Abstract—In this work we show that intensity interferometry may be used to send a non-trivial amount of data steganographically over the air. Intensity interferometry was developed by Hanbury Brown and Twiss [1], [2], and originally used to measure the angular diameter of stars [3] at both optical and radio frequencies. Since then, this method has been used in many other fields to measure the size of regions of interest. Here we introduce an opposite paradigm and show that the technique may be used to transmit information wirelessly.

This channel does not require additional frequency bands or additional bandwidth as it relies on a phenomenon that is already present but unexploited in current systems, and it has the potential to be highly secure against eavesdropping, and thus shows promise as a means of steganographic communication. We discuss the information theory of our new type of channel and address the trade-off between channel capacity and signaling rate. Finally, we propose communication through intensity interferometry as a method of secure steganographic communication in general and suggest its application in particular for secure communications in networks of wireless sensors.

Index Terms—Intensity interferometry, steganography, wireless sensor networks.

I. INTRODUCTION

Classical long-distance communication methods are based on the emission and detection of electromagnetic fields (EM fields). All current methods are based upon the modulation of the amplitude, phase, and frequency of these fields. Because EM fields are composed of photons, these fields have additional characteristics that hitherto have not been exploited to communicate. One of these characteristics is the spatial and time correlations that exists between photons because of their quantum-mechanical nature [4], [5], [6].

For almost sixty years the spatial correlations between photons have been exploited in science and technology through the use of a technique called intensity interferometry; for example\(^1\), to measure stellar angular diameters [3], an application pioneered by Hanbury Brown and Twiss [7], [2], who coined the term intensity interferometry; to investigate nuclear collisions [8]; to measure electron temperature fluctuations in fusion plasmas [9]; and head-disk spacing in hard drives [10]; to characterize hard synchrotron radiation [11]; as a diagnostic tool in Biology and Chemistry [12]; and recently to investigate the quantum state of Bose-Einstein condensates [13], [14], [15]. In short, up to know non-local spatial correlations between photons have been used through intensity interferometry as a measurement technique; however, can this technique be exploited as a communication tool? Here we attempt to answer this question.

To understand how intensity interferometry works [16], consider the situation presented in Figure 1: there are two distant random point sources of electromagnetic radiation, \(a\) and \(b\), and there are two independent detectors, 1 and 2. The detectors need not be directly connected (all field intensity calculations between the

\(^1\)The following list of references is not exhaustive but only representative, as there are hundreds of papers published on different applications of intensity interferometry.
two detectors can be done remotely). Assume that the sources are separated in space by \( D_S \), the two detectors by \( D_R \), and that the distance from the sources to the detectors, \( L \), is much larger than \( D_S \) and \( D_R \).

Without loss of generality, assume that the radiation pattern is isotropic, and let us write explicitly the time-dependence of the electric field radiated by each antenna, \( E_\alpha \), thus

\[
E_\alpha = A_\alpha \exp(-i\omega_\alpha t + i\phi_\alpha(t)), \tag{1}
\]

where the subscript \( \alpha \) identifies the antenna (\( \alpha = a, b \)) and \( A_\alpha \) is the amplitude.

On the receiving end, the second order correlation function is defined by

\[
C \triangleq \frac{\langle I_1 I_2 \rangle}{\langle I_1 \rangle \langle I_2 \rangle}, \tag{2}
\]

where \( I_j \) is the EM field intensity at detector \( j \), \( I_j = E_j E_j^* \) (the asterisk denotes complex conjugation) and \( E_j \) is the total electric field at detector \( j \) from both sources. The sharp brackets indicate a time average over time interval \( T_0 \). To simplify the discussion we assume that the emission from both sources is at the same frequency \( \omega_a = \omega_b = \omega \) and that both sources emit radiation with the same amplitude, \( A_a = A_b = A \). Furthermore, assume that \( \phi_a(t) \) and \( \phi_b(t) \) are statistically independent random variables; if we calculate the time averages over a time \( T_0 \) much larger than the coherence time \( T_c \) of the sources, i.e., the time over which \( \phi_a(t) \) is constant, then the factors that depend on

\[
\delta(t) \equiv \phi_a(t) - \phi_b(t) \tag{3}
\]

become vanishingly small and may be ignored. Thus, in the far-field region, i.e., \( D_S, D_R \ll L \), and with the above assumptions, the second-order correlation function in eq. (2) is given by [17]

\[
C \approx 1 + \cos^2(\Delta) \tag{4}
\]

where \( \lambda \) is the radiation’s wavelength and

\[
\Delta \triangleq \frac{\pi D_a D_R}{L \lambda}. \tag{5}
\]

Equation (4) is the basis of Hanbury Brown and Twiss interferometry: the linear size of the source, \( D_a \), is fixed but unknown, and the experimenter varies the distance between the receivers \( D_R \), records the intensities, and calculates the second-order spatial correlation. It is possible to find the angular size \( \theta_S = D_S/L \) of the source by plotting as a function of \( D_R \) the reduced second-order correlation, \( \gamma \),

\[
\gamma \triangleq \frac{C - 1}{C(0) - 1}, \tag{6}
\]

where \( C(0) \) is the value of \( C \) extrapolated to \( D_R = 0 \). Using eq.(4) we obtain

\[
\gamma = \cos^2(\Delta). \tag{7}
\]

The value of \( D_R \) where \( \gamma \) first vanishes corresponds to the angular size of the source, \( \theta_S \).

