Protection Management for Guaranteed User-Driven Virtual Circuit Services in Dynamic Multi-domain Environments: Design Issues and Challenges

Huhnkuk Lim

Fault management of virtualized network environments using user-driven network provisioning systems (NPSs) is crucial for guaranteeing seamless virtual network services irrespective of physical infrastructure impairment. The network service interface (NSI) of the Open Grid Forum reflects the need for a common standard management API for the reservation and provisioning of user-driven virtual circuits (VCs) across global networks. NSI-based NPSs (that is, network service agents) can be used to compose user-driven VCs for mission-critical applications in a dynamic multi-domain. In this article, we first attempt to outline the design issues and challenges faced when attempting to provide mission-critical applications using dynamic VCs with a protection that is both user-driven and trustworthy in a dynamic multi-domain environment, to motivate work in this area of research. We also survey representative works that address inter-domain VC protection and qualitatively evaluate them and current NSI against the issues and challenges.

Keywords: NPS, NSI, VC, NSA, network provisioning system, network service interface, virtual circuit, network service agent, protection management.

Manuscript received May 20, 2014; revised Oct. 2, 2014; accepted Nov. 4, 2014.

This research was funded by the User-driven Research Network Platform Service Development and Deployment project (Grant No.: K-14-L01-C03-S03) by the MSIP (Ministry of Science, ICT & Future Planning), Rep. of Korea, 2014.

Huhnkuk Lim (rooky13@hanmail.net) is with the Department of Networking Service Technology Development, Korea Institute of Science and Technology Information (KISTI), Daejeon, Rep. of Korea.

I. Introduction

Management issues in virtual network resources such as virtual circuits (VCs) are crucial for the proper operation of various network services supported by them [1]–[11]. Among the management issues, fault management of network virtualization environments is crucial for guaranteeing seamless virtual network services, irrespective of physical infrastructure impairments [2]–[11]. In user-driven VC services, a link or node fault in one domain results in end-to-end data plane VC failures within a dynamic multi-domain setup. A rerouting or protection scheme can be considered for fault restoration to reliably support user-driven VC services. A rerouting scheme can be time consuming in a dynamic multi-domain environment, because the availability of backup capacity is known only at the time of the fault. Thus, user-driven disjoint backup VCs should be reserved and provisioned in advance to support a reasonable level of protection in the dynamic multi-domain environment.

The network service interface (NSI) developed by the Open Grid Forum (OGF) underscores the need for a common standard management application programming interface (API) for the reservation, provisioning, modification, release, and termination of user-driven VCs across dynamic global networks [12]. NSI-based network provisioning systems (that is, network service agents (NSAs)) are recognized as extremely useful software to provide mission-critical applications in the dynamic multiple domains with the realistic VC setup

scenarios in a user-driven manner and have been successfully demonstrated in the Automated GLIF Open Lightpath Exchange (GOLE) infrastructure [13]–[16]. NSIs do not currently define protection management issues and challenges to be outlined for guaranteed user-driven VC services in a dynamic multi-domain environment. The works regarding inter-domain VC protection in the static Multiprotocol Labeled Switching (MPLS) and optical networks, which can be operated by an administrator rather than a user, expose limitations to cover the issues and challenges to be outlined for protection management on dynamic user-driven VCs across global networks [6]–[9], [17]. A few of these works have contributed partial efforts to overcome the protection management issues and challenges for guaranteed user-driven VC services in dynamic multiple networks [3], [5]–[6]. Backup VC reservation/provisioning for protection; primary/backup VC status management; VC switching control; topology service for disjoint-path computation; and management messages and their flow mechanisms form the main issues and challenges of a kind of protection management that can be described as being both user-driven and trustworthy in dynamic multi-domain environments. Among the issues and challenges, investigating how management information, such as fault/repair and VC protection/retrieval event information, and transport path coordination information is captured, disseminated, and managed across the domains of interest is a crucial key challenge to support trustworthy protection between domains of interest [3], [5], [7]. Efforts to overcome the issues and challenges in a common standard interface are required to provide the necessary trustworthy protection between dynamic component domains across global networks, in a user-driven manner.

In this article, design issues and challenges on protection management for user-driven VCs in a dynamic multi-domain environment are outlined systematically. We also survey representative works that address inter-domain VC protection and qualitatively evaluate them and the current NSI framework in terms of the issues and challenges.

The remainder of this paper is organized as follows. Section II briefly addresses the preliminaries of the current NSI framework, which reflects a recent and common standard interface that attempts to provide mission-critical applications with user-driven VC services across global networks. Section III outlines design issues and challenges on protection management for guaranteed user-driven VC services in a dynamic multi-domain environment. In Section IV, representative works that address inter-domain VC protection are surveyed. They, along with the current NSI, are then evaluated in terms of the issues and challenges. Finally, Section V presents concluding remarks.

II. Preliminaries

1. NSI Objectives

NSIs reflect a recent and global trend for the reservation, provision, release, modification, and termination of end-to-end user-driven VCs across dynamic multiple domains. The main objective of an NSI is to provide a common standardized interface for global reservation and resource negotiations, which can be easily adopted by already existing provisioning tools and enable automated inter-domain communication of peering control planes.

2. NSI Connection Service

A dedicated NSA manages each provider's network. These agents interact to realize the delivery of a network service supported by the network infrastructure. An NSA can take on the role of a requester, a provider, or both. As a requester, the NSA requests network resources, and as a provider, it delivers network resources to create a service. The NSA acts as both (also known as an aggregator) when it is a requester over one interface while acting as a provider on a different interface. NSI requests can be propagated through this framework of NSAs using a tree or chain workflow. Each NSI message includes a set of attributes, which provides each NSIA with the specific details of the service being requested. An NSI connection service (CS) allows requestors to set up a point-to-point circuit across multiple network domains using the NSI CS protocol's reserve, provision, release, termination, and query request messages. Inter-domain VC connections in NSIs are done by choosing appropriate service termination points (STPs) such that the egress STP of one VC connection (STP b) corresponds directly with the ingress STP of the successive VC connection (STP c), as shown in Fig. 1 [12]. A service demarcation point (SDP) indicates a grouping of two STPs belonging to adjacent domains (see Fig. 1). By using this shared point, SDP, the NSI is able to stitch inter-domain VC connections [12].

