Undergraduate Research Opportunity Program (UROP) Project Report KIOS Research and Innovation Center of Excellence

Michalis Piponidis

October 6, 2019

With the continuous growth of technology in everyday life (Smart Homes, Ultra High Definition video streaming, Cloud Services etc.), the networks that connect everything together are constantly being loaded more every day. So, to meet the increasing bandwidth requirements, network utilization efficiency must be increased as much as possible. Elastic Optical Networks (EONs) using Orthogonal Frequency-Division Multiplexing (OFDM) improve the efficiency a lot in comparison to the older Wavelength-division Multiplexing (WDM) networks. This however introduces the Routing and Spectrum Allocation (RSA) problem. For confidential and important connections, Security and Protection is needed. The purpose of Protection is to make sure that the signal gets to its destination, even in the event of a failure in the network. Security is implemented for confidential connections to reduce as much as possible the possibility of the signal being compromised.

In this project, we will implement and test the efficiency of different RSA methods for EONs and we will also implement and test Protection and Security algorithms. Finally, we will create a Graphical User Interface (GUI) Environment where these algorithms can be put to the test.

Elastic Optical Networks

Elastic Optical Networks (EONs) use Orthogonal Frequency-Division Multiplexing (OFDM) as a modulation technique to encode digital data on multiple carrier frequencies, where closely spaced orthogonal subcarrier signals with overlapping spectrum are emitted to carry data. This enables elastic bandwidth transmissions with a flexible grid where the subcarriers are low-data, allowing the use of many of them depending on the connection demands. In comparison, older Wavelength-Division Multiplexing (WDM) uses a fixed spacing grid where the subcarriers are much larger and doesn't allow the use of multiple subcarriers for a connection. This resulted in a lot of unused bandwidth from lower demand connections taking a whole subcarrier. For reference, usually OFDM subcarriers are 12.5GHz each whereas WDM ones are 50GHz each. OFDM however creates a new challenge with the added slots, the Routing and Spectrum Allocation problem.

For Example, in Figures 1 and 2 the same connections are implemented with WDM and OFDM, which shows the difference in spectrum efficiency.

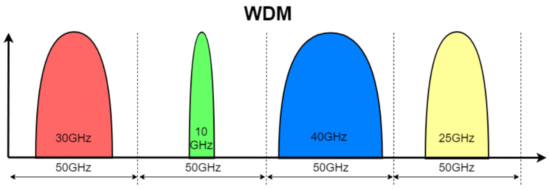


Figure 1: WDM Network with fixed grid.

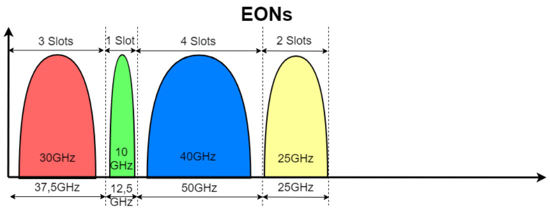


Figure 2: OFDM Network with flexible grid.

Routing and Spectrum Allocation

Routing and Spectrum Allocation (RSA) is about solving the problem of which path and slots are best for a specific new connection in the network. Since the problem is hard to solve simultaneously, in our work, we will divide the problem into two subcategories, namely the Routing and the Spectrum allocation subproblems. For the Routing part, we utilized two different metrics in order to select the candidate path: Path based on lowest Weight and Path based on lowest Hops. Weight represents the distance between two nodes and Hops represent the number of links the path uses. Dijkstra's algorithm is used to implement these two methods.

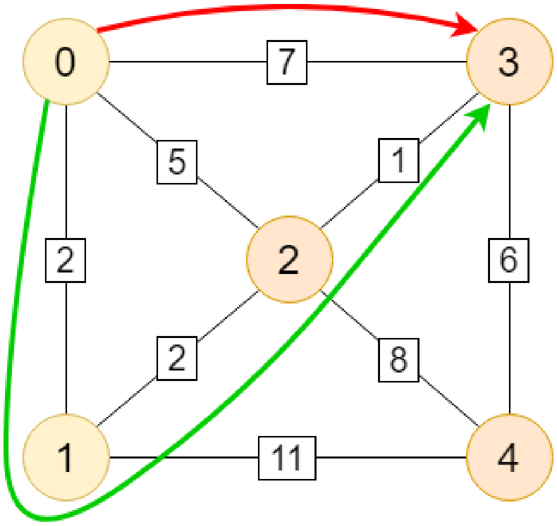
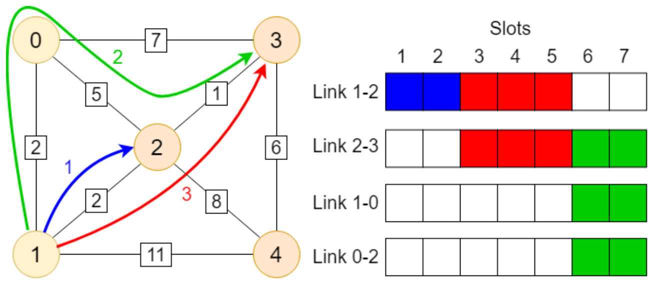


