Minimizing the Impact of In-band Jamming Attacks in WDM Optical Networks

Konstantinos Manousakis and Georgios Ellinas

KIOS Research Center for Intelligent Systems and Networks
University of Cyprus

EUROPEAN UNION

REPUBLIC OF CYPRUS

ΔΙΑΡΘΡΩΤΙΚΑ ΤΑΜΕΙΑ
οι ιδέες μας, πράξη και ανάπτυξη

Research Promotion Foundation

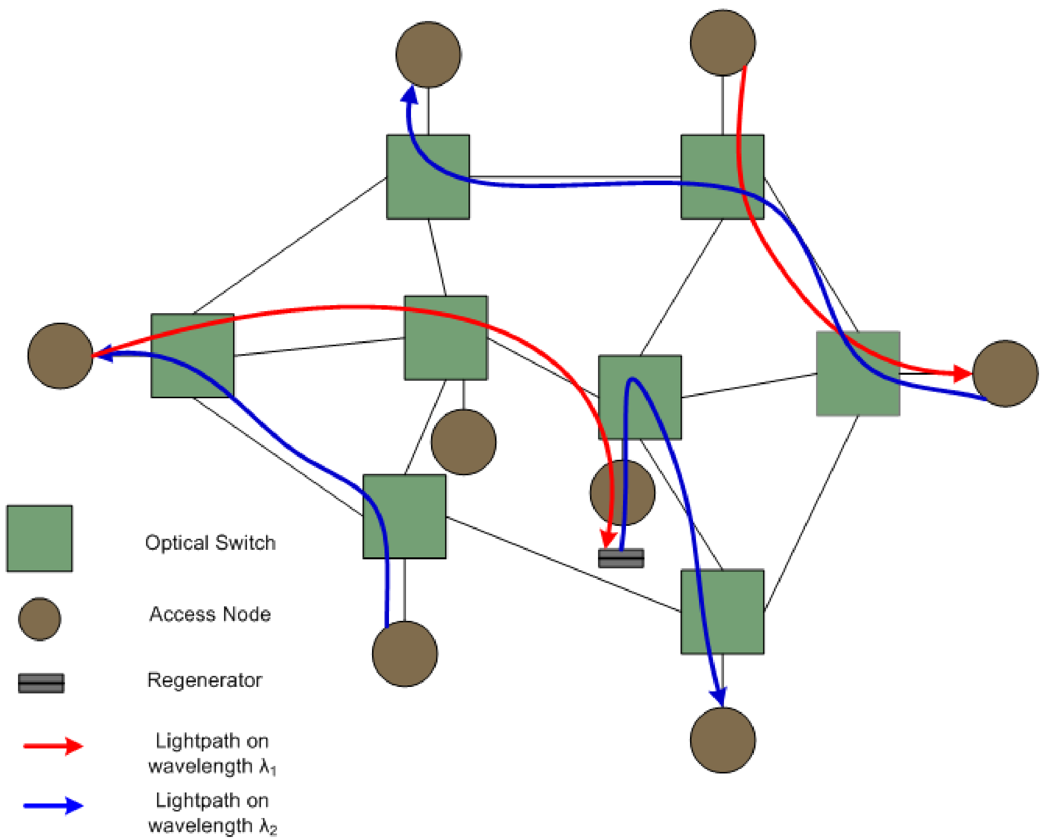
ΔΕΣΜΗ 2008

This work was supported by the Cyprus Research Promotion Foundation's Framework Programme for Research, Technological Development and Innovation (DESMI 2008), co-funded by the Republic of Cyprus and the European Regional Development Fund, and specifically under Grant Project New Infrastructure/Strategic/0308/26.

