Keynote Talk @ DRCN

Coimbra, Portugal
March 20th 2019

POLITECNICO DI MILANO

15th International Conference

Design of Reliable Communication Networks

March 19-21, 2019
Coimbra, Portugal

Reliable Optical Metro Networks for 5G communications

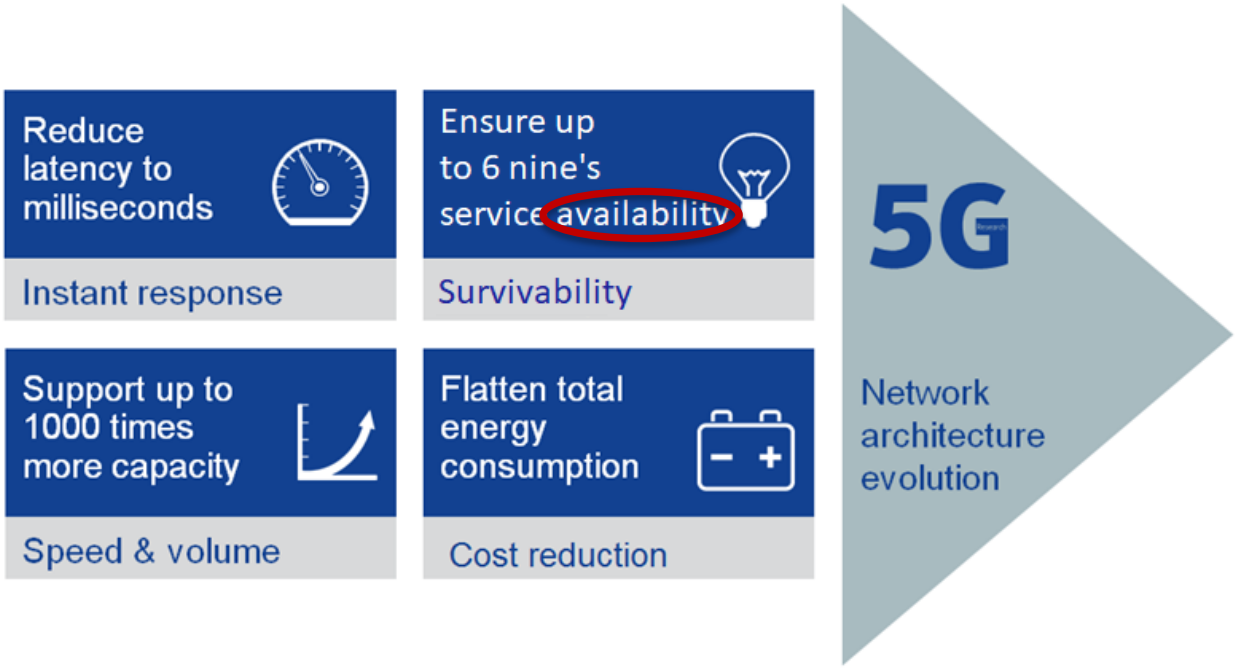
Massimo Tornatore
Politecnico di Milano, Italy & University of Calfornia, Davis

WG2 Leader
Cost Action RECODIS

RECODIS
Resilient communication services protecting end-user applications from disaster-based failures

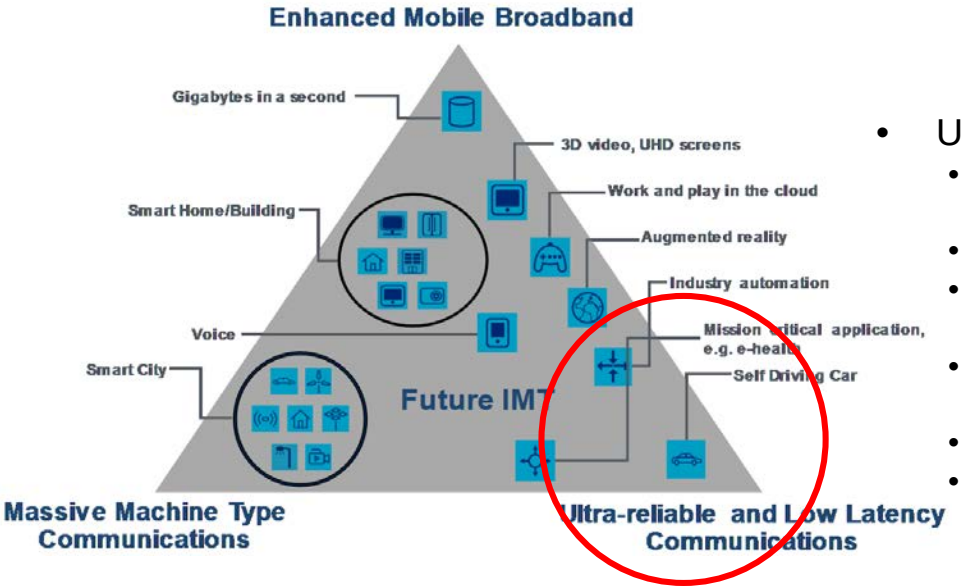
@MaxTornatore

Road to 5G



Source: Kanika Atri, Jan 2015

Ultra-reliable Communications



- URLLC
  - Automated Traffic Control and Driving
  - Collaborative Robots
  - eHealth (Extreme Life Critical)
  - Remote Object Manipulation (Remote Surgery)
  - 3D Connectivity (Drones)
  - Public Safety

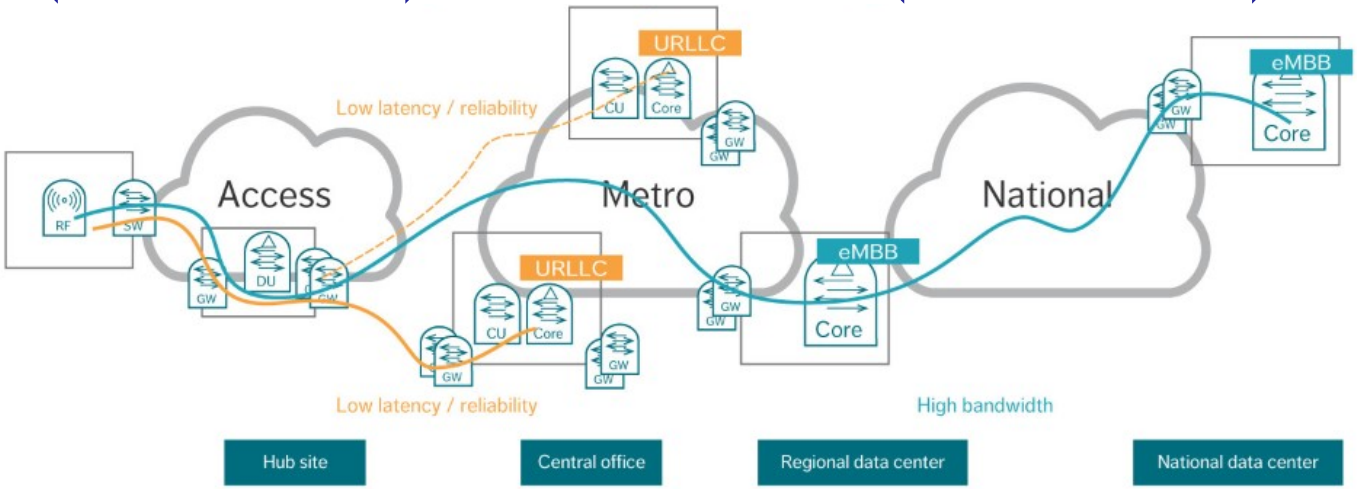
End-to-end 5G reliability

Per-segment reliability techniques

- Access techniques
  - packet duplication
  - massive MIMO
  - multi-connectivity (interface diversity)

Gap in research and solutions?

- Core techniques (!)
  - DRCN's bread and butter ☺
  - Protection vs. restoration
    - DPP, SBPP..
    - …



Source: https://www.ericsson.com/en/ericsson-technology-review/archive/2018/enabling-intelligent-transport-in-5g-networks

5G RAN and Optical Metro Networks

- Current Radio Access Networks (RAN)
- 5G RAN:
  - **more antennas** (densification)
  - **more spectrum**
  - (e.g., CoMP)
  - **MIMO**
  - Centralized RAN (**C-RAN**)
    - RAN coordination
    - High bandwidth
    - Low latency

A new generation of optical metro networks is needed to cope with the requirements of 5G communications

Evolution of Metro Networks (I)

- Today

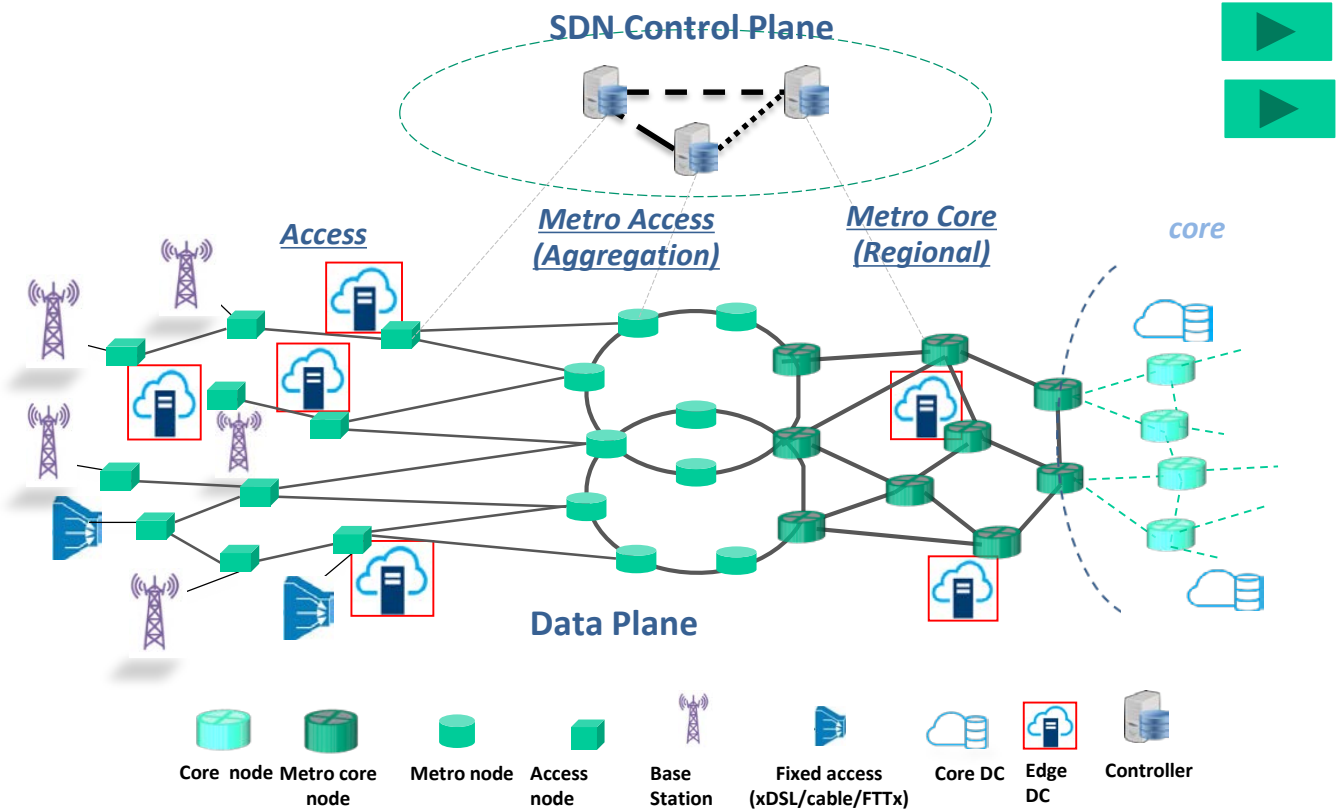
  a rigid tree/ring-based aggregation infrastructure

