applied sciences

MDPI

Systematic Review

A Systematic Literature Review of Reliable Provisioning for Virtual Network Function Chaining

Le Duytam Ly †, Mahsa Sadeghi Ghahroudi *,† and Victor Ponce

Dawson College, 3040 Sherbrooke St W, Montreal, QC H3Z 1A4, Canada; le.ly@dawsoncollege.qc.ca (L.D.L.); vponce@dawsoncollege.qc.ca (V.P.)

* Correspondence: msadeghi@dawsoncollege.qc.ca

† These authors contributed equally to this work.

Abstract: The abstraction of the network node functions using virtualization methods introduced an innovative architecture called Network Function Virtualization (NFV). In NFV, every virtualization software hosts a network service recognized as a Virtual Network Function (VNF). In general, the network provider creates a Service Function Chain (SFC) for every sequence of multiple requested VNFs by the customers. Although NFV allows for a more flexible and economical approach, it is more prone to error and failure. Therefore, providing reliable provisioning for VNF chaining is one of the key issues in NFV. In this paper, we present a systematic literature review to study the pioneer research efforts that provide reliable provisioning for VNF chaining by guaranteeing the availability of the service and resource optimization. Our review is the result of the analysis of 21 screened papers. This paper presents the result of our analysis, including different aspects of a reliable provisioning algorithm, various adopted techniques for reliable provisioning, and the superiority and drawbacks of each algorithm based on the proposed criteria for the evaluation of the provisioning algorithms.

Keywords: reliable provisioning; virtual network function; service function chain; failure; systematic literature review

check for updates

Citation: Duytam Ly, L.; Sadeghi Ghahroudi, M.; Ponce, V. A Systematic Literature Review of Reliable Provisioning for Virtual Network Function Chaining. *Appl. Sci.* **2023**, *13*, 5504. https://doi.org/10.3390/app13095504

Academic Editor: Andrea Prati

Received: 12 December 2022
Revised: 28 February 2023
Accepted: 6 March 2023
Published: 28 April 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Network function virtualization (NFV) is a relatively new technology that separates network functions from the hardware [1]. In contrast to traditional deployment, Virtual Network Functions (VNF), such as firewalls or load balancers, can be placed on virtualization software instead of dedicated hardware [2,3]. The VNF provides the same function as the relevant specific hardware network function, which is augmented by the ability to adapt to network requirements [4]. A sequence of these VNFs in the network can provide a service in the network that is called a Service Function Chain (SFC) [5]. Overall, FNV, VNFs, and SFCs are discarding the expensive network equipment and replacing them with software running on low-cost hardware [6], which can significantly reduce Capital Expenditure (CAPEX) and Operating Expenses (OPEX) [7]. Moreover, adopting the NFV technology in a network enhances its management and flexibility [8]. As a result, VNFs are increasingly popular due to their convenience and flexibility.

Although NFV architecture introduces new opportunities for service providers to provide services with minimum cost, there are drawbacks to these advantages that require resolving multiple performance, availability, security, and survivability problems [9]. For each VNF, there is one software that is running on physical hardware providing one of the hardware's functions that used to be offered by individual physical hardware. Therefore, in addition to physical hardware failure, VNFs are prone to software faults [10]. Moreover, despite hardware that is subjected to rigorous testing and validation processes, the software is notoriously unreliable, which is why we expect VNFs to fail more often in comparison to traditional middleboxes. Moreover, the failure of a VNF or a link may cause the whole SFC to fail, including the failure of the associated VNFs [11]. Therefore, Virtual Network

Function Infrastructure (NFVI) must meet resiliency and geo-redundancy requirements to be able to provide the requested performance, availability, security, and survivability for a continuous service [12]. Ensuring the reliability and resiliency in an NFV is more complex than hardware solutions. A reliable VNF network often requires dedicated mechanisms to ensure high availability while keeping costs low.

There have been various studies in the NVF provisioning field, which mainly focused on VNF placement and SFC mapping [13–16]. However, studies discussing reliable provisioning and failure recovery and comparing the different approaches are limited. There are various methods to ensure the service availability of the NFV, including resilience against single or multiple link failures, single or multiple node failures, or providing backup in which the evaluation methods and simulation setup could vary. Therefore, a comprehensive study to evaluate and discuss the differences is a necessity. The goal of this paper is to compare the existing reliable provisioning algorithms and identify the key parameters for the reliable provisioning for virtual network function chaining. The advantages and disadvantages of each algorithm alongside important features of the algorithm are discussed in detail through the sections.

The rest of the paper is organized as follows. In Section 2, recent reliable provisioning algorithms are discussed. In Section 3, we define the research method by explaining the research questions, search process, and study selection criteria. In Section 4, the result of our systematic literature is discussed. The result includes detailed answers to our research questions through different sub-sections. We present some guidelines for future research and discuss the existing problems of handling failure in an NFV environment in Section 5. Finally, we conclude the paper in Section 6.

2. Background

The reliable provisioning begins with the service allocation to the NFV infrastructure and continues while the service is alive. For example, Figure 1 shows a SFC that includes three different VNFs from the assigned source and destination. In Figure 2, the SFC in Figure 1 is mapped in a network through N_1, N_3, N_4, N_5, and N_6. The network should ensure that the survivability of this SFC by either providing a failure recovery mechanism in the case of any failure or that reliable provisioning can be provided by a comprehensive algorithm that maps the VNFs to ensure service availability while reducing resource usage. In this section, we review the existing techniques that are providing reliable provisioning for virtual network function chaining.