Outline

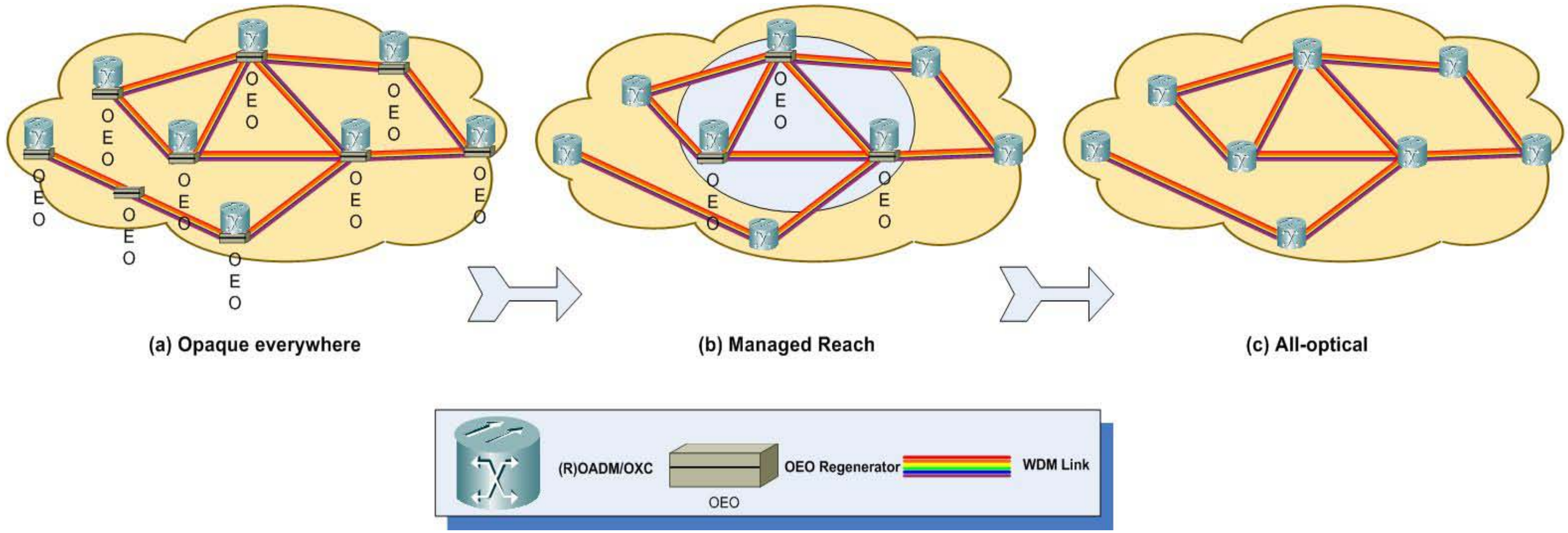
- Optical Networks
- Physical Layer Attacks
- Attack-Aware RWA in Transparent Networks
- Performance Results
- Conclusions
- Ongoing Work

WDM Optical Networks



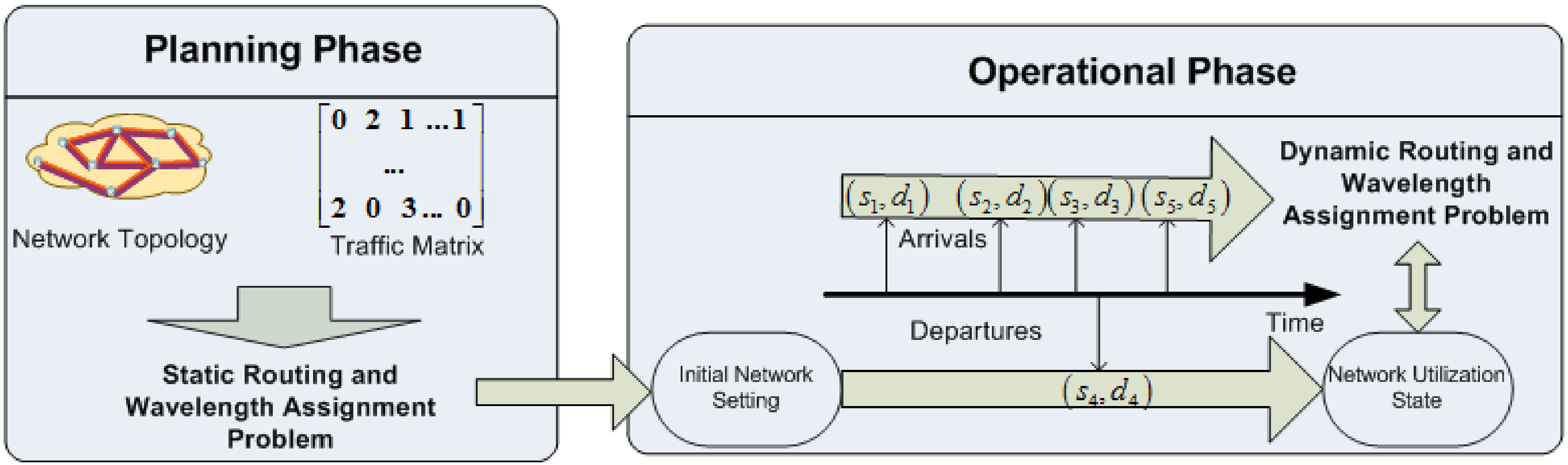
- Circuit switch
- Optical lightpath
- Distinct Wavelength Assignment
- Wavelength Continuity
- Routing and Wavelength Assignment (RWA)

