Survey on Survivable Virtual Network Embedding Problem and Solutions

Sandra Herker, Ashiq Khan, Xueli An
DOCOMO Communications Laboratories Europe GmbH
Munich, Germany
{herker, khan, an_de_luca}@docomolab-euro.com

***Abstract*—Survivability in networks has always been an important issue and lately becomes for network virtualization. Network virtualization provides to run multiple virtual networks on a shared physical network. Since a failure in the physical network can affect several virtual resources, therefore, the survivability has to be considered in the embedding of the virtual resources. In this paper, we present a survey on the survivable virtual network embedding problem and different approaches to solve this problem. The different approaches and algorithms are evaluated on their type of survivability.**

Keywords-survivability; virtualization; virtual network embedding; embedding algorithms

I. INTRODUCTION

Network virtualization is receiving more and more attention lately. It is the sharing of physical resources by subdividing a physical node or link into many virtual nodes or virtual links. Network virtualization is a technology which allows a service specific (virtual) network to be embedded onto a substrate network in a dynamic way. Using end-to-end virtualization it will be possible to create various service specific networks within one operator's network. The network can be tailored to the specific needs of a service with respect to topology, routing or QoS.

Multiple configurations of the virtual networks maybe created over the same physical setup. Some configurations may be more efficient than others in terms of different requirements such as, optimal use of physical resources, maximizing the revenue and/or minimizing the power consumption. The calculation of the effective allocation of the physical resources among the virtual network requests is known as the virtual network (VN) embedding problem. Since multiple virtual networks can share the physical resources of the underlying substrate, even a single failure in the substrate can affect a large number of VNs and the services they offer. Thus, the problem of efficiently mapping a VN to a substrate while guaranteeing the VNs survivability in the event of failures in the substrate becomes important. Many different basic solutions for embedding VNs are existing [1][2][3][4], however, the survivability issue in the VN embedding is not considered in these works. These algorithms are assuming that the substrate network after the embedding is operational at all times and ignoring the possibility of substrate link/node failures.

Link failure survivability problems and survivable routing have already been investigated for optical [5] and multi-protocol label switched (MPLS) networks [6]. However, the problems studied there are an offline version or assume the traffic demand matrix has been available in advance which is not the case in virtual network embedding.

In this paper, the focus is on survivable Virtual Network Embedding problem and solutions. The remainder of this paper is organized as follows. We first describe general and survivable Virtual Network Embedding problem in Section II. In Section III recent algorithms for solving the survivable Virtual Network Embedding problem are evaluated. Section IV and V gives a discussion on the algorithms and a conclusion.

II. THE SURVIVABLE VIRTUAL NETWORK EMBEDDING PROBLEM

A. The Virtual Network Embedding Problem

The virtual network (VN) embedding problem deals with finding a mapping of a virtual network request onto the substrate network/physical network. When an operator wants a Virtual Network (VN) to offer a specific service to his customers and he sends a VN request to a Virtual Network Provider (VNP). The VNP requests resources which meet the requirements of the VN request from the Physical Infrastructure Provider (PIP), who owns the substrate network/physical network, for the VN creation.

The substrate network/physical network is presented as a graph $G^S = (N^S, E^S)$ where vertices N^S represent the substrate nodes and edges E^S represent the links between nodes in the network. Both substrate nodes and links have constraints. Node constraints can be CPU, RAM, geographical location, etc. Link constraints can be bandwidth, delay, etc.

The virtual network request consists of virtual nodes and virtual links, which is also described by a graph $G^V = (N^V, E^V)$ with constraints that describes the requirements of the virtual nodes and links. The mapping of virtual nodes and links onto the substrate network is realized by an embedding algorithm.

The objective of the VN embedding is to find an effective and efficient embedding algorithm for the VN request. Embedding has been proven to belong to the NP-hard category of problems in [1][7]. Three approaches are commonly used to solve a heuristic for the embedding problem: backtracking [4], simulated annealing [8] and approximation algorithms [9].

