Abstract—Quality of service requirements and the increasing amount of data transmission demand for efficient protection mechanisms. Existing mechanisms like 1+1 and 1:N path protection offer instantaneous recovery but they suffer from high capacity needs and nodal degree requirements, respectively. The high nodal degree requirement makes an implementation of the 1+N mechanism in transport networks difficult. In this paper, we develop two new mechanisms by applying network coding on a virtualized protection scheme. These mechanisms are more resource-efficient compared to 1+1, and are implementable in transport networks even under stringent nodal degree constraints. The difference between the two mechanisms lies in complexity and performance. Therefore, either of them can be preferred as a good compromise between 1+1 and 1+N in different scenarios according to the needs and available resources.

I. INTRODUCTION

The amount of data transmitted in transport networks is increasing day by day, which has a direct influence on the importance of the resilience mechanisms against node and link failures. Moreover, due to service level agreements (SLAs) and higher end-to-end quality of service (QoS) guarantees for services like real-time streaming multimedia applications such as voice over IP and IP-Television, fast recovery mechanisms are required. Today, an availability of 99.999% is often committed, which corresponds to a network downtime of less than 5 minutes annually [1]. Fiber cuts are an important reason for failures in optical networks [2]. Therefore, fast reacting and efficient recovery mechanisms are of high importance for transport networks.

In the literature, there are different path protection mechanisms. Path protection in general means that for a working path established between two end nodes, a protection path is reserved. This protection path uses an alternate path to connect these end nodes. Path protection mechanisms can be divided in two groups namely dedicated and shared. In dedicated protection, for each working path a protection path is assigned and reserved. In case of failure, this assigned resource is used. The 1+1 and 1:1 protection mechanisms are examples of dedicated protection [3]. In 1+1 protection, both the working and protection paths are used simultaneously in normal operation. Hence, the receiver can choose the path with better signal quality and in case of failure it can switch directly to the protection path. The 1+1 mechanism is shown in Fig. 1(a). The difference of the 1:1 mechanism is that the protection path is used to carry low priority traffic in normal operation. Only in case of failure the traffic is directed on this one.

On the other hand, in case of the shared backup path protection the backup capacity is shared by some working paths. One or more paths can be reserved for backup depending on the type of the mechanism, namely 1:N and M:N respectively. In case of failure, the traffic of the failed path is switched to one protection path. These mechanisms are a more general case of 1:1 mechanism.

Note that the 1+1 mechanism is providing instantaneous recovery due to the simultaneous data flow on both working and protection paths. This is not the case for the other above mentioned mechanisms. In these latter cases, first the failure has to be detected and signaled to the egress node so that this one can switch the traffic to the protection path. Due to the higher availability levels that 1+1 offers, it is preferred in cases where high resilience is required and it is a wide-spread protection mechanism, which is implemented in transport networks.

A drawback of the 1+1 mechanism is that it uses at least double of the capacity needed for the actual transmission. The 1+N mechanism suggested by Kamal [4] has a comparable survivability rate as 1+1 and it is using resources in the range of 1:N. In this mechanism, shown in Fig. 1(b), network coding [5] is applied on the protection path. Network coding is a concept, where the network nodes are not only forwarding but also processing the incoming data. In case of 1+N, at the sender node the information of the working paths is exclusive-ORed (XORed) and transmitted additionally over the protection path. The receiver decodes the incoming data by XORing the information on the working paths and taking the difference with the protection path information. In case of failure, this difference gives directly the missing data flow. Thus, this mechanism is also providing instantaneous recovery and it is much more efficient than 1+1. The drawback of this mechanism lies in the fact that in order to be able to decode the XORed data stream, all the incoming data streams have to arrive to the end node on link-disjoint paths. This means that if there are N working paths then a nodal degree of N+1 is needed in the end nodes. Considering that the average nodal degree in some example networks of Germany and Europe, namely Germany17 [6], Europe28 [7] and Germany50 [8], is
only around 3, 1+N mechanism faces implementation problems in transport networks.

In conclusion, there is a trade-off between nodal degree and efficiency. The mechanisms 1+1 and 1+N set the limits for lowest nodal degree and highest efficiency respectively. In this paper we are suggesting two new mechanisms, which operate close to 1+N from efficiency point of view and require much lower nodal degree. In the remaining of the paper, in Section II, the theoretical and practical aspects of the proposed mechanisms are explained. In Section III, the performance of the suggested mechanisms is analyzed and a comparison with the 1+1 and 1+N mechanisms is provided. Finally, the paper is concluded with the summary and future work.

