Reliable networking in the Secure Networking for a Data Center Cloud in Europe (SENDATE) project

Keynote for the Design of Reliable Communication Networks (DRCN)

Presented by Yvan Pointurier on 2019-03-21

Agenda

- **The SENDATE project and network architecture**
- Attack detection
- Proactive orchestration
- Control plane reliability
- Determinist Dynamic Networking

General Project Information

SENDATE

Project Type	• Celtic+ project, funded by national funding agencies (France: DGE, Germany: BMBF, Sweden: vinnova, Finland: Business Finland) • Focus: Security, distributed data centers and virtualized network functions
Project Duration	• 01.04.2016 – 30.09.2019 • Different start and ending dates per sub-project
Project Volume	• ~ 68 Mio. €, ~ 482 person years • ~ 33 Mio. € funding
Project Partners	• 80 partners (industry, SME, universities and research institutes) • 4 countries (Germany, Finland, France, Sweden) • Grouped into 5 sub-projects + 4 working groups

Project Structure

SENDATE

Coordination Committee
Lead: NOKIA (Marco Hoffmann)

SENDATE Secure DCI
coord. ADVA

SENDATE TANDEM
coord. NOKIA

SENDATE FICUS
coord. Coriant / Infinera

SENDATE PLANETS
coord. NOKIA

SENDATE EXTEND
coord. Ericsson

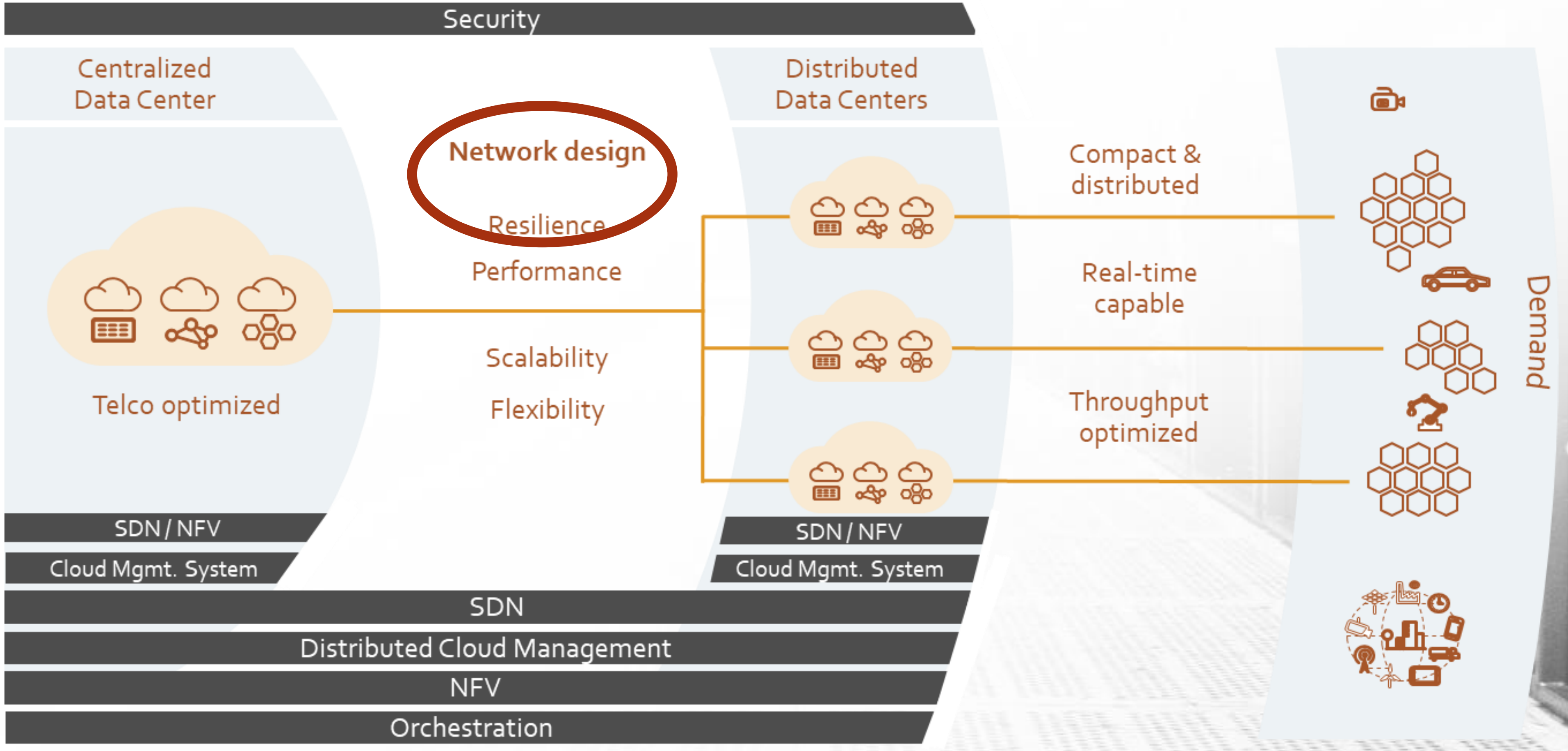
Project Structure

SENDATE

Coordination Committee
Lead: NOKIA (Marco Hoffmann)

	SENDATE Secure DCI coord. ADVA	SENDATE TANDEM coord. NOKIA	SENDATE FICUS coord. Coriant / Infinera	SENDATE PLANETS coord. NOKIA	SENDATE EXTEND coord. Ericsson
WG: Data Center coord. ADVA	●	●	●	●	●
WG: Networking coord. NOKIA	●	●	●	●	●
WG: Transport coord. Coriant	●		●		●
WG: Security coord. Thales	●	●	●	●	●

Distributed Data Centers

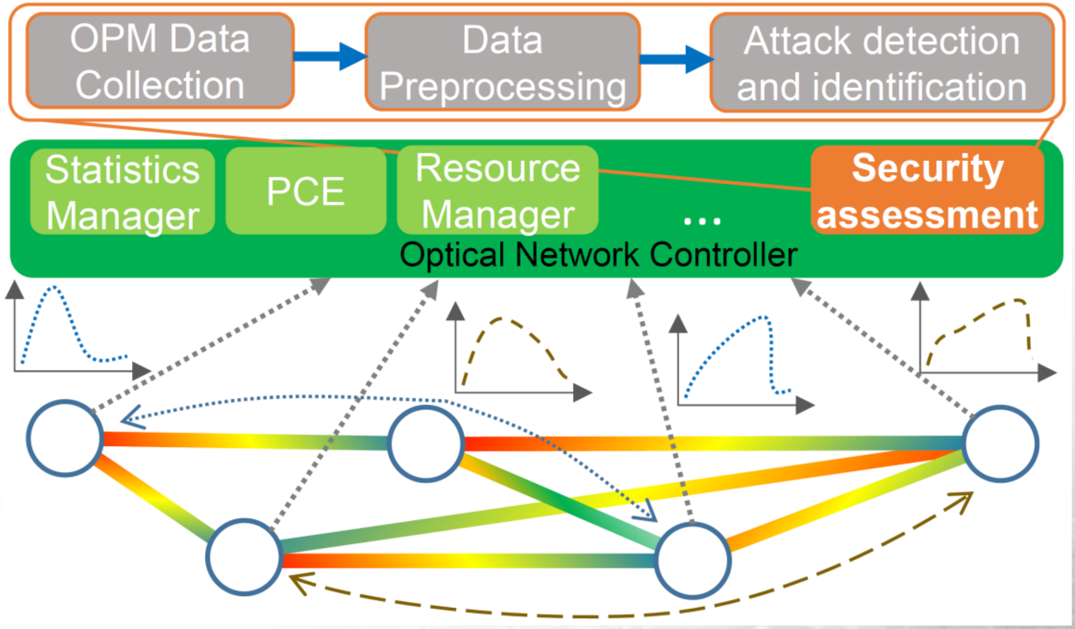


Agenda

- The SENDATE project and network architecture
- **Attack detection**
- Proactive orchestration
- Control plane reliability
- Determinist Dynamic Networking

Machine-learning-based identification of harmful signals

- Optical networks are vulnerable to physical-layer attacks
  - E.g.: fiber cuts, insertion of in- and out-of-band jamming signals
- **Two-fold problem:**
  - Attack classification → how to detect the presence of a known attack and identify its severity?
    - – Classical supervised learning problem
  - Attack detection → how to detect attacks that have never been seen before?
    - – Classical unsupervised learning problem
  - Evaluation metrics:
    - – False positive rate: Trigger unnecessary countermeasures (e.g., protection rerouting)
    - – **False negative rate**: Attacks remain undetected; may evolve to more disruptive events



- **OPM data collection** – commercially available transceivers record, e.g.,
  - Received and transmitted optical power (OPR & OPT)
  - State of polarization (SOP)
  - Optical signal-to-noise-ratio (OSNR)
  - etc.
- **Data preprocessing** – removal of outliers and feature normalization
- **Attack detection and identification** – supervised/unsupervised learning

C. Natalino, et al. "Field demonstration of machine-learning-aided detection and identification of jamming attacks in optical networks," ECOC, 2018.

SENDATE

Case study: Failure cuts in optical networks

Link failure causes :

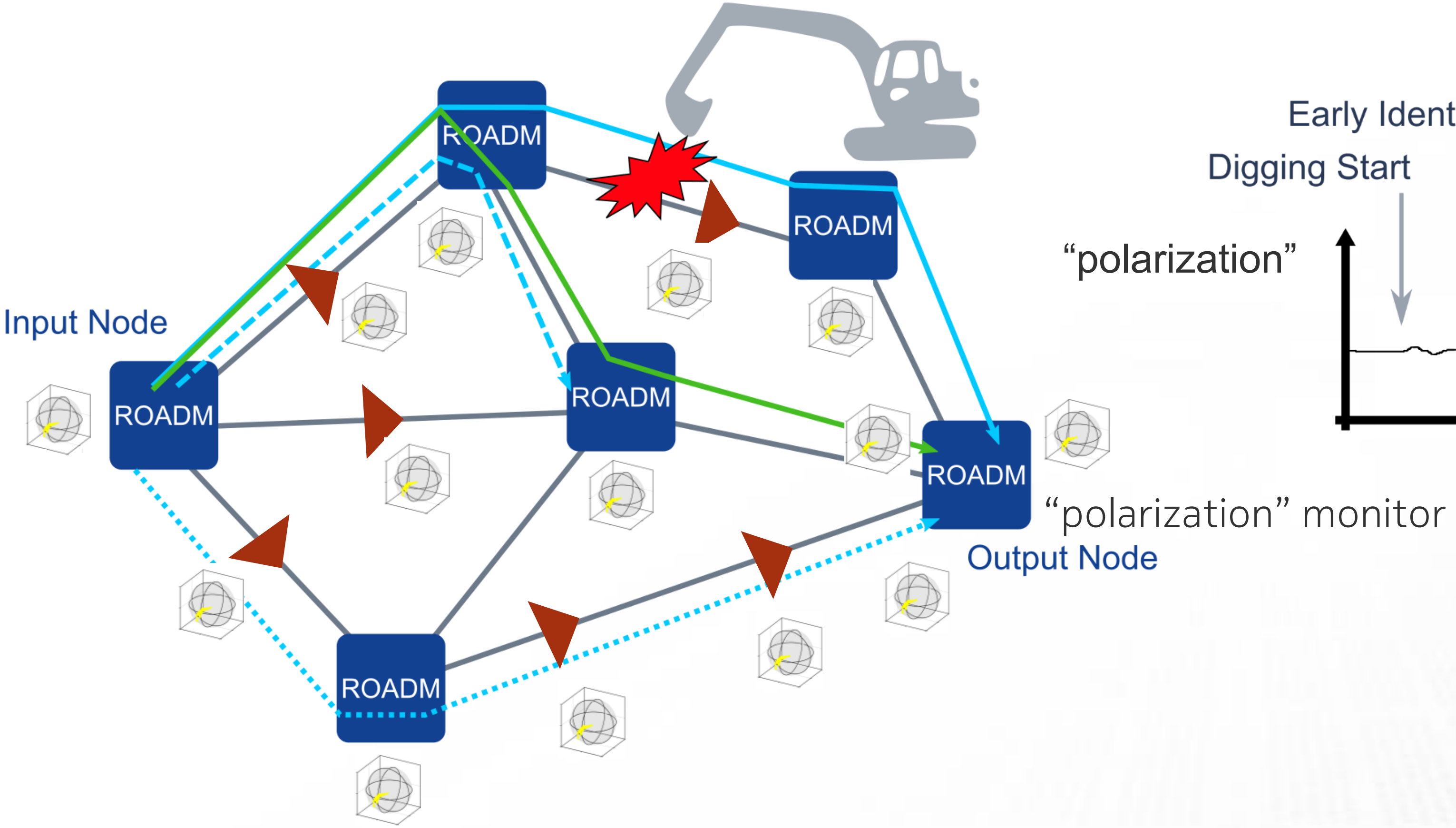
- According to the US Federal Communications Commission :
  - Fiber breaks are the main link failure cause (40%)
  - Metro networks experience 13 cuts annually for every 1000 miles of fiber
    → **1 cut / 120 km / year !**

