Revealing spoofing of classical radar using quantum noise

Jonathan N. Blakely,[1] Shawn D. Pethel,[1] and Kurt Jacobs[2]
[1]*U. S. Army DEVCOM Aviation & Missile Center, Redstone Arsenal, Alabama 35898, USA*
[2]*U. S. Army DEVCOM Army Research Laboratory, Adelphi, Maryland 20783, USA*

(Received 5 August 2023; accepted 14 December 2023; published 20 February 2024)

Electromagnetic remote sensing technologies such as radar can be misled by targets that generate spoof pulses. Typically, a would-be spoofer must make measurements to characterize a received pulse in order to design a convincing spoof pulse. The precision of such measurements is ultimately limited by quantum noise. Here we introduce a model of electromagnetic spoofing that includes effects of practical importance that were neglected in prior theoretical studies. In particular, the model includes thermal background noise and digital quantization noise, as well as loss in transmission, propagation, and reception. We derive the optimal probability of detecting a spoofer allowed by quantum physics. We show that heterodyne reception and thresholding closely approaches this optimal performance. Finally, we show that a high degree of certainty in spoof detection can be reached by Bayesian inference from a sequence of received pulses. Together these results suggest that a practically realizable receiver could plausibly detect a radar spoofer by observing errors in the spoof pulses due to quantum noise.

DOI: 10.1103/PhysRevResearch.6.013179

I. INTRODUCTION

It was recently shown that quantum mechanics fundamentally limits the ability to spoof electromagnetic pulses to fool a sensor [1]. Specifically, the measurement made by an adversary to characterize a pulse is generally insufficient to fully determine its quantum state. Thus, in principle, a radar operator can use knowledge of the transmitted quantum state to detect spoofs. A classic application of spoofing is where an airborne target emits spoof pulses to avoid being tracked by a ground-based radar [2,3]. Spoofing also has nonadversarial applications in hardware-in-the-loop testing [4–6]. A limitation of the work in Ref. [1] was the neglect of important practical considerations such as noise and loss. Clearly, a full understanding of the importance of quantum physics to real world spoofing requires a model that includes these effects. Here we introduce such a model including both thermal background noise and digital quantization noise, as well as loss in transmission, propagation, and reception.

The model provides insight into the relative importance of these effects in comparison to the purely quantum limits on spoofing previously identified. We analyze the performance of a quantum optimal receiver in discriminating spoofs. We find that, on one hand, loss and thermal noise degrade the ability to detect spoofing, while on the other hand, quantization noise in the spoof pulses acts similarly to quantum noise thus increasing the ability to discriminate. Finally, we examine a realizable receiver architecture, heterodyne reception combined with a thresholding procedure, which is shown to closely approach quantum optimal performance. Altogether, these results suggest that under realistic conditions of large loss and background noise, a realizable receiver can detect spoofing errors due to quantum noise. To be clear, quantum noise-based spoof detection is not a practical approach to current spoofing technologies. These devices introduce a variety of errors and a quantity of classical noise that provide the basis for existing spoof detection methods [2,3]. Rather, this work is forward looking to a future spoofing technology that can mimic a transmitted pulse with an accuracy approaching the quantum limit [1].

We introduce our model of spoof detection in Sec. II. The model takes the form of a quantum hypothesis test deciding between the presence or absence of a spoofer. In Sec. III, we determine the quantum optimal probability of discriminating between the hypotheses and present a specific architecture for realizing optimal detection. In Sec. IV, we analyze a more practically realizable detection scheme based on heterodyne reception and thresholding. In Sec. V, we examine a specific radar application where detection using heterodyne detection closely approaches optimal performance. In Sec. VI, we show how Bayesian inference can be used to aggregate information from multiple received pulses to detect spoofing with near certainty. Lastly, in Sec. VII, we give concluding remarks.

II. A QUANTUM MODEL OF RADAR SPOOFING

We model spoofing as a hypothesis test undertaken by the operator of a friendly receiver who must decide if a received pulse in a specific range-Doppler bin is a true reflection from a target of interest (hypothesis H_0), or a spoof pulse generated by an adversary (hypothesis H_1). We assume the target is probed by a narrowband, transform-limited pulse represented by a coherent state of a single, generalized, temporal mode (ignoring consideration of the spatial field pattern, for

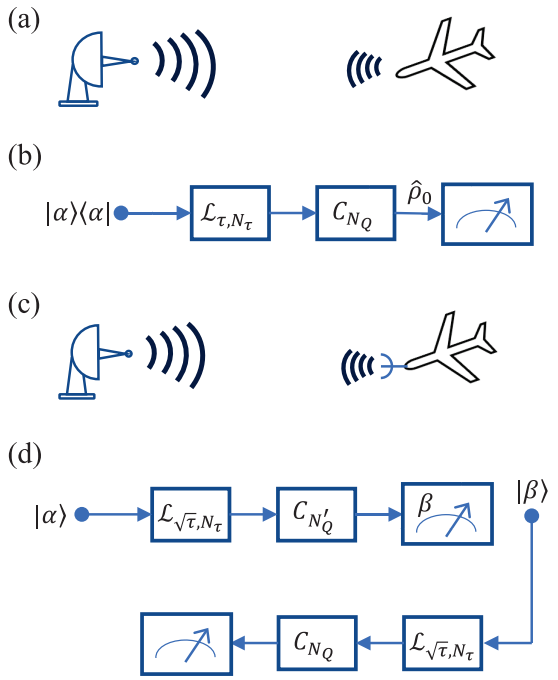

FIG. 1. Schematic depictions of the hypotheses to be discriminated where (a) and (c) illustrate a true echo from a target and a target-generated spoof, respectively, and (b) and (d) show the quantum channel models of each hypothesis. See text for more explanation.

simplicity). By design, the mean amplitude α of the transmitted coherent state is a complex random variable chosen to be distributed with the zero-mean Gaussian probability density given by

$$P(\alpha) = \frac{\lambda}{\pi} e^{-\lambda|\alpha|^2}, \tag{1}$$

where λ is a positive constant. The value of α is assumed to be known by the operator, but not by the adversary.