Wavelength Routed Networks



- All-optical transparent networks: advantages in capacity, cost and energy
- Transparent networks: more vulnerable to physical layer attacks (PLAs)
- Difficult to detect-locate failures
- ☑ Attack aware – RWA algorithms

Planning and Operation of WDM Networks



- Implementation of WDM network
  - **Planning phase (offline – static RWA)**
  - Operational phase (online –dynamic RWA)

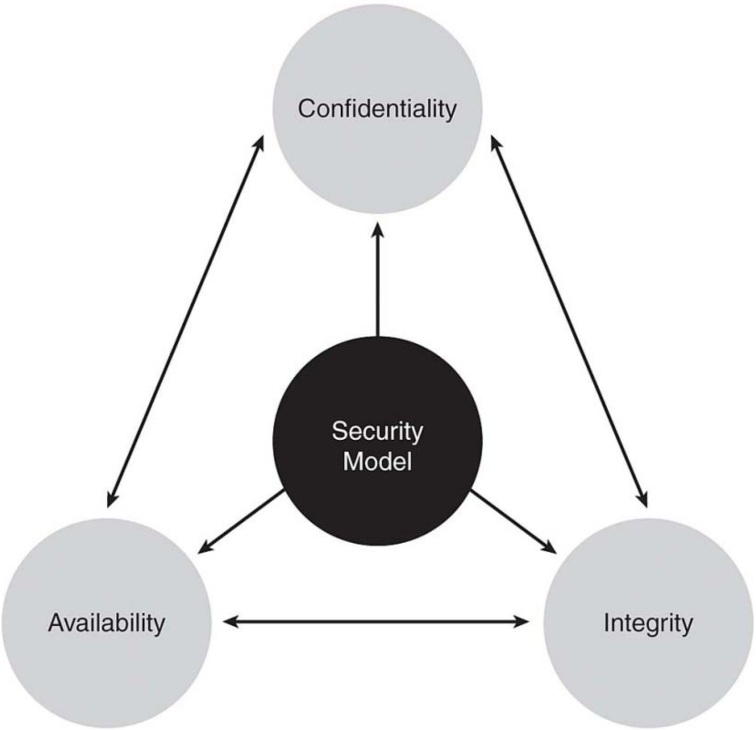
Attacks vs. Failures

- Attacks are much more hazardous than component failures and the damage they cause is much more difficult to prevent:
  - Attacks may spread to many users and many parts of the network, while a component failure affects only those connections passing through it.
  - Attacks are often designed in such a way as to appear sporadically and avoid detection, while a failure cannot do that.
  - Rerouting the traffic connections which use components which have failed is not effective in case of attacks, since the traffic itself is often used as the source of attacks.