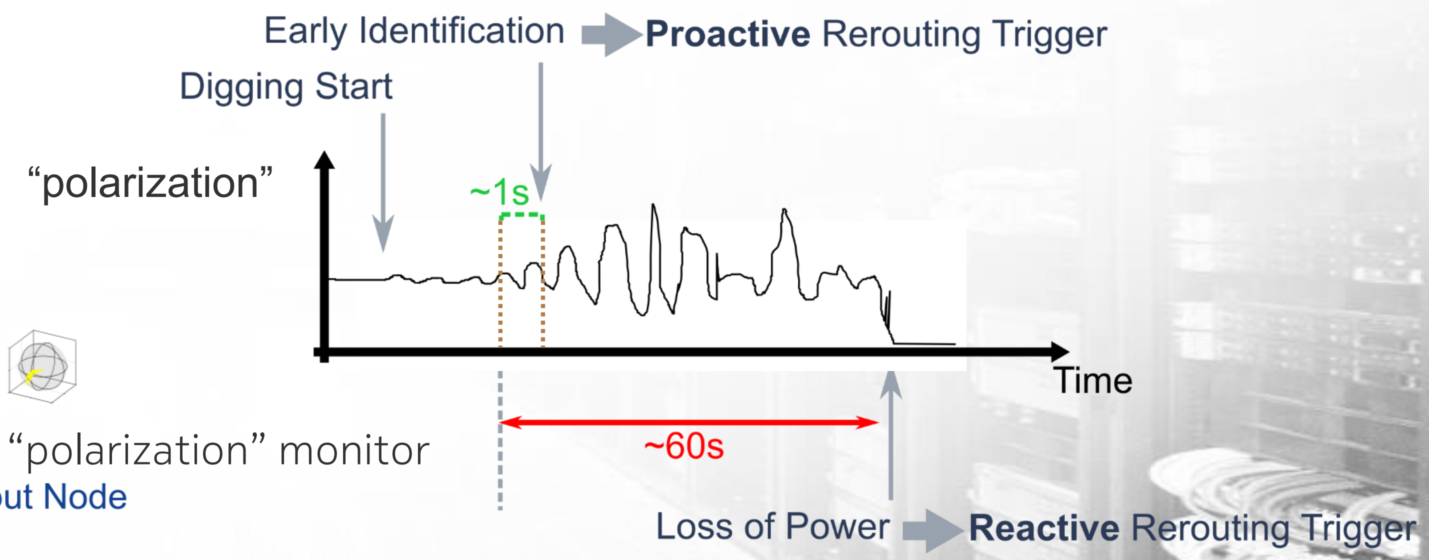
Link recovery options :

- Optical Dedicated Protection (fail-proof) :
  - Fast (50 ms)
  - Duplicated hardware, 50% of the network capacity idle with 1+1 protection
  - Working and backup path have same capacity but different reaches
- Optical restoration / Shared protection
  - Better utilization of network resources (reduces system margin)
  - Slow recovery (~ 60 s)

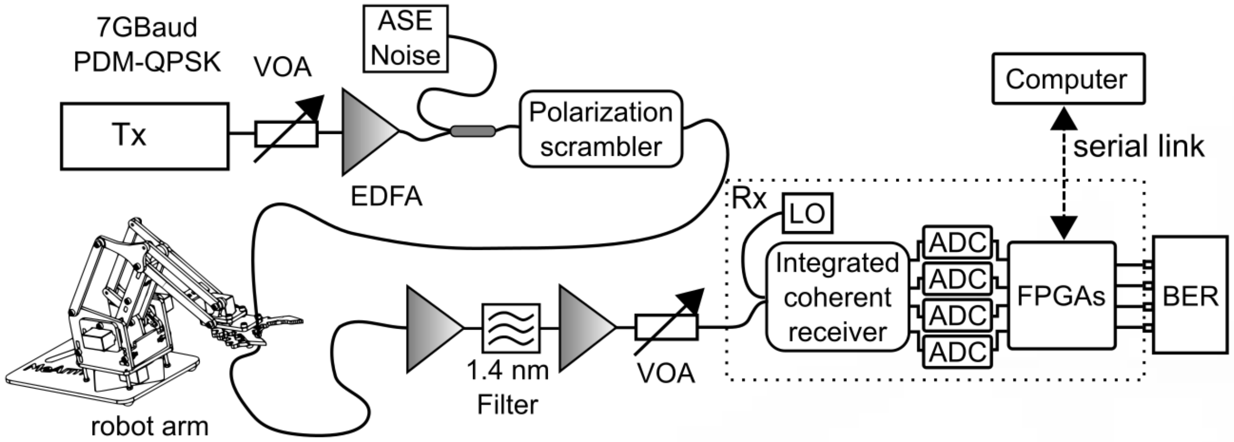
To recover fast, we need to predict the fiber cut !

Track mechanical stress thanks to real-time polarization monitoring

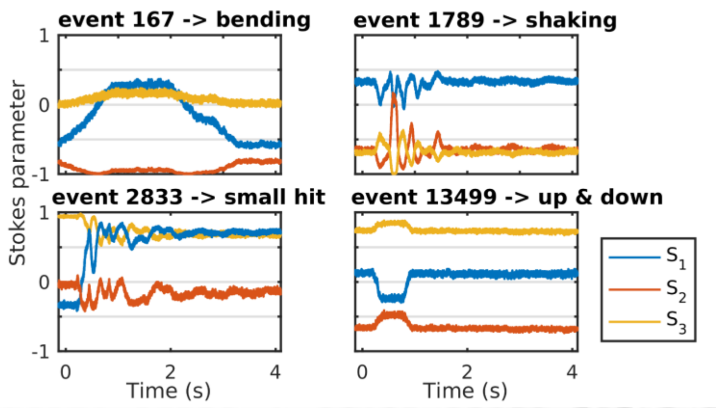




Coherent Transponder Polarization Sensing

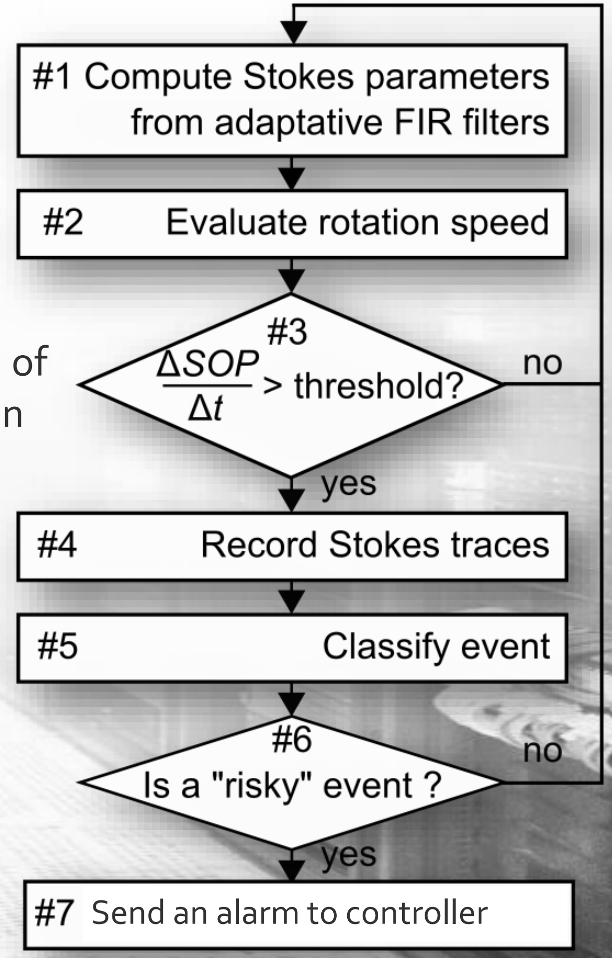


- Allows per-**path** intrusion detection and event classification
- Leverages coherent receivers already deployed
- Feed to supervised learning classification tool (Naïve Bayes)



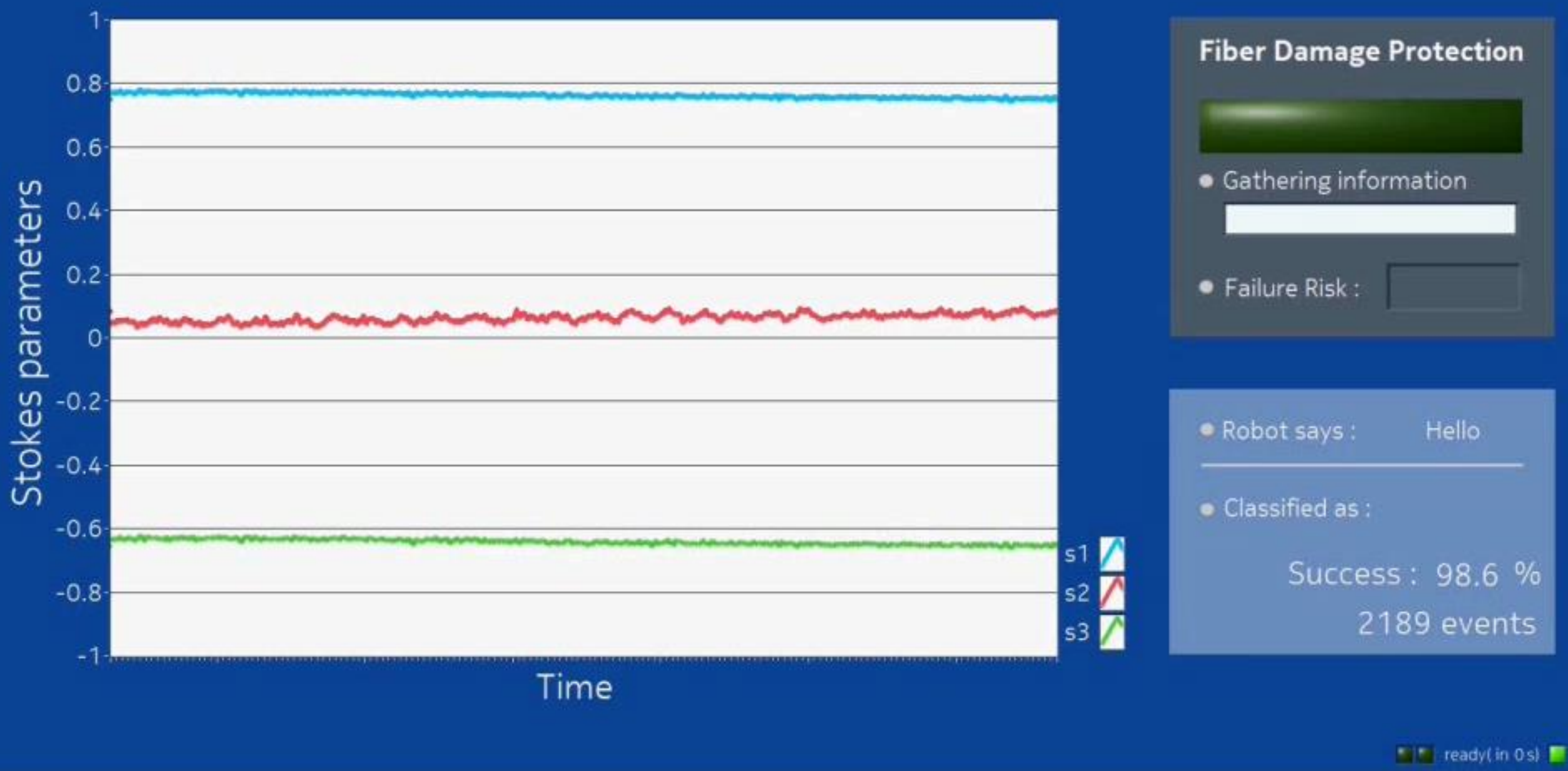
Event classification: $Y = f(X)$

SOP: state of polarization



F. Boitier et al., "Proactive fiber damage detection in real-time coherent receiver," ECOC 2017.

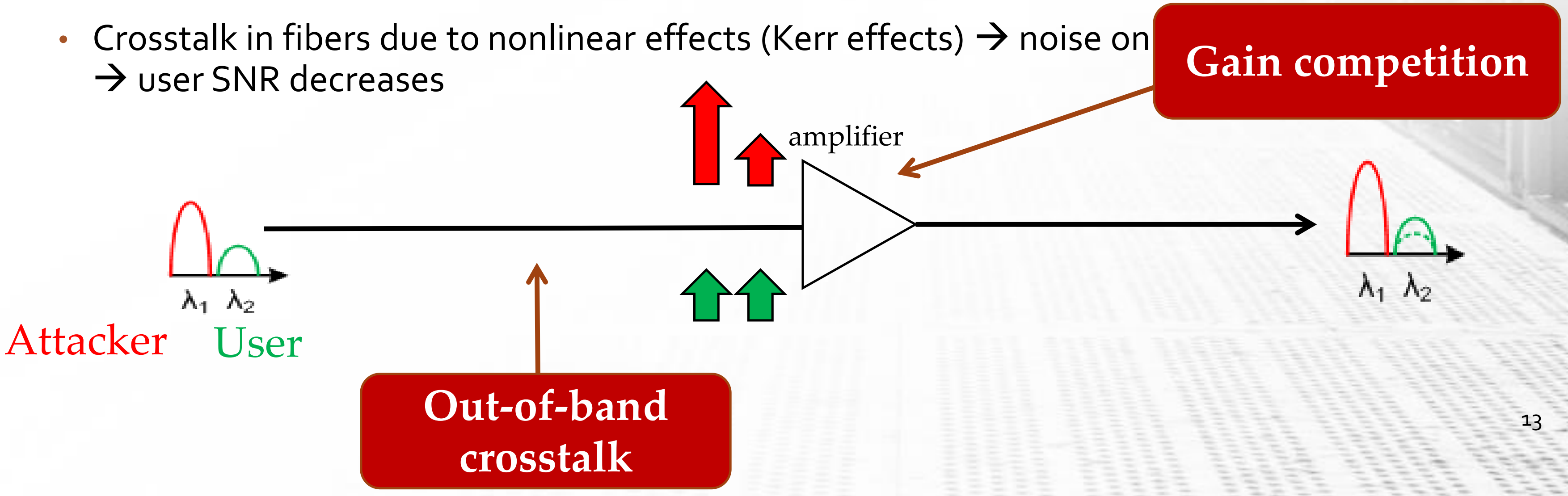
NOKIA Bell Labs SENDATE



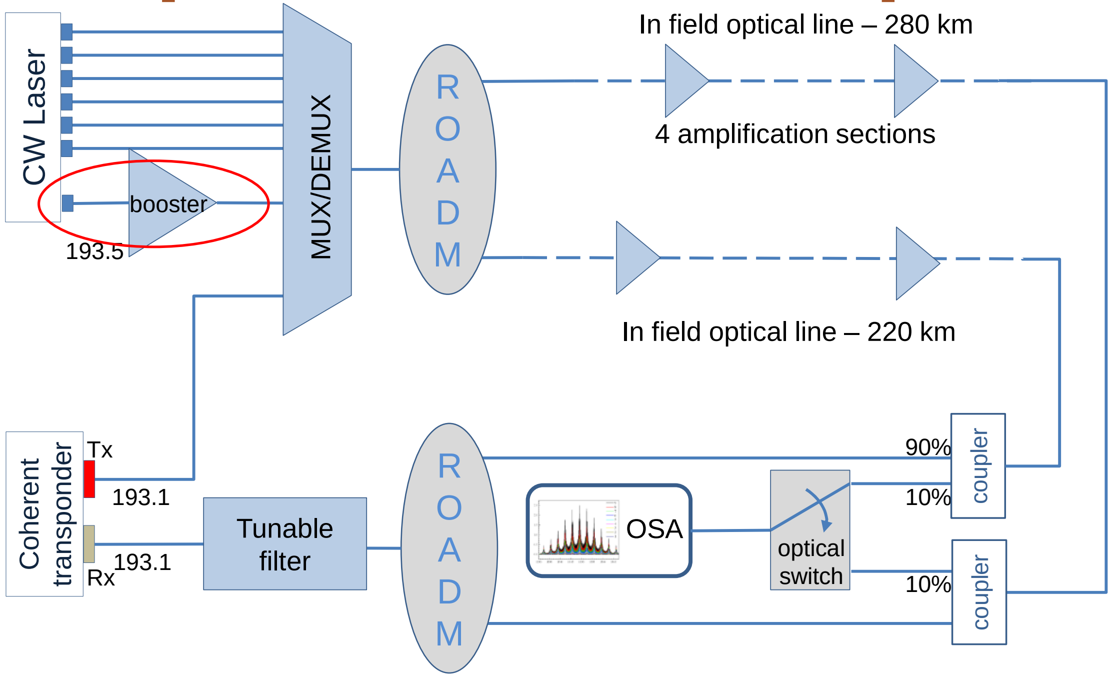
99% accuracy leveraging available information at coherent receiver