Under hypothesis H_0, the received pulse is a true reflection off a target of interest, as depicted in Fig. 1(a). In this case, the pulse suffers loss as it is radiated from a transmitting source (e.g., an antenna or a laser) with some degree of impedance mismatch, propagated out to the target and back, and is received by a detector (e.g., an antenna or photodetector). Thermal noise is added to the signal at transmission, reflection, and reception. We model these processes by a single-mode, lossy, Gaussian bosonic channel $\mathcal{L}_{\tau,N_T}$ with total transmissivity τ and mean noise photon number N_T [7]. The action of $\mathcal{L}_{\tau,N_T}$ on an input Gaussian state with displacement vector $\mathbf{x}$ and covariance matrix $\mathbf{V}$ is the transformation

$$\mathbf{x} \to \sqrt{\tau}\mathbf{x}, \tag{2}$$

$$\mathbf{V} \to \tau\mathbf{V} + (1-\tau)(2N_T+1)\mathbf{I}. \tag{3}$$

In the transformation of the covariance matrix, the first term represents the reduction of the size of fluctuations due to loss processes, while the second term represents fluctuations added by thermal noise. In what follows, it will be useful to let $N_T = N'_T/(1-\tau)$, where N'_T is a fixed mean noise photon number independent of τ.

Quantization noise is added upon digitization of the received signal. Typically, quantization noise in high resolution digitization is modeled as uniformly distributed over the range E corresponding to the least significant bit, with zero mean and variance $E/12$ [8]. For analytical convenience, it is here assumed that the quantization process is a classical Gaussian noise channel $\mathcal{C}_\xi$ that adds Gaussian noise with variance $\xi = E/12$ to the input signal. The action of $\mathcal{C}_\xi$ on an input Gaussian state with displacement vector $\mathbf{x}$ and covariance matrix $\mathbf{V}$ is the transformation $\mathbf{x} \to \mathbf{x}$, $\mathbf{V} \to \mathbf{V} + \xi\mathbf{I}$ [7,9].

The complete model under hypothesis H_0, including the final measurement made by the receiver, is depicted in Fig. 1(b). Assuming the transmitted state is $\hat{\rho} = |\alpha\rangle\langle\alpha|$, for which

$$\mathbf{x} = \begin{bmatrix} \alpha + \alpha^* \\ i(\alpha^* - \alpha) \end{bmatrix} \tag{4}$$

and $\mathbf{V} = \mathbf{I}$, where $\mathbf{I}$ is the identity matrix, the state measured by the receiver under hypothesis H_0, i.e., $\mathcal{C}_\xi(\mathcal{L}_{\tau,N_T}(\hat{\rho}))$, has displacement vector

$$\mathbf{x}_0 = \sqrt{\tau}\mathbf{x} \tag{5}$$

and covariance matrix

$$\mathbf{V}_0 = \{2N_0 + 1\}\mathbf{I}, \tag{6}$$

where

$$N_0 = N'_T + \xi/2 \tag{7}$$

and $\mathbf{I}$ is the identity matrix. The "0" subscripts in Eqs. (5) and (6) indicate that these quantities describe the quantum state at the receiver under hypothesis H_0. Equivalently, this state can be represented by the density operator

$$\hat{\rho}_0 = \frac{1}{\pi N_0} \int d^2\alpha' e^{-\frac{|\alpha' - \sqrt{\tau}\alpha|^2}{N_0}} |\alpha'\rangle\langle\alpha'|. \tag{8}$$

Under hypothesis H_1, the received pulse is a spoof, as represented in Fig. 1(c). We assume the spoof is generated by an adversary who has performed a single measurement on the transmitted state and aims to reproduce this state as closely as possible. We refer to this measure-and-prepare approach as *classical* spoofing [1]. We model propagation from the transmitter to the spoofer, and from the spoofer to the receiver as two separate passes through the lossy channel $\mathcal{L}_{\sqrt{\tau},N_T}$, which effects the transformation $\mathbf{x} \to \tau^{1/4}\mathbf{x}$, $\mathbf{V} \to \sqrt{\tau}\mathbf{V} + (1-\sqrt{\tau})(2N_T+1)\mathbf{I}$. When the output of the first channel is fed directly to the second channel, the result is equivalent to the single channel under hypothesis H_0, i.e., $\mathcal{L}_{\sqrt{\tau},N_T}(\mathcal{L}_{\sqrt{\tau},N_T}(\hat{\rho})) = \mathcal{L}_{\tau,N_T}(\hat{\rho})$. Thus, if the adversary were able to exactly copy the transmitted quantum state, the receiver would have no basis for discriminating a spoof from a real return. However, quantum physics does not allow the adversary to fully characterize the transmitted state with a single measurement.