II. THEORETICAL FRAMEWORK OF THE SUGGESTED MECHANISMS

In this section two new protection mechanisms will be explained, which differ in complexity, capacity, and nodal degree requirements. As stated before, 1+N and 1+1 protection mechanisms are taken as the extreme alternatives. The aim is to find efficient mechanisms, which are applicable to transport networks considering nodal degree constraints.

The key point of the new mechanisms is the combination of network virtualization with network coding. In virtualized networks, the protection can be implemented either in the physical or in the optical layer. In [9] some examples of both options are presented and a comparison is provided. In our case we provide protection in the virtual layer and due to the network coding gain, we achieve better performance than 1+1 and pure virtual layer protection. Our idea is providing protection against multiple link or node failures in the virtual domain. Afterwards, the virtual paths are mapped onto the physical paths in order to provide protection against single physical link or node failures like 1+1 and 1+N. The scheme can be extended to other failure patterns in the physical domain as well, but we concentrate on single failures here, which are the most important failure types in transport networks. Protection of N data streams against a certain number F of link or node failures in the virtual domain corresponds to a mapping, where F virtual paths are chosen arbitrarily and assigned to a physical path. In other words, each physical link can be shared by a maximum number of F different data streams. An example of the mapping between virtual and physical domains is shown in Fig. 2. In this example, F is chosen to be 2. Protection is realized using P additional virtual protection paths. Note that P depends on N and F. The detailed relation will be shown for each mechanism in the next section. The total N+P virtual paths are then mapped onto the physical domain, where any random pair of data streams is chosen and assigned to a physical path. Note that in the figure a specific example of the mapping is shown but it can be done in any random way. Now, the question is how to determine the protection path information and the number of the protection paths P.

A. 1st mechanism: Pure XORing

In the first mechanism only simple XORing is applied on the data streams to form the protection path information, for the sake of keeping the complexity low. The XOR function can be easily implemented in today's systems in hardware and it is principally even realizable in the all-optical domain.

To determine the necessary number of protection paths P, there is a simple rule. Protecting N data streams against F virtual link failures by using P protection paths means that when any x, with x ≤ F, of the total N+P paths fail, with the remaining N+P-x data streams, all the information should be uniquely decodable. Hence, the XORed information is generated in such a way that the remaining minimum N+P-F equations build a matrix with the rank N, in case of x=F virtual failures. The dimension of the matrix, nx(N+P), is given by the number of the data streams N and total number of the virtual paths.

Moreover, it should be ensured that each variable (each original data stream) shows up at least F+1 times in the matrix. This condition guarantees the decoding of this data stream uniquely, because even after F virtual link failures, there will be at least one equation containing this variable, i.e., there will be at least one remaining path transmitting the necessary information about this data stream. This path can be either the working path for this data stream or one of the protection paths. Thus, given F virtual link failures, to satisfy the given conditions the following inequality should hold:

$$2^P - \sum_{i=0}^{F-1} \binom{P}{i} = \sum_{i=F}^{P} \binom{P}{i} \geq N \text{ with } P \geq F \geq 2 \quad (1)$$

Equation (1) states that the number of valid assignments of P protection equations to N variables should be at least equal to N, where the protection level is given as protection against F virtual failures. In this case, there are a total number of 2^P combinations of P equations, which can be assigned to the variables. The invalid assignments, namely where less than F equations are assigned to a variable, or in other words, where a variable shows up in less than F equations, have to be eliminated. At the end, there should be at least N valid assignment possibilities since there are N variables. For example, if we have N=4 original data streams and want to have protection against F=2 virtual link failures, we have to use at least P=3 protection paths. For the case of F=1, 1+N mechanism should be applied, namely P should be 1. Note that for a certain value of F, increasing N increases also P because of the fact that the number of the unique assignments depends on P.

The number of the physical paths np after mapping can be determined as in (2).
\[ np = \left\lfloor \frac{N + P}{F} \right\rfloor \]  

(2)

Note that an XORed data stream \( S_j \) is defined as given in (3), where the sum stands for the XORing function and \( S_j \) is an original data stream. Depending on \( S_j \) being part of the XORed stream \( S \) or not, the coefficient \( a_{i,j} \) is either 1 or 0, respectively.

\[ S_j = \sum_{k} \alpha_{k,j} S_k \text{ with } \alpha_{k,j} \in \{0,1\} \]  

(3)

In this case the total required capacity \( C_i \) for this mechanism can be calculated as follows:

\[ C_i = \sum_{j=1}^{N} R_j + \sum_{j=1}^{P} R_j \text{ where } R_j = \max_{k,j \in M_j} (R_k, R_j) \]  

(4)

where \( R_i \) denotes the packet length of the stream \( S_i \). For each protection path stream \( S_j \), the maximum packet length of the streams participating in the XORing determines the overall packet length \( R_j \) of this protection stream. Note that in cases where the packet lengths of all different demands have the same value \( R \), then equation (4) simplifies to the following:

\[ C_{i,eq} = (N + P) \times R \]  

(5)

These equations apply also when TDM is used for different and equal bitrates of the data streams, respectively.

