Sensing intruders using entanglement: a photonic quantum fence

Travis S. Humble*[a], Ryan S. Bennink[a], Warren P. Grice[a], Israel J. Owens[b]
[a]Oak Ridge National Laboratory, 1 Bethel Valley Road, Oak Ridge, TN USA 37831-2008;
[b]Los Alamos National Laboratory, 30 Bikini Atoll Road, Los Alamos, NM USA 87545-1663

ABSTRACT

We describe the use of quantum-mechanically entangled photons for sensing intrusions across a physical perimeter. Our approach to intrusion detection uses the no-cloning principle of quantum information science as protection against an intruder's ability to spoof a sensor receiver using a 'classical' intercept-resend attack. Moreover, we employ the correlated measurement outcomes from polarization-entangled photons to protect against 'quantum' intercept-resend attacks, i.e., attacks using quantum teleportation. We explore the bounds on detection using quantum detection and estimation theory, and we experimentally demonstrate the underlying principle of entanglement-based detection using the visibility derived from polarization-correlation measurements.

Keywords: Quantum information, sensing, entanglement, teleportation

1. INTRODUCTION

The non-classical behavior of entanglement, e.g., as exhibited by non-local correlations in measurement outcomes, has been exploited previously for the development of unique computational and communication protocols. In particular, entanglement has served as an enabling resource in quantum key distribution protocols and as an essential resource in quantum computer architectures. The novel capabilities offered by these applications have encouraged investigation into entanglement-based solutions for other problems as well.

In this report, we explore how a sensing strategy using entanglement to validate the authenticity of a received signal improves sensor integrity. Verifying and maintaining the authenticity of a transmitted signal is important in many different sensing and security scenarios. In these proceedings, we discuss the particular case of an intruder crossing a physical perimeter, i.e., intrusion detection. However, other sensing and communication applications that require authenticated transmission are candidates for these ideas as well, e.g., locks and seals, eavesdropper detection.

Consider the concept of Fig. 1(a), in which a beam of light probes a physical perimeter. This 'laser tripwire' functions by transmitting light along the perimeter to a remote receiver. When the beam of light is blocked, its absence at the receiver signals an alarm. This sensing strategy is vulnerable, however, to an intercept-resend attack, i.e., an attack in which an intruder intercepts the incoming beam of light, accurately records its properties (to arbitrary precision), and resends a perfect duplicate to the receiver. This vulnerability arises in the context of a classical physical system because the intruder has the opportunity to reliably measure the classical information describing the light.[1]

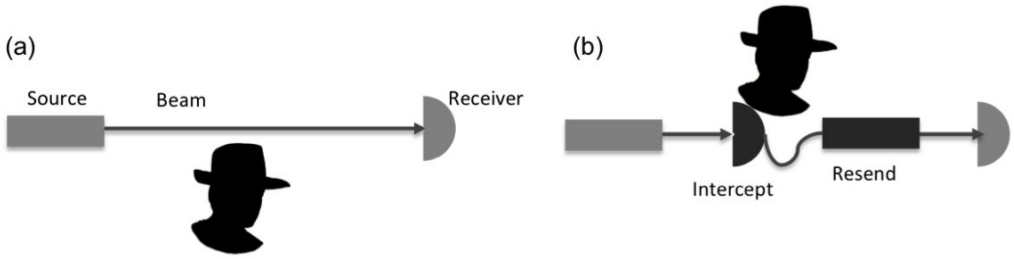

Fig. 1. (a) A laser tripwire operates by continuously monitoring the statistical properties of a beam transmitted from a source to a receiver; when the beam is broken, an alarm activates. (b) An intruder can spoof this classically defined sensor by intercepting the transmitted beam and resending a perfect duplicate to the receiver.

[1] While many laser/light sources exploit quantum effects, the macroscopic number of photons comprising the emitted light is adequately described using classical concepts, e.g., electromagnetic field modes.

Quantum Information and Computation VII, edited by Eric J. Donkor, Andrew R. Pirich, Howard E. Brandt,
Proc. of SPIE Vol. 7342, 73420H · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.820221

The vulnerability depicted in Fig. 1 requires the intruder to replicate the transmitted light. The ability to copy, or clone, information is a feature familiar to classical physical systems. This feature, however, does not exist within the context of quantum information systems. More specifically, the *no-cloning theorem* put forth by Wootters and Zurek states that an arbitrary quantum of information, e.g., an unknown qubit, cannot be reliably cloned due to fundamental restrictions imposed on measurement by the linearity of quantum mechanics [1].

Motivated by the no-cloning theorem, we propose an entanglement-based alternative to the transmission of classical information across a physical boundary that provides protection against the intercept-resent attack. As depicted in Fig. 2, this setup consists of a photon-pair entanglement source, in which one of the photons traverses the perimeter while the second remains secured near the source location. For convenience, we denote the transmitted photon as the *patrol photon* and the secured photon as the *guard photon*, and we refer to this setup as a *quantum fence*.

