Operation and Management Framework for Federated Heterogeneous Networks

Muhammad Shoaib Siddiqui, 홍충선, 박한솔, 양선희

경희대학교 컴퓨터공학과

shoaib@networking.khu.ac.kr, cshong@khu.ac.kr, sol4997@etri.re.kr, shyang@etri.re.kr

Abstract

After identifying the critical glitches in the current Internet architecture, the problems have been solved using patches and updates. These solutions have overloaded the system and it is widely believed that a new clean-slate approach must be adopted to redesign and reincarnate the Internet, namely the Future Internet. Many organizations have developed testbed for the evaluation of their designs. The need is to enable the federation among these heterogeneous networks. This federation must be equipped with well-planned and well-designed Operation and Management (O&M) framework. In this paper, we propose a meta-operation and management framework for the Future Internet federation. We also present a data model, an event notification mechanism and devised a solution for the heterogeneity among different data models. In the end, we analyzed our proposal using case studies for checking its consistency and compatibility.

Keywords: Network Management, Meta-Operation, Future Internet Management, Federation.

1. Introduction

The rapid increase of Internet has started a debate amongst experts [1] as to whether continue to patch up the faults in the current Internet architecture or start over with a clean slate approach. Research community with support to the former ideology believes that replacing an entire architecture is hard to envisaged, while the former ideology supporters believe that sooner or later the current architecture would collapse under the demands of future services and applications [2]. “Indeed, there are signs that the limitations of the protocol are already appearing in situations such as unusual (but legitimate) traffic load (e.g. flash crowds), delivery of real-time video services, high-mobility of nodes and sub-networks, requirements for multi-homing, weak, asymmetric, and episodic connectivity of wireless channels, unpredictable long delay paths either due to length (e.g. satellite, multi-hop, ad-hoc connections) or as a result of congestion, attacks against the network hardware, software, or protocol infrastructure failures due to mis-configuration or operational errors” [3].

In U.S., E.U., China, Japan and Korea, researchers and the industries have recognized the need to resolve the underlying limitations of the current Internet architecture and have started working towards developing a new Internet architecture namely the Future Internet. Such projects [4], [5], [6], [7], [8], [9], [10], [11], and [12] address several decentralized (i.e. autonomic or distributed) approaches for new Internet architectures and services, featuring self-organizing properties. These projects are developed as testbeds for supporting the research community in developing new designs, algorithms and frameworks and architectures for the Future Internet. To develop a large scale testbed for researchers, and to create, deploy and test their algorithms on these projects, the fundamental need is identified as providing a federation among these projects [13]. Most of the organizations are working on establishing a federation mechanism within their heterogeneous projects, but due to difference in data and control mechanism, the solution is required to be standardized.

A lot of research is being done by different organization for enabling the federation, such as [14], [13], [15], [16], [17], [18], and [19]. All these projects are working on either enabling federation among their own projects or with projects of different organizations. Our work focus on enabling the federation among such testbeds and providing operations, control and management in this federated environments. We have devised a meta-operation and management mechanism which can assist heterogeneous projects and organizational networks to be federated by defining adapters and standard interfaces among themselves.

The rest of the paper is articulated as follows. Section 2 discusses the issues of Future Internet and Federation. Section

3 presents our proposed meta-operation and management system. Section 4 gives a case study of the system. Section 5, discusses the related work in the field of federation and management of Future Internet and provides the analysis of the proposal. Section 6 concludes the paper.

2. Future Internet & Federation Issues

After identifying the critical glitches in the current Internet architecture, the problems have been solved using patches and updates. These solutions have overloaded the system and it is widely believed that a new clean-slate approach must be adopted to redesign and reincarnate the Internet, namely the Future Internet. Definition of Future Internet on Wikipedia is listed as "Future Internet is a summarizing term for worldwide research activities dedicated to the further development of the original Internet". There is a need of in-depth analysis of the lessons learnt from the shortcomings of the current Internet, and the new approaches must range from small, incremental evolutionary steps to complete redesigns (clean slate) towards the Future Internet and its architecture principles. There are two principal ways in which to evolve or change the current Internet system. The first method is the incremental one, in which the system is moved from one state to another with incremental patches, much like in the current Internet. The second and a more drastic approach is the clean-slate approach, in which the system is redesigned from scratch to offer improved abstractions and/or performance, while providing similar and new functionalities and services based on new core principles.