3. NSI Connection Management

Figure 1(a) shows an example of a connection managed by an NSA chain workflow. The management of connections within an NSI chain model is simpler and easier compared to that within an NSI tree model. However, an NSI chain model cannot detect the status of the VC control plane in each component domain. Each network is associated with one NSA as an NSA/network pairing. In this case, the NSI message is forwarded between NSAs in the same sequence as that of the connection that is transiting the networks [12]. The NSAs are connected as a chain: Application-NSA to NSA-X and NSA-X

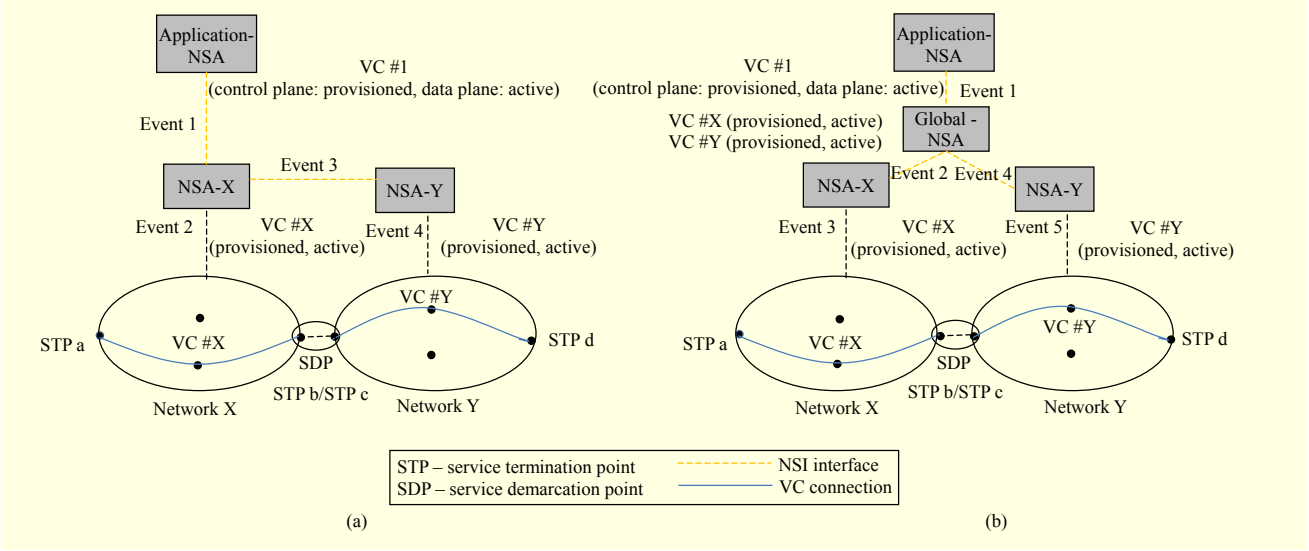

Fig. 1. NSI connection service architecture: (a) chain model and (b) tree model.

to NSA-Y. The Application-NSA gives a connection request to NSA-X, to reserve a connection from STP a to STP d (Event 1 in Fig. 1(a)). Then, NSA-X will look in the topology and determine to make this connection, and it will reserve a local connection from STP a to STP b (Event 2 in Fig. 1(a)), and then forward the request for the remainder of the connection to NSA-Y: STP c to STP d (Event 3 in Fig. 1(a)). NSA-Y receives this request and reserves a connection between STP c and STP d (Event 4).

Figure 1(b) shows an example of a connection managed by an NSA tree workflow. In this case, the NSI message is forwarded between NSAs in a different sequence compared to that of the connection that is transiting the networks. While Aggregator NSA (Global NSA) in the tree model can monitor the status of the VC control plane in each component domain, the tree model is a little more complicated than the chain model in terms of connection management. The NSAs are connected as a tree: Application-NSA to Global-NSA, Global-NSA to NSA-X and Global-NSA to NSA-Y. Assuming a connection request comes from Application-NSA to Global-NSA to reserve a connection from STP a to STP d (Event 1 in Fig. 1(b)), Global-NSA will look in the topology and determine that to make this connection NSA-X will have to reserve a local connection from STP a to STP b (Events 2 and 3 in Fig. 1(b)), and then Global-NSA forwards a request for the remainder of the connection to NSA-Y: STP c to STP d (Events 4 and 5 in Fig. 1(b)) [12]. Global-NSA consequently coordinates VC connection in each component domain across the dynamic multi-domain.

It should be noted that a multi-domain user-driven VC consists of many successive VC segments that are reserved and provisioned by a dedicated NSA in each domain, to provide a realistic end-to-end VC setup in a global network.

III. Design Issues and Challenges

In this section, the design issues and challenges required for providing user-driven and trustworthy protection in a dynamic multi-domain environment were mostly extracted and defined from the surveyed works regarding multi-domain VC protection in Section IV. To the best of our knowledge, all possible design issues and challenges are addressed.