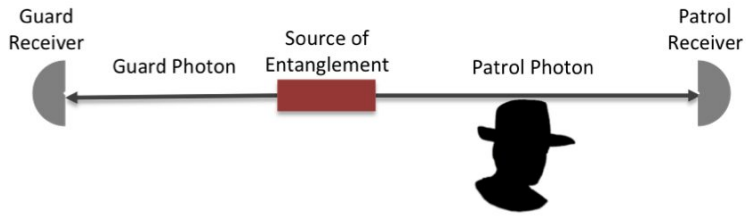

Fig. 2. A 'quantum fence' using entangled photons to detect intrusions: a photon-pair entanglement source generates a patrol photon that traverses the protected boundary while an accompanying guard photon remains at a secure location. The patrol and guard receivers measure correlations in the entangled degree of freedom, cf. the discussion for polarization-entangled photons, with an absence of entanglement indicating an intrusion.

Transmitting the patrol photon probes the boundary for the presence of an intruder. As in the classical case, if an obstacle is in the path, the photon is scattered or absorbed and the absence of a photon at the patrol receiver indicates an intrusion. A savvy intruder may intentionally block the patrol photon, however, and transmit an arbitrary doppelganger photon in its place, cf. Fig. 1(b). The intruder may also employ a measurement scheme that yields information about the state of the intercepted photon. Yet whether the intruder attempts to clone the patrol photon or not, the entanglement between the patrol and guard photon is destroyed due to the intruder's actions. The subsequent absence of entanglement between the guard and doppelganger photons then leads to a noticeable deviation in the joint measurement statistics registered by the receivers. While neither receiver alone can confirm the presence of an intruder due to the no-signaling condition, both receivers are assumed to communicate classically with a central monitoring (alarm) system that has access to both measurement records. Hence, an intruder's intercept-resend attack can be detected by the alarm system.

Before proceeding to a rigorous analysis of our proposal, we note that an intruder may also employ quantum techniques in a deception strategy, most notably, quantum teleportation. We examine quantum teleportation in Sec. 3, after analyzing the case of a quantum fence using single-mode, polarization-entangled photon pairs.

2. PROOF OF PRINCIPLE

We investigate more rigorously the arguments presented in the Introduction. First, we specialize the discussion to the case of polarization-entangled photon pairs, and we briefly summarize relevant properties of those states. Next, we analyze limits on the detection of the quantum state and the polarization-correlation visibility, and we derive the corresponding receiver operating characteristic (ROC) curves needed to diagnose sensor performance. Finally, we present ROC curves derived from experimental polarization-correlation measurements that demonstrate the feasibility of the quantum fence, and we interpolate these results to quantify the distance over which a quantum fence could operate.

2.1 Polarization-entangled photon pairs

The patrol and guard photons that underlie the quantum fence are required to be entangled in at least one degree of freedom, as it is entanglement that is used to verify the authenticity of the transmitted photons. A convenient form of photonic entanglement is polarization entanglement, which can be readily generated using the nonlinear optical process of spontaneous parametric down conversion (SPDC). An example SPDC setup yielding polarization-entangled photon pairs is shown in Fig. 3(a). The following arguments apply to both type-I and type-II SPDC; however, we restrict our analysis to the case of type-II SPDC, i.e., pairs generated with opposite polarizations, as this matches our experimental effort. Moreover, in order to simplify the analysis, we first consider photons generated in identical spectral and spatial modes but we lift this restriction in Sec. 3.

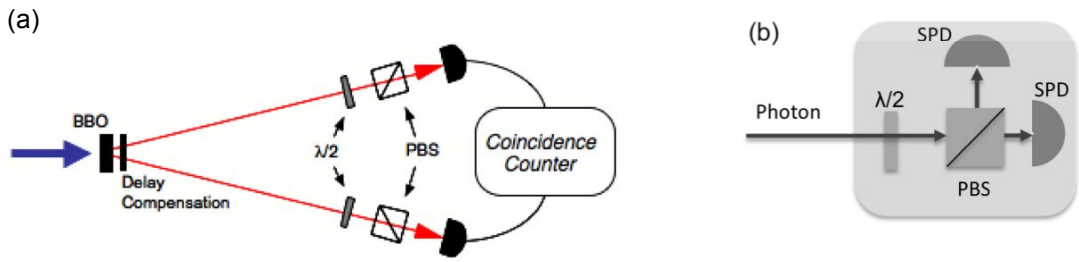

Fig. 3. (a) A polarization-entangled photon-pair source based on type-II SPDC: a nonlinear optical crystal (BBO) mediates the spontaneous down conversion of a high-frequency (blue) pump photon into a pair of lower frequency (red) photons, i.e., the patrol and guard photons. Conservation of energy and momentum requires that the photons satisfy the equations $\omega_{pump} = \omega_G + \omega_P$ and $\mathbf{k}_{pump} = \mathbf{k}_G^{\perp} + \mathbf{k}_P^{\perp}$, where ω_j and $\mathbf{k}_j^{\perp}$ denote the longitudinal frequency and the transverse momentum of the jth photon, respectively. (b) One of two polarization analyzers used for measuring polarization correlations between the patrol and guard photons: single-photon detectors (SPD's) at the output ports of the polarizing beam splitter (PBS) record changes in the detection rate as the λ/2 wave plate is rotated about the transmission axis.