The VN embedding problem can be divided into two separate problems:

 ISBN: 978-1-61208-256-1

a) Node mapping:

$$N^V \mapsto N^S \quad (1)$$

One virtual node needs to be mapped to exactly one substrate node, which satisfies the resource requirements of the virtual node (equation (1)). The node mapping problem is still a NP-hard problem, similar to the multi-way separator problem [1][7]. For node mapping, greedy methods [1][2] are often used.

b) Link mapping:

$$E^V \mapsto P^S \quad (2)$$

P^S is denoted as the set of all loop-free paths of substrate network. A virtual link between two virtual nodes can be mapped on a substrate path, which could consists one or multiple substrate links (equation (2)). For this problem, (k-) shortest path [2] or multi-commodity flow algorithms [10] are used.

B. The Survivable Virtual Network Embedding

1) Types and characteristics of failures: Survivable virtual network embedding deals with failures in the substrate and virtual network. The challenges to be considered are link and node failures, which have to be backed up before the failure or recovered after failure. Failures can occur at different layers in the network. For example at the physical layer, a fiber cut may cause a physical dis-connectivity. In [11], it is shown that 20 % of all failures in an IP backbone are resulting from maintenance activities. About 53 % of the unplanned link failures are due to router-related [11]. In a network, single and also multiple failures can occur. The single failure case happens more often than multiple simultaneous failures. The study [11] states that about 70 % of the unplanned link failures are single link failures. A study [12] about network-related failures in data centers found out that link failures happen about ten times more than node failures per day. Usually node failures are due to maintenance [12].

2) Survivable failure methods: There are two main survivability methods: protection and restoration [5]. Failure protection is done in a proactive way to reserve the backup resources before any failure happens. Reactive mechanisms, which are called restoration mechanisms, react after the failure occurs and start the backup restoring mechanism. However, some data loss is possible in the reactive case. There exist two kinds of backups for the protection scheme: dedicated backup or shared backup. In shared backup, the resources for the backup may be shared with other backups. In the dedicated case the backup resources are not shared for other backups.

Failures in the virtual network can be repaired through re-instantiation of the failed virtual network element (link or node) on the same substrate elements or some other suitable substrate elements. Failures in the substrate network require more effort to be restored or backed up, since sharing the substrate can affect several virtual resources. For substrate node failure, the virtual node or nodes has to be migrated to some other substrate nodes. For substrate link failure, a backup path over different substrate links has to be found,

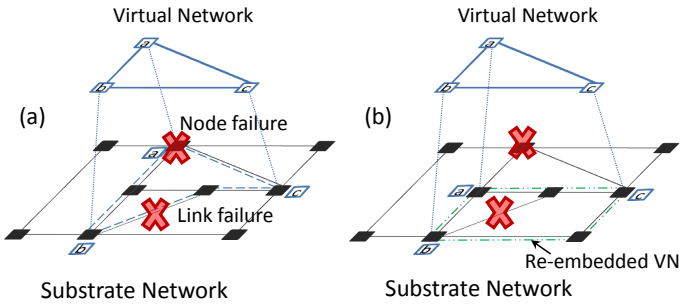

Figure 1. Survivable virtual network (VN) embedding

which can be done with a link or path based method. Link based methods means that each primary link is backed up by a pre-configured bypass path. In the path based methods, each end-to-end primary path is backed up by a disjoint path from the source node to the destination node.

The task is to embed a virtual network that can deal with virtual and substrate network failures in a way, that after the failure, the virtual network is still operating. The failure and the fixing/recovery should be transparent to the users of the virtual network.

One possibility can be to extend the virtual network graph with backup nodes N_B and backup links E_B (equations (3)) and embed the extended graph G_B^V. The backup links E_B are links between backup nodes and working nodes.

$$G_B^V = (N^V \cup N_B, E^V \cup E_B) \quad (3)$$

In the survivable mapping, virtual nodes of one virtual network should not be mapped on the same substrate node. Due to the fact, that a possible failure of this substrate node could affect several virtual nodes. For links, different virtual links should use distinct paths in the substrate network.

