


Planning and operating secure and resilient networks

Carmen Mas Machuca
Chair of Communication Networks
University of the Bundeswehr Munich
cmas@unibw.de

Universität der Bundeswehr München

EUCNC 6G Summit
Málaga, Spain ▪ 2-5 June 2026

Mobile Network Evolution

1G	2G	3G	4G	5G	6G
Analog Voice	Digital Messages	Mobile Data	Applications	IoT	Full intelligence & connectivity
2.4 kbps	64 kbps	+10 Mbps	+100 Mbps	+1 Gbps	~Tbps
1980	1990	2000	2010	2020	2030

Fixed Network Evolution

1G	2G	3G	4G	5G	6G
Analog Voice	Digital Messages	Mobile Data	Applications	IoT	Full intelligence & connectivity
2.4 kbps	64 kbps	+10 Mbps	+100 Mbps	+1 Gbps	~Tbps
1980	1990	2000	2010	2020	2030
MMF@850nm SMF@1310nm	SMF@1550nm Optical Amplifiers	FTTx Optical Switching	Coherent Flex Grid	NGPON2/50GPON Fiber sensing	QKD VHS-PON
Tens of kms 2.4 kbps	Hundreds of kms 64 kbps	Thousands of kms +10 Mbps	+4000 kms +100 Mbps	+1 Gbps	~Tbps

Towards 6G…

April 23 5G	China	EU	USA	Japan	SouthKorea
#BS	2,290,000	310,000	100,000	50,000	215,000
Population	1,402,000,000	447,706,000	329,500,000	125,800,000	51,780,000
#5G BS/100,000 inhabitants	163	69	30	40	415
5G Subscribers	357,000,000	31,000,000	79,000,000	14,190,000	25,000,000
Subscribers/ 100,000 inh.	25,464	6,924	23,976	11,280	48,281
June 25 5G	**China**	**EU**	**USA**	**Japan**	**SouthKorea**
#BS	4,251,000	351,600	140,000	151,000	346,460
Population	1,410,710,000	449,206,000	334,900,000	124,900,000	51,712,000
#5G BS/100,000 inhabitants	301	78	42	122	670
5G Subscribers	1,031,800,000	156,716,000	323,200,000	149,900,000	35,000,000
Subscribers/ 100,000 inh.	73,142	35,550	96,503	120,399	67,843

European 5G Observatory

Reliability Requirements Evolution

Survivability through dynamic routing

Tolerated occasional service interruption
Reparation times hours/days

Mobile keeps increasing # nines

5G/6G URLLC with 6 nines availabililty

1980 — 1990 — 2000 — 2010 — 2020 — 2030

Famous benchmark 99,999%
(~5min MDT/year) for PSTN

SLA, MDT, MTTR…
3-5 nines for different services

Cloud & Hyperscalers
“Failures are inevitable; systems must continue operating anyway”

ITU-T Technical Report (10/2025)

GSTR-ION-2030

Technical Report on international optical networks towards 2030 and beyond

But there are still many failures, disasters, attacks,…

- In the European Union, system failures acco… for 93.5% o… hour losses in 2022.
- Natural disasters triggered a record … work inc… ple the number in 2019.
- Undersea cables (carry m… rnet … ruptions annually.

Planning problems by operators

6G

- Extreme low latency (<1ms)
- Extreme high reliability (up to 7 nines)
- Massive connectivity (10M/km^2)
- Extreme high rate (+100Gbps)
- Extreme coverage, low energy, …

Optical

- High reliability
- Robustness
- Extreme Capacity (+Tbps)
- Security
- Low energy

Any service, at any time, on any device, anywhere and instantly

- Increase service requirements
- Increase demands
- Upgrade service portfolio

→ Network Upgrade

- More operators
- Regulators

→ Controled Revenues

Clever network planning and use of resources

Network evolution

Technologies

Optical
Wireless
Satellite
Mobile

Requirements

Reliability
BW
Security
Delay
Sovereignty
Mobility

Services

Games
VR
smartX
Autonomous driving
Computing
Industry
Sensing
eHealth
Data

Players

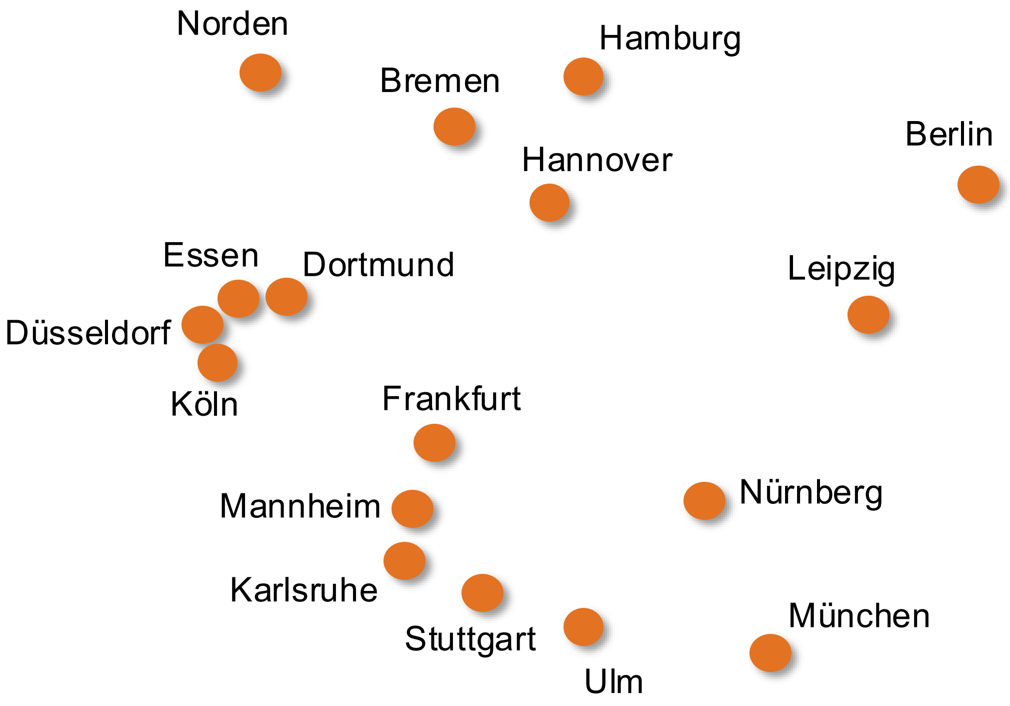
PIP
Data Centers
Hyperscalers
VNO
Telecom

Outline

- Network Operation
  - Secure
  - Resilient
- **Physical Infrastructure**
  - **Secure**
  - **Sovereign**
  - **Robust**

Robust Networks

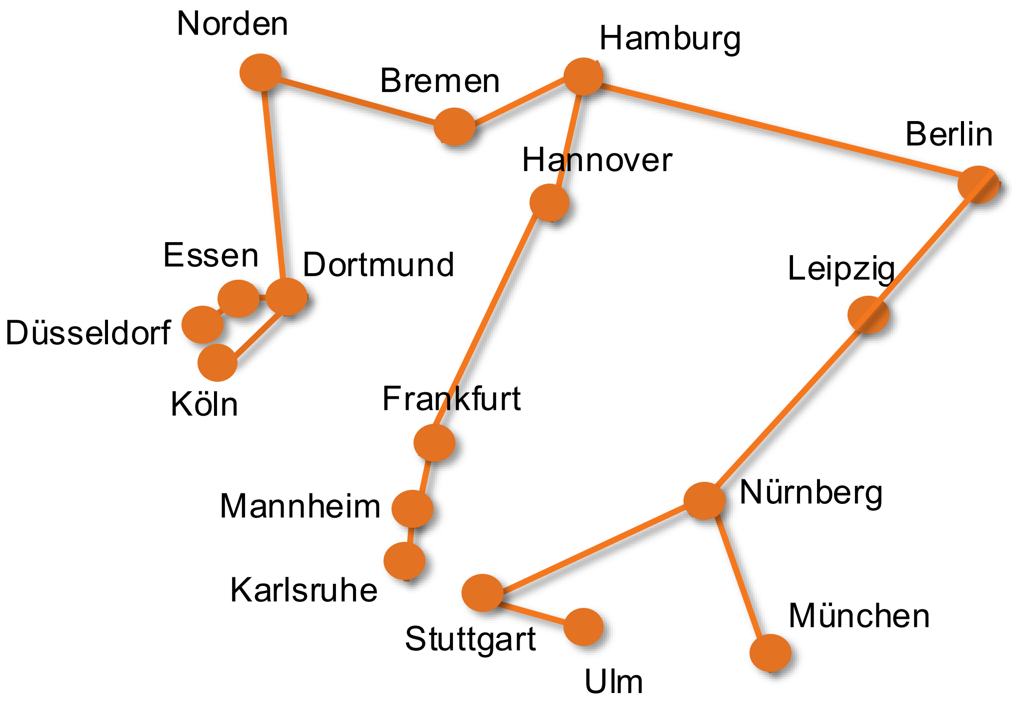
- **Network robustness** is a system's ability to maintain its functionality (e.g., connectivity) when components fail or are attacked.
- Operators **planning problem**



Robust Networks

- **Network robustness** is a system's ability to maintain its functionality (e.g., connectivity) when components fail or are attacked.
- Operators **planning problem**

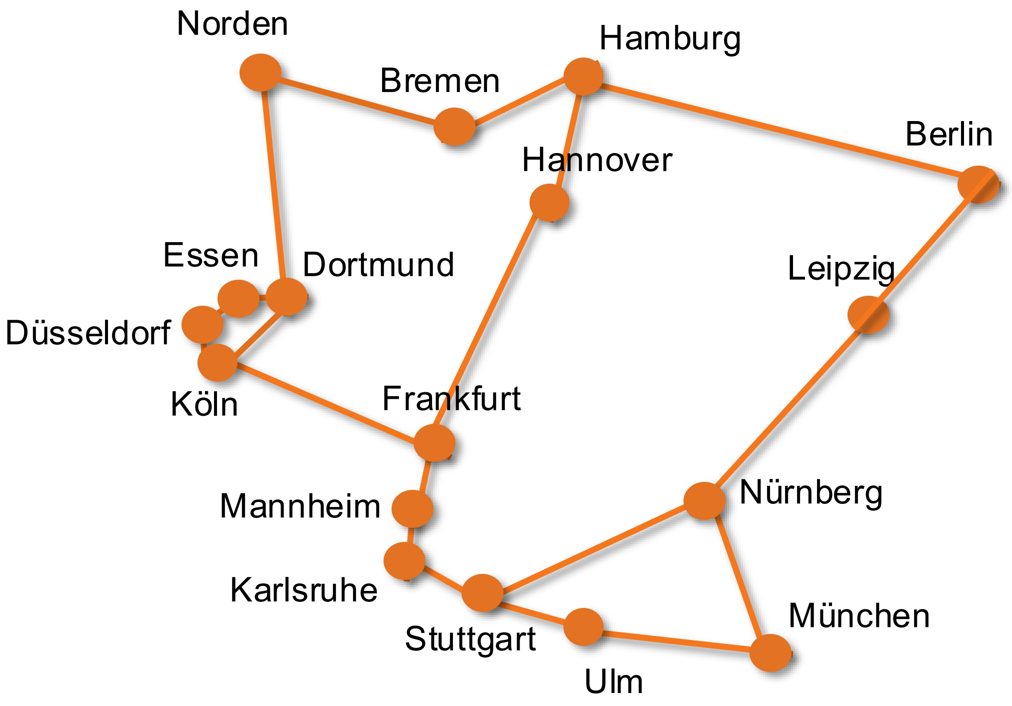
$ **Steiner Tree**



Robust Networks

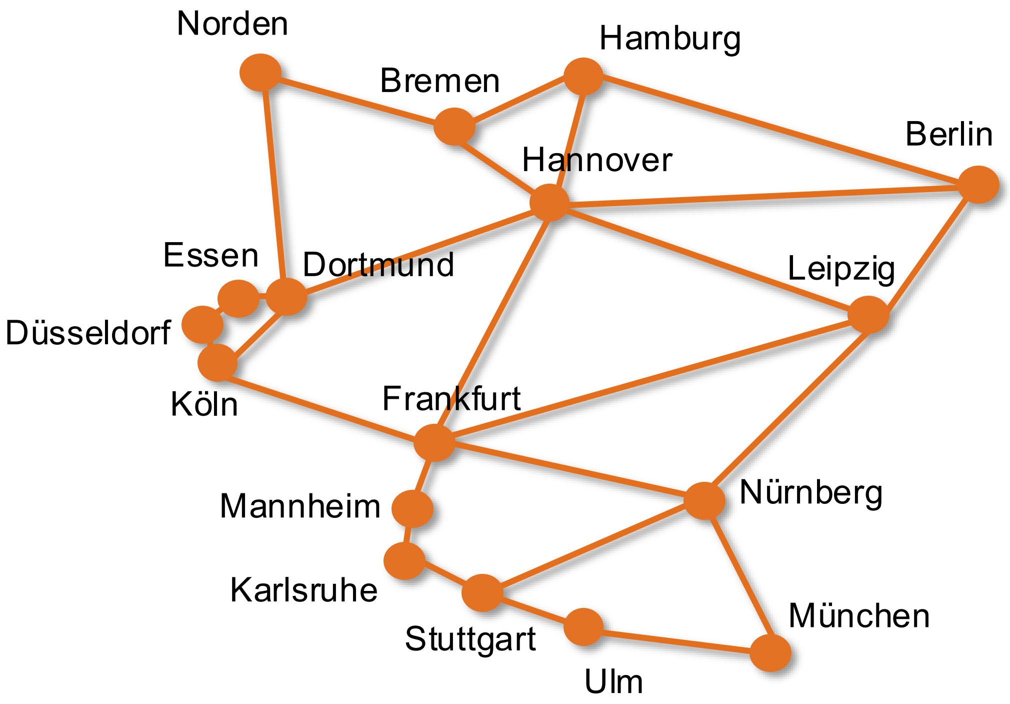
- **Network robustness** is a system's ability to maintain its functionality (e.g., connectivity) when components fail or are attacked.
- Operators **planning problem**