Most of the previous research has focused on failure recovery for non-distributed networks. Examples in the literature have addressed these failures by adding backup VNFs and paths [17]. Adding backups causes the network to be more resilient and less prone to failure. However, using backups in the network adds resource overhead and, consequently, costs. In [18], the authors propose a Joint-Path-VNF (JPV) backup model, including both path and VNF backup. To mitigate resource consumption, they propose an Affinity-Based Algorithm (ABA) to group physical machines with the same communication overhead, allowing for reduced resource consumption. A joint selective diversity and redundancy mechanism to provide resiliency is also proposed in [19]. Their solution for diversity is to split a VNF into a group of smaller VNF instances called replicas. A failure of a replica does not mean that the VNF is nonoperational since there are still other replicas. They also propose to provision backup VNFs in an inactive state to provide redundancy while at the same time reducing resource costs.

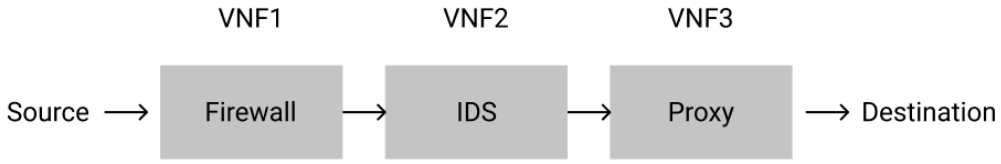


Figure 1. A service function chain.

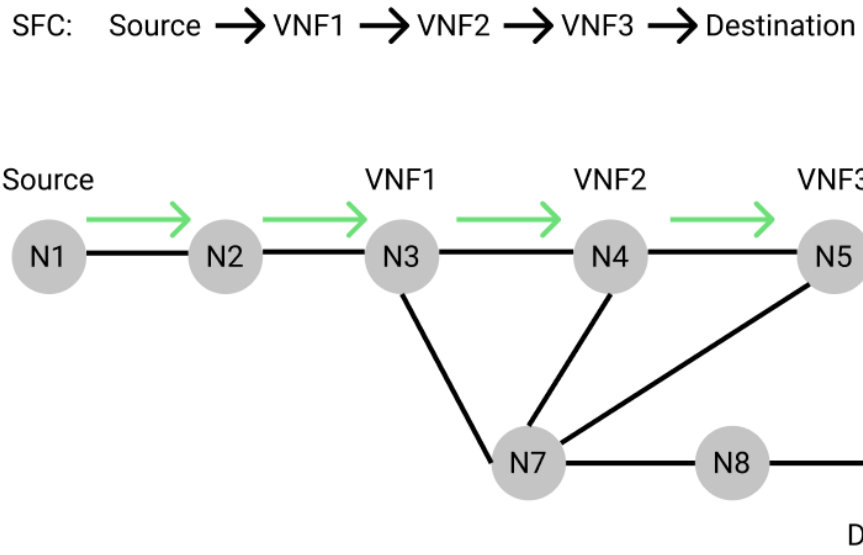


Figure 2. Provisioning of VNFs for a SFC.

Another approach is using multi-path protection to handle survivable VNF placement [20]. If a failure occurs in this approach, the connection will not be lost since the data can still be transmitted using other paths. The results shown in [20] confirms that multi-path protection performs better in blocking probability and spectrum efficiency compared to single-path protection. On the other hand, in [21], the K-node disjoint shortest path algorithm is used to handle the survivability of VNFs against multiple failures. K-node is a modified Dijkstra algorithm that aims to decrease the failure rate while minimizing computing and network resource usage. Another research proposes three methods of providing protection (Virtual-Node protection, Virtual-Link protection, and End-to-End protection) against failures [22]. Virtual-Node protection instantiates VNFs in two different physical nodes. Virtual-Link protection uses the same VNFs in the same physical node. However, the backup path cannot use the same physical links as the primary path. Finally, for End-to-End protection, both VNFs and paths must be different. The results in [22] show that End-to-End protection provides the protection level but costs up to 10% more OPEX. Virtual-Link protection consumed the least amount of network resources while decreasing the OPEX. In [23], an efficient algorithm called Optimal Fog-supported Energy-aware SFC (OFES) is introduced to minimize the fault probability and recover failure. The OFES optimizes the Fog nodes' energy consumption but the computational complexity limits the scalability of the algorithm. Therefore, a heuristic algorithm called Heuristic OFES (HFES) is proposed to be applicable to real-world networks. Both algorithms can keep the fault probability under the predefined threshold, while HFES is superior in the utilization of the link and Fog node. However, network devices' energy consumption, queuing delay, and VNF sequences are yet to be addressed.

Other examples in the literature propose using machine learning to handle failures. In [10], the authors present a Zero-Touch Proactive Failure Recovery (ZT-PFR) approach, which uses deep learning methods such as Soft-Actor-Critic (SAC) and Proximal-Policy-Optimization (PPO) to predict failures. The approach defines many VNF states, such as

Normal, Warning, and Critical. The agent will be rewarded for correctly predicting the state change and for doing the necessary actions to provision backup VNFs. In [24], an algorithm is proposed to use Elastic Virtual Network Function Orchestration (EVNFO) to predict the workload and properly scale the network. A deep reinforcement learning method called Double Deep Q-Networks Placements (DDQP) is introduced in [25]. DDQP is used to deploy active and standby instances of backups in real-time. For larger networks, they used Deep Neural Networks (DNN). Despite the different approach, it still uses backup VNFs and paths for the recovery mechanism. The proposed solution has a higher cost for smaller networks compared to larger ones. In addition, [26] proposes using the Diversity Coding method to provide near-instant failure recovery for 5G networks. The method consists of creating a single redundant disjoint link to handle any single failure. The downside of the solution is that it cannot handle multiple failures. On the other hand, in distributed approaches such as the one introduced in [27], the Tabu search algorithm is used to handle the VNF placement to minimize cost and meet the performance requirements. The problem with the proposed approach is that it does not perform well in larger environments. In [28], authors the present the use of game theory to properly place VNFs in a distributed network. VNF Managers, which can deploy VNFs, act as players in a game. Each player can decide to activate itself to maximize its utility. Due to the distributed network, VNF managers autonomously adapt to the network without central control.