Figure 1 (a) shows a mapping (dashed lines) of a virtual network (upper graph) onto a substrate network (lower graph). After embedding, a substrate node and link failure (represented by crosses) occur. The failed node has mapped the virtual node *a*, which need to be remapped. The substrate link failure is on the substrate path for the virtual nodes *b* and *c*. A possible re-embedding of the virtual network on the substrate after the failure is drawn in Figure 1 (b), where virtual node is migrated to a new substrate node and the links are re-embedded for the migrated node and the failed substrate link.

III. Algorithms for the Survivable Virtual Network Embedding

This section discuss existing algorithms and methods for survivable/resilient virtual network embedding for link or node failures.

A. Survivable VN Embedding against Link Failures

The following algorithms embed VN against links failures in the substrate network.

1) Link restoration and protection methods: In [13], a reactive backup mechanism to protect against a single substrate link failure for VN embedding is proposed. The idea is a fast rerouting of the links and to reserve bandwidth for backups

 ISBN: 978-1-61208-256-1

on each physical link. The polynomial time heuristic consists of three parts. Before any VN request arrives, backup paths for each substrate link are calculated with a path selection algorithm. Then node and link embedding is done for the arriving request with an existing embedding algorithm. When a substrate link failure occurs, the calculated backup paths are used to reroute the bandwidth of the affected link using their reactive online optimization mechanism. The optimization goal is to maximize revenue for the PIP. This backup mechanism is a restore approach, therefore after a failure it cannot guarantee 100 % recovery. In cases that the bandwidth resources are used for new VN requests, there may be not enough resources left for the recovery. With increase in traffic load, a failure can cause a big amount of data loss and the backup mechanism may not restore the VN.

Authors in [14] also investigate the problem of shared backup network provision for a single substrate link failure for VN embedding. In their solution, a link based backup approach is used to protect against the link failure similar to [13]. Two schemes are proposed: In Shared On-Demand approach, bandwidth resources are allocated to the primary flows and to restoration/backup flows when a new VN request arrives. Bandwidth sharing is possible for the restoration flows, however, not for the primary flows. After every VN embedding, the residual resource information needs to be updated. In Shared Pre-Allocation approach, backup bandwidth for each substrate link is pre-allocated during the configuration phase before any VN request arrives. Since the bandwidth pre-allocation only needs to be done once and not for every VN request, there is less computing done during the VN embedding phase. The overall optimization is to maximize the revenue for the Infrastructure Provider through accepting most VN requests. Advantage to the previous algorithm [13] is that the backup bandwidth is already allocated before the failure happens and not after the failure. Disadvantage of the Shared Pre-Allocation approach is that backup bandwidth is reserved independent of the VN requests and may not be used at any time if few VN requests arrive.

2) Path protection methods with node migration: In [15], the problem of survivability for link failure is tried to solve with optimizing the networking and computing resources to tolerate link failures through a node migration technique. Instead of backing up the each primary link like in [13] and [14], each end-to-end primary substrate path is protected by a backup path. Their approach, migratory shared protection, migrates and maps a VN node to another substrate node to increase the resource efficiency when a failure occurs. The relocated node should need less backup path length to the destination node than before the migration and save resources. All VN links connected with the migrated VN node have to be remapped, and the backup links must be link-disjoint to the primary links. The re-established paths from the new migrated node form a tree: the migratory backup tree. The survivable mapping solution with migratory protection includes: an one-to-one node mapping from the VN nodes to the substrate nodes, a mapping of each VN link to a primary path from the original source node to the original destination node and a mapping of each VN link to a link-disjoint backup path or migratory backup tree. For this protection method, intra-share can be applied, that means sharing resource among the migratory backup tree and the corresponding migrated primary paths. Also inter-share is possible that means sharing of backup resources between different backup paths. Migratory shared backup tree is only calculated to improve performance of the traditional backup protection or if no traditional link-disjoint backup path can be found. The optimization goal is to minimize the sum of the computing and bandwidth resource. However, the cost of less bandwidth resources cannot be compared to the cost of a node migration, since node migration costs are considered higher. Compared to the traditional backup protection where only one path needs to be migrated in their approach several links and at least one node need to be migrated.