Figure 3: Routing Example

For example, for a connection from node 0 to 3 (Figure 3)

- Lowest Hops: 1 | Path: 0 → 3 (Weight: 7)
- Lowest Weight: 5 | Path: 0 → 1 → 2 → 3 (Hops: 3)

In the network, C-band is used which has 4THz spectrum. Each slot has 12.5GHz so each link has (4T/12.5G) 320 slots for each direction. Each connection uses the number of slots it needs for its required Bandwidth. Also, each connection must satisfy 3 constraints: *continuity*, *contiguity* and *non-overlapping*. (Figure 4)



	Slots						
	1	2	3	4	5	6	7
Link 1-2	🟦	🟦	🟥	🟥	🟥	□	□
Link 2-3	□	□	🟥	🟥	🟥	🟩	🟩
Link 1-0	□	□	□	□	□	🟩	🟩
Link 0-2	□	□	□	□	□	🟩	🟩

Figure 4: Constraints

- **Contiguity:** If multiple slots are used, they must be contiguous.
- **Continuity:** The same slots must be used in each link of the connection.
- **Non-overlapping:** Each slot can only be used by one connection at a time.

Slots are assigned with the First Fit method: The first slots found that satisfy the constraints are used.

Protection

There are important connections that cannot fall, even in the event of a failure. To solve this problem, we implement Protected connections. In Protected connections, the signal is sent through 2 different paths so that if a node or link fails, the signal will still reach its destination through the other path. In order to impellent Protection, 4 new methods of finding paths had to be used: Lowest Weight Node/Link Disjoint and Lowest Hops Node/Link Disjoint. They are found the same way as Lowest Weight/Hops, but this time a temporary graph is used where the Nodes/Links that the original path uses are removed.
Protected connections must also satisfy the 3 constraints and also both paths have to use the same slots.

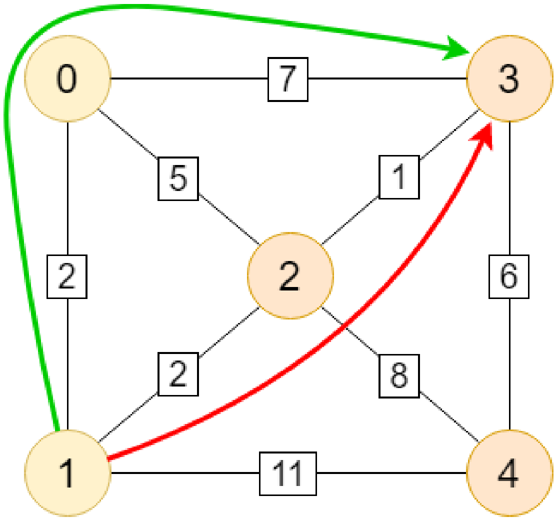


Figure 5: Protection Example

For example, for a Protected connection from node 1 to 3, 2 connections are made: (Figure 5)

- Lowest Weight: 3 | Path: 1 → 2 → 3
- Lowest Node Disjoint Weight: 9 | Path: 1 → 0 → 3

Security

Like Protected connections, there are connections that carry confidential data which need to be secured from possible invaders. Secured connections are XOR-ed with existing signals before being sent and are XOR-ed again when arrived at the destination with the same signals to reveal the original signal. A connection must satisfy two constraints to be able to secure a new connection:

1. It must have no common nodes or links with the new connection except the Source and Destination nodes.
2. It must have at least one common slot with the new connection.

Each link of the new connection can have different connections for security. The Level of Security for a connection is defined as the lowest number of connections that can be used for Security from every link.

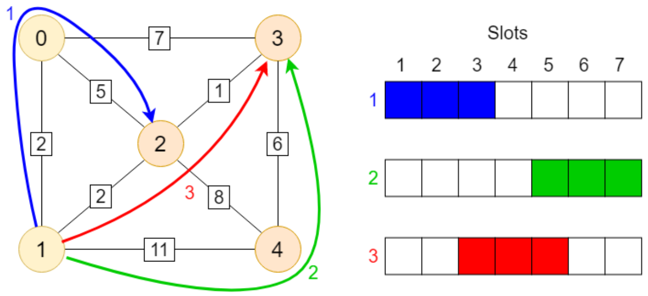


Figure 6: Security Example

For example: Connections 1 and 2 are already in the network and we want to add connection 3 as a Secured Connection. (Figure 6)
Path: 1 → 2 → 3
Link 1 → 2 can be secured by connections 1 and 2. Link Security Level: 2
Link 2 → 3 can be secured by connection 2. Link Security Level: 1
Connection 3 can be secured with Security Level 1.