- Tomorrow

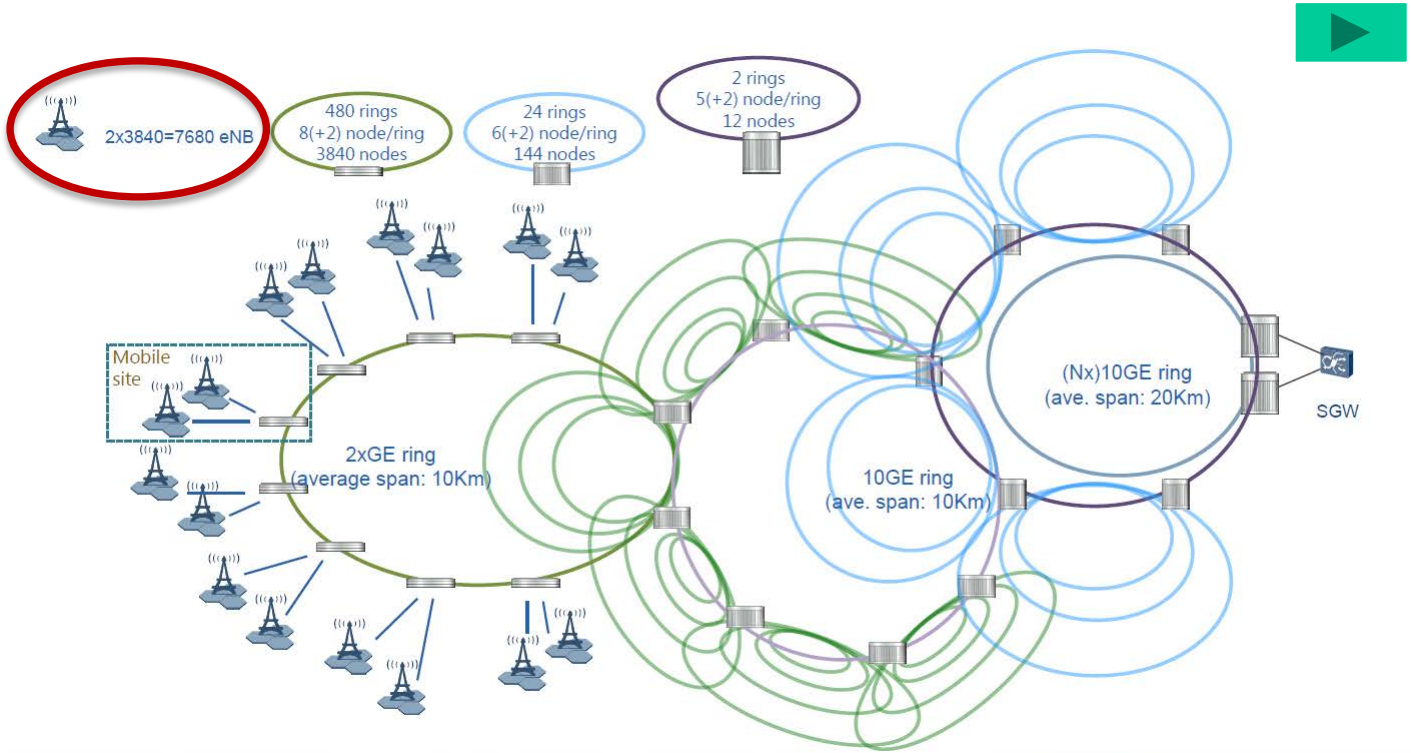
  a composite and meshed network-and-computing ecosystem

Evolution of Metro Networks (II)

Edge computing and SDN

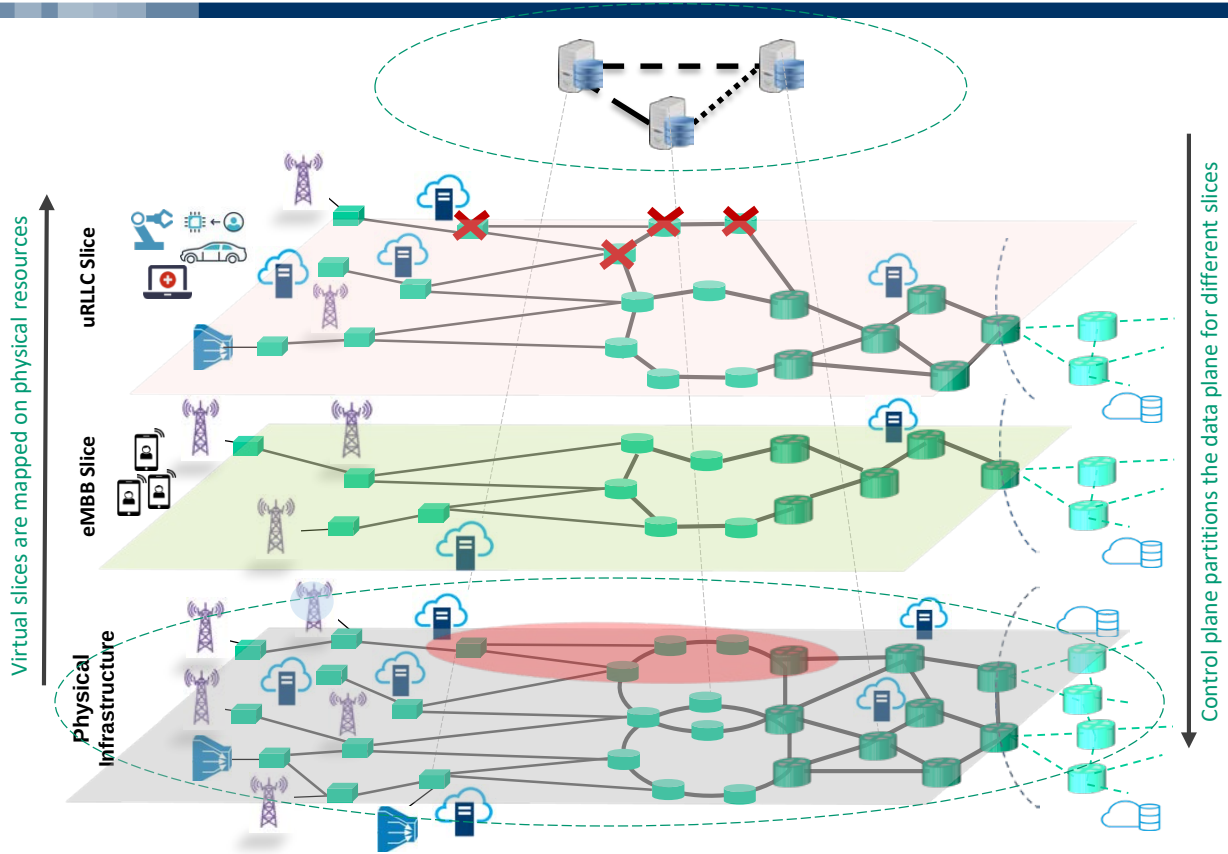


Well.. it looks much more like this one for a large metropolitan area…

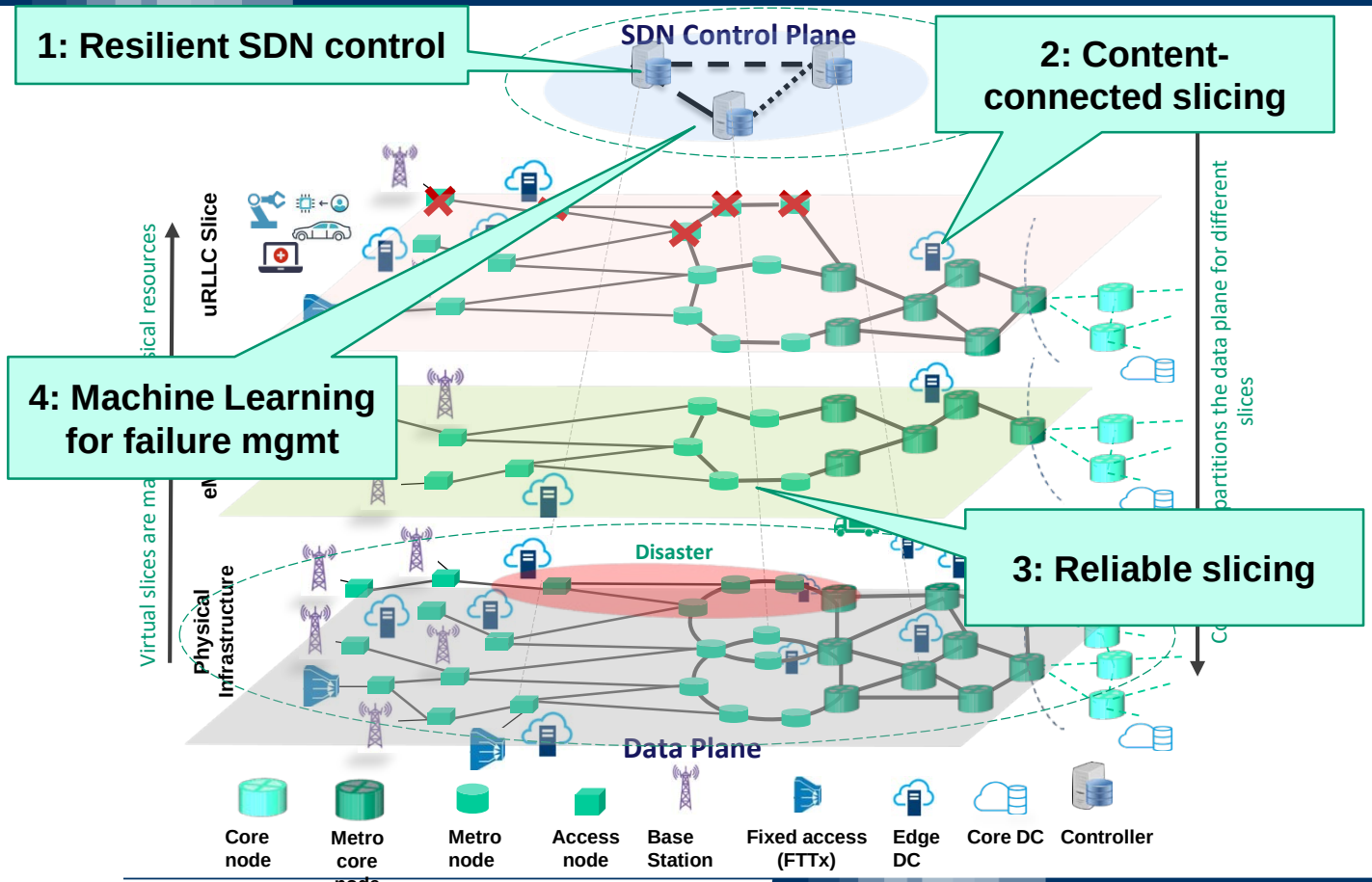


Evolution of Metro Networks (II)

Network Slicing



Rising Research Topics



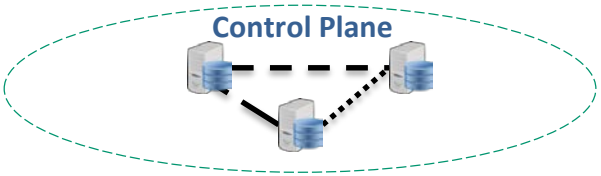
Outline

- Rising Topics
  1. **Resilient SDN control**
  2. **Content-connected slicing**
  3. **Reliable Service Chaining**
  4. **Machine Learning for failure mgmt**