3) Path protection methods with QoS: A mechanism, named QoSMap, attempting to consider both quality of service (QoS) and resiliency in constructing VNs over a substrate network is presented in [16]. Its aim is to map a QoS-specified overlay onto the substrate network using direct paths between nodes that are pre-selected possible candidates. Nodes with higher quality are selected first. Node quality depends on the average backup paths that a substrate node can provide. Path resiliency is provided by constructing alternate backup paths via one intermediary node that could be additional underlying nodes or selected hosting overlay nodes. However, the substrate topology is not considered when selecting backup paths. It could be possible that disjoint overlay paths share common substrate links or nodes. There is also high degree of overlap for working and backup paths in the mapped solution. They might fail together if they share common point of failures. It may not always be possible to find direct backup paths. Since QoSMap uses direct paths, back-tracking in the algorithm is required to find these (backup) paths. This may take exponential time and affect scalability of the algorithm.

The authors in [17] formulate and solve the previous QoS and resilience mapping problem [16] with an Integer Linear Program (ILP). Since the heuristic QoSMap solution [16] cannot guarantee the best QoS performance, due to sequential and heuristically node selection, a mathematical formulation is used to achieve a optimal solution. A simplified topology, that contains the candidate nodes connected for the mapping of the request, is constructed from the substrate network. This logical topology enables the mapping of the request with reduce in computational complexity. In the logical topology, the links between the candidate nodes are calculated using the shortest path first routing and considering the overlay delay requirements. The object to optimize is to minimize the delay and the number of additional substrate nodes used for backup path mapping for the overlay links. The ILP considers the substrate topology and assure working and backup paths avoiding link overlaps in the substrate network. Therefore, multiple overlay link failures caused by a single substrate link failure should be reduced.

 ISBN: 978-1-61208-256-1

In [18] a heuristic is developed for the previous ILP [17]. This heuristic improves the QoSMap heuristic [16] by considering the substrate topology information in the mapping procedure.

B. Survivable VN Embedding against Node Failures

The following different approaches try to embed VNs with backup for virtual nodes and protections against node failures in the substrate network.

1) Two-step approaches: In [19], a two-step paradigm to fully recover a VN from facility node failures is presented. The first step is to construct a graph of the VN request with backup virtual nodes and links, and then this enhanced VN request has to be mapped onto the substrate network. Two solutions are proposed: the 1-redundant scheme and the K-redundant scheme. A 1-redundant solution is a reliable VN graph with one redundant virtual node (backup node) and redundant connections, which is then mapped onto the substrate network. Assuming only single failure, the backup node of a certain virtual node can also be used as backup of some other virtual node for resource sharing. For the mapping, it can share the physical link resources when mapping them onto the substrate network (backup share) and also share the bandwidth link resources between the original working path and its associated backup path (cross share). In the K-redundant solution, a K-redundant reliable VN graph is designed, in which each critical node is permitted to have a corresponding backup node. The optimization objective is to minimize network resource costs. However, this approach may fail to provide a joint optimization for the allocation of both the active and backup resources. In worst case, there need to reserve a backup node for every critical node and links to every neighbor node.
Another two-step method is presented in [20] for surviving single facility node failures. This approach designs the enhanced VN with a failure-dependent strategy, instead of a failure-independent strategy like in the previous one [19]. It manages to further reduce the needed virtual resources and, therefore, less allocated backup resources compared to failure-independent strategy. The idea is that, when node i fails, the role of node i may be replaced by any other nodes after a rearrangement of all the nodes (including the backup node(s)) using graph transformation/decomposition and bipartite graph matching. The disadvantage of this approach is that the large amount of possible migrations of working nodes after a failure makes the approach less applicable in large networks.

