Quantum-secured covert sensing for the Doppler effect

Shuhong Hao[1] and Zheshen Zhang[2,*]

[1]*Department of Materials Science and Engineering, University of Arizona, Tucson, Arizona 85721, USA*
[2]*Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, Michigan 48109, USA*

(Received 2 August 2023; accepted 9 October 2023; published 5 December 2023)

Quantum mechanics has paved the way for establishing shared privacy among communicating parties through a secure regime known as quantum-secured communication. Recent advancements in both theory and experimentation have unveiled the potential of quantum resources in enhancing the performance and security of estimating unknown parameters. This has led to the emergence of a novel paradigm known as quantum-secured covert sensing, wherein the sensing operation is concealed from an adversary monitoring the environment by embedding the probe signal in a bright noise background. The performance and security of such protocols are quantified using quantum measurement theory. While previous investigations into quantum-secured covert sensing primarily focused on proof-of-concept phase estimation problems, this paper presents a pioneering quantum-secured covert sensing system designed for the Doppler effect—a versatile estimation problem with broad applications. Our research uncovers an inherent trade-off among measurement precision, security, and range within the system. This work establishes a new avenue for incorporating physical-layer security into sensing systems, thereby opening up exciting possibilities for future research in this field.

DOI: 10.1103/PhysRevResearch.5.043206

I. INTRODUCTION

Quantum cryptography utilizes the unique properties of quantum systems to ensure the utmost security, privacy, and integrity of processed data. Among various quantum cryptographic techniques, quantum key distribution (QKD) is arguably the most well-developed paradigm to create a significant impact on secure communication [1–4]. By leveraging the principles of the quantum no-cloning theorem [5], QKD enables the establishment of shared private keys between communicating parties. When combined with one-time pad encryption, QKD offers a communication security framework that relies on the fundamental laws of physics rather than assumptions about mathematical complexity. In recent years, QKD has experienced substantial growth, transitioning from proof-of-concept experiments in controlled laboratory environments [6–10] to practical field tests conducted between quantum communication satellites and ground stations [2,3,11]. The remarkable progress of QKD underscores the potential of quantum cryptography and underscores the need to explore protocols that go beyond mere key distribution [12–15]. As the field continues to advance, researchers are increasingly compelled to investigate additional aspects of quantum cryptography beyond key distribution. This exploration will uncover new possibilities and applications, further enhancing the capabilities and impact of quantum cryptography.

In the past decade, quantum-secured covertness has emerged as a new paradigm in quantum cryptography, extending beyond the realm of QKD [16–21]. This paradigm involves concealing the quantum signal within background noise, rendering the execution of quantum-secured covert protocols undetectable from the perspective of an adversary, referred to as Willie, thereby safeguarding the security and integrity of data. The concept of quantum-secured covertness was initially proposed [21,22] and demonstrated [16] in the context of transferring classical bits over a noisy channel. The analysis of quantum-secured covert communication protocols employs quantum measurement theory, revealing a trade-off between performance and security quantified by the square-root law.

In recent years, quantum-secured covertness has been extended to the domain of sensing, resulting in a multitude of proposed protocols [18,20,23] and an experimental implementation [24]. In these protocols, a transmitter generates a probe that is either classically correlated or entangled with a reference. This probe is then sent into a noisy and lossy environment where an object of interest resides, while the reference is retained locally. At the receiver, a joint measurement is performed on the probe returning from the environment and the locally retained reference, allowing for the extraction of the object's property. Due to the presence of intense background noise, Willie is unable to detect the sensing attempt, quantified by the probability of detection derived from quantum measurement theory. Similar to quantum-secured covert communication, quantum-secured covert sensing is bound by the squared-root law, which imposes a fundamental trade-off between the achievable performance and security. A

[*] zszh@umich.edu

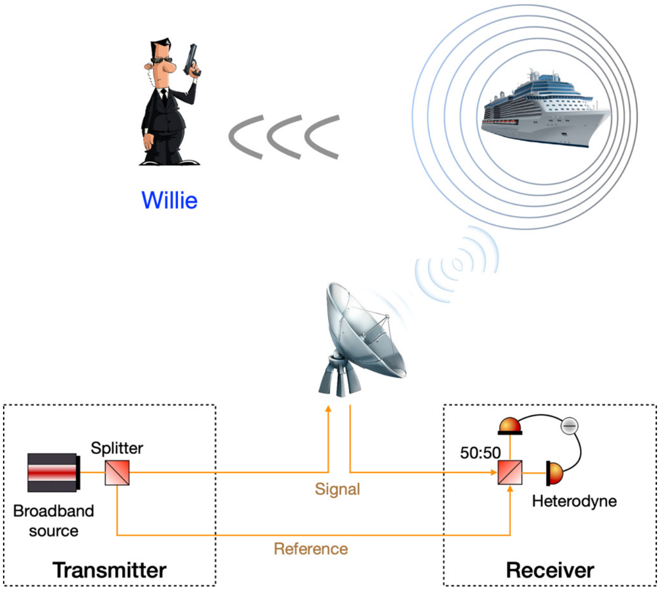

FIG. 1. Configuration for Doppler shift covert sensing. Transmitter generates a broadband signal and the associated reference and sends the signal to probe a moving object. The receiver performs a heterodyne measurement on the signal returned from a lossy and noisy environment. Willie captures photons not collected by the receiver and takes the optimal quantum measurement to detect the sensing operation.

recent proof-of-concept experiment on entanglement-enhanced covert sensing [24] demonstrated the capability of estimating a phase shift induced by the object, while effectively restricting Willie's detection probability within bounds defined by the protocol.

This study delves beyond the conventional phase-estimation problem and presents an experimental investigation into quantum-secured covert sensing of frequency shift—an aspect closely linked to velocity measurement through the Doppler effect. We explore the relationship between measurement precision, covertness, and various environmental parameters. Our findings reveal an inherent trade-off among measurement precision, range, and security. By shedding light on these intricate dynamics, our research paves the way for quantum cryptography to make a tangible impact on real-world applications such as target detection [25–27], object tracking [28–30], secure satellite navigation [31–33], and remote sensing [34–36]. This work opens up a new avenue for leveraging the power of quantum cryptography in addressing practical challenges in these domains.

II. COVERT-SENSING PROTOCOL

The quantum-secured covert velocity sensing protocol is illustrated in Fig. 1. The transmitter divides the output of a broadband source with the carrier angular frequency ω_c into two arms, each consisting of M temporal modes

$$\begin{aligned}\hat{a}_m &= \sqrt{\eta}\hat{s}_m + \sqrt{1-\eta}\hat{v}_m,\\ \hat{r}_m &= \sqrt{1-\eta}\hat{s}_m - \sqrt{\eta}\hat{v}_m,\end{aligned} \tag{1}$$

where $m \in \{1,\dots,M\}$, and $\hat{a}_m$, $\hat{r}_m$, $\hat{s}_m$, and $\hat{v}_m$ are the annihilation operators for the probe signal, reference retained at the sensor, broadband source, and vacuum modes, respectively. The parameter η is chosen to control the mean photon number $N_S \equiv \langle \hat{a}_m^\dagger \hat{a}_m\rangle$ of each signal mode. To operate covertly, it requires $N_S \ll 1$ to conceal the signal within the noise background. In the Schrödinger picture, the quantum state of each signal mode is described by the density operator $\hat{\rho}_{a_m}$. The transmitter emits the signal state, $\hat{\boldsymbol{\rho}}_S \equiv \hat{\rho}_{a_1} \otimes \hat{\rho}_{a_2} \dots \otimes \hat{\rho}_{a_M}$ to interrogate a moving object.