Case study: detection of power jamming attacks

- **High power jamming** – one of the most harmful physical-layer attack methods
  - Alien wavelengths could make this attack easier
- An optical signal inserted into the fiber with the objective to degrade the quality of co-propagating channels via
  - Reduction of gain in erbium-doped fiber amplifiers → output power of user decreases → user SNR decreases
  - Crosstalk in fibers due to nonlinear effects (Kerr effects) → noise on → user SNR decreases



Out-of-band jamming: experimental setup



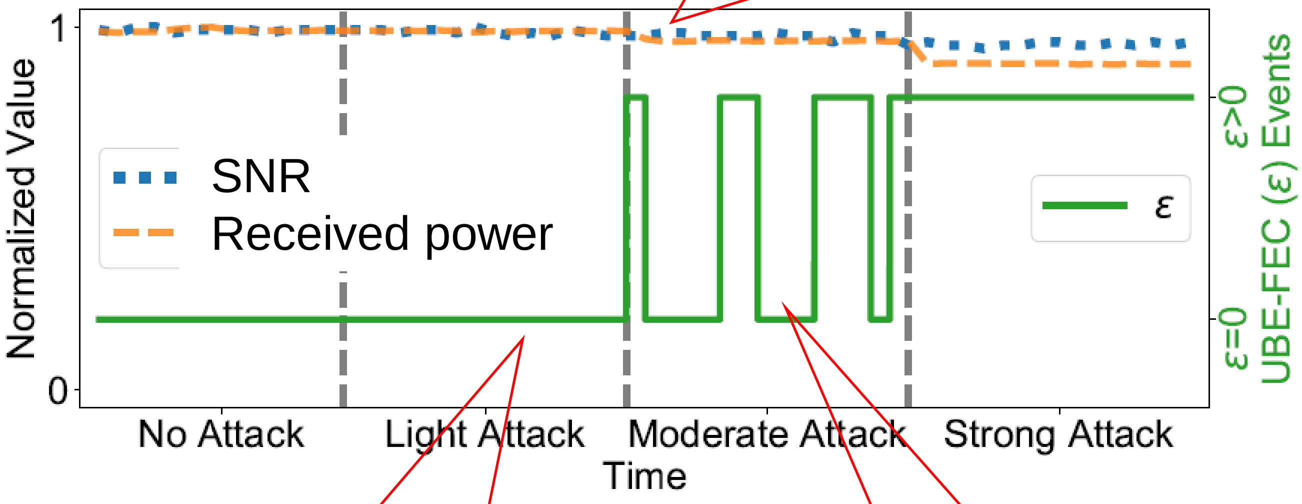
- Jamming signal inserted at the mux
  - Frequency: 193.5148 THz
  - Power:
    - 0 dB – light attack
    - 3 dB – moderate attack
    - 6 dB – strong attack

- Field-deployed testbed equipped with Coriant Groove G30 coherent transponders, 2 Flexgrid ROADMs and an optical line system with 4 amplification sections and 280 km of total length
- Channel under test: 200 Gbps, 16QAM, 193.1 THz nominal central frequency
- 6 CW channels to simulate realistic loading conditions

C. Natalino, et al. "Field demonstration of machine-learning-aided detection and identification of jamming attacks in optical networks," ECOC, 2018.

Supervised learning for attack detection

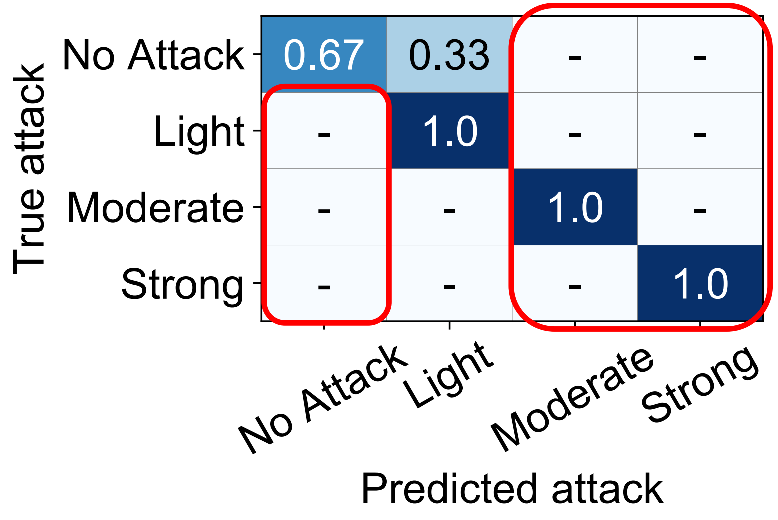
No distinct threshold values to be used as an attack indicator



No errors detected although a jamming signal is present

Error bursts within the same attack regime

Artificial Neural Network (ANN)



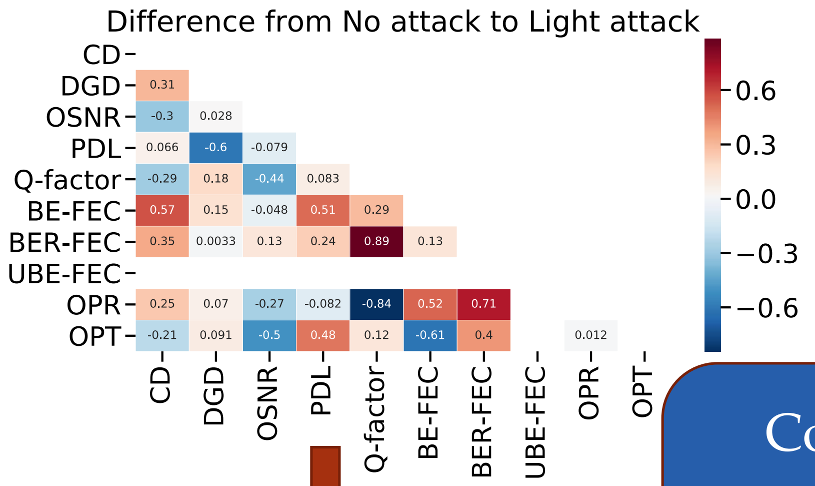
100% accuracy for moderate and strong attacks

No false negatives!

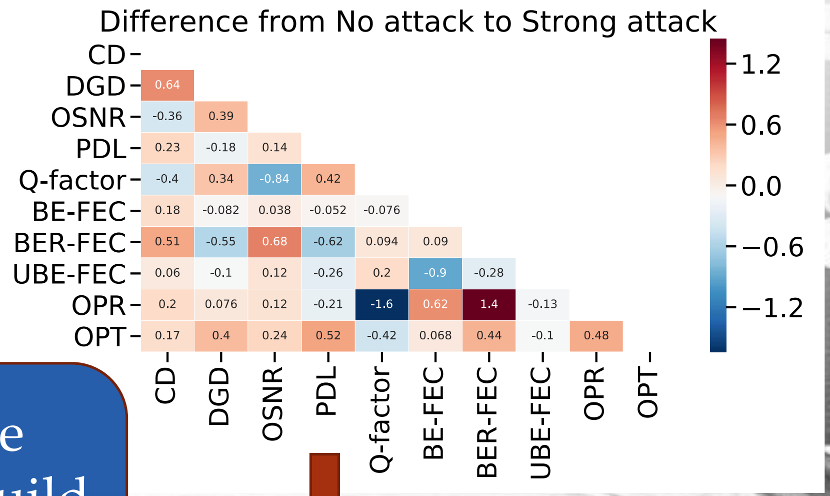
C. Natalino, et al. "Field demonstration of machine-learning-aided detection and identification of jamming attacks in optical networks," ECOC, 2018.

Unsupervised learning: parameter correlation as an attack indicator

- Normal operating conditions:
  - OPR (received power) and Q-factor – strong positive correlation
  - OPR and pre-FEC errors – strong negative correlation
- **Correlation changes when an attack is introduced**



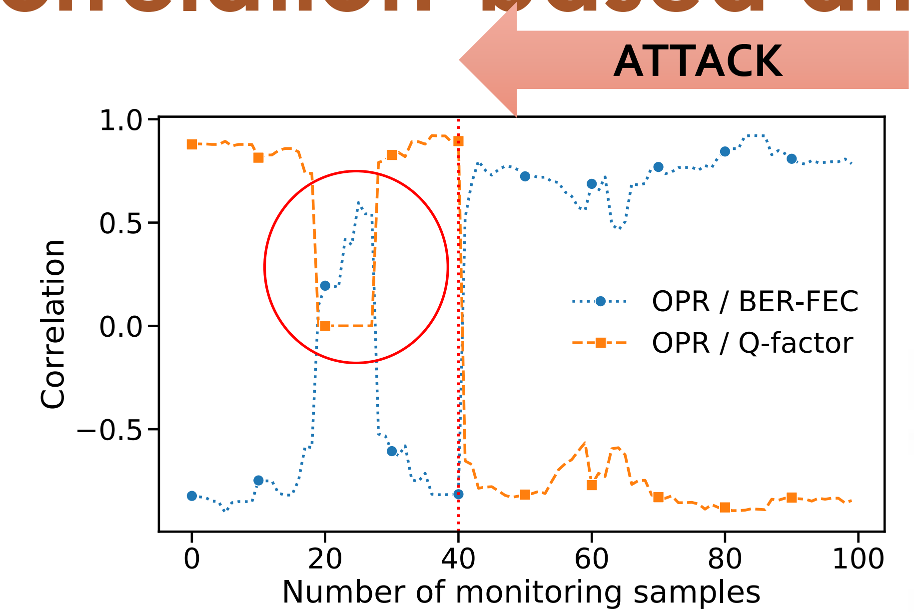
	Q-factor	BE-FEC	BER-FEC
OPR	-0.84	0.52	0.71

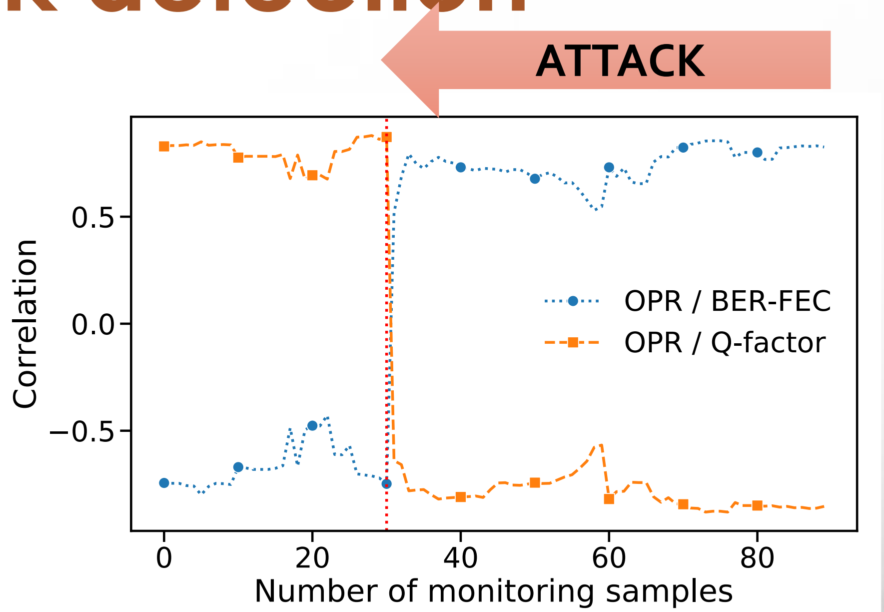


	Q-factor	BE-FEC	BER-FEC
OPR	-1.6	0.62	1.4

Could we use correlation to build an attack detection method?

