Oak Ridge National Laboratory

ORNL Quantum-Conventional Network Testbed

Nageswara S. V. Rao, Muneer Alshowkan, Joseph C. Chapman, Mariam Kiran, Hsuan-Hao Lu, Joseph M. Lukens, Alexander Miloshevsky, Nickolas A. Peters

Oak Ridge National Laboratory

ORNL is managed by UT-Battelle LLC for the US Department of Energy

Sponsored by Department of Energy
Advanced Scientific Computing Research office

U.S. DEPARTMENT OF ENERGY

U.S. DEPARTMENT OF ENERGY | Office of Science

4th Global Research Platform Workshop, October 9-10, 2023
co-located with 19th IEEE International Conference on e-Science, Limassol, Cyprus

Outline

1. Introduction
2. QNET Testbed
   - quantum and conventional connections
   - telescoping fiber loops and spools
3. Testbed Experiments
   - co-propagating noise characterization
   - two-mode squeezing and co-existence
   - entanglement distribution measurements
   - throughput and capacity estimates
   - IPSec authentication using QKD keys
4. Conclusions

Quantum and Conventional Networking

Quantum networks and **Quantum Internet**:

- promise game-changing capabilities for science discovery and facilities, quantum computing, higher throughput, and cyber security areas.

The Critical Connection: Practically and fundamentally, quantum networking is inextricably tied to conventional networking:

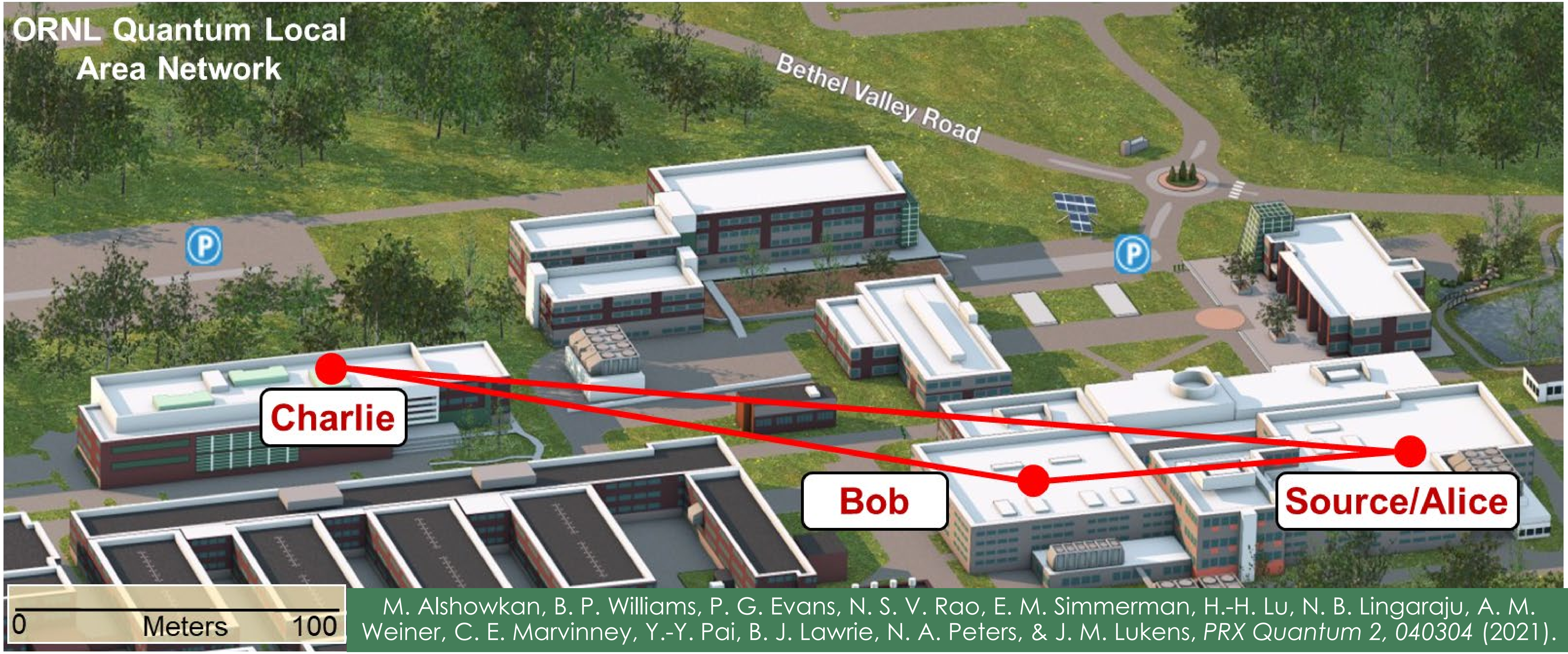
- **practical**: conventional telecom fiber infrastructure is critical to support Quantum Internet deployments
  - it is too early, expensive and unnecessary to build separate fiber infrastructure
  - control and management of quantum network devices rely on conventional
- **foundational**: critical protocols such as teleportation require both networking capabilities operating in concert

- **Example:** Need components that can send quantum signals over conventional telecom C-band fiber around 1500nm, while interacting with end systems

- **Need testbeds**: For capabilities to co-design, co-develop and co-test quantum-conventional networking technologies
  - Complement analytical and simulation approaches

ORNL Quantum Local Area Network (QLAN)

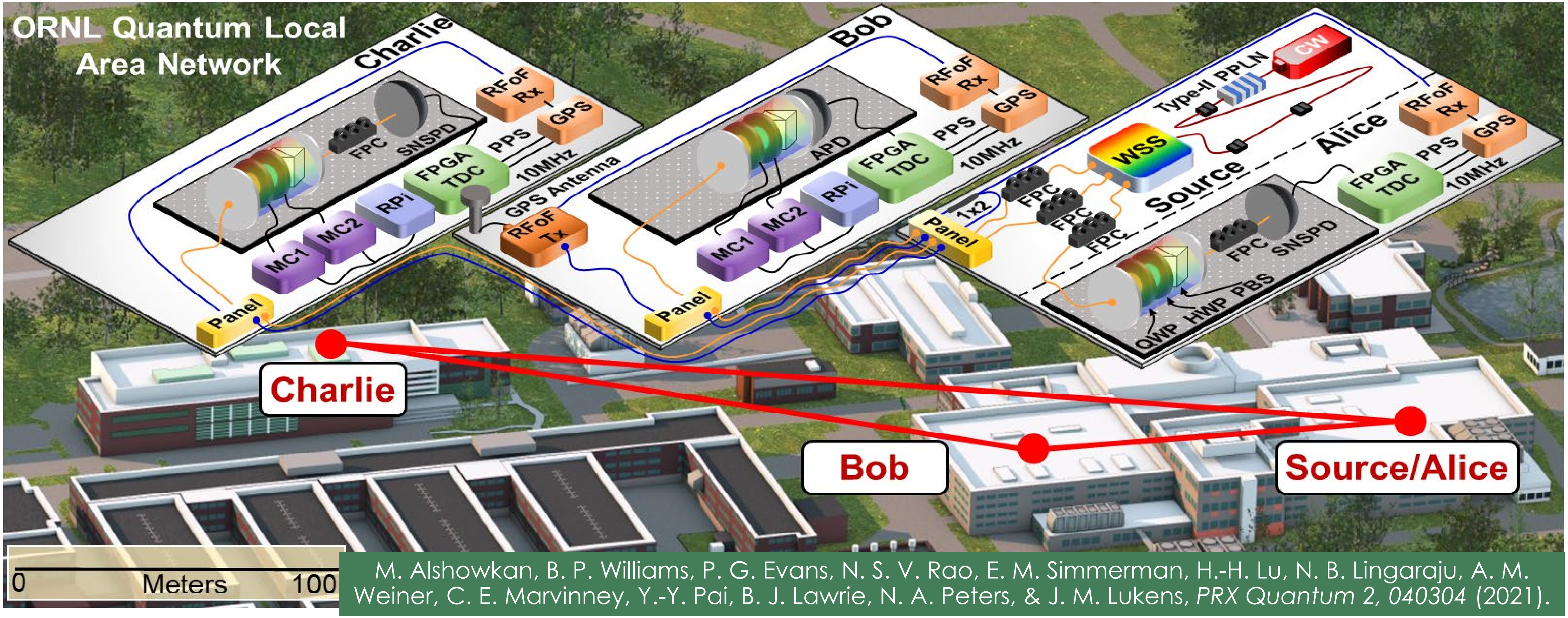
- Implemented flex-grid entanglement paradigm in deployed network.
- Receivers for all users are spatially distributed, requiring tight timing synchronization



M. Alshowkan, B. P. Williams, P. G. Evans, N. S. V. Rao, E. M. Simmerman, H.-H. Lu, N. B. Lingaraju, A. M. Weiner, C. E. Marvinney, Y.-Y. Pai, B. J. Lawrie, N. A. Peters, & J. M. Lukens, *PRX Quantum 2, 040304* (2021).

ORNL Quantum Local Area Network (QLAN)

- Implemented flex-grid entanglement paradigm in a deployed network
- Receivers for all users are spatially distributed, requiring tight timing synchronization



M. Alshowkan, B. P. Williams, P. G. Evans, N. S. V. Rao, E. M. Simmerman, H.-H. Lu, N. B. Lingaraju, A. M. Weiner, C. E. Marvinney, Y.-Y. Pai, B. J. Lawrie, N. A. Peters, & J. M. Lukens, *PRX Quantum 2, 040304* (2021).

SNSPD: Superconducting Nanowire single photon detector
APD: Avalanche photon diode
PPLN: Periodically polled lithium niobate

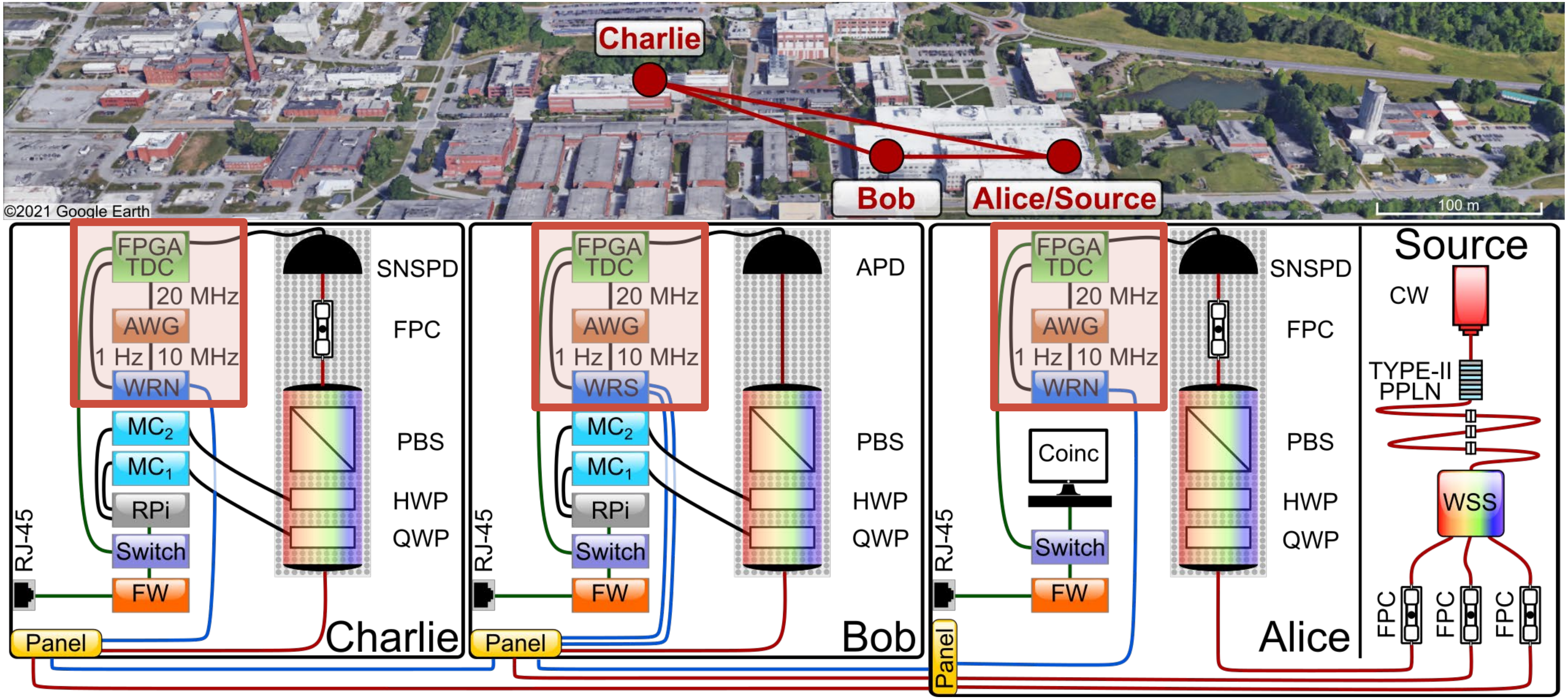
WSS: wavelength selectable switch
QWP: quarter wavelength plate
HWP: half wavelength place

FPC: fiber polarization controller
PBS: polarizing beam splitter

OAK RIDGE National Laboratory

Synchronizing QLAN with White Rabbit

- Improved QLAN that solves time synchronization in a **scalable** architecture
- Using commercial off the-shelf White Rabbit components and redesigned the time taggers