Due to the Doppler effect, a frequency shift of

$$\Delta\omega = \frac{2v}{c}\omega_c \tag{2}$$

is induced on all signal modes. Here, v represents the velocity of the target relative to the observer and c is the speed of light. The Doppler effect transforms the initial signal modes as follows:

$$\hat{a}_m \to \hat{a}'_m = e^{i\Delta\omega t_m}\hat{a}_m, \tag{3}$$

where t_m is the time associated with the mth temporal mode.

The environment where the target resides is characterized by the transmission efficiency κ_S between the transmitter and receiver for the signal and a noise background. The probe signal modes at the receiver, represented by $\hat{b}_m$, can then be derived as follows:

$$\hat{b}_m = \sqrt{\kappa_S}\hat{a}'_m + \sqrt{1-\kappa_S}\hat{n}_m, \tag{4}$$

where $\hat{n}_m$ represents the environmental background thermal modes with on average $\langle \hat{n}_m^\dagger \hat{n}_m\rangle = N_B/(1-\kappa_S)$ photons per mode.

The receiver performs a heterodyne detection using a reference with angular frequency ω_c on the returned probe to estimate the frequency shift $\Delta\omega$. In the Schrödinger picture, the signal and reference states at the receiver, denoted as $\hat{\boldsymbol{\rho}}'_S(v) \equiv \hat{\rho}_{b_1} \otimes \hat{\rho}_{b_2} \dots \otimes \hat{\rho}_{b_M} \otimes \hat{\rho}_{r_1} \otimes \hat{\rho}_{r_2} \dots \otimes \hat{\rho}_{r_M}$, are dependent on the velocity of the interrogated object. The performance of the measurement in estimating v can be quantified within the framework of the quantum Fisher information (QFI) derived as [37]

$$\mathcal{J}_v = 8 \times \lim_{v\to 0} \frac{1-\sqrt{\mathcal{F}[\hat{\boldsymbol{\rho}}'_S(v), \hat{\boldsymbol{\rho}}'_S(v+dv)]}}{dv^2}, \tag{5}$$

where the Uhlmann fidelity between two quantum states is defined as $\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2) = (\mathrm{tr}\sqrt{\sqrt{\hat{\rho}_1}\hat{\rho}_2\sqrt{\hat{\rho}_1}})^2$. Subsequently, a lower bound on the measurement sensitivity, applicable to any quantum measurement performed on $\hat{\boldsymbol{\rho}}'_S(v)$, can be obtained from the quantum Cramér-Rao bound (QCRB) as follows:

$$(\Delta v)^2 \geqslant \frac{1}{\mathcal{J}_v}. \tag{6}$$

To assess the covertness of the protocol, we consider an adversary named Willie, who is capable of capturing photons that are not collected by the receiver, in an attempt to infer the sensing operation. In the absence of the probe signal, Willie's quantum state, comprising M modes, is described as

$$\hat{w}_m^{(0)} = \sqrt{\kappa_W}\hat{v}'_m + \sqrt{1-\kappa_W}\hat{n}'_m, \tag{7}$$

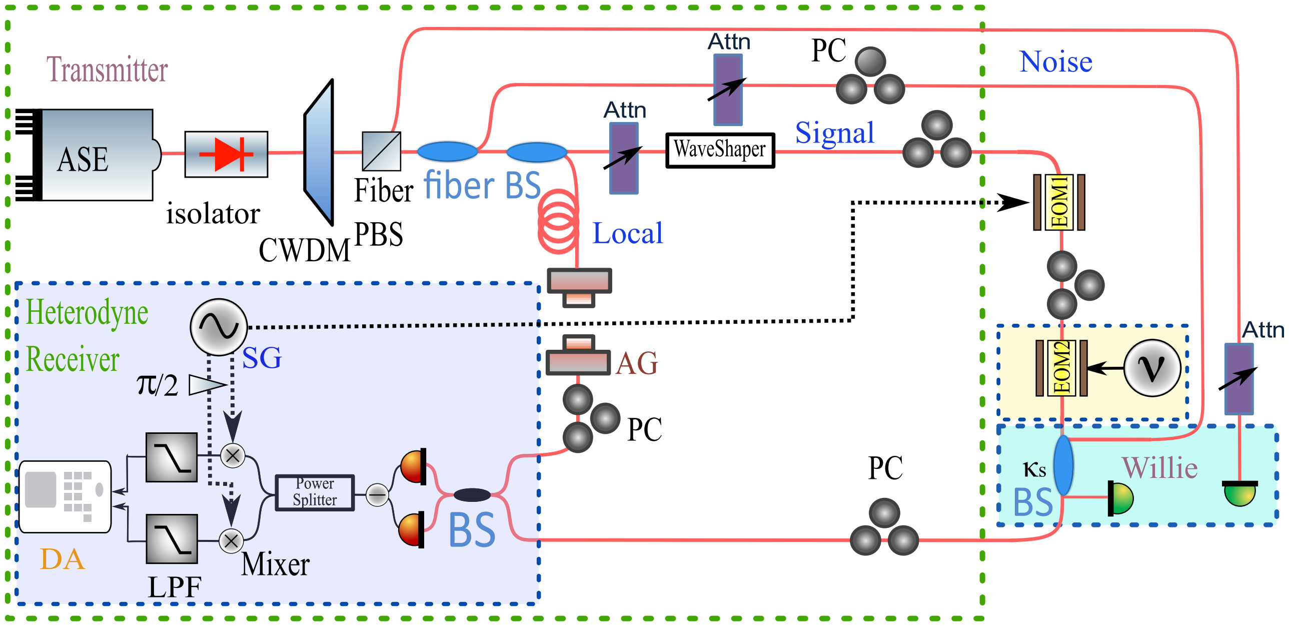

FIG. 2. Experimental setup. The transmitter is equipped with an amplified spontaneous emission (ASE) source that generates a broadband probe signal and a reference. A Doppler shift on the probe signal is introduced via phase modulation using an electrooptic modulator (EOM). The receiver comprises an air gap (AG) to fine-tune the propagation delay between the probe signal and the reference, followed by a balanced heterodyne detector that acquires the two quadratures of the returned probe signal measured by two photodiodes operating in a balanced setting. Other experimental components include a coarse wavelength-division multiplexer (CWDM), a polarizing beam splitter (PBS), optical attenuators (Attn), beam splitters (BS), a signal generator (SG), polarization controllers (PC), low-pass filters (LPF), and data acquisition (DA).

where $\hat{n}'_m$ represents the environmental modes from Willie's perspective, each with $N'_B/(1-\kappa_W)$ photons, and $\hat{v}'_m$ represents vacuum modes. Thus, in the Schrödinger picture, Willie's quantum state $\hat{\rho}_W^{(0)} \equiv \hat{\rho}_{w_1}^{(0)}, \rho_{w_2}^{(0)}, \ldots, \rho_{w_M}^{(0)}$ is a set of thermal states, each with a mean photon number N'_B. In the presence of the probe signal, Willie's quantum state becomes a mixture of a small portion of the probe and the background noise, formulated as

$$\hat{w}_m^{(1)} = \sqrt{\kappa_W}\,\hat{a}'_m + \sqrt{1-\kappa_W}\,\hat{n}'_m, \tag{8}$$

with the Schrödinger picture representation of $\hat{\rho}_W^{(1)} \equiv \hat{\rho}_{w_1}^{(1)}, \rho_{w_2}^{(1)}, \ldots, \rho_{w_M}^{(1)}$. Consequently, the presence of the probe signal increases Willie's collected mean photon number by $\kappa_W N_S$ per mode.