B. 2nd Mechanism: Higher complexity, higher efficiency

In the second method, the motivation is to further decrease the required nodal degree and the capacity usage. For this purpose, instead of using only simple XORing function, the weighted sum of the data streams will be used in protection information. In this case, the number of the needed protection paths \( P \) is equal to \( F \). This is reached by using some weighting coefficients, which enables all equations to be independent. Without using the coefficients, this independence cannot be reached and more and shorter equations are required, which was the case in the first mechanism. Hence, by choosing the weighting coefficients appropriately, the decoding matrix becomes full-rank and all the information streams can be decoded uniquely. The next questions to answer are, how and from which field to choose the coefficients and how much effect it has on the capacity requirement.

Note that if arithmetic operations are done in the field of real numbers, there is no guarantee for the packet size or the bit rate to remain unchanged. In the operations like addition or multiplication, there might be some carry bits, which cause fluctuation in the packet size. In cases, where the capacity of the transmission link is constant, this would create some problems. Therefore, finite field arithmetic has to be applied.

In our mechanism we use Galois Field \( GF(2^m) \). In general, a Galois field \( GF(p) \) is a finite field with \( p \) elements, where \( p \) is a prime number or a power of a prime number. It is defined simply as the ring of integers modulo \( p \). Therefore, the arithmetic operations, like addition, subtraction, multiplication, can be performed using the usual operation on integers, followed by reduction modulo \( p \) [10].

Moreover, data transmission in a transport network is realized on the binary level. Therefore, it is convenient to choose \( p \) as a power of 2, namely the Galois Field \( GF(2^n) \). By determining \( m \), there are two factors. On the one hand, the complexity of the system increases with the logarithm of the field size, which is \( m \), because the arithmetic operations are performed on code words of length \( m \) [11]. On the other hand, by choosing \( m \) large enough, it is ensured that a full-rank coefficient matrix exists [12].

In our mechanism, the field size should be at least equal to the number of the virtual paths because for each virtual path a new codeword is needed, which is different than the code words on the other paths. This rule ensures the decoding of the necessary information at the receiver side. Keeping in mind that it should be in the form of \( 2^n \), the rule can be summarized as in the following formula:

\[ 2^n \leq N + F, \]  

(6)

where \( N \) is the number of the working paths, which are protected against \( F \) virtual link or node failures. In this case, the codeword size will be \( m \)-bits. In scenarios, where the packet size is equal to the codeword size, the processing is straightforward. If the packet size is larger than \( m \), the packets can be chopped into \( m \)-bits long pieces and processed in this way. If the packets are shorter, they can be combined to be processed together. In general, while determining the optimum field size, the packet size should be considered.

For the second mechanism the required number of the physical paths \( np \) is given as follows:

\[ np = \left\lfloor \frac{N + F}{F} \right\rfloor \]  

(7)

The total required capacity \( C_2 \) for the second mechanism can be calculated as follows:

\[ C_2 = \sum_{j=1}^{N} R_j \text{ where } R_j = \max_{k,j \in M_j} (R_k, R_j) \]  

(8)

where \( R_i \) is the maximum packet length on the \( i^{th} \) virtual path. Note that in this case for all the virtual paths weighted XORing function is applied. Alike the 1st mechanism, in cases where the packet lengths of different demands have the same value \( R \), (8) simplifies to the following:

\[ C_{i,eq} = (N + F) \times R \]  

(9)

Comparing (4) and (8) or (5) and (9), it is seen that the second mechanism performs better than the first one since \( F \) is smaller than or equal to \( P \). Similarly, comparison of (2) and (7) shows that also the needed nodal degree of the second mechanism is mostly lower and in the worst case equal to the first mechanism.

III. PERFORMANCE COMPARISON OF THE NEW MECHANISMS

In this section, we will analyze the performance of the new mechanisms and provide a comparison with the existing mechanisms. As mentioned before, 1+1 mechanism uses at
least double the capacity needed for the data transmission but on the other hand it requires a nodal degree of 2 only. 1+N uses much lower capacity but requires a nodal degree of N+1, depending on the number of the data streams N. Therefore, these two mechanisms are determining the limits of the trade-off, namely of the capacity usage and nodal degree requirement.