Although, the clean slate approach seems to be the eminent choice, however, with a clean-slate approach, we need to create a firsthand architecture without knowing what it would look like. Also, we have to determine when the newly designed architecture is sufficiently good enough. Future Internet is required to be carefully designed to overcome all the drawbacks that exist in the current Internet. Hence, for a comprehensive evolutionary and/or revolutionary design would be crafted with proper testing and measurements at each step. For this, researchers require testbeds to emulate the Future Internet and test and collect measurements about their experiments and algorithms. Therefore, the use of prototypes is crucial, as one needs to build a system in order to evaluate it and to convince others that it is the appropriate solution. It is almost impossible to get a new idea adopted that has not yet been tried at scale and under realistic conditions. But more importantly it is needed intellectually as it enables the researchers to uncover things that would otherwise have been assumed away. Thus there is a further aspect to Clean-Slate Design besides research into new network architectures: building an experimental facility.

The National Science Foundation (NSF), in U.S., has initiated the Future InterNet Design (FIND) research program [6] within the NSF NeTS program which poses the following questions: "What are the requirements for the global network of 15 years from now – what should that network look like and do?" and "How would we re/conceive tomorrow's global network today, if we could design it from scratch?" As such FIND has a strong focus on defining an architecture for the Future Internet. Similar initiative can be observed in East-Asia and in the EU as FP7.

Global Environment for Networking Innovations (GENI) [5] initiative is a NSF Major Research Equipment aimed to "Build an open, large-scale, realistic experimental facility for evaluating new network architectures." The intention of GENI is to offer a shared, global facility designed to catalyze research on network architectures, services and applications. A similar initiative planned within the FP7, Future Internet Research and Experimentation (FIRE) is a program funded by the European Union with the objective to do research on the internet, its prospects, and its future. FIRE, on one hand, is promoting experimentally-driven long-term, visionary research on new paradigms and networking concepts and architectures for the future Internet; and on the other hand, is building a large-scale experimentation facility supporting both medium- and long-term research on networks and services by gradually federating existing and new testbeds for emerging or future Internet technologies.

Similar activities for network architecture and research facilities for Future Internet are supported by Japan, China and Korea. AKARI [9] & JGN+ by Japan; KOREN, KOREN2 and KGENI by Korea [11]; and CNGI-CERNET2 [12] from China are some of the most prominent ones.

2.1. Research Programs & Projects

Large research programs address both the development of new Internet architectures and suitable experimental platforms. In U.S., GENI focuses on the deployment of experimental platforms whereas FIND addresses foundational concepts and methods for the Future Internet. TIED [16], PlanetLab [8], ProtoGENI [20], ORCA [21], ORBIT [22] are five main competing testbed control frameworks are under development in GENI Program. In FIRE, several projects are contributing to the experimental facility (e.g. Onelab2 [18], Federica [17], PII). In Asia similar programs have been launched such as AKARI [9] in Japan. Joint Asian activities are carried out under the APAN (Asia-Pacific Advanced Network) [23] initiative, the Asia Future Internet Forum (AsiaFI) [24] as well as PlanetLab CJK (China, Japan, Korea), a joint PlanetLab cooperation by China, Japan, and Korea [25]. An in-depth discussion and comparison between the different control framework approaches for experimental facilities is given in [26].