To detect the sensing operation, Willie endeavors to discriminate between $\hat{\rho}_W^{(0)}$ and $\hat{\rho}_W^{(1)}$. Regardless of Willie's measurement, his detection error probability is bounded by

$$\mathbb{P}_e \geqslant \tfrac{1}{2}\left(1 - \tfrac{1}{2}\big\|\hat{\rho}_W^{(0)} - \hat{\rho}_W^{(1)}\big\|_1\right) \geqslant \tfrac{1}{2} - \epsilon, \tag{9}$$

where $\|\cdot\|_1$ denotes the trace distance and ϵ is defined as the covertness parameter. In the protocol, ϵ can be controlled by choosing appropriate values for N_S and M, subject to a security-performance trade-off as detailed in Sec. IV C. By setting $\kappa_W = 1 - \kappa_S$, Willie is granted full power in detecting the sensing operation by capturing all the signal photons that do not arrive at the receiver. Within the operational parameter range of the protocol, i.e., $N_S \ll 1$, $N_B \gg 1$ and $M \gg 1$, Willie's detection error probability is found to be [24]

$$\epsilon = \frac{\sqrt{M}(1-\kappa_S)^2 N_S}{4\kappa_S N_B} \propto \frac{\sqrt{M} N_S}{N_B}. \tag{10}$$

III. EXPERIMENT

Our experimental setup is sketched in Fig. 2. The output from a thermal-light source based on amplified spontaneous emission (ASE) is passed through a flat-top 16-nm optical filter centered at 1550 nm, defining the optical bandwidth $W \sim 2$ THz for the signal and reference. To ensure single-polarization light, a polarizer is employed to pass one polarization and filter out the other. The single-polarization light is then split by a 99:1 unbalanced fiber coupler (FC). The output at the 1% port serves as the probe signal, containing $N_S \ll 1$ photons per mode, while the light at the 99% port serves as the reference, with $N_R \gg 1$ photons per mode. A tunable fiber attenuator is used to further adjust the signal power to the desired level, according to the experimental conditions. To compensate for the disparity in dispersion between the signal and reference, a waveshaper (Finisar 1000A) is programed to apply wavelength-dependent phase shifts on the signal. For the heterodyne measurement, a frequency offset between the reference and the signal is created by phase modulating the signal with an electro-optic modulator (EOM1), driven by a 20-MHz sawtooth voltage from a signal generator (SG).

The Doppler effect introduces a frequency shift on the signal. In our experiment, EOM2 applies two phases, ϕ_1 and ϕ_2, separated by an interval $T = t_{m+1} - t_m$. The differential phase $\delta\phi = \phi_2 - \phi_1$ results in an effective frequency shift of $\Delta\omega = \delta\phi/T$ on the signal.

The covertness of the protocol relies on concealing the signal within a bright noise background. In our experiment, we create the noisy environment by mixing ASE noise with the same optical bandwidth as the signal. To control the magnitude of the environmental noise, a variable attenuator is applied to the ASE noise. We ensure that the polarization of the injected ASE noise aligns with that of the signal using a polarization controller (PC), making it indistinguishable from the signal in terms of polarization. Prior to the heterodyne detection at the receiver, we finely adjust the propagation delay of the reference using an air gap (AG) and perform polarization tuning to match it with the signal returned from the object. This step is crucial to ensure efficient interference between the reference and the returned signal.

Next, a 50:50 beam splitter (BS) mixes the reference and the signal, and its two output ports direct the combined signal to a balanced detector (Thorlabs PDB450C) with 80% quantum efficiency. The amplified voltage signal for the difference photocurrent of the two diodes is split into two arms, each equipped with a radio-frequency (RF) mixer. The RF local oscillators (LOs) for the two mixers are generated from the same SG that drives EOM1. We set the phases of the RF LOs to differ by $\pi/2$, enabling simultaneous measurement of both quadratures of the returned probe signal. The intermediate frequency (IF) voltage signals are then filtered by two low-pass filters (LPF) before undergoing data acquisition on a real-time oscilloscope. Subsequent postprocessing is performed to infer the frequency shift due to the Doppler effect and thereby determine the velocity of the object.

At Willie's terminal, he employs an FC with transmissivity $1-\kappa_S$ to capture a portion of the noisy signal. He uses a photodiode to measure the intensity difference of the tapped light, which allows him to infer the absence or presence of the probe signal. Additionally, Willie also measures the intensity of the ASE light from the source on the polarization orthogonal to the signal, enabling him to estimate and eliminate the source's technical intensity noise at low frequencies. By subtracting off the technical noise in postprocessing, Willie's measurement performance is solely limited by the intrinsic uncertainties of the quantum states.

IV. RESULTS

A. Sensing performance

We first demonstrate the system's ability to estimate the velocity of an object. To achieve this, we drive EOM2 with a square wave at 207 kHz. The voltages at the two output ports of the heterodyne detector carry information about the two quadratures of the measured optical field of the returned probe signal. Each voltage signal is filtered by a low-pass filter (LPF) with a 310-kHz cutoff frequency and then recorded by an oscilloscope at a sampling rate of 10×10^6 Sa/s. The applied differential phase shift $\delta\phi$ results in a pair of quadrature measurement data $\{V_{Q_1}, V_{P_1}\}$ and $\{V_{Q_2}, V_{P_2}\}$. The estimated differential phase shift is obtained as follows:

$$\widetilde{\delta\phi} = \arctan\left(\frac{V_{P_2}}{V_{Q_2}}\right) - \arctan\left(\frac{V_{P_1}}{V_{Q_1}}\right). \tag{11}$$

Subsequently, the emulated and estimated object velocity associated with the differential phase shift is derived as follows:

$$v = \frac{c}{2\omega_c}\frac{\delta\phi}{T}, \quad \tilde{v} = \frac{c}{2\omega_c}\frac{\widetilde{\delta\phi}}{T}. \tag{12}$$

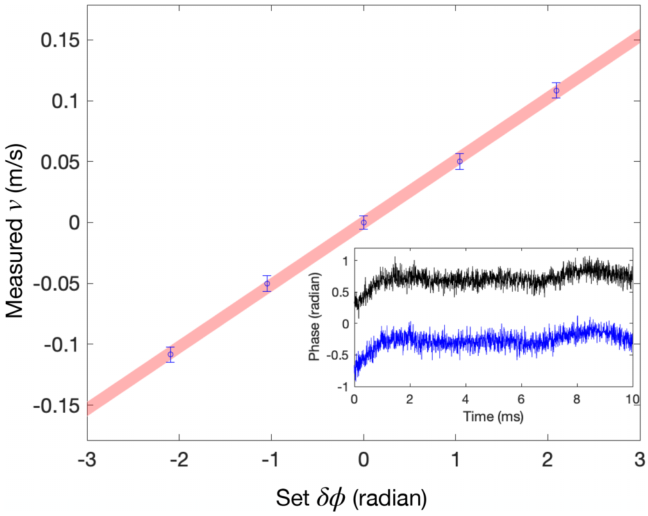

FIG. 3. Estimated velocity with respect to the applied differential phase $\delta\phi = \phi_2 - \phi_1$. The red area marks the theoretical root-mean-square error. Error bars obtained from 2000 measurements. The operational parameters are set to $\kappa_S N_S = 0.078$ and $N_B = 2495$. $M = 4.83 \times 10^6$. The inset displays a continuous-time measurement of fixed ϕ_1 (blue) and ϕ_2 (black) over 10 ms, showing robustness in $\delta\phi = \phi_1 - \phi_2$, even though the absolute phases drift due to thermal fluctuations and other imperfections.