This is the method that Hanbury Brown and Twiss used to measure the angular size of stellar sources both at radio and optical wavelengths [3], [7], [2], [17]. In their case, \( T_0 \gg T_c \) because the stellar radiation is incoherent on time scales much smaller than the integration time necessary to achieve a good signal to noise ratio (see [17]).

Up to now, intensity interferometry has been used to measure the angular size of the source \( \theta_S = D_S/L \) by varying the distance between receivers \( D_R \). Note that according to eq. (4) the second-order correlation \( C \) is unchanged upon permutation of \( D_a \) and \( D_R \).

Here we propose to exploit this symmetry to create a communication channel in the following way.

**II. A NEW METHOD OF COMMUNICATION**

Consider now \( a \) and \( b \) to be sources of digital transmission over the air. For the sake of simplicity we assume that both antennas transmit using BPSK modulation, and therefore

\[
\delta(t) \in \{0, \pi\}. \tag{8}
\]

Let us call this kind of transmission, i.e., the transmission by individual antennas, the baseline transmission, and let us call baseline symbols \( s_b \) the symbols thus sent.
In this case, and without any assumptions about the averaging time $T_0$, the reduced second order correlation calculated at the receivers is

$$\gamma = \cos^2(\Delta) \left( \frac{1 + \langle \cos \delta \rangle}{1 + \langle \cos \delta \rangle \cos \Delta} \right)^2,$$

(9)

where, as before, the sharp brackets indicate a time average over a time $T_0$. Note that the factor $(\cos \delta)$ is dependent upon the the averaging time $T$: when $T_0 \to \infty$ then $\langle \cos \delta \rangle \to 0$, and eq. (7) is recovered.

For a given distance $L$ between the sources and the detectors consider keeping $D_k$ fixed, while varying $D_s$. The different values of $D_s$ will result in different values of $\gamma$ at the receivers, and thus information can be sent.

To be specific, suppose now that it could be possible to change $D_s$ as a function of time, and that only two values of $D_s$ are allowed, $D_s = d_0$ and $D_s = d_1$. In other words, every $T_0$ seconds we change the transmitting baseline $D_s$ between $D_s = d_0$ and $D_s = d_1$. Furthermore, suppose that these values are chosen such that the second-order correlation at the receivers is $\gamma(d_0) = 0$, or $\gamma(d_1) = 1$. Then, these two values of $\gamma$ can be used to represent the two values of a bit of information through intensity interferometry. Let us call interferometry symbols $s_i$ and thus information can be transmitted.

Please note that it takes a time $T_0$ to transmit a single $s_i$ symbol.

Figure 2 (top and bottom) is a contour plot of $\gamma$ depending on $D_s$, $D_k$, and $L$ for a value of $\lambda = 3$ cm, which corresponds to a frequency of 10 GHz, a value typical of wireless channels. Note that the value $\gamma = 0.5$ is the bit-value discrimination boundary: any received value above 0.5 will be considered to be a “one;” otherwise, it will be considered as zero.

The novelty of this approach is that the additional information thus transmitted is independent of what each of the transmitters is broadcasting. Even if the baseline broadcast consists of pure noise, information can be sent by letting $D_s$ vary between $d_0$ and $d_1$ every $T_0$ seconds.

The transmitters need not be moved mechanically: for example, if four transmitters are set up along a line perpendicular to the direction of the receivers such that the distance between the innermost pair is $d_0$ and the distance between the outermost pair is $d_1$, then we can switch electronically between the outermost and innermost pair to transmit: we could use, say, the inner transmitter pair to send a zero, and the outer pair to send a one. It is worth mentioning that this kind of setup already exists in Multiple-Input-Multiple-Output (MIMO) communication systems, wherein the power allocated to each transmitter is varied according to the time-dependent attenuation of the multiple transmission paths [18], [19]. Therefore, we can effectively change electronically the pair of transmitting antennas by using standard MIMO technology.

