu s\ (1500\ m)$	0	0.93	1	1	1	0.3
$\alpha = 15\ \mu s\ (4500\ m)$	0	0.89	1	0.99	1	0.21
$\delta = 5\ \mu s\ (1500\ m)$	0	1	1	1	1	0.11
$\delta = 15\ \mu s\ (4500\ m)$	0.01	0.9	1	1	1	0.2

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 even when the offset is small.

The attack signal should fall over the legitimate signal to prevent its detection at the receiver. The legitimate and attack signals' arrival with different carrier frequency offsets inhibits the detection of the legitimate signal (higher BER)(Fig 18). Due to the signal integrity checker, V-Range does not discard such a signal as noise but detects an increase in variance thereby exposing the attack.

E. Showcasing arrival time manipulation of PRS signals

We show PRS arrival time manipulation attack against an LTE/5G system, discussed in Section III-D, using MATLAB LTE toolbox and USRPs. To realize the PRS enabled ToA estimation, we generated a resource grid containing Primary and Secondary Synchronization signals (PSS, SSS), cell-specific reference signals, and PRS using the example provided by the MATLAB [54]. We transmit this signal using USRP at the sampling rate of 3.84 MHz, using the reference measured channel (RMC) 5 configuration. Another USRP receives the signal to acquire cell-related information, such as cell identity and ToA estimation. The attacker has all the necessary information for PRS generation and transmits the PRS signal in advance by α or delay δ duration. At the receiver, we check the reference signal received quality (RSRQ) and the cell-related data's correctness. The attack is considered successful if both RSRQ and cell data are correct and the estimated ToA matches the time offset intended by the attacker. The probability of the attack success is shown in Table IV. By symbol overshadowing attack, an attacker succeeded in distance reduction and enlargement by 1500 m (for α and δ of 5 μs) and 4500 m (15 μs) for LTE signal transmitted at the sampling rate of 3.84 MHz. Since this setup is used only for ToA estimation, we can perform testing with nearby devices. Such attacks are not possible on the V-Range symbols due to shorter effective symbol duration and integrity checks. We show that the attack can manipulate the arrival time estimation without manipulating other references or data that the receiver needs for cell detection. The probability of attack success reduces if an attacker uses very low or high transmit power, as the received signal does not fit the reference signal received quality (RSRQ) check. To position a user device at the intended location, the attacker needs to repeat this attack for all base stations in the communication range. The attack we present here achieves a very high success rate and represents the best-case scenario. In the real settings, an attacker would need to use accurate offsets for the base station signals to position the user at the intended location, as in the GPS spoofing.

VII. DISCUSSION

Compatibility 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 [55]. 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 mechanism brings a series of challenges that could result in increased false positives (noise due to packet collision) and higher latency (longer packet length, random backoff time).

UWB pulses enable short symbols and this feature heavily motivated the V-Range design. In fact, V-Range's physical layer follows the single-pulse bit sequences concept similar to the low-repetition-pulses in the 802.15.4z, but with extra checks and a verification function to detect distance enlargement attacks. Also, UWB and 5G serve entirely different purposes with different underlying architectures. Even though there are a few secure UWB-based ToF ranging systems, they are not sufficient to fulfill all upcoming use cases. 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 high-order modulation mitigates guessing attacks but receivers are susceptible to carrier-frequency offset attacks if not handled explicitly.

Practical Implications of V-Range As stated by the receiver design, V-Range's performance is limited by the channel's hardware clock inaccuracies and coherence time. Currently, V-Range uses brute-search for CFO estimation,increasing processing overhead at the receiver. However, it does not limit the ranging performance of the system. As shown in the appendix IX-D, the higher clock synchronization error can limits the maximum number of symbols we can send due to sampling rate mismatch. However, for the clock accuracy of .1 ppm (recommended for V2X scenarios), the sampling rate mismatch between the first and 20^{th} symbols is $\approx 10^{-1}$ ns, insufficient to increase ranging error.