Attack Classification

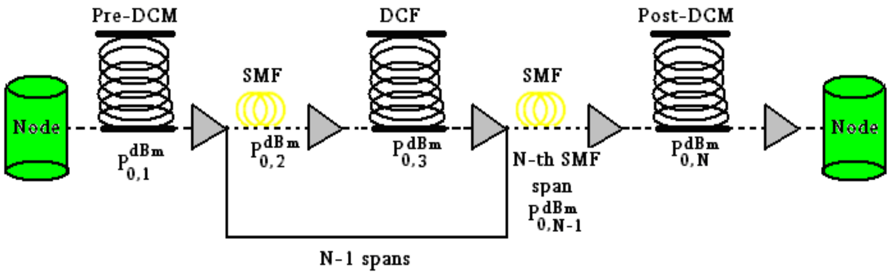
- Eavesdropping
  - Unauthorized users access to data
  - Encryption – Modulation techniques

- Service disruption
  - Prevents communication
  - Degrades the QoS
  - Intelligent Routing



Vulnerable Components

- Optical Fibers
  - Cut or bend the fiber
    - the light can be radiated into or out of the core
  - Fiber nonlinearities
    - Cross phase modulation



- Optical Amplifiers
  - Optical amplifiers are used to transparently amplify optical signals and restore their power to an acceptable level
  - Optical amplifiers are vulnerable to attacks even from remote locations
- OXCs

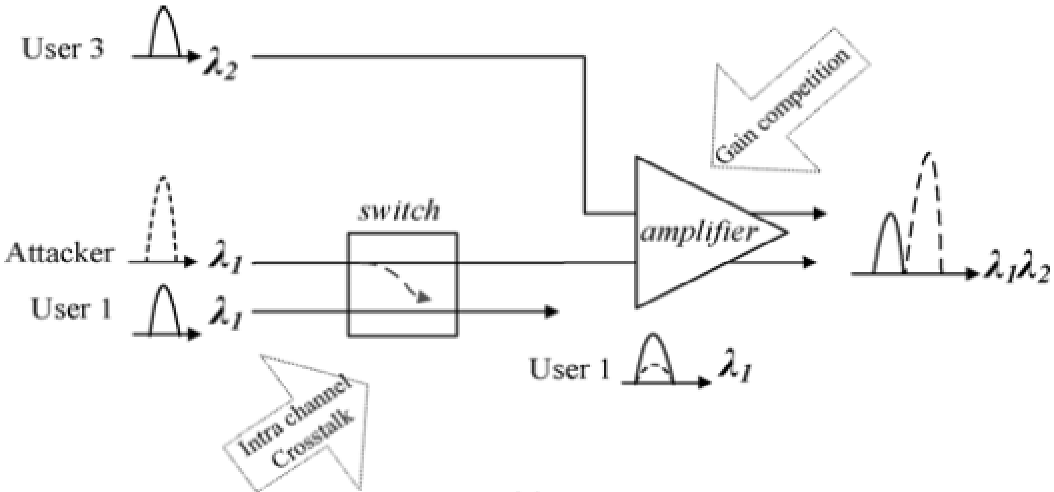
Fiber Optic Network – Data Vulnerability

- In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany.
- In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network
- International incidents include optical taps found on police networks in the Netherlands and Germany and on the networks of pharmaceutical giants in the U.K. and France.
- The required equipment has become relatively inexpensive and common place and an experienced hacker can easily pull off a successful attack.



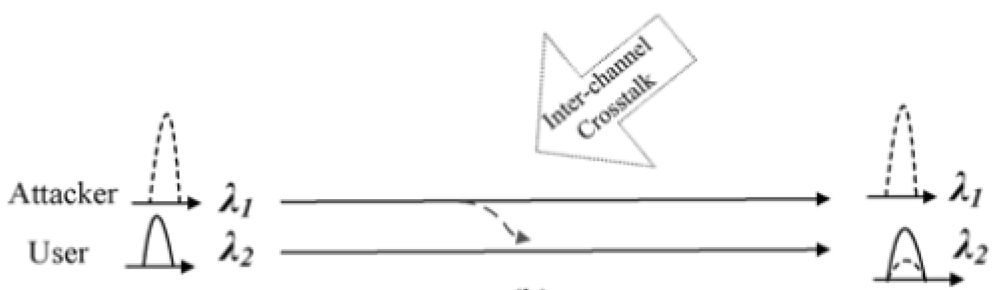
Physical Layer Attacks

- Gain Competition and in-band jamming



(a)

- Out-of-band Jamming



(b)

Objective

- Lightpath establishment
  - minimize the possible disruption caused by various attack scenarios, i.e., minimize the maximum number of lightpaths that can be disrupted in such situations.
- if fewer lightpaths are attacked
  - network service disruption reduced
  - failure detection and localization algorithms can be faster since they search for the source among fewer potential lightpaths.