Unsupervised learning: correlation-based attack detection





Considering last 20 samples (1 per min)

- Shorter time to attack detection (here, 2 mins)
- More prone to false positives

Considering last 30 samples (1 per min)

- Longer time to detect attack (here, 4 mins)
- Less prone to false positives

A more autonomous approach needed that does not require prior human knowledge

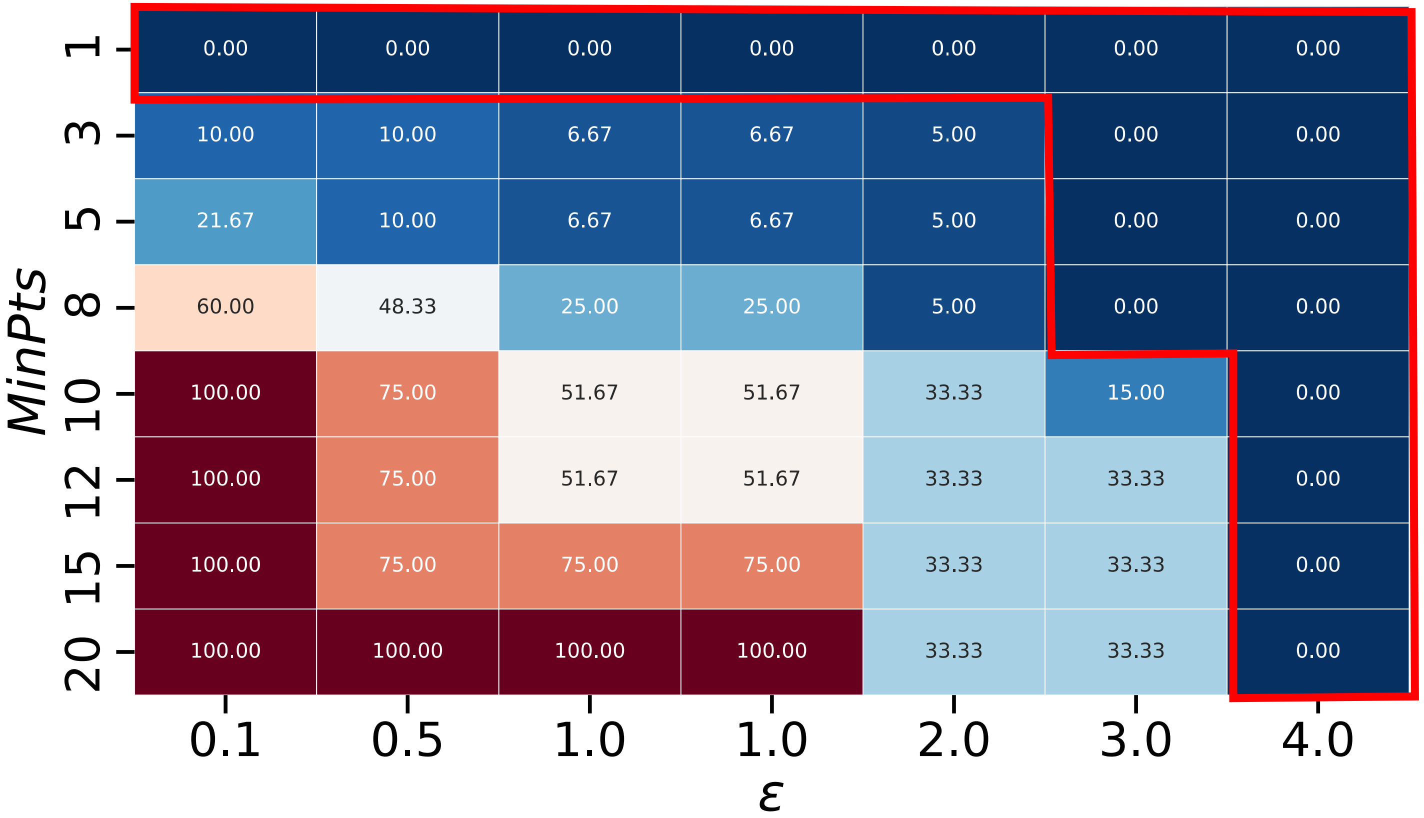
Unsupervised learning: Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

- Separates the monitoring samples into clusters and outliers
- In this context, outliers can be considered the anomalies we are trying to identify, i.e., the attacks
    - No prior knowledge of attacks
- Two key parameters:
    - **ε** defines the maximum [Euclidean] distance for two samples to be considered neighbors
    - **MinPts** defines the minimum number of neighbors for a sample to be considered a core sample

Unsupervised learning: how to configure algorithm to detect unseen attacks?

Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

Percentage of *false positives*, i.e., percentage of instances from normal operating conditions clustered as abnormal instances



M. Furdek, et al. "Experiment-based detection of service disruption attacks in optical networks using data analytics and unsupervised learning." Photonics West, 2019.

Unsupervised learning: how does the configuration impact false positives and false negatives?

False positive

False negative

	ϵ						
MinPts	0.1	0.5	1.0	1.0	2.0	3.0	4.0
	Light attack						
1	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69
3	3.08, 0.00	3.08, 0.00	3.08, 3.08	3.08, 3.08	3.08, 7.69	0.00, 7.69	0.00, 7.69
5	21.54, 0.00	15.38, 0.00	15.38, 3.08	15.38, 3.08	3.08, 7.69	0.00, 7.69	0.00, 7.69
8	78.46, 0.00	64.62, 0.00	38.46, 3.08	38.46, 3.08	10.77, 6.15	0.00, 7.69	0.00, 7.69
10	92.31, 0.00	64.62, 0.00	38.46, 3.08	38.46, 3.08	23.08, 6.15	23.08, 6.15	0.00, 7.69
12	92.31, 0.00	64.62, 0.00	38.46, 3.08	38.46, 3.08	23.08, 6.15	23.08, 6.15	0.00, 7.69
15	92.31, 0.00	64.62, 0.00	38.46, 3.08	38.46, 3.08	23.08, 6.15	23.08, 6.15	0.00, 7.69
	Moderate attack						
1	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69
3	3.08, 0.00	3.08, 0.00	3.08, 0.00	3.08, 0.00	3.08, 7.69	0.00, 7.69	0.00, 7.69
5	21.54, 0.00	15.38, 0.00	15.38, 0.00	15.38, 0.00	3.08, 7.69	0.00, 7.69	0.00, 7.69
8	78.46, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	10.77, 7.69	10.77, 7.69	0.00, 7.69
10	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 7.69	23.08, 7.69	0.00, 7.69
12	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 7.69	23.08, 7.69	0.00, 7.69
15	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 4.62	23.08, 7.69	0.00, 7.69
	Strong attack						
1	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69	0.00, 7.69
3	3.08, 0.00	3.08, 0.00	3.08, 0.00	3.08, 0.00	3.08, 0.00	0.00, 0.00	0.00, 4.62
5	21.54, 0.00	15.38, 0.00	15.38, 0.00	15.38, 0.00	3.08, 0.00	0.00, 0.00	0.00, 4.62
8	78.46, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	10.77, 0.00	10.77, 0.00	0.00, 4.62
10	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 0.00	23.08, 0.00	0.00, 4.62
12	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 0.00	23.08, 0.00	0.00, 4.62
15	92.31, 0.00	64.62, 0.00	38.46, 0.00	38.46, 0.00	23.08, 0.00	23.08, 0.00	0.00, 1.54

Higher MinPts makes it harder for attacks to go undetected (should be balanced with ε)

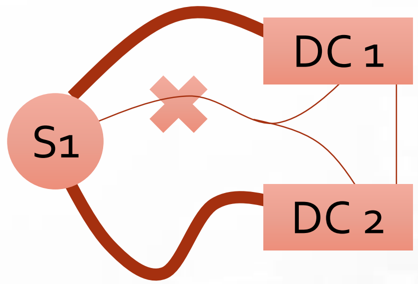
ε=4 ensures no false positives and 7.69% false negatives for no prior knowledge of attacks

Strong attacks are easier to distinguish

Agenda

- The SENDATE project and network architecture
- Attack detection
- **Proactive orchestration**
- Control plane reliability
- Determinist Dynamic Networking

Proactive resilient orchestration of optical cloud services



- Proactive (protection)

Provision spare (backup) resources

Failure

Switch to backup resources

Time

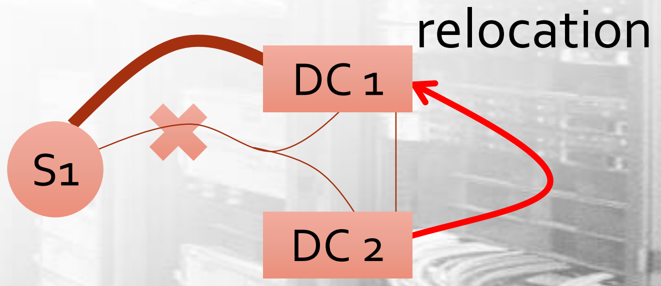
- Reactive (restoration/relocation)

Provision working resources

Failure

Compute restoration and switch to backup resources

Time



- Proposed proactive strategy based on failure prediction

Provision working resources

Proactive restoration

Failure

Failure prediction

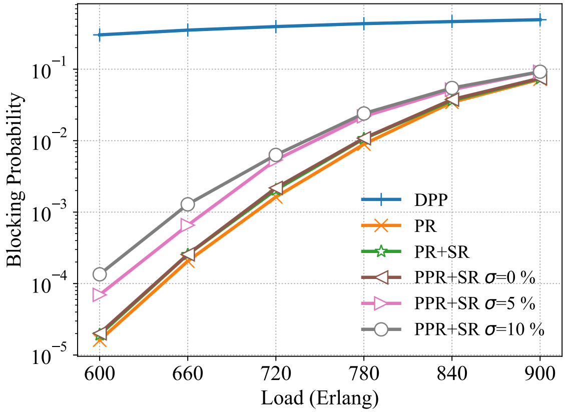
Time

Compute restoration and switch to backup resources

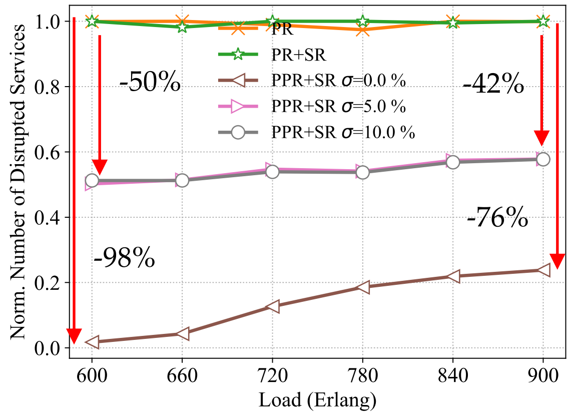
C. Natalino et al. "A proactive restoration strategy for optical cloud networks based on failure predictions," ICTON, 2018.

Simulation Results

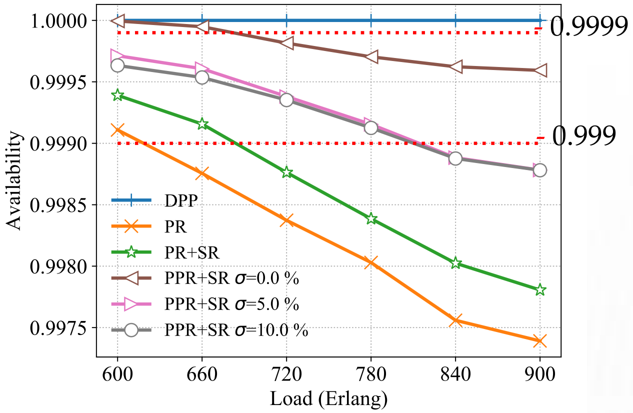
Blocking probability: the probability of a service not being served due to lack of free resources



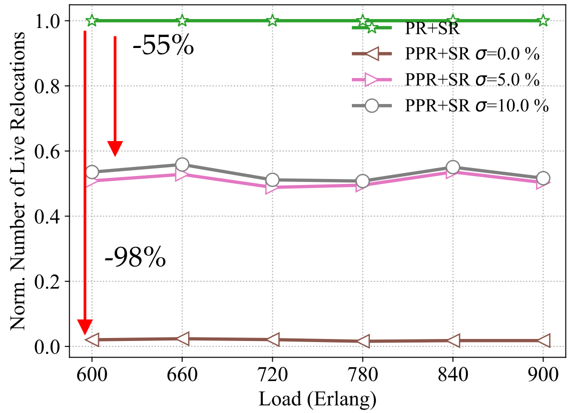
Normalized number of disrupted services: considers the number of services disrupted by a link failure



Availability: the ratio between the service uptime over the requested service time



Normalized number of live service relocations: considers the service relocations performed upon a link failure



DPP: Dedicated Path Protection
PR: Path Restoration
PR+SR: PR with Service Relocation
PPR+SR: Proactive PR with Service Relocation
σ: Prediction error in time

C. Natalino et al. "A proactive restoration strategy for optical cloud networks based on failure predictions," ICTON, 2018.