1. Network Issues

A. Protection Capabilities

To allow user-driven protection by a network provisioning system (NPS), network devices must support protection switching capabilities (for example, MPLS, SONET, and so on). User-driven protection means that an NPS should serve a disjoint-path backup VC for protection as well as a primary VC on a user VC service request. For per-domain protection service, any independent protection scheme (for example, 1:1, 1:*N*, *M*:*N*, and 1+1 protection) can be supported within the domain [18]–[19]. However, to allow an end-to-end protection service, all domains must support an interoperable protection switching scheme. In the case of 1:1 protection, a backup path on a disjoint physical path can be used to protect the primary path, in an active/standby configuration. In the case of *M*:*N* protection, *N* primary paths share *M* backup paths [18]–[19]. For 1+1 protection, data traffic is transferred through both primary and backup paths, resulting in an active/active configuration.

B. Detection of Network Fault/Repair Events

Fault signals from network devices need to be sent to an NPS in each domain to report a link or node fault. Use of the Simple Network Management Protocol can be a candidate for the detection of a link or node fault event by a network resource manager (NRM) in an NPS [18]–[19]. For detection of a node repair event, periodic polling messages from an NRM in an NPS to a network node can be used [18]–[19].

2. Network Provisioning System Issues

A. Protection Service Request

A service request should support the selection of protection options by the user; for example, per-domain protection (that is, protection within each domain only) or complete end-to-end protection, and so on. For per-domain protection, domain-specific protection by an NPS can be enabled on a user VC service request.

B. VC Reservation and Provisioning for Protection

As both the primary and backup VCs are treated distinctly, a requester NPS must make consistent requests (for example, a reserve, provision, release, terminate, and modify request in the NSI connection service) for each primary/backup VC independently, which are composed of successive VCs in the dynamic multi-domain environment. Consequently, this issue results in user-driven protection for dynamic multi-domain VCs.

C. Disjoint-Path Computation

An NRM in an NPS should be able to search path-disjoint VCs in each domain for per-domain and end-to-end protection in a dynamic multi-domain environment. For per-domain protection, an NPS needs to find path-disjoint VCs in its domain only. For end-to-end protection, a path computation engine (PCE) in an NPS is needed to reserve path-disjoint diverse VCs based on a user request, using a global network topology view. Existing algorithms regarding disjoint-path computation in IP/MPLS and optical networks that can be operated by an administrator, such as Suurballe's algorithm [20], representatively, can be applied to an NRM.

D. Network Topology Service for Path Computation

Most works regarding inter-domain VC provisioning by an administrator rather than a user have addressed aggregation approaches by PCE-PCE communication to provide path finding in multiple domains [6]–[8]. On the other hand, NSI v2.0 is currently completing on a standard network topology exchange API service between NPSs using the Network Markup Language to support path finding for user-driven VCs in a dynamic multi-domain environment [12]. Using a dynamic topology exchange service of the NSI, end-to-end VC connections with disjoint paths can be more easily supported by NPSs. In the current Automated GOLE infrastructure, a static global topology file is used for path computation of dynamic multi-domain VCs.

E. VC Switching Control

Explicit control over both primary and backup VCs is necessary to maintain consistent control-plane status and manage risk mitigation in a dynamic multi-domain environment. Specifically, when primary VCs have failures due to a network fault in one domain, an NPS should be able to control and manage backup VCs implicitly via user requests [3]. This issue addresses one of the representative reasons that protection should be provided in a user-driven manner for guaranteed user-driven VC services in a dynamic multi-domain environment.

F. Management Messages

The exchange of network fault/repair, VC protection/retrieval success/failure information, and the coordination information of transport paths between NPSs are necessarily required to support trustworthy protection between component domains in a dynamic multi-domain environment. To serve as a partial contribution for this key challenging issue, the work of Lim and Lee [3] addressed an API message strategy to support the monitoring information of network and primary/backup VC state between NPSs. In the work, an *InterfaceDown* API message was used to notify an NSA of a faulty interface on a network device in a domain. An *InterfaceUp* API message was used to notify an NSA of a repaired interface on a network device in a domain. A *NodeDown* API message was used to notify an NSA of a faulty network device in a domain. A *NodeUp* API message was used to notify an NSA of a repaired network device in a domain. The API messages *ProtectionSuccess* and *ProtectionFail* were used to provide notification that backup VCs pre-assigned in backup links or nodes in a domain are currently operating in the active state and at least one backup VC is not operating in the active state, respectively. On the other hand, *RetrievalSuccess* and *RetrievalFail* API messages were used to provide notification that all VCs in a repaired primary link (interfaces) or node in a domain have been restored in the active state and to indicate that at least one VC has not currently been restored in the active state, respectively. Using the API message strategy, monitoring capability between NPSs has been serviced to provide