3. Research Method

Our systematic literature review starts with defining the research questions that develop the search string. The fetched articles based on the search string compose comprehensive literature to answer the questions. The outcome of the systematic literature review assists researchers in having a comprehensive understanding of the problem and identifying the research gaps and possible future work. In this paper, we review the existing literature about reliable provisioning for VNF chaining and discuss the systematic review results in detail.

3.1. Research Questions (RQ)

The following are the research questions that we intend to analyze in this paper:

3.1.1. RQ1

What are the different strategies used for reliable service function chaining? What are the characteristics of those approaches?

3.1.2. RQ2

What are the different approaches used by researchers for effective reliable provisioning? What are the strengths and weaknesses of the existing techniques in the literature? The different methods they propose to address the reliable provisioning and the considered situations such as different types of failure and their occurrence.

The main goal of this paper is to answer the mentioned research questions after reviewing all the related literature. In RQ1, we focused on the various strategies researchers considered to address the failure in VNF chaining. The different approaches proposed for reliable VNF placement are elaborated in RQ2. We analyze those approaches and compare the techniques to recognize the strengths and weaknesses of the existing techniques and their challenges.

3.2. Search Process

The search process started by finding related articles from academic search engines. We conducted searches in IEEE Xplore [29], ACM Digital Library [30], Scoup [31], WoS [32], and Google Scholar [33]. The search strings we used to search within the mentioned digital libraries are reliable provisioning, protection strategies, and failure recovery that are used alongside VNF, service chain, NFV, and service function chain. Afterward, we narrowed

down the articles based on the title, abstract, and full text to refine the results. The screening process of the papers is summarized in Table 1. The visual overview of the research process is shown in Figure 3.

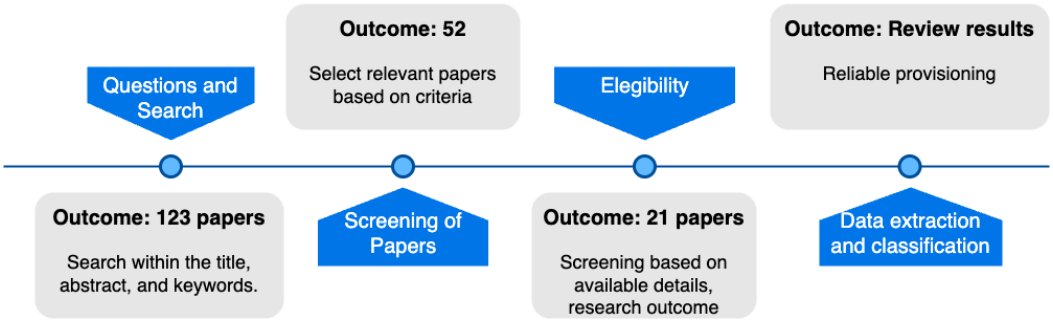


Figure 3. overview of the search process.

Table 1. Screening of papers.

Consideration	Criteria for Inclusion	Eligibility
Publication year	No restrictions. Results from 2014 to 2023	The final range after screening is from 2015 to 2021
Relationship with the subject	Papers related to NFV, VNF, and SFC. The paper discusses provisioning	Included when the main contribution is related to reliable provisioning
Type of document	The research is published in IEEE, ACM, SCOPUS, Web of Science, or Google Scholar	The research outcome is published in proceedings and journals

3.3. Study Selection Criteria

We have introduced additional criteria to select the relevant literature. In the first stage, only articles that could answer the research questions are added. Initially, we obtained 52 documents from the mentioned databases. In the next phase, we discarded 31 papers mainly due to duplication or unrelated subjects. In the subsequent phases, we critically analyzed papers and withdrew 21 papers based on the following considerations:

- Articles include sufficient information to answer the research questions. The papers cover different aspects of the algorithm and explain the problem in more detail.
- Studies that proposed novel reliable provisioning algorithms. The algorithm considers new approaches to address the issue and resolve the problem differently.
- Papers that are not outdated and published in recent years.
- Studies are relevant to the research topic. The ones that discuss the research questions and consider the same perspective.

4. Results of the Systematic Literature Review

In this section, we present the result of our systematic literature review in detail. The answer to each research question is described in different subsections. Every subsection is organized to separate different aspects of the question to demonstrate the detail.

4.1. Different Strategies Used for Reliable Service Function

One of the key issues in the deployment of Service Function Chains (SFCs) is reliability, especially as VNFs are more prone to software failure and connectivity errors [18,25,34]. Moreover, telecom network services are required to have even higher availability in the Service Level Agreements (SLA) compared to previous IT applications that demand 99% and 99.9% [35]. SLA violations cost providers penalties and decrease the quality of the

service a customer experiences. For example, IT downtime and data recovery cost IT businesses in North America USD 26.5 billion in revenue each year [36]. Therefore, ensuring the reliability of the deployment service function chain and increasing its availability is of high importance.

4.1.1. Reliable Provisioning by a Protection Scheme or Recovery Plans

Reliable service provisioning can be provided in various ways. Generally, existing work can be categorized into two groups: ones that increase the service availability by protection schemes to decrease the failure in the network and the ones that have recovery plans to cause the service to be available with no or less failure time. Most of the existing literature introduces backup models to provide reliable provisioning.

