Trusted Relay Node Networking
Los Alamos National Laboratory (LANL)

Raymond Newell PhD
Cybersecurity for Energy Delivery Systems Peer Review
November 6-8, 2018
Summary: Trusted Relay Node Networking

Objective
• We will demonstrate that a succession of quantum-secured links, joined by relay nodes located in physically-secured locations, can overcome existing distance limitations.

Schedule
• Start Feb 2018, end Feb 2021
• Field tests:
  • Q1 2019 (TBD)
  • Q1 2020
  • Q4 2020
• Demonstrate interoperability of different Quantum Communication systems
• Bring security benefits of quantum communications to long-range links
• Show that quantum communication systems can exchange cryptographic key material over different physical-layer implementations

Total Value of Award: $ 400,000
Funds Expended to Date: 19.7%
Performer: Los Alamos National Laboratory
Partners: Oak Ridge National Laboratory, EPB
Advancing the State of the Art (SOA)

• Existing quantum links are limited in range to ~100 miles, in practice much less. We will demonstrate that a succession of such links, joined by relay nodes located in physically-secured locations, can overcome this limitation.

• Nationwide deployment of quantum technologies will require interoperable systems from multiple vendors. An operator must be able to “plug-and-play” a quantum device without regard for the underlying physics. It is essential to deploy quantum technologies without the undue burden on operators that would result from disparate technologies.
The primary objective of this effort will be to develop and demonstrate a three-node network extending quantum communications by building and deploying trusted relay nodes. This work will address two existing impediments to widespread implementation of quantum communications technology: limitations on the maximum link range, and non-interoperable implementations. By developing and implementing a systems-level approach to interoperable trusted relay nodes, we will bring the security assurances of quantum communication systems to long-haul distances.
Challenges to Success

Lack of existing Quantum Communication standards

- There are several competing standards for classical key management and authentication, and very many homebrew solutions. But no standards are dedicated to quantum comms.

- The team has agreed on a standard keyfile format, with metadata in a header, 256-bit keys, and checksum

Sensitive equipment in a harsh environment

- Quantum signals are inherently weak, so detection equipment must be sensitive

- Reliable operation in a substation environment is challenging: thermal range, vibration, and EMF can be challenging

- The team includes seasoned engineers with decades experience in design for harsh environments
Major Accomplishments

- Site visit and technical working meeting, July 2018

Photographs of optical fiber patch panel at EPB’s Riverside and Tennessee Tech power distribution substations. Duplex SMF28e+ single mode fiber with LC terminators.

- Agreement on keyfile data format
Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Industry acceptance will be pursued by
  1. Establishing strong IP portfolio (13 granted, 26 pending at last count)
  2. Licensing agreements with commercialization parts (negotiations ongoing)
  3. Cooperative Research and Development Agreements with partners to transition technology out of LANL
  4. Mature products available for sale to asset owners
Next Steps for this Project

In December 2018 or January 2019 (exact date TBD) we will transport our Quantum Hardware Security Module system to EBP for integration and testing with a comparable system delivered by ORNL.
80 km range would enable 70% of ESNet’s links

This is a histogram of all 734 fiber spans that comprise ESnet, sorted according to span length.

A cumulative histogram of the same data set shows that 70% of all spans are 80km or less.

Data courtesy of Christopher Tracy, ESnet LBNL. Thanks to Sean Peisert.
A graded approach

This talk

**Trusted Relay Nodes**
- Fully quantum links
- Classical relay
- Building is assumed to be secure

Next talk

**Trustworthy Relay Nodes**
- Fully quantum links
- Classical relay
- Classical Crypto + Physically Unclonable Functions
- No secure building needed

**Quantum Repeaters**
- Fully quantum links
- Fully quantum relay
- Outside of scope for OE (but very worthwhile!)

Vulnerability

Cost