$	**Steiner Tree**
$$	**Bi-connected**



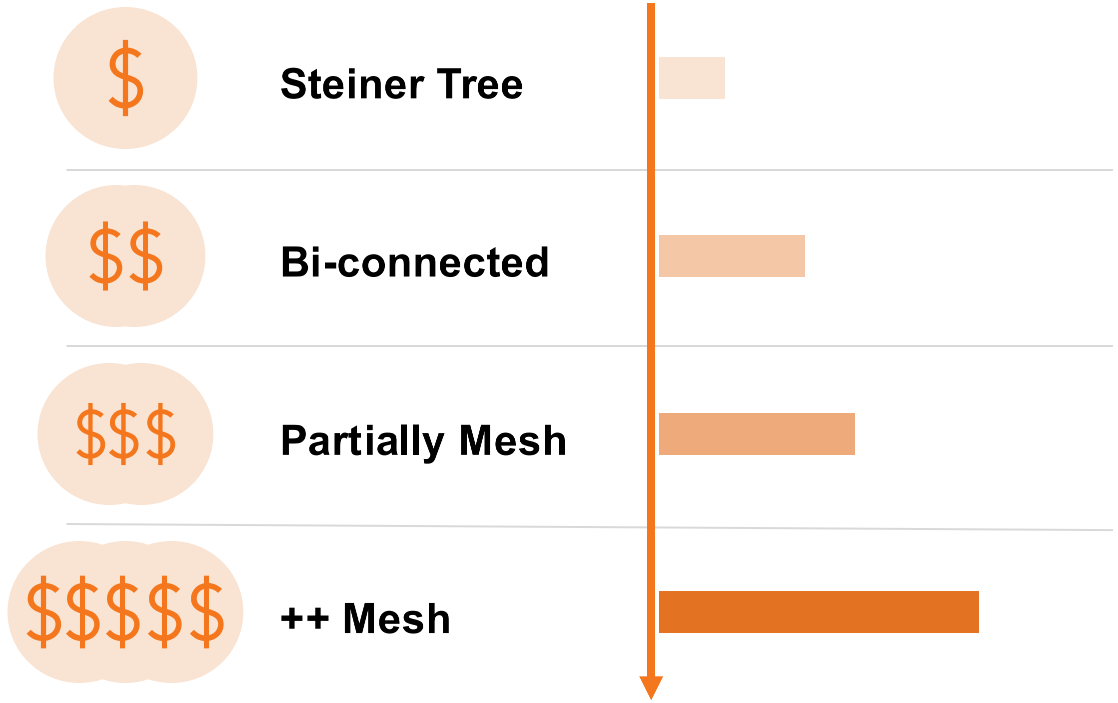
Robust Networks

- **Network robustness** is a system's ability to maintain its functionality (e.g., connectivity) when components fail or are attacked.
- Operators **planning problem**



Robust Networks

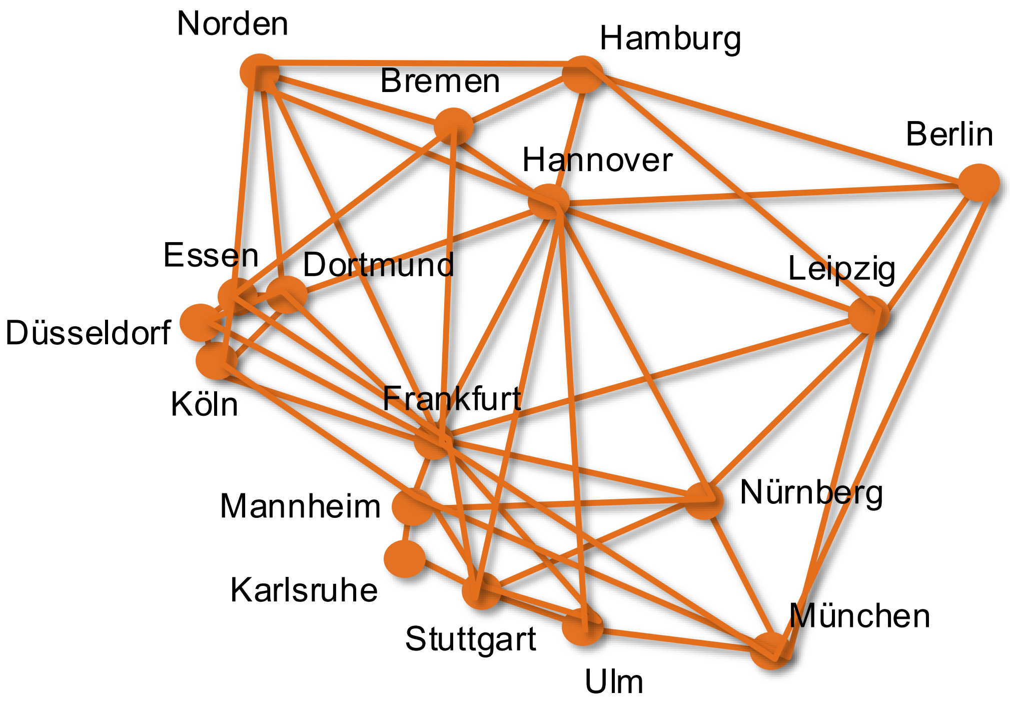
- **Network robustness** is a system's ability to maintain its functionality (e.g., connectivity) when components fail or are attacked.
- Operators **planning problem**



But

How to **measure** robustness?

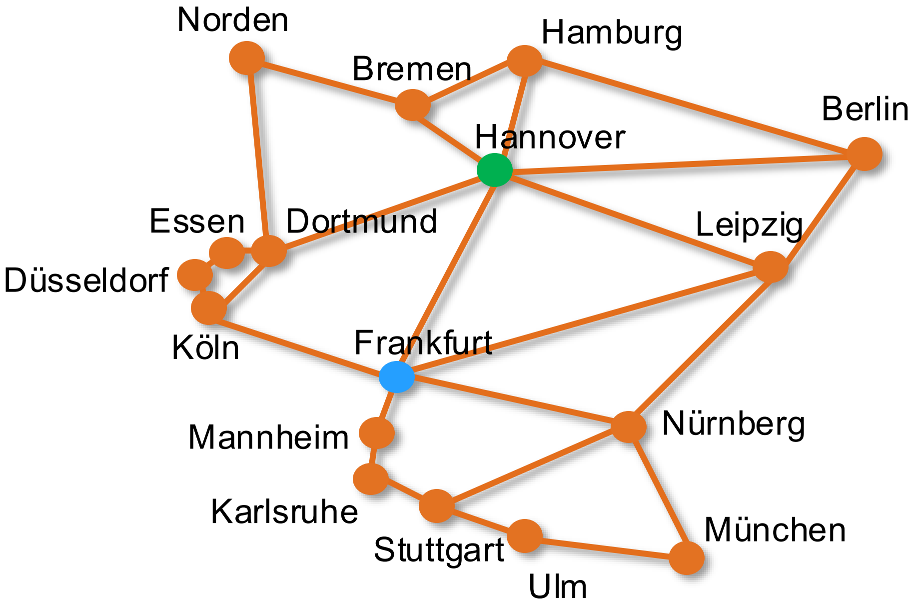
Against **what?**



Robust Networks

Centrality metrics

- Node centrality (NC)
- Closeness centrality (CC)
- Betweenness centrality (BC)
- Eigenvector centrality (EC)



Frankfurt highest **CC** and **BC**

Hannover highest **NC** and **EC**

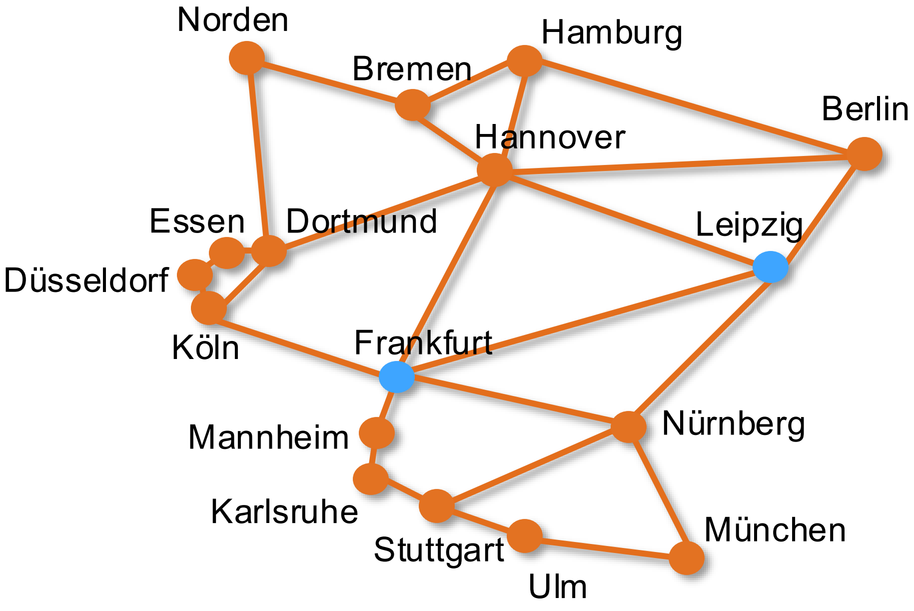
Robust Networks

Centrality metrics

- Node centrality (NC)
- Closeness centrality (CC)
- Betweenness centrality (BC)
- Eigenvector centrality (EC)

Structural metrics

- Relative Size of the Largest Component (rLLC)
- Connectivity
- MinCutSet
- …



rLLC = 17

Connectivity = 136

MCS$_{(\text{München},\text{Hannover})}$ = {Nürnberg, Stuttgart},
{Leipzig, Frankfurt},
{Mannheim, Nürnberg},
…

Robust Networks

Centrality metrics

- Node centrality (NC)
- Closeness centrality (CC)
- Betweenness centrality (BC)
- Eigenvector centrality (EC)

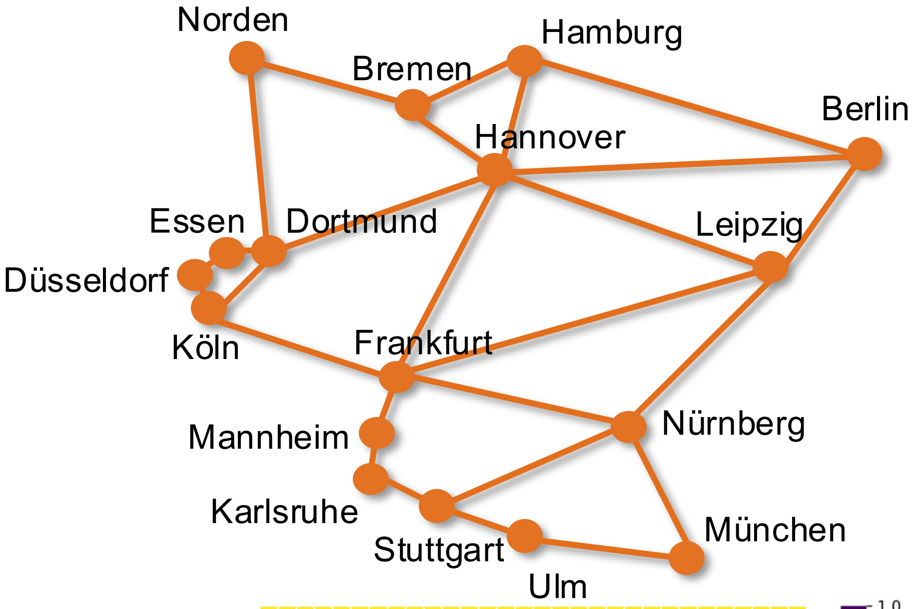
Structural metrics

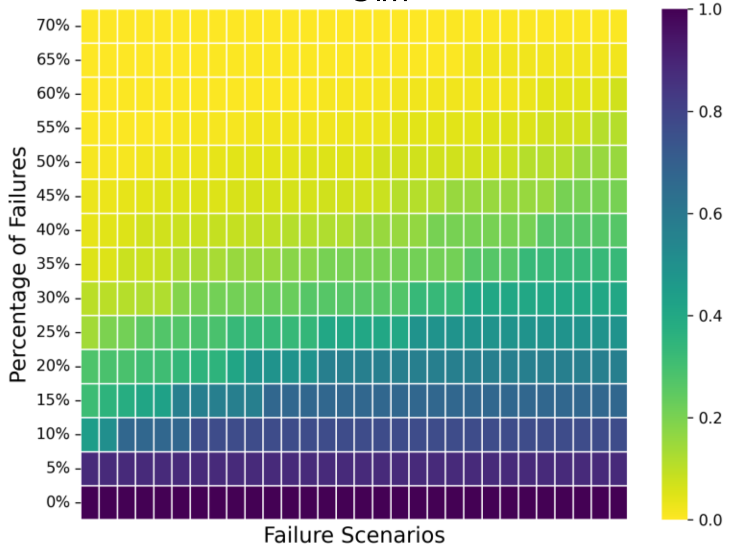
- Relative Size of the Largest Component (rLLC)
- Connectivity
- MinCutSet
- …

