DemoQuanDT: Controlling Quantum Key Distribution Networks
IRTF Quantum Internet Research Group Meeting IETF-118

Malte Bauch*, Johanna Henrich†, Fabian Seidl*, Martin Stiemerling*

da/net* & UCS†, Computer Science, Darmstadt University of Applied Sciences, Germany

2023-11-07
Outline

1 DemoQuanDT Overview
2 Controlling QKDNs
3 Summary & Outlook
4 Demo
DemoQuanDT Overview
DemoQuanDT Project Overview

- **Goal:** setup a Quantum Key Distribution Network across Germany
  - from Bonn to Berlin (approx. 600 km)
  - multi-hop QKDN
  - multi-vendor

- **Partners:** Adva, Deutsche Telekom, Hochschule Darmstadt, KeeQuant, Rhode & Schwarz, Technical University Darmstadt

- **Funded by Germany’s Federal Ministry of Education & Research (2022 to 2024)**

- QKDNs probably a first step towards Quantum Internet
Controlling QKDNs
Controlling QKDNs

- In an nutshell: end-to-end user-key forwarding
  - encryption keys to transport user-key out of quantum layer (QL)
  - encryption of user keys between two adjacent peer Key Management Systems (KMS)
  - KMS: key retrieval from QL, key management, and forwarding

- centralized control of network
  - multiple quantum links: mainly network management
  - key management systems for key routing and forwarding
  - routing decisions done in QKDN Controller
  - forwarding path is a "switched-circuit"

- placement in DT’s carrier network
  - actual behavior of a real "complete" QKDN deployment with all pros and cons
  - study country-wide behavior of QKDN with all "bells and whistles"
  - separation of user, access & network parts
DemoQuanDT System Architecture (simplified)
Current Implementation (h_da)

- Routing-App: simple, static routing
- QKDN-Controller basis: goSDN [4]
  - model-driven SDN controller
  - gnmi-based agent for controlling network elements
  - self-developed Yang-Model (not ETSI GS QKD 015)
- KME/KMS basis: proto-kms [2]
  - a yet very naive implementation of a KMS
- QKD link emulation part of proto-kms [2]
  - using plain random numbers
- Using a system emulator (runs in containerlab [1])
  - source code is all BSD3 open-source
  - constantly moving forward, feel free to ask
Summary & Outlook
A naive implementation of (parts) QKDN network
- taking the quantum layer as just given
- tons of open questions

Research questions (some of them ;-) )
- actual behavior of a real "complete" QKDN deployment
- how secure are quantum links in real networks?
- the need and the implementation of key hybridization
  - combined quantum derived keys with post quantum cryptography (PQC)
  - centralized vs decentralized control/routing (classical question, isn’t)

Outlook
- authentication of quantum modules and KMS peers with Wegman-Carter Hashes
- system emulator, including coupling with live QKDN
Demo
Containerlab web site. 

da/net proto-kms implementation. 

gosdn gnmi-target. 

gosdn sdn controller. 