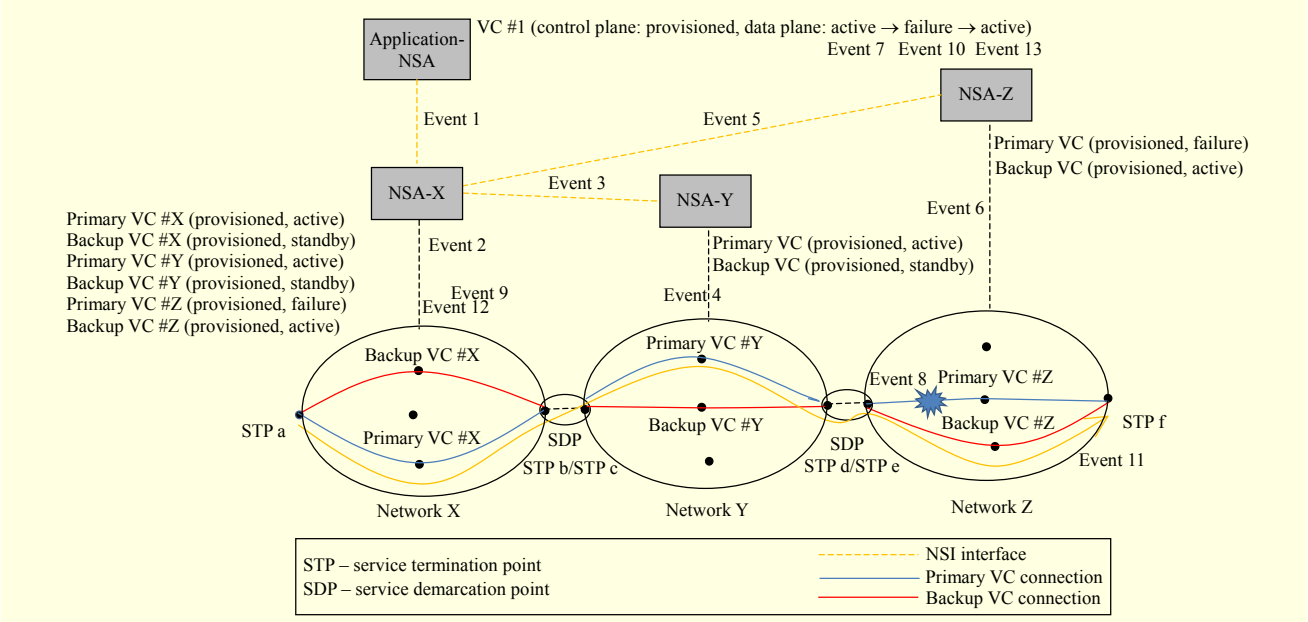

Fig. 2. One per-domain protection management service scenario in dynamic multi-domain environment (1:1 protection scheme in each domain is assumed).

trustworthy protection within a user-driven VC service network [3].

However, it still exposes the limitation to present transport-path coordination information required for the support of end-to-end protection in a dynamic multi-domain environment. Additional API messages to switch transport paths in component domains are required to support end-to-end protection in dynamic multiple networks.

G. Management-Message Flow Mechanism

Due to administrative and scalability reasons, a fault/repair trigger in an intra-domain is not generally disseminated externally. Thus, for the trustworthy protection of a user-driven multi-domain VC composed of successive VCs in component domains, collaboration of management information between NPSs in domains of interest is essential for communicating network and protection events and coordinating transport paths across domains of interest. A chain and tree model for the management-information exchange mechanism can be generally considered. Management-message flow mechanisms between NPSs should be investigated for the support of trustworthy per-domain and complete end-to-end protection, which are representative protection schemes in multiple domains. We address the needs of mechanisms in two general protection service scenarios, based on a common standard interface (that is, an NSI framework).

Figure 2 presents a per-domain protection management service scenario based on a tree model between NPSs with NSI (that is, NSAs) within a dynamic multi-domain framework. A 1:1 protection scheme is assumed in each domain. A disjoint backup VC is reserved and provisioned to protect a primary VC in each network via a per-domain protection service request from an aggregator NSA (Events 2, 3, 4, 5, 6, and 7 in Fig. 2), in response to a per-domain protection service request from STP a to STP f from Application-NSA (Event 1 in Fig. 2). A primary and backup VC in each network use identical SDPs for the inter-domain VC connection to instantiate per-domain protection management service in networks X, Y, and Z. Network Z has a link fault on primary VC #Z causing the Application-NSA to reflect a failure in the VC #1's data plane (Events 8, 9, and 10 in Fig. 2). User traffic on primary VC #Z is switched to the disjoint backup VC #Z due to 1:1 protection in network Z (Event 11 in Fig. 2). NSA-Z needs to notify the aggregator NSA (NSA-X) and Application-NSA of protection success in network Z (events 12 and 13 in Fig. 2). Consequently, investigation of a management-message flow mechanism is required to support a trustworthy per-domain protection management service scenario in a dynamic multi-domain environment.

Figure 3 presents an end-to-end protection management service scenario considering diversity between NPSs with NSI (that is NSAs) within a dynamic multi-domain framework. This scenario provides a 1:1 end-to-end protection scheme across the multi-domain VC. The initial request by Application-NSA for an end-to-end protected VC between STP a and STP j results in the reservation and provisioning of backup VC #1 across the domains of interest coordinated by aggregator NSA-X (Events 1, 2, 3, 4, 5, and 6 in Fig. 3). In this scenario, it is assumed that