Evaluation

- Robustness surface
- Robustness line
- …

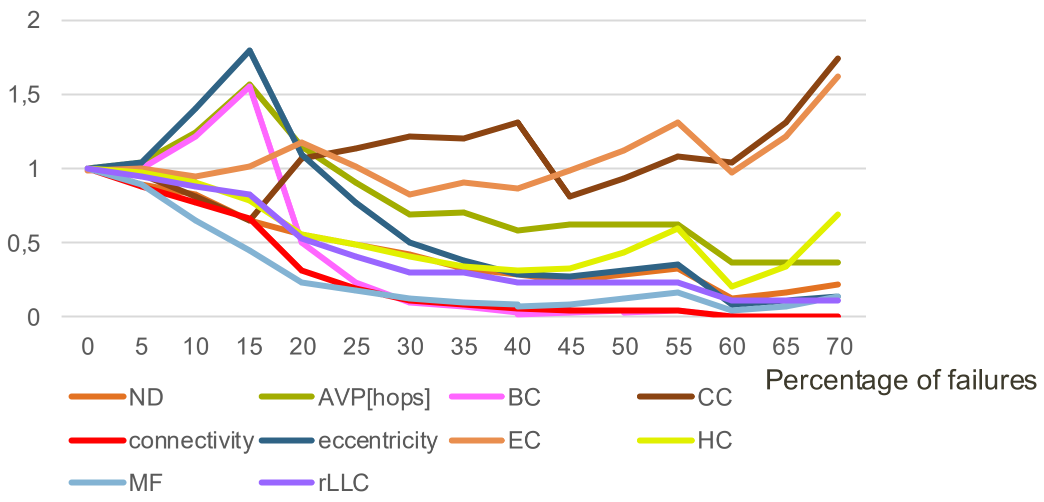
https://github.com/shakthij98/PyRobust/

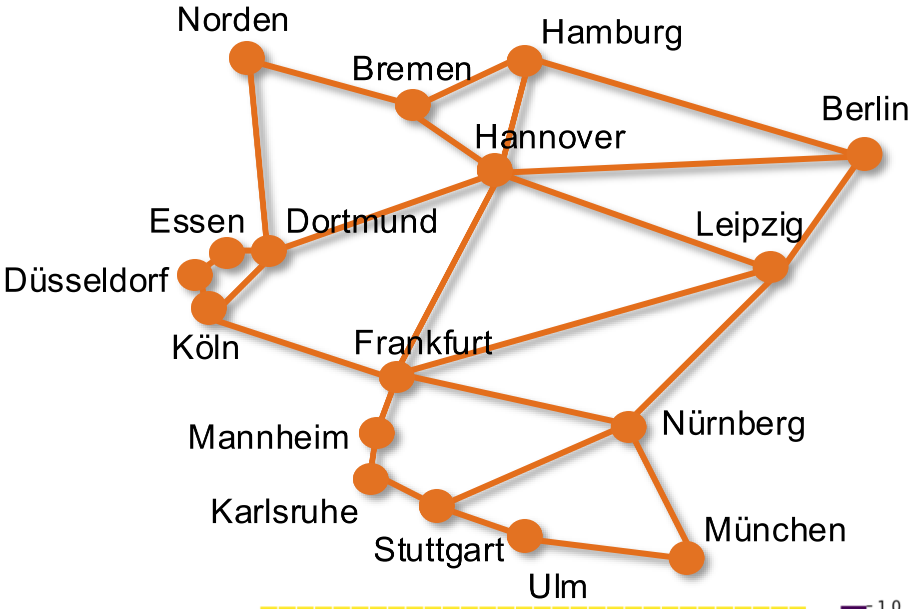


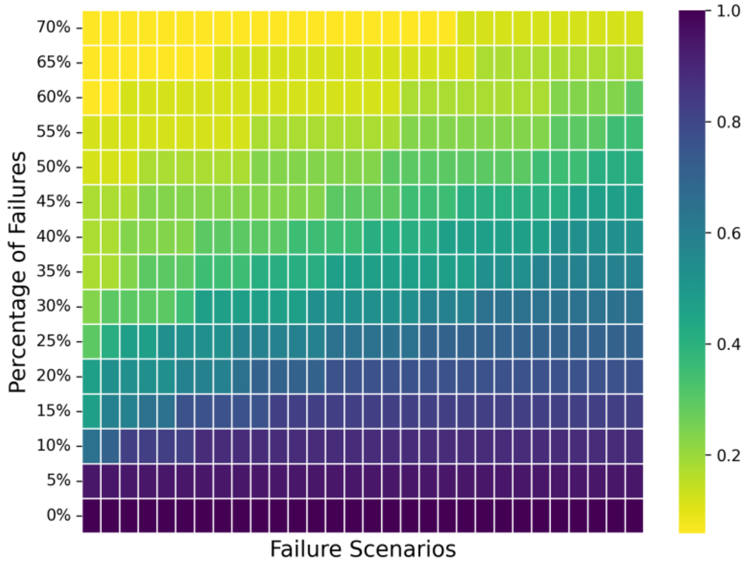


Connectivity
Random Failures

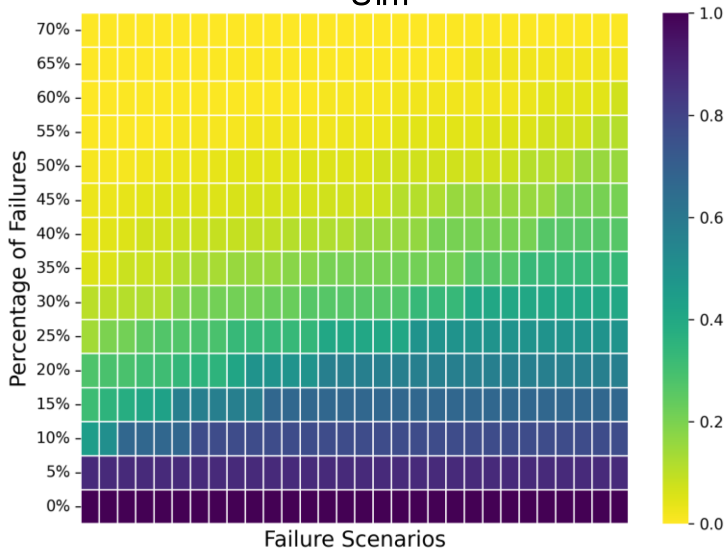
Robust networks





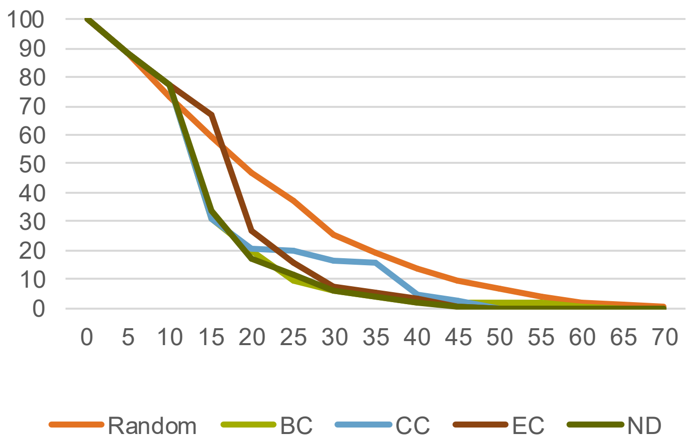


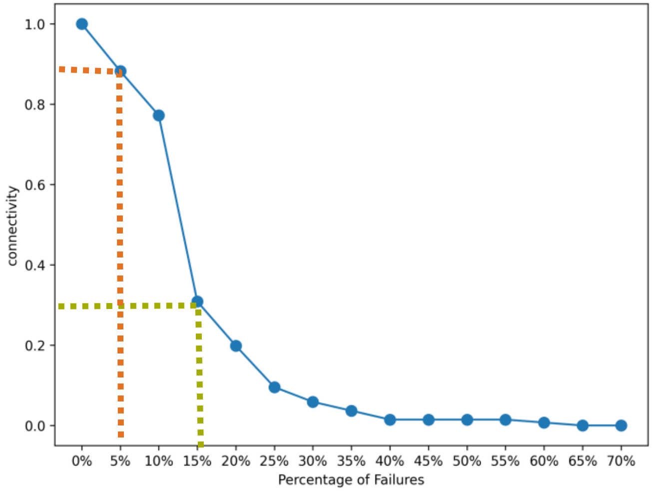
rLLC Random Failures



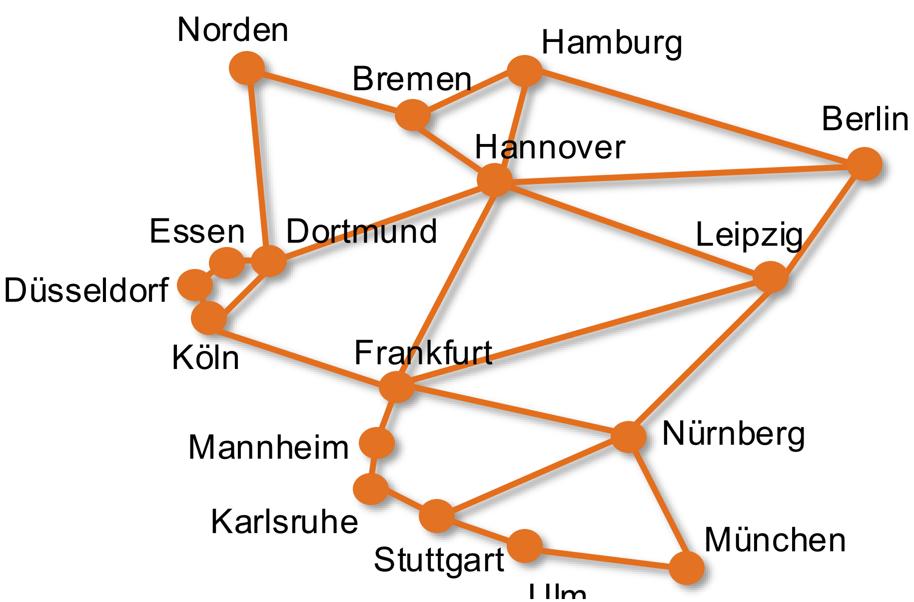
Connectivity
Random Failures

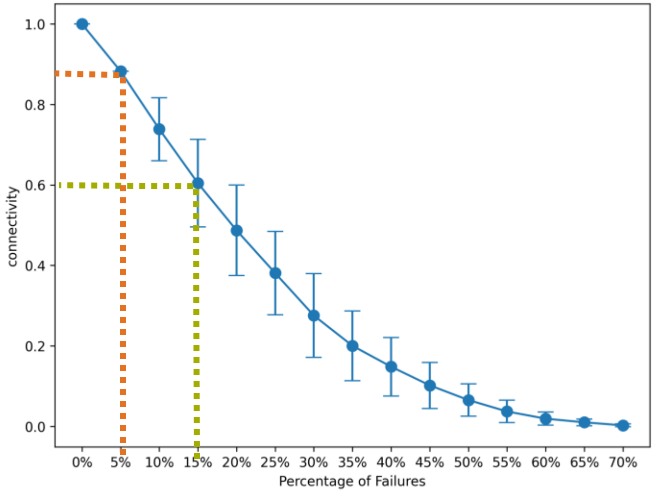
Robust Networks





Connectivity
Targeted Failures (according to BC)