The optimal single measurement for estimation of the Gaussian-distributed mean amplitude of a noisy coherent state, such as is received by the adversary, is heterodyne detection [10]. Thus, we assume the adversary makes a heterodyne measurement of the complex amplitude. Heterodyne detection has a long history in quantum optics, but is also essentially the operation performed by a coherent radar receiver insofar as the

received signal is mixed down to an intermediate frequency and then input to a quadrature detector and matched filters that output the real and imaginary parts of the complex amplitude. We further allow for the introduction of quantization noise by the adversary as the quadrature signals are typically digitized.

Ideal heterodyne detection realizes the positive operator-valued measure with measurement operators $|\beta\rangle\langle\beta|/\sqrt{\pi}$ [11]. The statistics for heterodyne measurement on the output of the lossy channel representing propagation from the transmitter to the spoofer with added quantization noise, i.e., $\mathcal{C}_{\xi'}(\mathcal{L}_{\sqrt{\tau},N_T}(\hat{\rho}))$, are described by the probability density

$$P(\beta) = \mathrm{tr}\left[\frac{|\beta\rangle\langle\beta|}{\pi}\mathcal{C}_{\xi'}(\mathcal{L}_{\sqrt{\tau},N_T}(\hat{\rho}))\right], \tag{9}$$

$$= \frac{\exp\left(-\frac{|\tau^{1/4}\alpha-\beta|^2}{(1+\sqrt{\tau})^{-1}N_T'+\xi'/2+1}\right)}{\pi[(1+\sqrt{\tau})^{-1}N_T'+\xi'/2+1]}, \tag{10}$$

where β is the complex measurement outcome. The variance of the additive quantization noise is ξ', which is generally not equal to that of the friendly receiver, ξ. The quantization noise levels are different for these two receivers because they are typically receiving signals of very different amplitudes.

The adversary generates a spoof pulse in the same generalized temporal mode with complex amplitude β and it passes through the lossy channel $\mathcal{L}_{\sqrt{\tau},N_T}$ representing the path from the adversary to the friendly receiver. The receiver is assumed to introduce quantization noise upon reception, resulting in the state $\mathcal{C}_{\xi}(\mathcal{L}_{\sqrt{\tau},N_T}(|\beta\rangle\langle\beta|))$. It is assumed that the receiver knows the adversary's measurement statistics, but not the measurement outcome β. Thus, the state of the pulse at the receiver is a mixture of coherent states weighted by the density Eq. (10) as expressed by the displacement vector

$$\mathbf{x}_1 = \mathbf{x}_0 \tag{11}$$

and the covariance matrix

$$\mathbf{V}_1 = \mathbf{V}_0 + 2\sqrt{\tau}(1+\xi'/2)\mathbf{I}. \tag{12}$$

The subscripts in Eqs. (11) and (12) indicate that these quantities describe the quantum state under hypothesis H_1. Equivalently, this state can be represented by the density operator

$$\hat{\rho}_1 = \frac{1}{\pi N_1}\int d^2\alpha' e^{-\frac{|\alpha'-\sqrt{\tau}\alpha|^2}{N_1}}|\alpha'\rangle\langle\alpha'|, \tag{13}$$

where

$$N_1 = N_T' + \xi/2 + \sqrt{\tau}(1+\xi'/2). \tag{14}$$

Upon reception, a decision must be made as to whether a received pulse is most consistent with the state specified by Eqs. (5) and (6) under hypothesis H_0 or by Eqs. (11) and (12) under hypothesis H_1. Comparing Eqs. (5) and (11), it can be concluded that the displacement vector provides no basis for a decision because it is the same under both hypotheses. The second term on the right hand side of Eq. (12) does provide a basis for a decision. The first term in parentheses in this equation represents the quantum noise in the heterodyne measurement outcome. One half of this noise is attributable to quantum noise in the transmitted coherent state. The other half is quantum noise associated with the Heisenberg uncertainty relation between the real and imaginary field quadratures in the course of an ideal heterodyne measurement. The second term in parentheses in Eq. (12) represents the noise added by the adversary through digital quantization. Interestingly, the adversary's quantum and classical noise enter the discrimination problem in the same manner even though their physical origins are distinct.

Having now framed spoof detection as a hypothesis test, we next turn to the analysis of specific measurement strategies that the receiver operator might adopt when seeking to detect the presence of a spoofer. In the sections that follow, the optimal measurement strategy allowed by quantum mechanics will be examined, as well as a practically realizable strategy that closely approaches the optimum.

III. QUANTUM OPTIMAL DETECTION OF SPOOFING

Quantum detection theory enables the calculation of the probability of successful detection assuming the receiver executes the measurement and decision criterion that minimizes the Bayesian total probability of error over all positive operator-valued measures [12]. In this section, we examine this optimal performance and the receiver architecture that would achieve it. Throughout this section, the Bayesian prior probability that a pulse is a spoof is assumed to be 0.5. It is straightforward to generalize the results that follow to allow for other values of this probability. But for the sake of clarity, only the one case will be discussed. Letting P_{opt} denote the probability of choosing the hypothesis that corresponds to the truth using the optimal receiver, then

$$P_{\mathrm{opt}} = \tfrac{1}{2}\left(1+\tfrac{1}{2}||\hat{\rho}_1-\hat{\rho}_0||_1\right), \tag{15}$$

assuming equal Bayesian prior probabilities for the two hypotheses, equal costs for all types of error, and where $||\cdot||_1$ denotes the trace norm [12].