The mean squared error (MSE) of the velocity estimation is then given by

$$(\Delta v)^2 = \langle(\tilde{v} - v)^2\rangle. \tag{13}$$

Figure 3 plots the estimated velocity as a function of the phase shift, demonstrating strong linearity within the full range of $\delta\phi \in [-\pi, \pi)$. The theoretical root-mean-squared (RMS) error, Δv, is represented by the red shaded area and the experimentally measured RMS values are depicted in the error bars, indicating excellent agreement. Despite not implementing phase locking in the experiment, the differential phase estimation exhibits robustness against the drift in the relative phase between the signal and reference, as long as the estimation is performed at a much higher rate than such a drift. This robustness is illustrated in the inset of Fig. 3, showing a strong correlation between ϕ_1 and ϕ_2 even though they both drift over time due to thermal fluctuations and other imperfections.

B. Covertness

Willie's error probability in detecting the sensing operation serves as a critical performance metric for the covert sensing protocol. For the task of discriminating the probe signal from its embedded bright noise background, Willie's optimal quantum measurement is direct photon counting. This is due to both the signal and noise following thermal statistics, characterized by a diagonal photon-number distribution in the Fock basis. To experimentally measure the error probability as a function of the transmission efficiency between the transmitter and the receiver, we fix the signal and background noise brightness N_S and $N_B/(1-\kappa_S)$. With operating conditions of $N_S \ll 1$ and $N_B \gg 1$, we derive Willie's detection error

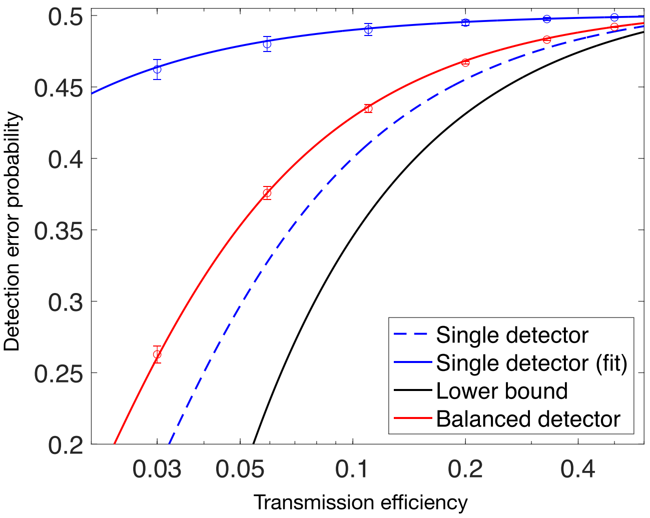

FIG. 4. Willie's detection error probability with respect to signal transmission efficiency in the single-detector scheme (blue) and the balanced-detection scheme (red). Blue dashed curve: Theory for an ideal single-detector scheme without being affected by low-frequency noise from the source. Blue solid curve: Fitted theoretical model for experimental data acquired with a single detector. Red curve: Fitted theoretical model for experimental data acquired with a balanced-detection scheme. Black curve: A lower bound for Willie's error probability. Integration time $T = 2.42$ µs. The single-detector scheme uses a photodiode (Thorlabs FGA01FC) and a current amplifier (Femto DLPCA-200), while the balanced-detection scheme employs two photodiodes (Thorlabs PDB450C) to measure the difference photocurrent.

probability as follows [24]:

$$P_e = \frac{1}{2}\text{erfc}\left[\sqrt{M/12\gamma}\,\frac{P_S}{P_B}\right], \tag{14}$$

where $P_S/P_B = (1-\kappa_S)^2 N_S/\kappa_S N_B$ represents Willie's signal-to-noise ratio and γ is a fitting parameter accounting for suboptimality due to experimental imperfections. For an ideal ASE source without technical noise, direct photon counting using a single detector achieves $\gamma = 1$. In our experiment, we find that $\gamma = 100$ provides a good fit to Willie's detection error probability data acquired with a single detector. With a balanced detection scheme, γ reduces to 2, indicating the removal of technical noise due to low-frequency intensity fluctuations, albeit at the cost of doubling the number of noise modes.

In the experiment, we set the power levels of the probe signal and noise background at 40 nW and 1.28 mW, respectively, resulting in $N_S = 0.156$ and $N_B/(1-\kappa_S) = 4990$. We vary κ_S over 0.030, 0.059, 0.11, 0.20, 0.33, and 0.50 to test Willie's detection error probability at different transmission efficiencies. We first turn off the probe signal and utilize Willie's photodetector to measure the intensity of the light tapped from his FC. The output voltage of the photodetector is filtered by an LPF with a bandwidth of 310 kHz and sampled by an oscilloscope at a rate of $1/T = 414$ kHz, yielding $M = WT = 4.83 \times 10^6$ modes. The same measurement is repeated with the probe signal on. By setting a decision threshold, we can readily derive Willie's detection error probability for different values of transmission efficiency. The experimental data, depicted in Fig. 4, align well with the fitted theoretical model. For comparison, we also plot the projected detection error probability for an ideal ASE source (blue dashed curve) and a lower bound for the detection error probability (solid black curve).

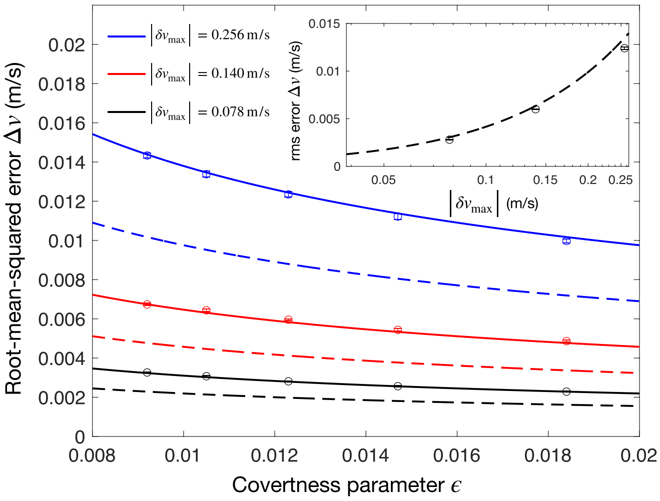

FIG. 5. RMS error of velocity estimation as a function of the covertness parameter ϵ at different $|\delta v_{\max}|$. In the experiment, we set $\kappa_S = 0.5$, $N_S = 0.11$ (27 nW) for $T = 1.52$ µs and $|\delta v_{\max}| = 0.256$ m/s; $N_S = 0.078$ (20 nW) for $T = 2.78$ µs and $|\delta v_{\max}| = 0.140$ m/s; and $N_S = 0.058$ (14.9 nW) for $T = 5$ µs and $|\delta v_{\max}| = 0.078$ m/s. N_B is set to 2497, 2185, 1873, 1561, 1248 for the five ϵ values. Inset shows the RMS error of velocity estimation as a function of $|\delta v_{\max}|$ at $\epsilon = 0.012$. Dashed lines: QCRB, which is saturated by the dual-homodyne detection in the large noise limit (see the Appendix).