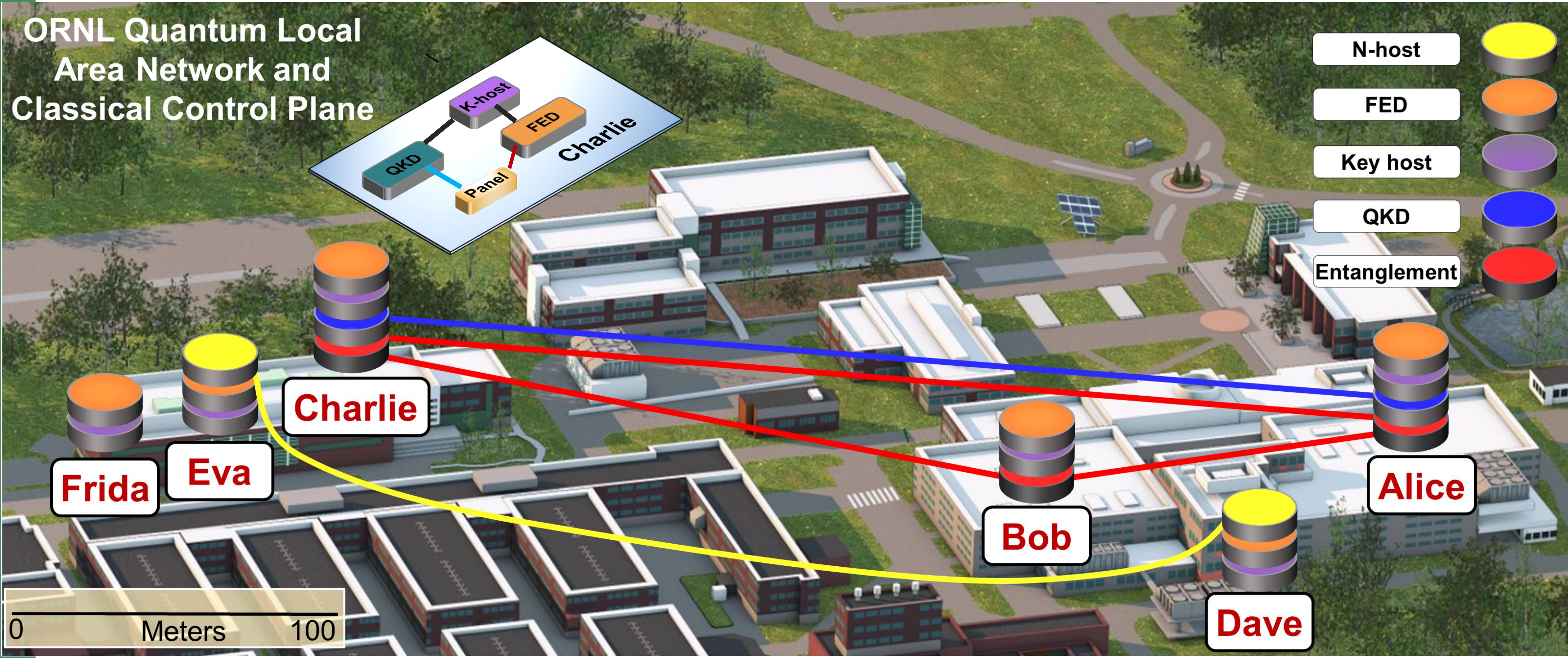


AWG: arbitrary waveform generator
FW: Firewall

MC: motion controller
WRN: white rabbit controller

RPi: Raspberry Pi
WRN: white rabbit controller

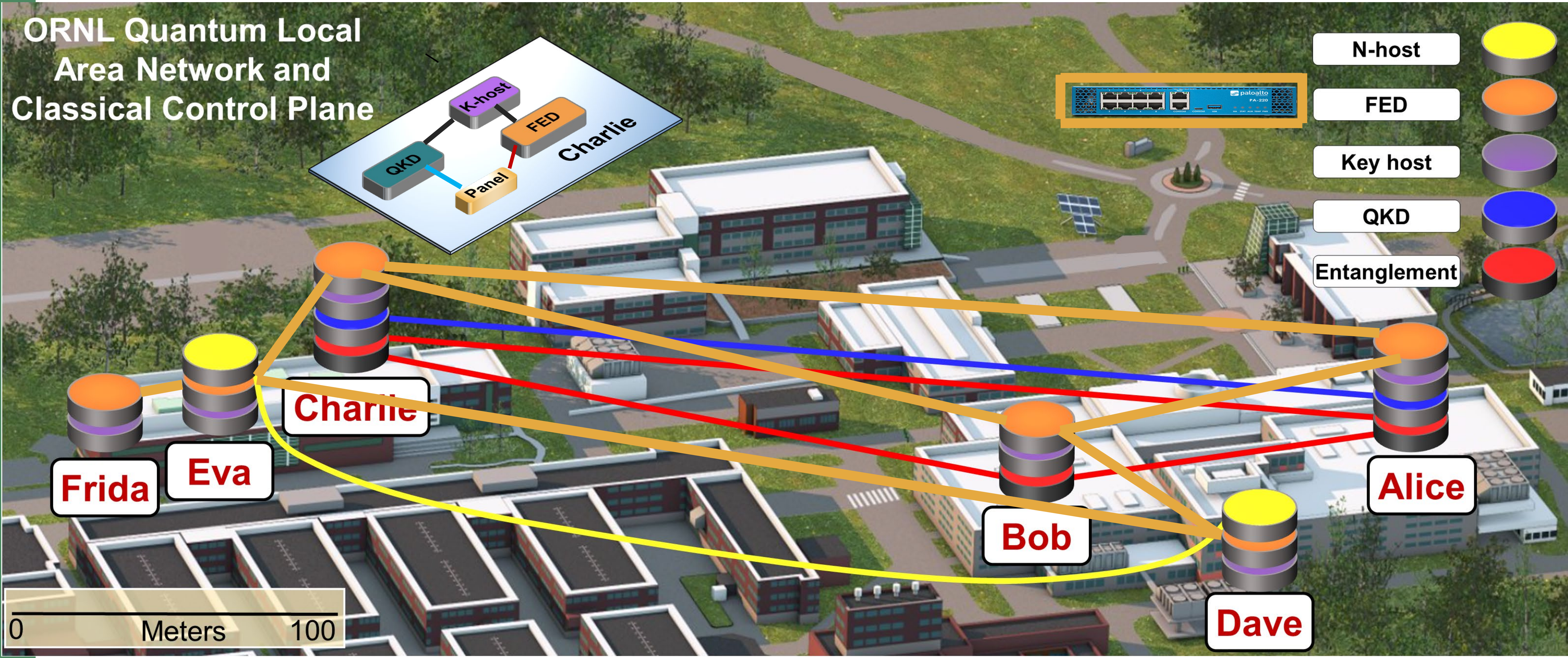
ORNL QLAN Quantum and Conventional Networking



Dave: Critical quantum-conventional node

ORNL QLAN quantum and conventional networking

Control Plane Implemented using Palo Alto PA-220 devices

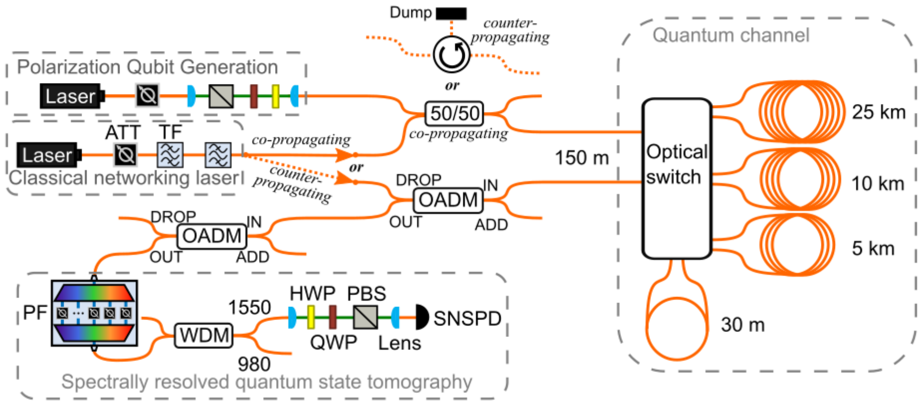


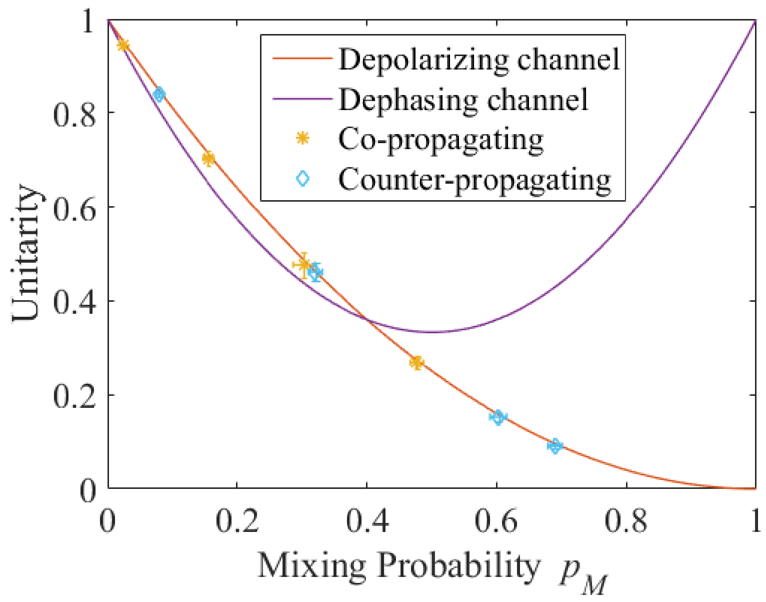
OAK RIDGE National Laboratory

FED: Firewall and Encryption Device (FED): PA-220

Noise Characterization of Co-Propagating Signals

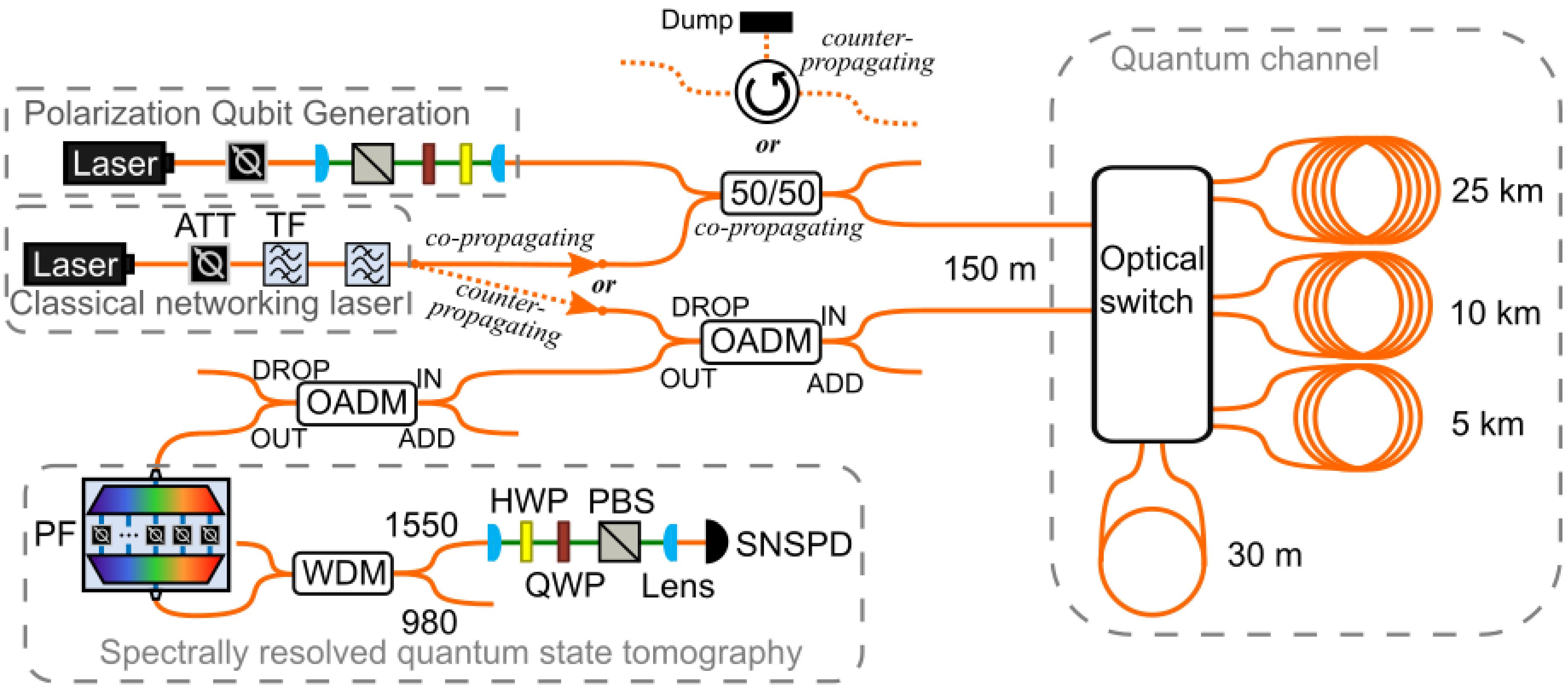
- Developed spectrally resolved quantum process tomography measurement system
- Characterized coexistence noise for co-propagating and counter-propagating channels of varying lengths
- Found Raman scattering to be the dominant noise source
- Showed the noise can be modeled extremely well with a depolarizing channel model





JOSEPH C. CHAPMAN,[1,*] JOSEPH M. LUKENS,[1] MUNEER ALSHOWKAN,[1] NAGESWARA RAO,[2] BRIAN T. KIRBY,[3] AND NICHOLAS A. PETERS, Coexistent quantum channel characterization using spectrally resolved Bayesian quantum process tomography, *Phys. Rev. Applied* ***19***(4), *044026 (2023).*