Another aspect of using the V-Range system is carefully selecting modulation schemes, no. of symbols per ranging message, and various detection thresholds. We have found the parameters that work best for our experimental setup — some of the values like T_{Noise} may differ for each receiver. Similarly, we need to choose the number of symbols and the modulation based on the application requirements. The coherence time depends on the relative velocity of the device measuring distance. If devices are static (or move with a very low speed), we can use more symbols with high order modulation. Arbitrarily choosing the number of symbols and modulation scheme is not feasible when the devices are moving, as shown by simulations of the urban channel in Section VI-D (and appendix IX-D). Transmitting 20 symbols with 4-QAM provides performant and secure ranging systems

for use-cases supported by 5G-NR, including V2X.

Practical challenges in the deployment of V-RANGE Although V-Range provides a secure ranging technique for 5G-NR, we need infrastructure and frameworks to enable secure positioning. In order to realize V-Range implementation, we need to update the firmware of existing 5G transceivers and need infrastructure that is optimized for positioning applications. We also need to identify frameworks for key exchange, scheduling, etc.. The frameworks may differ for use-cases as they demand different positioning accuracy, latency, and security guarantees. Some architectures, like SEAL for V2X, are under discussion; the overhead of using them to enable ranging and positioning is unclear.

V-RANGE compliance with the requirements 3GPP is currently exploring physical layers designs for positioning in 5G-NR. It does not define any strict compliance requirement, except that applications targeted by 5G-NR require high accuracy and low latency. 3GPP also specifies the kind of clock inaccuracies expected for the V2X and critical infrastructure. We show that V-Range satisfies these requirements and provides configurations (modulation and no. of symbols) for the given clock inaccuracies. The V-Range is implemented by minimal changes in the transmitter design, i.e., by changing data transmitted per symbol. We are currently unaware of the total throughput requirement, spectral shape, antenna configuration that 5G-NR ranging systems must adhere to during deployment. Still, it would not limit the V-Range's ranging accuracy or security guarantees.

Practical challenges in performing ToA manipulation The difficulty of ToA manipulation can vary for different physical layer designs. Since LTE/5G uses PRS signal for the ToA estimation, distance manipulation is easier due to the predictable structure. Similarly, distance enlargement on OFDM symbols can be performed if an attacker can precisely synchronize the transmission of the attack signal. The ED/LC attack on the OFDM symbol is considered feasible, but it is not yet shown practically.

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: V-Range carefully selects V_{Noise}, SER_{Signal} and SER_{Noise} to handle the receiver's noise. Any ranging system's physical layer is susceptible to interference, and is applicable for V-Range too. The presence of an interference signal leads to denial of service, as it is hard 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.

VIII. Conclusion

We proposed V-Range, the first 5G-compatible secure ranging system resilient to distance reduction and enlargement attacks. We enumerated the challenges in realizing secure positioning in 5G and in the process identified a novel carrier-frequency offset attack that specifically affects 5G systems. V-Range can be readily deployed over existing 5G standards to achieve high precision ranging on both mm-wave and sub-6GHz frequency bands. We demonstrated that V-Range detected distance manipulation attack with a false negative rate of $\approx 10^{-5}$.

IX. Acknowledgment

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program under grant agreement No 726227. This work was partially supported by NSF grant 1850264.

References

[1] "5G - GPP 38.855 ;Technical Specification Group Radio Access Network; Study on NR positioning support," https://www.3gpp.org/ftp/Specs/archive/38_series/38.855/, [Online; Accessed 17. June 2020].

[2] "5G; study on scenarios and requirements for next generation access technologies (3gpp tr 38.913 version 14.2.0 release 14)."

[3] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 2267–2281. [Online]. Available: https://doi.org/10.1145/3319535.3339815

[4] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1527–1544. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

[5] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 931–948. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/shen

[6] "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].

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

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

[9] R. Raulefs, A. Dammann, T. Jost, M. Walter, and S. Zhang, "The 5g localization waveform," 01 2016.

[10] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," 2012.

[11] A. Ranganathan, B. Danev, A. Francillon, and S. 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*. ACM, 2012, pp. 15–26.

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

[13] ——, "The cicada attack: Degradation and denial of service in ir ranging," in *2010 IEEE International Conference on Ultra-Wideband*, 2010, pp. 1–4.