The polarization-entangled state of a photon-pair generated by SPDC can be approximated by the Bell state[2]

$$\left|\varphi_{PG}\right\rangle \cong \frac{1}{\sqrt{2}}\left(\left|h_P, v_G\right\rangle + \left|v_P, h_G\right\rangle\right), \tag{1}$$

where the joint-polarization state $|h_P, v_G\rangle = |h_P\rangle\otimes|v_G\rangle$ is the direct product of single-photon horizontal and vertical polarization states $|h\rangle$ and $|v\rangle$, respectively, and the subscripts denote patrol (P) or guard (G) photons. This Bell state represents one of four maximally polarization-entangled biphoton states. Moreover, the polarization entanglement of this state can be expressed in terms of the experimentally measureable polarization-correlation visibility.[3] The visibility V quantifies the fringe contrast of the polarization-correlation spectrum obtained in either the h-v measurement basis or the conjugate diagonal-anti-diagonal (+/–) measurement basis.[4]

One of the two receivers required for evaluating the visibility consists of a polarizing beam splitter (PBS) and a λ/2 wave plate rotated about the transmission axis by an angle θ, cf. Fig. 3(b). A single-photon detector monitors each output port of the PBS and a record of the coincident counts is accumulated over a series of trials.[5] Assuming the PBS transmits horizontally polarized photons and reflects vertically polarized photons, the conditional probability for joint horizontal detection of the state (1) at the patrol and guard receivers is

$$R_C\left(\theta_P, \theta_G\right) = \sin^2\left(\theta_P + \theta_G\right), \tag{2}$$

where θ_P and θ_G are the corresponding analyzer angles. Measurements made in the conjugate +/– basis are obtained by rotating the incoming photons using a λ/2 wave plate. Moreover, those measurements yield a result similar to Eq. (2) apart from a π/2 phase shift. Hence, for the polarization-entangled state of Eq. (1), the empirical definition of the visibility as the contrast

$$V = \frac{R_C^{\max} - R_C^{\min}}{R_C^{\max} + R_C^{\min}}, \tag{3}$$

has a maximum of unity *in either basis*. In contrast, an unentangled state is predicted to have a visibility of zero *in at least one basis*, independent of whether the received state is a pure state, e.g., $|h_P, v_G\rangle$ or $|v_P, h_G\rangle$, or the classical mixture

$$\rho_{PG} = \frac{1}{2}\left(\left|h_P, v_G\right\rangle\left\langle h_P, v_G\right| + \left|v_P, h_G\right\rangle\left\langle v_P, h_G\right|\right). \tag{4}$$

[2] The validity of this approximation is determined by the pulse power and the magnitude of the second-order susceptibility.
[3] There is a one-to-one correspondence between the visibility and the von Neumann entropy of the state.
[4] Here the diagonal (+) and anti-diagonal (–) basis states are defined as $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.
[5] Single-photon detectors are not strictly required, but we invoke them here to simplify the presentation of our analysis.

Thus, measuring the visibility provides an experimental means to quantify polarization entanglement and, therefore, differentiate between an ensemble of polarization-entangled states and the unentangled states prepared by a would-be intruder.[6]

2.2 Entanglement detection

As noted in the preceding section, the difference in the polarization-correlation visibility between entangled and unentangled photon pairs is sufficient to distinguish between a patrol-guard state transmitted by the trusted entanglement source and a doppelganger-guard state prepared by an intruder. In this section, we expand our analysis to quantify the sensitivity and specificity of a sensor that detects entanglements using the visibility. We incorporate additive Gaussian noise into our description and we subsequently describe a binary decision problem that uses the measured visibility to discriminate between entangled and unentangled quantum states.

The binary decision problem is a formulation of (classical) detection theory for discriminating between two hypotheses based on an observed signal [2]. Here s_i represents the ith instance of the observed visibility and it is used to discriminate between the two hypotheses

$$H_0 : s_i = V_0 + n \quad \text{and} \quad H_1 : s_i = V_1 + n \,. \tag{5}$$

In Eq. (5), $V_0 = 0$ and $V_1 = 1$ are the visibilities predicted for unentangled and entangled photon pairs, respectively, and n is a zero-mean Gaussian random noise variable of variance σ^2. Considering M measurements, the corresponding log-likelihood ratio test is found to be

$$\sum_i^M \tilde{s}_i \underset{H_0}{\overset{H_1}{\gtrless}} \frac{\ln\lambda}{d} + \frac{d}{2} \tag{6}$$

with $\tilde{s}_i = s_i / \sigma M^{1/2}$ is the normalized sample data, λ defines the threshold for detection, and

$$d = M^{1/2}(V_1 - V_0)/\sigma \tag{7}$$

is the normalized displacement of the visibilities.