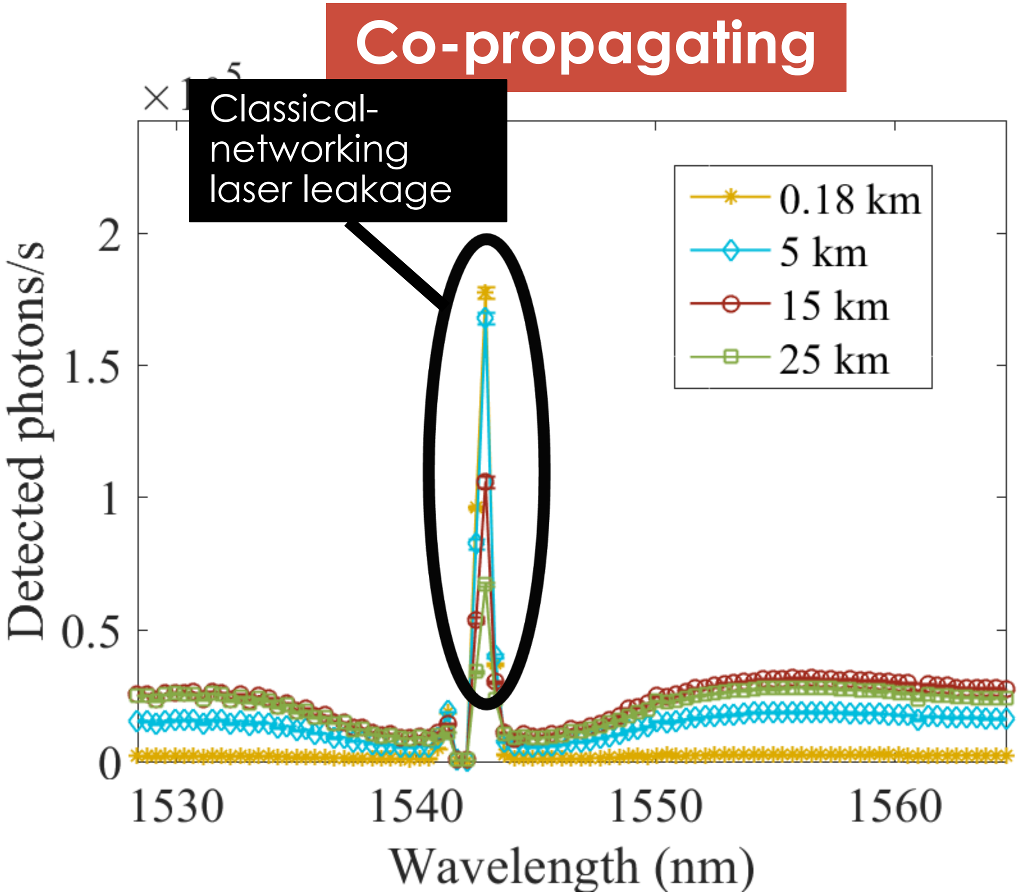
Noise Characterization Experimental Setup

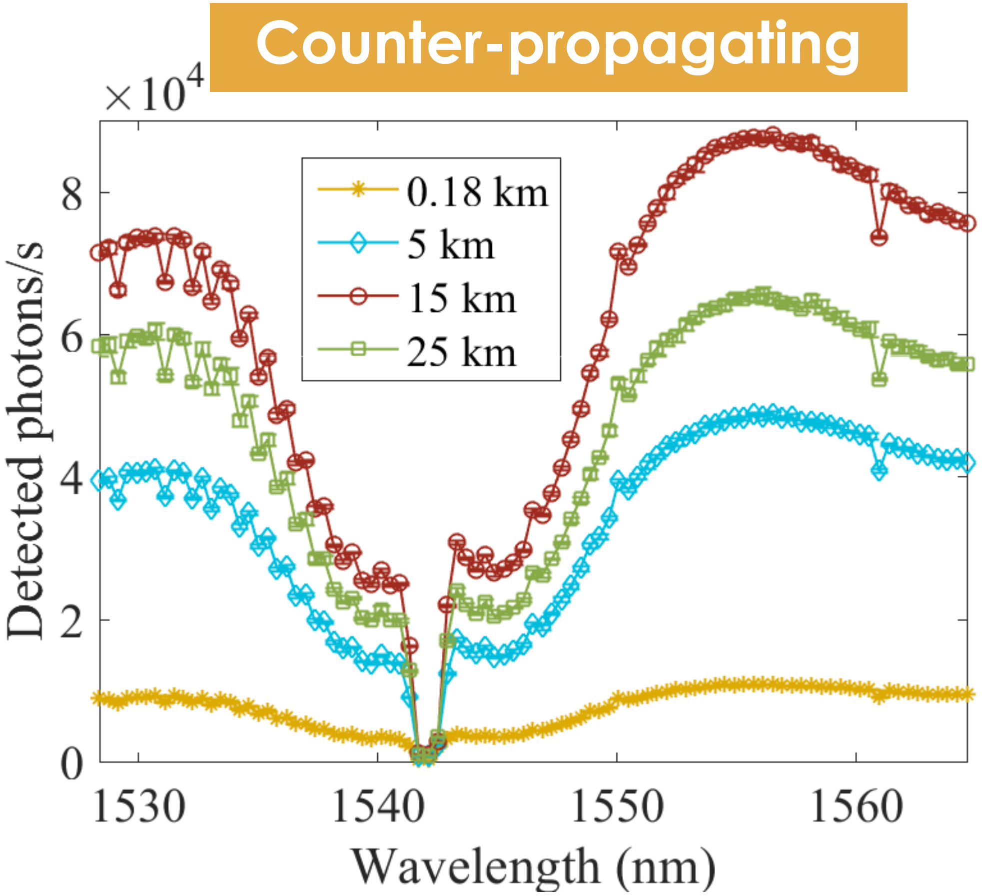


ATT = Attenuator
TF = Tunable filter
OADM = Optical add/drop multiplexer
PF = programmable filter
WDM = wavelength-division multiplexer
HWP = half-wave plate
QWP = quarter-wave plate
PBS = polarizing beamsplitter
SNSPD = superconducting-nanowire single-photon detector

- Wavelength-selective state generation and measurement
- Tested channel lengths up to 25 km
- Tested co-propagating and counter-propagating quantum and classical signals.

Coexistence Noise



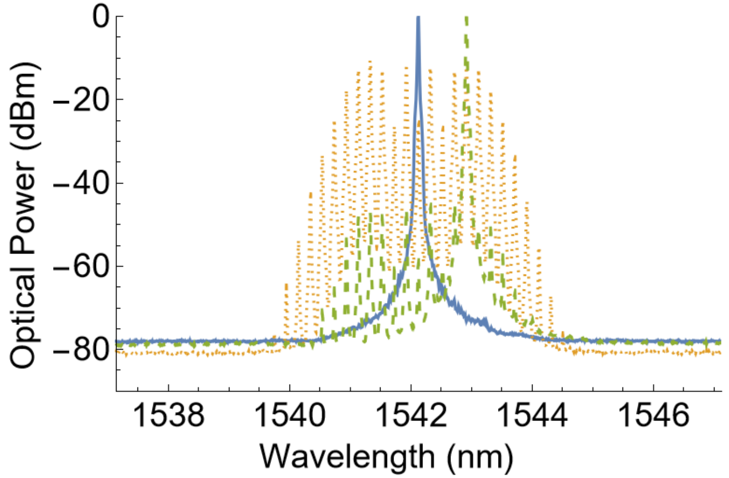


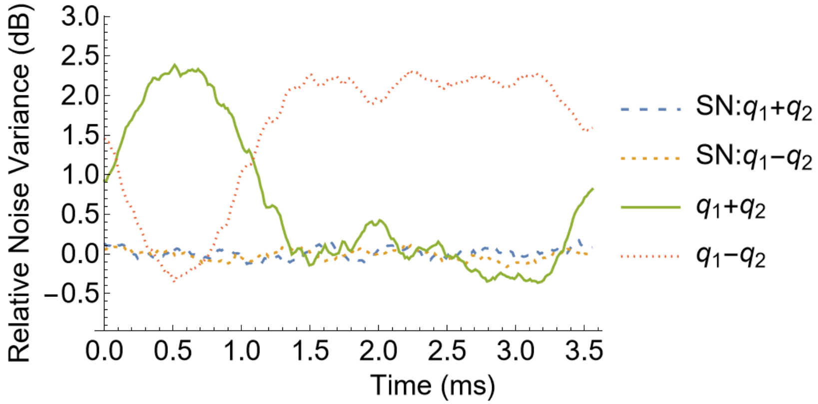
Noise dominated by Raman scattering & it is different for each wavelength

J. C. Chapman, J. M. Lukens, M. Alshowkan, N. Rao, B. T. Kirby, and N. A. Peters, "Coexistent quantum channel characterization using spectrally resolved Bayesian quantum process tomography," accepted, *Physical Review Applied* (2023).

Coexistence Two-Mode Squeezing

- Demonstrated coexistent two-mode squeezing distributed on 3-node campus network with over 1.2-km deployed fiber measuring 0.5±0.1-dB squeezing.
- Demonstrated coexistent two-mode squeezing distributed on two 5-km fiber spools measuring 0.9±0.1-dB squeezing.
- No degradation observed for squeezing frequency-multiplexed with multiple classical signals, spacing as little as 100-GHz, except added insertion loss.
- Demonstrated distributed joint homodyne detection enabled by: (1) multiplex squeezing with phase and sideband optical references; (2) triggered low-noise time-domain homodyne detection.



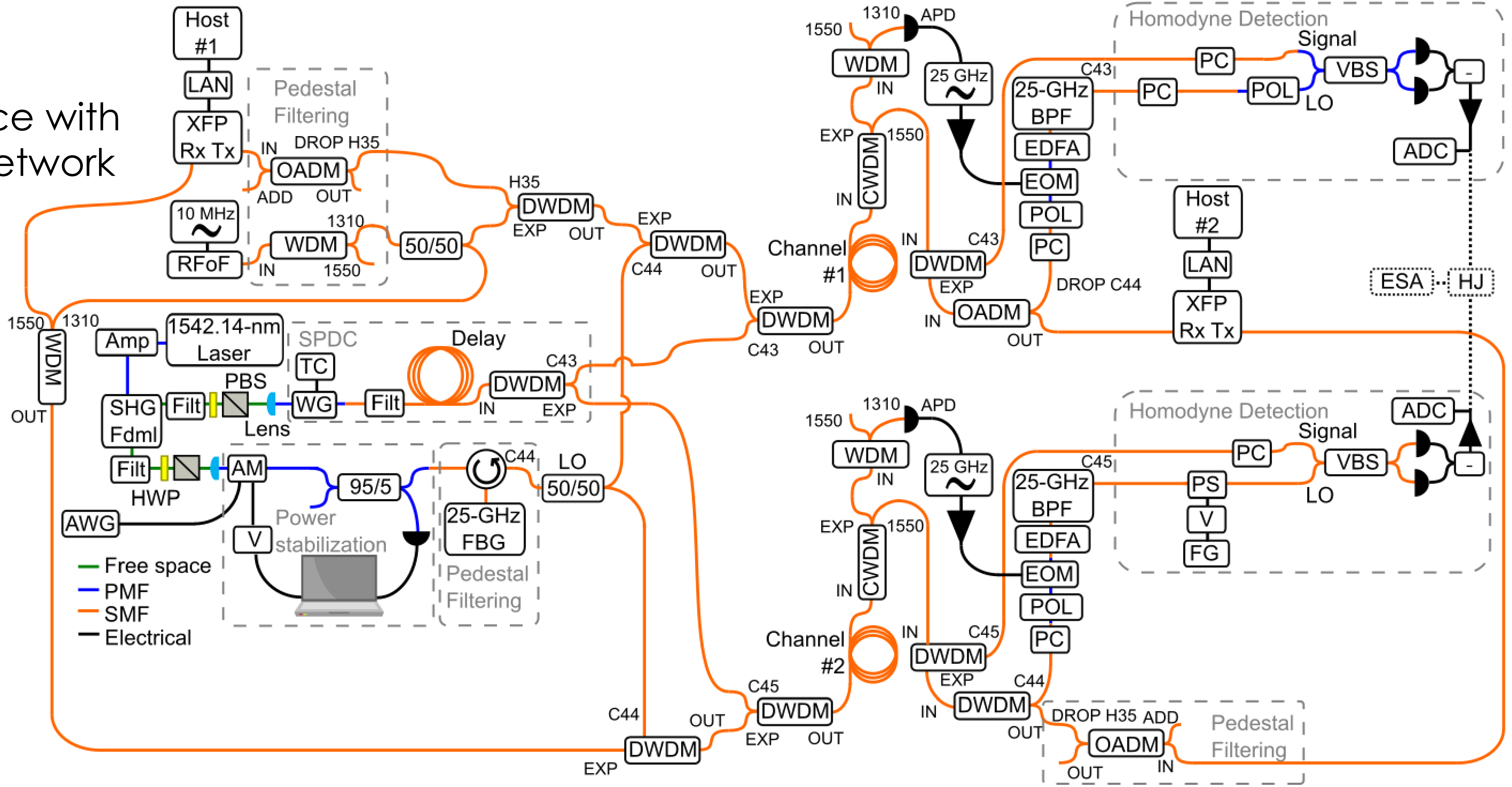


JOSEPH C. CHAPMAN*[,1], ALEXANDER MILOSHEVSKY[1], HSUAN-HAO LU[1], NAGESWARA RAO[2], MUNEER ALSHOWKAN[1], AND NICHOLAS A. PETERS[1,]Two-mode squeezing over deployed fiber coexisting with conventional communications, *Opt. Express*, ***31***(*16*), *26254-26275 (2023)*.