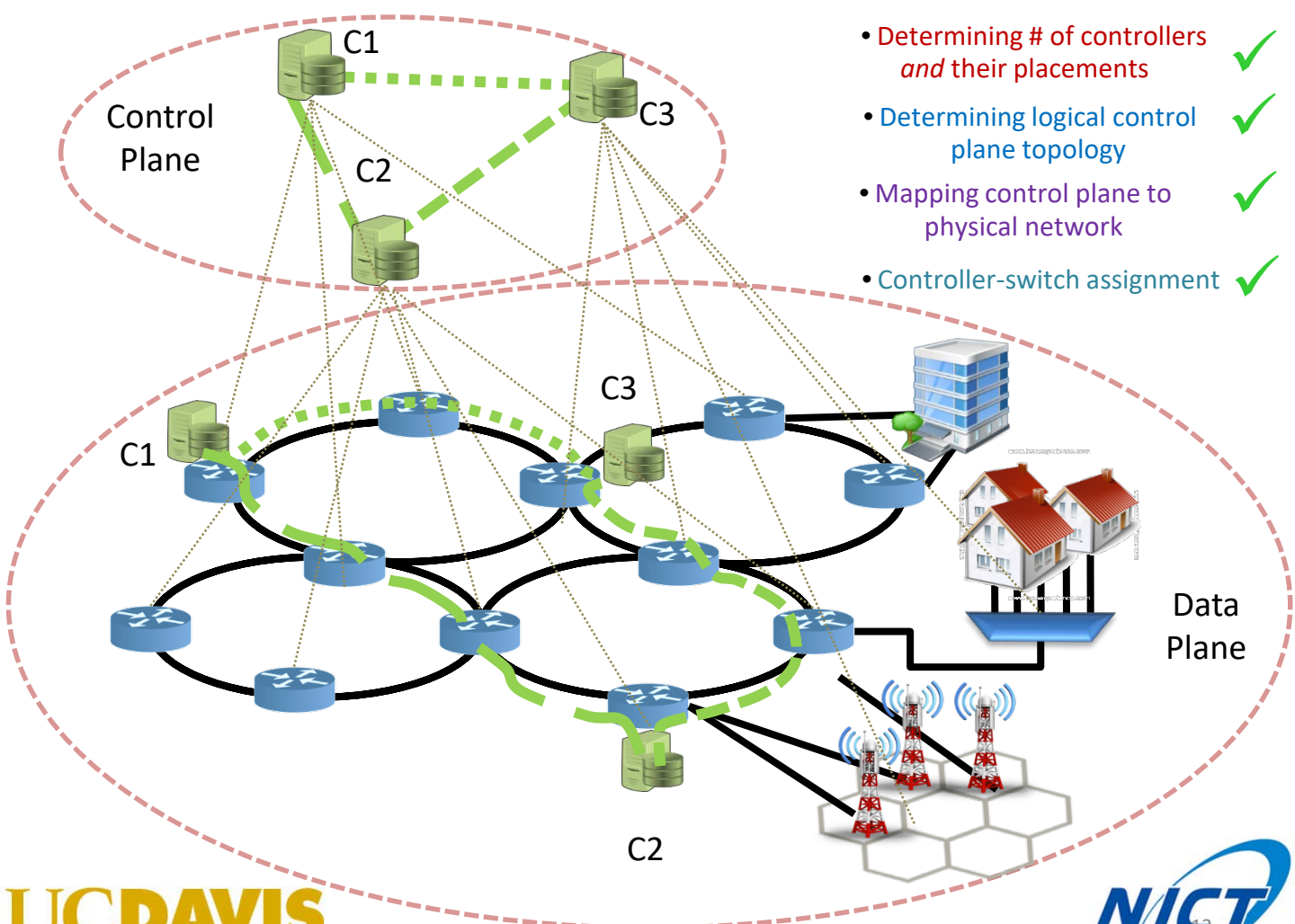
- Conclusion and Future Directions

Resilient SDN Control

- Control plane resiliency→ redundancy → distributed controllers



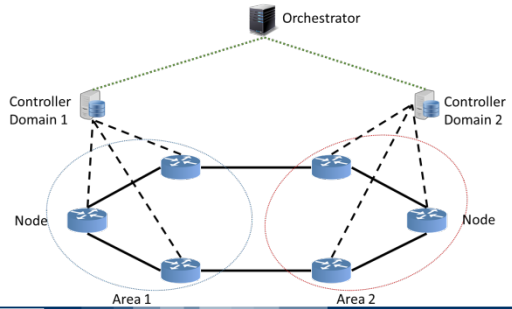
  - *How many controllers?*
  - *Where to place them?*
  - *Consider latency, survivability, capacity requirements, synchronization overhead, etc.*



- Determining # of controllers *and* their placements ✓
- Determining logical control plane topology ✓
- Mapping control plane to physical network ✓
- Controller-switch assignment ✓

Existing work on controller placement (CP)

- **CP problem (no resiliency)**:
  - B. Heller, et al., The controller placement problem, in: Proc. of the ACM HotSDN, New York, NY, USA, 2012.
  - **[Capacitated]** G. Yao, et al., On the capacitated controller placement problem in software defined networks, IEEE Comm. Lett. 18 (8) (2014) 1339–1342.
  - **[WAN]** P. Xiao, et. al, The SDN controller placement problem for WAN, in: Proc. of the IEEE/CIC ICCC, 2014.
  - **[Dynamic]** M.F. Bari, et al., Dynamic controller provisioning in software defined networks, in: Proc. of the IEEE CNSM, 2013.
  - **[Elastic]** A. Dixit,et. al, Towards an elastic distributed SDN controller, in: Proc. of the ACM HotSDN, New York, NY, USA, 2013.
  - **[T-SDN (Orchestrator+Controllers)]** R. Lourenço, et. al, “Robust hierarchical control plane for transport software-defined networks,” Optical Switching and Networking, vol. 30, 2018



Existing work on resilient CP

- **Fault tolerant CP problem (resiliency)**:
  - **[Pre-planned controller replicas]** (F.J. Ros, P.M. Ruiz, Five nines of southbound reliability in software-defined networks, in: Proc. of the ACM HotSDN, New York, NY, USA, 2014) & (B. Killi, et al., Capacitated next controller placement in software defined networks, IEEE Trans. Netw. Service Manage. 14 (3) (2017) 514–527)
  - **[Path diversity]** F. Müller, et al., Survivor: an enhanced controller placement strategy for improving SDN survivability, in: Proc. of the IEEE GLOBECOM, 2014
  - **[Disaster awareness]** S. Savas, et al., "Disaster-resilient control plane design and mapping in Software-Defined Networks," *In Proc. of HPSR,* Budapest, Hungary, July 2015
  - **[Malicious Attacks]** D. Santos, A. de Sousa, C.M. Machuca, Robust SDN controller placement to malicious node attacks, in: Proc. of IEEE DRCN, 2018.
  - **[Several types of failures]** D. Hock, et al., Pareto-optimal resilient controller placement in SDN-based core networks, in: Proc. of the 25th International Teletraffic Congress (ITC), 2013.

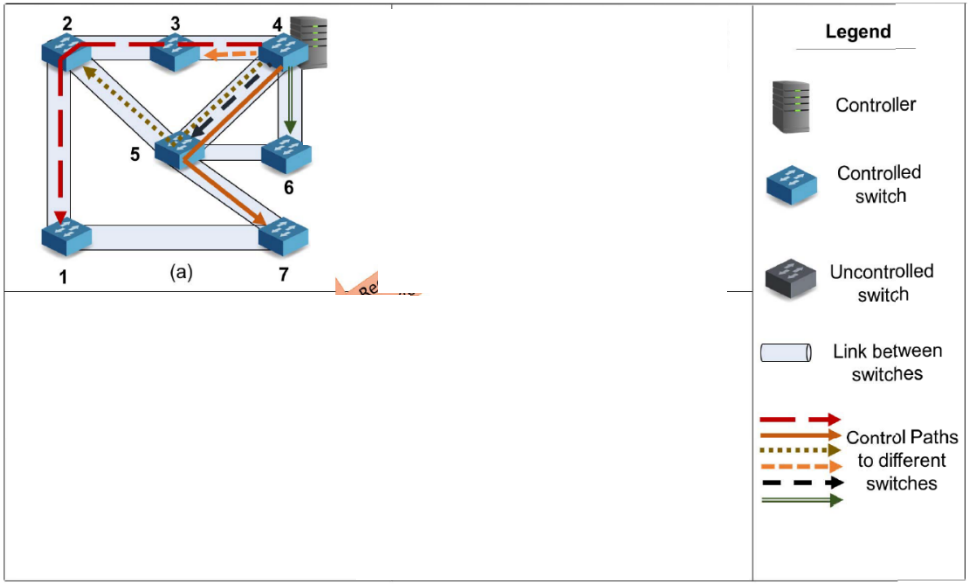
- Ok controller has been properly placed…
- .. still *how we interconnect controllers to switches* is crucial to minimize recovery time!

S. Savas et. al, "RASCAR Recovery-Aware Switch-Controller Assignment and Routing in SDN", IEEE Transactions on Network and Service Management

Looking at “controller to switch” paths!

Multi-stage recovery

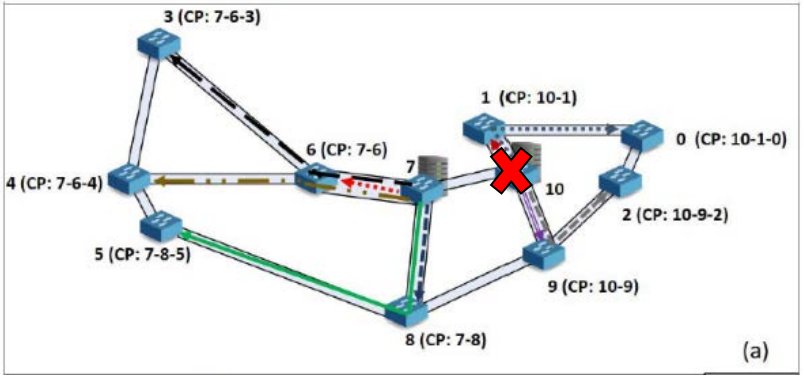
- Even a single failure affects multiple switch-to-controller **control paths**
- When switches lose control paths, they become “**uncontrolled**”:
  - route traffic using old flow entries
  - cannot exchange control messages (e.g., flow setup request, flow installation)
  - cannot be used for data path restoration



Recovery aware vs. unaware (I)

Recovery speed depends on how you route control paths

- A single failure may affects multiple switch-to-controller **control paths.**



Shortest-Path-Based Control Path Routing	
0 - 1 – 10	**3** - 6 – 7
1 – 10	**4** - 6 – 7
2 - 9 – 10	**5** - 8 – 7
9 – 10	**6** – 7
	8 – 7

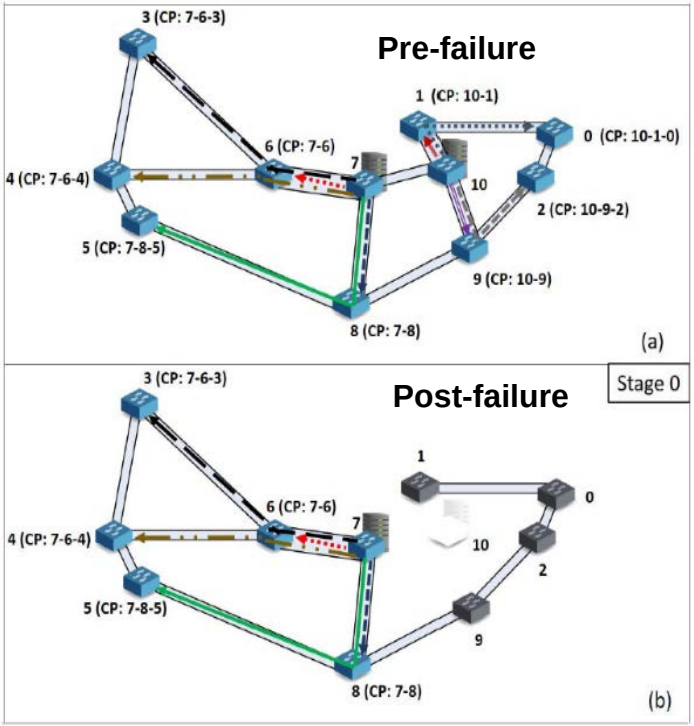
→ Node 10 fails.

Affected control paths:
Node 0-1-2-9

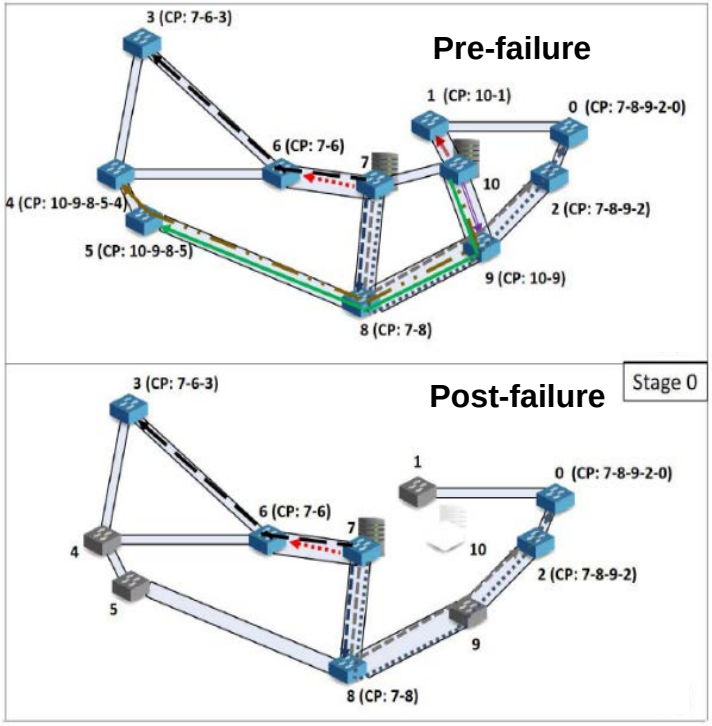
→ All control is lost.