Discriminating between two known values in additive Gaussian noise leads to well-known results for the corresponding probability of detection Q_d and false alarm probability Q_0 [2];

$$Q_d = erfc(x_1) \quad \text{and} \quad Q_0 = erfc(x_0) \,. \tag{8}$$

Here the complimentary error function is defined as

$$erfc(y) \equiv (2\pi)^{-1/2} \int_y^\infty \exp\left[-x^2/2\right] dx \,, \tag{9}$$

and the limits for Q_0 and Q_d,

$$x_0 = (\ln\lambda)/d + d/2 \quad \text{and} \quad x_1 = (\ln\lambda)/d - d/2 \,, \tag{10}$$

are expressed in terms of the threshold λ and the dimensionless displacement d. These results can be conveniently represented by the receiver operating characteristic (ROC) curve, which demonstrates the trade-off in detection sensitivity and detection specificity using a parametric plot of (Q_0, Q_d) with respect to the detection threshold λ. We use the ROC curve to quantify our experimental results found in subsection 2.3 and Fig. 5.

From the analysis above, we conclude that measurements of the visibility are useful for quantitatively discriminating between entangled and unentangled photon pair states. Also, we note that this detection scheme need not know *a priori* the types of quantum states prepared by the intruder, i.e., the detector works just as well for pure states as mixed states.

---

[6] An unentangled pure state implies the intruder chose the 'correct' measurement basis, while a mixed state implies the conjugate basis was used. For the unentangled states above, the visibility vanishes when measured in the +/– basis.

2.3 Experimental demonstration

A polarization-entangled quantum fence can be experimentally realized using current quantum optical technology. In particular, SPDC-based entanglement sources are readily available for generating pulsed polarization-entangled photon pairs at rates up 250,000/pairs/sec/mW of pump power [3]. In addition, measurement of the polarization-correlation visibility in conjugate bases can be performed using an entirely passive experimental apparatus, i.e., on-the-fly reconfiguration is unnecessary. Moreover, both free-space and fiber-based sensors are candidates for development.

As a first demonstration of these principles, we have implemented a free-space quantum fence using a polarization-entanglement source. Specifically, an Argon laser operating at 351.1 nm pumped a 1-mm Beta Barium Borate (BBO) crystal with the crystal axis oriented for degenerate type-II SPDC at 702 nm. Horizontally and vertically polarized photons were emitted into different directions under the constraint of conservation of energy and momentum. By adjusting the orientation of the BBO crystal, the two emission patterns can be made to intersect. In this cross-ring configuration, one photon was emitted into each of the two spatial paths defined by intersecting emission cones [4]. A second, rotated BBO crystal immediately followed the first to compensate for group velocity differences between the down-converted photons. Each photon then traveled ~60 cm to a polarization analyzer, which consisted of rotated $\lambda/2$ wave plates, polarizing beam splitters, and single-photon detectors with the measurement basis for each analyzer station was chosen by the orientation of an inserted wave plate, cf. Fig. 3(a).

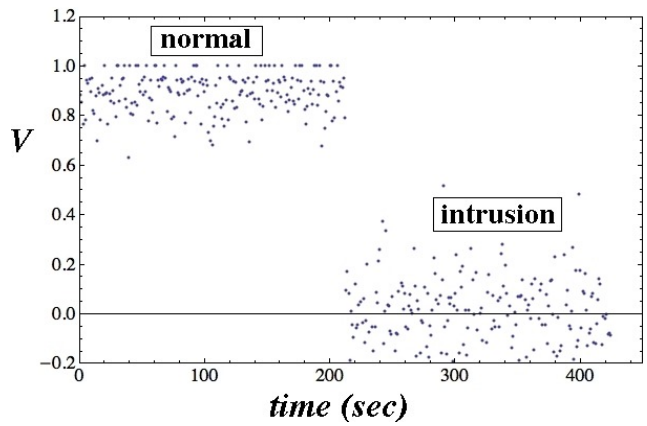

Fig. 4. A time series of visibility measurements made in the +/– basis for both entangled and unentangled photon pairs. Each time-point corresponds to a 1-s collection window for measuring the maximum and minimum coincident counts of Eq. (3). Subtraction of the relatively high dark count rate leads to some artifacts in the data, i.e., 'normal' visibilities of 1.0 and 'intrusion' visibilities less than 0.