Distributed Coexistent Two-mode Squeezing

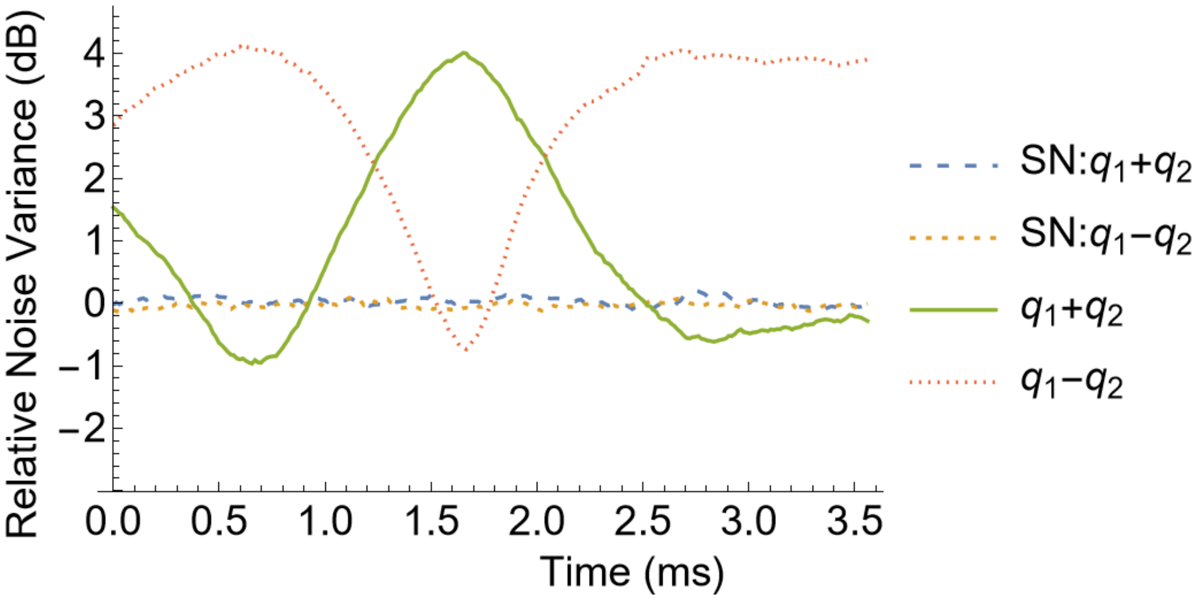
Includes:

- Distributed LO using freq. multiplexing
- Distributed detection
- Coexistence with classical network

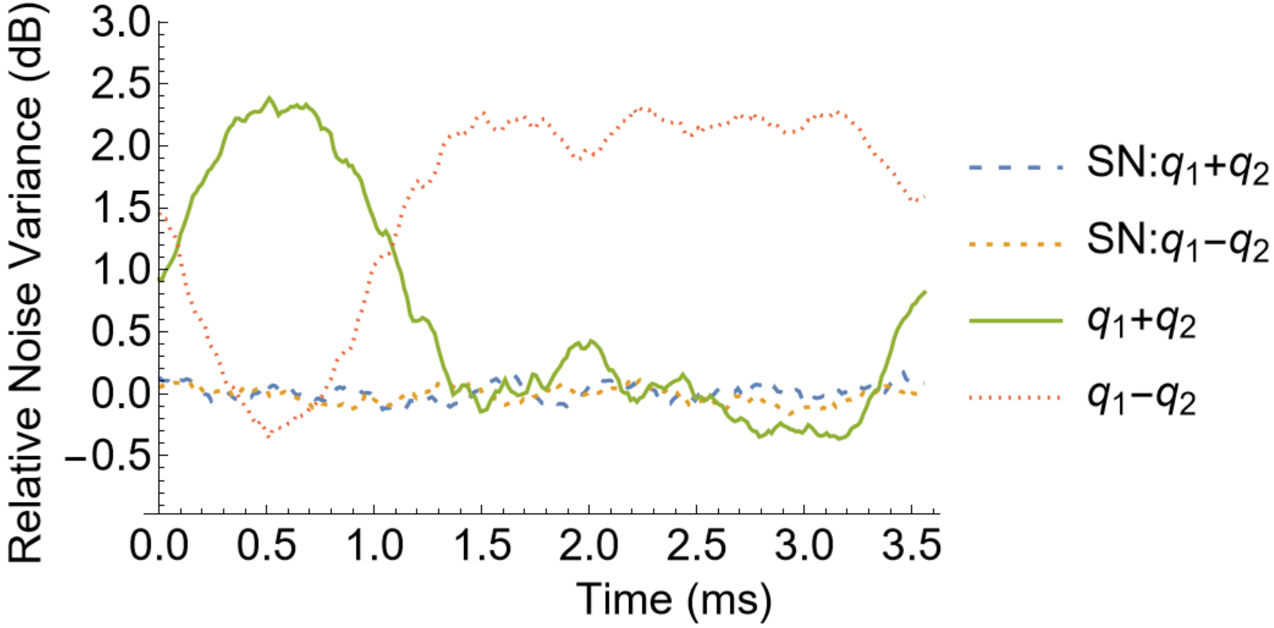


OAK RIDGE National Laboratory

First network transmission of squeezing with conventional signals



Two-mode squeezing: 0 km, w/o coexistence or RFoF



Two-mode squeezing: deployed campus fiber, with coexistence and RFoF

“Two-mode squeezing over deployed fiber coexisting with conventional communications,” J. C. Chapman, A. Miloshevsky, H.H. Lu, N. Rao, M. Alshowkan, and N. A. Peters (draft, 2023)

Conventional-Quantum Network Testbed - QNET

Conventional-quantum testbed

- provides measurements to support comparison of bps and ebps
- ebps measurements over fiber connections of different lengths
- corresponding capacity estimates using light intensity measurements used for approximate transmissivity parameter

Fiber-spool Augmentation:

- fiber spools to provide a suite of single-mode fiber connections
  - three 25 km, one 10 km, one 5 km, and twelve 30m single-mode fibers
    - attached to all-optical switch
  - telescope spools combinations: provide connections suite
    - 30 m; and 5, 10, 15, 25, 30, 35, 40, 50, 55, 60, 65, 75, 80 and 90 km
  - measure light intensities for these connections measured
    - used in analytical formulae to derive the corresponding ebps capacity estimates

Testbed provides common platform to support

- comparison of bps and ebps measurements and capacity estimates

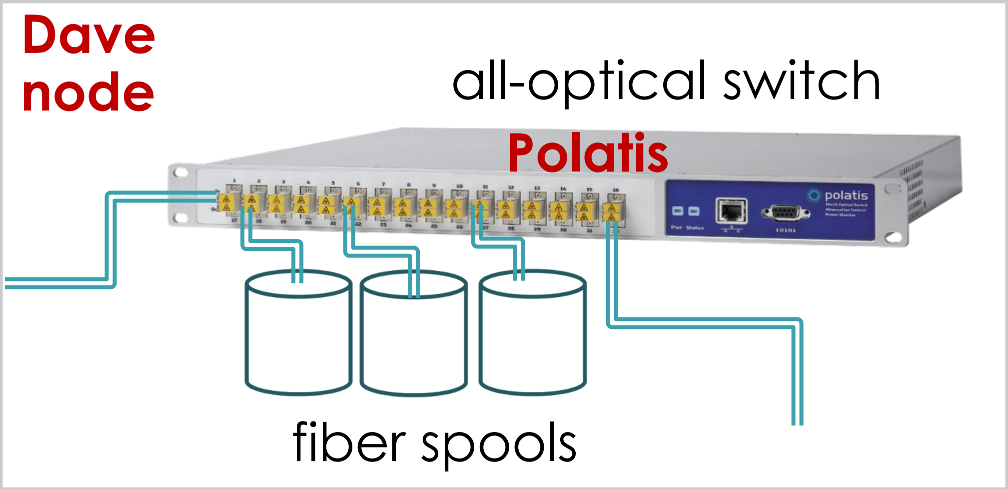
Telescoping Fiber Design: A Critical Testbed Component

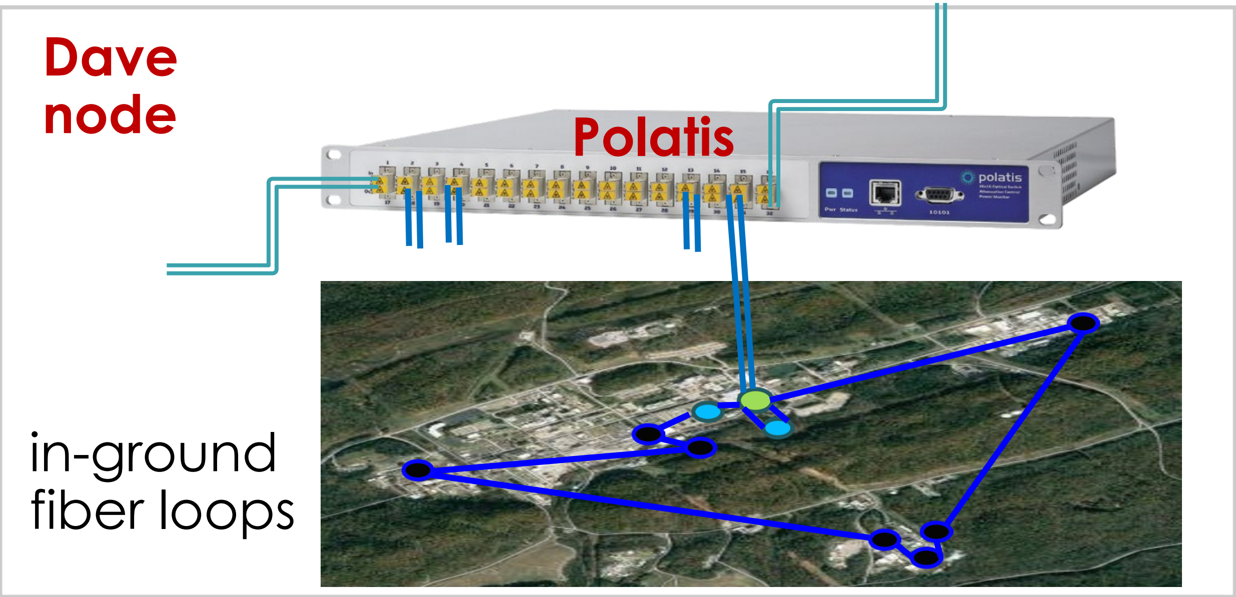
Conventional-Quantum Infrastructure

- augment ORNL quantum network (QNET) with fiber spools and in-ground loops
  - fiber spools: suite of single-mode fiber connections 0 – 90 km
    - 3*25km, 10 km, 5km
  - In-ground fiber loops: suite of single-mode fiber connections 0--200~km
    - 20 loops: each 15km
- **Utilize spools and loops in combinations to realize a suite of connections**

Measurements and estimates

- measure light intensities for these connections
- conventional and quantum throughput measurements





Throughput Measurements and Capacity Estimates

Methodology

conventional-quantum testbed provides measurements:

- ebps measurements over fiber connections of different lengths
- estimates of corresponding capacities
  - using light intensity measurements to approximate transmissivity parameter η

- compare bps and ebps measurements and capacity estimates

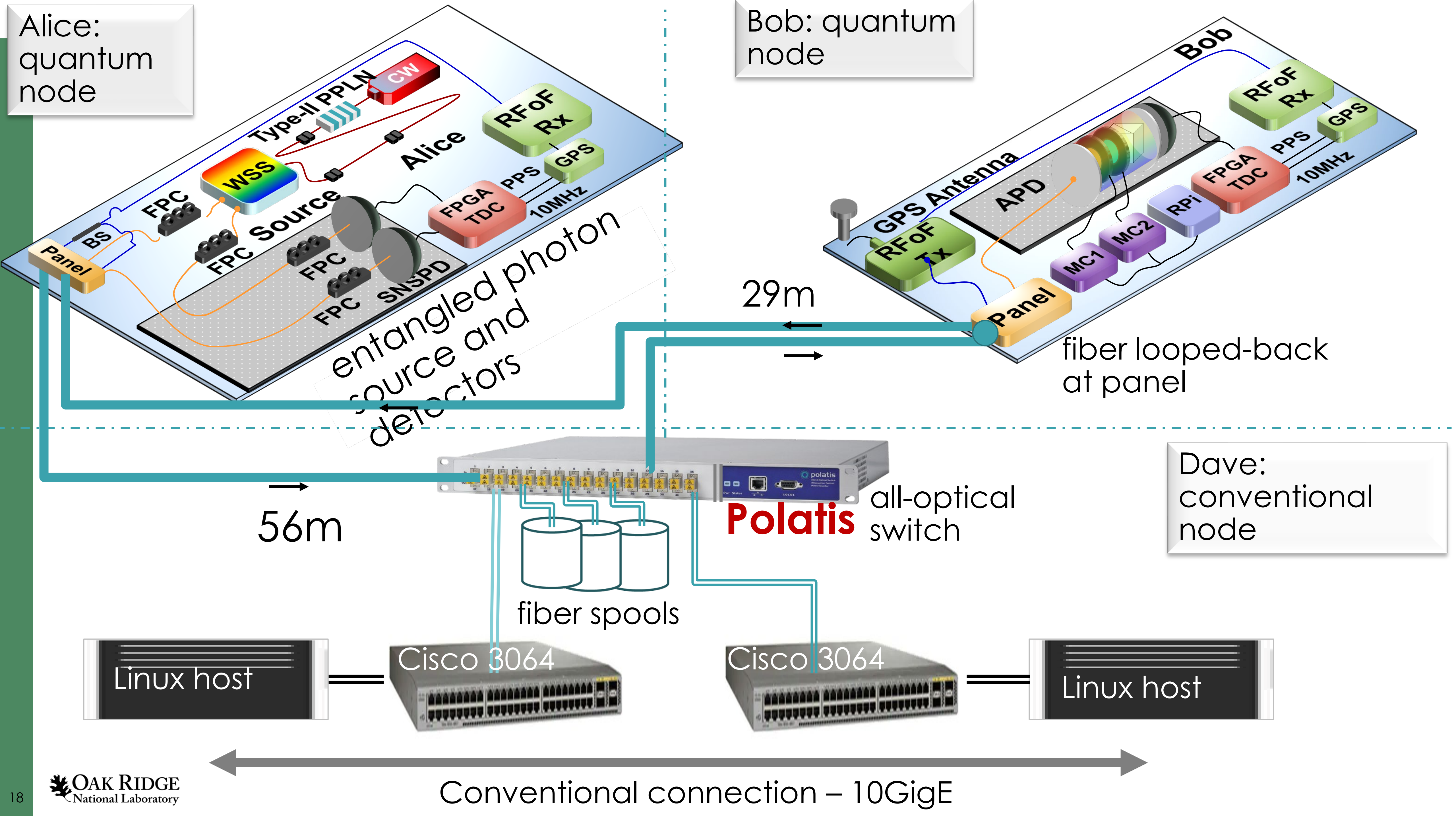
Conventional-Quantum Infrastructure

- conventional-quantum testbed that provides measurements
  - support comparison measurements and capacity estimates both qualitatively and quantitatively
- augment ORNL quantum network (QNET) with fiber spools
  - to provide a suite of single-mode fiber connections 0--90~km in length.