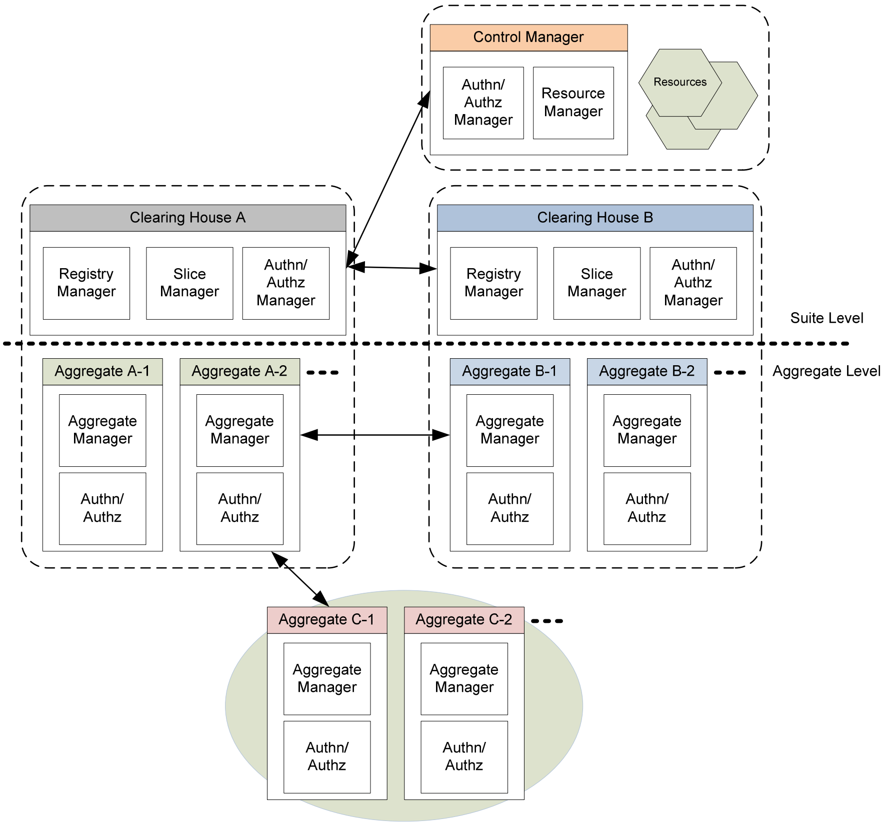

Figure 1. GENI federation scenario for Inter-GENI suites and GENI with other organization.

2.2. Federation

According to the Longman dictionary of contemporary English, the meaning of the word Federation is "a group of organizations, clubs, or people that have joined together to form a single group". Similarly, in networking, federation is a group of networks or network organizations working in coherence for achieving a single goal or providing large scale services.

In the Future Internet perspective, Federation is a means to meet requirements from research that cannot be met by individual testbeds. In particular, as the above mentioned research architectures and experimental facilities are heterogeneous in nature with various resources; a federation of experimental facilities is needed. Federation enables access to additional resources increasing scale, or access to resources with unique properties to enrich experiments and combine resources from different communities and promotes the collaboration between the related research groups.

While several initiatives are currently establishing large scale testbeds, the mechanisms for federating such environments across the boundaries of administrative domains are unclear. This is due to the lack of established and agreed federation models, methods, and operational procedures.

Federation is based on two main characteristics, i.e.; it creates (virtual) resources and the relations between these resources only when they are needed and it must carefully map the virtual resources to the substrate to ensure the best reproducibility to researchers. The first step for project (like GENI) is to federate in the overlay model. Federation requires an agreed (standard) resource description set, a common AAI (Authentication & Authorization Infrastructure), data plane and information exchange protocol at the substrate level offering a slice, and must impose less configuration complexities to other facilities.

There are certain problems that are faced in enabling federation, such as identity and authority management based on different local policy, different mechanisms used for AAI, incompatibility between control procedures, and use of different schemes for resources and experimentation description. The resilient problems for federating a number of projects are:

(1) Reproducibility of experiments, in particular the amount of variation of average values
(2) Monitoring and combination of data
(3) How to combine physical resources and virtual resources in a seamless environment
(4) Signaling between the (many) control planes and ensure the separation between the user control plane and the facility control plane
(5) Standards for resource and topology description

(6) Check pointing and error recovery/restart
(7) AAI, scheduling and naming

However, these problems may be solved using common interfaces or adapters for different control framework. The authority service can use unified profiles for certificate and authority management. Similarly, a common data access interface and a common resource and experimentation description language may also be used.

For the federation problem, the research community has proposed a number of solutions, which present federation models, operational data models, common control and data planes, and conceptual designs [14], [13], [15], [16], [17], and [18]. Figure 1 shows scenarios for suite level and aggregate level federations defined by GENI researchers. The problem, however, lies with the operation and management of the federated experimental facilities and network architecture. These, solutions fail to provide a management scenario or mechanism which directs our attention towards developing an operation and management framework for federated heterogeneous networks.