Recovery unaware vs. aware (I)

Recovery unaware → 4 recovery steps



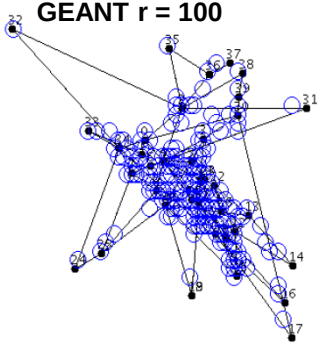
Recovery aware → only 2 recovery steps

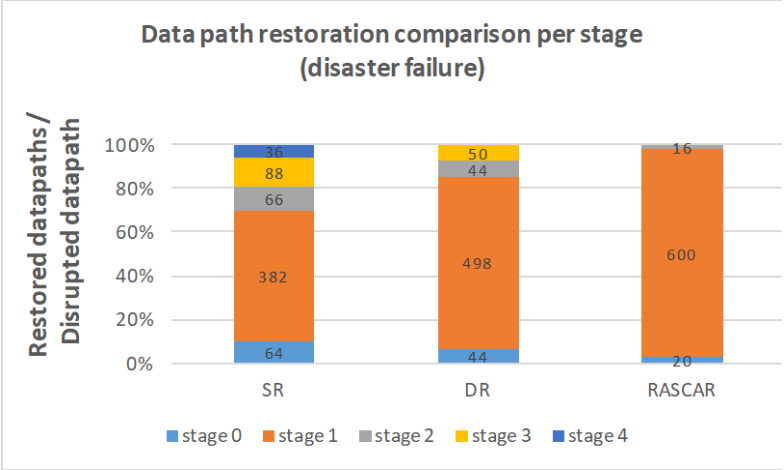


Take away: perform "load balancing" of control paths against node failures

Results: recovery speed vs. cost

GEANT r = 100





Note: what about additional cost?

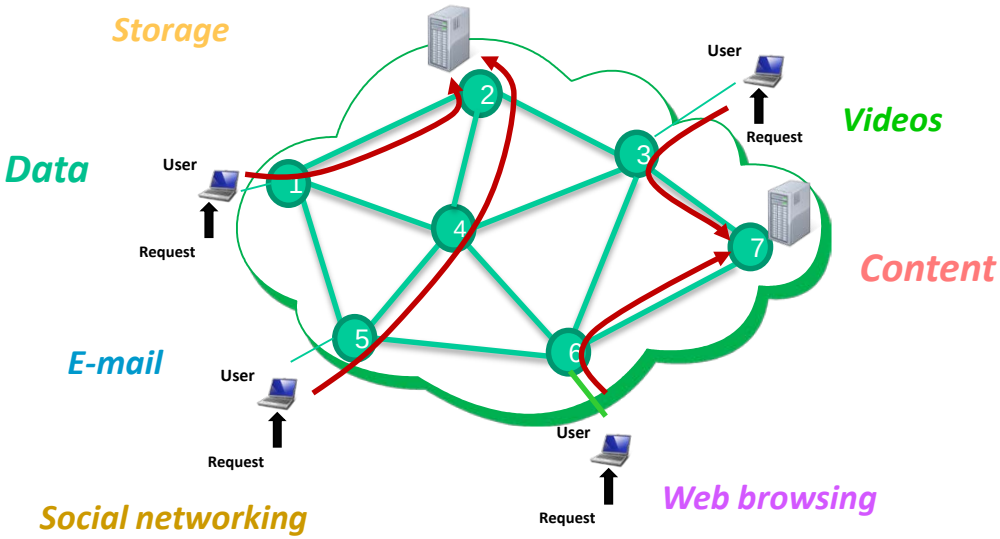
Less than 1% additional resource consumption.
Only control paths become longer!

Outline

- Evolution of optical networks towards 5G
- Rising Topics
  1. **Resilient SDN control**
  2. **Content-connected slicing**
  3. **Reliable Service Chaining**
  4. **Machine Learning for failure mgmt.**
- Conclusion and Future Directions

Cloud Services

Any Content, Anywhere, Any Time



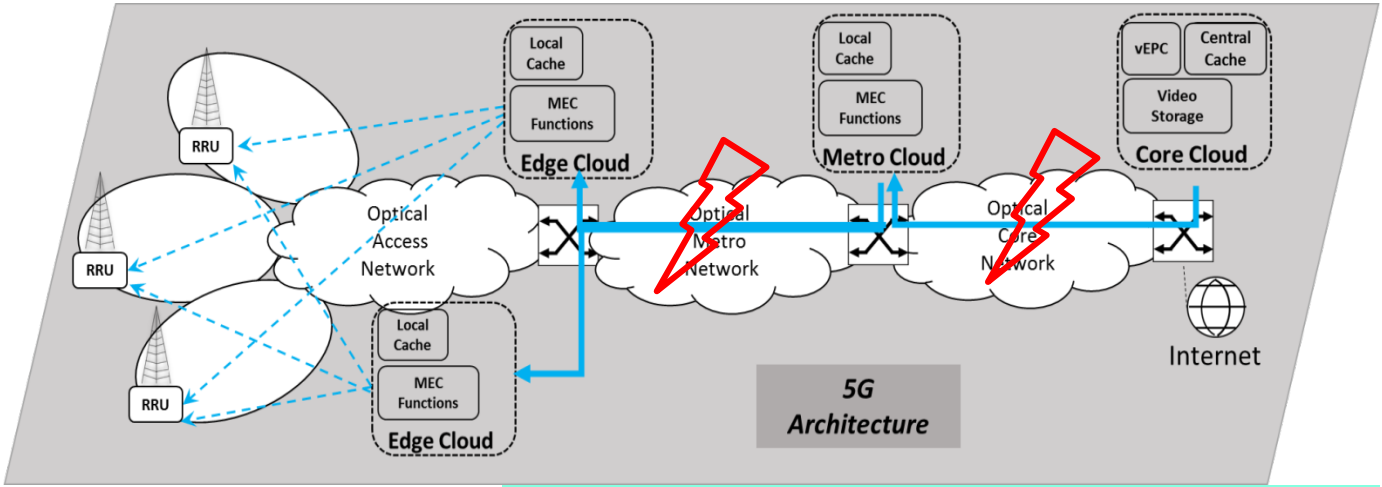
90% of the total Internet traffic is content/cloud [2]

- **What really matters is the connectivity to content**
- **End-to-End → End-to-Content**

[2] CISCO. Cisco Visual Networking Index: Forecast and Methodology, 2011-2016. in White Paper, May 2012

From Cloud to Edge Computing

- 5G networks must provide 99,999% service availability [4]
  - Can we rely on a mesher network? No, costly..
  - Idea: **Alternative DCs can be accessed in case of disconnection!**
  - Enabler: Fog Computing, Mobile Edge Computing (MEC), Surrogate Servers, Caches, CORD,…
  - Latency? Traffic Offloading?.... Reliability!



[4] NGMN Alliance "5G white paper." *Next generation mobile networks, white paper* (2015).

New Survivability Metric: Content Connectivity

Traditional metric:

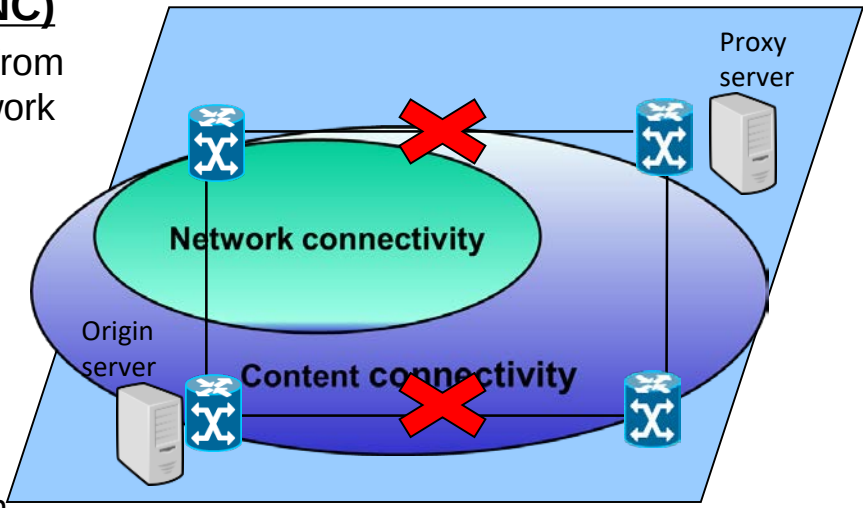
Network connectivity (NC)

- Reachability of all nodes from any other node in the network

New metric:

Content connectivity (CC)

- Reachability of content from any node in the network



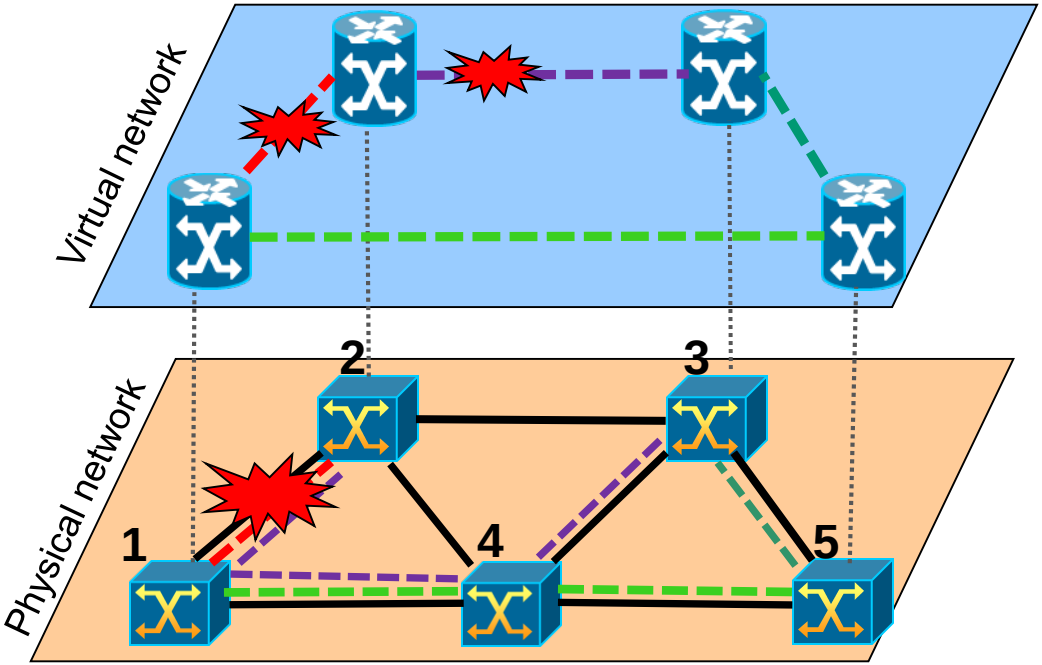
M. F. Habib et al., "Fault-Tolerant Virtual Network Mapping to Provide Content Connectivity in Optical Networks,"OFC 2013

Many open questions on Content Connectivity!