SENDATE

Agenda

- The SENDATE project and network architecture
- Attack detection
- Proactive orchestration
- **Control plane reliability**
- Determinist Dynamic Networking

Software Defined Networking (SDN)

Architecture

Applications:

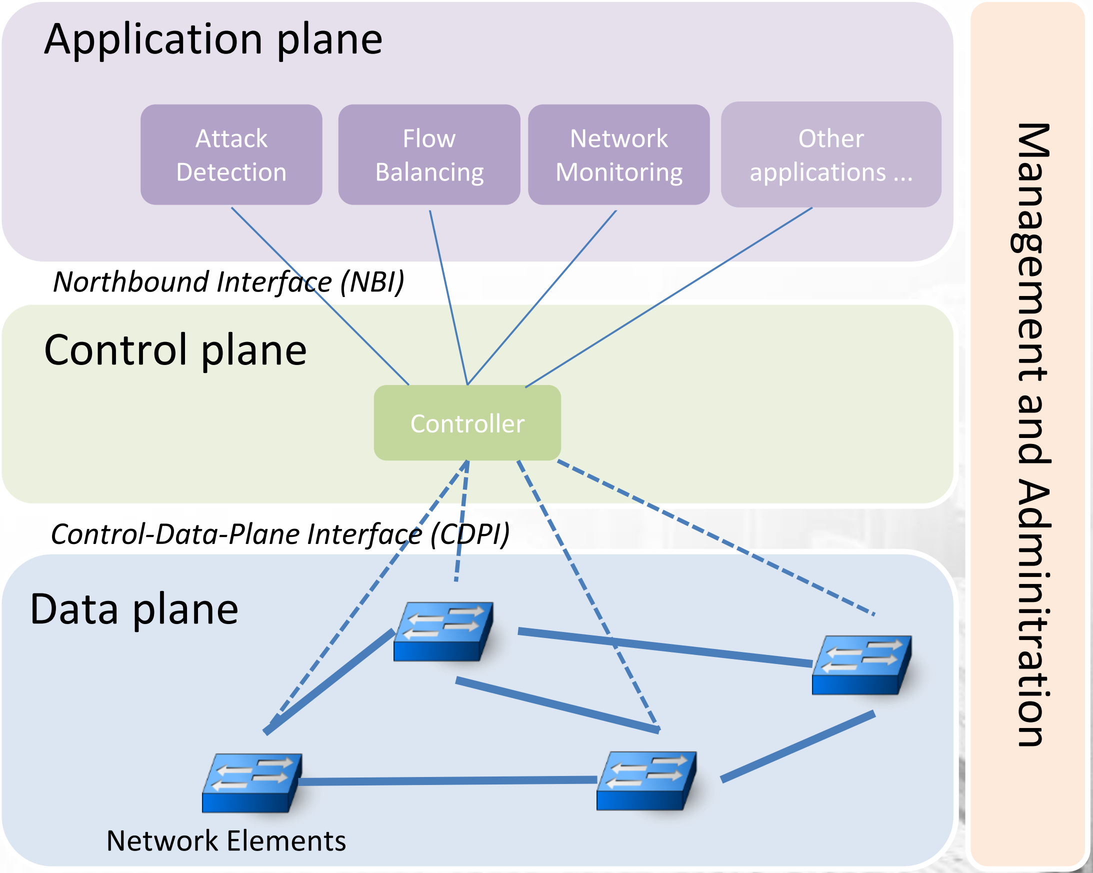
- Communicate with controller to communicate behaviors and request network resources.
- Collect info from controller

SDN Controller:

- Logical entity to set up rules at data plane based on instructions/requirements of appl.
- Extracts information from data plane to inform appl.

Network Element:

- Forwarding and data processing

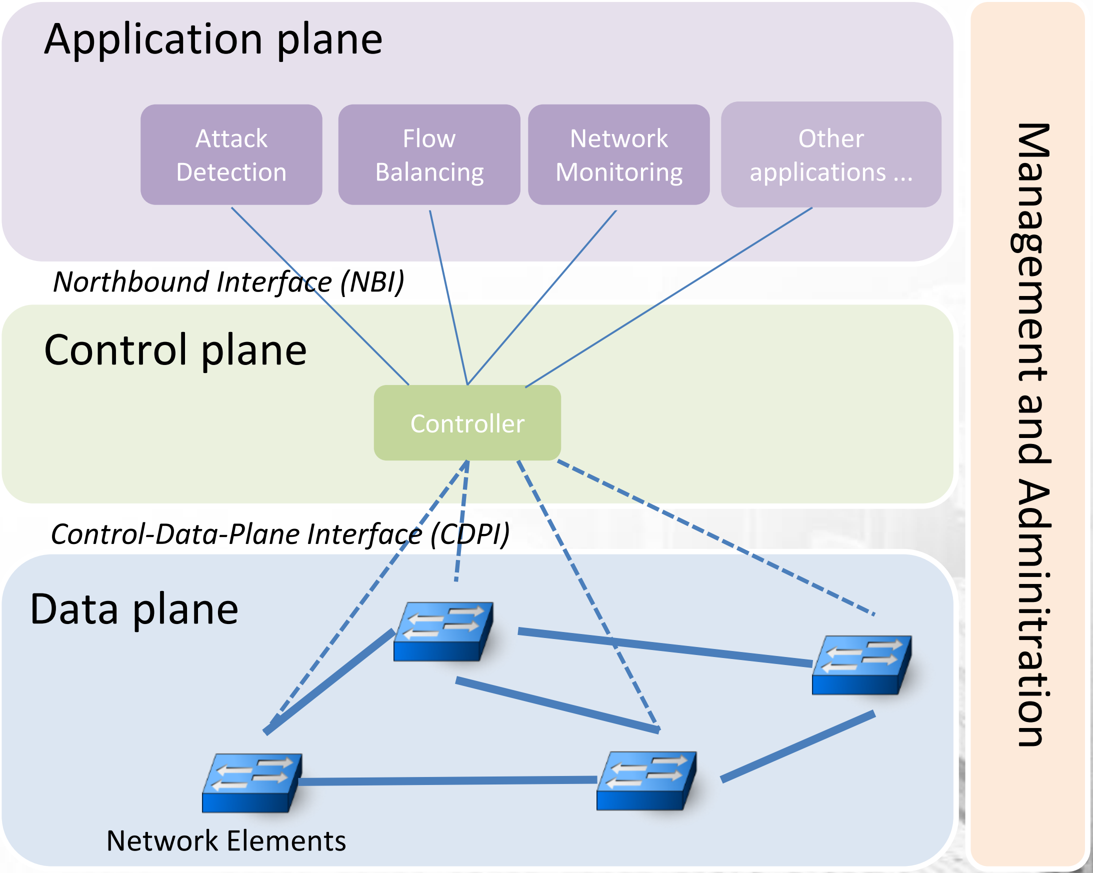


Software Defined Networking (SDN)
Threats

Application plane:
- Security

Control plane:
- *Single* entity
- Software (running on hardware)

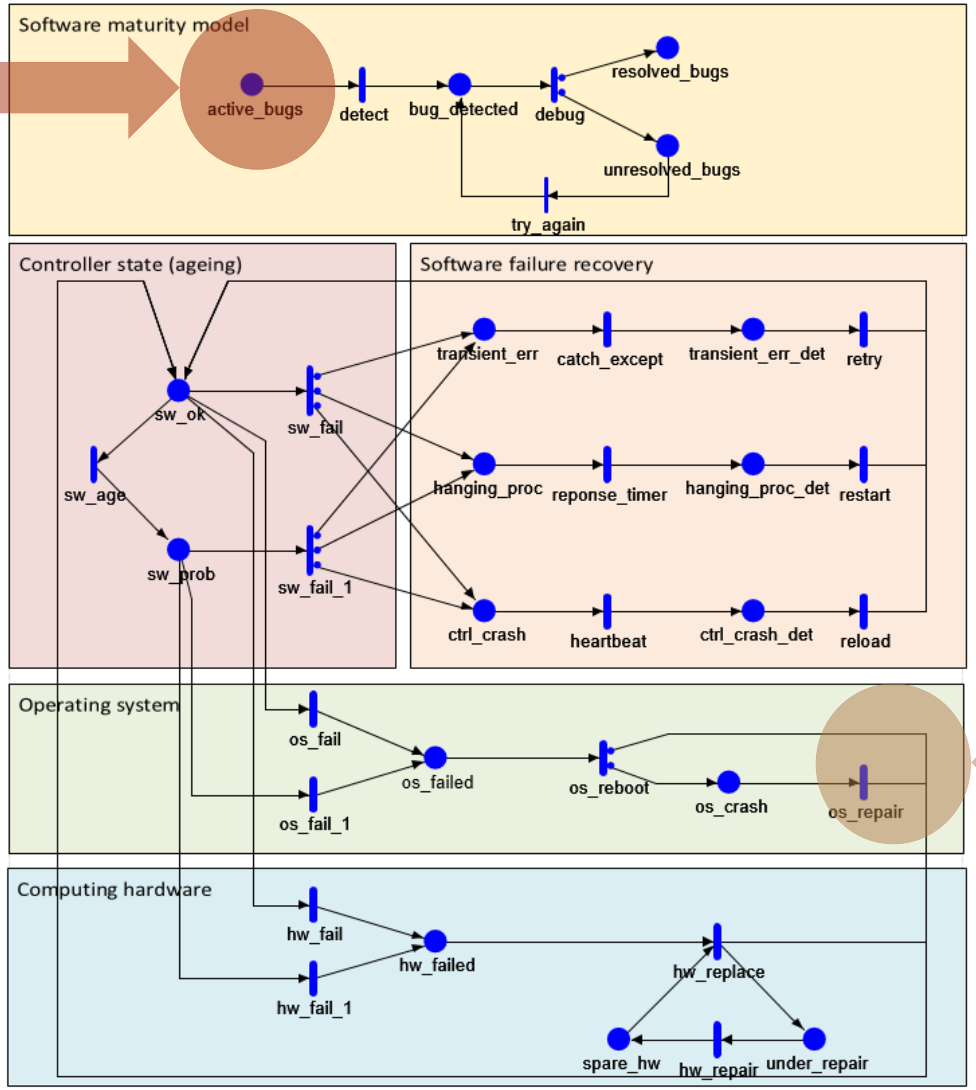
Data plane:
- Failures / Disasters
- Attacks



Failure dynamics in Software Defined Networking *SDN controller as Stochastic Activity Network (SAN)*

PLACE

- places contain a number of tokens (markings)
- combination of markings in all places represent system state



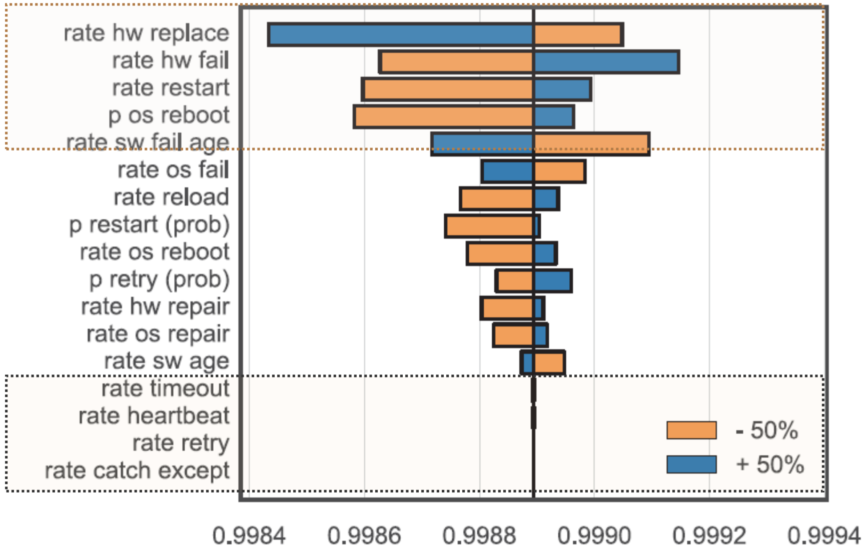
- activities change the system state upon firing
- firing times can be deterministic (constant) or random (following a predefined distribution)

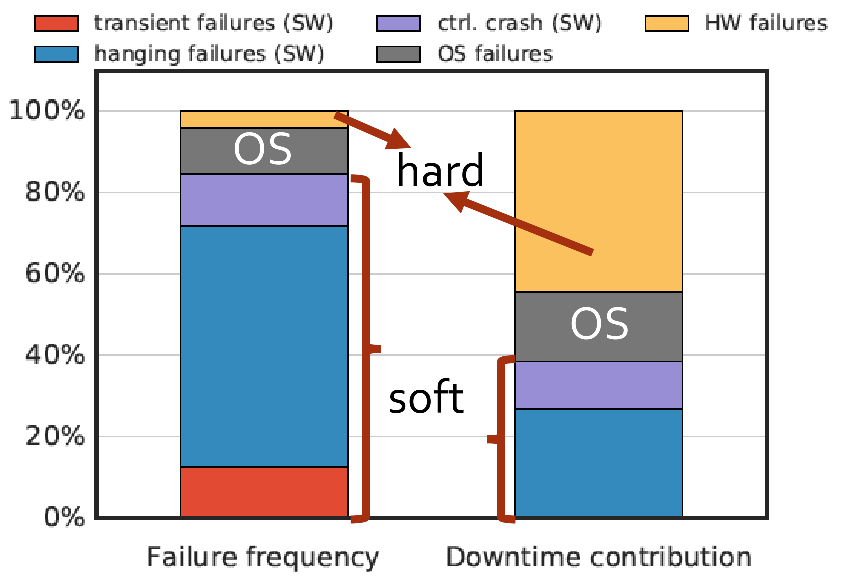
ACTIVITY

P. Vizarreta, et al. "Characterization of Failure Dynamics in SDN Controllers", RNDM 2017

Failure dynamics in Software Defined Networking *Controller availability Analysis*

- A controller has less than "3-nines" availability
  → At least two controllers are needed to achieve "5-nines" availability





- Software failures lead to more frequent, but shorter, outages
- Software failures account for 84% of all failure, but contribute to only 38% of downtime
- Hardware failures represent less then 4% of all failures but contribute to 44% of downtime

P. Vizarreta, et al. "Characterization of Failure Dynamics in SDN Controllers", RNDM 2017

Network softwarization

Open source

+Threats→ Bugs!!