3. Proposed Network Operation & Management for Federated Networks

3.1. Motivation

GENI is arguably the most famous experiment facility being made for the research towards Future Internet. One of the main goals of GENI is "to support at-scale experimentation on shared, heterogeneous, highly instrumented infrastructures". As many other experimental facilities and research projects look towards GENI for solving the federation problem, a Slice based Federation Architecture (SFA) is being designed by GENI researchers. Projects such as PlanetLab [8], Emulab, and VINI [7] have already started SFA implementation and GeniApi has implemented the key interfaces of the SFA draft.

SFA is a control framework architecture which defines the minimal set of interfaces and data types that permit a federation of slice-based network substrates to interoperate [14]. Although, SFA draft [14] is a founding stone towards the federation standardization but it still lacks the key issues such as operation and management. GENI employs a separate working group on the issues of operation and management names OMIS WG (Operation, Management, Integration & Security Working Group), which tackles the problem as GMOC (GENI Meta-Operation & Control) for operation and control and has not yet defined a management framework or mechanism.

One of the major faults of the current Internet architecture is that the key issue of management was considered after the design, which has caused significant drawbacks and we believe that critical issues of operation and management should be considered during the design process. That is why we have proposed an Operation & Management Framework for federation of slice-based network substrates to interoperate.

3.2. Proposed Framework

Our proposal adopts the SFA draft and provides an operation and management framework for federation among heterogeneous networks. The main theme of our proposal is to enable cross-domain interactions using adapters and apply a decentralized locally autonomous management mechanism. Instead of defining a centralized management framework in which all resources are centrally managed and operated; or a distributed management framework in which each project

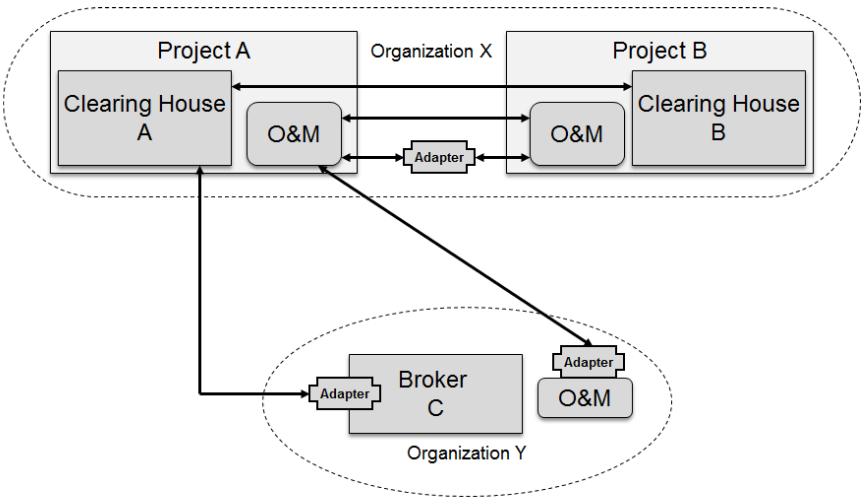

Figure 2. A simplified view of the proposed mechanism showing federation among different projects within an organization and different organizations.

federation, the Meta-O&M framework guides each project to manage itself as an autonomous system and enables singular interfaces to coordinate operation and management across the projects for users, managers and operators. The simplified mechanism of our proposal is shown in Figure 2. As shown in the figure, each project has its own O&M module which is derived from our designed O&M module, it exposes interfaces to other projects' O&M for exchange of operation data, control messages and management functions.

The proposed O&M system is a globally distributed-locally centralized management system, working on the basis of meta-operations & management. Each project has its own O&M, which centrally manages the aggregates and components. For federated aggregates, O&M of federated projects shares meta-data along with management data for distributed management. A specialized federator module enables the federation with the support of clearing house (or broker). SFA defines a federated control plane which is used by O&M for exposing interfaces in between the O&Ms of federated projects. We utilize this control plane and identify and define data elements to be shared, translation mechanism of heterogeneous data types, interfaces for real- and non-real-time data sharing, and interfaces for management functions.