- How do survivability problems evolve in case of Content Connectivity?
  - My example in the following: Survivable Virtual Network Mapping (Multi-layer protection)

Survivable Virtual Network Mapping (SVNM)

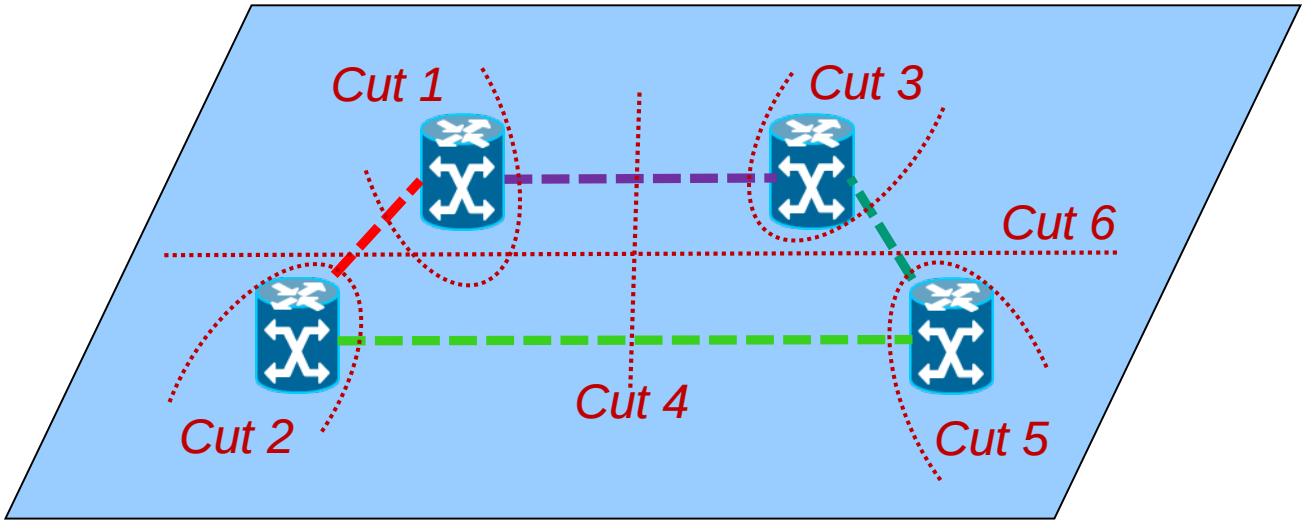
A non-survivable example



- Note: Embedding vs. Mapping

Condition to ensure SVNM

- **Cut: set of links whose removal will partition the network into two distinct sets**

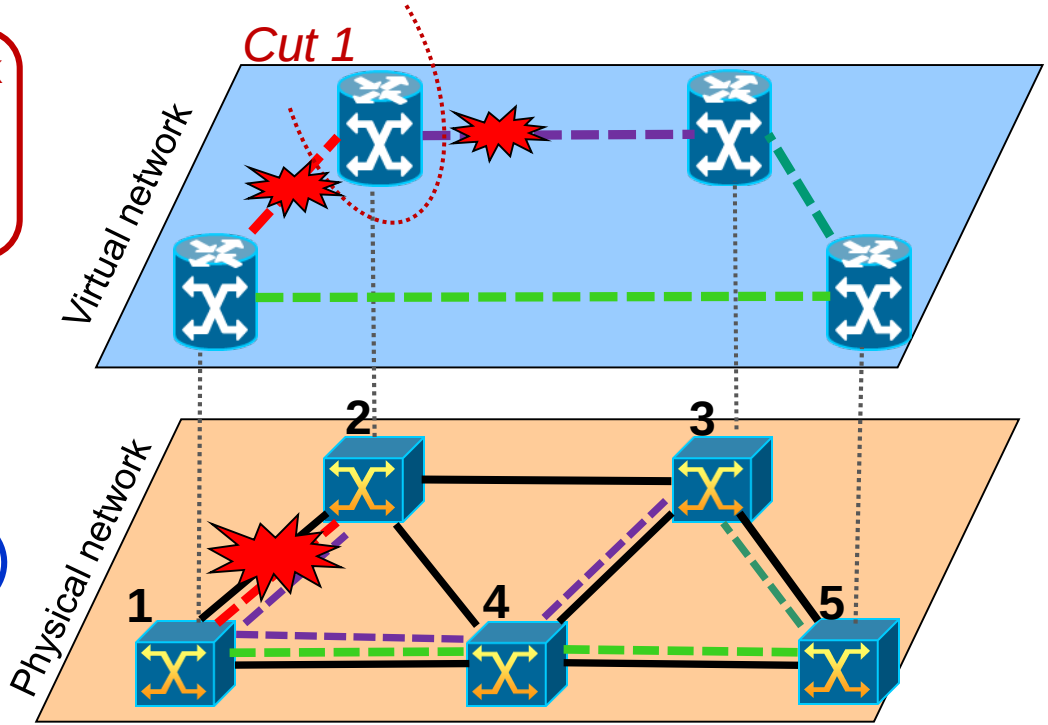


- **Condition: no physical link shall support all the virtual links in a virtual cutset**

Non-Survivable Mapping For Net. Connectivity

Example

e.g., physical link (1-2) supports all virtual links of *Cut 1*

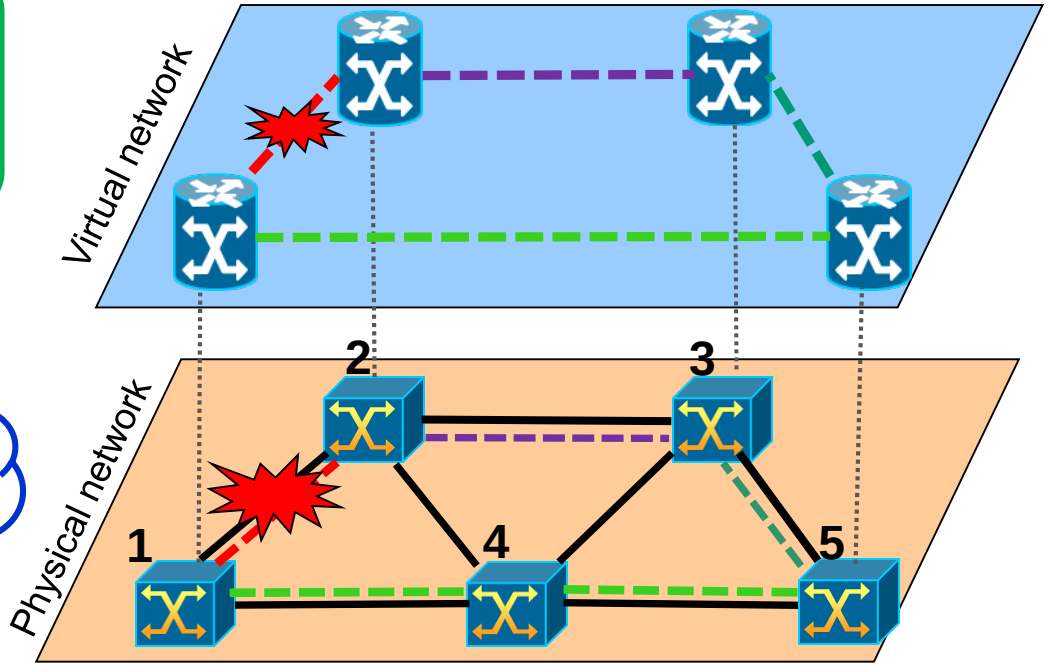


Non Survivable Mapping

Survivable Mapping For Network Connectivity

Example

No physical link that supports all the virtual links of any cutset



Survivable Mapping

SVNM: Condition For Content Connectivity

NC: no physical link shall support all the virtual links in a virtual cutset

≠

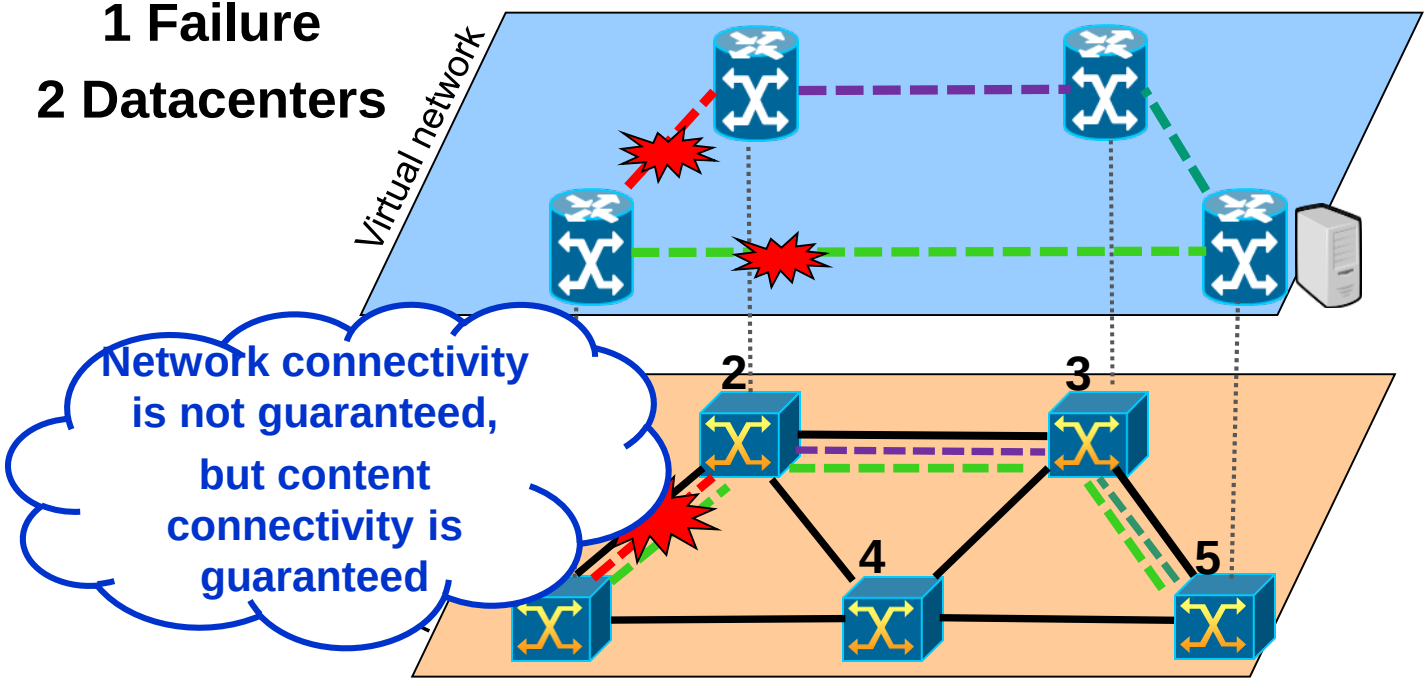
CC: all virtual nodes can reach at least one content replica after the occurrence of a failure

SVNM with Content Connectivity

Scenario

1 Failure

2 Datacenters



NC1 vs CC1 vs NC2 vs CC2

- **Approaches against single-link failures:**
- Network Connectivity (NC1)
- Content Connectivity (CC1)

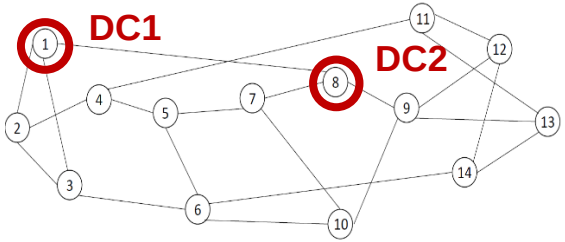
- **Approaches against double-link failures:**
- Network Connectivity (NC2)
- Content Connectivity (CC2)

Can we provide NC1 after first failure? and maintain CC2 after second failure, until failure recovery is complete?

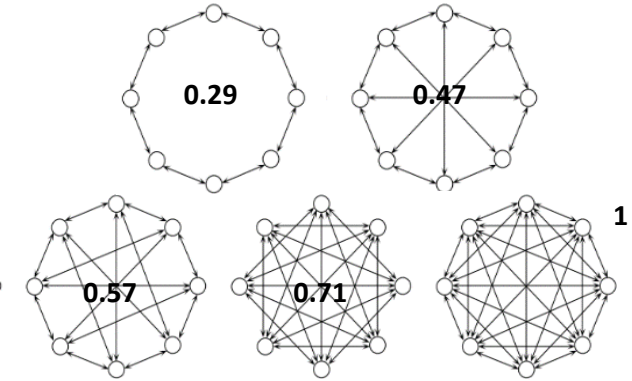
NC1 + CC2

Resource Occupation

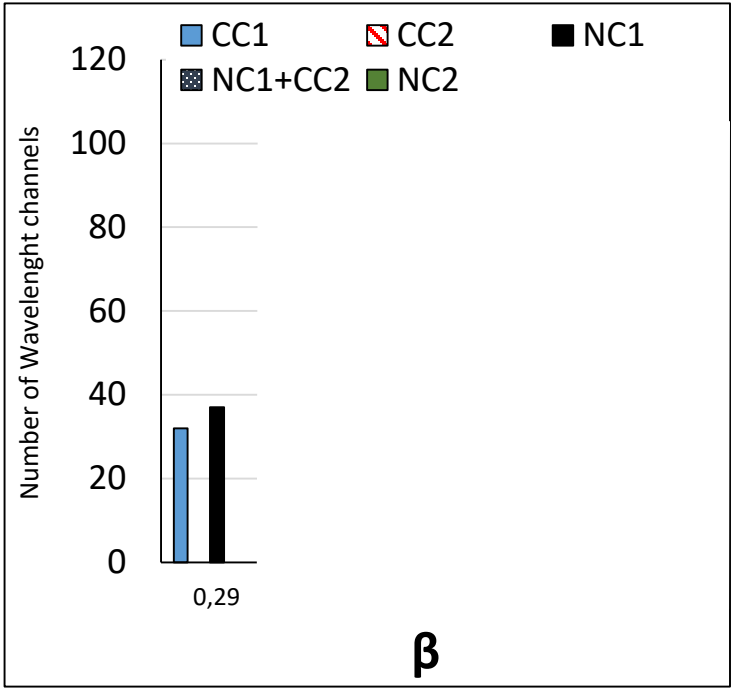
Physical topology: NSFNET
(14 nodes, 22 bidirectional links)



Logical topologies: Different connectivity degrees (**β**)



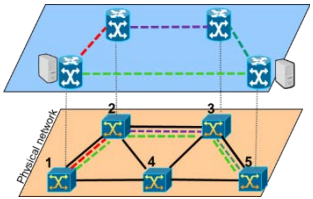
- Number of datacenters: 2
- Number of wavelengths per link: 20

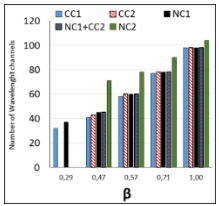


Lesson Learned

- **Network connectivity for 1 failure augmented with content connectivity for two failures (NC1+CC2)** requires minimum additional resources and a limited number of datacenters

- **Several open questions, e.g.,** which strategy is better to ensure content connectivity?
  - Increase number of replicas (more datacenters)?
  - Increase connectivity of virtual network (more links)?