PLA RWA - Problem Definition

- Input:
  - Network topology: connected graph $G=(V,E)$
    - V: set of nodes (**no** wavelength conversion)
    - E: set of point-to-point single-fiber links
  - Each fiber is able to support
    - a set $C=\{1,2,\ldots,W\}$ of W distinct wavelengths
  - A-priori known traffic scenario given in a matrix Λ of requested bandwidth
- Output: The RWA instance solution, in the form of routes, assigned wavelengths
- Objective: minimize the number of used wavelengths and select lightpaths with minimum in-band interactions

Variables

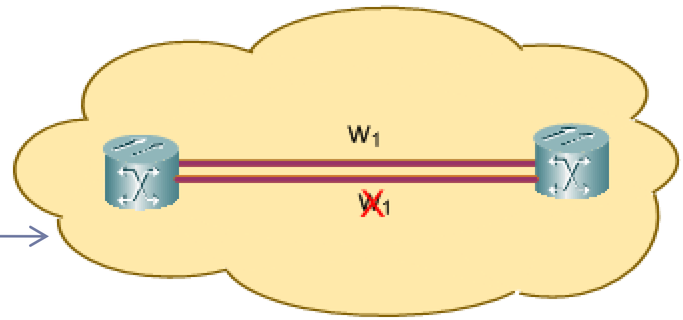
- $x_{p,w}$: a binary variable, equal to 1 if path *p* occupies wavelength *w*, and 0 otherwise
- W_l : the number of used wavelengths on link *l*
- S_p : the number of in-band lightpath interactions on path *p*, that is, the number of the different lightpaths that affect lightpath *p* through intra-channel crosstalk

ILP Formulation

minimize : $\sum_{l} W_l + m \cdot \sum_{p} S_p$

- Distinct wavelength assignment constraints,

$$\sum_{\{p|l\in p\}} x_{p,w} \le 1, \text{ for all } l \in E, \text{ for all } w \in C$$



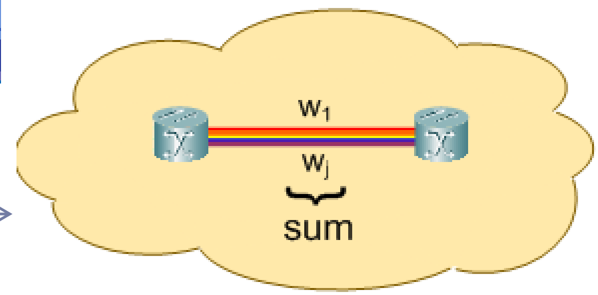
- Incoming traffic constraints,

$$\sum_{p\in P_{sd}} \sum_{w} x_{p,w} = \Lambda_{sd}, \text{ for all } s\text{-}d \text{ pairs}$$

$$\begin{bmatrix} 0 & 2 & 1 \ldots 1 \\ & \ldots & \\ 2 & 0 & 3 \ldots 0 \end{bmatrix}$$

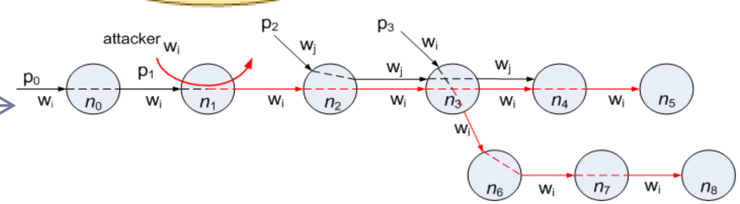
- Number of wavelengths per link

$$W_l = \sum_{p|l\in p} \sum_{w} x_{p,w}, \text{ for all } l \in C$$



- Jamming attack related to intra-channel crosstalk

$$\sum_{\{p'|p'\in P_{pp'}^{cn}\}} x_{p',w} + B \cdot x_{p,w} - S_p \le B, \text{ for all } p \in P \text{ and all } w \in C$$