C. Performance-security trade-off

Similar to other covert sensing and communication protocols [16,17,19,24,38], our present protocol is subject to a performance-security trade-off. Specifically, the differential phase shift $\delta\phi$ between two consecutive phase measurements, ϕ_1 and ϕ_2, must lie within the range $[-\pi, \pi)$ to ensure an unambiguous estimation. This constraint limits the range of velocity estimation to $|\delta v_{\max}| = \pi c/2\omega_c T$. A higher $|\delta v_{\max}|$ requires a shorter T, leading to a reduced number of measured modes M. However, to maintain a constant security level quantified by ϵ, $\sqrt{M}N_S$ must remain constant, as shown in Eq. (10). Consequently, the signal-to-noise ratio MN_S/N_B decreases as the range for velocity estimation increases, resulting in higher RMS errors, as illustrated in the inset of Fig. 5.

To further analyze the performance-security trade-off, we fix $|\delta v_{\max}|$ and examine the RMS error for velocity estimation as a function of the covertness parameter ϵ at different background noise levels. The data are plotted in Fig. 5, revealing the trade-off between the security level (lower ϵ) and the precision of velocity estimation (lower RMS error).

The inset in Fig. 5 depicts the RMS error of velocity estimation as a function of $|\delta v_{\max}|$ at a fixed $\epsilon = 0.012$. The dashed lines represent the QCRB, which is saturated by the dual-homodyne detection in the large noise limit (see the Appendix). The main plot shows the RMS error of velocity estimation as a function of ϵ for different values of $|\delta v_{\max}|$. The data points correspond to different experimental parameters, demonstrating the trade-off between security and precision in the covert-sensing protocol.

V. DISCUSSION

The present proof-of-concept quantum-secured covert sensing for the Doppler effect is conducted in the optical domain within the telecommunication band centered at 1550 nm (193 THz). At this wavelength, the ambient thermal noise due to blackbody radiation is exceptionally weak, and thus, in the experiment, ASE light is injected to emulate the environmental noise background. However, in practical applications, strong optical thermal light may arise from active jamming or intense sunlight during the daytime. On the other hand, background noise due to blackbody radiation becomes much more prominent in the microwave wavelength regime. For instance, at $\omega_c = 2\pi \times 100$ GHz in the W band, one can estimate $N_B \sim 60$ at room temperature [39]. By reducing N_S while keeping ϵ constant, one can move into the covert sensing parameter region in the microwave domain. Doing so would substantially broaden $|v_{\max}|$, as Eq. (12) indicates. Specifically, with a ~2000 times reduction in the carrier frequency, $|v_{\max}|$ would be extended to >500 km/hour, calculated based on the parameters used in Fig. 5. However, there is a trade-off as this would increase the interrogation time due to the lower density of spectral modes in the microwave frequencies. Assuming $W = 2$ GHz, the velocity estimation down to the same precision would take 1.5 ms to 5 ms, in contrast to the microsecond interrogation time in the optical domain. Nonetheless, the relative precision, defined as $\Delta v/|\delta v_{\max}|$, would remain independent of the carrier frequency given the interrogation time.

In the experiment, the demodulation frequency at the heterodyne detector matches the frequency shift applied by EOM1 to the probe signal. However, with prior knowledge of the object's velocity, one could employ a different demodulation frequency with an offset δf from the signal. By doing so, the velocity estimation can be carried out in the vicinity of $\lambda_c \delta f/2$, where λ_c is the carrier wavelength. Such a technique would effectively increase the range of velocity estimation if prior knowledge is available.

The attenuation on the probe signal due to environmental loss affects both the sensing performance and security. On the one hand, both the QFI and the classical Fisher information for homodyne measurements scale linearly with the transmissivity between the transmitter and the receiver, as shown in Eqs. (A1) and (A2). A reduced tranmissivity would lift the curves presented in Fig. 5. On the other hand, Willie's detection error probability drops as the transmissivity decreases as he collects more signal photons to facilitate the detection of the sensing attempt, as Fig. 4 illustrates. To offset the performance and security degradation caused by a more lossy environment, one can increase the number of signal modes while reducing the mean photon number per mode, subject to a fundamental performance-security tradeoff quantified by the square-root law [16,24].

To further enhance the present protocol, entanglement has been shown to boost the performance of covert sensing, as demonstrated in a phase estimation experiment [24]. There, entangled probe signal and a local reference improved the SNR by nearly 3 dB. Similarly, for covert sensing of the Doppler effect, entanglement is expected to bring about enhancements. However, current quantum receivers that harness entanglement can only measure one quadrature [22,24,40,41], while covert sensing for the Doppler effect requires the measurement of both quadratures of the optical fields. The development of quantum receivers for entanglement-enhanced sensing protocols, capable of measuring both quadratures of the optical fields, remains a subject for future investigations.

VI. CONCLUSION

In conclusion, we successfully demonstrated covert sensing for the Doppler effect, enabling the accurate and secure estimation of an object's velocity. Our protocol's measurement performance and security have been rigorously analyzed using quantum measurement theory using the QFI and QCRB as the principal tool. Notably, we observed a performance-security trade-off, which allows us to balance the range of velocity estimation with the detection error probability against potential adversaries.

An essential advantage of our experimental scheme is that it does not require active phase locking and can be implemented using readily available off-the-shelf components. This significantly enhances the practical feasibility of our approach and opens up promising avenues for real-world quantum cryptography and sensing applications. Overall, our work represents a notable step forward in the advancement of quantum-based sensing technologies, with the potential to impact a wide range of fields based on the Doppler effect such as remote sensing, secure positioning and navigation, and target detection and tracking, where covert and high-precision measurements are of utmost importance.

ACKNOWLEDGMENTS

This work is funded by the Office of Naval Research (ONR) Grants No. N00014-19-1-2190 and No. N00014-23-1-2296 and the National Science Foundation (NSF) Grants No. 2326780 and No. 2317471. We also thank the University of Michigan for the support in rebuilding the laboratory.

APPENDIX: FISHER INFORMATION AND SIGNAL-TO-NOISE RATIO

In the experiment, a heterodyne detector using a reference with a frequency offset from the signal is exploited to measure both quadratures of the optical field of the returned probe signal. Figure 6(b) sketches a different detector in the dual-homodyne configuration that is also capable of simultaneously measuring both quadratures. In the dual-homodyne detector, the signal is evenly split and measured by two homodyne detectors supplied with local oscillators differing by a $\pi/2$ phase such that each homodyne detector measures one quadrature. In the literature, the terms "heterodyne detector" and "dual-homodyne detector" have been used interchangeably because in many scenarios, they share nearly identical measurement characteristics. In particular, their

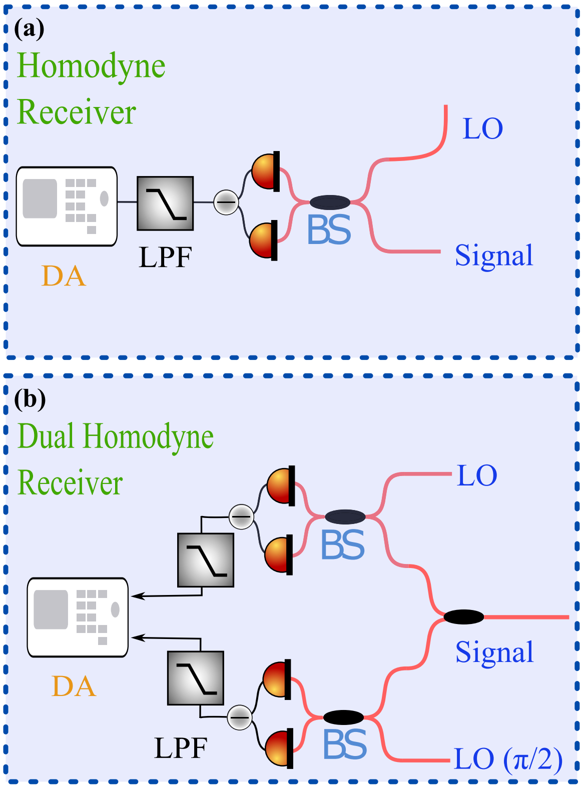

FIG. 6. Schematics of coherent optical detection. (a) In homodyne detection, the signal beats with the local oscillator (LO) on a 50:50 beam splitter (BS). The difference photocurrent from two photodiodes is filtered by a low-pass filter (LPF). (b) In dual-homodyne detection the signal is evenly split into two arms and beats with two LOs. One LO is in phase with the signal to address the amplitude ($\hat{q}$) quadrature while the other LO's phase differs by $\pi/2$ to address the phase quadrature ($\hat{p}$). DA: data acquisition.