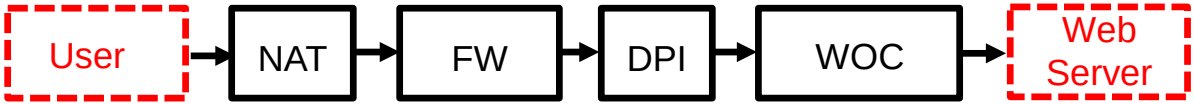


Outline

- Evolution of optical networks towards 5G
- Rising Topics
  1. **Resilient SDN control**
  2. **Content-connected slicing**
  3. **Reliable Service Chaining**
  4. **Machine Learning for failure mgmt**
- Conclusion and Future Directions

Slices and Service Chains

- Slice: set of interconnected virtualized resources (net+comp) to provision a service
- Service Chain (SC): an element (one specific sequence of virtualized rescources) in a slice
- Example: Web-Service SC

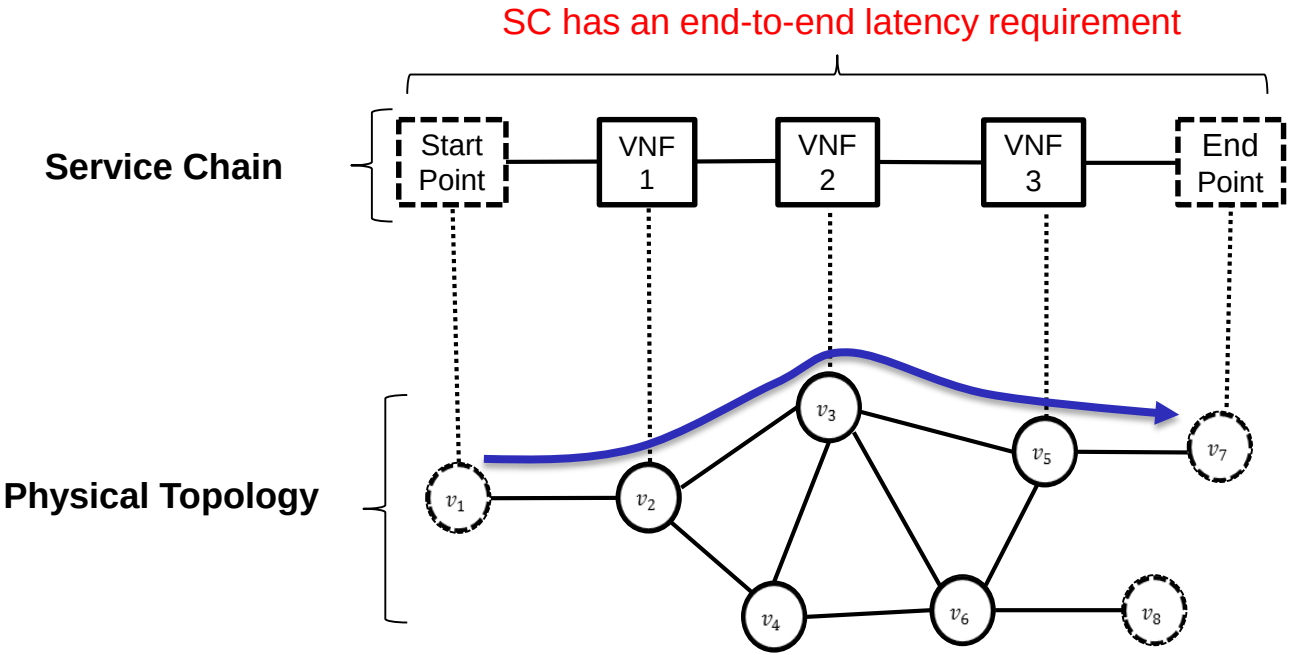


NAT: Network Address Translator
FW: Firewall
DPI: Deep Packet Inspection
WOC: WAN Optimized Controller

- Each SC has its own requirements in terms of
  - Bandwidth
  - Latency
  - Resiliency

Service Chaining

VNF placement + Traffic routing



Resilient Service Chaining

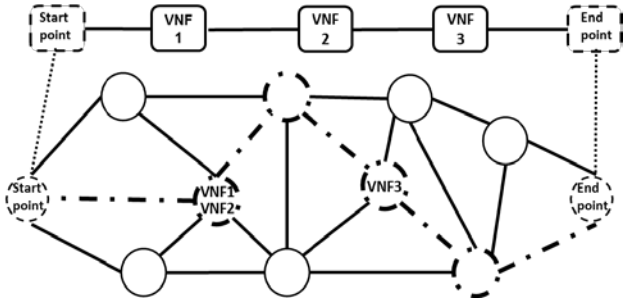
Questions to be answered

- Where do we place VNFs and route traffic to **ensure resiliency** against link/node failures?
- Which protection schemes shall we apply?

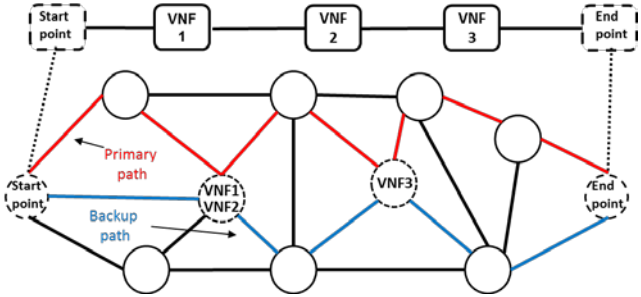
Protection schemes

Several possible combination/choices

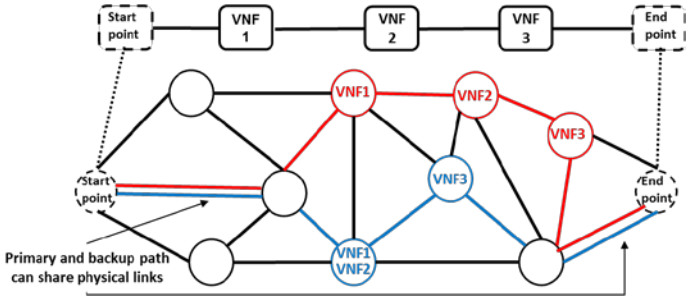
Unprotected



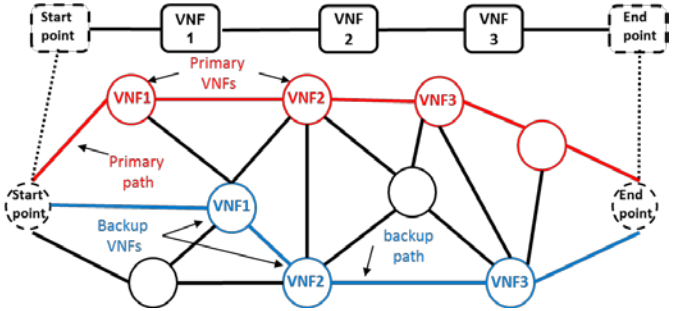
(Virtual) Link Protection (Vl-P)



(Virtual) Node Protection (Vn-P)



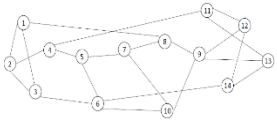
End-to-End Protection (E2E-P)



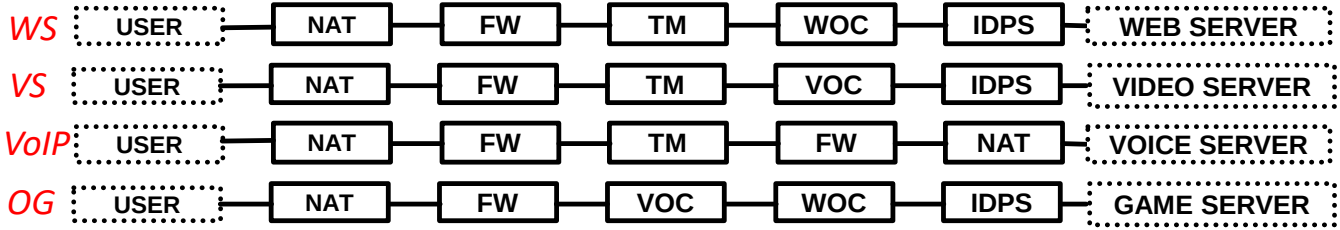
A. Hmaity et al. "Protection strategies for virtual network functions placement and service chains provisioning, " Networks, Vol. 70, no. 4, pp. 373-387, 2017

Case study

- NSFNET network topology (14 nodes, 22 links @1Gb/s)



- 5 different types of SCs



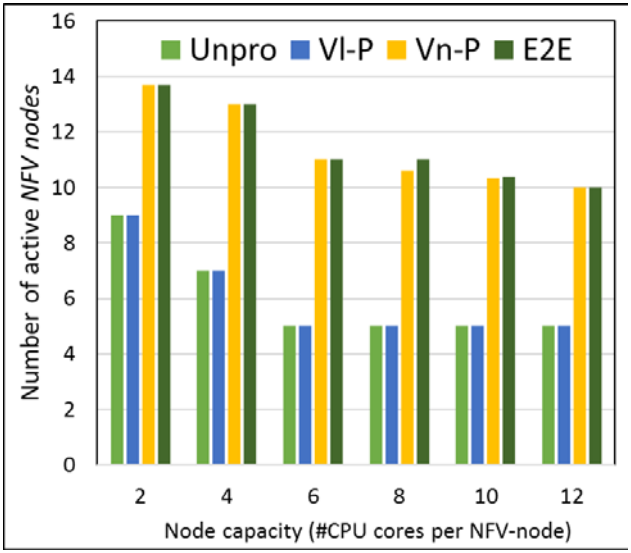
NAT: Network Address Translator, **FW**: Firewall **TM**: Traffic Monitor, **VOC**: Video Optimization Controller, **IDPS**: Intrusion Detection Prevention System, **WOC**: WAN Optimized Controller

Service Chain	Bandwidth (kb/s)	Max latency (ms)
Web Service (WS)	100	500
Video Streaming (VS)	4000	100
VoIP	64	100
Online Gaming (OG)	50	60

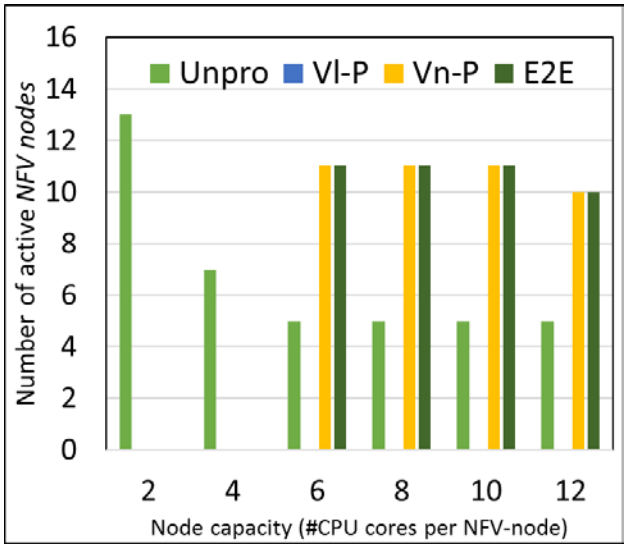
[8] *M. Claypool and K. Claypool, Latency and player actions in online games, Commun. ACM 49, 11 (November 2006), 40-45*
[9] A. Hmaity et al. "Virtual Network Function placement for resilient Service Chain provisioning," 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, 2016, pp. 245-252.