The experiment monitored coincidence counts over a 1-second window and yielded maximal count rates of 188 pairs/sec and 35 pairs/sec in the *h*-*v* and the +/– bases, respectively.[7] The visibility was calculated by recording coincidence counts in the orientations expected to provide maxima and minima for both the *h*-*v* and the diagonal-anti-diagonal bases; the average corrected visibility in each basis was 0.9755±0.0169 (*h*-*v*) and 0.9139±0.0834 (+/–), respectively.[8]

Visibility measurements for unentangled photons were also performed. In this experiment, 1-second windows of stray photons were collected at each detector to simulate a maximally mixed state. A maximal rate of 7.7 pairs/sec was detected with an average visibility –0.01±0.160, which is consistent with the theoretical prediction of zero. The small negative contribution is an artifact of using the same analyzer orientations as in the entangled photon case; the maximum and minimum in the polarization correlation of the stray room light were probably at slightly different angles.

The ability of the quantum fence to sense an intruder's presence was tested by combining the visibilities acquired for entangled and unentangled light into the time series shown in Fig. 4. The visibility in the diagonal-anti-diagonal basis was plotted as a function of sample number with the first 213 points representing entangled pairs and the last 200 points representing unentangled light.

[7] The lower count rate in the +/– basis was due to the use of a single-mode fiber in front of one SPD.

[8] Visibilities presented in Fig. 4 were obtained by subtracting the average dark count rate of the detector(s) from the raw count rate. While much higher visibilities have been reported, the present results are entirely sufficient for the proof of principle sought here.

Taking the average visibility in the normal region as a baseline, the dimensionless displacement d was calculated with respect to the visibility observed in the transition or intrusion regions. Assuming a decision based on a standard deviation of $\sigma = 0.1$, the average dimensionless displacement in the intrusion region was $d \approx 7.3$ for a value $\langle V_0 \rangle = 0.16$ (one σ away from the mean). The corresponding ROC curve is shown in Fig. 5.

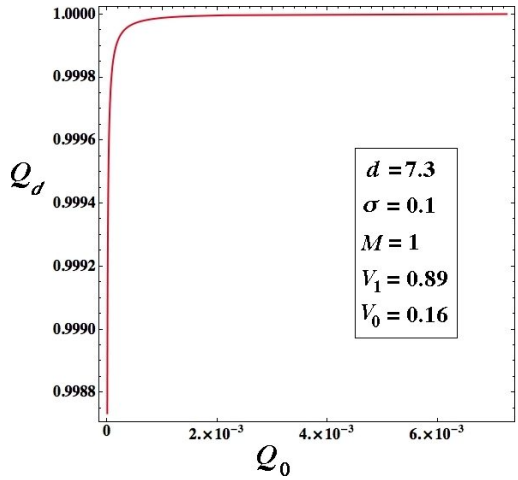

Fig. 5. Experimentally derived ROC curve for the polarization-entangled quantum fence: the probability for intrusion detection Q_d and the corresponding false alarm rate Q_0 are plotted for values of the dimensionless distance $d = 7.3$ and the standard deviation $\sigma = 0.1$ assuming a single measurement $M = 1$. For reference, note that for a threshold value of $\lambda = 1$ the experiment yields $Q_d \cong 0.9999$ and $Q_0 \cong 1.311 \times 10^{-4}$.

We have used the results obtained from our experimental setup, which transmitted each photon 0.6 m, to extrapolate the sensor's performance across longer distances. Specifically, we have accounted for atmospheric attenuation in our model of the patrol photon transmitted across a distance L.[9] At a wavelength of 800 nm, the effects of atmospheric attenuation can be as low as 0.2 dB/km under best weather conditions and as high as 20 dB/km in the presence of heavy mist [5].[10]

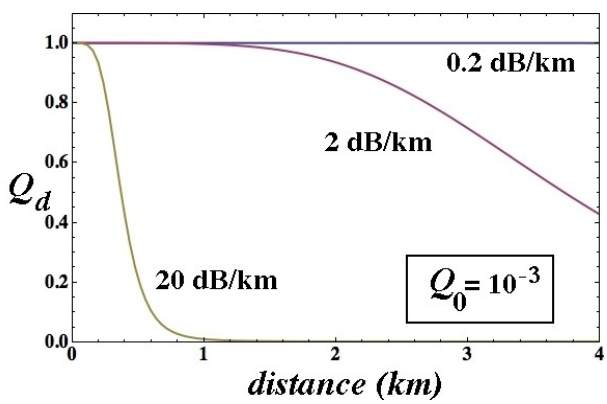

Fig. 6. Detection probability as a function of transmission distance and atmospheric attenuation: curves are labeled by the value of the attenuation factor and Q_d is calculated for the fixed false alarm rate of $Q_0 = 10^{-3}$.