Objective functions

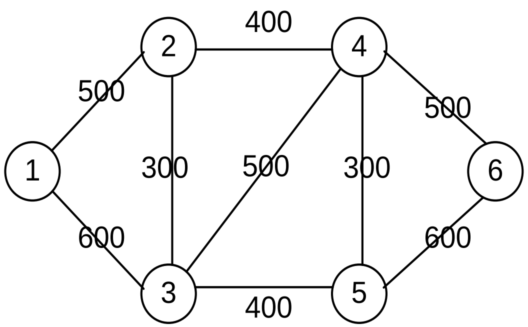
- **Minimize:** $\sum_{l} W_l + \sum_{p \in P} S_p$, where S_p defines the number of in-band crosstalk interactions of path p.
- **Minimize:** $\sum_{l} W_l + \sum_{p \in P} \sum_{w \in C} S_{pw}$, where S_{pw} defines the number of in-band crosstalk interactions of path p on a specific wavelength w.
- **Minimize:** $\sum_{l} W_l + S$, where S defines the maximum number of in-band crosstalk interactions over all paths.

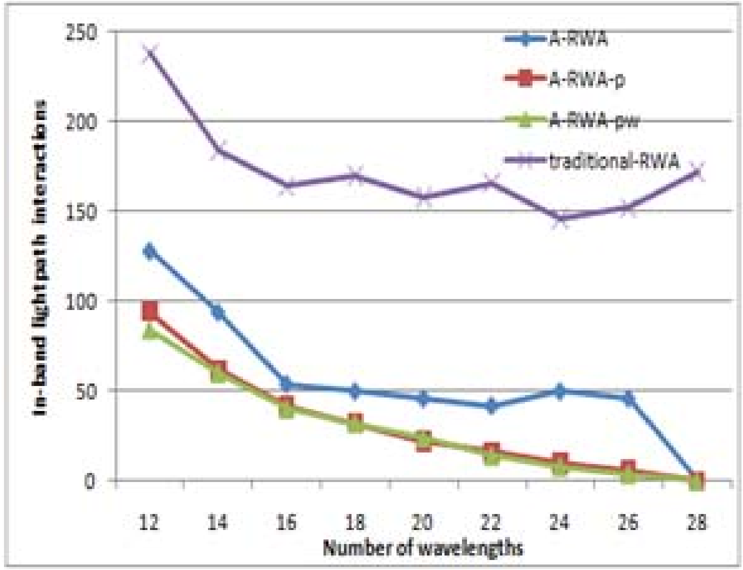
Handling non-integer solutions

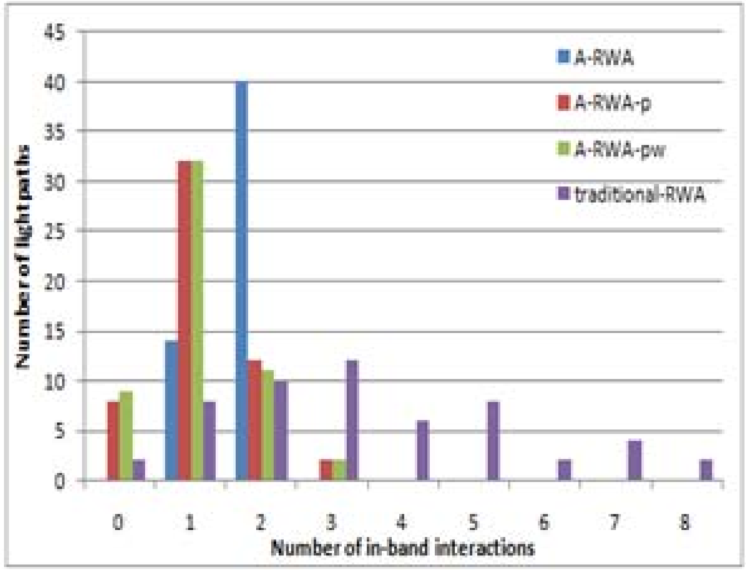
- Iterative fixings
  - Fix the integer variables of the solutions and solve the remaining (reduced) LP problem
  - The objective cost does not change → if we get to an integer solution it is optimal
  - When fixing does not further increase the integrality, we proceed to the rounding process
- Iterative rounding
  - Round a single variable, the one closest to 1, and continue solving the reduced LP problem
  - Rounding helps us move to a higher objective and search for an integer solution there
  - If the objective changes we are not sure anymore that we will find an optimal solution