Results – Number of required NFV Nodes

Web Service



Online gaming



Lessons learned

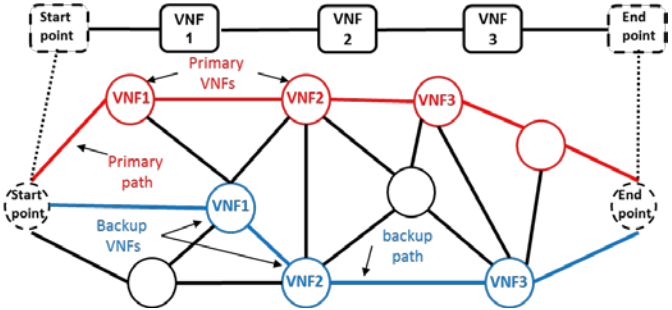
- Applications have diverse requirements (latency, computing intensity, bandwidth, reliability)
- → no one-size-fit-all protection solution

- Low-latency service are especially constrained in their protection alternatives

Growing interest
(*e.g., these two papers in incoming INFOCOM19*)

Jiao Zhang, et al., RABA: Resource-Aware Backup Allocation For A Chain of Virtual Network Functions

D. Chemodanov, et al., A Near Optimal Reliable Composition Approach for Geo-Distributed Latency-Sensitive Service Chains



Why «all or nothing»?

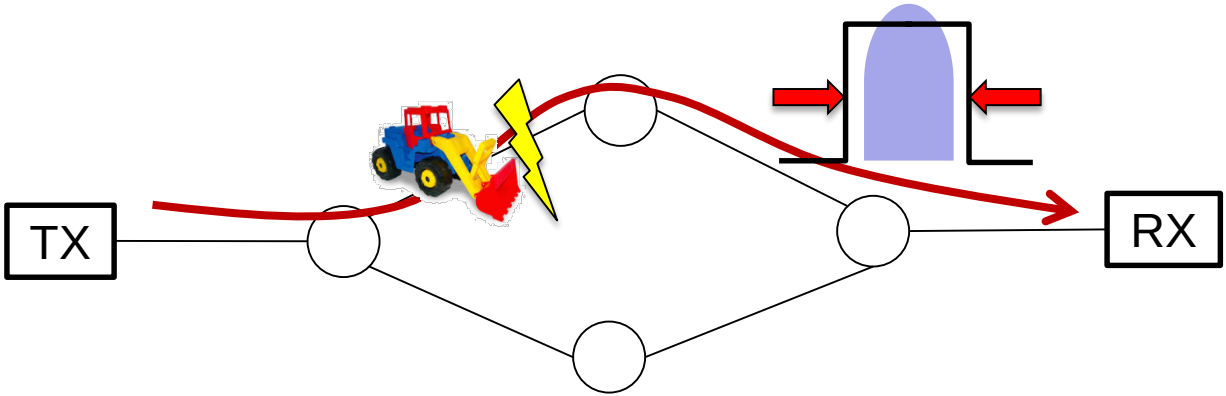
- Main research question: do we really need full (100%) replica/backup?
  - To catch an availability target, it could be enough partial protection

Outline

- Evolution of optical networks towards 5G
- Rising Topics
  1. **Resilient SDN control**
  2. **Content-connected slicing**
  3. **Reliable Service Chaining**
  4. **Machine Learning for failure mgmt**
- Conclusion and Future Directions

Two main failure types in optical networks

- Hard-failures
  - Sudden events, e.g., fiber cuts, power outages, etc.
  - Unpredictable (? Yvan!), require «protection» (*reactive procedures*)
- Soft-failures:
  - Gradual transmission degradation due to equipment malfunctioning, filter shrinking/misalignment…
  - Trigger early network reconfiguration (*proactive* procedures)



Handling soft-failures

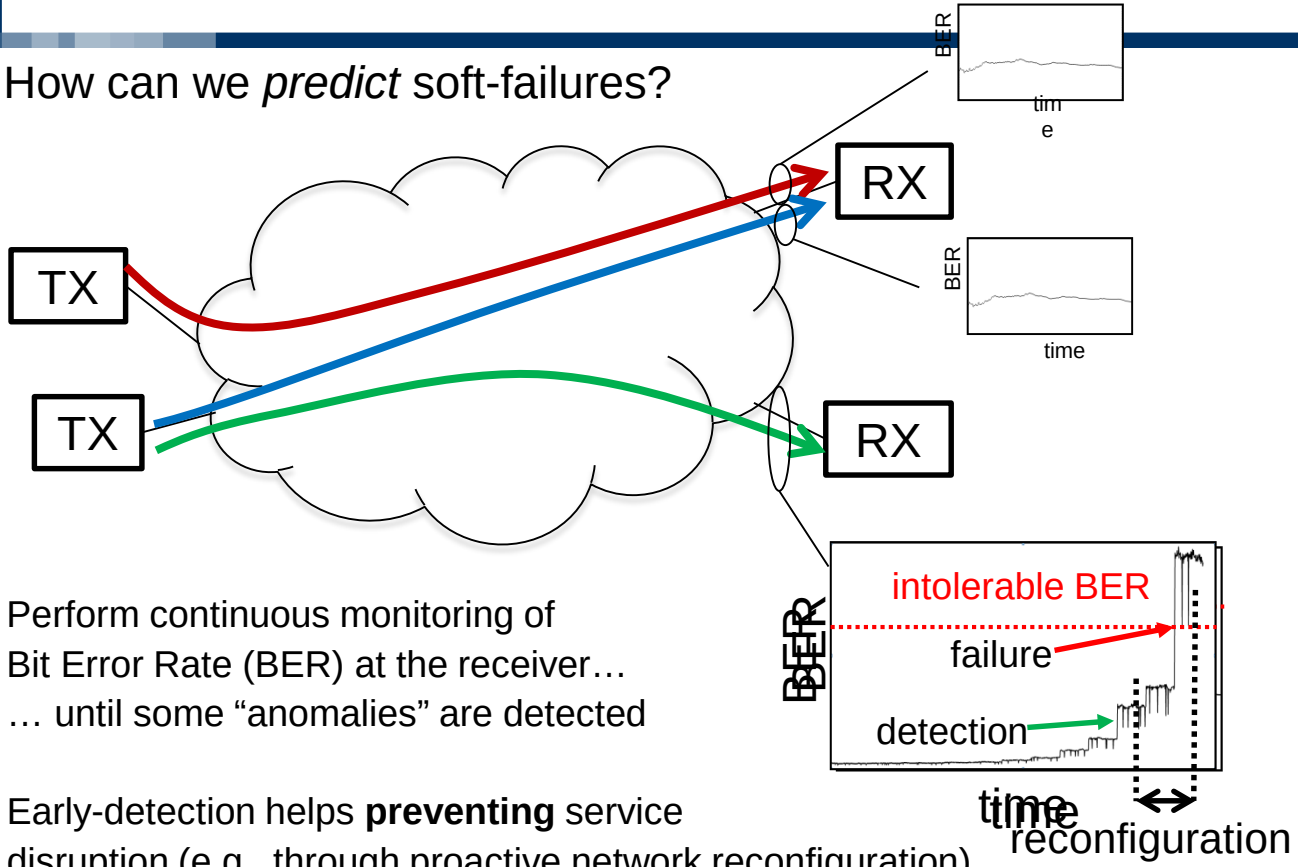
1. **Early detection** (When?)
   - «Predict» that BER will go above a threshold
   - Allows early/quick activation of proactive procedures

2. **Localization** of soft-failures (Where?)
   - e.g., which node/link along the path?

3. **Identification** (Which element?)
   - e.g., filter misalignment or amplifier malfunctioning o
   - Reduced Time To Repair (TTR)

Soft-failure *early detection*

- How can we *predict* soft-failures?



Perform continuous monitoring of
Bit Error Rate (BER) at the receiver…
… until some “anomalies” are detected

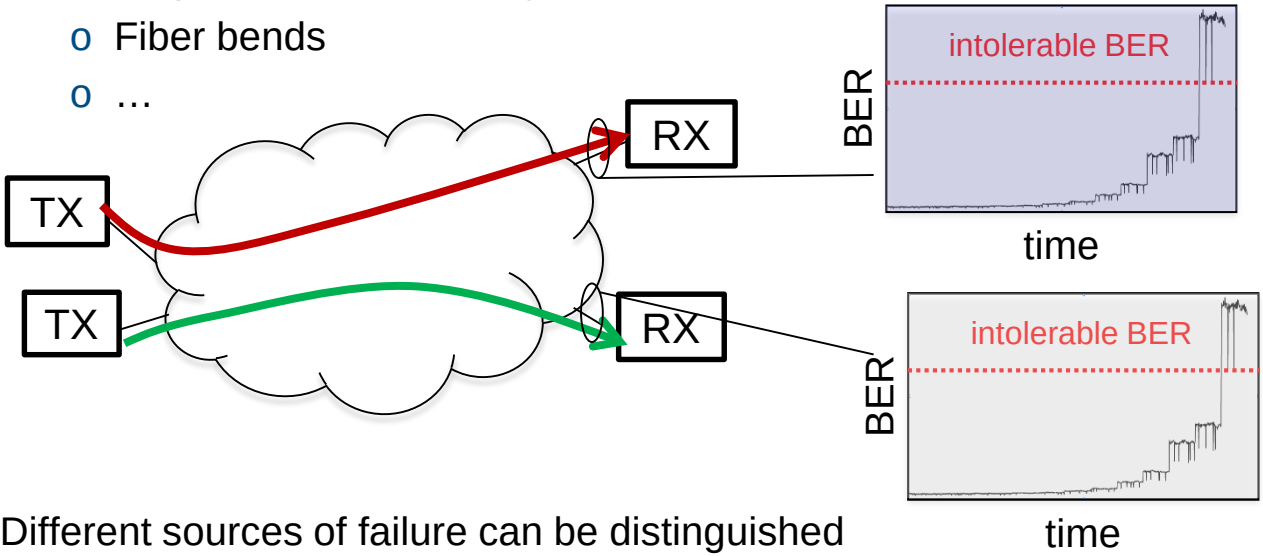
Early-detection helps **preventing** service disruption (e.g., through proactive network reconfiguration)

A. Vela *et al*., “BER degradation Detection and Failure Identification in Elastic Optical Networks”, in Journal of Lightwave Technology, vol. 35, no. 21, pp. 4595-4604, Nov.1, 1 2017