Assuming the measurement error scales as (count rate)$^{-1/2}$, we express the standard deviation in terms of the transmission distance L and the atmospheric attenuation using the initial condition $\sigma = 0.0788$ at $L = 0.6$ m. A plot of the probability of detection Q_d with respect to transmission distance L is shown in Fig. 6 for a constant false alarm rate $Q_0 = 10^{-3}$. For the case of 0.2 dB/km loss, a high probability of detection (above 0.9999) is maintained across 3 km. For an attenuation of 20 dB/km, the transmission range for detection probability above 0.999 is approximately 120 m.

[9] We only model the reduction in count rate due to attenuation, neglecting losses in the coincidence counts due to decoherence.
[10] Our experiment generated photon pairs at 702 nm, but this wavelength can be tuned by changing the pump pulse wavelength and the properties of the nonlinear optical crystal.

Results presented in this section demonstrate that visibility measurements provide a viable means of authenticating the entanglement of a photon pair. Even with this modest experimental setup, a polarization-entangled quantum fence senses intrusions with a high probability of detection and a low false-alarm rate over a long range of transmission distances. A quantum fence using brighter, pulsed sources of polarization-entangled photon pairs, with count rates reported as high as 250,000 pairs/sec, could yield similar performance characteristics while requiring a collection window as short as 1 ms.

3. A QUANTUM-TELEPORTATION INTRUSION

In the previous section, we analyzed the behavior of a quantum fence based on single-mode, polarization-entangled photon pairs. We showed that when an intruder attempts to measure and clone the polarization state of the patrol photon, the destruction of entanglement leads to a noticeable change in the measurement statistics recorded by the receivers. In this section, we consider the case that the intruder, aware that the transmitted patrol photon is entangled with the secured guard photon, uses quantum teleportation to transfer the entangled state of patrol photon to a doppelganger photon.[11]

For the case of polarization-entangled photon pairs, the intruder may employ a pair of entangled doppelganger photons, as shown in Fig. 7. Then, by performing a Bell-state measurement on the patrol photon and the doppelganger photon, the intruder could prepare an entangled state between the secured guard photon and the second, transmitted doppelganger photon. This form of teleportation, known as entanglement swapping, preserves the entanglement generated by the source.

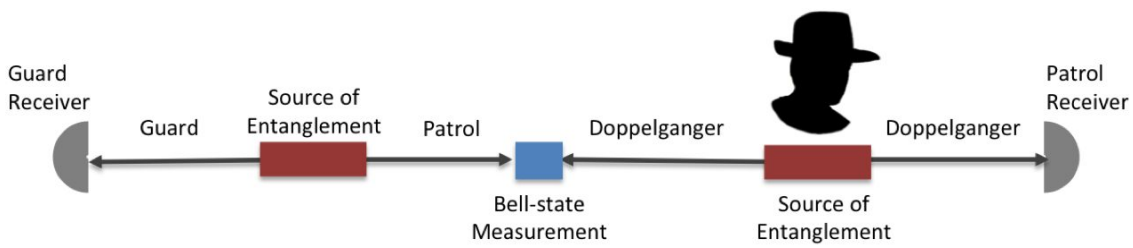

Fig. 7. A quantum-teleportation intrusion attack: an entangled pair of doppelganger photons is used to perform quantum teleportation, or entanglement swapping, with the patrol-guard photon pair. The patrol photon and one of the doppelganger photons are subjected to a Bell-state measurement (BSM), the outcome of which projects the guard and second doppelganger photons into a polarization entangled state.

Yet the description above overlooks several considerations that may undermine the quantum teleportation attack. The foremost concern is that when the Bell-state measurement succeeds, the guard and doppelganger photons are randomly projected into a state chosen from the set of four orthonormal Bell states.[12] As each of the sampled entangled states yields a distinct set of measurement outcomes, the visibility derived from measurements made on a series of these randomly prepared states would be zero.

It is possible for the intruder to locally correct the action of Bell-state measurement; however, doing so would require the intruder to delay the transmission of the second doppelganger photon until after the measurement of the patrol photon had occurred. When the patrolled perimeter is the shortest distance between two points (a straight line), then this delay in transmission is, in principle, always detectable by the receiver. On the other hand, if the patrol photon takes a less direct route, e.g., by patrolling a perimeter that turns or curves, then it is possible for the intruder to 'cut corners' and 'make up' time loss in implementing these corrective actions.

Consequently, the above objections notwithstanding, we extend our analysis of the quantum fence to consider the case that the intruder may employ quantum teleportation. Moreover, we propose a counterattack to quantum teleportation that effectively limits the ability of the intruder to swap entanglement between photons. Our counterattack results from considering spectrally multimode, polarization-entangled photon pairs. Briefly, we examine the visibility of the received states before and after quantum teleportation while assuming the intruder has applied the appropriate local unitary operation to complete the teleportation protocol. Furthermore, we examine how the polarization-correlation visibility behaves following teleportation with respect to the characteristics of the spectral modes and spectral entanglement.