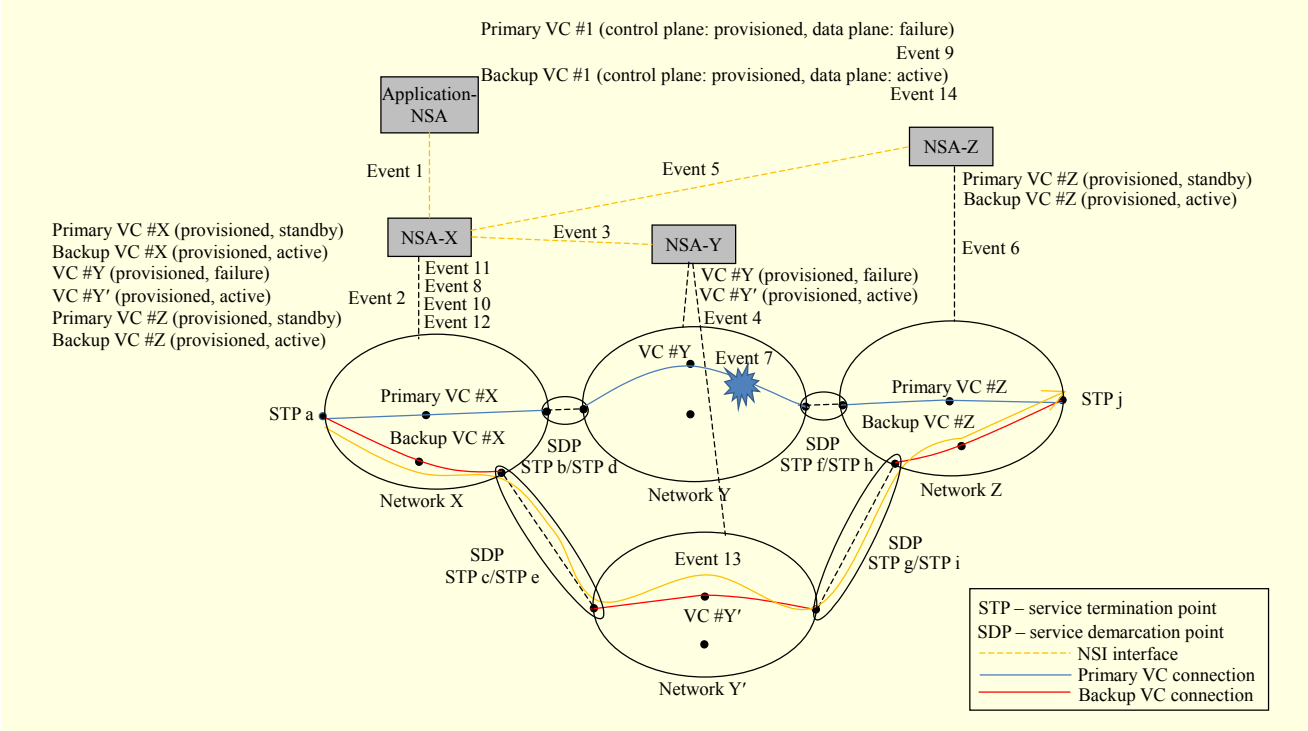

Fig. 3. One end-to-end protection management service scenario in dynamic multi-domain environment (1:1 end-to-end protection is assumed in each domain).

NSA-Y controls two domains (Network Y and Network Y′) and that VC #Y′ has been reserved and provisioned to support a diverse end-to-end backup path. When Network Y has a link fault (Event 7 in Fig. 3), it triggers a failure on the primary VC #1 for the Application-NSA (Events 8 and 9 in Fig. 3). For the end-to-end protection management, NSA-Y needs to notify NSA-X (aggregator NSA) and Application-NSA of a link fault in Network Y (Events 11 and 12 in Fig. 3), followed by a request to activate the path in the VC #Y′. If VC #Y′ reports an active state in Network Y′ (Event 10 in Fig. 3), then NSA-Y needs to notify NSA-X of a protection success on VC #Y′ in Network-Y′ (Events 11 and 12 in Fig. 3). Consequently, NSA-X needs to instruct its network devices to switch a transport path in its network domain. In addition, NSA-X needs to inform NSA-Z to switch a transport path in its network domain and notify Application-NSA of protection success in all network domains (Events 10, 11, and 12 in Fig. 3). Consequently, user traffic on the primary VC #1 for Application-NSA should then be switched to the backup VC #1 (Events 13 and 14 in Fig. 3). Investigation of a management-message flow mechanism is crucial for supporting the end-to-end protection management service scenario depicted as an example in Fig. 3. In the flow mechanism, how to minimize the processing time of messages to switch transport paths across domains of interest forms a challenge in NPSs.

H. Primary/Backup VC Reservation Table Management

A VC reservation table must manage both the data plane status and the control plane status of the primary/backup VCs. The data plane status information of the primary and backup VCs can be provided by management messages for trustworthy protection across domains of interest [3]. This issue is essential for supporting protection of dynamic multi-domain VCs in a user-driven manner. Primary/backup VC reservation table management with data/control plane status enables a user to control each VC tentatively via user VC service requests.

I. Multi-layer Protection

The use of multi-layer VCs can offer several benefits, such as the offloading of traffic from higher network layers (for example, layer 3) to lower ones (for example, layer 1) when there is a large data flow, and flexible VC services in heterogeneous networks [4]. The use of lower-network-layer VCs reduces the number of interfaces/devices the traffic flow must traverse, which leads to cheaper operational cost. However, multi-layer VCs make multi-layer protection difficult, as it may not be easy to determine which layer of protection offers the best cost–benefit tradeoff. Existing path computation algorithms [17] that have considered multi-layers to provide inter-domain VC provisioning in IP/MPLS and

Table 1. Comparison between representative inter-domain VC protection works and current NSI in terms of protection management issues and challenges for guaranteed user-driven VC services in a dynamic multi-domain environment.

Protection management issues and challenges on dynamic user-driven VCs	Standard (NSI v2.0)	Monga et al.	Lim and Lee	Contreras et al.	Douville et al.	Yannuzzi et al.	Sprintson et al.
User-driven protection (protection service request and VC reservation/ provisioning for protection)	Not defined yet	User-driven protection issues are addressed but not implemented.	User-driven primary/backup VC reservation and provision are implemented.	Not a user-driven protection, but depends on control plane	It depends on control plane for provisioning only.	It depends on control plane for provisioning only.	It depends on control plane for provisioning only.
Protection capability	Protection capability is recommended in each domain but currently not required.	Per-domain protection in a production network	Per-domain protection in a production network	End-to-end protection is implicitly addressed in a prototype test-bed.	End-to-end protection with ISP alliance between three domains	Per-domain protection in IP/MPLS networks	End-to-end protection with peering between multiple IP/MPLS domains
Management messages	*errorEvent* API message can be a candidate for network fault and protection failure notification only.	Issues are addressed but not implemented yet.	API messages for the monitoring of network and VC state were implemented but it needs to be extended.	No	NOK message from local NMS to SA, in the case of a protection failure in multi-domain	No	No
Management-message flow mechanism between NPSs in component domains	Not mentioned	Need of management-information flow mechanism is mentioned.	Management API message flow mechanism for per-domain protection is implemented.	No	No	Need of it for mission-critical applications is mentioned.	No
VC switching control	Not defined yet	No	Yes	No	No	No	No
VC reservation table management with data plane status of VCs	Yes, but it has a limitation to express standby state.	Issues are addressed but not implemented yet	Yes	No	No	No	No
Multi-layer protection	Not defined yet	No	Layers 2–3 only	Coordinated protection for layers 1 and 3	It is implicitly addressed based on GMPLS-TE technology.	Layers 2–3 only	Layers 2–3 only
Disjoint path computation algorithm	NSI recommends that aggregator NPS is responsible for path finding in multi-domain.	Not mentioned	Differentiated links for a primary/backup path are used	Algorithm is not mentioned in PCE.	Algorithm is not mentioned in PCE.	Not mentioned	Distributed routing algorithm decoupled from the BGF protocol that can be employed to PCE.
Network topology service for disjoint-path computation within multi-domain	NSI is currently completing a standard work for it.	PCE aggregation approach	No	PCE aggregation approach	PCE-PCE communication protocol	PCE-PCE communication protocol	PCE-PCE communication protocol