We can obtain a fairly simple expression for P_{opt} by noting that it is unchanged if we apply a unitary transformation to both $\hat{\rho}_0$ and $\hat{\rho}_1$. Since according to Eq. (11) both states have the same displacement vector (phase space centroid), we can apply a displacement transformation to reduce the displacement vectors of both to zero while leaving the variances unchanged. This unitary transformation does not affect P_{opt}, but the resulting states are then thermal states and are thus diagonal in the Fock basis. Following Helstrom [13], the optimal probability of successful discrimination for any value of α is then

$$P_{\mathrm{opt}} = \frac{1}{2}\frac{1}{N_0+1}\sum_{n=0}^{m}\left(\frac{N_0}{N_0+1}\right)^n + \frac{1}{2}\frac{1}{N_1+1}\sum_{n=m}^{\infty}\left(\frac{N_1}{N_1+1}\right)^n, \tag{16}$$

with

$$m = \mathrm{floor}\left\{\frac{\ln\frac{N_1+1}{N_0+1}}{\ln\left[\frac{N_1(N_0+1)}{N_0(N_1+1)}\right]}\right\}. \tag{17}$$

For the $\alpha = 0$ case, Helstrom found optimal discrimination could be performed by photon counting followed by comparison to a threshold of value m [13]. It follows that for $\alpha \neq 0$, optimal discrimination can be performed by a receiver that first displaces the received signal by α and

then counts photons and compares to the threshold. In the context of microwaves, the displacement can be realized by homodyne down conversion. In principle, photon counting could be done on the resulting baseband signal. Unfortunately, existing single photon detectors in the microwave regime have low quantum efficiencies [14,15]. Thus, we next analyze heterodyne detection and thresholding, a currently realizable architecture. Importantly, this approach will be shown to perform close to optimally.

IV. DETECTION OF SPOOFING WITH HETERODYNE RECEPTION

Consider a receiver that makes a heterodyne measurement whose outcome is a complex amplitude that is compared to a threshold to discriminate the two hypotheses. Under hypothesis H_k, with $k = 0, 1$, the heterodyne measurement outcome β is a random variable with probability density [11]

$$P(\beta|H_k) = \mathrm{tr}\left(\frac{|\beta\rangle\langle\beta|}{\pi}\hat{\rho}_k\right) = \frac{e^{-|\beta-\sqrt{\tau}\alpha|^2/(N_k+1)}}{\pi(N_k+1)}. \tag{18}$$

We introduce a threshold μ such that if $|\beta| \leqslant \mu$ we select hypothesis H_0, and conversely if $|\beta| > \mu$ we select hypothesis H_1. The set of β values satisfying the former condition, which we will refer to as Z_0, is a filled circle (a disk) with radius μ centered on $\sqrt{\tau}\alpha$. The set satisfying the latter condition, referred to as Z_1, is the rest of the complex plane. The probability of success in choosing the true hypothesis, P_{het}, is the sum of the probability of choosing H_0 when it is true and the probability of choosing H_1 when it is true. Mathematically, this is

$$P_{\mathrm{het}} = \frac{1}{2}\int_{Z_0} d^2\beta P(\beta|H_0) + \frac{1}{2}\int_{Z_1} d^2\beta P(\beta|H_1), \tag{19}$$

$$= \frac{1}{2}(1 - e^{-\mu^2/(N_0+1)}) + \frac{1}{2}e^{-\mu^2/(N_1+1)}, \tag{20}$$

where, again, an assumption of equal prior probabilities has been made. It follows that the value of the threshold μ that optimizes P_{het} is equal to the magnitude of β where the curves $P(\beta|H_0)$ and $P(\beta|H_1)$ intersect. Specifically, the optimal threshold is

$$\mu_{\mathrm{opt}} = \sqrt{\frac{N_0+1}{1-\frac{N_0+1}{N_1+1}}\ln\left(\frac{N_1+1}{N_0+1}\right)}. \tag{21}$$

In the next section, we will compare this detection scheme with optimal detection in a specific application.

V. AN EXAMPLE

As a specific example, we use the parameters of a W-band radar designed to probe a small aircraft defined in Refs. [16,17]. Conventional radar theory relates radar characteristics, target range R, and target properties through the "radar equation" [18]

$$\tau = \left(\frac{G_T}{4\pi R^2}\right)\left(\frac{\sigma A_R}{4\pi R^2}\right), \tag{22}$$

where τ is interpreted as the ratio of power transmitted to power received, $G_T = A_R/(2\pi c/\omega_0)^2$ is the radar antenna gain, A_R is the antenna's effective area, σ is the target cross section, ω_0 is the pulse angular center frequency, and c is the speed of light. The first factor in parentheses on the right in Eq. (22) accounts for losses on propagation to the target, and the second factor accounts for losses upon reflection and propagation back to the radar antenna. The most significant loss mechanism in this model is the spreading of the spherical waves that make up the radar pulse such that τ decreases with the inverse square of the range R on each leg of the round trip. In the case of the W-band radar defined in Refs. [16,17], $A_R = 1\ \mathrm{m}^2$, $\sigma = 0.01\ \mathrm{m}^2$, and $\omega_0/2\pi = 100$ GHz.