[11] We further assume the intruder has accurate knowledge about the transmission of the patrol photon, e.g., path, bandwidth, center frequency, timing information, etc.
[12] Aside from its probabilistic outcome, there is no linear optical form of the BSM that succeeds deterministically.

3.1 Spectrally multimode, polarization-entangled photon pairs

The spectrally multimode analog of the polarization-entangled state presented in Eq. (1) is

$$\left|\varphi_{23}\right\rangle = \frac{1}{\sqrt{2}}\int d\omega \int d\omega' \left[f(\omega,\omega')\left|h_P(\omega), v_G(\omega')\right\rangle + g(\omega,\omega')\left|v_P(\omega), h_G(\omega')\right\rangle \right] \tag{11}$$

where $f(\omega,\omega')$ and $g(\omega,\omega')$ are normalized joint spectral amplitudes and $|h_P(\omega)\rangle = |h_P\rangle\otimes|\omega_P\rangle$ is a horizontally polarized patrol photon in the spectral eigenstate having frequency ω, etc. These states are typical of the polarization-entangled biphoton states prepared by SPDC when a pulsed pump pulse initiates the down-conversion process [6].

The specific forms of the joint spectral amplitudes in Eq. (11) are strongly dependent on the type of SPDC, as well as the material properties of the nonlinear optical medium being used. Furthermore, the joint spectral amplitudes need not be identical or even individually separable with respect to frequency. The joint spectral amplitude is, however, generally decomposable as

$$f(\omega,\omega') = \sum_{n=0}^{\infty} \lambda_n^{1/2} u_n(\omega) v_n(\omega') \tag{12}$$

where λ_n is the nth Schmidt coefficient and the Schmidt modes u_n and v_n form a complete biorthonormal set for the joint spectral Hilbert space.[13] The joint amplitude $g(\omega, \omega')$ is likewise represented by a Schmidt decomposition. For the case that Eq. (12) has more than one term in the summation, then the joint spectral amplitude is said to be spectrally entangled, and this spectral entanglement can be quantified in terms of the Schmidt number K defined by

$$K^{-1} = \sum_{n=0}^{\infty} \lambda_n^2 \,. \tag{13}$$

The Schmidt number has a minimum of $K = 1$ (an unentangled joint spectrum) and grows monotonically as the number of modes increases.

Analogous to the discussion in Sec. 2.1, the polarization entanglement of a spectrally multimode state may be quantified in terms of the polarization-correlation visibility. An analysis of the polarization-correlation experiment finds the theoretical maximum for the visibility is given by [7]

$$V = \mathrm{Re}\int d\omega \int d\omega' f(\omega,\omega') g(\omega,\omega')^* \,, \tag{14}$$

which is unity only when the joint spectral amplitudes are identical. Moreover, the maximal visibility is independent of the spectral entanglement, a fact which we make use of below.

3.2 Quantum teleportation of the polarization state

Quantum teleportation of a spectrally multimode, polarization-entangled biphoton state has been treated before [8]. In the current context, we assume that two pairs of photons are each prepared in a state of the general form (11), with the first state representing the patrol-guard (*PG*) pair and the second state representing the doppelganger *(DD)* pair. The patrol photon and one of the doppelganger photons are then subjected to a polarization-based Bell-state measurement, which is accomplished by interfering the two photons at a 50:50 beam splitter and analyzing each output mode, e.g., in the *h*-*v* basis. Conditioned upon the coincident detection of two photons, the resulting reduced, polarization density matrix of the guard and second doppelganger photons is [8]

$$\tilde{\rho}_{GD} = \frac{1}{2}\left(\left|h_G, v_D\right\rangle\left\langle h_G, v_D\right| + G\left|h_G, v_D\right\rangle\left\langle v_G, h_D\right| + G^*\left|v_G, h_D\right\rangle\left\langle h_D, v_G\right| + \left|v_G, h_D\right\rangle\left\langle v_G, h_D\right| \right), \tag{15}$$

where the off-diagonal coherence term

$$G = \int d\omega \int d\omega' \int d\omega'' \int d\omega''' f_{GP}(\omega,\omega''') g_{DD}(\omega''',\omega')^* g_{GP}(\omega,\omega'')^* f_{DD}(\omega'',\omega') \tag{16}$$