SNRs in measuring one quadrature are both 3 dB inferior to that of the homodyne detector in the shot-noise-limited regime. However, we next show that the dual-homodyne detector outperforms the heterodyne detector in the presence of broadband thermal noise, as is the case for covert sensing.

The disparities between the three types of detectors, homodyne, dual-homodyne, and heterodyne, can be visualized in the frequency domain, as illustrated in Fig. 7. We first discuss the SNRs in the shot-noise-limited regime, plotted in the top panel. In the homodyne detection scheme, the LO shares the same carrier frequency as the signal represented by the green bar. The shot noise is white, exhibiting a flat spectrum. The measurement conducted over the signal's bandwidth is added by the shot noise in the same band. As a comparison, in the measurement of one quadrature in the dual-homodyne detection scheme, the signal is split in half by the 50:50 beam splitter while the spectrum of the shot noise remains unchanged, resulting in a 3-dB reduction in the SNR.

In the heterodyne detection scheme, the LO is shifted from the signal's carrier frequency by Ω. While the signal power does not get attenuated, the shot noise residing within the signal's band and within the image band, which is situated at $\omega_c - 2\Omega$, both contribute to the measurement [42,43], causing the noise power to be twice that of the homodyne detection. As such, the SNRs for the dual-homodyne detection and heterodyne detection are both half of the SNR for the homodyne detection.

We now turn our attention to the SNRs in the thermal-noise-dominant regime, sketched in the lower panel of Fig. 7. Both thermal noise and shot noise contribute to the homodyne detection. In the dual-homodyne detection scheme, both the signal and the thermal noise are attenuated by 50%, while the shot noise's spectrum remains unchanged. Since the thermal noise dominates the shot noise, the SNR for the dual-homodyne detection is nearly identical to that of the homodyne detection.

In contrast, the noise power in the heterodyne detection remains twice that of the homodyne detection due to the broadband nature of the thermal noise. Hence, in the thermal-noise-dominant regime, the homodyne and dual-homodyne detection schemes have the same SNR in measuring one quadrature, whereas the SNR for the heterodyne detection is 3 dB lower.

At this juncture, we will formally derive the SNRs for the three types of detectors. Since covert sensing for the Doppler effect builds on phase estimation, we first present its QFI associated with M ASE probes in the limit of $N_R \gg N_B, N_S$ [24]:

$$\mathcal{J}_\phi^{\mathrm{Q},M} \simeq M \cdot \frac{4\kappa N_S}{1+2N_B}. \tag{A1}$$

Here, the term 1 in the denominator is the contribution from the shot noise, while $2N_B$ is caused by the thermal noise.

The classical Fisher information (CFI) for estimating the phase shift using the homodyne detector in the same parameter region has been derived as

$$\mathcal{J}_\phi^{\mathrm{Homo},M} \simeq M \cdot \frac{4\kappa N_S \sin^2\phi}{1+2N_B}. \tag{A2}$$

We now consider the estimation of $\cos\phi$. Since the CFI for a function of ϕ is given by

$$\mathcal{J}_\phi = [\partial\phi f(\phi)]^2 \mathcal{J}_f, \tag{A3}$$

we immediately obtain

$$\mathcal{J}_{\cos\phi}^{\mathrm{Homo},M} = \mathcal{J}_\theta / \sin^2\phi = M \cdot \frac{4\kappa N_S}{1+2N_B}. \tag{A4}$$

One finds that $\mathcal{J}_{\cos\phi}^{\mathrm{Homo},M}$ is independent of ϕ, which is because the output of the homodyne detector is simply proportional to $\cos\phi$. We next proceed with defining the signal as the difference between the homodyne outcome at $\phi = 0$ and $\phi = \pi$. The SNR for the homodyne detector can be readily derived as

$$\begin{aligned}\mathrm{SNR}^{\mathrm{Homo},M} &= \frac{4(\cos 0 - \cos\pi)^2}{\left(\sqrt{1/\mathcal{J}_{\cos 0}^{\mathrm{Homo},M}} + \sqrt{1/\mathcal{J}_{\cos\pi}^{\mathrm{Homo},M}}\right)^2} \\ &= 4\mathcal{J}_{\cos\phi}^{\mathrm{Homo},M} = M \cdot \frac{16\kappa N_S}{1+2N_B}.\end{aligned} \tag{A5}$$

We now address the dual-homodyne detector in the same parameter region. A single homodyne detector in the dual-homodyne setting effectively measures half of the signal while the noise is also cut in half. As such, it is straightforward to