In [18], an availability model is introduced that considers both physical devices and VNF failures when evaluating the SFC availability. On the other hand, Joint Path-VNF (JPV), which considers both path backup and VNF backup is proposed. The availability model is used with the defined backup model, Joint Path-VNF (JPV), which, along with the Affinity-Based Algorithm (ABA), decreases the physical link consumption during VNF mapping and improves the availability. A protection mechanism is also proposed in [37] that combines VNF replicas and backup path protection for SFC availability improvement. In addition, [38] introduced another joint protection scheme that focuses on path backup and uses one physical node for the two physical nodes' backup. Different protection schemes can be followed to avoid the failure of the SC [22]. Three different protection schemes (Virtual-Node protection, Virtual-Link protection, and End-to-End protection) are introduced in [22] to discard the SC failure. The proposed heuristic algorithm for each of them considers the dynamic provisioning of the SC to address the issue. The simulation results confirm the priority of the End-to-End approach in latency requirement while the Virtual Link protection algorithm requires less network and computational resources [22]. A deep reinforcement learning (DRL)-based online SFC placement approach called DDQP (Double Deep Q-networks Placement) is proposed to provide a fault-tolerance VNF chain placement [25]. The DDQP allows deploying active (main SC) and standby (backup) instances in real-time to increase the model's fault tolerance. The main purpose of the algorithm is to ensure service reliability while managing resource usage for various requests. Therefore, five different schemes for resource reservation are proposed to address different customers' requests. The simulation results of the DDQP present a rapid response to the requests and near-optimal performance. In every protection scheme, a primary SC provides the requested service in normal conditions while a backup SC is considered for each SC in the case of failure.

Another reliable approach for increasing availability is to recover the failed component as quickly as possible without reserving extra resources. In [39], the VNF placement and chaining are initially protected through a decision tree approach, reducing the complexity compared to the existing approaches. Moreover, using a decision tree eases the search process for a replacement of a failure through a reliable algorithm called R-SFC-MCTS [39]. The proposed recovery algorithm initially chooses reliable components to avoid failure and re-map to a fault-tolerant one if a failure happens. The reported results confirm a higher acceptance rate while decreasing the penalties. Failure recovery approaches are categorized into proactive failure recovery (PFR) and reactive failure recovery (RFR) schemes [40–42]. In PFR, an algorithm predicts the chance of failure and starts the recovery procedure to reduce the recovery time. On the other hand, RFR approaches initiate the recovery process when a failure is reported. In [10], a deep reinforcement learning (DRL)-based Proactive Failure Recovery framework named ZT-PFR is proposed to simultaneously reduce the recovery delay and the resource cost. In Table 2, the key features of the protection scheme and recovery plans are presented.

Table 2. Reliable provisioning algorithms strategies.

Protection Scheme	Recovery Plans
Reduce the chance of failure	Re-provision efficiently in case of a failure
Use backup resources	Only use resources if a failure happens
A common approach in provisioning algorithms	Not considered much due to its complexity in provisioning solutions

4.1.2. Evaluation Approaches and Simulation Setup

The existing reliable provisioning algorithms demonstrate their performance by introducing a simulation setup. The simulation setups are usually embraced from the literature for consistent results. However, most existing algorithms consider either different parameters or change the scale of the simulation due to simplicity or as their algorithm is proposed for another scenario. Network topology, number of VNFs per Service Function Chain (SFC), and simulation platform are among the most affecting factors in the performance evaluation of VNF placement and the service function chaining algorithm.

One of the main components of every evaluation is the network topology. Considering a realistic network topology to run the proposed algorithm can ease the prediction of the algorithm's performance in real-life scenarios. However, the network topology can vary depending on the purpose of the algorithm. The ones considered for virtual network function chaining are usually limited to a few models. For instance, the authors in [25] consider DC topologies such as Abilene, ANS, AboveNet, Integra, and BICS, located in Europe, Japan, the United States, and across these regions. In [18], a three-layer fat-tree topology data center architecture is used in the simulation. Moreover, fat-tree topology is also considered in [43–46]. Fat-tree topology is a popular data center model that includes redundant switches, links, and servers. The tree network model (fat-tree) is one of the dominant topologies for service function chain algorithms.

Another common parameter that needs to be defined when evaluating a VNF Chain Placement algorithm is the SFC and the number of the VNFs per SFC. In [10], every considered SFC in the simulation includes three VNFs. The proposed algorithm in [21] also considered three VNFs for each SFC in their simulation. The number of VNFs is randomly selected for each SFC in [25] and is considered between one and seven. In another algorithm, from two to six VNFs are considered in an SFC where every VNF provides one network function. In [46], every SFC includes from two to four VNFs. Each of these VNFs is usually chosen randomly from a list of different types VNFs such as Firewall, Load Balancer (LB), and Network Address Translation (NAT).

One of the main components of the simulation setup is the simulation platform. The simulation has filled the algorithms' evaluation process gap for researchers as it is a cost-efficient approach, less complicated, and independent of the environment's performance characters in comparison to large-scale test-beds [47]. The simulations are used to create a close-to-real-scenario environment to predict and evaluate the performance of an algorithm in a real-life scenario [48]. Depending on its existing features and characteristics, every simulation platform presents a limited version of the real-life scenario. Therefore, depending on those limitations, the achieved results of the same algorithm can vary under different simulation platforms. For example, an algorithm that is simulated through Matlab can present a different result when simulated using Python. It is not always the case where results have a huge difference but mostly a slight difference or another behavior depending on the simulation environment and its features. Therefore, when comparing the performance of various algorithms, it is necessary to consider the same platform.

Different simulation platforms are used for provisioning algorithms. In [10], the Networkx library in Python is used for simulation. In [18], the fat-tree network topology is implemented based on Alevin [16], and the provisioning algorithm is simulated in Java.

In [22], a discrete dynamic even-driven simulator in C++ is developed to evaluate their proposed algorithm. In [25], a Python-based simulator that includes the Pytorch library is used to evaluate the performance of their algorithm. In Table 3, the simulation setups of three reliable provisioning algorithms are shown.