2) Node protection for regional failures: In [21], an approach for solving the problem of survivable VN mapping for single regional failures in a federated computing and networking system is presented. In a federated computing and networking system, facility nodes from a data center are interconnected. These facility nodes need to be backed up to achieve a survivable VN mapping. Their approach is based on the assumption, that the number of distinct regional failures is finite in a specified geographical area and that a regional failure refers to a set of substrate nodes and links, which is in the same shared risk group. The proposed approach first solves the non-survivable VN mapping problem with a heuristic and extends this heuristic to handle the survivable VN mapping problem. Two failure dependent survivable VN mapping algorithms are developed. The Separate Optimization with Unconstrained Mapping (SOUM) decompose problem into separate non survivable problems for each possible regional failure plus one for the initial working mapping of the VN request. Each problem is mapped in a way that the costs of the used resources are minimized. The other approach, Incremental Optimization with Constrained Mapping, maps first the initial working mapping and then handles each regional failure after another. Compared to the SOUM, the additional computing and networking resources, that are needed to handle the failure, are tired to minimize. With this strategy, the mapping of unaffected virtual nodes is not changed. The disadvantage of SOUM is the re-calculating virtual mapping of unaffected nodes, which results in more costs and more time to be calculated.

3) Node protection with location-constraint: The Location-constrained Survivable Network Embedding (LSNE) problem to protect against any single facility node failure is investigated in [22]. The location constraint of a virtual node is considered for its backup node. The goal is to map the VN with minimum resources while satisfying the bandwidth constraints for the links and capacity constraints for the nodes including meeting the location constraints for the primary and protection node. The idea is to construct a graph with the virtual and substrate graph in one graph. Thereby, each virtual node is connected to some candidate substrate nodes, which satisfy the location and capacity constraints. This problem is formulated as an ILP framework and for large scale a heuristic algorithm is developed. The heuristic algorithm (sequential survivable embedding algorithm) is based on the decomposition of the LSNE problem. First the VN request is mapped with an existing embedding algorithm and then the backup request is mapped.

4) Backup node sharing with reliability: Authors in [23] tried to recovery from both substrate node and link failures while minimizing backup resources through pooling. Further a relationship between reliability and the amount of redundant resources is tried to be found. Redundant (backup) virtual servers are created dynamically and are pooled together to be shared between VNs to assure the requested reliability level. The higher the reliability level, the higher number of backup nodes needed. It is possible to share the backup nodes such that the total number of backup nodes is lower than each VN separately has their own backup nodes. Every backup node can be a standby node for all other critical nodes. With the Opportunistic Redundancy Pooling (ORP) mechanism, backup nodes can be shared between VNs as long as the reliability of every network is satisfied. The ORP shares these redundancies for both independent and cascading types of failures. Therefore, VNs with different reliability guarantees can be pooled together and it is flexible in adding or removing VNs to the exciting ones.

5) Node protection in data centers: An optimization framework for the survivable virtual infrastructure mapping in virtu-

 ISBN: 978-1-61208-256-1

alized data centers is presented in [24]. Multiple correlated Virtual Machines (VMs) and their backups are grouped together to form a Survivable Virtual Infrastructure (SVI) for a service or a tenant. The aim is to minimize the backup resources (number of active servers and needed bandwidth) while guaranteeing no-disruption no-degradation fail-over. This problem is similar to the VN embedding problem, however, multiple VMs are allowed to be placed on a common server to minimize the number of active servers. An additional goal is to minimize the total reserved bandwidth. This problem of a SVI can be divided in the VM Placement (VMP) and Virtual Link Mapping (VLM) Problem that can be solved separately. For the Virtual Machine Placement subproblem, an efficient heuristic algorithm (back tracking) based on Depth First search is designed. For each VMP solution, the Virtual Link Mapping subproblem is calculated using a Linear Program (LP)-based algorithm (LP-VLM). Further an algorithm to jointly solve the two subproblems at the same time is developed. This joint mapping algorithm determines a server pair for each virtual link and allocates the bandwidth between with a LP and after that solves the LP-VLM. For the VMP problem, quite a large number of possible solutions are calculated, even when it is restricted, and again for all the possible VMP solutions, the VLM must be calculated. This results into high computing overhead for large networks and not guaranteeing to get always closed to the optimum.