O&M uses the control & data planes for control messages and data gathering. The federation handler manages the heterogeneity of control & data planes, while security is complimented with the existing SFA model by using credentials, GID and Public keys and mainly handling access control, authorization and authentication. Data is gathered from the resources at slice level for monitoring the performance and based on that, fault monitoring is performed both actively & passively. Administration is performed according to the defined policies for the users and accounting for each resources against a user or/and experiment are measured. Similarly, configuration is supported by aggregate manager interface (as defined in the SFA draft document).

3.3. O & M Module

The main module that enables the meta-O&M is shown in Figure 3. It assist a broker or a clearing house during federation and expose interfaces for the projects to exchange operational data, provides data translation, authentication and authorization, event management, management functions and provides adapters for communication amongst different projects.

3.3.1. Admin & Op

Admin & Op repository is basically a list of administrators, operators and users, who have the authorities and access to the federated projects, slices and components. The repository maintains user identification, credentials and ASpecs (accessibility specifications), which are used by Administration and Accounting component for granting access and communication for different users and operators of the federated slice. Admins are the administrators for the networks and Principal Investigator [14]. Operators are owners of substrates, operators of the substrates working for organizers, researchers and developers running experiments on the slice and identity anchors who drive authorizations for other operators.

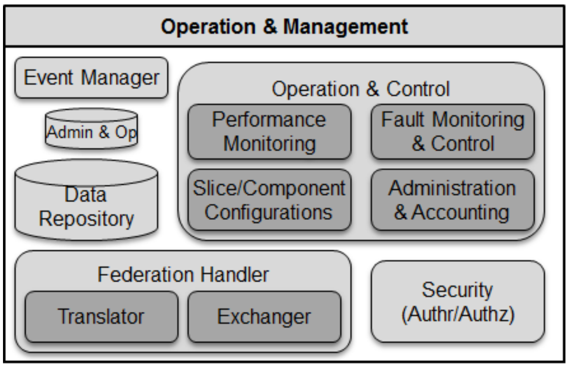

Figure 3. The Operation and Management module with its internal components.

3.3.2. Data Repository

For the management and visualization purposes, slice wide operational data is gathered by the O&M module from the participate components of the projects. This operational data is gathered for overall performance measurements, fault detection and providing federation-wide-views and measurements of the experiment for the user. Operational data model and structure is shown in Figure 4. Data Repository is the central data storage for this operational data from all federated projects (related to the slice).

3.3.3. Security: Authr/Authz

The security mechanism for O&M functions is adopted from SFA with some alterations. This component is responsible for providing authorization and authentication mechanism for the users and administrators (defined in section 3.3.1). A signed Global Identification (GID) is used for secure communication, authentication and authorization. GID is created as a tuple of public key, UUID (Universally Unique Identification), lifetime of the GID and a signature generated by a responsible endorsing authority. Trust chains are created to provide signed assertions about entities and their attributes. Trust chains are enables by defining Identity Providers (attributes: public key, memberships, roles, privileges, 'budget') for users and Resource Brokers (attributes: time duration, required user attributes) for resource assignments.

3.3.4. Event Manager

All the incident and affairs of a project or a network are handled within, however, for a certain event, a user or an operator can register a notification. Event manager at the O&M is responsible for this. Certain administrative events such as device failures can lead to an emergency shutdown, which is needed to be notified to the administrators and operators. For such an event the administrators can define a policy such as shutdown the device, find a new device and attach it to the experiment.

Event Manager collaborates with the event & policy repositories at the Clearing Houses. For notification, a principal can register an event and define a policy accordingly. A policy is defined as a set of event, conditions & actions. A principal registers or unregister its GUID, event identification, and a policy (set) by using the registerEvent(principal_id, event_id, policy_rule) and the unregisterEvent(principal_id, event_id) interfaces. New events can be created with an associated resource identification, condition and default policy using the interfaces such as createEvent(resource_id, admin_state, condition, policy_rule) and exposeEvent(resource_id).

3.3.5. Federation Handler: Exchanger

Federation Handler is responsible for assisting the broker or clearing house in federation between the projects and aggregates to construct a slice for an experiment. It exposes certain interfaces for exchanging information and data and help interpreting this operational data among federated projects.