For Security, Best Fit RSA is implemented based on best Security Level. For each Security Call being allocated, every Path and Starting Slot is checked and the one which gives the highest Security Level is selected.
To find the Security Calls and Level for a connection, every existing connection is checked for each link if it satisfies the two constraints. If it does, that call can be used for Security and the Security Level of that link is increased by 1.

Performance Evaluation

In order to test the efficiency of different Routing methods, the same call requests are allocated with the different methods and Spectrum Utilization (Slots Used) and Blocking Probability are recorded for each one. Slots used are the total slots used by all the connections in the network. A lower number of slots used for the same calls is better because it is using less resources of the network, being more efficient. Blocking Probability is the percentage of the calls that were blocked and couldn't be inserted in the network. A lower blocking probability is better because less calls are rejected from the network. For this test, 20 random sets of call requests (3000 calls each) with a step of 50 for each iteration are allocated with each method. Then, the average is calculated and plotted.

RSA

6 methods of allocations are used:

1. **Hops**: Calls allocated using only Lowest Hops path.
2. **Weight**: Calls allocated using only Lowest Weight path.

3. **Hops** → **Weight**: Calls allocated using Lowest Hops path. If Lowest Hops cannot be used, Lowest Weight is used.

4. **Weight** → **Hops**: Calls allocated using Lowest Weight path. If Lowest Weight cannot be used, Lowest Hops is used.

5. **Hops** → **Weight** → **Disjoint**: Calls allocated using Lowest Hops path. If Lowest Hops cannot be used, Lowest Weight is used. Then Lowest Weight Node Disjoint is used and then Lowest Hops Node Disjoint.

6. **Weight** → **Hops** → **Disjoint**: Calls allocated using Lowest Weight path. If Lowest Weight cannot be used, Lowest Hops is used. Then Lowest Weight Node Disjoint is used and then Lowest Hops Node Disjoint.

The results are shown in Figures 7 and 8.

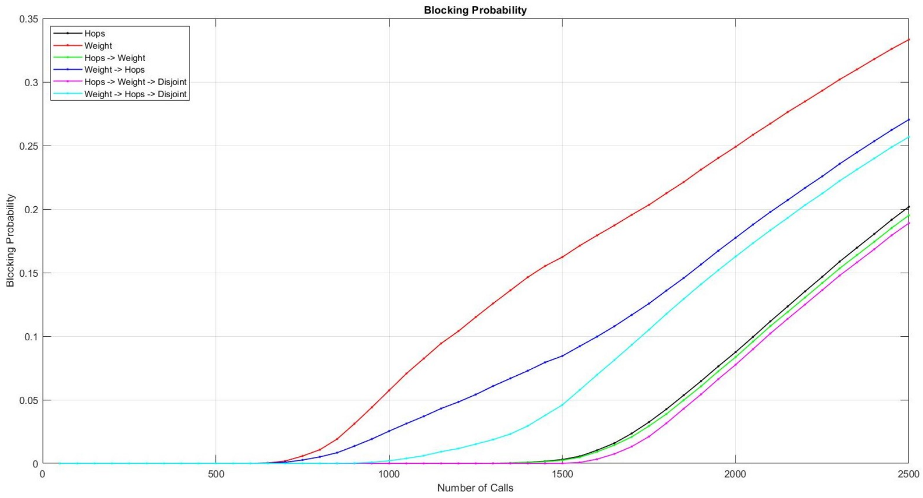


Figure 7: Blocking Probability for RSA

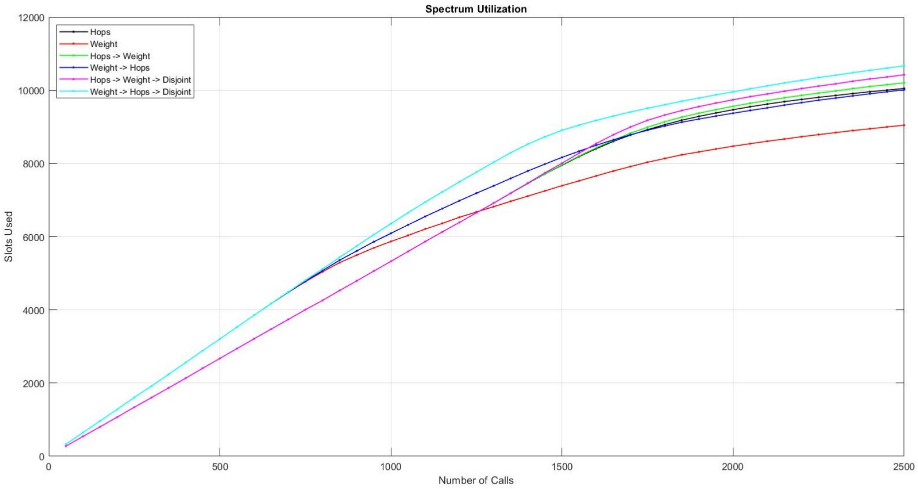


Figure 8: Spectrum Utilization for RSA

RSA with protection requirements

4 methods of allocations are used:

1. **Hops Protected (Nodes)**: Calls allocated using both Lowest Hops and Lowest Hops Node Disjoint paths.
2. **Weight Protected (Nodes)**: Calls allocated using both Lowest Weight and Lowest Weight Node Disjoint paths.
3. **Hops Protected (Links)**: Calls allocated using both Lowest Hops and Lowest Hops Link Disjoint paths.
4. **Weight Protected (Links)**: Calls allocated using both Lowest Weight and Lowest Weight Link Disjoint paths.

The results are shown in Figures 9 and 10.

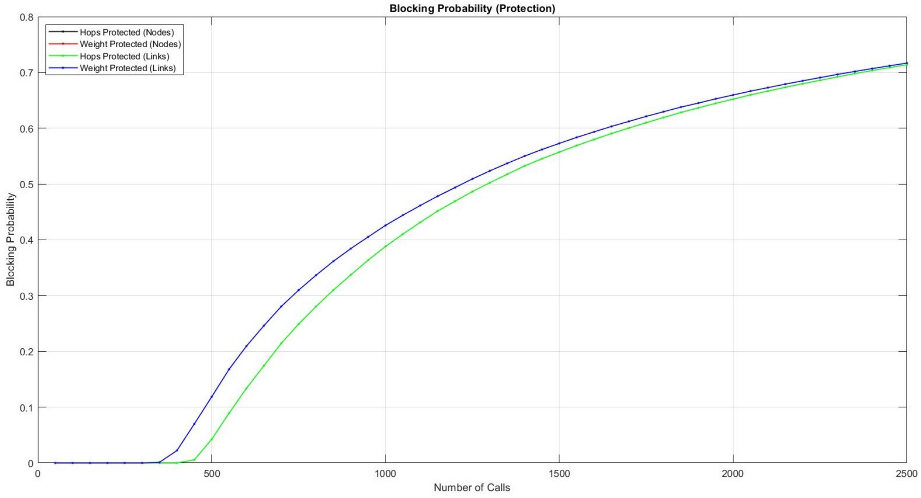


Figure 9: Blocking Probability for RSA with protection

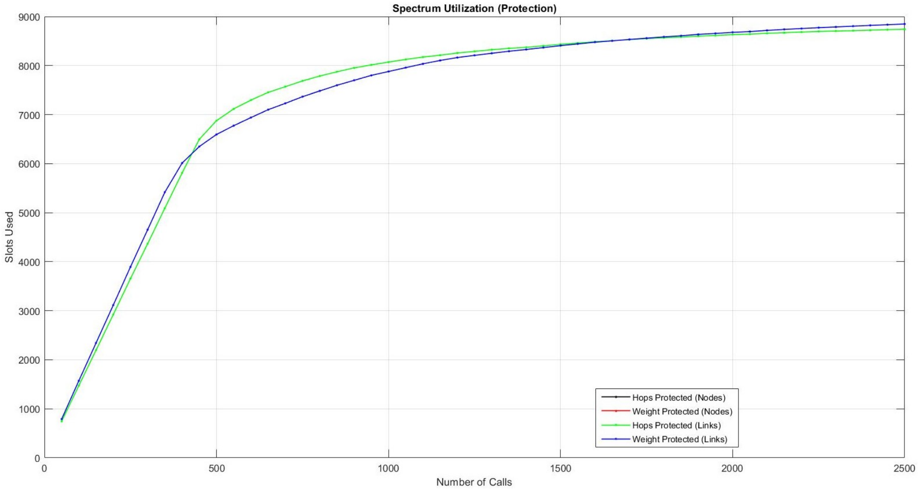


Figure 10: Spectrum Utilization for RSA with protection

Graphical User Interface

Using Matlab's App Designer a Graphical User Interface (GUI) environment was created. The Source (From) and Destination (To) Nodes can be given and the lowest path will be highlighted on the network based on Hops or Weight. Also, if a Protection option is selected, the Disjoint path will also be highlighted. This feature shows the six different Paths found.

For Security, the Call number can be given. The Security calls for each link of the call will be displayed and highlighted in order (each will be highlighted for 5 seconds). Also, the Security Level of the Call will be displayed.

Conclusions

1. In the routing part, the hop-based approach performs better than weight-based approach

2. Protection for all connections requires a lot of additional resources and increases dramatically the blocking probability

3. Security requires more resources than a typical RSA method due to the paths chosen in the routing process