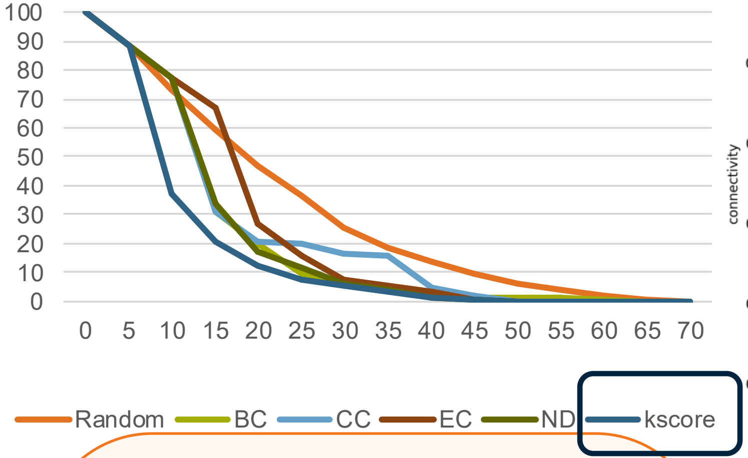




Connectivity
Random Failures

Connectivity
Random Failures

Robust Networks



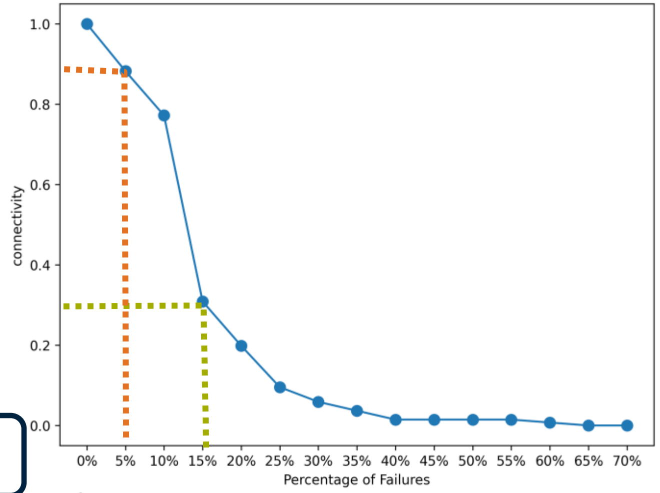
Given (s,d),

- find the MCSs,
- Sort them according to cardinality

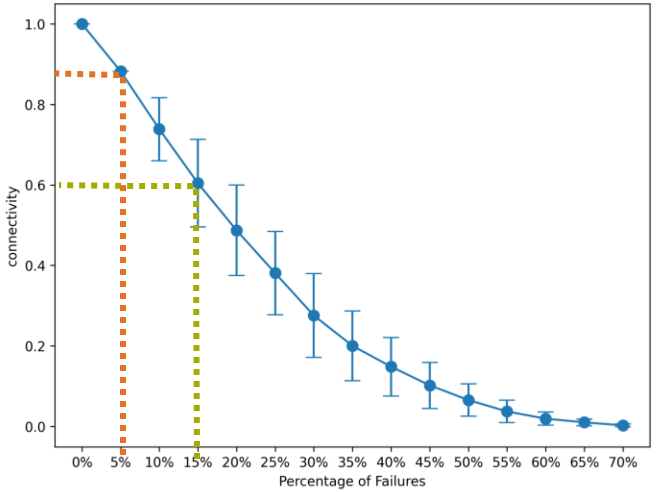
→ the smaller MCS_{small} → the lower the robustness

→ better to „target“ nodes that appear in more MCS

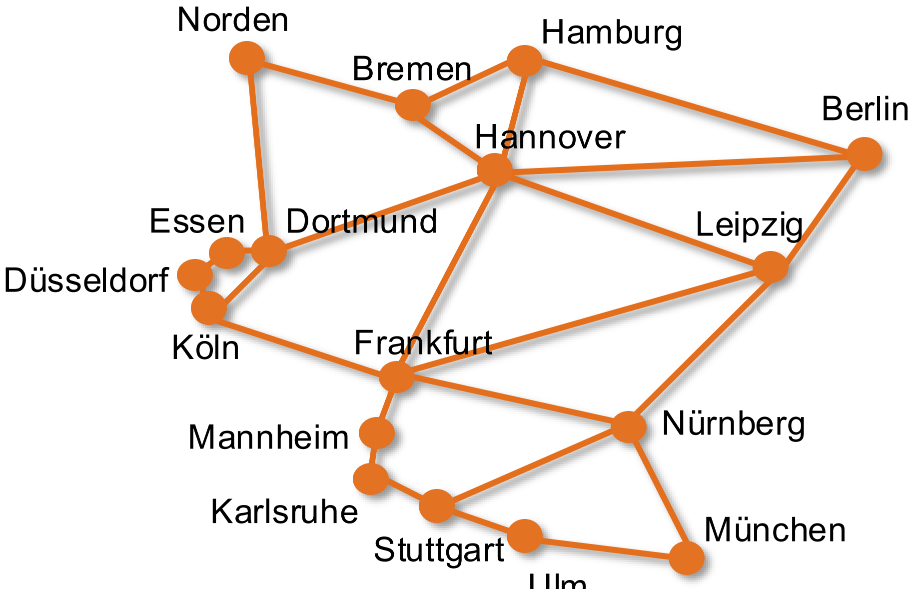
→ preference to smaller MCS than larger MCS

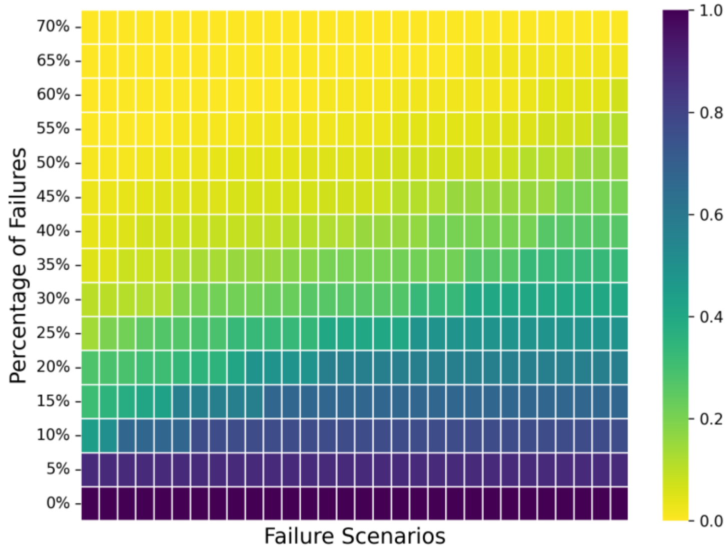


Connectivity
Targeted Failures (according to BC)