C. Distributed Survivable VN Embedding

In all the previous approaches, the survivable VN embedding is done by centralized entity. In [25], an adaptive VN embedding framework is proposed for a distributed survivable VN mapping algorithm, without a centralized controller. The proposed system is distributed and based on *agents*, which monitor physical elements. *Agents* detect failures and change the VN allocation to maintain the constraints of each VN. The fault-tolerant embedding algorithm can handle three resource failures: virtual node, substrate node and link failure. When a virtual node failure is detected by a substrate agent, a new virtual node has to be created on the same substrate node or on another substrate node. When a substrate node fails, alternative nodes have to be found and the affected virtual nodes and links have to be migrated. For link failure, the agent substrate nodes, which are connected to this link, try to find an alternative link or path. The embedding algorithm also monitors the bandwidth in the substrate nodes, therefore, can recognize congestion or overload in the substrate links. When a failure occurs the distributed embedding algorithms works following: If a substrate node agent detects a node failure, it sends a failure notification message to all substrate agents in the same cluster. All agents receiving this message check if they can host the node. Each agent calculates dissimilarity metric to compare their similarity to requested node. The substrate node, which metric is minimal, will be used. The last step is to map the virtual links to the substrate paths between substrate nodes using a distributed shortest-path algorithm [26]. For link failures only the last step need to be done.

IV. Discussion

In summary, Table I presents a comparison of the embedding algorithms presented in this paper.

A. Limitation of Previous Work

The approaches are mostly protection methods for link or node failures, which reserve/backup before any failure happens. Restoration methods like in [13] may need less reserved bandwidth compared to protection methods, however, it cannot provide against a possibility of data loss during the failure. Most works focus on single substrate failure. Types of failures are single link, single facility node and single regional failures in the network. They assume that the network failures are independent from each other and only one failure happens at a time. In [21], a single regional failure which destroys more than one facility node is addressed. Several approaches [15], [16] uses path protection against link failures which could provide bandwidth saving over link protection. However, path protection is more vulnerable to multiple link failures than link protection. Shared protection for the backup links or nodes is also part of some approaches [14], [15], [19] which saves resources over dedicated protection, however, it is more vulnerable to multiple link failures. Also none of them deal with node and link failure occurring at the same time. They only focus on link backup or node backup with the concerned links. However, combining node and link failure for survivability in the network is also important.

The approaches focus on solving the survivable embedding problem in a single PIP environment. At least in [21] a federated computing and networking system is considered.

The main objective for optimization of the presented approaches is maximizing the revenue while minimizing the total cost through minimizing the redundant resources. Each substrate resources like bandwidth or computing resource has a unit cost. The total cost is the sum of all resource costs of the used substrate resources.

B. Open Research Issues

Multiple node or link failures occur at the same time in the network and the correlations between node/link failures are not addressed in any approach. Further work could be done to extend the existing heuristics/algorithms to deal with multiple link or node failures and to combine link and node protection or migration methods.

Survivability in a multi-domain VN environment could have new challenges for inter and inter domain link failures. Multiple simultaneous inter-domain and intra-domain failures could require to develop new mechanism than for single domain environment.