The suggested mechanisms decrease the required nodal degree compared to 1+N mechanism and perform better than 1+1 mechanism from the capacity point of view. Hence, they can be considered as a compromise between these two methods.

For the analysis it is assumed that there is a demand pair with a varying number of demands. These demands are mapped on the working paths established between the end-nodes and they should be protected against any single link or node failure in the physical domain. For illustration, the transmission is assumed to be packet-based and each demand has the same packet size.

In the performance analysis of the suggested mechanisms, the number of the demands is varied and the exact demand values, where the required nodal degree is changing, are determined. For these demand values, the used capacity value is calculated using (4) and (8) respectively. The calculations are generally applicable to all networks and are performed using MATLAB. These capacity values are compared with the capacity requirement of the 1+1 mechanism. The capacity gain of the proposed mechanisms is shown in percentage form. Note that in this analysis, the used capacity is given as capacity per path, which does not necessarily correspond to the capacity requirement in the actual network. The capacity requirement for the network would depend strongly on the network topology, i.e. on the physical properties of the available paths between the demand pair.

Additionally, for each case the nodal degree requirement of 1+N mechanism is compared with the obtained nodal degree from the proposed mechanisms. Moreover, in the analysis, the protection level $F$ in the virtual domain is also varied in order to investigate the effect of the choice of this level. These levels are shown in the first column of the Tables I and II. For the same number of demands, increasing $F$ reduces the nodal degree requirement but also the capacity gain. Therefore, by the implementation of the mechanism it should be adjusted depending on the minimum nodal degree in the network. For the nodal degree analysis only the nodes that originate and terminate the traffic are considered. Note that, in general, it is better to keep $F$ as low as possible.

Note that in Table II only the values, where the second mechanism requires a nodal degree of 3, are shown, which is the average nodal degree of some example networks for Germany and Europe mentioned in the introduction. In Table I, the obtained capacity gain and nodal degree values for the same demand values as in Table II are given in order to provide a comparison between the two mechanisms. The results in Tables I and II show that the second mechanism performs better than the first one regarding the capacity gain and nodal degree values. This is because of the fact that fewer protection paths are required for the second mechanism. Note that for both mechanisms, only the situations, where the number of the demands $N$ is higher than or equal to $F$, are considered. Note that for a certain nodal degree, the first mechanism results in different capacity gain values for each $F$. Decreasing $F$ for a certain number of demands increases the obtained capacity.

### Table I: Performance Results of the 1st Mechanism

<table>
<thead>
<tr>
<th>$F$</th>
<th># Demands</th>
<th>Nodal degree</th>
<th>Capacity gain relative to 1+1</th>
<th>Nodal degree for 1+N</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>100</td>
<td>4</td>
<td>24%</td>
<td>101</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>4</td>
<td>20%</td>
<td>61</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>4</td>
<td>20%</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>4</td>
<td>15%</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
<td>13%</td>
<td>5</td>
</tr>
</tbody>
</table>

### Table II: Performance Results of the 2nd Mechanism

<table>
<thead>
<tr>
<th>$F$</th>
<th># Demands</th>
<th>Nodal degree</th>
<th>Capacity gain relative to 1+1</th>
<th>Nodal degree for 1+N</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>100</td>
<td>3</td>
<td>25%</td>
<td>101</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>3</td>
<td>25%</td>
<td>61</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>3</td>
<td>25%</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>3</td>
<td>25%</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>25%</td>
<td>5</td>
</tr>
</tbody>
</table>

Figure 3: Capacity comparison of the second mechanism with 1+1 and 1+N

Figure 4: Required nodal degree comparison of the second mechanism with 1+1 and 1+N

TABLE I

**PERFORMANCE RESULTS OF THE 1ST MECHANISM**

<table>
<thead>
<tr>
<th>$F$</th>
<th># Demands</th>
<th>Nodal degree</th>
<th>Capacity gain relative to 1+1</th>
<th>Nodal degree for 1+N</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>100</td>
<td>4</td>
<td>24%</td>
<td>101</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>4</td>
<td>20%</td>
<td>61</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>4</td>
<td>20%</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>4</td>
<td>15%</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
<td>13%</td>
<td>5</td>
</tr>
</tbody>
</table>