Background noise in conventional radar theory is often modeled as black body radiation with an effective noise temperature [18]. For context, the noise temperature of the ground is roughly 300 K, while the noise temperature of the night sky is just a few K. At the horizon, the noise temperature takes an intermediate value of 100 to 150 K. Following Refs. [16,17], we consider a noise temperature of 150 K, which corresponds to a mean noise photon number $N_T' = 32$.

The magnitude of the quantization noise depends on the transmittivity τ because (i) the dynamic range of a quantizer is typically chosen to match the signal size at the receiver, and (ii) the signal size at the receiver depends on the loss in the channel, which is quantified by τ. To determine this magnitude, we note that the real and imaginary parts of the mean complex amplitude of the transmitted pulse are zero mean random variables with variance $(2\lambda)^{-1}$. So the average mean photon number in such pulses is $(2\lambda)^{-1}$. The signal under hypothesis H_0 passes through the channel $\mathcal{L}_{\tau,N_T}$ before arriving at the receiver. The signal would emerge from this channel with an average mean photon number $\tau/(2\lambda)$. We assume this signal is quantized at the receiver with n bits of resolution such that the least significant bit corresponds to a range $E \approx 2^{-n}\tau/(2\lambda)$ with units of photon number. The variance of the quantization noise is then taken to be $\xi = E/12$. The value of $(2\lambda)^{-1}$ is chosen by assuming the pulse width $T = 1\ \mu$s, and the average power $P_{\mathrm{ave}} = 10$ kW, giving an average pulse energy of 10^{-2} J. Under the assumption of narrow bandwidth, the energy per photon is approximately $\hbar\omega_0$. Then the effective mean photon number for quantization noise at the radar receiver is

$$\xi \approx \tau\frac{2^{-n}TP_{\mathrm{ave}}}{12\hbar\omega_0}. \tag{23}$$

A common value for n in existing microwave technology is ten, giving $\xi \approx 9 \times 10^4$ at a range of 1 km. But due to

the rapid increase of loss with increasing range, ξ drops to approximately one at 17 km. Beyond this level of resolution, the quantization noise is small compared to the quantum noise in this model. Existing ultra high resolution analog-to-digital converters can have $n = 32$, giving $\xi \approx 1$ at just 375 m.

The quantization noise introduced by the spoofer will necessarily have larger variance than ξ because the spoofer receives the signal after passing through the less lossy channel $\mathcal{L}_{\sqrt{\tau},N_T}$. By the same reasoning as above,

$$\xi' \approx \sqrt{\tau}\frac{2^{-n}TP_{\mathrm{ave}}}{12\hbar\omega_0}. \tag{24}$$

In this case, with $n = 10$, ξ' falls to approximately one at the impractical distance of 180 000 km, and with $n = 32$, $\xi' \approx 1$

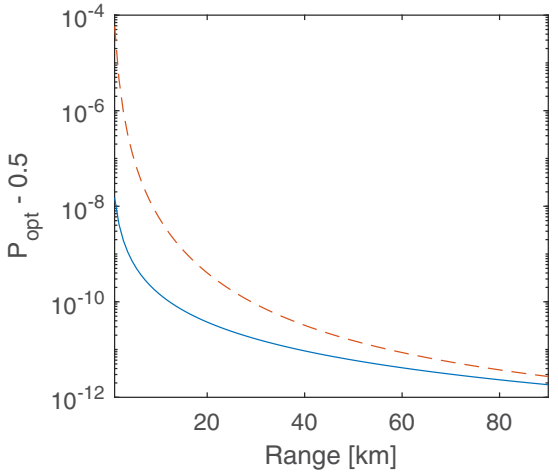

FIG. 2. The probability of successfully discriminating between true and spoofed pulses for an optimal receiver with quantization noise due to digitization with bit resolution $n = 32$ (dashed red line) and with no quantization noise (solid blue line).

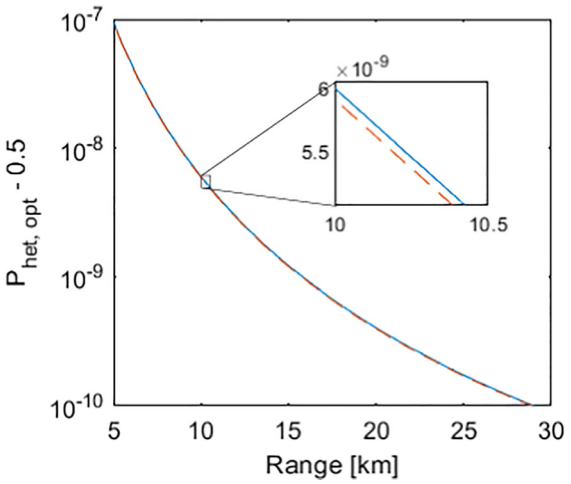

FIG. 3. The probability of successfully discriminating between true and spoofed pulses with quantization noise due to digitization with bit resolution $n = 32$ for an optimal receiver (solid blue line) and a heterodyne receiver with threshold detection (dashed red line).

at 88 km. Beyond this range, the spoofer can be said to be limited chiefly by quantum noise.