Connectivity
Random Failures





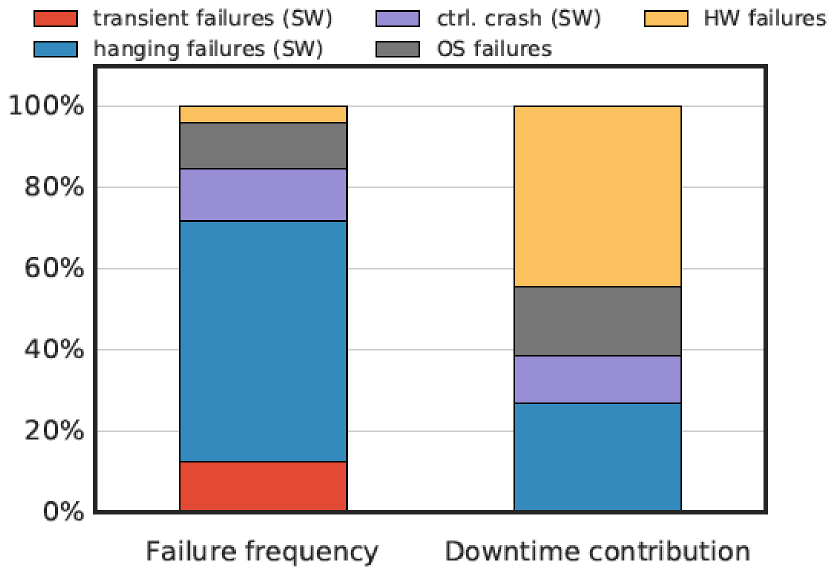
Connectivity
Random Failures

Toward robust networks

Increase Connectivity

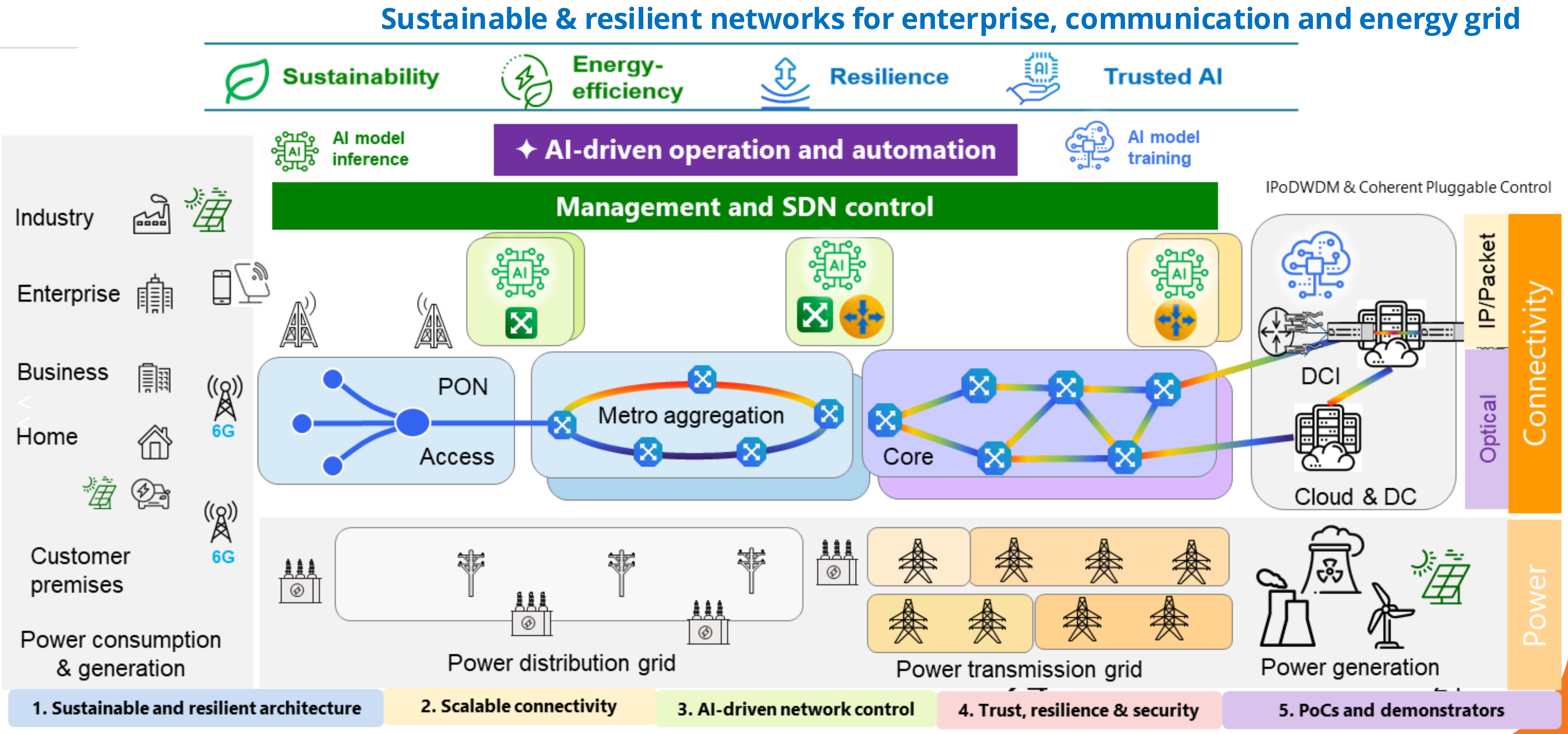
Update Awareness

And capacity…
without increasing
spare



Toward robust networks

SUSTAINET-advance



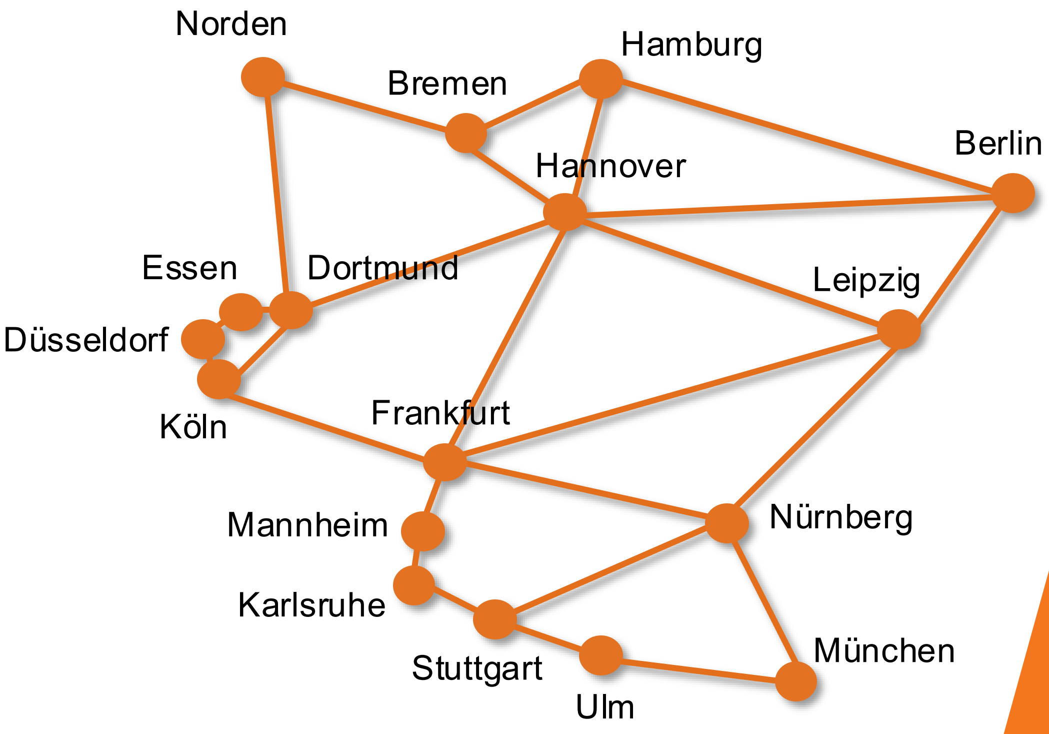
Toward robust networks

Increase Connectivity

Update Awareness

Reduce Dependability

Sovereignty



Sovereignty

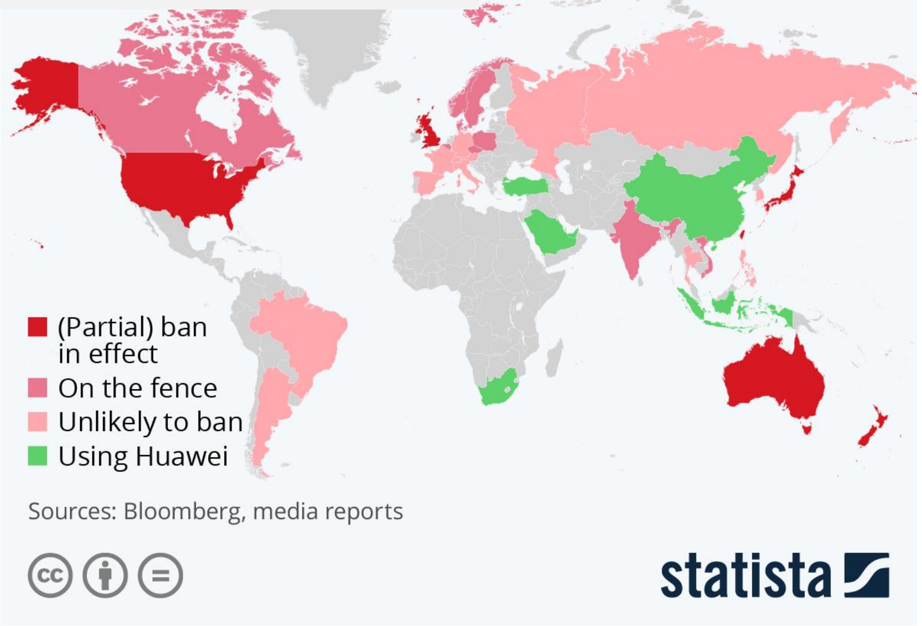
Sovereginty: It is a system's ability to maintain its functionality and connectivity when manufacturer’s components fail or are unavailable

By European Interest

January 21, 2026

EU plans phase-out of telecom suppliers from “high-risk” countries

CROWDSTRIKE



Availability vs. Sovereignty

Availability of a component

Which component?

Independent component failures

Architecture

Cost

Routing

Availability of a manufacturer

Which manufacturer?

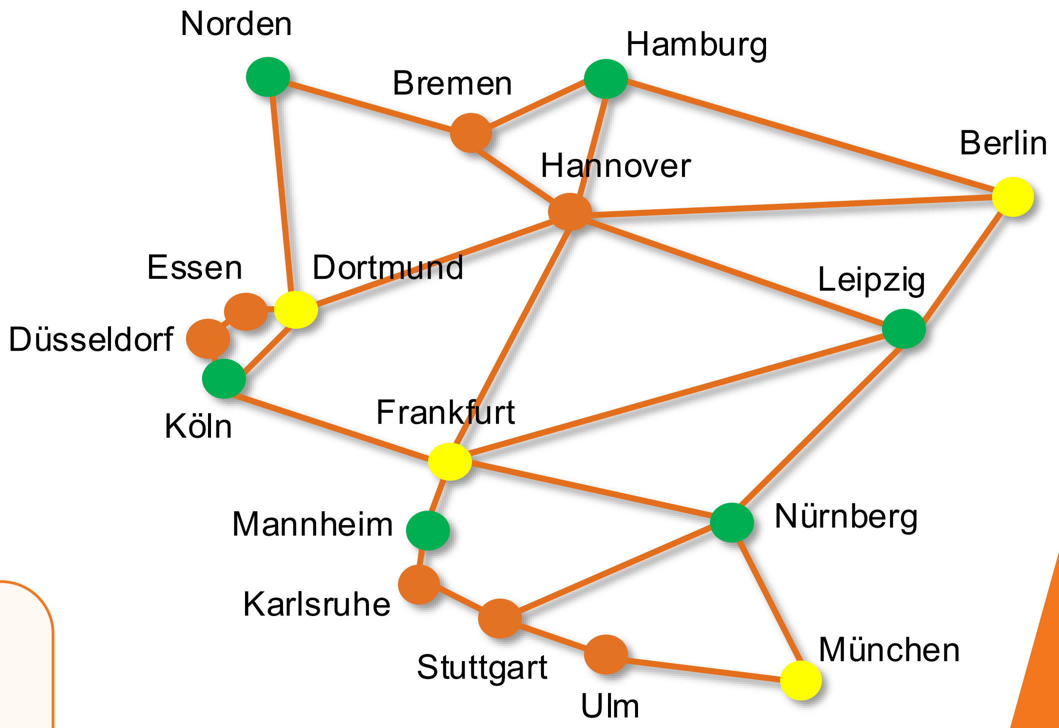
Where to be placed?

How many?

All components of a manufacturer considered to be failed

Towards robust and sovereign networks

- Sovereignty metric missing
- Communication required between operators, regulators, government, manufacturers, etc.
- At which level?
- Operators: Network planning problem(s):
  - How many different manufacturers are required?
  - Where to place them?
  - Interoperability?

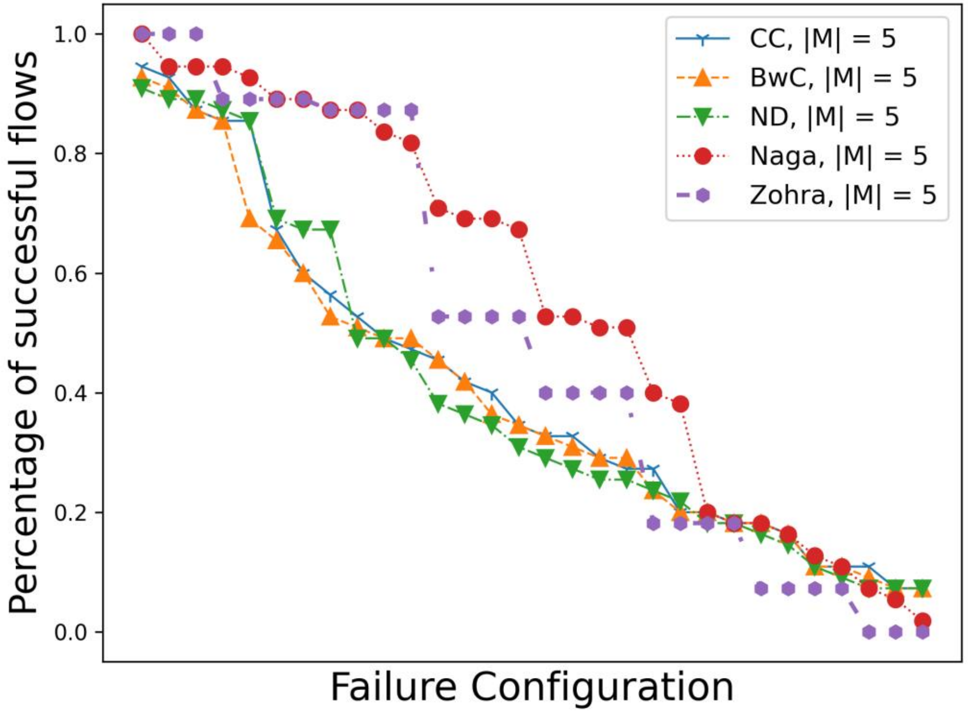


Given a network, the expected traffic, and the number of manufacturers in the market

What is the best manufacturer assignment possible such that the impact of manufacturer failures is minimized?

Manufacturer Assignment for Sovereignty (MAS) problem

- Proposed solution: based on the Path Set Diversity Score → Reduce diversity of manufacturers along the different paths.



Abilene with 5 manufacturers

Janardhanan et al. „Network Sovereignty: A Novel Metric and its Application on Network Design" IEEE Trans. On Reliability 2026

Towards secure networks: PQC and QKD

Quantum computers threat asymmetric public-key cryptosystems. potentially break current cryptographic algorithms, namely Diffie-Hellmann or Rivest-Shamir-Adleman~(RSA) algorithm in polynomial time.

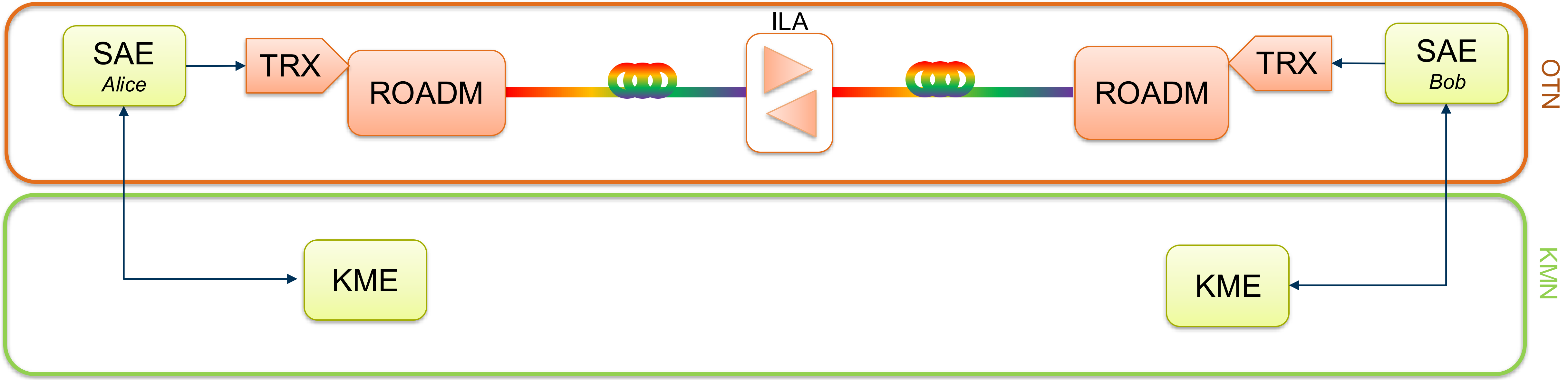
PQC

- Software
- Hard mathematical problems
- Scalable
- Performance overhead

QKD

- Hardware
- Quantum mechanics (Heisenberg's uncertainty principle)
- Low/Costly scalability
- Eavesdropper detection