optical networks can be applied to an NRM in a global NPS.

Finally, a block diagram is shown in Fig. 4 to integrate the issues and challenges faced in attempting to provide a user-driven and trustworthy protection management in a dynamic multi-domain environment.

3. Discussion

Outlined protection management issues and challenges must be integrated into the workflow to support data plane resiliency for user-driven VCs in a dynamic multi-domain environment. Although protection capability depends on the control plane of

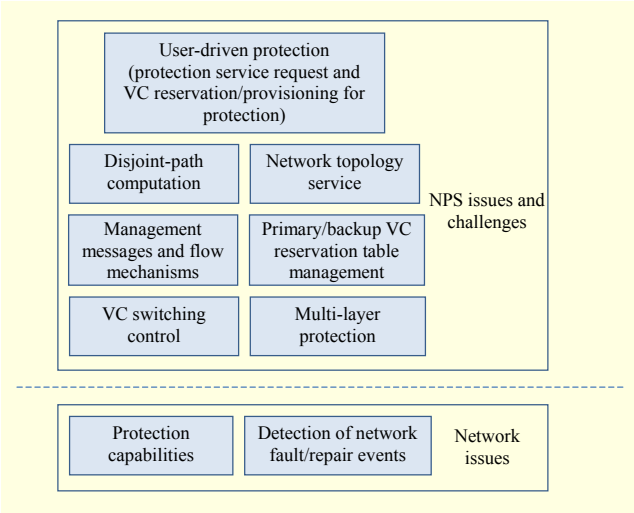

Fig. 4. Block diagram to integrate the issues and challenges faced in attempting to provide user-driven and trustworthy protection management in a dynamic multi-domain environment.

each component domain, the management issues and challenges of networks and NPSs should be overcome to provide user-driven and trustworthy protection in a dynamic multi-domain environment. In particular, the design of management messages and investigation of exchange mechanisms between NPSs are key challenges for both the monitoring of network topology and primary/backup VC state change due to a fault/repair in a component domain and the coordination of transport paths in component domains. It should be noted that a primary/backup VC may not operate as expected due to unforeseen circumstances, such as unintentional configuration changes made by a third party faults in local network devices, and unrecoverable faults in other domains.

Two general protection scenarios (per-domain and end-to-end protection) are possible within a realistic multi-domain VC setup in a user-driven manner. However, end-to-end protection is relatively difficult to set up because it requires the switching of transport paths in multiple domains in the case of a fault in one domain. It also leads to higher switchover times, as a fault/transport path–coordination information trigger has to traverse multiple domains to switch over at each domain. A management API message capability between NPSs in dynamic component domains can be a candidate for the communication of protection management information. The NSI API reflects a recent and common standard interface for user-driven VC services across global networks. The design of protection management messages in a common standard interface such as NSI can be a good method to realize a user-driven and trustworthy protection between component domains in a dynamic multi-domain environment.

IV. Survey on Related Efforts

1. Related Efforts

Representative works on multi-domain VC protection in conventional VC networks (IP/MPLS and optical networks) and a few works on representing user-driven or trustworthy VC protection were selected to address comprehensive works on multi-domain VC protection in this section.

Table 1 provides a qualitative comparison between representative works on inter-domain VC protection and the current NSI in terms of the issues and challenges outlined for protection management on user-driven VCs in a dynamic multi-domain environment. It should be noted that an NSI is the best standardization interface that can allow a user-driven and trustworthy protection management across dynamic multiple domains.

The work of Lim and Lee [3] represented a working example to show how a user-driven protection service can be implemented based on an NSI framework, whereas most other works have mainly addressed administrator-driven inter-domain VC protection provided by control planes only in IP/MPLS and optical networks [4], [6]–[8]. It should be noted that protection management for user-driven VCs for mission-critical applications should be provided in a user-driven manner [5]. That is, a user rather than an administrator should be able to control and monitor both backup VCs and primary VCs. In an effort to overcome it in a common standard interface, Network Service Interface Working Group is going to start management standardization for user-driven protection in a dynamic multi-domain environment.

Contreras and others [4] implicitly addressed an end-to-end protection capability using PCE aggregation in a prototype testbed by an administrator, whereas NSI recommends, but does not currently require, domain protection capabilities. The works of Monga and others [5] and Lim and Lee [3], however, do address per-domain protection capability in production networks by a user rather than an administrator. The works of Douville and others [6] and Sprintson and others [8] addressed end-to-end protection with ISP alliance (peering) in static multiple domains by an administrator. However, those are not realistic scenarios to provide mission-critical applications with dynamic inter-domain VC protection in a user-driven manner. On the other hand, Yannuzzi and others [7] addressed a per-domain protection that is responsible for its corresponding segment of an end-to-end VC path by an administrator.