In addition, the results in Figure 2 (bottom panel) show that this method of communication is potentially secure against eavesdropping. This follows from the rapid variation of $\gamma$ with $D_s$, $D_k$ and $L$. Indeed, by carefully choosing the separation between the source antennas and the baseline of the receivers, the transmission can be targeted to a specific distance $L$. For values of $L$ much smaller than this target distance, $\gamma$ varies so fast that an eavesdropper will need to know the value of $D_k$ to high accuracy. On the other hand, at distances much larger than $L$, $\gamma$ does not change, and therefore no information is available at these distances. In addition, by using modulation schemes more sophisticated than $\gamma \in \{0, 1\}$, eavesdropping can be made more difficult.

Finally, we want to stress that this method of communication does not require additional bandwidth or additional frequencies, because it relies on the variation of spatial correlations between the EM fields. Thus, the data throughput of existing wireless links can be enhanced in an already crowded EM spectrum.

III. INFORMATION THEORY

We wish to see how much information may be passed via the new method that we have described.

As any wireless method, it is subject to two main sources of error: electronic noise which appears in the form of additive noise, and atmospheric fading. In addition, our method is subject to the error introduced through the signaling time $T_0$ used (recall that every $T_0$ seconds we switch antenna pairs to transmit a different $s_i$ symbol).

Note that we intend to use this method as an addition to an existing wireless channel used to transmit the $s_b$ symbols. Because any electronic noise or atmospheric fading are already accounted for in the baseline channel design, their impact on the interferometric channel is likely to be minimized further because we rely on the time average over several $s_b$ symbols to send a $s_i$ symbol. Therefore, here we choose to concentrate on the role of the time average that is intrinsic to the method, and consider how capacity depends on $T_0$, and whether any information may be passed for finite $T_0$.

As explained above, we fix the distance $D_k$ between the receivers, and vary the distance between transmitters $D_s$ between two values, $d_0$ and $d_1$ every $T_0$ seconds. Let $\gamma_s$ be the value of the second-order correlation thus sent, i.e., this is the ideal value sent (and received) in the absence of time averaging errors:

$$\gamma_s = \cos^2(\Delta),$$

(10)
where $\Delta$ may take the values $\Delta_0$ and $\Delta_1$ depending on whether $D_S = d_0$ or $D_S = d_1$. When $T_0$ is finite, the computed value at the receivers, $\gamma_R$, is

$$\gamma_R = \gamma_S \left( \frac{1 + X}{1 + \gamma_S^{1/2} X} \right)^2,$$

where for the sake of compactness we have written

$$X \triangleq \langle \cos \delta \rangle.$$ (11)

Note that if we were able to place the transmitting antennas exactly at the values of $D_S$ required to get $\Delta_0 = \pi/2$ and $\Delta_1 = 2\pi$, then $\gamma_S(\Delta_0) = 0$ and $\gamma_S(\Delta_1) = 1$ and $\gamma_R = \gamma_S$ identically for any value of the averaging time $T_0$. Therefore, in the ideal case of perfectly placed antennas the error probability is zero.

 Practically, however, errors in the values of $d_0$ and $d_1$ will make $\gamma_S \not\equiv 0, 1$, and the time averaging procedure will introduce errors at the receiving end. Let $\gamma_0 \triangleq \gamma_S(\Delta_0)$ and $\gamma_1 \triangleq \gamma_S(\Delta_1)$ be the values of $\gamma_S$ obtained when placement errors occur. It is straightforward, but lengthy, to show that when $\gamma_0 \approx 0.33$ then $\gamma_R(\gamma_0) \approx 0$ for any averaging interval, i.e., subject to this bound on $\gamma_0$ transmitted zeros are recovered without any error. The same is not true for $\gamma_1$: for any finite averaging value errors are introduced. Therefore, if the placement errors when transmitting a zero are not too large ($\gamma_0 < 0.33$ means that $d_0$ is accurate to within $20\%$, a very loose tolerance), then our channel is a Z-channel [20].

What is the capacity of this Z-channel? It depends on the probability of $\gamma_R(\gamma_1) < 0.5$, which depends, through eqs. (11–12), on the averaging time used.

Because the baseline transmission is digital, averaging over $T_0$ means that we are averaging over $N s_b$ symbols of duration $T_S$ each; i.e.,

$$T_0 = N T_S.$$ (13)

Thus, if we average over $N s_b$ symbols, and $k$ of them have $\delta = \pi$ while $N - k$ have $\delta = 0$, then

$$X = \frac{N - 2k}{N}.$$ (14)
Because \( s_0 \) symbols with \( \delta = 0 \) and \( \delta = \pi \) occur with equal probability, then \( k \), and therefore \( X \), follow a binomial distribution with probability \( p = 0.5 \), and the probability of getting a given value of \( X \) is

\[
P(X = (N - 2k)/N) = 2^{-N} \binom{N}{k}.
\]  

According to eq. (15) the expectation value of \( X \) is

\[E(X) = 0.\]