Table 3. Simulation Setup.

Algorithm	Simulation Platform	Network Topology	Number of VNFs Per SFC
JPV-ABA [18]	Java(Alevin)	Tree Topology	2–6 VNFs
P-E2E [22]	C++	Optical metro Topology	2–5 VNFs
DDQP [25]	Python	Abilene, ANS, AboveNet, Integra, and BICS DC topologies	1–7 VNFs

4.2. Different Algorithms to Provide a Reliable Provisioning

4.2.1. Failure Type

There are several points of failure in an NFV environment. Failures can occur at a VNF level or at a link level. Different approaches and algorithms provide a reliable NFV environment depending on which type of failure it accommodates. The proposals can even simultaneously provide for both VNF and link failure.

For VNF failures, a common way to handle failure is to use backup VNFs. In [25], deep reinforcement learning was used to automatically deploy active and standby backup VNFs to increase the fault tolerance. They use several backup schemes ranging from level 0, with no backups, to level 4, which reserves resources for backup in advance. In [10], a deep reinforcement learning approach is proposed. However, it is a proactive backup approach. It can predict the next VNF failure and limit the overall recovery delay. In [21], a SFC routing based on the K-node disjoint shortest path and VNF deployment is proposed. It is a heuristic algorithm that aims to minimize computing and network resource consumption. In [19], replicas are used that are different from backups. The replicas are smaller instances of a VNF, and a pool of replicas can collectively process the same amount of traffic as the original VNF. Other protection strategies are introduced in [22], including Virtual-Node protection, Virtual-Link protection, and End-to-End protection, where VNFs are instantiated in two different physical locations to improve the resiliency against single-node failures.

For link failures, the methods for increasing fault tolerance are different. In [20], they propose using multi-path protection instead of conventional single-path protection. When data are transmitted through several link disjoint paths, a failure in one path does not cause the interruption of the service. In [39], the authors propose a decision tree approach based on the Monte-Carlo Tree Search strategy. The algorithm would select and assign reliable paths to prevent and reactively re-map the impacted virtual links to more stable physical paths to avoid outages due to link failures. In [22], the authors also propose a Virtual-Link protection. Each virtual link connecting two VNFs is mapped and embedded through two disjoint physical paths. One is a primary path and the other is a backup path.

Some papers propose solutions that can handle both VNF and link failures. In [22], they propose strategies for VNF and link failures. The authors also propose an End-to-End protection strategy that increases the resiliency for both VNF and link failure. This strategy is the combination of the two previous strategies where there are backup VNFs on different physical nodes and backup links different from the primary one that connects the backup VNFs together. In [18], the authors propose to use a Joint Path-VNF backup model combining both path backup and VNF backup in a joint way. They also used the Affinity-Based Algorithm to reduce the physical link consumption when mapping VNFs. In Table 4, different types of failure for the mentioned algorithms are presented.

Table 4. Different types of failure in reliable provisioning algorithms.

Algorithm	VNF Failure	Link Failure
ZT-PFR [10]	✓	
JPV-ABA [18]	✓	✓
P-E2E [22]	✓	✓
DDQP [25]	✓	
MP-VPS [20]		✓
CS-VA [49]		✓
Proposed algorithm [21]	✓	
BS-PUSH-BS-Pull [42]	✓	
N+P [19]	✓	
EVNFO [24]		✓
Proposed algorithm [50]		✓

4.2.2. Occurrence of the Failure

Real-world applications are prone to failure. Failures occur once or multiple times at different points of the algorithm execution or at the same time, depending on the application and its components. However, the algorithms that were proposed can either handle single or multiple failures. The solutions that handle a single failure are the first step in providing a resilient NFV environment. Extending the solution to handle multiple failures is ideal because it is closer to the real-world implementation of VNF-enabled networks.

In [22], the algorithm accommodates both VNF and link failure. Despite being able to handle both types of failure, the algorithm only protects against single failures. The algorithm in [20] uses multiple disjoint paths but can only handle single link failure. However, using multiple paths will improve network performance in terms of blocking probability and spectrum efficiency. The authors in [19] used replicas to replace a single VNF handling a failure by increasing its resiliency. In [21], the algorithm's main goal is to handle multiple failures. The authors consider failure multiplicity, in other words, multiple simultaneous failures. The drawback is that the proposed solution has high resource consumption compared to other algorithms mentioned in the paper. This is the main point of improvement for future work. In [18], the authors consider the Mean Time Between failures (MTBF). They used a three-year event log of realistic real-world failures. Their approach is to have both backup nodes and links to be able to handle multiple failures. In [39], the authors focus mainly on multiple link failures. Similar to the previous paper, they also used MTBF as part of the algorithm to predict failures. The solution differs from the two previous papers because it is a recovery algorithm. In [10], deep reinforcement learning was used to handle multiple VNF failures. It is a proactive approach that can predict failures and significantly help meet the SLA. In Figure 4, the discussed algorithms are categorized based on the considered number of failure occurrences in their approach.