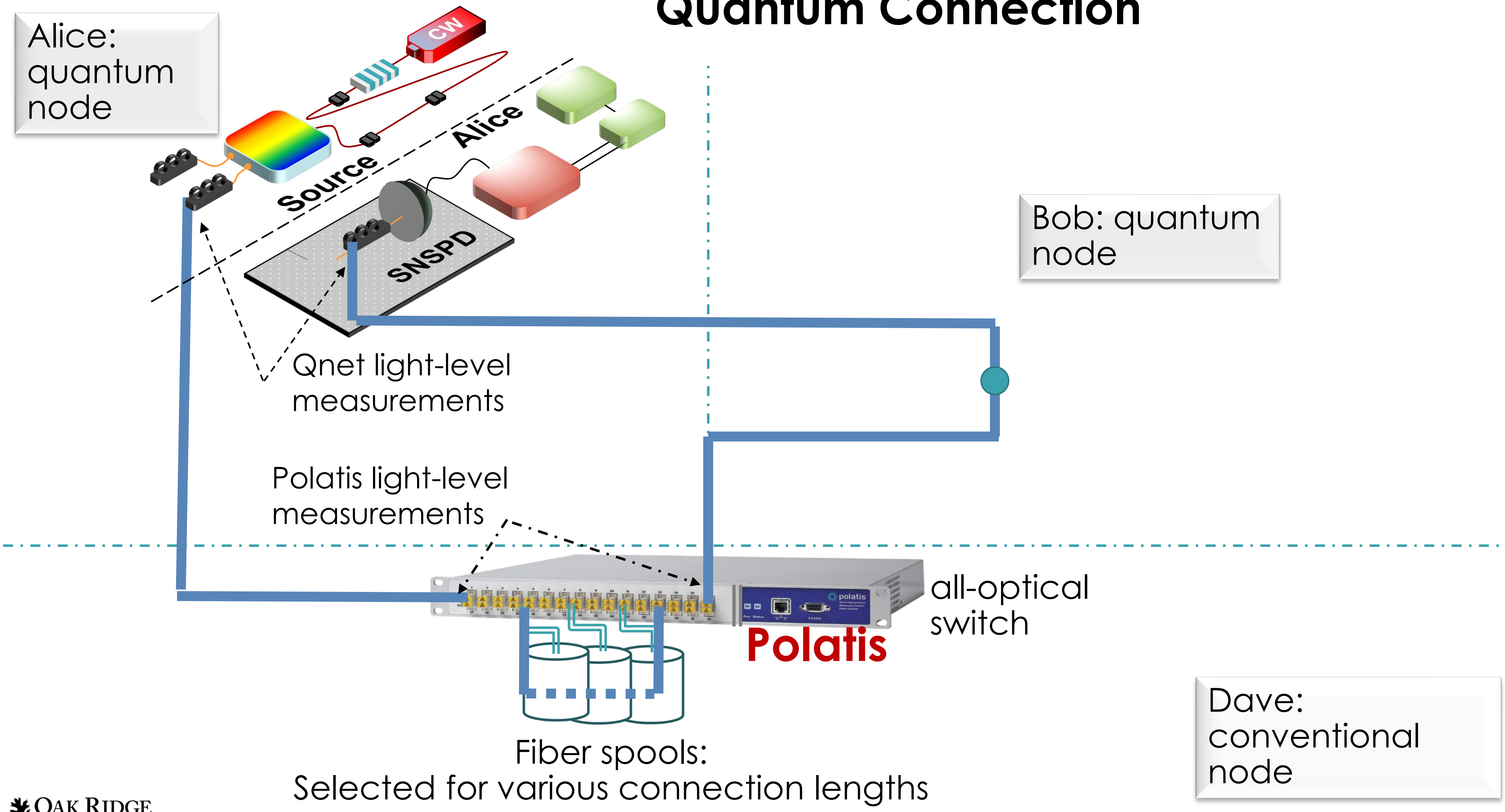
Measurements and estimates

- measure light intensities for these connections
- use them in analytical formulae for ebps capacity estimates

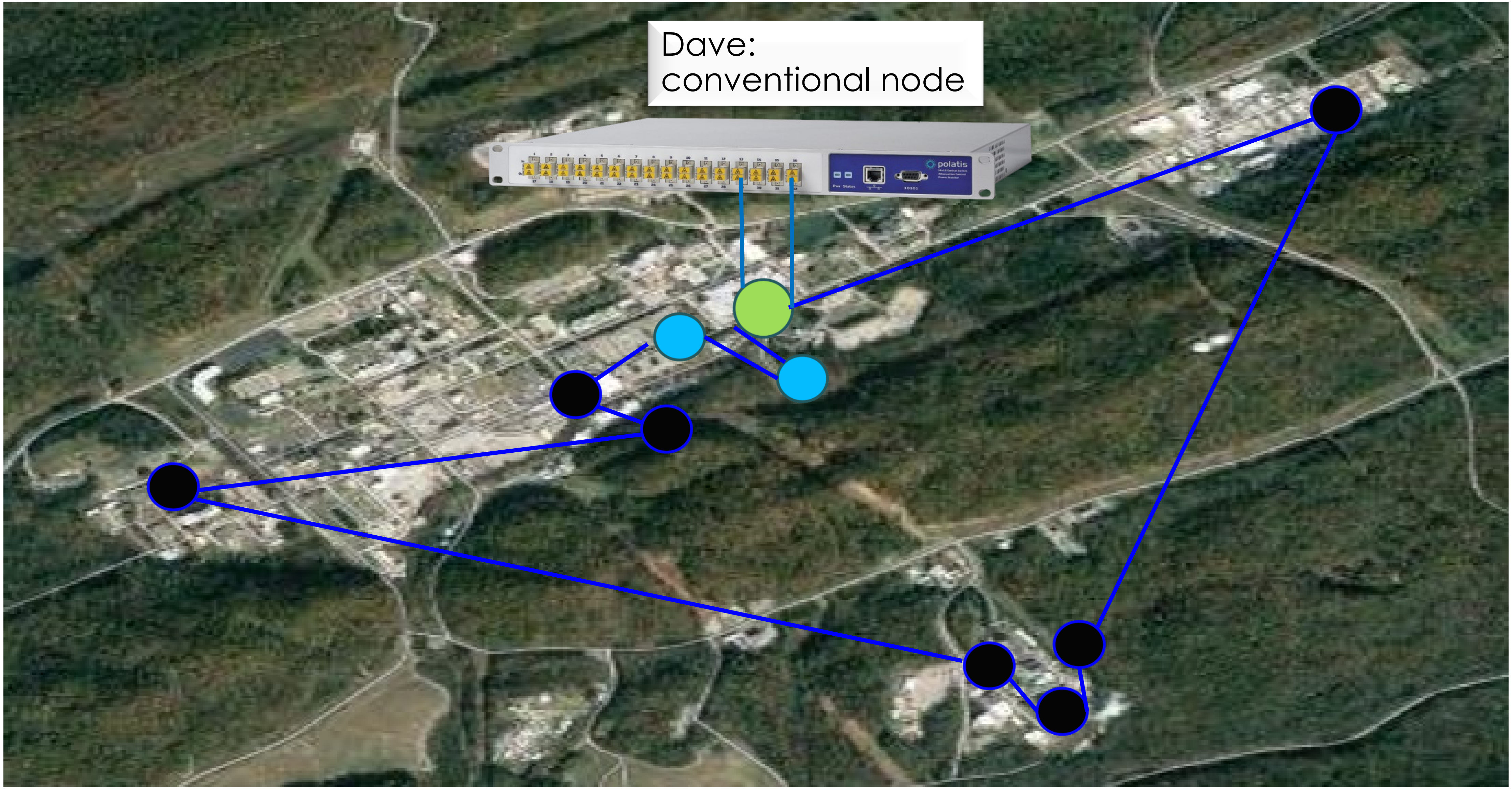
N. S. V. Rao, M. Alshowkan, J. C. Chapman, N. A. Peters and J. M. Lukens, "Throughput Measurements and Capacity Estimates for Quantum Connections," *IEEE INFOCOM 2023 - NetSciQCom 2023: IEEE INFOCOM Network Science for Quantum Communication Networks Workshop*, Hoboken, NJ, USA, 2023, pp. 1-6, [DOI: 10.1109/INFOCOMWKSHPS57453.2023]


Alice: quantum node
Bob: quantum node
Type-II PPLN
CW
RFoF Rx
WSS
Alice
FPC
BS
Source
GPS
PPS
FPGA TDC
10MHz
Panel
SNSPD
entangled photon source and detectors
Bob
RFoF Rx
GPS
PPS
FPGA TDC
10MHz
GPS Antenna
APD
RPi
MC2
MC1
RFoF Tx
Panel
29m
fiber looped-back at panel
56m
Polatis
all-optical switch
Dave: conventional node
fiber spools
Linux host
Cisco 3064
Cisco 3064
Linux host
Conventional connection – 10GigE

Quantum Connection



20 single-mode fiber loops: each 15km



Comparison of bps and ebps measurements and capacity estimates

Conventional connections

10 Gbps peak throughput achieved over 90 km distances

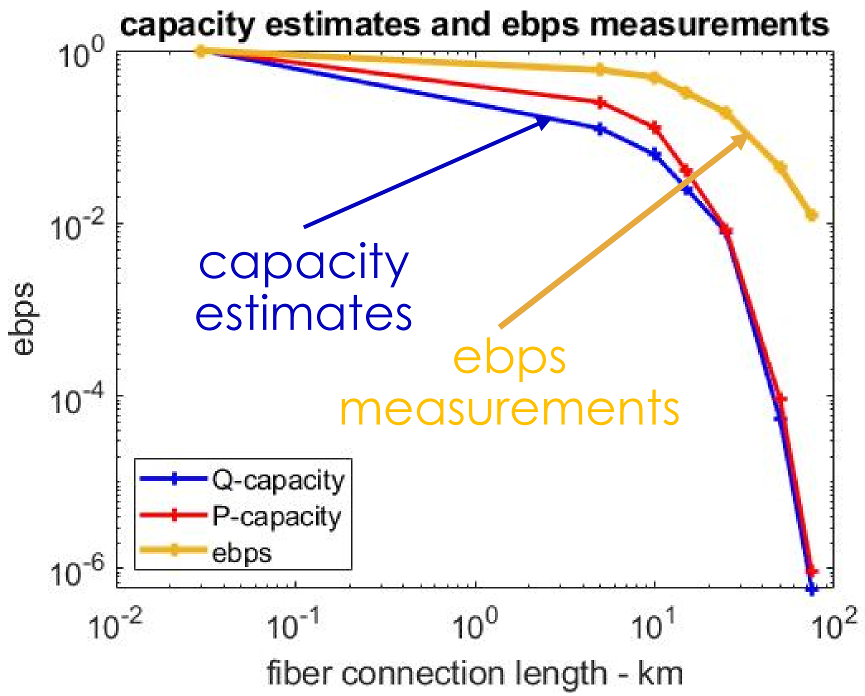
- buffers and loss detection and retransmission mechanisms of Transmission Control Protocol (TCP)
- mechanisms are not (commonly) used in ebps measurements and capacity estimates

Quantum connections,

- ebps decays with connection length
  - sharply: faster than linear, compared to bps
  - but, slower than capacity estimates using light intensity

ebps throughput higher than estimated capacity

- indicates mismatch between
  - analytical model
  - physical connection properties



- Overall, this comparison
  - highlights difference in throughput due to underlying transport mechanisms
  - potential approach for achieving higher ebps by using TCP-like mechanisms