Software bugs are major root cause of customer-impacting incidents [Microsoft2017]

SENDATE

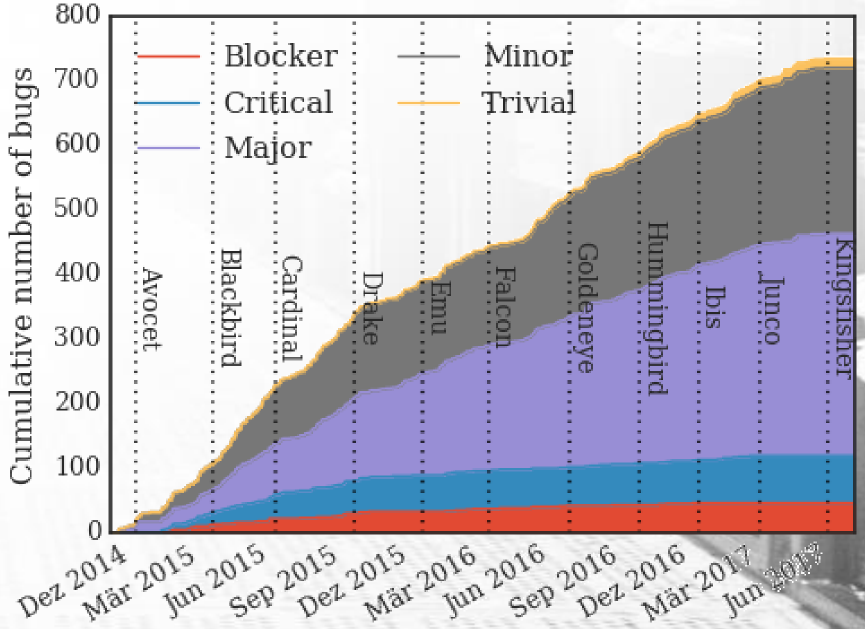
Failure dynamics in Software Defined Networking

Software maturity

Gather empirical data

Open Network Operating Systems (ONOS)

- New releases published quarterly
- Fault reports available online in JIRA issue tracker
- Bugs grouped by and priority and affected release



P. Vizarreta, et al. "An Empirical Study of Software Reliability in SDN Controllers", Int. Conference on Network and Service Management (CNSM) 2017.

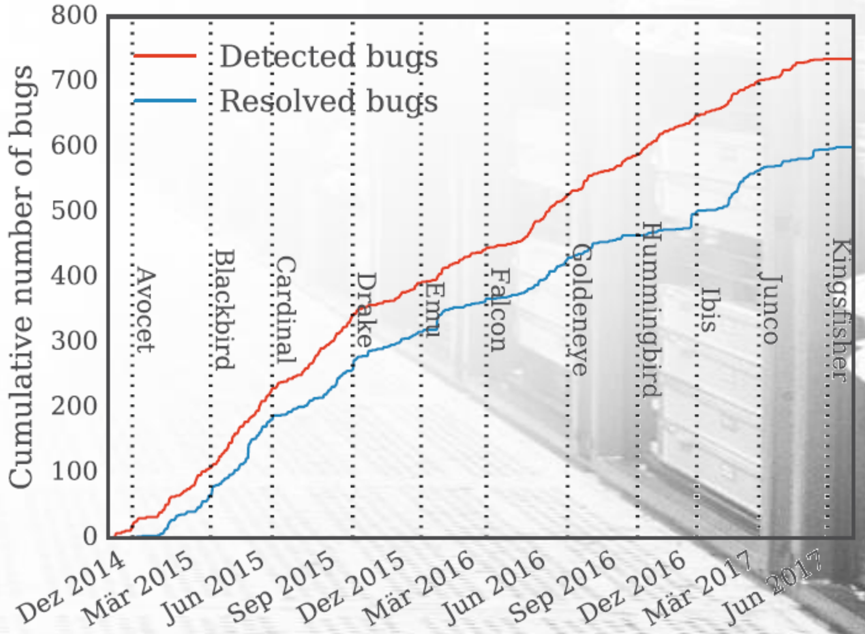
Failure dynamics in Software Defined Networking

Software maturity

Gather empirical data

Open Network Operating Systems (ONOS)

- New releases published quarterly
- Fault reports available online in JIRA issue tracker
- Bugs grouped by and priority and affected release



P. Vizarreta, et al. "An Empirical Study of Software Reliability in SDN Controllers", Int. Conference on Network and Service Management (CNSM) 2017.

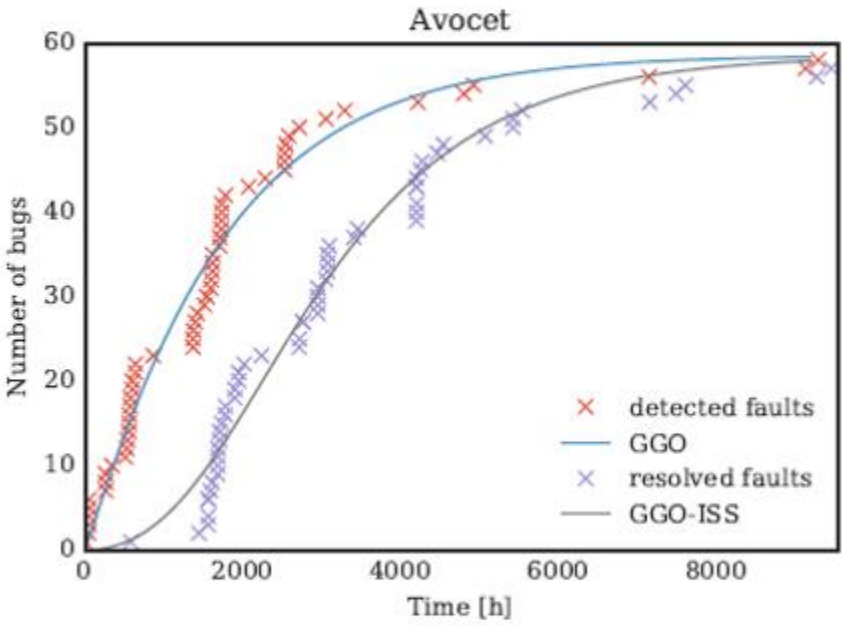
Failure dynamics in Software Defined Networking

Software maturity

Gather empirical data → Find best SRGM model

Software reliability growth modeling (SRGM)

Fault detection



Find best model according to different Goodness of Fit (GoF) such as Mean Square Error, Coefficient of determination, etc.

GGO: Generalized Goel Okumoto
ISS: Inflection S-Shaped (ISS)

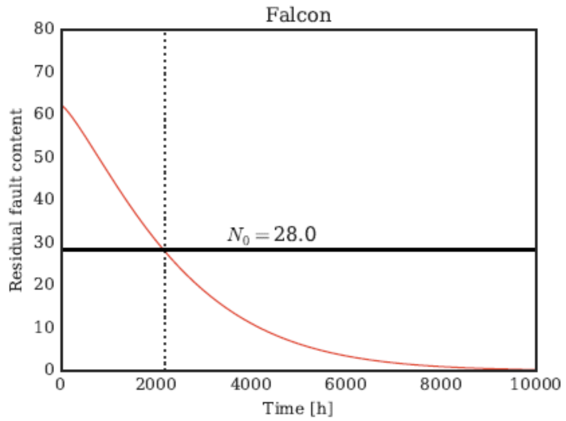
P. Vizarreta, et al. "An Empirical Study of Software Reliability in SDN Controllers", Int. Conference on Network and Service Management (CNSM) 2017.

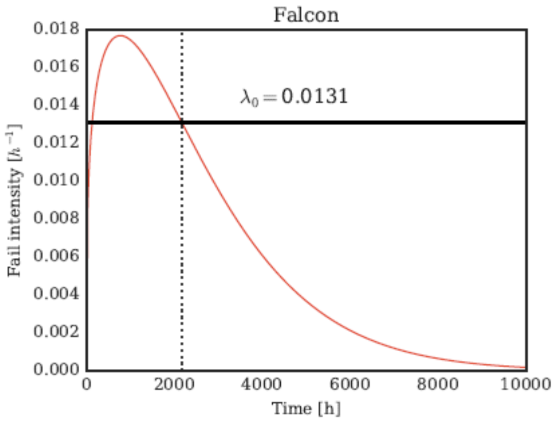
Failure dynamics in Software Defined Networking

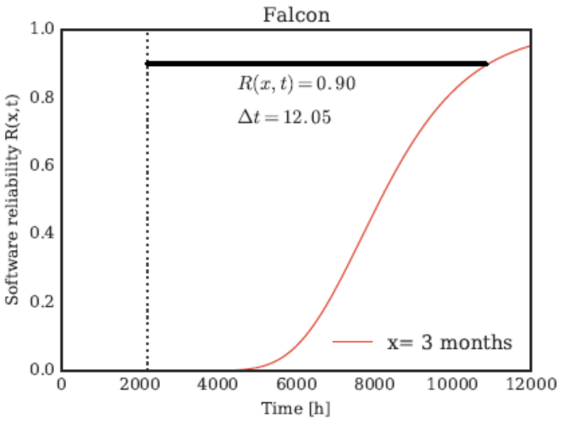
Software maturity

Gather empirical data → Find best SRGM model → Reliability Evaluation

Evaluation results: **Residual bug content** **Failure intensity** **Cond. software reliability**







At the day of software release 28 severe bugs were expected

Expected time till next severe software bug manifestation was 3 days

Postpone software adoption 12 months until software matures

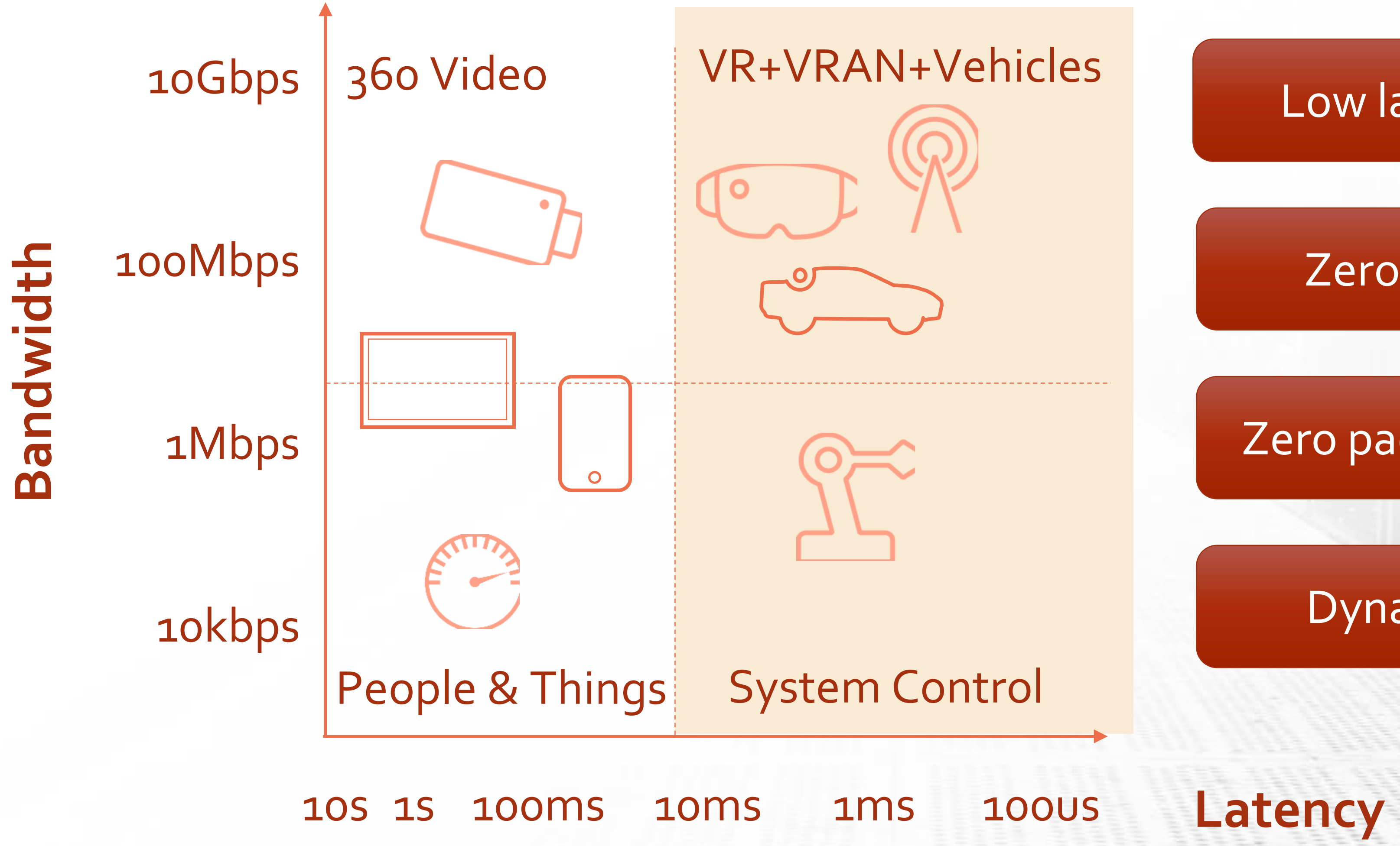
P. Vizarreta, et al. "An Empirical Study of Software Reliability in SDN Controllers", Int. Conference on Network and Service Management (CNSM) 2017.