TABLE II

**PERFORMANCE RESULTS OF THE 2ND MECHANISM**

<table>
<thead>
<tr>
<th>$F$</th>
<th># Demands</th>
<th>Nodal degree</th>
<th>Capacity gain relative to 1+1</th>
<th>Nodal degree for 1+N</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>100</td>
<td>3</td>
<td>25%</td>
<td>101</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>3</td>
<td>25%</td>
<td>61</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>3</td>
<td>25%</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>3</td>
<td>25%</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>25%</td>
<td>5</td>
</tr>
</tbody>
</table>
gain but also the required nodal degree. On the other hand, for the second mechanism independent of the value of $F$, for a certain nodal degree $np$ the capacity gain remains constant when the equation $npN/F$ is satisfied. Still, increasing the minimum nodal degree increases the capacity gain. For the nodal degree 3, which is a realistic nodal degree assumption for the transport networks, 25% gain is obtained for the second mechanism.

From the results, it is seen that both mechanisms provide a high amount of capacity saving while decreasing the needed nodal degree compared to $1+N$ at the same time. However, there is an inverse correlation between the capacity gain and nodal degree constraint. If we let the nodal degree increase, the capacity gain also increases, up to 50%. As shown in Fig. 3, the $1+N$ mechanism determines the lower bound of the used capacity and $1+1$ the upper bound. Fig. 3 and 4 are the performance results obtained by varying the number of the demands between 10 and 100 and applying protection against 10 link or node failures in the virtual domain. In both graphs, the performance of the second mechanism is given compared to $1+1$ and $1+N$. As shown in Fig. 3, when the minimum nodal degree is only 2, the capacity usage becomes equivalent to $1+1$ mechanism, thus no capacity gain is obtained. Increasing minimum nodal degree increases also the capacity gain and throughout the analysis interval, new mechanism’s performance is close to the lower limit.

In Fig. 4, the comparison for the required nodal degree is shown. In this case, the lower limit is the $1+1$ mechanism, which requires a constant nodal degree of 2. The nodal degree requirement of $1+N$ is increasing linearly with the number of the demands. The proposed mechanism performs again close to the lower limit. Hence, with its efficiency and applicability in transport networks, the proposed mechanism is a very good compromise of $1+1$ and $1+N$.

Finally, for the choice of the suitable protection mechanism for a specific scenario, the decisive point is the minimum nodal degree of the given network. For a demand matrix, which contains various connections of different sender-receiver nodes, the decision has to be taken for each demand group belonging to a sender-receiver pair. If the minimum nodal degree is high enough, $1+N$ mechanism should be chosen from these four mechanisms. If only a nodal degree of 2 is available, $1+1$ has to be deployed. In general cases, where the nodal degree is between these limits, the proposed mechanisms should be deployed in order to save resources. Depending on the computational capacity and the minimum nodal degree, the appropriate one of the two new mechanisms should be chosen. Thus, by selecting the proper mechanism for different parts of a network, the best suitable solution can be obtained.

IV. CONCLUSION AND OUTLOOK

In this paper we have proposed two new mechanisms for protection of transport networks against single link or node failures. These existing $1+1$ and $1+N$ mechanisms have the drawback of high capacity usage and high nodal degree requirement, respectively. The limitations on nodal degree in transport networks prohibit the implementation of $1+N$. Thus, the importance of the proposed mechanisms is that they offer a good compromise between the $1+1$ and $1+N$ mechanisms. This provides an efficient solution applicable to transport networks.

The difference between the two new mechanisms lies in the performance vs. complexity trade-off. The second mechanism performs better regarding both capacity usage and nodal degree requirement, but requires higher complexity in the network nodes. Hence, in cases where a simple architecture is needed, the first mechanism can be applied. In other cases, the second one is preferable.

The analysis shows that the second mechanism provides 25% capacity gain compared to the $1+1$ mechanism with a minimum nodal degree of only 3. Moreover, this mechanism becomes equivalent to $1+1$ with a minimum nodal degree of 2 and performs like $1+N$ when the minimum nodal degree increases sufficiently. In the middle regions, it performs very close to the best cases regarding capacity and nodal degree requirements achieved by $1+N$ and $1+1$, respectively.

Regarding the second mechanism, the research area for choosing the most appropriate coding scheme is still open. The advantages and disadvantages of different codes should be determined considering efficiency and complexity for realizing this mechanism in transport networks.

Moreover, in our analysis the comparison of the mechanisms is given considering various points. Still, some simulations, where the mechanism is applied in a whole transport network and the mapping from virtual domain to the physical domain is realized, are needed to determine the exact behavior and advantages of the mechanism in a real world implementation.

REFERENCES