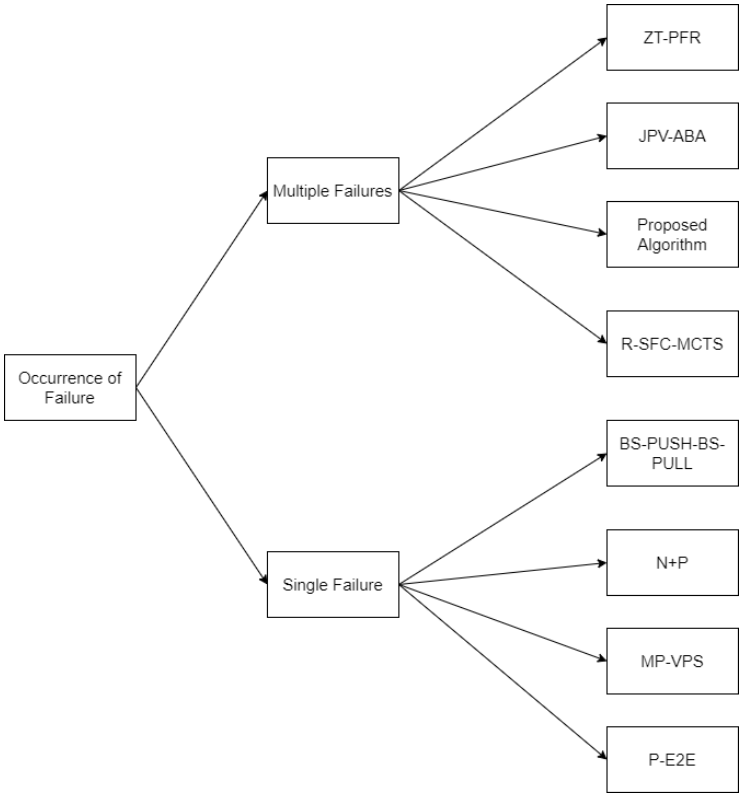


Figure 4. Occurrence of failure in provisioning algorithms.

5. Discussion

Network Function Virtualization separates network functions from the hardware that improves the CAPEX and OPEX. However, since network functions are defined in the software, they are more prone to bugs and failures. Therefore, providing more reliable provisioning algorithms becomes more challenging. The algorithms discussed in this paper provide resilient NFV through various reliable provisioning approaches. We defined various criteria to evaluate the reliable provisioning algorithms. These criteria represent the most common features that can categorize these algorithms and evaluate them through a consistent assessment. In Table 5, all discussed attributes are mentioned along with the relevant research questions that each explored.

5.1. Protection Scheme or Recovery Plans

The main difference between the reliable provisioning algorithms is their approach to providing a reliable algorithm. Some algorithms rely on avoiding failure by proposing a protection scheme [18,37,38] to increase the service availability, while others focus on recovery plans to deliver the service at the earliest point without increasing the resource usage and overhead for the network [10,39]. In protection schemes, backup VNFs or links are considered to be active when a failure occurs, increasing resource usage. On the other hand, recovery plans are proposed to be used when a failure happens without considering extra resources. In comparison to protection schemes, they create a balance between the resource usage and service availability. Therefore, where service availability is crucial, protection schemes could be a better solution, and, in scenarios where resource usage is important, recovery plans could be used. Although there are many existing algorithms with each of these approaches, there is limited research on recovery plans, especially where only the failed link or VNF will be re-routed without re-routing the whole SFC. Moreover, the solutions that consider both protection and recovery at the same time to increase service availability and reduce resource usage at the same time are insignificant. Hence, future studies can focus on reducing resource usage while providing higher service availability.

Table 5. Classification and contribution to review.

Attribute	Related RQ
Reliable Provisioning	1
Protection Scheme	1, 2
Recovery Plan	1, 2
Simulation Comparison Criteria	1
Network Topology	1
Number of VNFs	1
Simulation Platform	1
Failure Type	2
Link Failure	2
VNF Failure	2
Single Failure	2
Multiple Failure	2

5.2. Failure Type

The reliable provisioning algorithm can be categorized by the type of failure they consider and the number of occurrences of those failures. Many reliable provisioning algorithms consider only VNF failure while others study link failure solely or consider both VNF and link failures. Furthermore, the assumed number of failure occurrences can vary for each of these algorithms. Generally, algorithms consider a single failure to be able to build their reliable algorithm with less complications. However, failure is unpredictable and can occur multiple times. Therefore, recently, more researchers have been studying reliable provisioning algorithms that can address multiple failures. However, there is still a gap for a comprehensive approach that manages multiple types of failure.

6. Conclusions

Network Function Virtualization (NFV) enables telecommunications service providers to reduce their costs while providing more flexible solutions. The diversity that the NFV offers by deploying the Virtual Network Functions instead of the dedicated hardware devices allows for a reduction in operational expenditure (OpEx) and capital expenditure (CapEx). Network services are deployed as Service Function Chains (SFCs) in this infrastructure where each SFC includes a set of VNFs. Although the software-based infrastructure results in a cost-efficient and more flexible approach, the failure of a single or multiple VNFs utilizing the computing and network resource usage are among critical issues. In this study, we reviewed relevant research papers on reliable provisioning for VNF chaining through the Systematic Literature Review (SLR) protocol. We categorized the proposed algorithms based on the considered strategy, evaluation approaches, failure type, and occurrence of the failure and studied the advantages and disadvantages of each category. The most considered strategy for a reliable provisioning in NFV is the protection schemes, where the higher availability of a service is achieved by using more resources. In addition, many algorithms only consider one type of a failure or a single failure through the network, which is not a realistic scenario. Moreover, evaluation of the algorithms in different simulation settings is not possible and a common assessment setting is required for precise evaluation. Therefore, there is still a demand for a reliable, realistic, scalable, and cost-efficient provisioning algorithm for VNF placement in real-life scenarios.

Author Contributions: Conceptualization, M.S.G.; methodology, M.S.G. and V.P.; software, M.S.G., V.P. and L.D.L.; validation, M.S.G., V.P. and L.D.L.; formal analysis, M.S.G. and V.P.; investigation, M.S.G., V.P. and L.D.L.; resources, M.S.G., L.D.L. and V.P.; data curation, M.S.G. and L.D.L.; writing—original draft preparation, M.S.G. and L.D.L; writing—review and editing, M.S.G. and V.P.; visualization, L.D.L. and V.P.; supervision, M.S.G. and V.P.; project administration, M.S.G. and V.P.; funding acquisition, V.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Mitacs through the Mitacs Accelerate program.