[13] Normalization of $f(\omega,\omega)$ implies $\sum_n \lambda_n = 1$

represents the overlap of the spectral amplitudes. The real component of G yields the visibility expected for the guard-doppelganger (GD) photon pair, i.e.,

$$V_{GD} = \mathrm{Re}\, G \,. \tag{17}$$

As noted in Eq. (14) above, the initial patrol-guard state yields maximal visibility when the joint spectral amplitudes are identical. Assuming this relationship for both the PG and DD pairs, we insert the Schmidt decomposition of Eq. (12) into Eq. (16) to find the resulting coherence. We further simplify our analysis to the case that the photons produce identical marginal spectra, which gives the best possible visibility of the GD pair. Specifically, the visibility following teleportation is inversely proportional to the spectral entanglement carried by the joint spectral amplitude, i.e.,

$$V_{GD}^{\max} = K^{-1} \,. \tag{18}$$

In the absence of spectral entanglement, $\lambda_n = \delta_{n0}$, $K = 1$, and the visibility of the swapped GD pair matches the unit visibility of the original pair, cf. Eq. (14). However, in the limit of strong spectral entanglement, e.g., when $\lambda_n \approx 1/N$ and $K^{-1} \approx N$ (with N an effective number of spectral modes), the visibility of the GD pair can be much less than the original, expected visibility. Consequently, when the initial spectral entanglement between the patrol-guard photons is high, an intruder's attempts to use quantum teleportation can be detected based on the decrease in the observed visibility.

We emphasize that this last approach to verifying the authenticity of the polarization-entangled photon pair does require any knowledge about discrepancies in the time of arrival of the patrol or doppelganger photons. Hence, even when the intruder has sufficient time to implement teleportation, the visibility it generates will be poor and, therefore, the intruder's presence will be detectable.

3.3 Beyond quantum teleportation of the polarization state

We conclude our analysis of a quantum teleportation intrusion by noting that the arguments presented above assume the intruder attempts only to teleport the polarization state of the entangled guard-patrol photon pair. However, this does not exhaust the intruder's possibilities. In particular, the intruder may attempt to teleport the full quantum state of the patrol photon. This action, which would require teleporting all the degrees of freedom of a single photon, is the ideal attack for the intruder, assuming no discernable delay in the photon arrival time is introduced.

We have not analyzed this full implementation of teleportation in detail because the capability of 'total teleportation' has not yet been demonstrated. Rather, we have recently reported a proposal for teleporting the spectral, spatial, and polarization degree of freedom of a single photon, and we believe that implementing those ideas is a near term possibility [9]. However, in its current form, our proposal for total teleportation would not appear sufficient to spoof the receiver, as it depends on a probabilistic Bell-state measurements (based on nonlinear optics) and a series of up-conversion events as the local corrective action. Future technological developments may improve that proposal, but even then, the fact that making and detecting entanglement is much easier than swapping entanglement gives users of the quantum fence a new advantage over would-be intruders.

4. CONCLUSIONS

We have presented an application of quantum entanglement for the detection of intrusions across a physical perimeter. The quantum fence verifies the initial entanglement generated between a secured guard photon and a transmitted patrol photon exists when the patrol photon reaches the distant receiver. We have analyzed the sensitivity and specificity of the quantum fence using the polarization-correlation visibility as a measurement of polarization entanglement. We have implemented these ideas in a proof-of-principle experiment that demonstrated excellent sensing characteristics, as shown by the ROC curve in Fig. 5. We have modeled the sensor performance for when the patrol photons traverse longer distances and suffer atmospheric attenuation. The results suggest the quantum fence could operate under a variety of conditions. Finally, we have analyzed the potential that an intruder could use quantum teleportation to spoof the patrol receiver and we have concluded that by introducing entanglement in a secondary degree of freedom (spectral entanglement) that a limit can be placed on the maximal visibility the intruder can prepare.

The submitted manuscript has been authored by a contractor of the U.S. Government under Contract No. DE-AC05-00OR22725. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

REFERENCES

[1] Wootters, W. K. and Zurek, W. H., "A single quantum cannot be cloned," Nature 299(5886), 802-803 (1982).

[2] van Trees, H. L., [Detection, Estimation, and Modulation Theory Part 1], John Wiley & Sons, New York (2001).

[3] Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T., and Zeilinger, Z., "A wave-length tunable fiber-coupled source of narrowband entangled photons," Opt. Express 15, 15377-15386 (2007).

[4] Kwiat, P. G., Mattle, K., Weinfurter, H., and Zeilinger, A., "New high-intensity source of polarization-entangled photon pairs," Phys. Rev. Lett. 75(24), 4337-4341 (1995).

[5] Dusek, M., Lutkenhaus, N. and Hendrych, M., "Quantum Cryptography," Progress in Optics 49, ed. E. Wolf, Elsevier, New York, (2006).

[6] Grice, W. P. and Walmsley, I. A., "Spectral information and distinguishability in type-II down-conversion with a broadband pump," Phys. Rev. A 56(2), 1627-1634 (1997).

[7] Humble, T. S., and Grice, W. P., "Spectral effects in quantum teleportation," Phys. Rev. A 75, 022307 (2007).

[8] Humble, T. S., and Grice, W. P., "Effects of spectral entanglement on polarization-entanglement swapping and type-I fusion gates," Phys. Rev. A 77, 022312 (2008).

[9] Humble, T. S., Bennink, R. S., and Grice, W. P., "Total teleportation of a single-photon state," Proc. SPIE 7092 Quantum Communications and Quantum Imaging VI, 7092V (2008).