SENDATE

Agenda

- The SENDATE project and network architecture
- Attack detection
- Proactive orchestration
- Control plane reliability
- **Determinist Dynamic Networking**

5G needs a deterministic and dynamic network



- Low latency
- Zero jitter
- Zero packet loss
- Dynamics

Requirements for Edge Cloud networks

Low latency

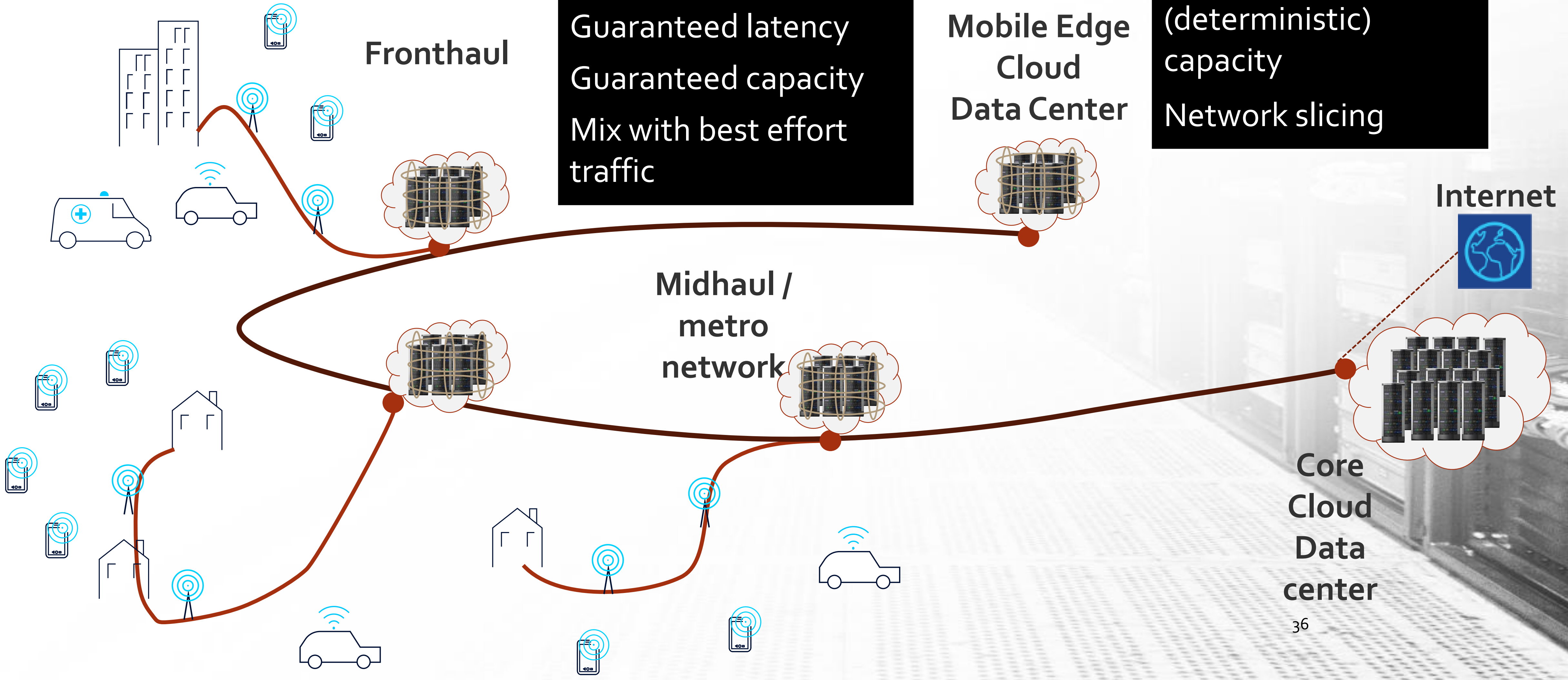
Guaranteed latency

Guaranteed capacity

Mix with best effort traffic

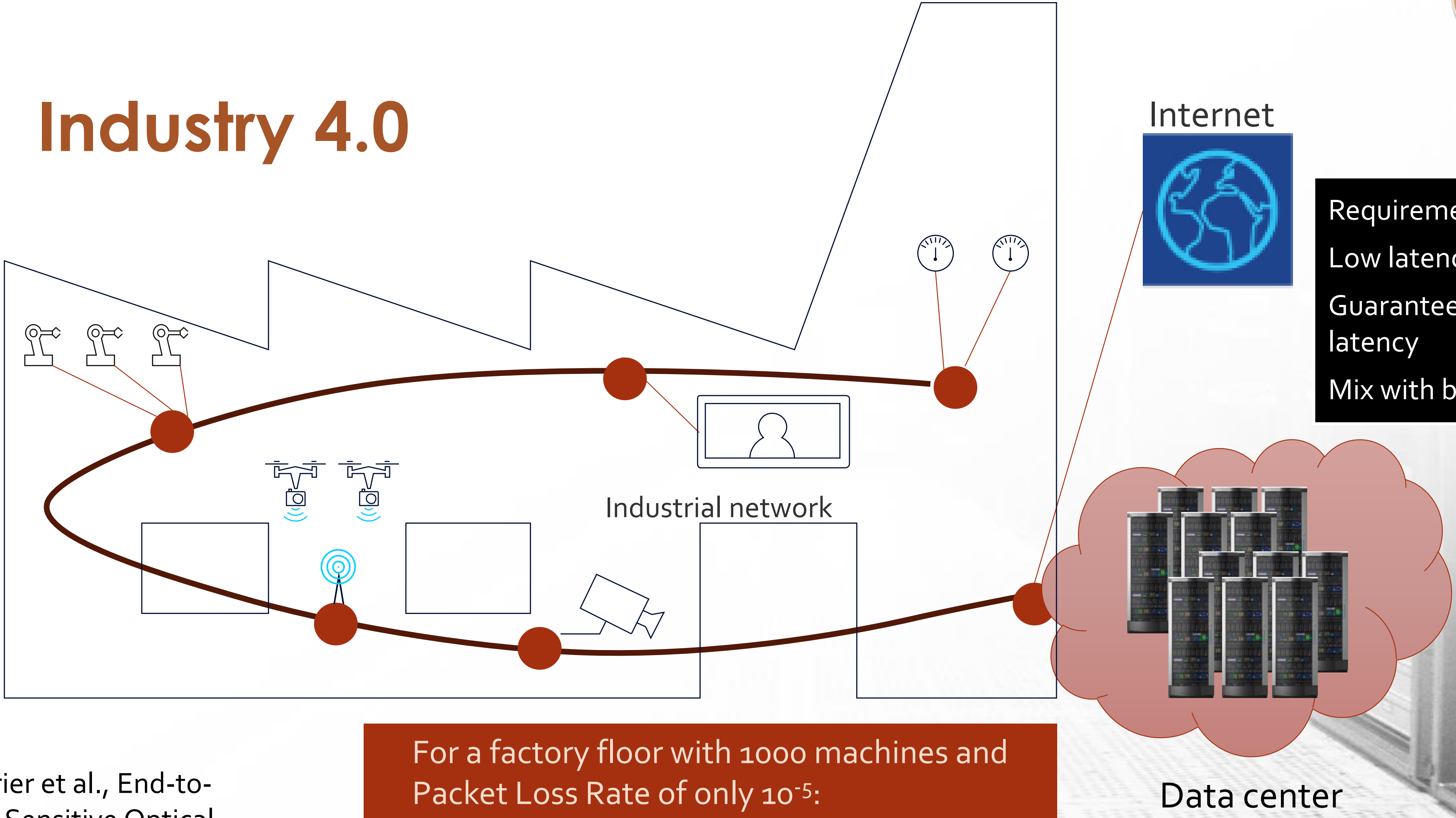
Guaranteed (deterministic) capacity

Network slicing



SENDATE

Industry 4.0



Requirements:

Low latency

Guaranteed (deterministic) latency

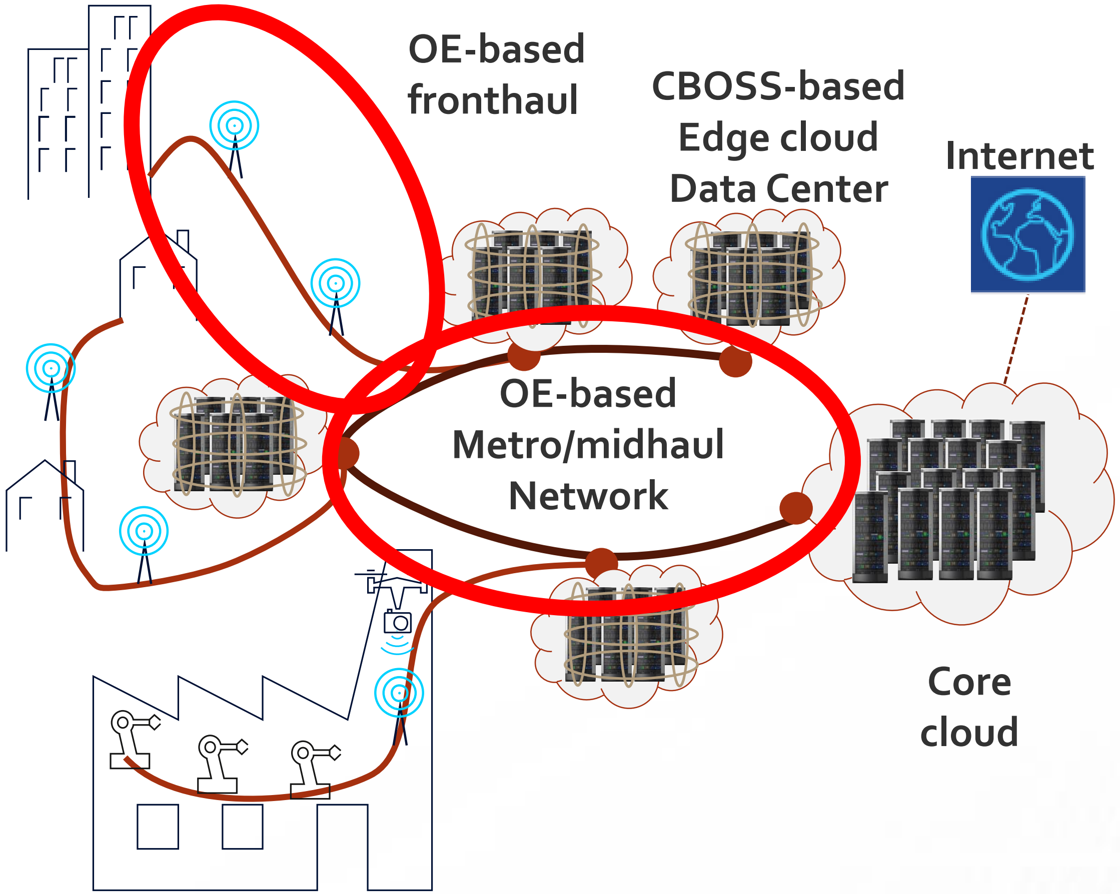
Mix with best effort traffic

For a factory floor with 1000 machines and Packet Loss Rate of only 10^{-5}:
10 factory halts per day

Y. Pointurier et al., End-to-End Time Sensitive Optical Networking: Challenges and Solutions, JLT, Jan. 2019.

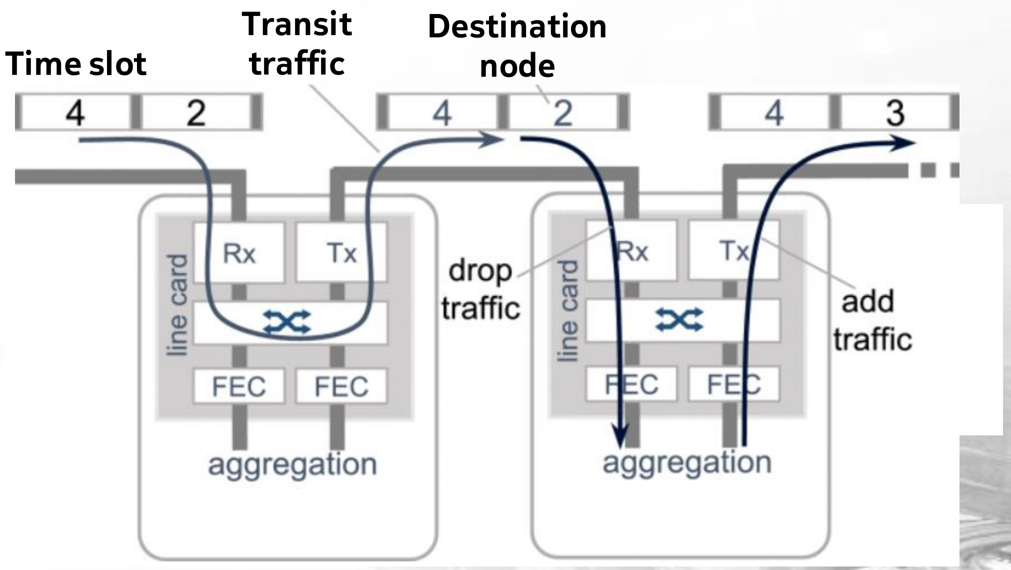
Dynamic Deterministic Network: Optical Ethernet for fronthaul/midhaul/metro

Network architecture



W. Lautenschlaeger et al., "Optical Ethernet – Flexible Optical Metro Networks," in JLT, Jun. 2017.

Optical Ethernet (OE)



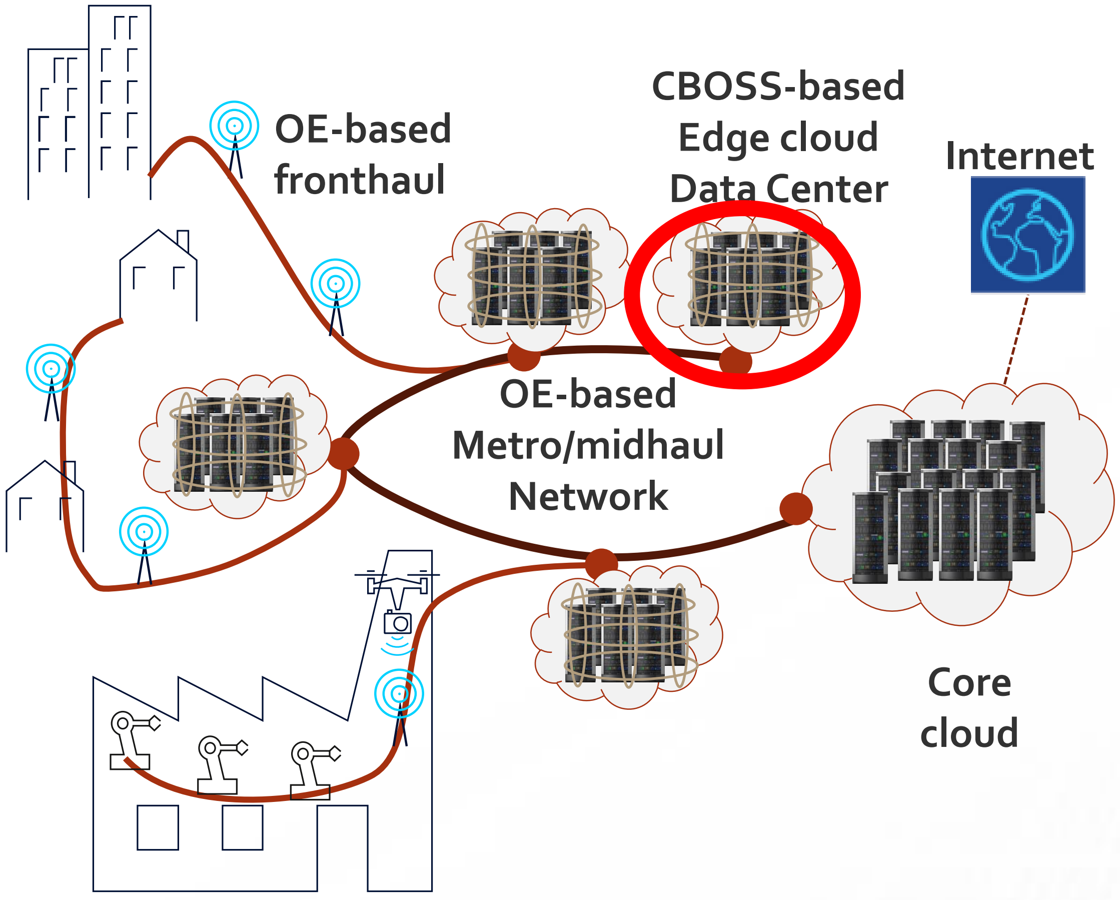
Instantaneous communication without prior path allocation

