Title: "*Secure Submarine Communications*"

Author: Marco Lanzagorta, ITT Corporation

Abstract:
Secure communications with submarines are critical to maintain our nuclear deterrence capability and to enact the Network Centric Warfare doctrine of naval operations. As a consequence, the deployment of efficient and secure communication links with submarines is one of the greatest technological challenges presently confronted by the US Navy. Indeed, due to their strategic and tactical importance, submarine communications require perfectly secure cryptographic protocols such Vernam (one-time) pads. Clearly, this solution not only presents the problem of efficient distribution of secret keys before the submarine departs the base, but also imposes a limit on the number of secret keys available onboard a submarine during prolonged seaborne missions. Furthermore, because of absorption and scattering processes, the underwater environment is very challenging for any type of communication systems. Existing systems employ Vey-Low-Frequency (VLF) and Extremely-Low-Frequency (ELF) radio communications because waves of these frequencies can partially penetrate a body of water. However, these systems impose severe operational limitations: these are extremely low bandwidth one-way systems that require towed antennas or buoys, and submarines need to steer specific courses and reduce their speed.

In recent years, ITT Corporation has been exploring the possibility of provably secure communications with submerged submarines using quantum key distribution over an underwater optical channel. To this end, we have explored the feasibility of optical communication links connecting satellites with submarines submerged below the thermocline layer (strategy employed to avoid acoustic detection by passive or active sonar systems). In addition, we have considered the possibility of an underwater quantum channel and its potential benefits for strategic communications with submarines. We have developed analytical descriptions of attenuated quantum channels based on quantized electromagnetic fields in material media. We have also performed numerical simulations that show the performance of the BB84 quantum key distribution protocol on different types of oceanic water.

Emerging Technology Space: Submarine Communications and Network Centric Warfare

Class of Cryptographic Requirements: Quantum Key Distribution