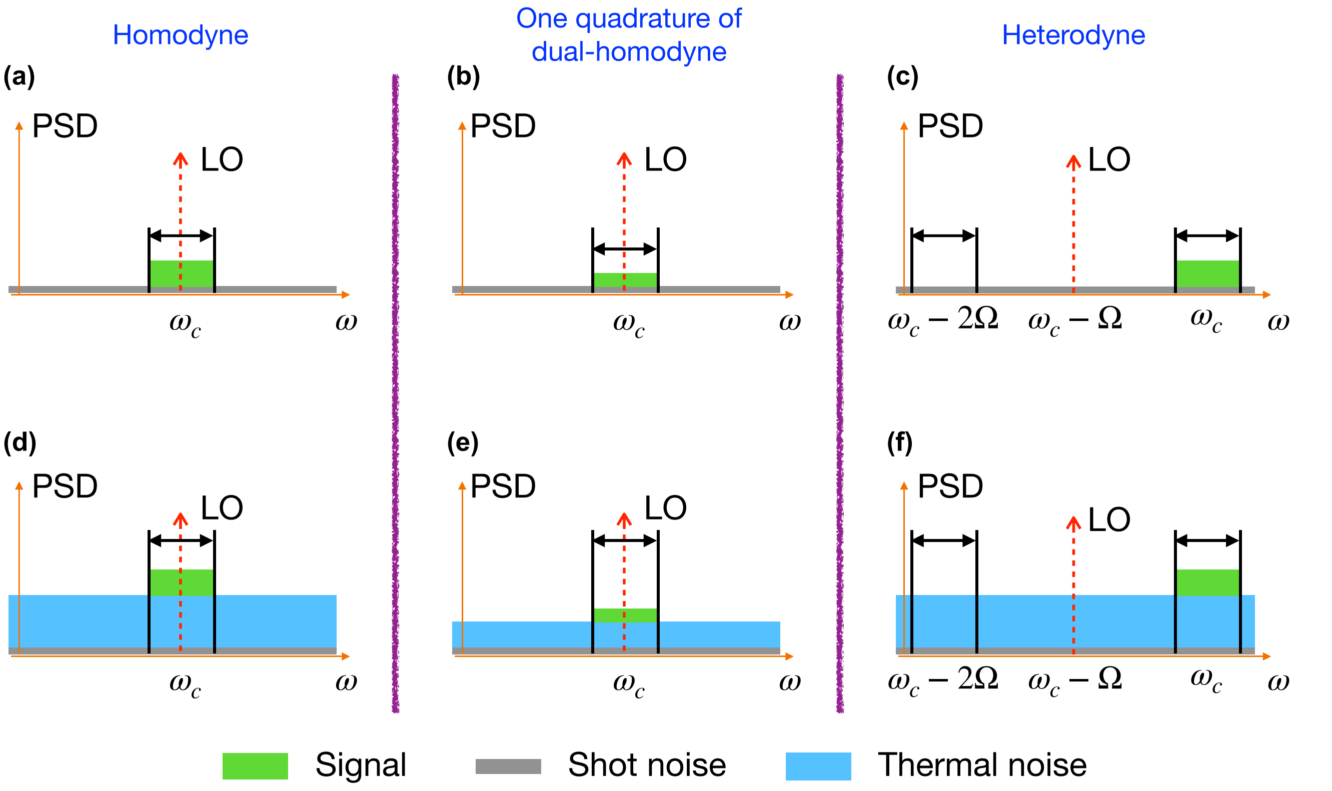

FIG. 7. The power spectral density (PSD) for the three measurement configurations. (a)–(c) Shot-noise-limited regime. (d)–(f) Thermal-noise-dominant regime. (a), (d) Homodyne detection. (b), (e) One quadrature of dual-homodyne detection. (c), (f) Heterodyne detection. The signal and noise within the areas enclosed by the black solid lines contribute to the measurement. LO: local oscillator.

derive the SNR for the single dual-homodyne detector as

$$\mathrm{SNR}^{\mathrm{Dual},M} = 4\mathcal{J}^{\mathrm{Dual},M}_{\cos\phi} = M\cdot\frac{8\kappa N_S}{1+N_B}. \tag{A6}$$

As discussed at the outset, the noise in the heterodyne detection in the thermal-noise-dominant regime is 3-dB higher than that in the homodyne detection. As such, one can derive the heterodyne's SNR as follows:

$$\mathrm{SNR}^{\mathrm{Hetero},M} = 4\mathcal{J}^{\mathrm{Hetero},M}_{\cos\phi} = M\cdot\frac{8\kappa N_S}{1+2N_B}. \tag{A7}$$

Further accounting for the detector's quantum efficiency η, one can readily derive the SNRs for the three types of detectors as

$$\mathrm{SNR}^{\mathrm{Homo},M,\eta} = M\cdot\frac{16\eta\kappa N_S}{1+2\eta N_B},$$
$$\mathrm{SNR}^{\mathrm{Dual},M,\eta} = M\cdot\frac{8\eta\kappa N_S}{1+\eta N_B},$$
$$\mathrm{SNR}^{\mathrm{Hetero},M,\eta} = M\cdot\frac{8\eta\kappa N_S}{1+2\eta N_B}. \tag{A8}$$

We perform an experiment to verify the theory for the SNRs at $\kappa_S N_S = 7.8\times10^{-4}$ and different N_B's. The experimental data reported in Fig. 8 are in accordance with the theoretical model, proving that the dual-homodyne detection and heterodyne detection do not always yield the same measurement performance.

We next derive the QFI and CFI for velocity estimation. The employed heterodyne detector is capable of simultaneously measuring both quadratures, with the

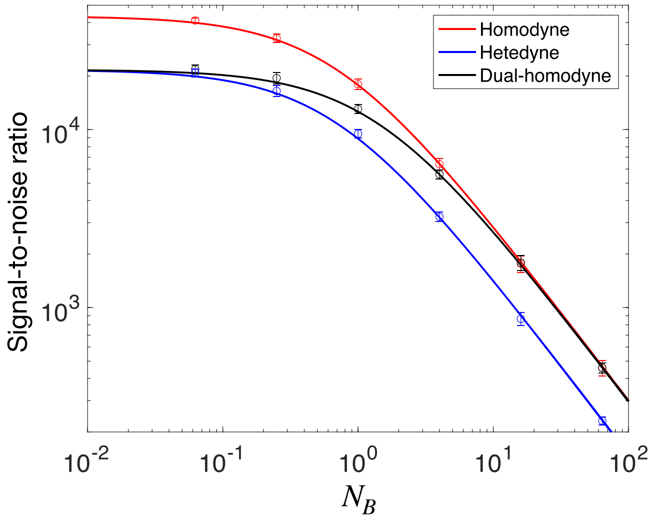

FIG. 8. SNRs for the homodyne (red), dual-homodyne (black), and heterodyne (blue) detection as a function of the background noise brightness N_B. Circles: experimental data; solid curves: theoretical model. $\kappa_S N_S = 7.8\times10^{-4}$, $N_B = 1/16$, $1/4$, 1, 4, 16, and 64, and $M = WT = 4.83\times10^6$. The quantum efficiency $\eta = 0.72$ (detector efficiency 0.8 and coupling efficiency 0.9). Error bars are calculated based on ten measurements each with 200 samples. $\Omega = 2\pi\times3$ MHz in heterodyne detection.

following CFI:

$$\mathcal{J}_{\cos\phi}^{\text{Hetero},M} = \mathcal{J}_{\sin\phi}^{\text{Hetero},M} = M\cdot\frac{2\kappa N_S}{1+2N_B}. \tag{A9}$$

With both quadratures measured, we can calculate the CFI for $\tan\phi$ as follows:

$$\frac{1}{\mathcal{J}_{\tan\phi}^{\text{Hetero},M}} = \frac{1}{\cos^2\phi}\frac{1}{\mathcal{J}_{\sin\phi}^{\text{Hetero},M}} + \frac{\sin^2\phi}{\cos^4\phi}\frac{1}{\mathcal{J}_{\cos\phi}^{\text{Hetero},M}}, \tag{A10}$$

as well as the CFI for ϕ:

$$\mathcal{J}_{\phi}^{\text{Hetero},M} = (\partial_\phi \tan\phi)^2\mathcal{J}_{\tan\phi}^{\text{Hetero},M} = \mathcal{J}_{\cos\phi}^{\text{Hetero},M}. \tag{A11}$$

The velocity estimation requires two uncorrelated consecutive phase measurements. Thus, the CFI for velocity estimation is derived as

$$\mathcal{J}_{v}^{\text{Hetero},M} = (\partial_v\delta\phi)^2\mathcal{J}_{\delta\phi} = \left(\frac{2\omega_c T}{c}\right)^2\mathcal{J}_{\cos\phi}^{\text{Hetero},M}/2. \tag{A12}$$

For the CRB,

$$(\Delta v)^2 = \langle(\tilde{v}-v)^2\rangle = 1/\mathcal{J}_{v}^{\text{Hetero},M}. \tag{A13}$$

Likewise, we can obtain the QFI for velocity estimation as

$$\mathcal{J}_{v}^{\text{Q,M}} \simeq \left(\frac{2\omega_c T}{c}\right)^2\mathcal{J}_{\phi}^{\text{Q,M}}/2. \tag{A14}$$

Using the QCRB, a lower bound on the measurement sensitivity in estimating the velocity reads

$$(\Delta v_Q)^2 \geqslant \frac{1}{\mathcal{J}_{v}^{\text{Q,M}}}. \tag{A15}$$

As discussed at the outset, the dual-homodyne detector generally outperforms the heterodyne detector in the thermal-noise-dominant regime. Indeed, one can show that the CFI for the dual-homodyne detector approaches the QCRB, i.e.,

$$\mathcal{J}_{v}^{\text{Dual},M} = \left(\frac{2\omega_c T}{c}\right)^2\mathcal{J}_{\cos\phi}^{\text{Dual},M}/2 \simeq \mathcal{J}_{v}^{\text{Q,M}} \tag{A16}$$

in the limit of $N_B \gg 1$. However, the dual-homodyne detection requires phase locking between the LO and signal, thereby adding extra complexities.