Capacity Estimates: Transmissivity of Fiber

For fiber connections, ebps capacity estimate per channel use – Pirandola et al 2017 based on transmissivity η of optical fiber:

$$D_2(\eta) = -\log_2(1-\eta).$$

Bound on ebits for channel use - channel rate under fixed source rate

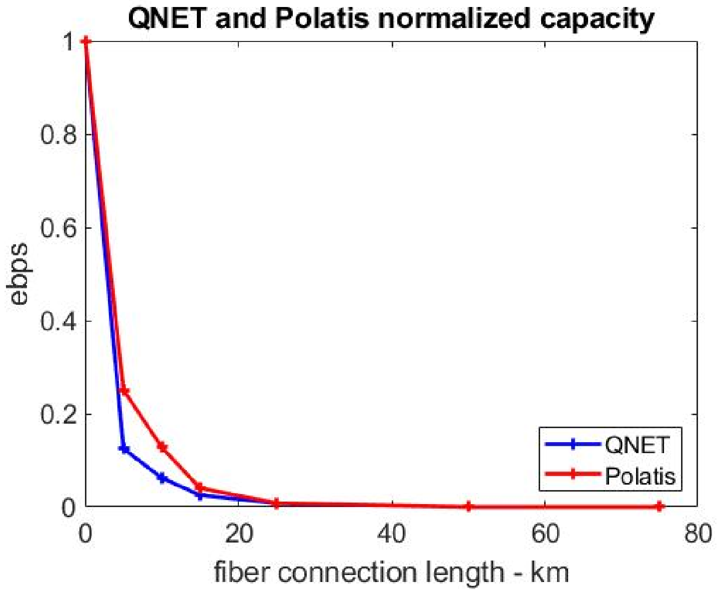
Here, η is typically linear in connection length – implies capacity profile is typically convex

Transmissivity in this case: fraction of entangled photons successfully transmitted over channel

- our approximation: fraction of power that passed through
  - convert loss in dB into fraction and subtract from 1
  - connections treated as fiber – not patching and switching

Using QLAN and Polatis measurements, we approximate η and compute $D_2(\eta)$

- P-capacity: Polatis measurements- shorter connection of only fiber spools
- Q-capacity: includes connection between quantum and conventional nodes

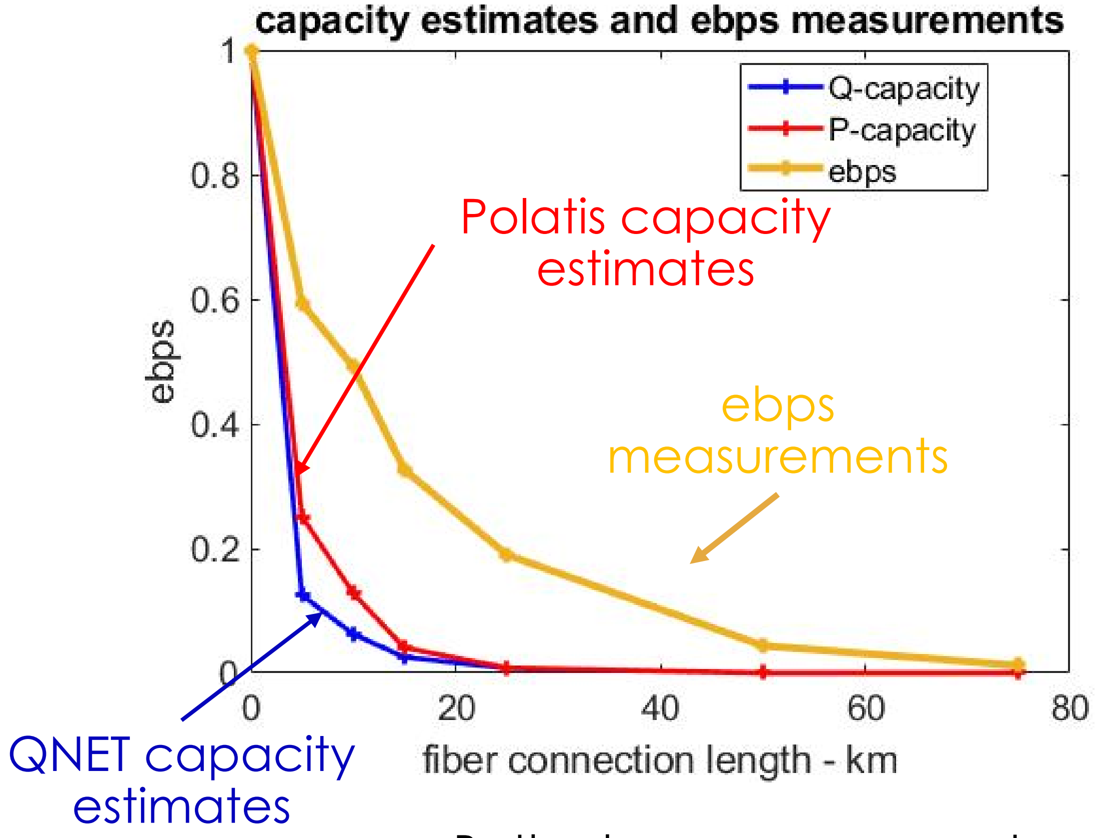


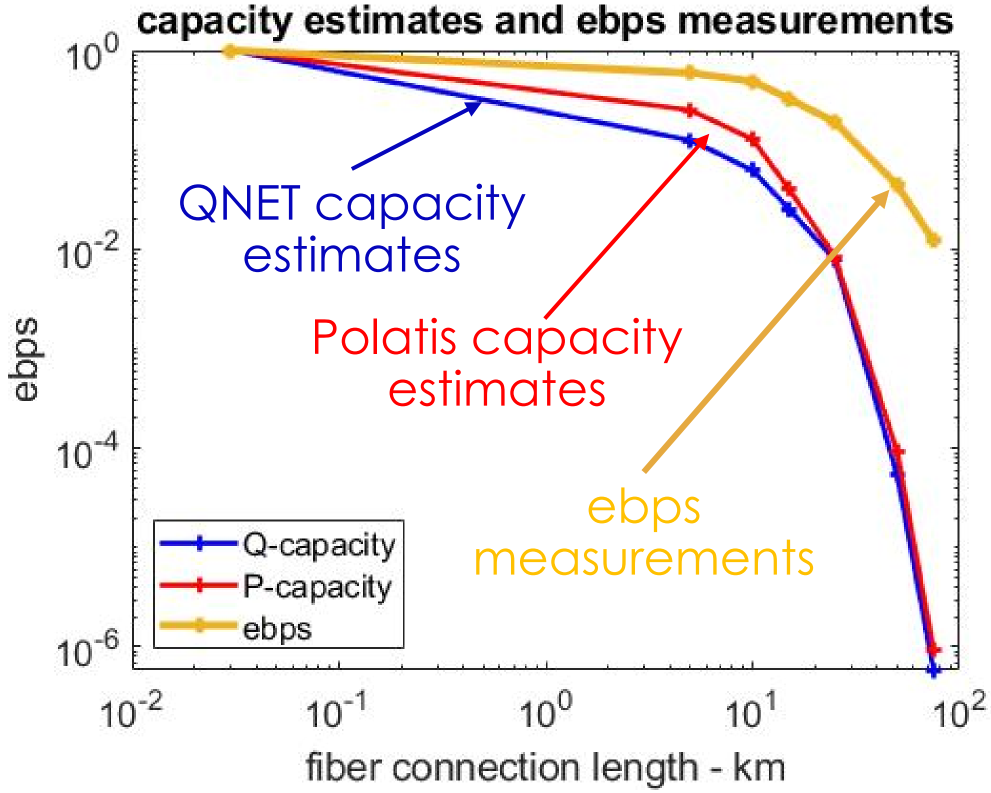
OAK RIDGE National Laboratory

Comparison: Measurements and Estimates

ebps measurements and capacity estimates based on QNET measurements

- normalized with highest values over 30-m fiber spool connection for illustration
- estimates based on Polatis measurements - smaller connection losses by about 12.22dB





Both ebps measurements and corresponding capacity estimates

- decrease rapidly with distance as expected
- shape is **convex** - similar to TCP profile under severe bottlenecks
- capacity estimates based on Polatis measurement higher

Authenticating IPsec Tunnels using QKD keys

IPsec protocols:

- used to establish a secure tunnel for VPN traffic - data included in TCP/IP packets can be encrypted and authenticated
- IP packet (header and payload) is encapsulated within another IP payload, a new header is added, and the packet is then routed over the IPsec tunnel.
- new header contains local VPN peer's source IP address and VPN peer's destination IP address at the other end of the tunnel
- When packet reaches the remote VPN peer, the outer header is stripped off, and the actual packet is routed to its destination

Authentication

- peers must first be authenticated before VPN tunnel can be established
- After authentication, peers agree via security associations (SAs) on parameters necessary for secure transmission - security protocol, destination IP address, and security parameter index
- To establish SAs for the IPsec tunnel IKE (Internet Key Exchange) employs certificates or PSKs

Our scheme: QKD keys used as PSKs by automated scripts in IKE process between two site FEDs

N. S. V. Rao, M. Alshowkan, A. Al-Najjar, S. E. Hicks, P. G. Evans, J. M. Lukens, N. A. Peters, "Site-to-Site Tunnels Authenticated by Quantum Keys," IEEE Photonics Conference, Nov. 13, 2022.

OAK RIDGE National Laboratory

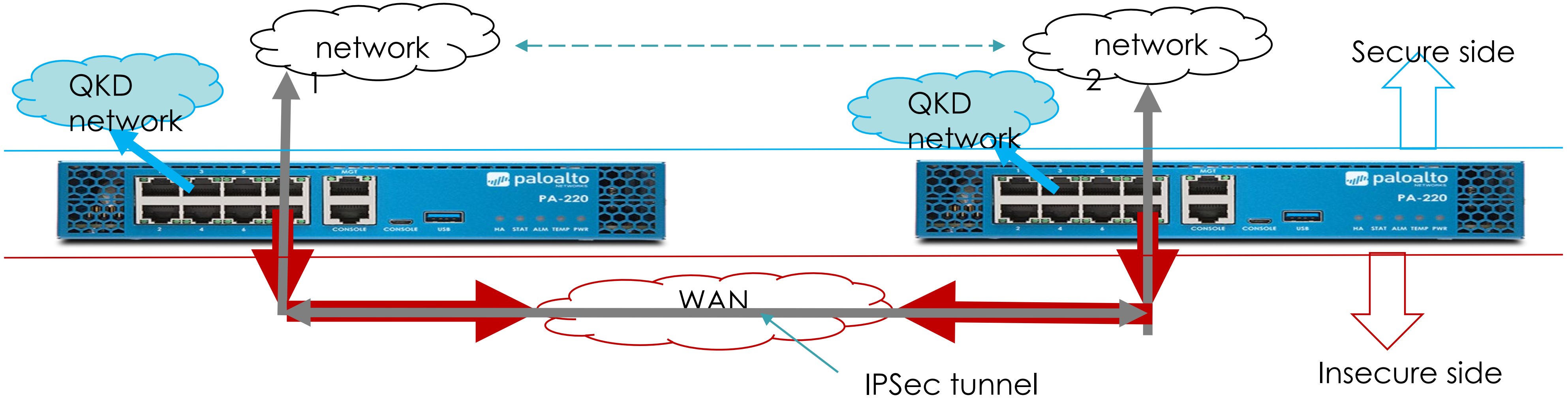
Secure, Separate Connections

Our scheme: implemented using PA-220 FED devices used as site firewalls

- enable subnets on secure side and connections to an open network on insecure side
- Separate physical ports devoted to
  - (i) secure zone of site network - connected to routers, switches and hosts that belong to site network over dedicated physical ports
  - (ii) QKD secure zone consists of dedicated connection to Ethernet port of key host

Dedicated management access configured on FED port in QKD secure zone, and is

- used to access an application programming interface (API) for installation of QKD keys using a dedicated account
- firewall rules are established to enable traffic flows between various zones.