Simulation Results

- Matlab, Gurobi
- Network load = 4.5
- W=14
- Time limit =3 hours





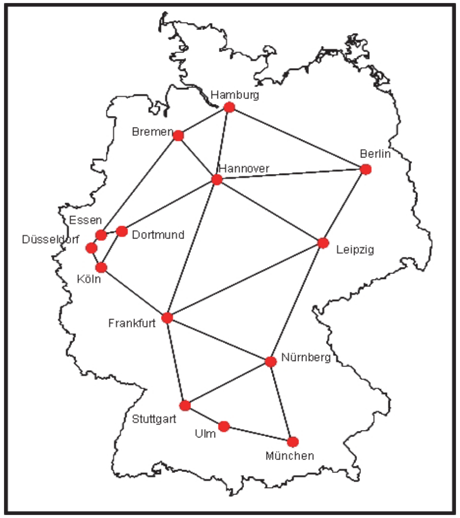


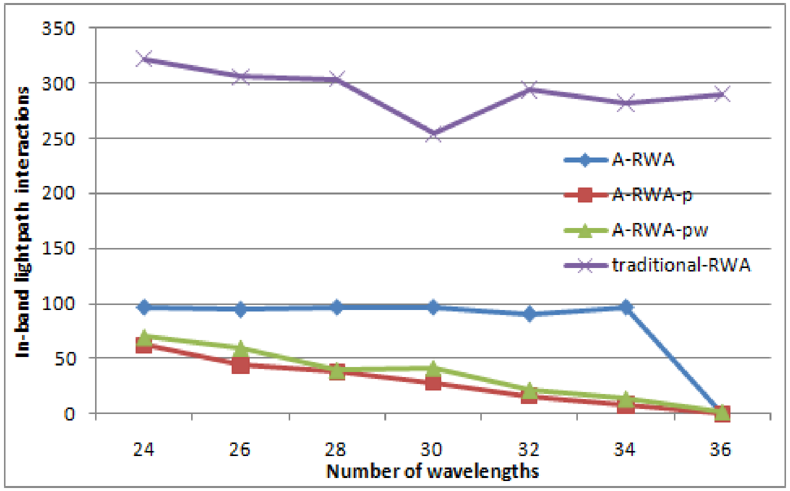
University of Cyprus

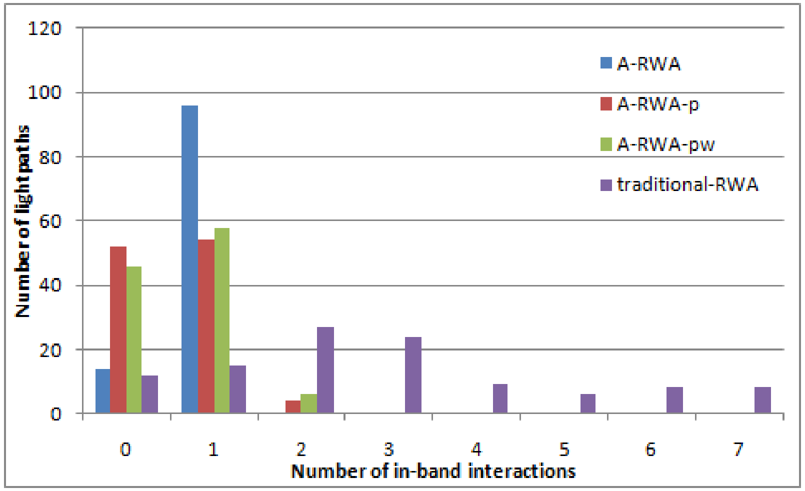
Center for Intelligent Systems & Networks

Simulation Results

- Matlab, Gurobi
- Network load = 0.6
- W=24
- Time limit =3 hours







University of Cyprus

Center for Intelligent Systems & Networks

Conclusions

- Transparent network design
- ILP formulations
- Minimize the propagation of high-power in-band crosstalk
- The proposed solution outperforms the traditional RWA algorithms
- Failure detection and localization algorithms can be faster since they search for the source among fewer potential lightpaths

Thank You!!!