With all the model parameters now set, we first examine the performance of optimal spoof detection. The optimal probability of successful discrimination, as given by Eq. (17), is shown as a function of range in Fig. 2. Since the prior probability of spoofing is 0.5, the probability of successful discrimination before transmitting any signal is also 0.5. Thus, in the figure 0.5 is subtracted from P_{opt} to emphasize the increase due to the gain of information from reception and measurement of a pulse. The blue line is the probability with no quantization noise, i.e., $\xi = \xi' = 0$. The nonzero value (after subtracting 0.5) indicates that, in principle, quantum noise alone provides a sufficient physical basis for detecting the spoofer. Importantly, since the spoofer is assumed to employ the quantum optimal measurement for estimating the transmitted quantum state, no other measure-and-prepare strategy can be devised to eliminate this physical basis.

The dashed red line in Fig. 2 is the success probability for quantization with a bit resolution of $n = 32$ bits. At shorter ranges, the success probability can be orders of magnitude higher with quantization present simply because the noise it introduces is much larger than the quantum noise. As range increases, the $n = 32$ probability approaches the quantization-noise-free probability. This trend illustrates the decreasing relative importance of classical quantization noise versus quantum noise at long ranges where the signal size at the spoofer is greatly reduced by losses, but the quantum noise is not.

Optimal performance can be compared to that of heterodyne reception and thresholding. For $n = 32$, the probability, P_{opt}, is shown (solid blue line) along with the corresponding success probability for heterodyne reception, P_{het}, (dashed red line) in Fig. 3. Importantly, the more practical heterodyne detection scheme closely approaches the performance of optimal detection. The inset shows how the former falls just short of the latter.

With either detection method, the success probability is very small at most ranges. For example, at a range of 10 km, $P_{\text{het}} - 0.5$ for this receiver is approximately 10^{-8}. One might conclude that the increase in success probability over the prior probability would be too small to be of practical use in many applications. However, even a very small increase can be exploited by aggregating information from multiple transmissions through a process such as Bayesian inference, as described in the following section [1].

VI. BAYESIAN INFERENCE FROM MULTIPLE PULSES

The small effect of quantum noise added by an adversary can be exploited by aggregating the information collected from multiple pulses, each with a different random amplitude. Previously, Bayesian inference was used to update the prior probabilities in a noise-free, loss-free, spoofing model for a binary phase shift keying signal set [1]. Here we apply the same approach to the current model of spoofing with heterodyne reception and threshold detection.

Bayesian inference involves updating the prior probability after each new measurement outcome [19]. Let P_0 (P_1) be the prior probability of hypothesis H_0 (H_1), respectively, after M measurements. It is shown in the Appendix that the difference between the prior probabilities after $M \gg 1$ trials will on average take the value

$$\langle |P_1 - P_0| \rangle \approx \frac{|1 - e^{M\Delta_0(\Delta_0 - \Delta_1)}|}{1 + e^{M\Delta_0(\Delta_0 - \Delta_1)}}, \tag{25}$$

where

$$\Delta_0 = 2e^{-\mu^2/(N_0+1)} - 1 \tag{26}$$

and

$$\Delta_1 = 2e^{-\mu^2/(N_1+1)} - 1. \tag{27}$$

This approximation to the mean difference in probabilities as a function of M is shown to approach unity at large M in Fig. 4 for the example parameters of Sec. V (and, in particular,

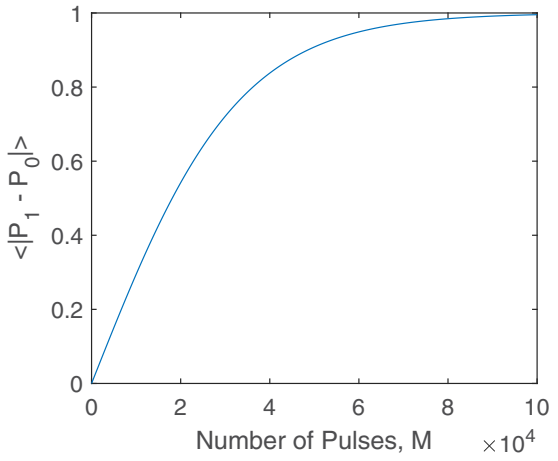

FIG. 4. Mean difference in prior probabilities as a function of number of pulses received. The prior probabilities are updated after each new pulse is received according to the procedure of Bayesian inference. The range is 1 km and the bit resolution is 32.

$n = 32$). This result means that certainty is approached by one of the two hypotheses when enough pulses have been received. For example, $\langle |P_1 - P_0| \rangle > 0.95$ after about 6×10^5 pulses. To achieve a desired value of $\langle |P_1 - P_0| \rangle$ near one, the required number of samples is

$$M \approx \frac{1}{\Delta_0(\Delta_0 - \Delta_1)} \ln \frac{1 + \langle |P_1 - P_0| \rangle}{1 - \langle |P_1 - P_0| \rangle}. \tag{28}$$

Dividing this number by a pulse repetition rate would give the required dwell time on target to achieve a desired average level of certainty. Figure 5 shows the required dwell time as a function of range for the example parameters assuming a desired $\langle |P_1 - P_0| \rangle$ of 0.9 and a pulse repetition rate of 500 kHz. At 1 km, the required dwell time is about 120 ms. During such an interval, a target with a velocity as high as 10^2 m/s would not move by a significant fraction of the range of 1 km.