Soft-failure *identification*

Root cause analisis

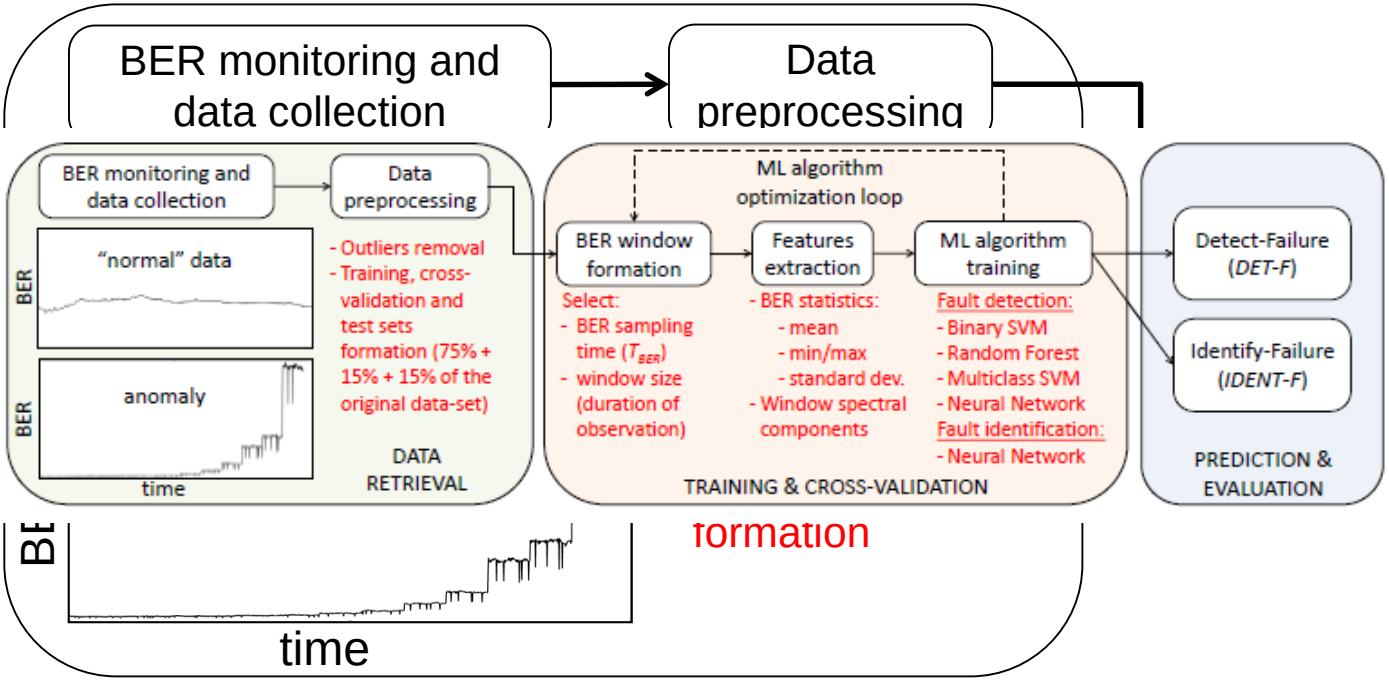
- How can we identify the *cause* of the failure?
  - Failures can be caused by different sources
    - Filters shrinking/misalignment
    - Amplifier malfunctioning
    - Fiber bends
    - …



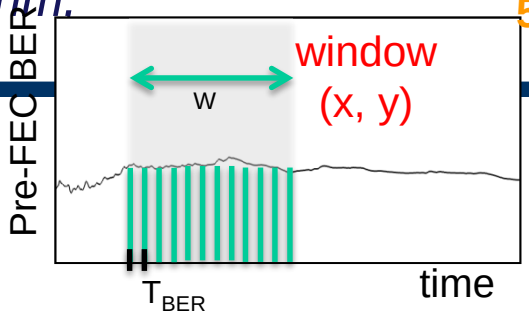
Different sources of failure can be distinguished via the different effects on BER (i.e., via different BER “features”)

S. Shahkarami, F. Musumeci, F. Cugini, M. Tornatore, Machine-Learning-Based Soft-Failure Detection and Identification in Optical Networks,"in Proceedings, OFC 2018, San Diego (CA), Usa, Mar. 11-15, 2017

1st Phase: *Data Retrieval*



2nd Phase: *Deciding ML algorithm. Training &Validation*



1. Data Retrieval

3 decisions

Validation (optimization of hyperparameters)

BER window → Features → ML algorithm

3. Prediction and Evaluation

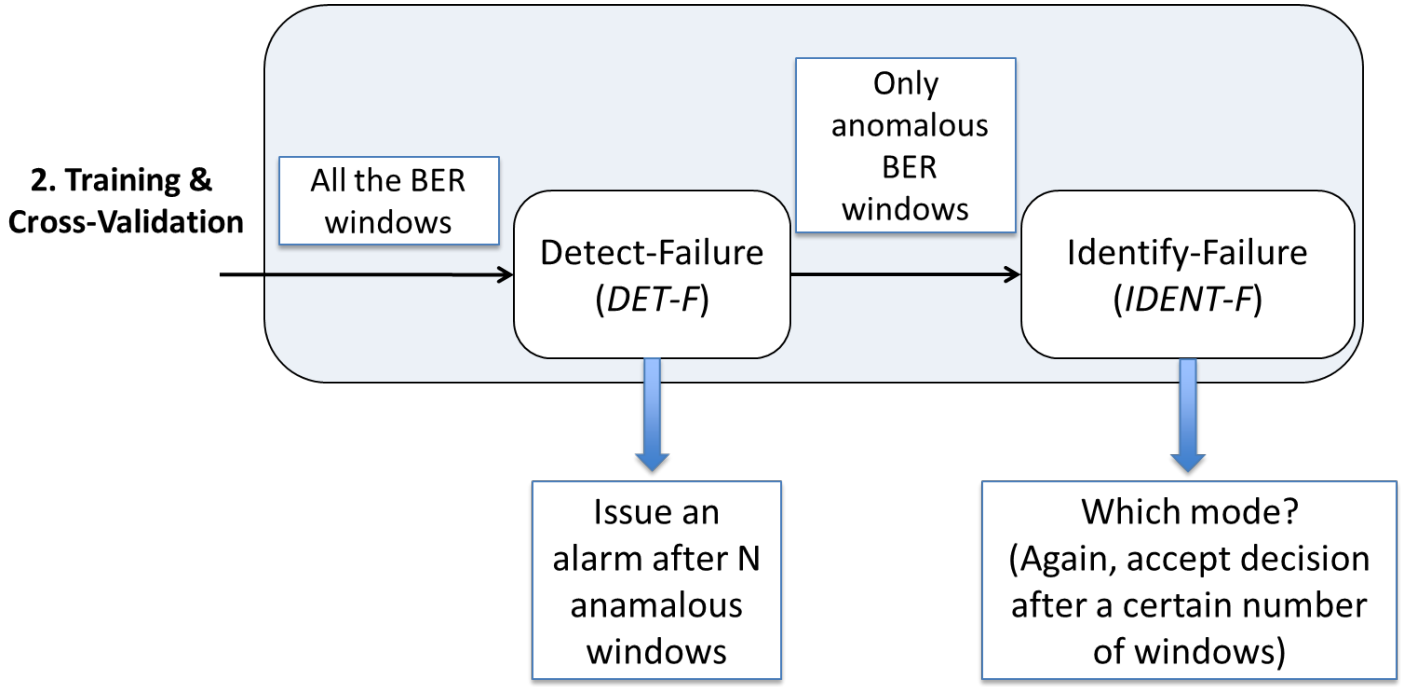
Select:
- BER sampling time (T_{BER})
- window size (duration of observation)

- BER statistics:
  - mean
  - min/max
  - standard dev.
- Window spectral components

Fault detection:
- Binary SVM
- Random Forest
- Multiclass SVM
- Neural Network

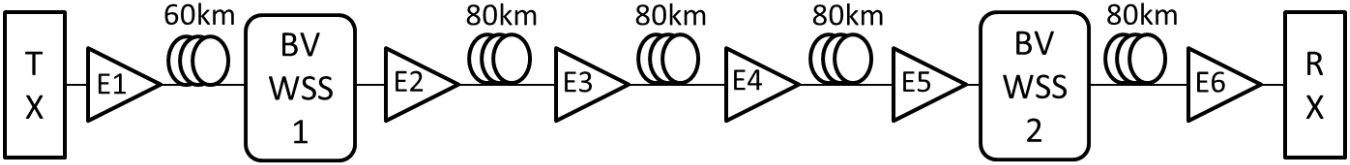
Fault identification:
- Neural Network

3rd Phase: *Detection and Identification*



Testbed setup

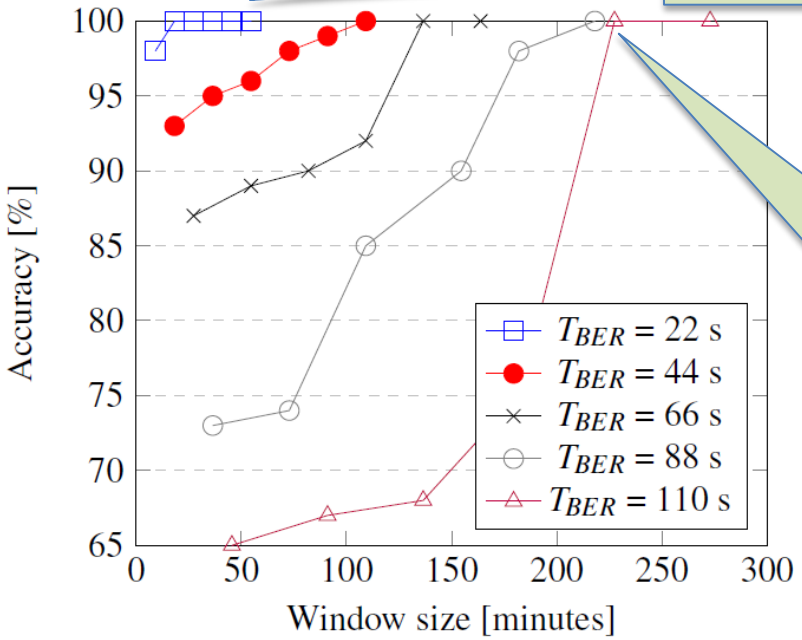
- Testbed for real BER traces
  - Ericsson 380 km transmission system
    - 24 hours BER monitoring
    - 3 seconds sampling interval
  - PM-QPSK modulation @ 100Gb/s
  - 6 Erbium Doped Fiber Amplifiers (EDFA) followed by Variable Optical Attenuators (VOAs)
  - Bandwidth-Variable Wavelength Selective Switch (BV-WSS) is used to emulate 2 types of BER degradation:
    - **Filter misalignment**
    - Additional attenuation in intermediate span (e.g., due to **EDFA gain-reduction**)



Numerical results: *Detection*
Accuracy vs window features

- Binary SVM

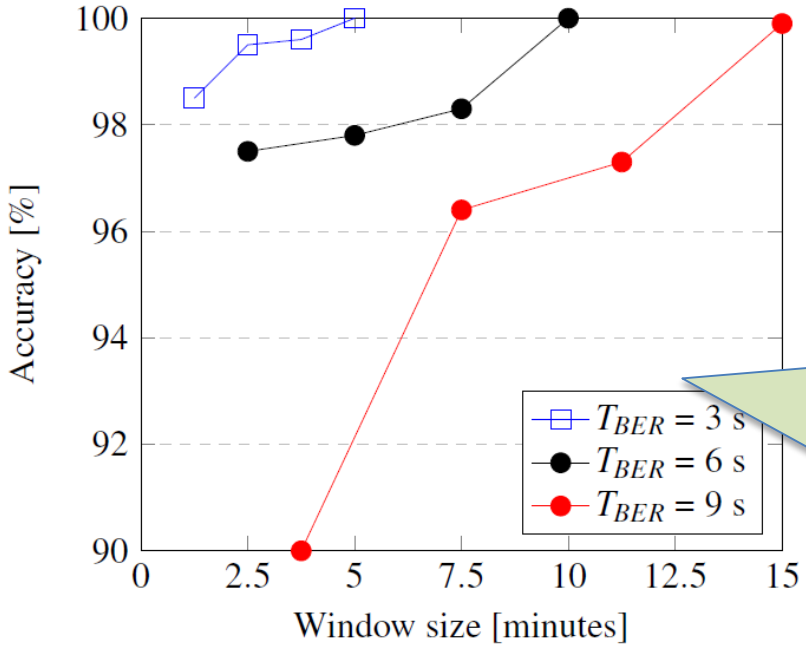
Take-away 1: Higher performance for with low sampling time
→ Fast monitoring equipment is required



Take-away 2: For increasing sampling time, longer "Windows" are needed for high accuracy

Numerical results: *Identification*
Accuracy vs window features

- Neural Network



Take-away 3: To perform failure-cause identification, much smaller sampling period is needed wrt failure detection

Lesson learned

- Automated soft-failure detection and identification
  - Can reduced Time To Repair (TTR)
    - Almost instantaneous troubleshooting
  - Successful identification of root cause of failures in a controlled scenario
    - Sampling BER each few seconds led to satisfactory accuracies
    - Identification is more complex than detection (to be confirmed..)

Thank You!

..and thanks to them!

POLITECNICO MILANO 1863

Achille Pattavina
Ali Hmaity
Francesco Musumeci

Biswanath Mukherjee
Farhan Habib
Sedef Savas
Sifat Ferdousi

H2020 Metro Haul

European Commission | Horizon 2020 European Union funding for Research & Innovation

National Science Foundation WHERE DISCOVERIES BEGIN

Disaster-Resiliency Strategies for Next-Generation Metro Optical Networks ATN: 1818972

cost EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

RECODIS
Resilient communication services protecting end-user applications from disaster-based failures