Data Availability Statement: Not applicable.

Acknowledgments: We are grateful to Mitacs and its partner Ciena for creating this opportunity. We extend our gratitude to Patricia Campbell and Computer Science department at Dawson College and special thanks to Joel Trudeau, DawsonAI Project Lead whose support made this research possible.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kibalya, G.; Serrat, J.; Gorricho, J.L.; Bujjingo, D.G.; Sserugunda, J.; Zhang, P. A reinforcement learning approach for placement of stateful virtualized network functions. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 18–20 May 2021; pp. 672–676.
2. Grinberg, S.; Weiss, S. Architectural virtualization extensions: A systems perspective. *Comput. Sci. Rev.* **2012**, *6*, 209–224. [CrossRef]
3. Kuribayashi, S.I. Allocation of Virtual Cache & Virtual WAN Accelerator Functions for Cost-Effective Content Delivery Services. In Proceedings of the 2019 XXVII International Conference on Information, Communication and Automation Technologies (ICAT), Sarajevo, Bosnia and Herzegovina, 20–23 October 2019; pp. 1–6. [CrossRef]
4. Kaur, K.; Mangat, V.; Kumar, K. A comprehensive survey of service function chain provisioning approaches in SDN and NFV architecture. *Comput. Sci. Rev.* **2020**, *38*, 100298. [CrossRef]
5. Xing, H.; Zhou, X.; Wang, X.; Luo, S.; Dai, P.; Li, K.; Yang, H. An integer encoding grey wolf optimizer for virtual network function placement. *Appl. Soft Comput.* **2019**, *76*, 575–594. [CrossRef]
6. Naudts, B.; Tavernier, W.; Verbrugge, S.; Colle, D.; Pickavet, M. Deploying SDN and NFV at the speed of innovation: Toward a new bond between standards development organizations, industry fora, and open-source software projects. *IEEE Commun. Mag.* **2016**, *54*, 46–53. [CrossRef]
7. Wang, X.; Xing, H.; Zhan, D.; Luo, S.; Dai, P.; Iqbal, M.A. A two-stage approach for multicast-oriented virtual network function placement. *Appl. Soft Comput.* **2021**, *112*, 107798. [CrossRef]
8. Venâncio, G.; Duarte, E.P., Jr. NHAM: An NFV High Availability Architecture for Building Fault-Tolerant Stateful Virtual Functions and Services. In Proceedings of the LADC'22: The 11th Latin-American Symposium on Dependable Computing, Fortaleza, Brazil, 21–24 November 2022; Association for Computing Machinery: New York, NY, USA, 2023; pp. 35–44. [CrossRef]
9. Asdikian, J.P.H.; Askari, L.; Ayoub, O.; Musumeci, F.; Bregni, S.; Tornatore, M. Availability Evaluation of Service Function Chains Under Different Protection Schemes. In Proceedings of the 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 5–8 September 2022; pp. 244–249.
10. Shaghaghi, A.; Zakeri, A.; Mokari, N.; Javan, M.R.; Behdadfar, M.; Jorswieck, E.A. Proactive and AoI-Aware Failure Recovery for Stateful NFV-Enabled Zero-Touch 6G Networks: Model-Free DRL Approach. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 437–451. [CrossRef]
11. Yamada, D.; Shinomiya, N. Computing and Network Resource Minimization Problem for Service Function Chaining against Multiple VNF Failures. In Proceedings of the TENCON 2019—2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019 ; pp. 1478–1482. [CrossRef]
12. Hmaity, A.; Savi, M.; Musumeci, F.; Tornatore, M.; Pattavina, A. Protection strategies for virtual network functions placement and service chains provisioning. *Networks* **2017**, *70*, 373–387. [CrossRef]
13. Kibalya, G.; Serrat-Fernandez, J.; Gorricho, J.L.; Bujjingo, D.G.; Serugunda, J. A multi-stage graph aided algorithm for distributed service function chain provisioning across multiple domains. *IEEE Access* **2021**, *9*, 114884–114904. [CrossRef]
14. Mechtri, M.; Ghribi, C.; Soualah, O.; Zeghlache, D. Etso: End-to-end sfc orchestration framework. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 903–904.
15. Mechtri, M.; Ghribi, C.; Soualah, O.; Zeghlache, D. NFV orchestration framework addressing SFC challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–23. [CrossRef]
16. Herrera, J.G.; Botero, J.F. Resource allocation in NFV: A comprehensive survey. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 518–532. [CrossRef]
17. Hmaity, A.; Savi, M.; Musumeci, F.; Tornatore, M.; Pattavina, A. Virtual network function placement for resilient service chain provisioning. In Proceedings of the 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, 13–15 September 2016; pp. 245–252.