QKD Architecture



ROADM: Reconf. Optical Add Drop Multiplexer

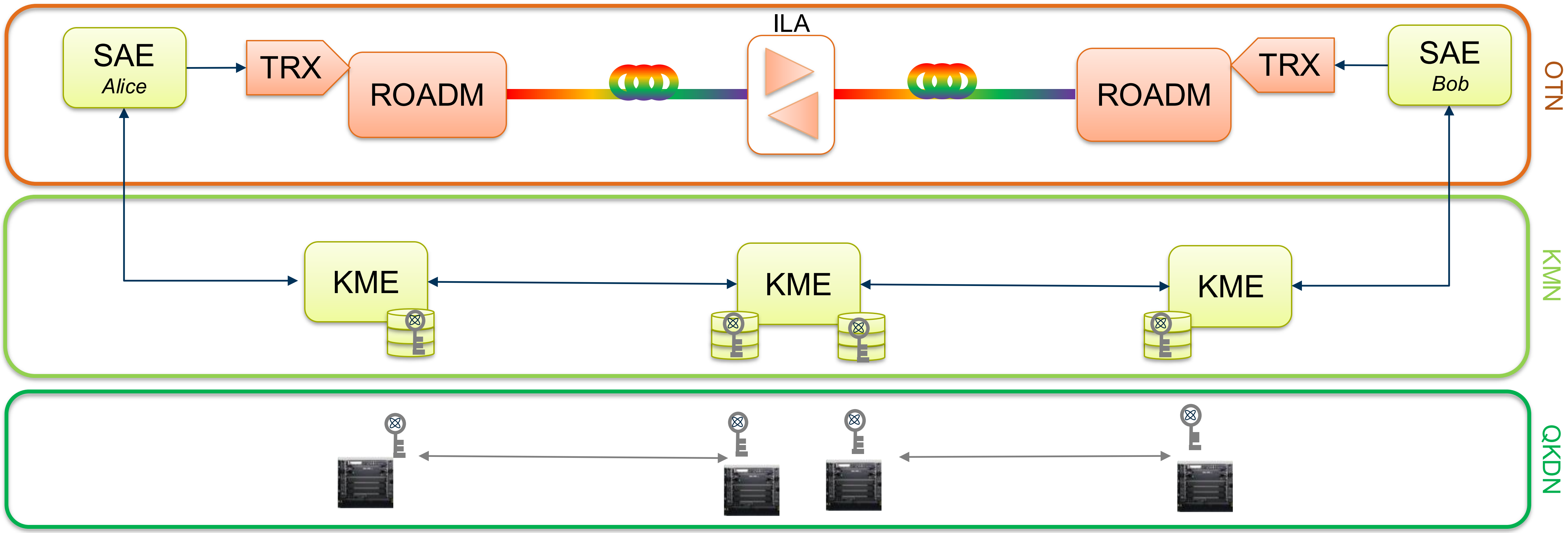
ILA: In-Line Amplifier

SAE: Secure Application Entity

KME: Key Management Entity

M. Wenning et al. „Multi-layer optimization for QKD and key management networks“ JOCN 15 (11), 2023

QKD Architecture



ROADM: Reconf. Optical Add Drop Multiplexer

ILA: In-Line Amplifier

SAE: Secure Application Entity

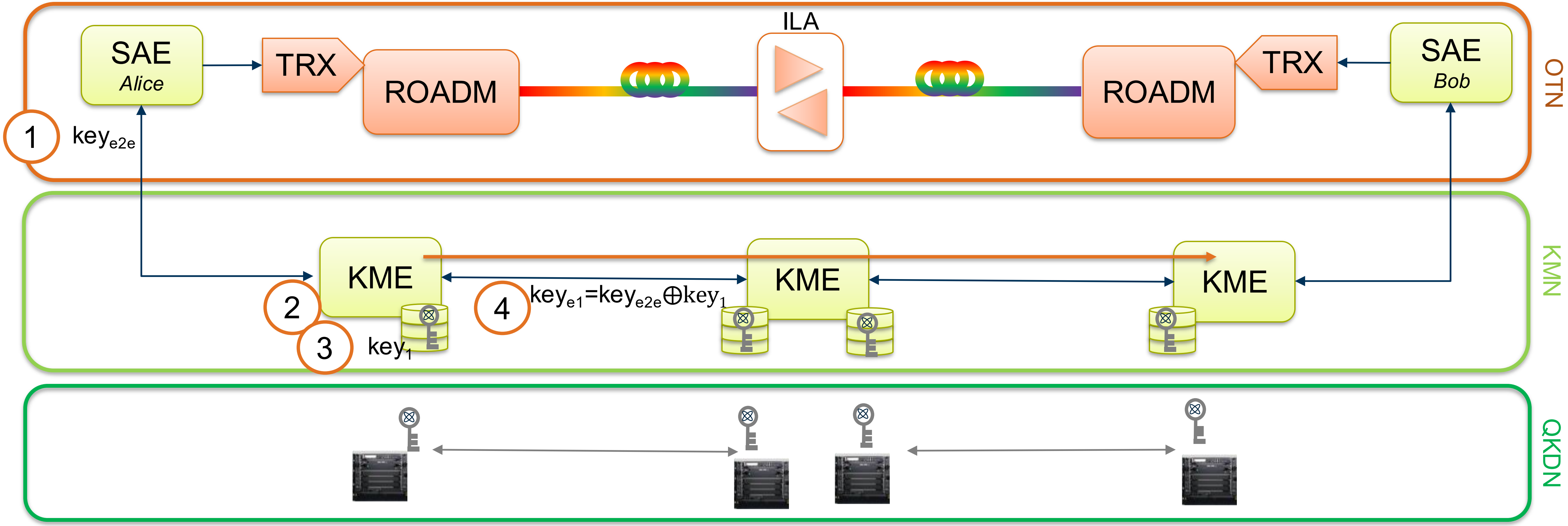
KME: Key Management Entity

Classical channel

P2P QKD links

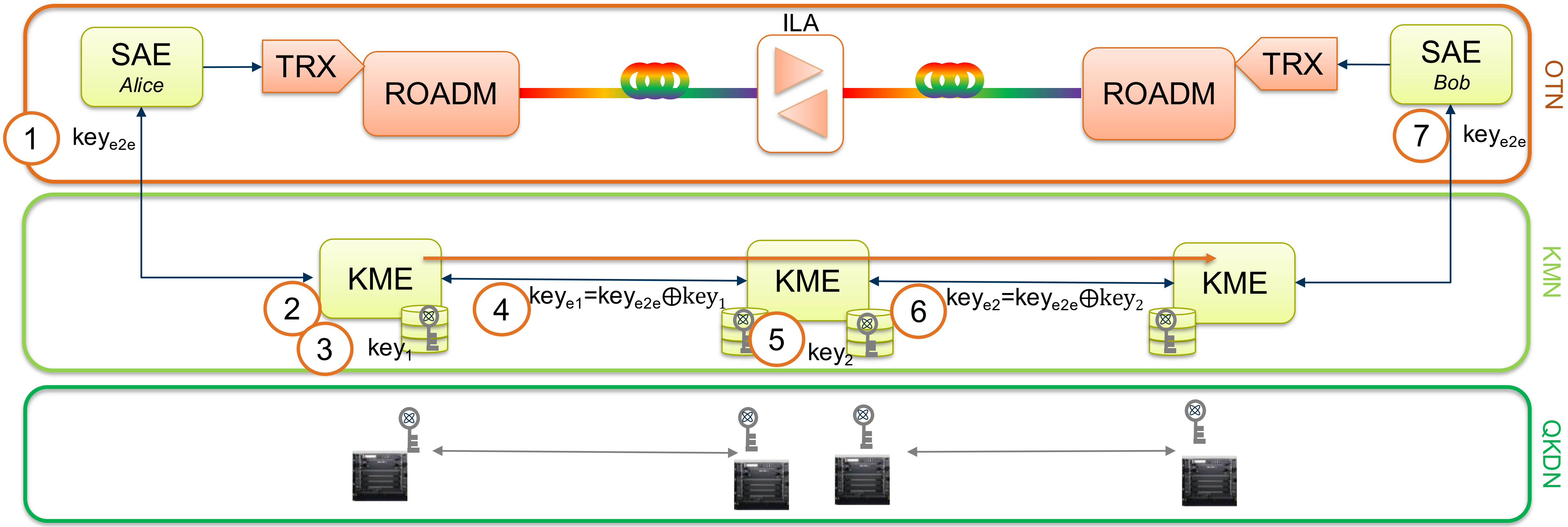
M. Wenning et al. „Multi-layer optimization for QKD and key management networks" JOCN 15 (11), 2023

QKD Architecture



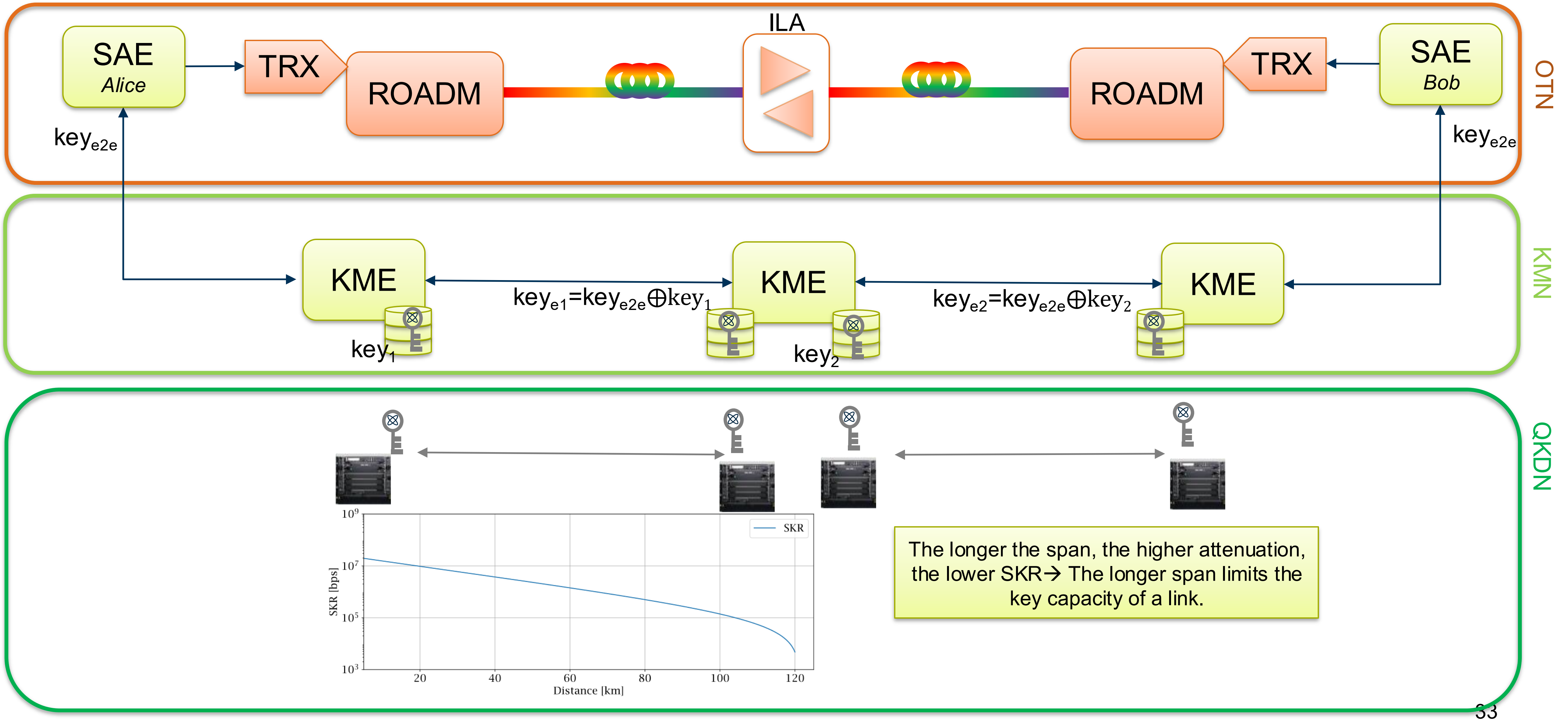
M. Wenning et al. „Multi-layer optimization for QKD and key management networks“ JOCN 15 (11), 2023

QKD Architecture



M. Wenning et al. „Multi-layer optimization for QKD and key management networks" JOCN 15 (11), 2023

QKD Architecture

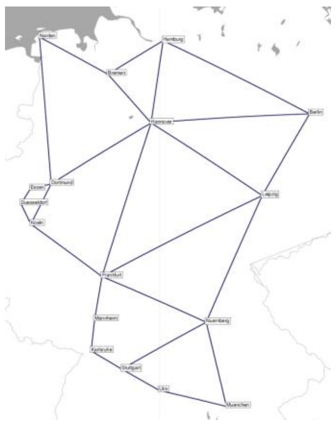


M. Wenning et al. „Multi-layer optimization for QKD and key management networks" JOCN 15 (11), 2023

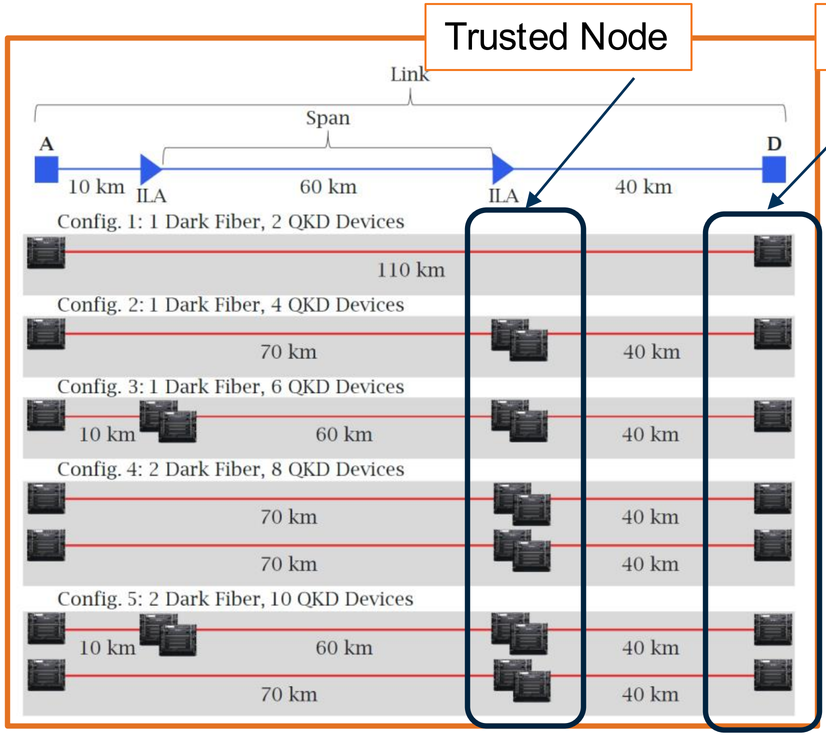
Multi-Layer Optimization

QKD- and KM-Networks: Static Scenario

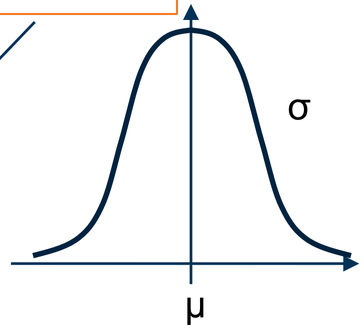
Find the minimum required number of QKD devices to assure the required keys.