For polling and/or receiving operational data from aggregates from different networks, the O&M utilizes the Exchanger of the Federation Handler. The component exposes its interfaces which are utilized by projects' O&M for exchange of the operational data, operation and control information and management functions.

3.3.6. Federation Handler: Translator

The Translator component of the federation handler is responsible for translating information from other formats into consistent data format. One of our proposed solutions is to use one schema for multiple XML vocabularies. This mechanism is discussed in detail in section 3.4.2.

3.3.7. Operation & Control: Performance Monitoring

O&M defines a component management interface, which is used to assess the performance parameters of a component/slice. It is also used to gather the operational data. The components and aggregates within the slice are expected to support the performance interface. Performance interface includes operations like; get the state of a component (on/off/ suspend), get operational data for the component and current state of resources listed in the RSpec (resource specification).

3.3.8. Operation & Control: Fault Monitoring & Control

Fault Monitoring & Control has two main functions. Fault detection is based on active and passive monitoring of resources, while fault localization is related to identifying where the fault has occurred. Fault detection is normally followed by shutdown control and/or finds new/alternate resource operations.

3.3.9. Operation & Control: Administration & Accounting

Administration & Accounting is related to the fact that which user, operator and administrators are allowed to use

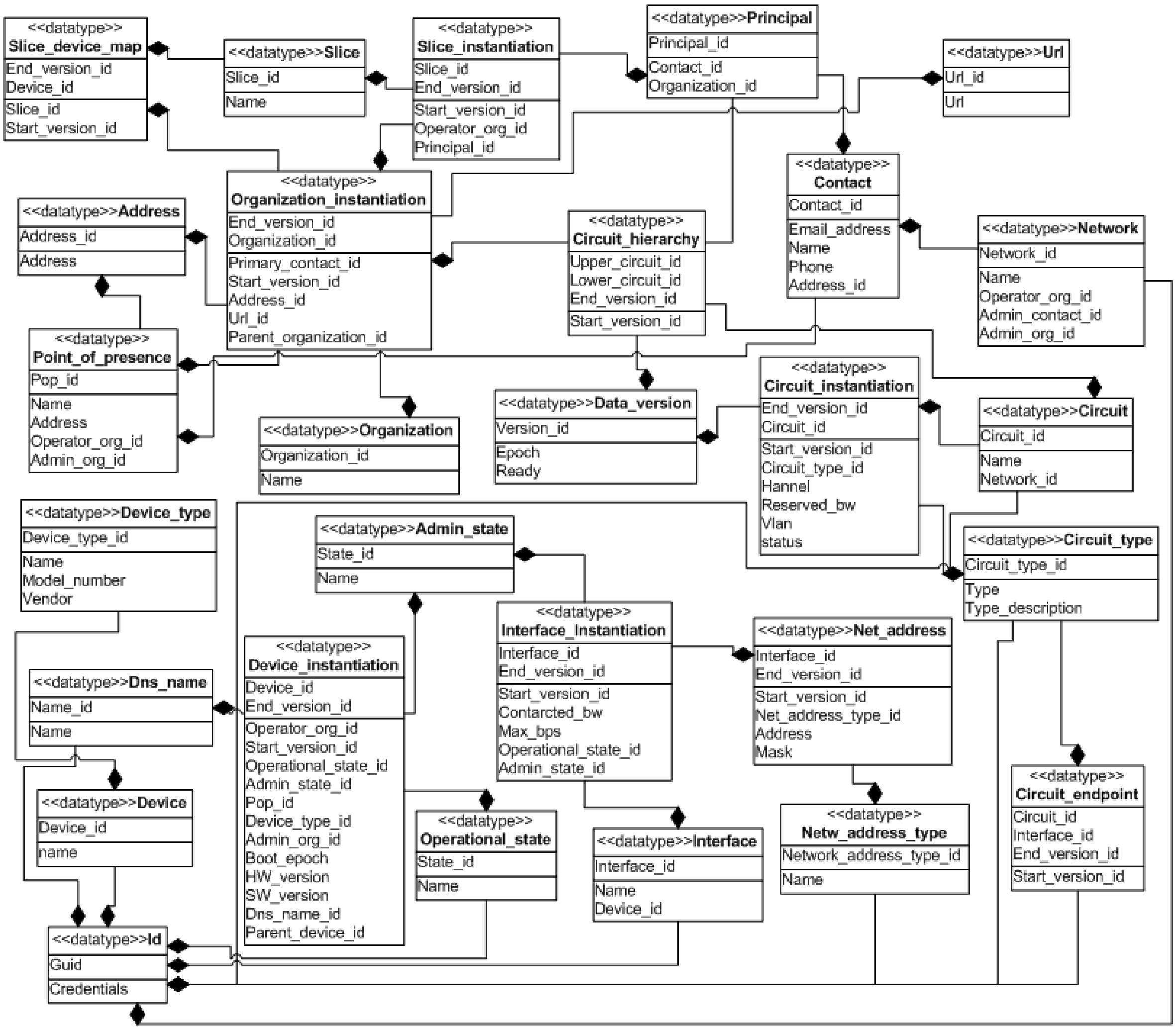

Figure 4. Data Model & structure (some associations are removed for the clarity of the figure

which resources. Accounting measures the resource usage by certain user/operator. Experiment measurements are collected and viewed to the researcher or organizer of the experiment. Utilization data about the data flowing on components, slices, backbones, such as link utilization, CPU utilization, memory utilization and traffic measures etc. are gathered by the accounting system and reported to the administration or to the cross-domain view of the experiment. Administration utilizes the authorization and authentication mechanism provided by Security component to grant access of this accounting information to the authorized users and operators.

3.3.10. Operation & Control: Configurations

For the configuration of the slices, aggregates and slivers, component management interface is used. Interfaces are used to bring the component into a safe state, boot them and turn their states to on/off. All components and aggregates are supported by the configuration interface by delegating tasks through SFA Slice Manager, Component Manager and Aggregate Manager. Configuration interface includes three operations;

(8) Set the boot state of a component to one of the following four values; Debug (component fails to boot, but should keep trying), Failure (hardware failure, component is taken offline), Safe (component available only for operator diagnostics), Production (component available for hosting slices)
(9) Learn a component's state