V. Conclusion

This paper presented a survey on existing survivable VN embedding algorithms. Several approaches to solve the problem are examined. The redundancy and the survivability issue in networks has always been an important aspect of network operators and especially for mobile operators. Due

 ISBN: 978-1-61208-256-1

TABLE I
SUMMARY OF THE SURVIVABLE EMBEDDING ALGORITHMS

References	Survivability	Type of failure	Optimization Objective	Survivable failure mechanism
Survivable virtual network embedding [13]	Link	Single substrate link failure	Maximize revenue for Infrastructure Provide	reactive, after failure (Restoration)
Shared backup network provision for virtual network embedding [14]	Link	Single substrate link failure	Maximize revenue/accepting VN requests	proactive, before failure (Protection)
Migration based protection for virtual infrastructure survivability for link failure [15]	Link	Single substrate link failure	Minimize sum of costs	before failure
QoSMap: Achieving Quality and Resilience through Overlay Construction [16]	Link	Single substrate link failure	Minimize delay and additional resources for backup	before failure
An overlay mapping model for achieving enhanced QoS and resilience performance [17] / An overlay mapping model for achieving enhanced QoS and resilience performance [18]	Link	Single substrate link failure	Minimize delay and additional resources for backup	before failure
Survivable virtual infrastructure mapping in a federated computing and networking system under single regional failures [21]	Node	Single regional failure	Minimize sum of cost	before failure
Cost efficient design of survivable virtual infrastructure to recover from facility node failures [19]	Node	Single facility node failure	Minimize sum of cost	before failure
A novel two-step approach to surviving facility failures [20]	Node	Single facility node failure	Minimize resources/total cost	before failure
Location-constrained survivable network virtualization [22]	Node	Single facility node failure	Minimize resources	before failure
Designing and embedding reliable virtual infrastructures [23]	Node	Single substrate node failure	Minimize amount of resources used	before failure
Survivable virtual infrastructure mapping in virtualized data centers [24]	Node	single server failure	Minimize operational cost	before failure
Adaptive virtual network provisioning [25]	Node or Link	single node failure or single link failure	-	after failure

to revenue reduction of the operators, the redundancy has to be optimized against cost. Most operators have very large nationwide networks that fast approximation algorithms for the survivability embedding problem have to be found. The ILP and MILP are limited in scaling and not applicable to larger networks. Therefore, approximations and heuristic algorithms are necessary which can cope with multiple failures in the network. Future directions could be to investigate the survivability VN embedding issue in a multi-domain NV environment or to extend to handle multiple link and node failures at the same time.

REFERENCES

[1] M. Yu, Y. Yi, J. Rexford, and M. Chiang, "Rethinking virtual network embedding: substrate support for path splitting and migration," *SIGCOMM Comput. Commun. Rev.*, vol. 38, pp. 17–29, March 2008.

[2] Y. Zhu and M. Ammar, "Algorithms for assigning substrate network resources to virtual network components," in *IEEE INFOCOM 2006. Proceedings*, April 2006, pp. 1 –12.

[3] J. Lu and J. Turner, "Efficient Mapping of Virtual Networks onto a Shared Substrate," Washington University in St. Louis, Tech. Rep., 2006. [Online]. Available: http://www.arl.wustl.edu/˜jl1/research/tech_report_2006.pdf

[4] J. Lischka and H. Karl, "A virtual network mapping algorithm based on subgraph isomorphism detection," in *Proceedings of the 1st ACM workshop VISA*, ser. VISA '09. ACM, 2009, pp. 81–88.

[5] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable wdm mesh networks," *Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870 – 883, April 2003.

[6] Y. Liu, D. Tipper, and P. Siripongwutikorn, "Approximating optimal spare capacity allocation by successive survivable routing," *IEEE/ACM Transactions on Networking*, vol. 13, no. 1, pp. 198 – 211, Feb. 2005.

[7] D. G. Andersen, "Theoretical approaches to node assignment," Dec. 2002, unpublished Manuscript.

