Intrusion Detection with Quantum Mechanics: A Photonic Quantum Fence

Travis S. Humble, Ryan S. Bennink, and Warren P. Grice
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA

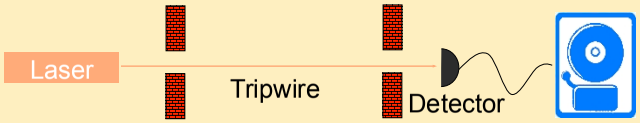
Israel J. Owens
Los Alamos National Laboratory
Los Alamos, New Mexico, USA

ABSTRACT

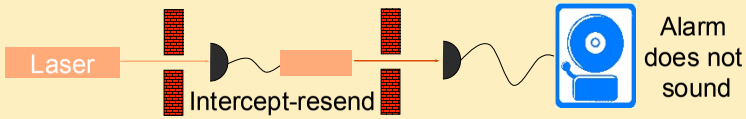
We describe the use of quantum-mechanically entangled photons for sensing intrusions across a physical perimeter. Our approach to intrusion detection uses the no-cloning principle of quantum information science as protection against an intruder's ability to spoof a sensor receiver using a 'classical' intercept-resend attack. 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.

PROBLEM ADDRESSED

Intrusions can be detected by monitoring transmission of a probe beam, e.g., a laser 'trip wire', where absence of the probe at a receiver signifies an intrusion.



But an intruder can spoof this sensor by sending a doppelganger beam that perfectly replicates the probe.

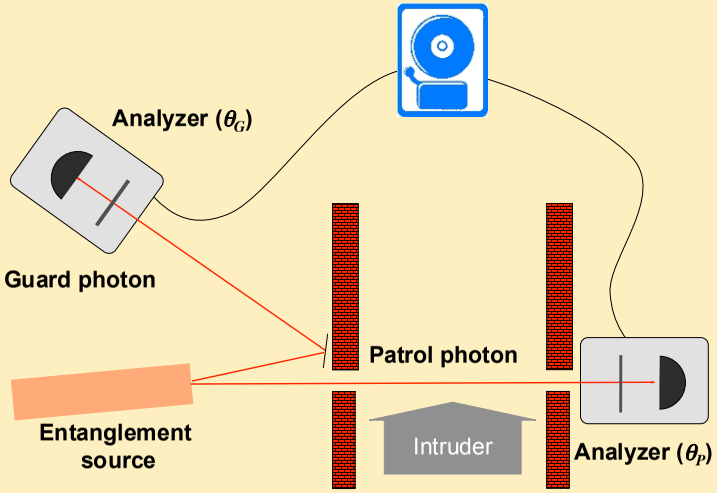


Validating the authenticity of a probe signal is fundamental to many sensing applications, including fences, locks, seals, surveillance and eavesdropper detection methods.

SOLUTION PROPOSED

The no-cloning principle of quantum information science prohibits an intruder from reliably copying an arbitrary qubit of information. This 'quantum fence' against intrusion can be implemented by transmitting a patrol photon across the perimeter while retaining an entangled guard in a secure location. The absence of entanglement between received particles indicates an intruder's presence. This additional layer of security could complement existing methods for monitoring the state of sensor or communication channel.

CONCEPT DIAGRAM



A source of entangled photons transmits a patrol photon across a perimeter to a distant receiver (analyzer) and sends the guard photon to a second, secure receiver. An alarm system monitors the entanglement, and the alarm sounds if the measured entanglement drops below a threshold value.