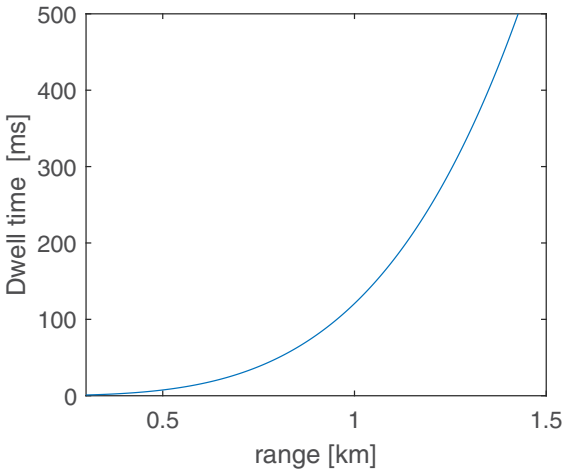

FIG. 5. Dwell time to reach a mean difference in prior probabilities of 0.9 as a function of range with a pulse repetition rate of 500 kHz.

VII. CONCLUSION

In this article, we have shown that a practically realizable receiver could plausibly detect a radar spoofer by observing errors in the spoof pulses due to quantum noise. In practice, information from many pulses would have to be aggregated to reach a meaningful degree of certainty, but in an example application this requirement was shown to be achievable.

To arrive at these results, we introduced a new model of radar spoofing that includes noise and loss. Key assumptions of the model were (i) the set of signals used by the radar (specifically coherent states with Gaussian-distributed amplitudes), and (ii) the limitation of the spoofer to a measure-and-prepare strategy. Extensions of this work could explore the consequences of modifying either of these assumptions. On the one hand, expanding the set of possible signals which the spoofer must discriminate could enhance the radar operator's ability to detect the spoofer. On the other hand, spoofing strategies that exploit more of the information available in the received quantum state than is extracted by a single measurement might allow for more deceptive spoofing. Our current work is pursuing both of these threads.

APPENDIX: CONVERGENCE OF BAYESIAN INFERENCE

Here we derive Eq. (25) assuming the radar transmits M pulses, each with an independent, randomly chosen amplitude. Under either hypothesis, the radar operator's measurement has two possible outcomes, a determination that the received pulse is either a true return or a spoof. Let the symbols $-$ and $+$ indicate the measurement outcomes corresponding to a true return and a spoof, respectively. In general, if H_i is true (where i is either zero or one), then the probabilities of the two outcomes are

$$P(\pm|H_i) = \frac{1}{2} \pm \frac{\Delta_i}{2} = \frac{1}{2}(1 \pm \Delta_i), \tag{A1}$$

where $-1 \leqslant \Delta_i \leqslant 1$, and the specific value of Δ_i depends on the particular choice of measurement. These probabilities are known as *likelihood* functions. For heterodyne detection and thresholding,

$$P(\pm|H_i) = \int_{Z_i} P(\beta|H_i)\, d^2\beta, \tag{A2}$$

from which follows Δ_0 and Δ_1 as given by Eqs. (26) and (27), respectively.

Let the prior probability of the hypothesis H_i before the first pulse is received be $P_0(H_i)$. After the nth pulse is received and measured, our new state of knowledge is obtained by multiplying the prior probabilities by the corresponding likelihood function and normalizing the result [19]. If we leave off the normalization (which we can always do after all M measurements have been made) the prior probabilities after

the nth pulse is received are

$$P_n(H_i) = P(\pm|H_i)P_{n-1}(H_i), \tag{A3}$$

$$= \tfrac{1}{2}(1 \pm \Delta_i)P_{n-1}(H_i), \tag{A4}$$

$$\approx \tfrac{1}{2}\exp(\pm\Delta_i)P_{n-1}(H_i), \tag{A5}$$

where the approximation in the last line is valid to the extent that $\Delta_i \ll 1$. Repeating this procedure for M measurements, and still without normalizing, we have

$$P_M(H_i) \approx \frac{1}{2^M}\exp\left(\Delta_i \sum_{n=1}^{M} x_n\right)P_0(H_i), \tag{A6}$$

where $x_n = 1$ if the outcome of the nth measurement indicates a spoof and $x_n = -1$ if it indicates a true return. Now assuming equal initial prior probabilities and normalization, the prior probabilities conditioned on the random variable $X \equiv \sum_n x_n$ are

$$P_M(H_0|X) = \frac{\exp(\Delta_0 X)}{\exp(\Delta_0 X) + \exp(\Delta_1 X)}, \tag{A7}$$

$$P_M(H_1|X) = \frac{\exp(\Delta_1 X)}{\exp(\Delta_0 X) + \exp(\Delta_1 X)}. \tag{A8}$$

A measure of our average certainty as to which hypothesis is true is

$$\langle |P_M(H_1|X) - P_M(H_0|X)| \rangle, \tag{A9}$$

where the average is over all possible sets of measurement outcomes $\{x_n\}$.