(10) Configure certain attribute of the component; provisions & configures resources listed in RSpec, release all resources no longer listed in RSpec, returns current state of resources as RSpec, etc.

3.4. O & M Essentials

As discussed in the motivation section, the most critical problems in enabling federation and providing operation and management for cross-domain networks are selecting which data to gather, how to make the data model consistent and understandable and enabling communication between the different projects. We have devised a common data model, compatible schemas for different data schemes and a communication model for critical data transfer for O&M framework.

3.4.1. Operational Data Model

After surveying different projects and from their available documentation, we have identified the potential types of operationally significant data. The data model can be divided into following parts:

System-wide view contains the topological information consisting of information and configuration of the components and aggregate which constitutes the slice of the experiment. It shows aggregates, components, resources, interfaces, circuits/links, slivers and their relationship among themselves. Operational status provides the status of a given component, sliver, aggregate, or slice, at a given time. Administrative status provides the expected state of a given component, sliver, aggregate, or slice for the comparison with the Operational status for monitoring and fault detection purposes. Utilization data provides the time series measures of a resource in use by a slice, user, operator etc. Specialized data specifies the data specific to the type of component, or a situation. Identification data for each slice, aggregate, component and resource is described using a GID. Each member of a federation behaves as a certification authority (CA), and holds a self-signed CA certificate. These root certificates are assumed to be well-known throughout the federation, and it is the responsibility of the clearing house or broker to distribute the certificates. Certificates follow the standard X.509 format (v3). Every credential object includes at least one certificate, which provide authenticity, and credential, which also describes permission and policy information. Example is shown in Figure 5. The data model is shown in Figure 4 along with the associations amongst the data structures. Cross-domain data related to a slice, which needs to be globally identified, is accessed as:

Ex: <slice_id>.<aggregate_id>.<component_id>.<operational_data>

3.4.2. Data Translation

Local O&M is responsible for generating operational data in standard specification, for which O&M translator services and shared XML schemas are used. We developed a method for defining the data in a compatible form for more than one projects by using a single schema for multiple XML vocabularies. Example in Figure 6 shows how two schemas can be combined to support compatibility between two different schemas. Here schema A has one type of tags for attributes, while schema B follows its own scheme. The combined schema (A&B) can contain data from both the mechanism and support both schemes by using the class tag of the XML. Example given in Figure 6(c) can read both XML example data shown in Figure 6(a) and (b).