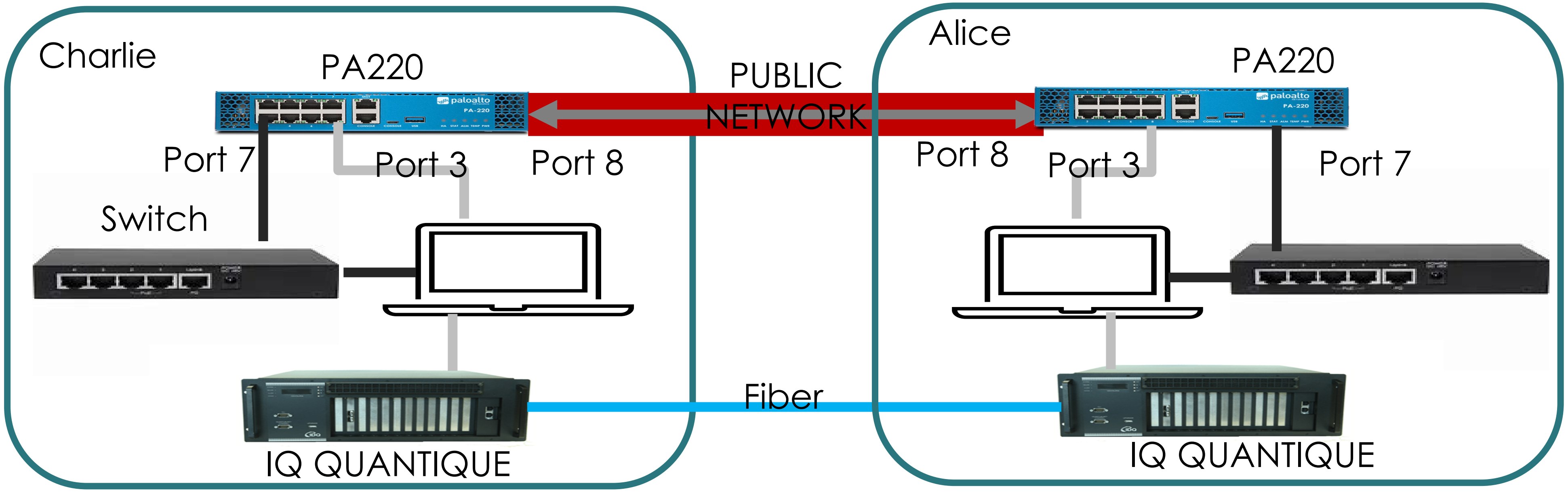
Oak Ridge National Laboratory

Secure Zones and Connections

Our scheme: implemented using PA-220 FED devices used as site firewalls that

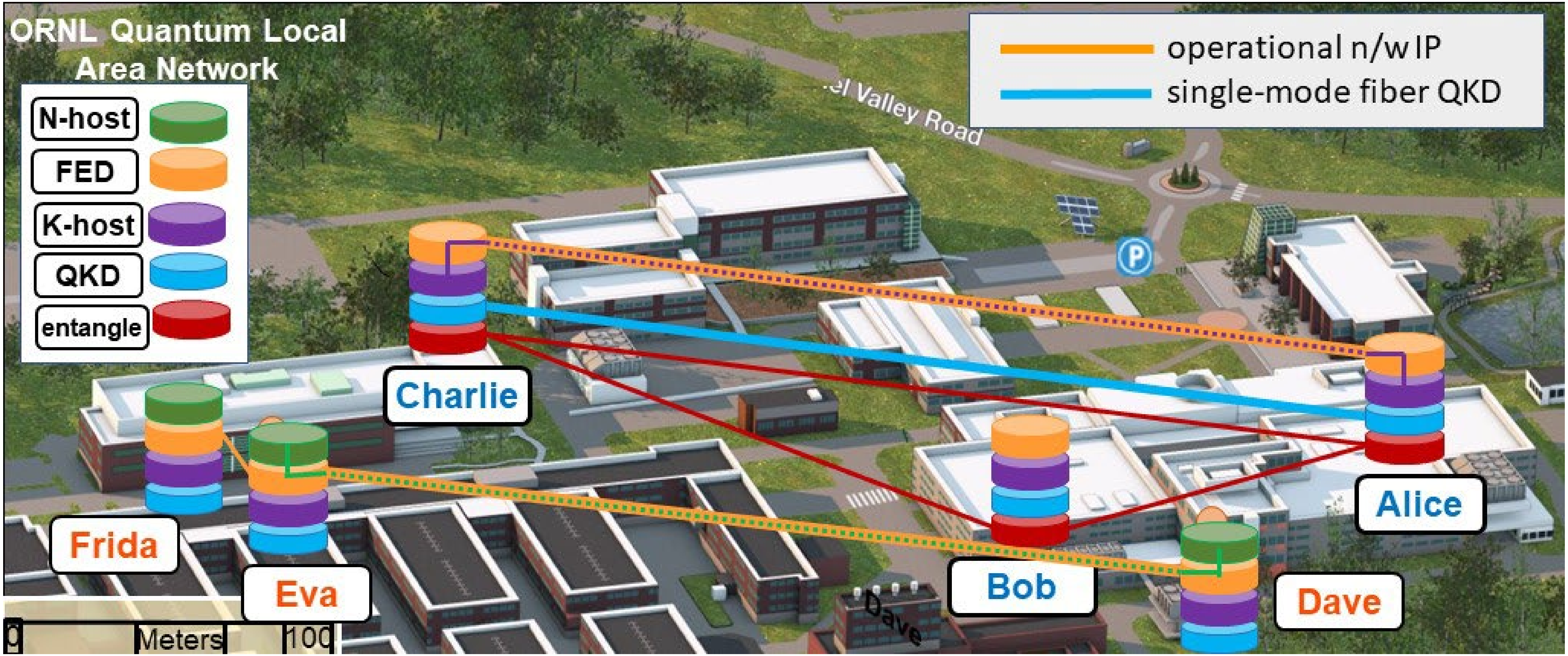
- enable subnets on secure side and connections to an open network on the insecure side
- Separate physical ports are devoted to
    - (i) secure zone of site network which may be connected to routers, switches and hosts that belong to the site network over dedicated physical ports, and
    - (ii) QKD secure zone which consists of a dedicated connection to the Ethernet port of key host

Dedicated management access is configured on aFED port in the QKD secure zone, and is used to access an application programming interface (API) for installation of QKD keys using a dedicated account. Additionally, firewall rules are established to enable traffic flows between various zones.



Oak Ridge National Laboratory

IPsec Tunnel Authentication:
Alice and Charlie quantum nodes



OAK RIDGE National Laboratory

Conclusions

Summary:

- Described quantum conventional network testbed: support variety of network R&D projects
- Augmented QNET testbed with
  - fiber spools to provision suite of optical connections: bps and ebps throughput and power levels during ebps measurements, which are used for ebps capacity estimates.
- Briefly described experiments:
  - Noise characterization
  - Two mode squeezing co-existing with conventional traffic
  - Entanglement distribution
  - Throughput and capacity estimation
  - Securing IPSec tunnels with QKD

Future Work:

- In near future - several testbed capabilities needed
  - wide-area fiber connections
  - repeaters and routers – infrastructure to test them
  - software for operations, provisioning and orchestration
- **An Open question**: testbed for potential role of buffers and loss recovery for ebps throughput
  - similar to TCP mechanisms in conventional networks

Thank you

29

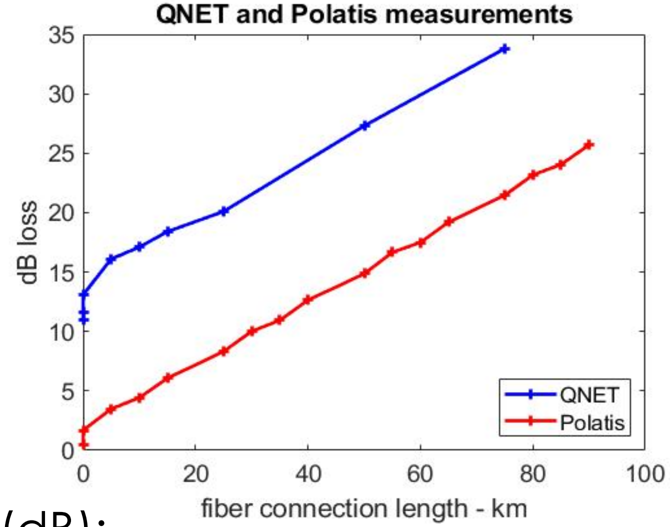
Light-level Measurements

For conventional and quantum connection

- light levels (dBm) measured on all-optical switch - Polatis measurements.

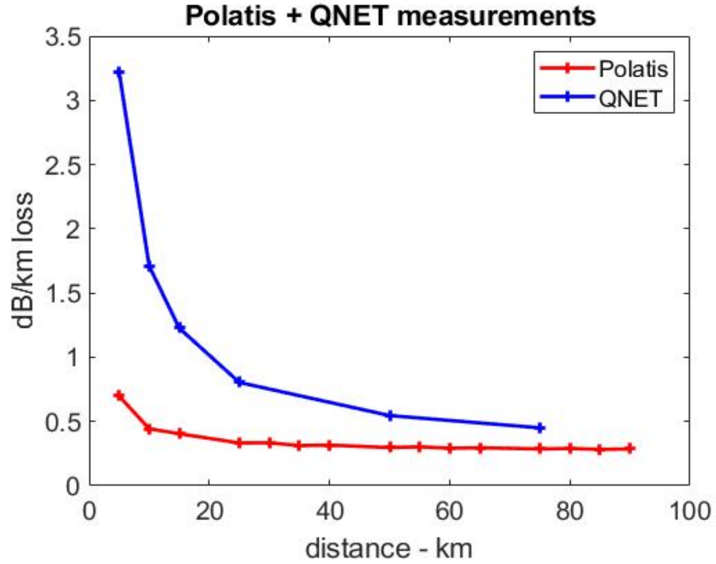
For quantum connections,

- additional light level measurements at source and detectors in node Alice - QNET measurements



Connection loss (dB):

- subtract destination from source levels
- function of connection length in km - nearly linear
- constant additional 15 -20 dB loss for quantum connections
  - additional fiber connections to Alice and Dave - direct and via Bob and at source and detectors.



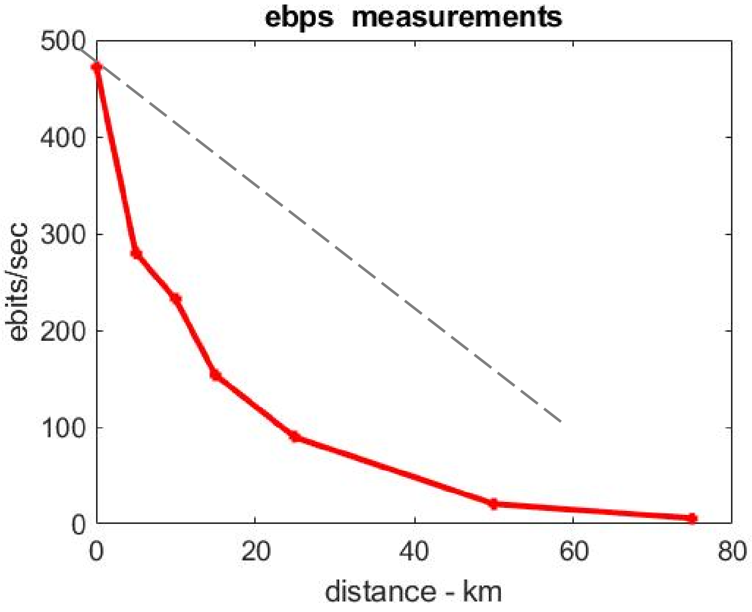
Loss rate per distance estimate - divide connection losses by length,

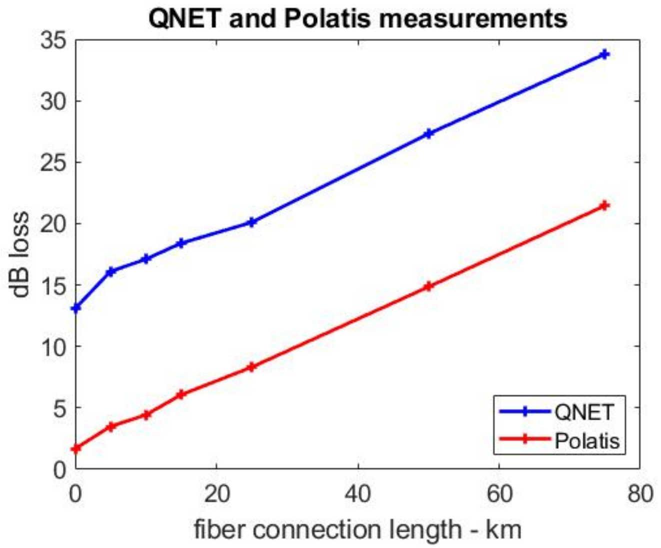
- decreasing trend with connection length
- higher values at shorter connections
  - higher fraction of losses due to
  - fiber patches at nodes, cross-connects optical switch, and at source and detectors

OAK RIDGE National Laboratory

ebps measurements over quantum connections

- Coincidence rate measurements of entangled photon source at various distances
  - calculate entanglement throughput assuming 100% quantum state fidelity.
- in practice, measured fidelities >90% on QNET





ebps measurements
- decrease with connection length
- profile is convex

sharp contrast with TCP bps measurements.