[8] R. Ricci, C. Alfeld, and J. Lepreau, "A solver for the network testbed mapping problem," *SIGCOMM Comput. Commun. Rev.*, vol. 33, pp. 65–81, April 2003.

[9] N. Chowdhury, M. Rahman, and R. Boutaba, "Virtual network embedding with coordinated node and link mapping," in *INFOCOM 2009, IEEE*, April 2009, pp. 783 –791.

[10] W. Szeto, Y. Iraqi, and R. Boutaba, "A multi-commodity flow based approach to virtual network resource allocation," in *GLOBECOM '03. IEEE*, vol. 6, Dec. 2003, pp. 3004–3008.

[11] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an ip backbone," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 4, march 2004, pp. 2307 – 2317.

[12] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: measurement, analysis, and implications," in *Proceedings of the ACM SIGCOMM 2011 conference*. ACM, 2011, pp. 350–361.

[13] M. R. Rahman, I. Aib, and R. Boutaba, "Survivable virtual network embedding," in *Proceedings of the 9th IFIP TC 6 international conference on Networking*, ser. NETWORKING'10, 2010.

[14] T. Guo, N. Wang, K. Moessner, and R. Tafazolli, "Shared backup network provision for virtual network embedding," in *IEEE International Conference on Communications (ICC)*, June 2011, pp. 1 –5.

[15] H. Yu, V. Anand, C. Qiao, and H. Di, "Migration based protection for virtual infrastructure survivability for link failure," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference*, March 2011, pp. 1 –3.

[16] J. Shamsi and M. Brockmeyer, "Qosmap: Achieving quality and resilience through overlay construction," in *4th International Conference on Internet and Web Applications and Services, ICIW '09*, May 2009.

[17] X. Zhang, C. Phillips, and X. Chen, "An overlay mapping model for achieving enhanced qos and resilience performance," in *3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011*, Oct. 2011, pp. 1 –7.

[18] X. Zhang and C. Phillips, "A novel heuristic for overlay mapping with enhanced resilience and qos," in *IET International Conference on Communication Technology and Application (ICCTA 2011)*, Oct. 2011.

[19] H. Yu, V. Anand, C. Qiao, and G. Sun, "Cost efficient design of survivable virtual infrastructure to recover from facility node failures," in *IEEE International Conference on Communications (ICC)*, June 2011.

[20] C. Qiao, B. Guo, S. Huang, J. Wang, T. Wang, and W. Gu, "A novel two-step approach to surviving facility failures," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference*, March 2011, pp. 1 –3.

[21] H. Yu, C. Qiao, V. Anand, X. Liu, H. Di, and G. Sun, "Survivable virtual infrastructure mapping in a federated computing and networking system under single regional failures," in *GLOBECOM 2010, IEEE*, 2010.

[22] Q. Hu, Y. Wang, and X. Cao, "Location-constrained survivable network virtualization," in *Sarnoff Symposium (SARNOFF), 2012 IEEE*, May 2012, pp. 1 –5.

[23] W.-L. Yeow, C. Westphal, and U. Kozat, "Designing and embedding reliable virtual infrastructures," in *Proceedings of the second ACM SIGCOMM workshop VISA*, ser. VISA '10. ACM, 2010, pp. 33–40.

[24] J. Xu, J. Tang, K. Kwiat, W. Zhang, and G. Xue, "Survivable virtual infrastructure mapping in virtualized data centers," in *IEEE 5th International Conference on Cloud Computing (CLOUD), 2012*, June 2012.

[25] I. Houidi, W. Louati, D. Zeghlache, P. Papadimitriou, and L. Mathy, "Adaptive virtual network provisioning," in *Proceedings of the second ACM SIGCOMM workshop VISA*. ACM, 2010, pp. 41–48.

[26] I. Houidi, W. Louati, and D. Zeghlache, "A distributed virtual network mapping algorithm," in *ICC '08. IEEE International Conference on Communications*, May 2008, pp. 5634 –5640.

 ISBN: 978-1-61208-256-1