For management messages to provide a trustworthy protection service between domains of interest, an *errorEvent* API message defined in an NSI can be a candidate for network fault and protection failure notification only. Attribute information for network and protection failure events should be

defined in an *errorEvent* message. However, this cannot fully cover information required for per-domain and end-to-end protection management between NPSs in a dynamic multi-domain VC scenario. Lim and Lee [3] proposed an API message strategy for notification between NPSs. However, to support a user-driven end-to-end protection service in a dynamic multi-domain environment, additional messages for the coordination of transport paths must be defined. The works of Douville and others [6] and Sprintson and others [8] implicitly address the exchange of a fault trigger between control planes based on ISP alliance in multiple domains, even though those are not realistic inter-domain VC protection methods for user-driven VCs across dynamic multiple networks. On the other hand, the work of Douville and others [6] addresses the use of an NOK message from a network management system (NMS) in a source domain to a central service agent (SA) for an administrator, in the event of a protection failure in a source domain. In addition the work of Monga and others [5] mentioned the need for a fault trigger and transport path coordination information exchange between component domains to provide end-to-end protection at the application level for dynamic user-driven VCs.

For the management-message flow mechanism issue between NPSs, Lim and Lee [3] proposed an API-message flow mechanism that can be used for the exchange of network and VC state monitoring information between NPSs for per-domain protection. However, it still does not address an end-to-end management flow mechanism required for the switching of a transport path in each domain. The works of Monga and others [5] and Yannuzzi and others [7] also mentioned the need for a management-message flow mechanism between domains of interest to support the prompt switching of an end-to-end transport path for mission-critical applications.

Lim and Lee [3] addressed the issue of how backup VCs can be controlled based on primary/backup VC data plane status management. In the case where primary VCs have failures due to a network fault and a network operator requires a long time for their repair, an NPS could be able to control backup VCs implicitly via user requests, based on primary/backup VC data plane status management. Although an NSI also provides end-to-end VC data plane status management, it lacks the ability to fully express additional data plane status, such as the standby state [12]. Both control plane and data plane status management of primary/backup VCs are essential for providing mission-critical applications with protection management in a user-driven manner. The works that have addressed inter-domain VC protection in the static IP/MPLS and optical networks by an administrator expose the limitation to control backup VCs, due to the dependency on control planes only for protection [4], [6]–[9].

The study of Contreras and others [4] offered multi-layer coordinated recovery in a prototype testbed, using a multi-layer network control strategy to offload traffic from layer 3 to layer 1 of the network under high traffic load situations, whereas the works of Lim and Lee [3], Yannuzzi and others [7], Sprintson and others [8], and the current NSI did not address this. On the other hand, the work in Douville and others [6] implicitly addressed multi-layer protection based on GMPLS-TE technology.

For disjoint-path computation, the work of Sprintson and others [8] addressed a distributed routing algorithm decoupled from the BGF protocol that can be employed to PCE in a static multi-domain environment, while other works did not mention a specific algorithm in PCE.

Contreras and others [4] and Monga and others [5] addressed path-finding approaches by using PCE aggregation in a multi-domain environment, whereas the work reported in Lim and Lee [3] did not address end-to-end disjoint paths because of the lack of a global network topology service in the NSI. Similarly, the works of Douville and others [6]; Yannuzzi and others [7]; and Sprintson and others [8] addressed disjoint-path-finding approaches by a PCE-PCE communication protocol. On the other hand, NSI is currently completing work to provide a standard network topology exchange service between NPSs so as to be able to support end-to-end multi-domain path finding for user-driven VC services in dynamic multiple networks.

2. Discussion

Only a few of the works regarding user-driven VC services have partially addressed protection management issues and challenges to overcome physical layer impairment in a dynamic multi-domain environment [3], [5]. Most of the works regarding inter-domain VC protection in IP/MPLS and optical networks by an administrator rather than a user have mainly focused on issues such as disjoint-path finding and multi-layer protection under the assumption of interoperable control planes by static ISP alliance in multiple domains [4], [6]–[9], [17]. However the aforementioned works are limited in that they fail to fully cover the issues and challenges to support dynamic VC protection service scenarios for mission-critical applications across global networks. Although NPSs, such as UCLP, Dragon, DRAC, and OpenNSA, have represented user-driven VC services, they have not addressed user-driven and trustworthy protection management due to the use of a VC protection that is dependent on only control planes, which were generally used in static conventional VC networks (IP/MPLS and optical networks) [16]. The works of Douville and others [6] and Yannuzzi and others [7] have presented the need for trustworthy protection for inter-domain VC provisioning,

even when administrator-driven inter-domain VC provisioning was done by a control plane in a static multi-domain environment. The works of Lim and Lee [3] and Douville and others [6] have represented implementation cases to reflect an API message strategy for the monitoring of network and VC states in component domains. These days, current solutions have begun to address those aforementioned partial efforts that attempted to provide user-driven and trustworthy protection in a dynamic multi-domain environment. The issues and challenges that were not properly covered by each of the aforementioned solutions are summarized in Table 1. A common standard interface, such as an NSI, can be a good tool to realize trustworthy protection service scenarios for user-driven VCs in a dynamic multi-domain environment if it overcomes the issues and challenges.