Connection losses between source and detectors
- corresponding Polatis values

Losses nearly linear with connection length
- mean offset of 12.22 dB between QNET and Polatis losses

Used in capacity estimates

Quantum Channel Models: Capacity Estimates

Capacity estimates for fiber connections

- derived under various conditions using variety of parameters
- specializing general quantum channels specified by mathematical descriptions - Wilde 2017

Generic quantum communications channel

- defined as linear, completely positive, trace preserving map
  - corresponds to quantum physical evolution
- Takes particular form according to Choi–Kraus decomposition in terms of Kraus operators
- Several versions of quantum capacity are defined and estimated under parametrizations
  - for example, dephasing and loss channels
  - channel models inferred by process tomography using QNET measurements - Chapman etal2023

Our Model: specific characterization of simplified optical fiber channels without repeaters

- uses transmissivity parameter η for pure loss channel – Pirandola et al 2017

Capacity estimates: Approximations

Derived treating connections as fiber no explicit accounting for patching and switching
Estimation is approximate:

- measured power level includes other components

Connection power level transmission to approximate transmissivity approximations:

- **Non-selective losses**: QNET measurements utilize spectral filtering and calibration for 1560-nm entangled photons, and
  - represent that includes singles and entangled photons
  - **assumption**: losses are not selective and represent entangled ones
- **Broader spectrum**:
  Polatis measurements:
  - broader spectrum than QNET measurements and have a
  - coarser resolution with no spectral filtering and calibration.
  - **Assumption:** l osses are somewhat uniform around entangled photon bandwidth
- **Not pure fiber**: connections consist of
  - multiple cross-connects at patch panels
  - connections to and within Polatis switch
  -

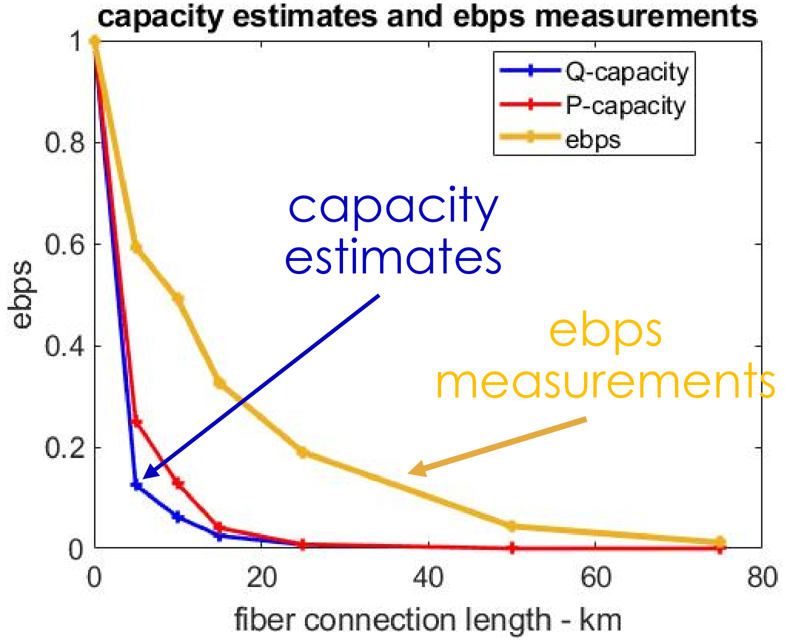
Overall, capacity estimates derived using ``pure'' fiber models

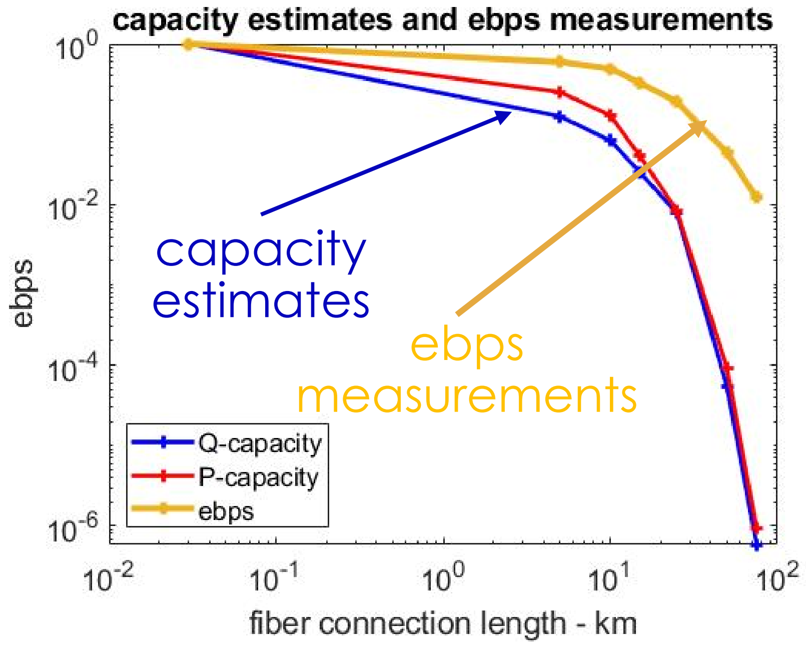
- additional losses effect both throughput measurements and light levels,
- assumption: play secondary role particularly at longer connection lengths

Comparison: Models and Physical Connections

Both ebps measurements and corresponding capacity estimates

- while both decrease rapidly, **ebps measurements are higher than capacity estimates**





Postulation: degree of misalignment between

- assumptions used for the capacity estimation and
- QNET conditions under which the light intensity measurements are collected

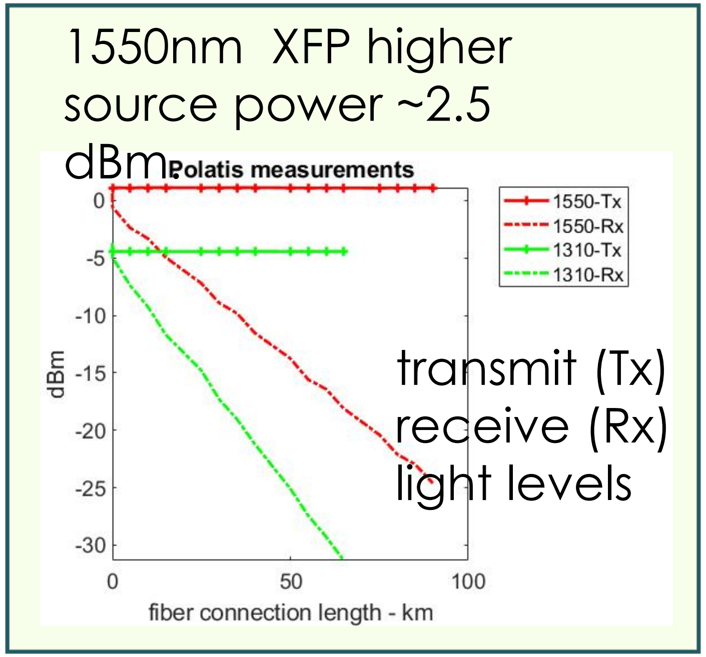
Further refinements needed to correlate measurements with theoretical estimates

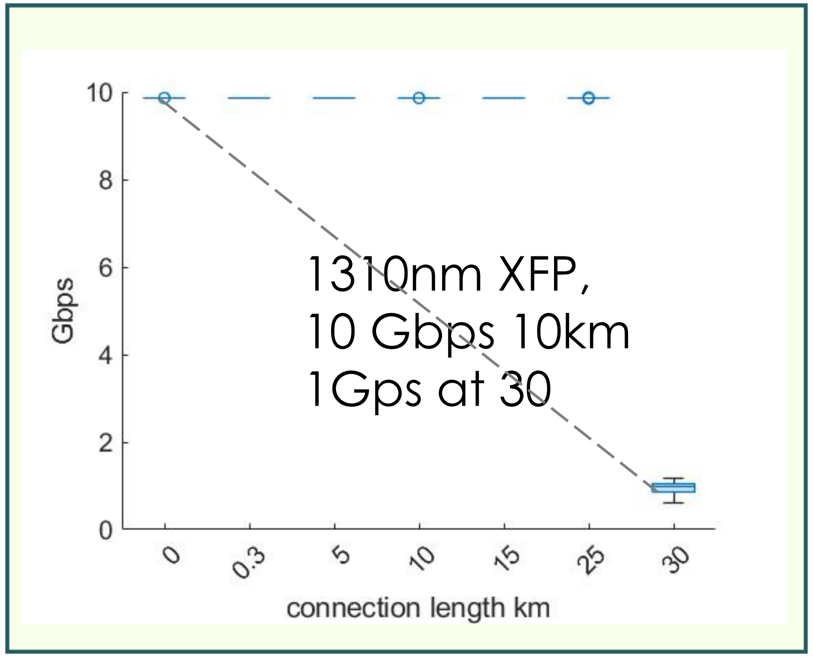
Comparison: somewhat similar to Shannon limit estimation (conventional optical connections) several refinements needed to correlate measurements with theoretical estimates

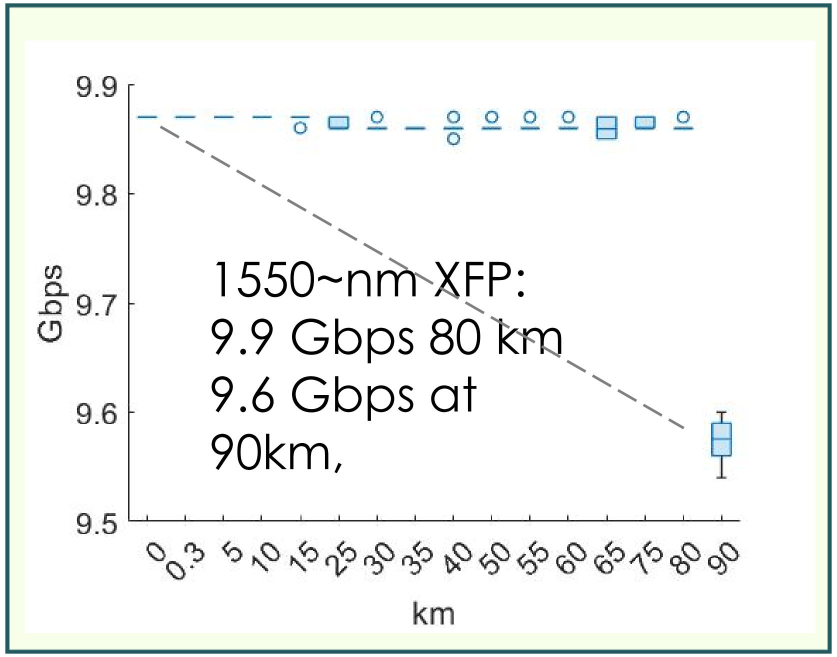
Conventional throughput measurements

The bps using iperf3 between two Linux hosts at Dave connected through all-optical switch.

1310 nm XFP 10~km target distance
1550 nm XFP 80 km target distance







Shape of the throughput profile

- **concave** – typical in optimized conventional networks.
- **convex** – indication of bottlenecks (insufficient TCP or other buffers) Rao et al 2018

- convex shape observed both for ebps measurements capacity estimates
- Shannon capacity bps based on signal-to-noise ratio
  - qualitatively convex shape - do not include effects of buffers and loss of TCP

OAK RIDGE National Laboratory

Secure Zones and Connections

Keys of IPsec tunnel periodically updated

- key hosts use identical QKD keys available at both sites
- sustain VPN connectivity except during brief key update periods

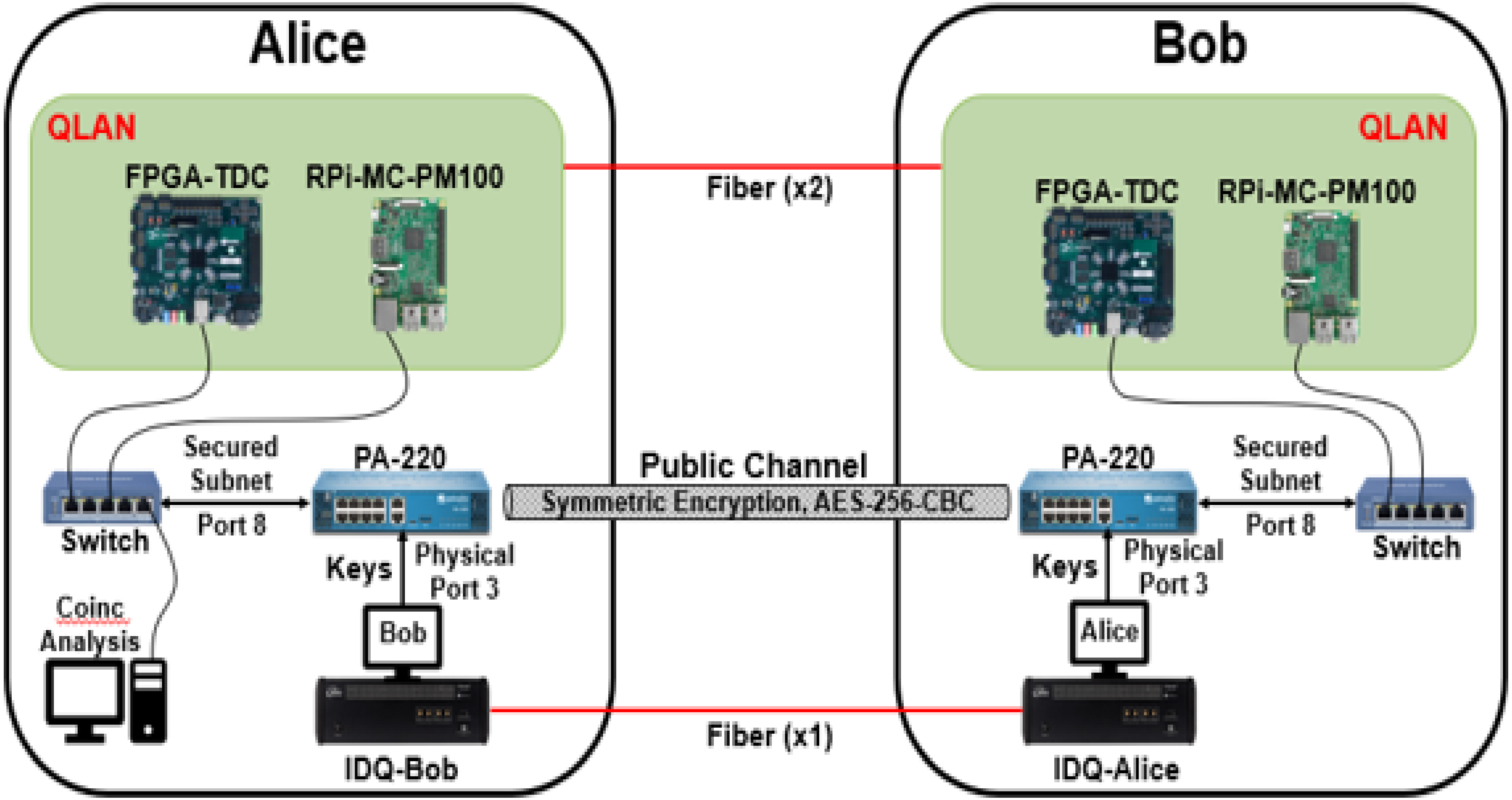
Our architecture: logical secure zones and dedicated physical ports and connections

Secure, separate two types of traffic:

(i) site traffic within site networks and over VPN tunnels
(ii) QKD traffic between key host and dedicated FED port for key installation

Two traffic streams are physically separated at the connection level and logically separated on a FED using security zones

QKD-IP Implementation Details



Oak Ridge National Laboratory