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

[15] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[16] M. Singh, P. Leu, A. Abdou, and S. Capkun, "Uwb-ed: Distance enlargement attack detection in ultra-wideband," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 73–88. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/singh

[17] 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*, vol. 18, no. 2, pp. 257–260, 2014.

[18] S. Čapkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *IEEE Computer and Communications Societies.*, vol. 3, 2005, pp. 1917–1928.

[19] 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].

[20] "LTE Positioning Protocol (LPP)," https://www.etsi.org/deliver/etsi_ts/136300_136399/136355/13.00.00_60, [Online; Accessed 12. January 2021].

[21] 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*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[22] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5G mmwave positioning for vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, Dec 2017.

[23] S. Dwivedi, R. Shreevastav, F. Munier, J. Nygren, I. Siomina, Y. Lyazidi, D. Shrestha, G. Lindmark, P. Ernström, E. Stare, S. M. Razavi, S. Muruganathan, G. Masini, Åke Busin, and F. Gunnarsson, "Positioning in 5g networks," 2021.

[24] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *IEEE INFOCOM*, vol. 2, 2000, pp. 775–784.

[25] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *USENIX NSDI*, 2016, pp. 165–178. [Online]. Available: https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/vasisht

[26] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. 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*, ser. ESAS'06. Springer, 2006, pp. 83–97. [Online]. Available: http://dx.doi.org/10.1007/11964254_9

[27] B. Kempke, P. Pannuto, and P. Dutta, "Surepoint: Exploiting ultra wideband flooding and diversity to provide robust, scalable, high-fidelity indoor localization," in *ACM SenSys*, 2016, pp. 318–319.

[28] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Network and Distributed System Security Symposium (NDSS)*, 2011.

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

[30] "Relay Setup," https://www.thesun.co.uk/motors/7804489/keyless-car-100-ebay-gadgets-relay-attacks/, [Online; Accessed 1. Feb 2021].

[31] M. Singh, P. Leu, and S. 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.

[32] 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)*, 2006, pp. 15 pp.–294.

[33] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing," in *USENIX Security Symposium*, 2011.

[34] "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].

[35] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[36] K. B. Rasmussen, S. Capkun, and M. Cagalj, "Secnav: secure broadcast localization and time synchronization in wireless networks," in *MobiCom*, 2007.

[37] A. A. Nasir, S. Durrani, H. Mehrpouyan, S. D. Blostein, and R. A. Kennedy, "Timing and carrier synchronization in wireless communication systems: A survey and classification of research in the last five years," *CoRR*, vol. abs/1507.02032, 2015. [Online]. Available: http://arxiv.org/abs/1507.02032

[38] "802.15.4z Task Group," http://www.ieee802.org/15/pub/TG4z.html, [Online; Accessed 17. June 2020].

[39] 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)*, 2012, pp. 1–8.

[40] Y. Qi, M. Hunukumbure, H. Nam, H. Yoo, and S. Amuru, "On the phase tracking reference signal (PT-RS) design for 5g new radio (NR)," *CoRR*, vol. abs/1807.07336, 2018. [Online]. Available: http://arxiv.org/abs/1807.07336

[41] X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlen *et al.*, "5g new radio: Unveiling the essentials of the next generation wireless access technology," *arXiv preprint arXiv:1806.06898*, 2018.

[42] Qualcomm, "Snapdragon 800 Processor," https://www.qualcomm.com/products/snapdragon-processors-800, [Online; Accessed 30. October 2020].

[43] "srsLTE," https://github.com/srsLTE/srsLTE, [Online; Accessed 12. December 2020].

[44] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Čapkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 500–516.

[45] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," 03 2019.

[46] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.

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

[48] 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*, vol. 65, no. 12, pp. 6521–6533, Dec 2017.

[49] S. Ahmadi, "Toward 5 g xilinx solutions and enablers for next-generation wireless systems," 2016.

[50] "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].

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

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

[53] "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].

[54] "MATLAB PRS," https://www.mathworks.com/help/lte/ug/time-difference-of-arrival-positioning-using-prs.html, [Online; Accessed 12. December 2020].