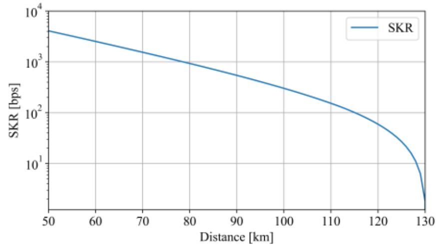


Network topology
Demands (s_i, d_i, c_i)



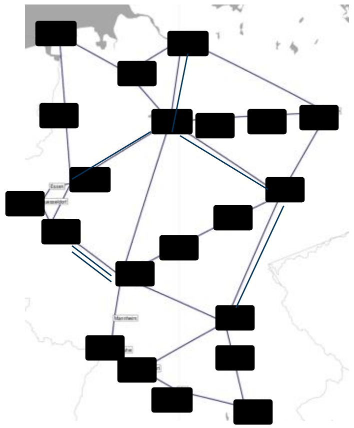
Possible QKD Link Configurations and associated costs





SKR Link Model

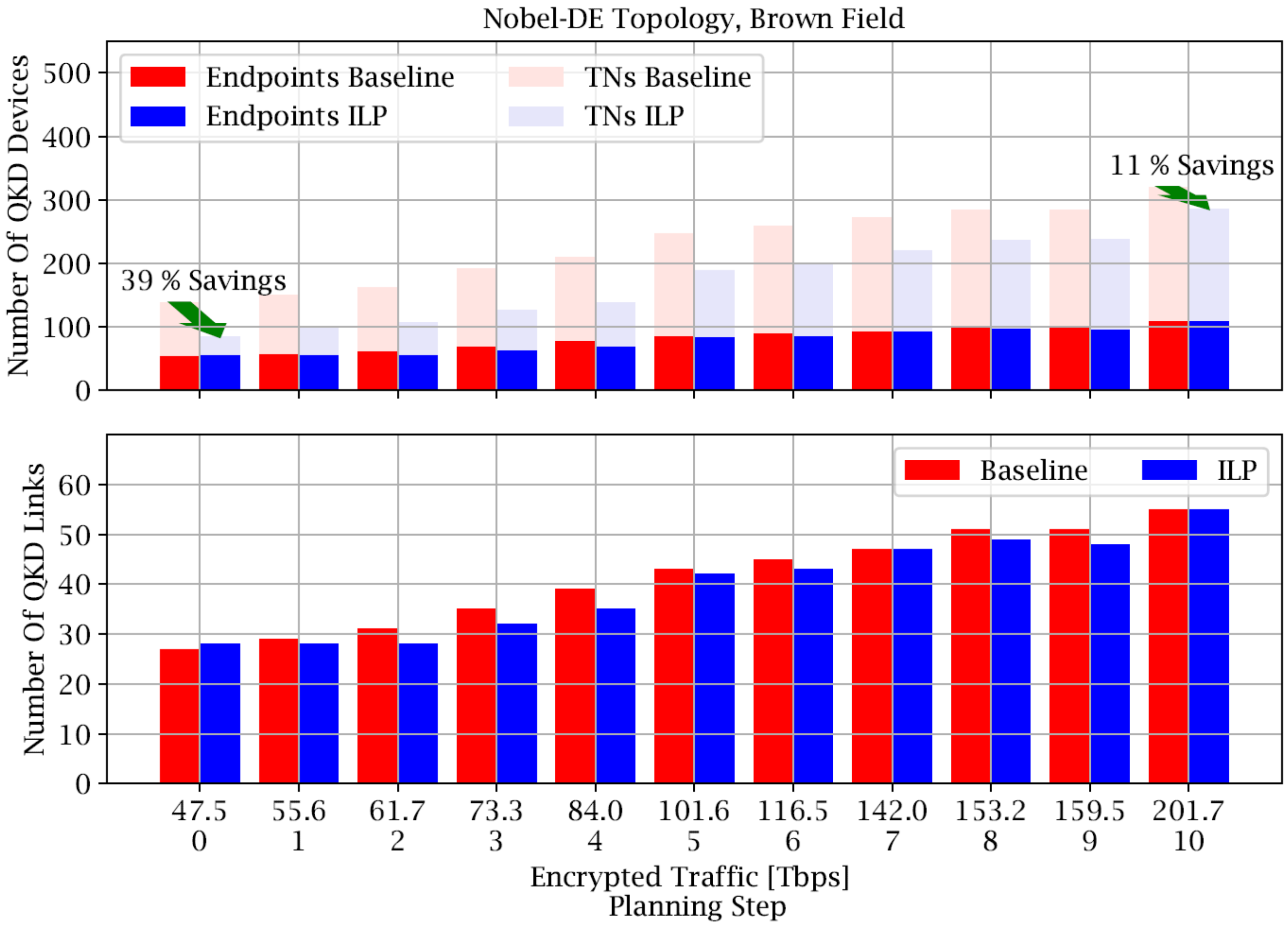
ILP



QKD Deployment

Multi-Layer Optimization

QKD- and KM-Networks: Static Scenario



The number of QKD links is equal to the number of endpoint QKD devices / 2

First period:

- Savings of 39% in QKD devices compared with the baseline thanks to joint routing and deployment.
- Similar QKD links, but ILP uses less costly links.

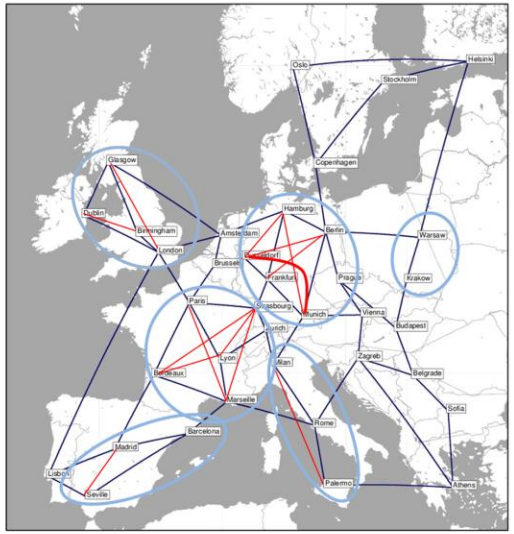
Savings decrease for higher traffic

Towards network operation

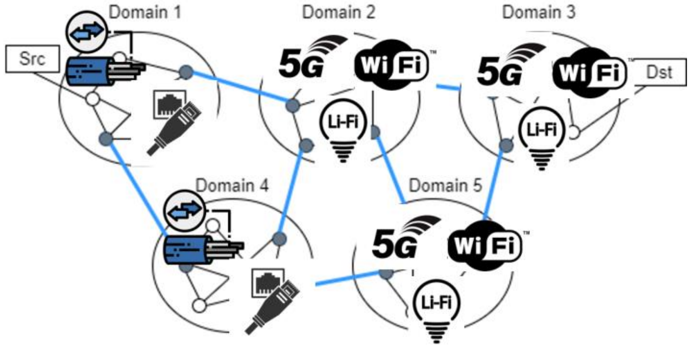
Network Operation	Secure
	Resilient
Physical Infrastructure	Secure
	Sovereign
	Robust

Resilient communications

- Protection mechanisms (1+1, 1:1, 1:N…)
- Restoration algorithms
- Importance of risk sharing (link, node, duct, power supply, disasters, etc.)
- Monitoring and Fiber sensing, crucial for early failure detection
- Pro-active restoration: flows, data, computation, etc.
- Multi-domain: how to guarantee resilience across operators, technologies, etc.



M. Samonaki et al "Survivable Node-Disjoint Routing in Multi-Domain Networks" ICC 2023

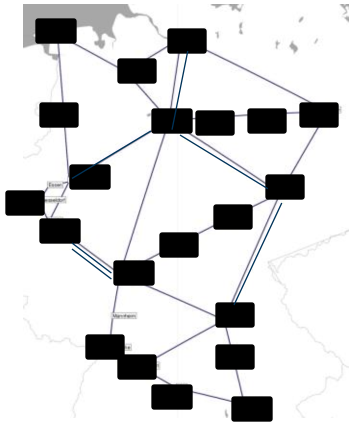


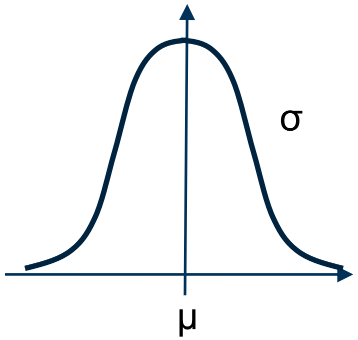
M. Samonaki "Planning for Reliable Multi-Technology Networks Under QoS Guarantees" WiOpt 2026

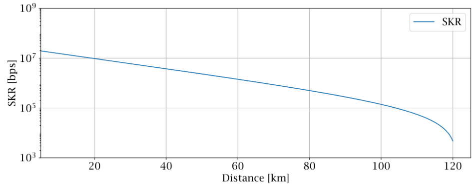
Resilient and secure key distribution

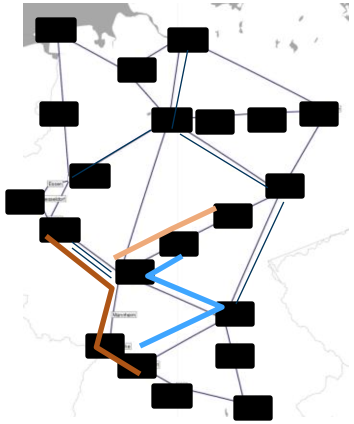
QKD- and KM-Networks: Dynamic Scenario

Dynamic placement of QKD paths based on SKR and Buffers









QKD Deployment

SKR Link Model to fill the buffer

ILP-based routing depending on key buffer filling

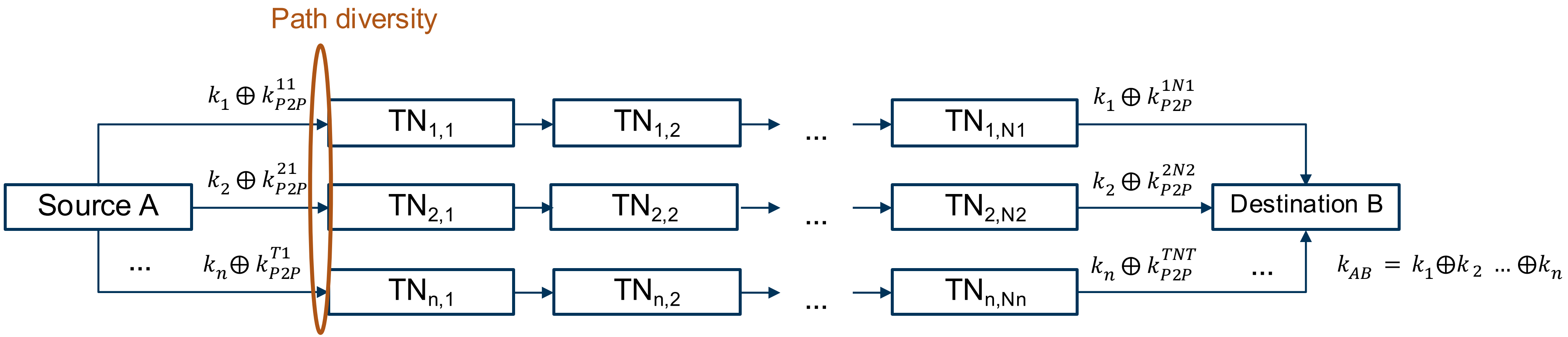
“Multi-Layer Optimization for QKD- and Key-Management-Networks” M. Wenning et al. JOCN’23

E2E Security

Secret sharing

The shorter the QKD path and the less number of trusted nodes→ the higher the security

To increase security→ secret sharing→ leverages node-disjoint paths to distribute shares (k_i) of the E2E (k_{AB}) key



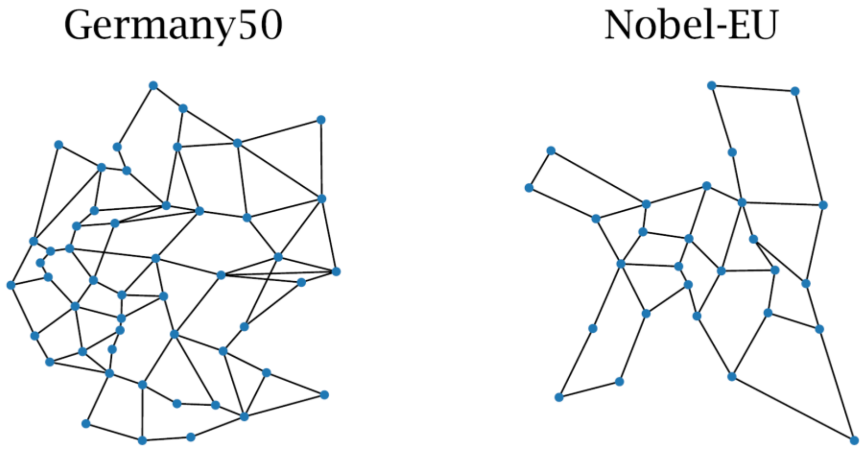
With n =1, all TNs know the secret.