Re-use of reserved but underutilized capacity

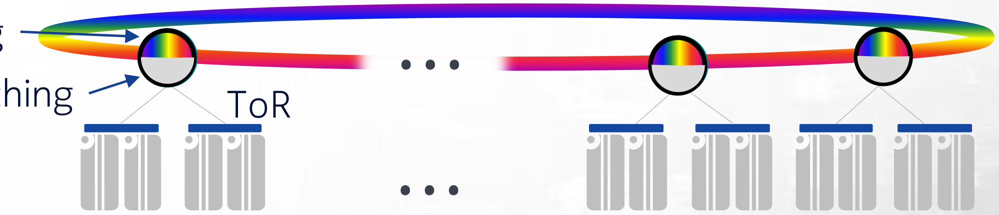
FEC processing only at end-points

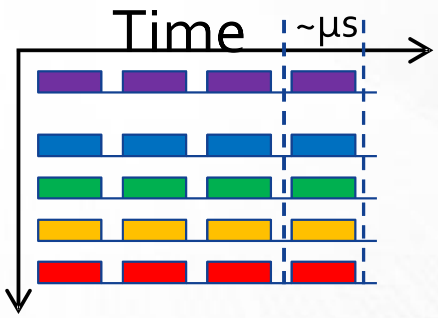
Dynamic Deterministic Network: Cloud-BOSS for Intra-DC

Network architecture



Cloud Burst Optical Slot Switching (CBOSS)





Data traffic arrangement

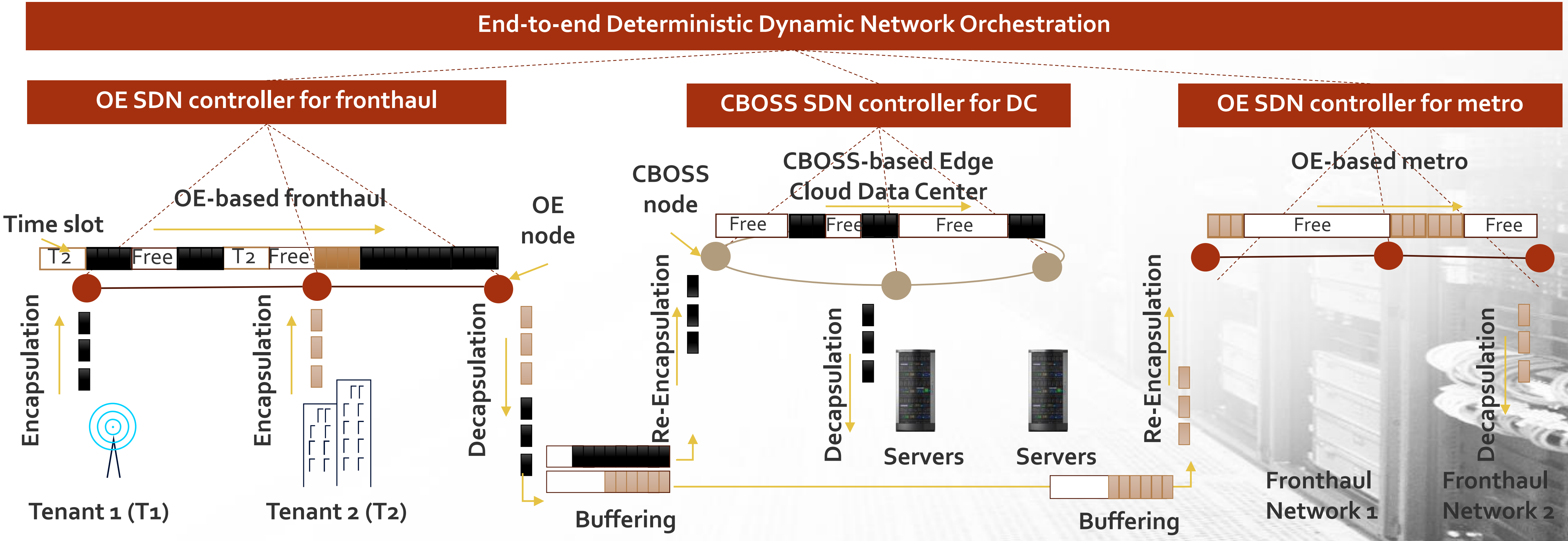
Reservation policies on us-scale time slots

Fast tunable Tx (ns scale)

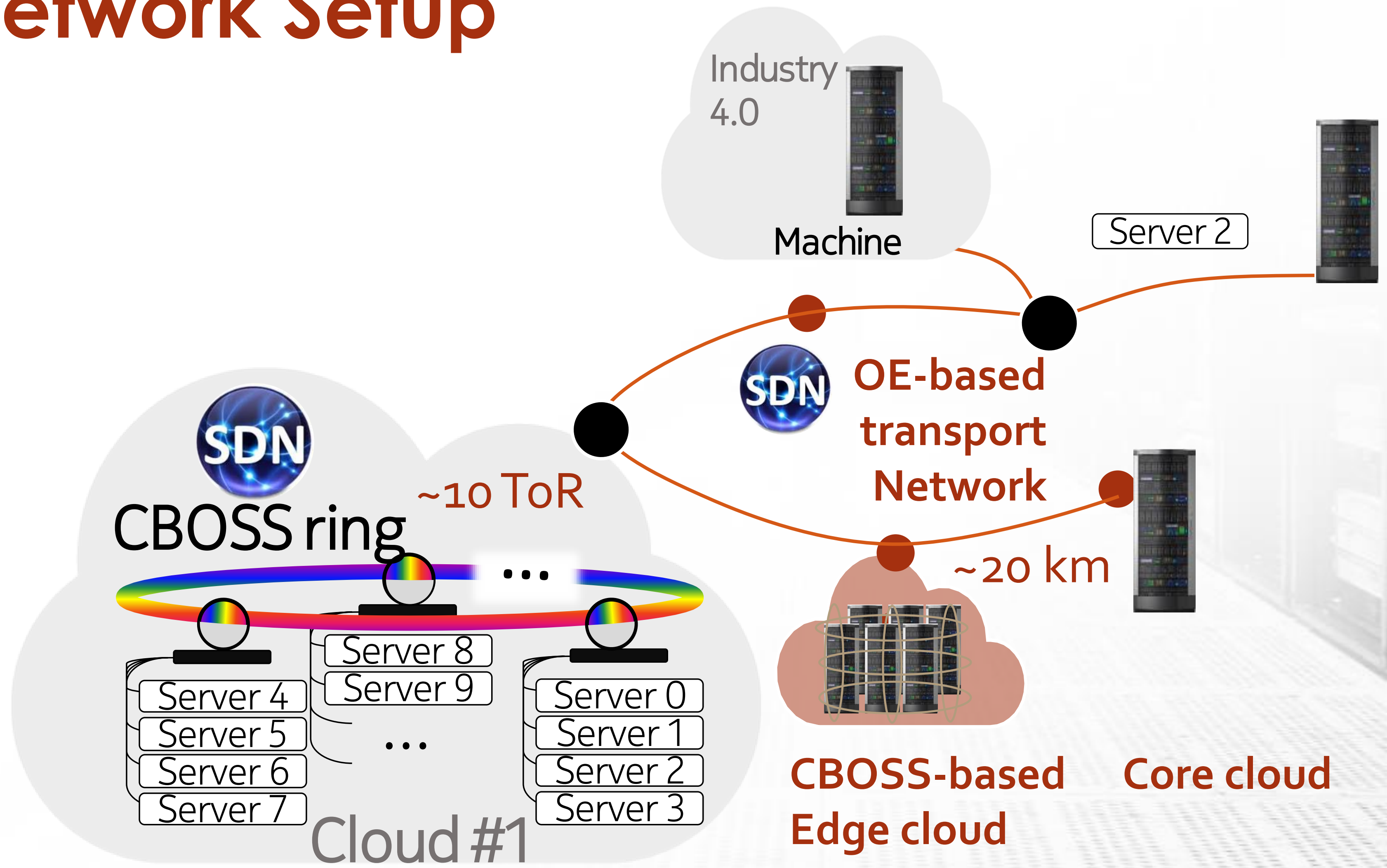
Wavelength-based scaling

N. Benzaoui et al., "Cloud-BOSS Intra-Data Center Network: on-Demand QoS Guarantees via µs Optical Slot Switching," in JOCN, Jul. 2018

Dynamic Deterministic Network (DDN): End-to-end architecture



End to end Dynamic Deterministic Network Setup

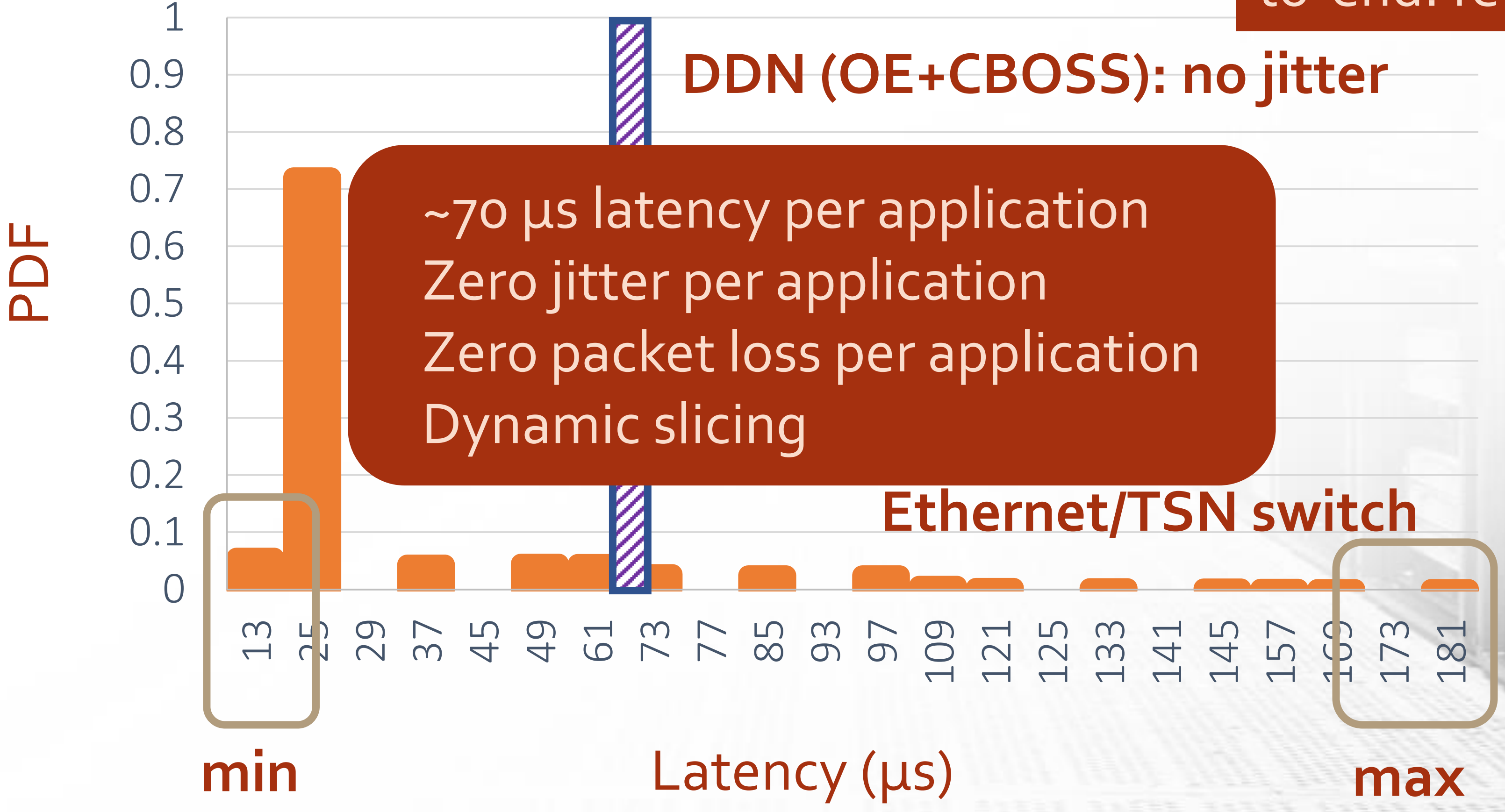


SENDATE

Deterministic Dynamic Network vs. Ethernet

Load of 50% generated by **7 flows**

Time to establish a flow end-to-end: few milliseconds



N. Benzaoui et al., "DDN: Dynamic Deterministic Networks," ECOC 2018 PDP

Thanks to all SENDATE colleagues and specially material from: Nihel Benzaoui, Fabien Boitier, Marija Furdek, Carmen Mas Machuca, Rastin Pries, Petra Vizarreta

supported by

Federal Ministry of Education and Research

DGE DIRECTION GÉNÉRALE DES ENTREPRISES

Tekes

VINNOVA

Celtic-Plus Smart Connected World

http://www.sendate.eu/