[1] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[2] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai *et al.*, Satellite-to-ground entanglement-based quantum key distribution, Phys. Rev. Lett. **119**, 200501 (2017).

[3] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu *et al.*, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. **120**, 030501 (2018).

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[5] W. K. Wootters and W. H. Zurek, The no-cloning theorem, Phys. Today **62**(2), 76 (2009).

[6] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Floodlight quantum key distribution: demonstrating a framework for high-rate secure communication, Phys. Rev. A **95**, 012332 (2017).

[7] Z. Zhang, C. Chen, Q. Zhuang, F. N. Wong, and J. H. Shapiro, Experimental quantum key distribution at 1.3 gigabit-per-second secret-key rate over a 10 dB loss channel, Quantum Sci. Technol. **3**, 025007 (2018).

[8] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, Nat. Photon. **9**, 163 (2015).

[9] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[10] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photon. **16**, 154 (2022).

[11] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photon. **15**, 570 (2021).

[12] M. Ben-Or and A. Hassidim, Fast quantum byzantine agreement, in *Proc. ACM Symp. Theory Comput. (STOC)* (ACM, New York, 2005), pp. 481–485.

[13] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing, Science **335**, 303 (2012).

[14] M. Ganz, Quantum leader election, Quantum Info. Process. **16**, 73 (2017).

[15] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Experimental quantum fingerprinting with weak coherent pulses, Nat. Commun. **6**, 8735 (2015).

[16] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, Quantum-secure covert communication on bosonic channels, Nat. Commun. **6**, 8626 (2015).

[17] M. Tahmasbi and M. R. Bloch, Covert and secret key expansion over quantum channels under collective attacks, IEEE Trans. Inf. Theory **66**, 7113 (2020).

[18] M. Tahmasbi and M. R. Bloch, On covert quantum sensing and the benefits of entanglement, IEEE J. Sel. Areas Inf. Theory **2**, 352 (2021).

[19] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, Fundamental limits of quantum-secure covert communication over bosonic channels, IEEE J. Sel. Areas Commun. **38**, 471 (2020).

[20] C. N. Gagatsos, B. A. Bash, A. Datta, Z. Zhang, and S. Guha, Covert sensing using floodlight illumination, Phys. Rev. A **99**, 062321 (2019).

[21] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, Hiding information in noise: Fundamental limits of covert

wireless communication, IEEE Commun. Mag. **53**, 26 (2015).

[22] H. Shi, Z. Zhang, and Q. Zhuang, Practical route to entanglement-assisted communication over noisy bosonic channels, Phys. Rev. Appl. **13**, 034029 (2020).

[23] D. Goeckel, B. A. Bash, A. Sheikholeslami, S. Guha, and D. Towsley, Covert active sensing of linear systems, in *Proc. Asilomar Conf. Signals Syst. Comput.* (IEEE, Pacific Grove, CA, 2017).

[24] S. Hao, H. Shi, C. N. Gagatsos, M. Mishra, B. Bash, I. Djordjevic, S. Guha, Q. Zhuang, and Z. Zhang, Demonstration of entanglement-enhanced covert sensing, Phys. Rev. Lett. **129**, 010501 (2022).

[25] T. Thayaparan, L. Stanković, and I. Djurović, Micro-Doppler-based target detection and feature extraction in indoor and outdoor environments, J. Franklin Inst. **345**, 700 (2008).

[26] S. Björklund, Target detection and classification of small drones by boosting on radar micro-Doppler, in *Proceedings of the 2018 15th European Radar Conference (EuRAD)* (IEEE, New York, 2018), pp. 182–185.

[27] N. Prasad, V. Shameem, U. Desai, and S. Merchant, Improvement in target detection performance of pulse coded Doppler radar based on multicarrier modulation with fast Fourier transform (FFT), IEE Proc., Radar Sonar Navig. **151**, 11 (2004).

[28] Y.-T. Chan and F. L. Jardine, Target localization and tracking from Doppler-shift measurements, IEEE J. Oceanic Eng. **15**, 251 (1990).

[29] M. Neinavaie, J. Khalife, and Z. M. Kassas, Acquisition, Doppler tracking, and positioning with starlink leo satellites: First results, IEEE Trans. Aerosp. Electron. Syst. **58**, 2606 (2021).

[30] B. Kusy, A. Ledeczi, and X. Koutsoukos, Tracking mobile nodes using RF Doppler shifts, in *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems* (ACM, New York, 2007), pp. 29–42.

[31] C. Zhao, H. Qin, and Z. Li, Doppler measurements from multi-constellations in opportunistic navigation, IEEE Trans. Instrum. Meas. **71**, 1 (2022).

[32] W. Guier and G. Weiffenbach, A satellite Doppler navigation system, Proc. IRE **48**, 507 (1960).

[33] M. L. Psiaki, Navigation using carrier Doppler shift from a leo constellation: Transit on steroids, Navigation **68**, 621 (2021).

[34] J. L. Garrison, J. R. Piepmeier, and R. Shah, Signals of opportunity: Enabling new science outside of protected bands, in *Proceedings of the 2018 International Conference on Electromagnetics in Advanced Applications (ICEAA)* (IEEE, New York, 2018), pp. 501–504.

[35] A. D. Droitcour, O. Boric-Lubecke, V. M. Lubecke, and J. Lin, 0.25 μm CMOS and BICMOS single-chip direct-conversion Doppler radars for remote sensing of vital signs, in *Proceedings of the 2002 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No. 02CH37315)* (IEEE, New York, 2002), Vol. 1, pp. 348–349.

[36] T. Wei, H. Xia, B. Yue, Y. Wu, and Q. Liu, Remote sensing of raindrop size distribution using the coherent Doppler lidar, Opt. Express **29**, 17246 (2021).

[37] M. Cerezo, A. Sone, J. L. Beckey, and P. J. Coles, Sub-quantum Fisher information, Quantum Sci. Technol. **6**, 035008 (2021).

[38] M. Tahmasbi and M. R. Bloch, Toward undetectable quantum key distribution over bosonic channels, IEEE J. Sel. Areas Inf. Theory **1**, 585 (2020).

[39] C. Weedbrook, C. Ottaviani, and S. Pirandola, Two-way quantum cryptography at different wavelengths, Phys. Rev. A **89**, 012309 (2014).

[40] Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, Entanglement-enhanced sensing in a lossy and noisy environment, Phys. Rev. Lett. **114**, 110506 (2015).

[41] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, Entanglement's benefit survives an entanglement-breaking channel, Phys. Rev. Lett. **111**, 010501 (2013).

[42] S. D. Personick, B.S.T.J. brief: An image band interpretation of optical heterodyne noise, Bell Syst. Tech. J **50**, 213 (1971).

[43] J. H. Shapiro, The quantum theory of optical communications, IEEE J. Sel. Top. Quantum Electron. **15**, 1547 (2009).