[55] "802.11az," http://www.ieee802.org/11/Reports/tgaz_update.htm, [Online; Accessed 24. September 2019].

[56] 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)*, Sep. 2012, pp. 2281–2286.

APPENDIX

TABLE V. PARAMETERS AND VARIABLES

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
$s_i(t)$	t^{th} sample of i^{th} OFDM symbol

A. 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 Fig 20, an attacker can send a late commit signal to achieve an advancement of $\alpha = 3$ samples, which translates to 9 m distance reduction for the system bandwidth of 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 $t = [1 \quad \hat{N} - \alpha - 1]$ 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 Fig 19. 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.

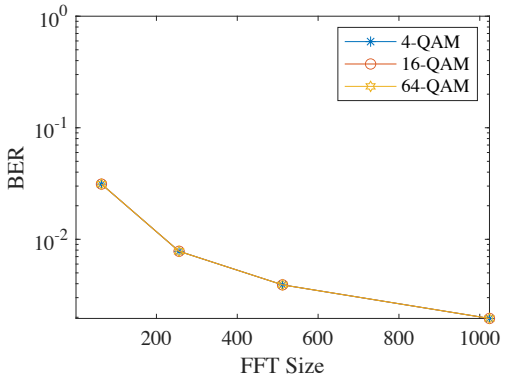

Fig. 19. Bit error when attacker perform late commit attack on the V-Range OFDM symbol, and attack signal is procesed by FFT-based receiver.

B. Signal Integrity Check

Suppose ranging data is not pre-shared between entities, as in some classes of distance bounding protocols. Consequently, the receiver needs to perform the signal-integrity check without any knowledge of the expected data sequence. The attacker can check messages' integrity using the maximum number of

$S_k = Sort(Power(S_k))$;
$B = \{S_k(1)\}$;
$NumBins = 1$;
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

TABLE VI. THE PROBABILITY OF ANNIHILATION AND OVERSHADOWING ATTACK DETECTION USING INTEGRITY-CHECK WITHOUT PRE-SHARED DATA.

	Annihilation			Overshadowing		
SNR [dB]	**4**	**6**	**8**	**4**	**6**	**8**
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

power levels expected (e.g., three power levels in 16-QAM). 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}. For example, by using algorithm 1, which optimize the number of bins, where the variance of each bin should be less than V_{Noise}

As shown in Table VI, the attack detection probability of this approach is similar to the approach with pre-shared data for 4-QAM and 16-QAM (4-QAM has only one power level). 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.

C. Data Detection

The use of reference signals for frequency 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 frequency offset effect manifests itself in a rotation of the constellation diagram, as shown in Fig 21a. 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

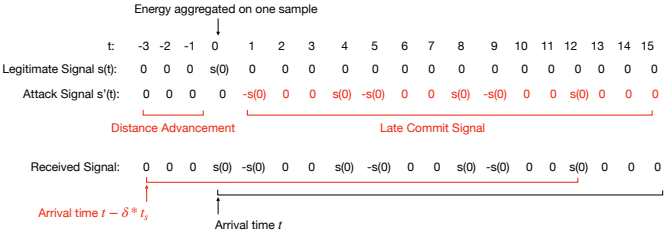

Fig. 20. An example of the ED/LC attack on the V-Range symbol when a receiver performs FFT for data detection.

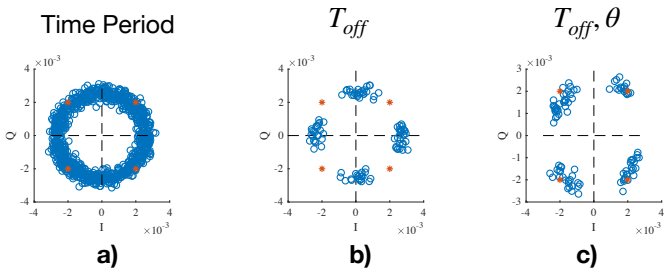

Fig. 21. The residual frequency creates imbalance in the in-phase and quadrature components of the signal.