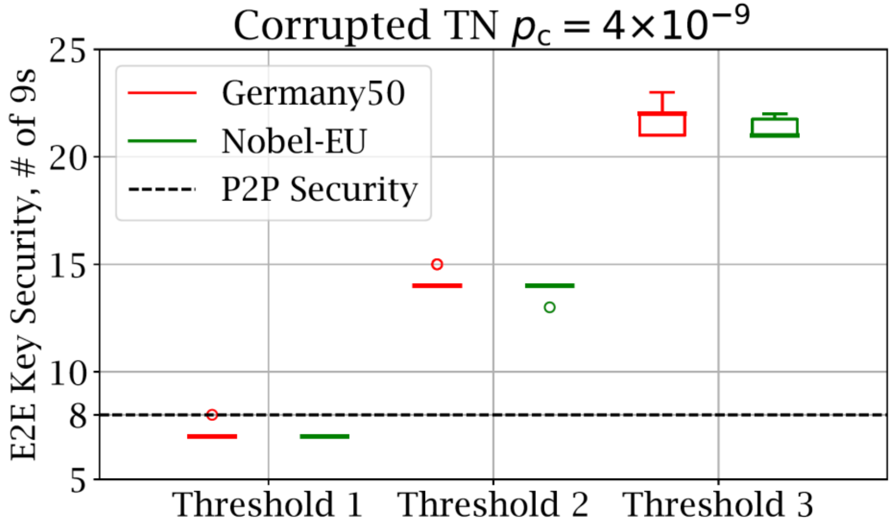
Applying a (n, n) secret sharing scheme over TN-disjoint paths → n shares need to be known to find the E2E key→ Increases the minimum number of hacked TNs to n to learn the secret key.

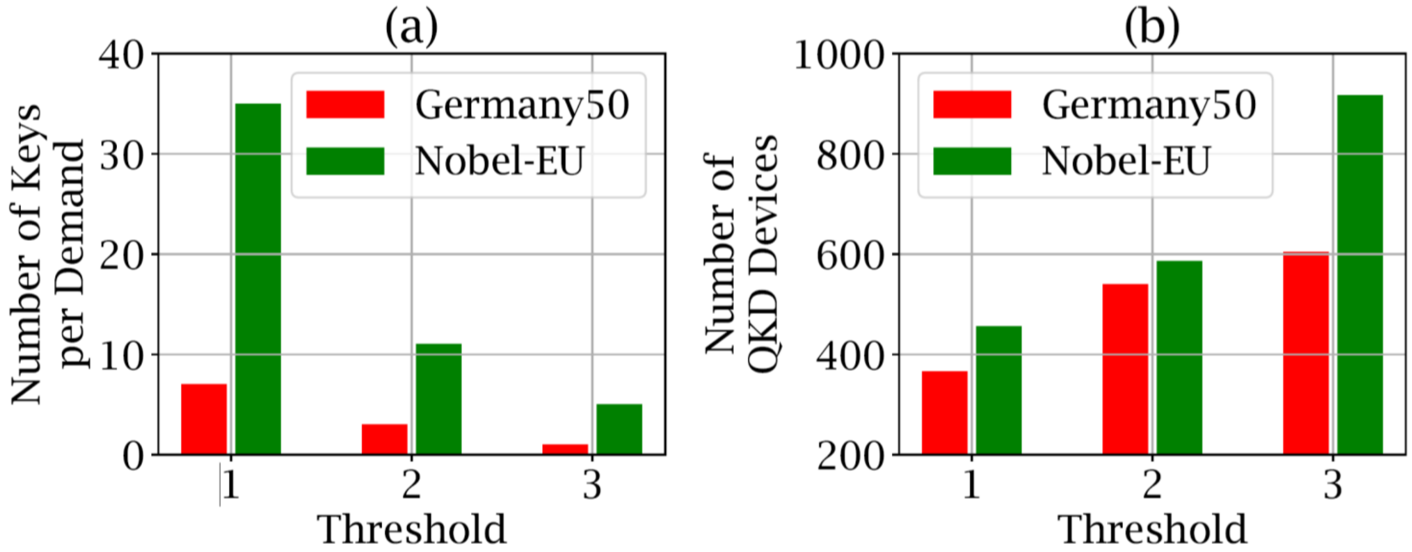
Potential attackers need to hack at least one TN of n different paths to obtain the E2E key.

E2E Security

Security analysis







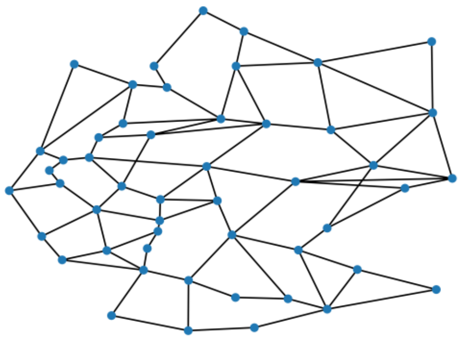
Security has increased, but what about the E2E availability?

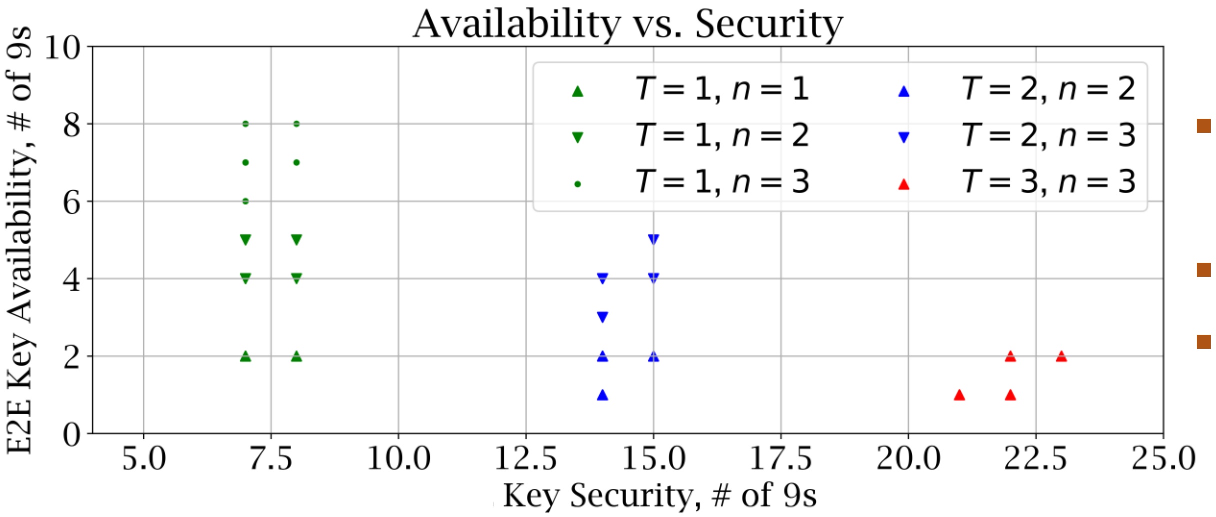
↑ Availability for T=1 and higher n

↑ Security for T=n

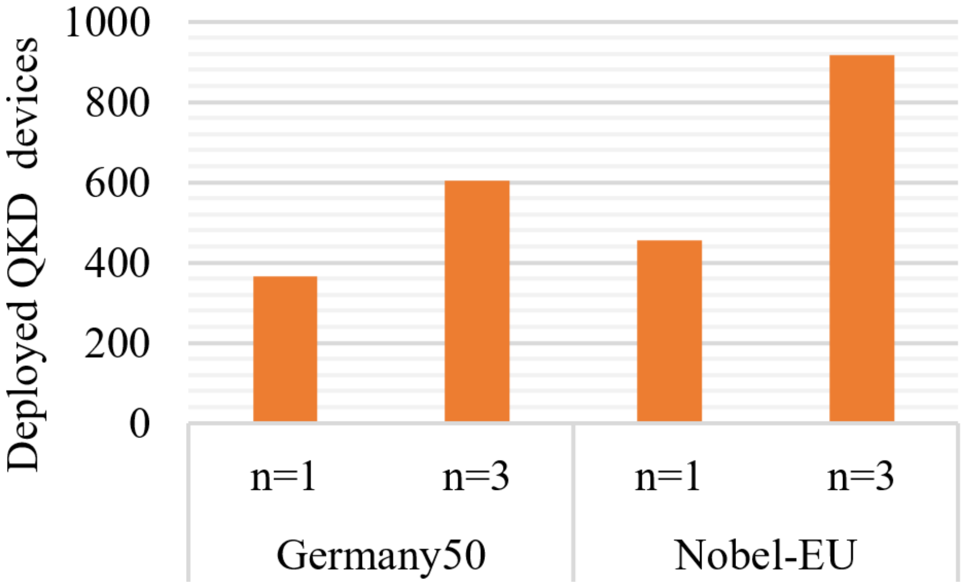
E2E Security

Secret sharing: increasing security and availability





- T directly related to the security
  - → larger T (in colors), + security.
- For a given T→ larger n, + availability
- → But n limited by topology



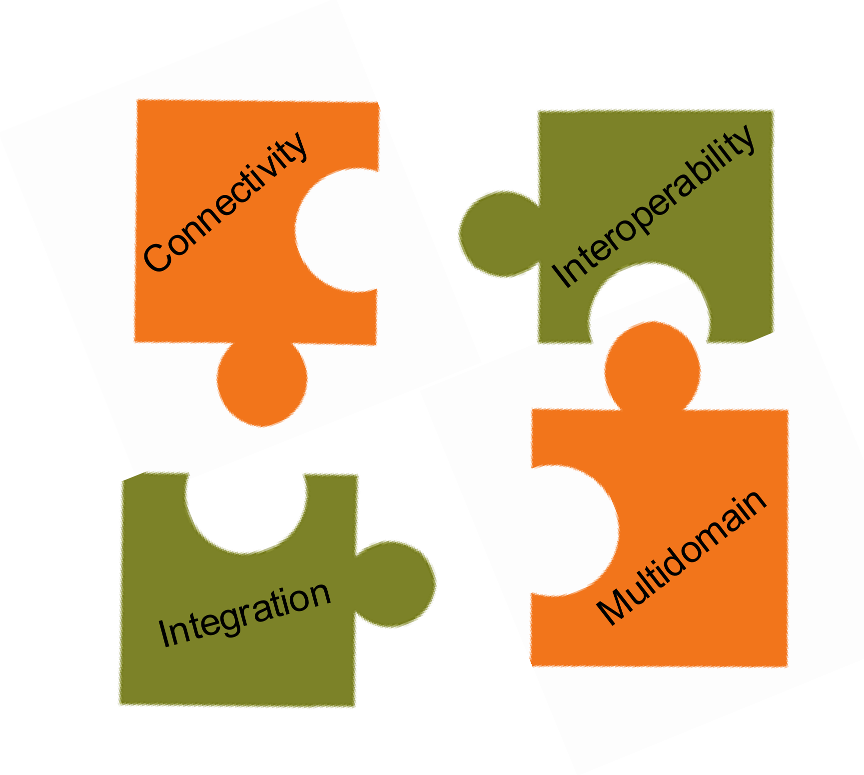
Germany50 requires 65% more QKD devices to increase the E2E availability from two to more than six 9s.

The large size of Nobel-EU requires almost twice the QKD devices to increase the E2E availability to more than six 9s.

Closing remarks

Network Operation
- Secure
- Resilient

Physical Infrastructure
- Secure
- Sovereign
- Robust





Thank you!


Dr. A. Sharma


C. Bermudez


M. Zitkovich


R. Agarwal


C. Vasquez


C. Anzola


M. Wenning


S. Janadhanan


M. Samonaki

Carmen Mas Machuca
Chair of Communication Networks
University of the Bundeswehr Munich
cmas@unibw.de

Universität der Bundeswehr München