To evaluate this average, we need the distribution for X under each hypothesis. Since X is the sum of independent random variables it will be Gaussian for large enough M. Under the hypothesis H_i this Gaussian random variable has mean and variance

$$m_i = \sum_{n=1}^{M} \frac{1}{2}(1+\Delta_i) - \frac{1}{2}(1-\Delta_i) = \sum_{n=1}^{M} \Delta_i = M\Delta_i, \tag{A10}$$

$$V_i = \sum_{n=1}^{M}\left[(1-\Delta_i)^2\frac{1}{2}(1+\Delta_i) - (1+\Delta_i)^2\frac{1}{2}(1-\Delta_i)\right]$$

$$= M\left(1-\Delta_i^2\right). \tag{A11}$$

The Gaussian distribution under hypothesis H_i is then

$$P_i(x) = \frac{1}{\sqrt{2\pi V_i}}\exp\left[-\frac{(x-m_i)^2}{2V_i}\right]. \tag{A12}$$

The total distribution for X is

$$P(x) = P_0(H_0)\frac{1}{\sqrt{2\pi V_0}}\exp\left[-\frac{(x-m_0)^2}{2V_0}\right] + P_0(H_1)\frac{1}{\sqrt{2\pi V_1}}\exp\left[-\frac{(x-m_1)^2}{2V_1}\right]. \tag{A13}$$

With equal initial prior probabilities, the distribution for X is

$$P(x) = \frac{1}{\sqrt{8\pi V_0}}\exp\left[-\frac{(x-m_0)^2}{2V_0}\right] + \frac{1}{\sqrt{8\pi V_1}}\exp\left[-\frac{(x-m_1)^2}{2V_1}\right]. \tag{A14}$$

Thus, our certainty measure, defined in Eq. (A9), averaged over all possible measurement results is

$$\langle |P_M(H_1|X) - P_M(H_0|X)| \rangle = \frac{1}{\sqrt{8\pi}}\int_{-\infty}^{\infty}\frac{e^{\Delta_1 x} - e^{\Delta_0 x}}{e^{\Delta_0 x} + e^{\Delta_1 x}}\left(\frac{1}{\sqrt{V_0}}\exp\left[-\frac{(x-m_0)^2}{2V_0}\right] + \frac{1}{\sqrt{V_1}}\exp\left[-\frac{(x-m_1)^2}{2V_1}\right]\right)dx. \tag{A15}$$

The Gaussian functions in parentheses in the integrand act as sampling functions that pick out the value of the preceding factor at $x = \Delta_0 M$ and $x = \Delta_1 M$. Then, since $\Delta_0 \approx \Delta_1$, Eq. (25) follows. The notation in Sec. VI is simplified by using P_i to mean $P_M(H_i|X)$.

[1] J. N. Blakely and S. D. Pethel, Quantum limits to classically spoofing an electromagnetic signal, Phys. Rev. Res. **4**, 023178 (2022).

[2] D. C. Schleher, *Electronic Warfare in the Information Age*, Artech House radar library, Artech House, 1999.

[3] J. Genova, *Electronic Warfare Signal Processing*, Artech House electronic warfare library, Artech House, 2018.

[4] J. J. Strydom, J. E. Cilliers, M. Gouws, D. Naicker, K. Olivier, *Hardware in the loop radar environment simulation on wideband drfm platforms*, in IET International Conference on Radar Systems (Radar 2012), IET, 2012, pp. 1–5.

[5] J. J. Strydom, J. J. de Witt, and J. E. Cilliers, *High range resolution x-band urban radar clutter model for a drfm-based hardware in the loop radar environment simulator*, in 2014 International Radar Conference, IEEE, 2014, pp. 1–6.

[6] C. P. Heagney, Digital radio frequency memory synthetic instrument enhancing US navy automated test equipment mission, IEEE Instrumentation & Measurement Magazine **21**, 41 (2018).

[7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[8] W. R. Bennett, Spectra of quantized signals, Bell Sys. Tech. J. **27**, 446 (1948).

[9] R. Zamir, M. Feder, On lattice quantization noise, IEEE Trans. Inf. Theory **42**, 1152 (1996).

[10] M. Guţă, P. Bowles, G. Adesso, Quantum-teleportation benchmarks for independent and identically distributed spin states and displaced thermal states, Phys. Rev. A **82**, 042310 (2010).

[11] J. Shapiro, S. Wagner, Phase and amplitude uncertainties in heterodyne detection, IEEE J. Quantum Electron. **20**, 803 (1984).

[12] C. W. Helstrom, Quantum Detection and Estimation Theory (ISSN, Elsevier Science, 1976).

[13] C. W. Helstrom, Detection theory and quantum mechanics, Inf. Control. **10**, 254 (1967).

[14] Y.-F. Chen, D. Hover, S. Sendelbach, L. Maurer, S. Merkel, E. Pritchett, F. Wilhelm, R. McDermott, Microwave photon counter based on Josephson junctions, Phys. Rev. Lett. **107**, 217401 (2011).

[15] A. Pankratov, L. Revin, A. Gordeeva, A. Yablokov, L. Kuzmin, E. Il'ichev, Towards a microwave single-photon counter for searching axions, npj Quantum Inf. **8**, 61 (2022).

[16] Q. Zhuang, J. H. Shapiro, Ultimate accuracy limit of quantum pulse-compression ranging, Phys. Rev. Lett. **128**, 010501 (2022).

[17] B.-H. Wu, S. Guha, Q. Zhuang, Entanglement-assisted multiaperture pulse-compression radar for angle resolving detection, Quantum Sci. Technol. **8**, 035016 (2023).

[18] M. Skolnik, *An Introduction and Overview of Radar*, Radar Handbook **3**, 1–1 (2008).

[19] R. Winkler, *An Introduction to Bayesian Inference and Decision*, Probabilistic Publishing, 2003.