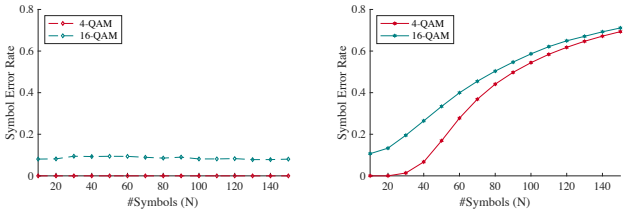

Fig. 22. a) By correcting both frequency and phase offset, the device can exchange more symbols for ranging

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 has a relative rotation of less than a certain ϵ, no exhaustive search for the frequency offset is needed. Fig 21b shows the constellation representation of the symbols transmitted in time T_{off}. The length $T_{off} = \epsilon/(2\pi\Delta_{max})$, where Δ_{max} is maximum frequency offset between the devices and ϵ is acceptable relative rotation. As Fig 21c shows, the correct phase offset (θ) yields the correct symbols. The value of ϵ and θ depends on the modulation scheme and results in the different symbol error rates [56].

The range to exhaustively search depends on the clock error and modulation scheme, respectively. As shown in Fig 22a, 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 $8\,\mathrm{dB}$; 16-QAM exhibits a higher symbol error than 4-QAM, as it has more constellation points. As Fig 22 the phase offset correction is compulsory for data detection, but frequency offset correction can be made redundant when using only a few symbols and a (very) accurate clocks, such as those specified for 5G-based vehicular networks and critical systems).

D. Ranging Duration

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, offset 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 manipulate the distance. If the optimization technique addresses this challenge by limiting the symbol duration and the ranging duration, the offset is minimized. The offset is higher in the mm-wave (i.e., higher center frequency), so the value of ϵ increases faster. However, it

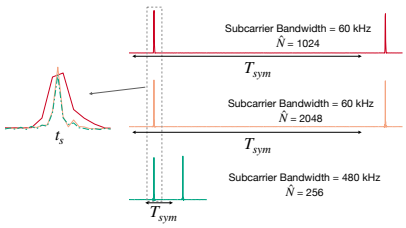

Fig. 23. Special OFDM ranging symbols for different subcarrier configurations. Second and third instantiation have higher system bandwidth and thus the lobe is shorter. For the shorter symbols (second and third form above), a multi-path component can be seen.

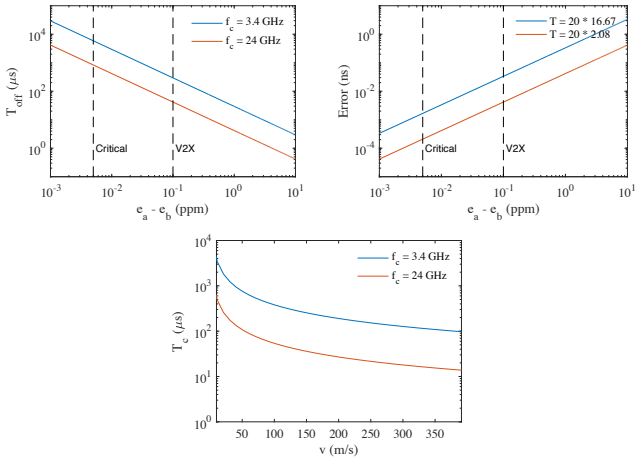

Fig. 24. The total length of the signal recoverable at the receiver for the secure distance measurements depends on the hardware capabilities (frequency offset) and channel conditions (coherence time)

is compensated by the shorter symbol durationT_{Sym}, as shown in Fig 24a.

The frequency offset also leads to the sampling rate mismatch between devices, which can translate into bit error as well as distance manipulation. However, the mismatch between the first and the last symbol should be more than $t_s/2$ to have any considerable effect. As shown in Fig 24b, the mismatch in the first and last sample of 20 symbols is less than 10^{-2} ns for the clock accuracy of .01 ppm (critical).

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. Fig 24c show coherence time for different velocity. It is important to send V-Range symbols within coherence time to check physical layer integrity, i.e., detect distance enlargement attacks using variance check. Thus, the V-Range slot duration should be bounded by clock offset inaccuracies and available channel conditions (coherence time).