For a given \( \gamma = \gamma_1 \) we can use eqs. (11), (12), and (14–15) to compute the probability of error for a \( s_i = 1 \) symbol as a function of the number of \( s_0 \) symbols averaged. Figure 3 is a plot of this error probability when sending \( s_i = 1 \) for two cases: first, when the placement of the antennas is accurate to within 10%, i.e., \( \Delta_1 = 1.8\pi \) and therefore \( \sqrt{\gamma_0} = \sqrt{\gamma_1} = 0.809 \) (instead of the ideal value \( \gamma_1 = 1 \)), and when \( \Delta_1 = 1.9\pi \) (5% placement error, \( \sqrt{\gamma_0} = \sqrt{\gamma_1} = 0.951 \)).

Armed with the error probability \( P \), we can compute the capacity of the interferometric channel \( C_i \):

\[C_i(P) = \frac{C_2(P)}{NT_s},\]

where \( C_2(P) = \log_2(1 + (1 - P)P^{P/(1-P)}) \) is the capacity for a Z-channel [21]. Note that in eq. (16), \( C_2(P) \) must be divided by \( NT_s \) because this is the time it takes to send a \( s_i \) symbol. Figure 4 is a plot of \( C_i \) (in units of bits/\( T_s \)) as a function of \( N \) for two values of the antennas’ placement error.

Also, note that as \( P \to 0 \) then \( C_2 \to 1 \), and, therefore, \( C_i T_s \to 1/N \). This limit is illustrated in Figure 4 as well.

At first glance, it seems that the best strategy to increase capacity would be to use the smallest \( N \) possible. This is true, but it does not take into account the coding difficulties. As the probability of error decreases, one can basically ignore error-correction coding [21] and just send the raw symbols, and take an error every now and then. Therefore, instead of sending one \( s_i \) symbol every two \( s_0 \) symbols \((N = 2)\) and use error-correction coding to overcome the high error probability \((P = 0.25)\) and achieve \( C_i \approx 0.35/T_s \), it is better to use, say, \( N = 16 \) for which \( P = 3 \times 10^{-2} \) or \( P = 1.8 \times 10^{-4} \) (depending on the antenna placement error; see Figure 3) and send the raw symbols, achieving \( C_i \approx 0.06/T_s \). Naturally, more work and the specific applications of our method are necessary to clarify further these trade-off questions.

IV. POTENTIAL APPLICATIONS

In general, our method allows to piggyback additional data onto an existing wireless data stream. This requires duplicating the number of antennas in Single Input-Single Output systems and additional hardware for antenna switching. Therefore, in general, we envision that our method will be used to send additional, low-priority data, or to send additional data steganographically.

We cannot overstate the steganographic potential of our method: an eavesdropper will need to know, first, that intensity interferometry is being used, and, second, the particular parameters of the link, i.e., \( D_h, D_s, L, \) and \( N \). Note that \( \gamma \) varies rapidly with \( D_h, D_s, \) and \( L \) (Figure 2); furthermore, errors in \( D_h \) by the eavesdropper will corrupt the received \( s_i \) symbols. Note that the use of intensity interferometry can not be told by merely eavesdropping on the baseline transmission.

In particular, we suggest intensity interferometry to communicate securely additional data within a wireless sensor network wherein power availability is at a premium [22].

Because of scarcity of resources, there is a conflict between the amount of data that the sensors can collect and the amount of data that can be communicated to the user. Therefore, a decision must be made as to the data to drop to avoid compromising the longevity of the sensors due to the extra power consumption. The use of intensity interferometry will require the fitting of sensors with duplicate antennas (each transmitting at half the original power), but, on the other hand, allow the transmission of additional data that otherwise is dropped.

In addition, the security against eavesdropping in a wireless sensor network is a topic of active research ([23],[24], [25]). Cryptography based on asymmetric key distribution is not suitable in a resource limited wireless sensor network [26], and a different approach is necessary (i.e., [26]). In addition to cryptography (or instead of it) we propose the use of steganography to secure the data in wireless sensor networks. Because of the steganographic potential of the method presented here, we suggest that the use of intensity interferometry in wireless sensor networks is worthy of further study.

V. SUMMARY

We presented a new type of wireless channel based on intensity interferometry. Intensity interferometry is a technique that exploits the non-local spatial correlations between photons, and it has been used extensively for over sixty years as a measurement technique. Here we have advanced for the first time its use as a wireless transmission method, and we have shown that this channel has the characteristic of a Z-channel and has non-zero capacity.

We propose that these new technique may be used to send additional low-priority data through an existing data
link suitably modified to support intensity interferometry, or to send data steganographically.

In addition, we propose that the use of intensity interferometry may be relevant for secure communications in wireless sensor networks.

References