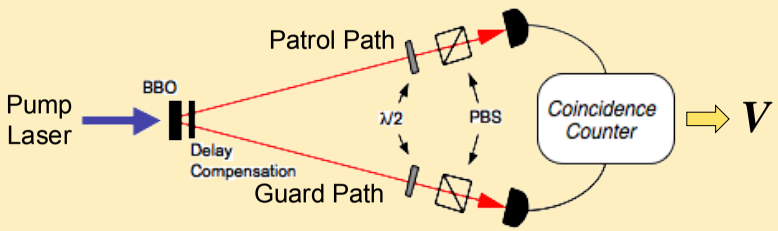
Intrusion Detection with Quantum Mechanics: A Photonic Quantum Fence

Travis S. Humble, Ryan S. Bennink, and Warren P. Grice
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA

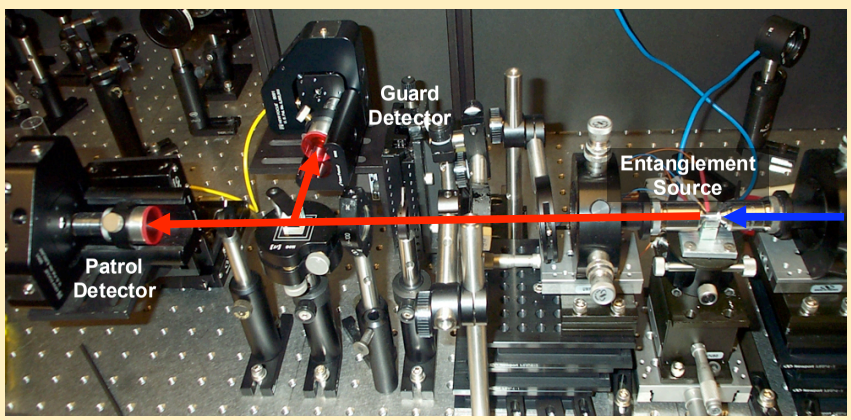
Israel J. Owens
Los Alamos National Laboratory
Los Alamos, New Mexico, USA

PROOF OF PRINCIPLE

Entangled photon pairs were generated using spontaneous parametric down conversion (SPDC). Non-local correlations in polarization were quantified using the visibility V, i.e., the contrast in the interference fringes.



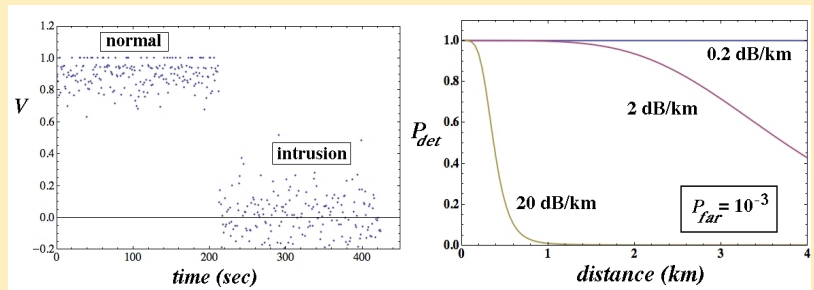
Schematic illustrating the role of SPDC in the production of patrol and guard photon pairs. The photon polarization states is monitored by a coincidence counter.



Generation of polarization-entangled photon pairs using a cross-ringed, type-II SPDC configuration with a 1-mm BBO crystal pumped by a cw Ar^+ laser operating at 351.1 nm.

SENSOR PERFORMANCE

A ROC curve was derived from visibilities for normal and intrusion cases. Performance over longer transmission distances was modeled assuming atmospheric attenuation.



(Left) Measured visibilities for normal and intrusion scenarios. Samples collected in a 1-s window at a max rate of 35 pairs/s. (Right) Probability for detection at constant false alarm rate modeled with respect to transmission distance. Conditions here: 0.2 dB/km best weather, 2 dB/km light rain, 20 dB/km heavy mist.

SUMMARY

Intrusion detection using entangled photons was proposed and demonstrated. Whereas an intruder could spoof a classical 'trip wire' sensor, a photonic quantum fence can discern between between normal and intrusion scenarios. This concept should prove useful anywhere the integrity of a transmitted or probe signal is paramount, e.g., in perimeter protection, eavesdropper detection, and containment and surveillance technologies.

ACKNOWLEDGEMENTS This poster has been authored by a contractor of the U.S. Government under Contract No. DE-AC05-00OR22725. Accordingly, 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. This material is based on work supported by the Defense Advanced Research Project Agency,