V. Concluding Remarks

In this paper, we outlined protection management issues and challenges for guaranteed user-driven VC services in a dynamic multi-domain environment, which must be integrated into the workflow to support a user-driven and trustworthy protection. Representative works regarding inter-domain VC protection in a multi-domain environment were surveyed and qualitatively evaluated in terms of the outlined issues and challenges. These works were limited in that they failed to fully cover the protection management issues and challenges outlined for guaranteed user-driven VCs in dynamic heterogeneous networks. A few of the works regarding user-driven VC services have partially contributed to the issues and challenges for guaranteed VC services in a dynamic multi-domain environment. The current NSI reflects a recent and common standard interface for user-driven VC services across a dynamic multi-domain environment but lacks the capability to support user-driven protection management in the face of physical layer impairments. The design of management messages and the implementation of a management-message flow mechanism in a common standard interface are crucial challenges to be overcome in the drive toward providing a trustworthy protection service between domains of interest for dynamic user-driven VCs.

References

[1] R. Esteves, L. Granville, and R. Boutaba, "On the Management of Virtual Networks," *IEEE Commun. Mag.*, vol. 51, no. 7, July 2013, pp. 80–88.

[2] S. Peng, R. Nejabati, and D. Simeonidou, "Impairment-Aware Optical Network Virtualization in Single-Line-Rate and Mixed-Line-Rate WDM Networks," *J. Opt. Commun. Netw.*, vol. 5, no. 4, Apr. 2013, pp. 283–293.

[3] H. Lim and Y. Lee, "Toward Reliability Guarantee VC Services in an Advance Reservation Based Network Resource Provisioning System," *Int. Conf. Syst. Netw. Commun.*, Venice, Italy, Oct. 27–31, 2013, pp. 112–120.

[4] L.M. Contreras et al., "Toward Cloud-Ready Transport Networks," *IEEE Commun. Mag.*, vol. 50, no. 9, Sept. 2012, pp. 48–55.

[5] I. Monga et al., "Hybrid Networks: Lessons Learned and Future Challenges Based on ESnet4 Experience," *IEEE Commun. Mag.*, vol. 49, no. 5, May 2011, pp. 114–121.

[6] R. Douville et al., "A Service Plane over the PCE Architecture for Automatic Multidomain Connection-Oriented Services," *IEEE Commun. Mag.*, vol. 46, no. 6, June 2008, pp. 94–102.

[7] M. Yannuzzi et al., "On the Challenges of Establishing Disjoint QoS IP/MPLS Paths across Multiple Domains," *IEEE Commun. Mag.*, vol. 44, no. 12, Dec. 2006, pp. 60–66.

[8] A. Sprintson et al., "Reliable Routing with QoS Guarantees for Multi-domain IP/MPLS Networks," *IEEE INFOCOM*, Anchorage, AK, USA, May 6–12, 2007, pp. 1820–1828.

[9] C. Huang and D. Messier, "A Fast and Scalable Inter-Domain MPLS Protection Mechanism," *J. Commun. Netw.*, vol. 6, no. 1, Mar. 2004, pp. 66–67.

[10] I. Houidi et al., "Adaptive Virtual Network Provisioning," *ACM SIGCOMM Workshop Virtualized Infrastructure Syst. Archit.*, New Delhi, India, Sept. 3, 2010, pp. 41–48.

[11] H. Yu et al., "Migration Based Protection for Virtual Infrastructure Survivability for Link Failure," *OFC/NFOEC*, Los Angeles, CA, USA, Mar. 6–10, 2011, pp. 1–3.

[12] GFD-173, *NSI Connection Service Protocol v2.0*, OGF NSI-WG, UK, Feb. 2013.

[13] Z. Zhao et al., "Planning Data Intensive Workflows on Inter-Domain Resources Using the Network Service Interface (NSI)," *SC Companion: High Performance Comput., Netw. Storage Anal.*, Salt Lake City, UT, USA, Nov. 10–16, 2012, pp. 150–156.

[14] R. Krzywania et al., "Network Service Interface: Gateway for Future Network Services," *Terena Netw. Conf.*, Reykjavík, Iceland, May 21–24, 2012, pp. 1–15.

[15] C.P. Guok et al., "A User Driven Dynamic Circuit Network Implementation," *IEEE Globe Commun.*, New Orleans, LO, USA, Nov. 30–Dec. 4, 2008, pp. 1–6.

[16] N. Charbonneau et al., "Advance Reservation Frameworks in Hybrid IP-WDM Networks," *IEEE Commun. Mag.*, vol. 49, no. 5, May 2011, pp. 132–139.

[17] A. Urra et al., "An Enhanced Dynamic Multilayer Routing for Networks with Protection Requirements," *J. Commun. Netw.*, vol. 9, no. 4, Dec. 2007, pp. 377–382.

[18] R. Hughes-Jones et al., "Network Performance Monitoring, Fault Detection, Recovery, and Restoration," in *Grid Networks*, USA: Wiley, 2006, pp. 253–275.

[19] K. Ogaki et al., "Prototype Demonstration of Integrating MPLS/GMPLS Network Operation and Management System," *Opt. Fiber. Commun.*, Anaheim, CA, USA, Mar. 5–10, 2006, pp. 1–8.

[20] M. German et al., "On the Challenges of Finding Two Link-Disjoint Lightpaths of Minimum Total Weight across an Optical Network," *European Conf. Netw. Opt. Commun.*, Valladolid, Spain, June 10–12, 2009, pp. 217–224.

Huhnkuk Lim received his PhD degree in information and communications from the Gwangju Institute of Science and Technology (GIST), Gwangju, Rep. of Korea, in 2006. He joined the Korea Institute of Science and Technology Information, Daejeon, Rep. of Korea, in 2006 as a senior researcher. He was a core network researcher in the architectural design and development of a user-driven network provisioning system deployed in a production research network in the Rep. of Korea. He is currently researching management issues of user-driven virtual networks. He has published more than 40 refereed papers in the area of user-driven virtual networks, information centric networking, and optical networks in archival journals and conference proceedings. He was a recipient of an Excellent Paper Award for a paper presented at APIC-IST 2008. He served as an associate editor of the Journal of Internet Computing and Services from 2007 to 2013.