18. Wang, M.; Cheng, B.; Chen, J. Joint availability guarantee and resource optimization of virtual network function placement in data center networks. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 821–834. [CrossRef]
19. Alleg, A.; Ahmed, T.; Mosbah, M.; Boutaba, R. Joint diversity and redundancy for resilient service chain provisioning. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1490–1504. [CrossRef]
20. Gao, T.; Li, X.; Zou, W.; Huang, S. Survivable VNF placement and scheduling with multipath protection in elastic optical datacenter networks. In Proceedings of the 2019 Optical Fiber Communications Conference and Exhibition (OFC), San Diego, CA, USA, 3–7 March 2019; pp. 1–3.
21. Yamada, D.; Shinomiya, N. A solving method for computing and network resource minimization problem in service function chain against multiple VNF failures. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019; pp. 30–38.
22. Askari, L.; Tamizi, M.; Ayoub, O.; Tornatore, M. Protection Strategies for Dynamic VNF Placement and Service Chaining. In Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 19–22 July 2021 ; pp. 1–9.
23. Tajiki, M.M.; Shojafar, M.; Akbari, B.; Salsano, S.; Conti, M.; Singhal, M. Joint failure recovery, fault prevention, and energy-efficient resource management for real-time SFC in fog-supported SDN. *Comput. Netw.* **2019**, *162*, 106850. [CrossRef]
24. Gu, Y.; Hu, Y.; Ding, Y.; Lu, J.; Xie, J. Elastic virtual network function orchestration policy based on workload prediction. *IEEE Access* **2019**, *7*, 96868–96878. [CrossRef]
25. Mao, W.; Wang, L.; Zhao, J.; Xu, Y. Online fault-tolerant VNF chain placement: A deep reinforcement learning approach. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–25 June 2020; pp. 163–171.
26. Siasi, N.; Jaesim, A.; Aldalbahi, A.; Ghani, N. Link Failure Recovery in NFV for 5G and Beyond. In Proceedings of the 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 21–23 October 2019; pp. 144–148.
27. Abu-Lebdeh, M.; Naboulsi, D.; Glitho, R.; Tchouati, C.W. On the placement of VNF managers in large-scale and distributed NFV systems. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 875–889. [CrossRef]
28. Chiang, M.J.; Yen, L.H. Distributed approach to adaptive VNF manager placement problem. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–6.
29. IEEEXplore Digital Library. Available online: https://ieeexplore.ieee.org/Xplore/home.jsp (accessed on 11 December 2022).
30. ACM Digital Library. Available online: https://dl.acm.org (accessed on 11 December 2022).
31. Scoups. Available online: https://www.scopus.com/home.uri (accessed on 27 February 2023).
32. Web of Science. Available online: https://wos-journal.com/ (accessed on 27 February 2023).
33. Google Scholar. Available online: https://scholar.google.ca (accessed on 11 December 2022).
34. Deng, L.; Hinton, G.; Kingsbury, B. New types of deep neural network learning for speech recognition and related applications: An overview. In Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–30 May 2013; pp. 8599–8603.
35. Fan, J.; Jiang, M.; Rottenstreich, O.; Zhao, Y.; Guan, T.; Ramesh, R.; Das, S.; Qiao, C. A framework for provisioning availability of NFV in data center networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 2246–2259. [CrossRef]
36. Gill, P.; Jain, N.; Nagappan, N. Understanding network failures in data centers: Measurement, analysis, and implications. In Proceedings of the ACM SIGCOMM 2011 Conference, Toronto, ON, Canada, 15–19 August 2011; pp. 350–361.
37. Kong, J.; Kim, I.; Wang, X.; Zhang, Q.; Cankaya, H.C.; Xie, W.; Ikeuchi, T.; Jue, J.P. Guaranteed-availability network function virtualization with network protection and VNF replication. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
38. Fan, J.; Ye, Z.; Guan, C.; Gao, X.; Ren, K.; Qiao, C. GREP: Guaranteeing reliability with enhanced protection in NFV. In Proceedings of the 2015 ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization, London, UK, 21 August 2015 ; pp. 13–18.
39. Soualah, O.; Mechtri, M.; Ghribi, C.; Zeghlache, D. A link failure recovery algorithm for virtual network function chaining. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017 ; pp. 213–221.
40. Natalino, C.; Coelho, F.; Lacerda, G.; Braga, A.; Wosinska, L.; Monti, P. A proactive restoration strategy for optical cloud networks based on failure predictions. In Proceedings of the 2018 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 1–5 July 2018; pp. 1–5.
41. Huang, H.; Guo, S. Proactive failure recovery for NFV in distributed edge computing. *IEEE Commun. Mag.* **2019**, *57*, 131–137. [CrossRef]
42. Aidi, S.; Zhani, M.F.; Elkhatib, Y. On improving service chains survivability through efficient backup provisioning. In Proceedings of the 2018 14th International Conference on Network and Service Management (CNSM), Rome, Italy, 5–9 November 2018; pp. 108–115.
43. Wang, Z.; Zhang, J.; Huang, T.; Liu, Y. Service function chain composition, placement, and assignment in data centers. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 1638–1650. [CrossRef]
44. Qi, D.; Shen, S.; Wang, G. Towards an efficient VNF placement in network function virtualization. *Comput. Commun.* **2019**, *138*, 81–89. [CrossRef]

45. Zhang, S.; Wang, Y.; Li, W.; Qiu, X. Service failure diagnosis in service function chain. In Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, Republic of Korea, 27–29 September 2017; pp. 70–75. [CrossRef]
46. Aiko, O.; Nakajima, M.; Soejima, Y.; Tahara, M. Reliable design method for service function chaining. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
47. Sun, J.; Wo, T.; Liu, X.; Cheng, R.; Mou, X.; Guo, X.; Cai, H.; Buyya, R. CloudSimSFC: Simulating Service Function chains in Multi-Domain Service Networks. *Simul. Model. Pract. Theory* **2022**, *120*, 102597. [CrossRef]
48. Ingalls, R.G. Introduction to simulation. In Proceedings of the 2011 Winter Simulation Conference (WSC), Phoenix, AZ, USA, 11–14 December 2011; pp. 1374–1388. [CrossRef]
49. Fei, X.; Liu, F.; Xu, H.; Jin, H. Towards load-balanced VNF assignment in geo-distributed NFV infrastructure. In Proceedings of the 2017 IEEE/ACM 25th IWQoS, Vilanova i la Geltru, Spain, 14–16 June 2017.
50. Soualah, O.; Mechtri, M.; Ghribi, C.; Zeghlache, D. A green VNFs placement and chaining algorithm. In Proceedings of the NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; pp. 1–5.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.