3.4.3. Cross-Domain Data Sharing

For each project, local O&M gathers operational data, which includes values such as, bandwidth, utilization, etc. Sharing of the operational data requires common resource specification among different projects. The possible solution is

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<signed-credential>
  <credential xml:id="ref1">
    <type>privilege</type>
    <serial>12345</serial>
    <owner_urn>urn:publicid:IDN+emulab.net+user+gary</owner_urn>
    <target_urn>urn:publicid:IDN+emulab.net+slice+mytestslice</target_urn>
    <expires>2010-01-01T00:00:00</expires>
    <privileges>
      <privilege>
        <name>*</name>
        <can_delegate>1</can_delegate>
      </privilege>
    </privileges>
  </credential>
  <signatures> ---XML Signature elements (signatures and certificates) go here---
  </signatures>
</signed-credential>
```

Figure 5. XML Schema showing an example of a credential structure

```
<?xml version="1.0"?>
<resource>
     <id>197001012</id>
     <user>19700827</user>
</resource>
```

(a) Schema A

```
<?xml version="1.0"?>
<printer>
     <gid>197001012</gid>
     <operator>19700827</operator>
</printer>
```

(b) Schema B

```
<?xml version="1.0"?>
<resource class="printer">
     <id class ="gid">197001012</gid>
     <user class ="operator">19700827</user>
</resource>
```

OR

```
<?xml version="1.0"?>
<printer class = "resource">
     <gid class ="id">197001012</gid>
     <operator class="user">19700827</operator>
</printer>
```

(c) Schema C: Supporting Schema A & Schema B

Figure 6. The combined schema (A&B) can contain data from both the mechanism and support both schemes

messages. This has been implemented by PlanetLab, VINI and GeniApi. However, within a federation, real-time data sharing is tough. One solution is to define critical data and non-critical data according to real-time and non-real-time sharing requirements. We have defined configuration data, performance data, utilization data (measurements), and administration data as the non-real-time (non-critical) data types. While, fault & error data, emergency control data, operational status, and event triggered control and measurement data are defined as real-time or critical data.

For real-time data sharing, whenever an event occurs, agents at components send the data directly to Operations and Control (O&C) by calling interface exposed by O&M manager. Similarly, O&C sends control message with component credentials. This critical data is sent in small messages for fast delivery. For Real-time data RTxxx(param) interfaces are defined in the framework. Such as RTsendStatus(credential, status) for fault notification, RTshutDown(credential) for emergency shutdown, etc. For critical data sharing among federation, messages are classified as high priority packets on the network.

Non-critical data is shared periodically and normally in forms of reports (XML). Component manager gathers data, sends it to aggregate manager, who sends the data to the slice manager and the slice manager sends the data to the O&C functions.

4. Case Studies

We have performed our first case study as an enhancement to the use case given in [13]. In [13], use case for FIRE resource federation framework is presented. We have adopted their FIRE-GENI federation scenario and implemented our

O&M framework over it. This scenario adopts the Panlab [27] federation with the SFA architecture at the GENI side (implemented by PlanetLab), hence it is quite similar to our framework which is also based on the SFA draft implementation. Figure 7 shows the scenario with O&M module at the PlanetLab side. Panlab use its own O&M module for local management and utilizes the interfaces exposed by our O&M at the PlanetlLab. Panlab implements an SFA wrapper for enabling federation with the PlanetLab SFA implementation. The federation mechanism of Panlab is used through the implementation of an aggregate manger module and light-weight SFA registry to support the SFA mechanism, while the operation and management is according to our O&M framework.

In our second case study, we analyzed the federation of PlanetLab-Central (PLC) and PlanetLab European (PLE). At both side the implementation is according to the SFA draft for sake of providing similar control framework as our framework is also based on the SFA draft implementation. Here, we only discuss the operation and management aspect of the scenario. Figure 8 shows the scenario with our O&M module at the PLC side. PLE uses a simple O&M module for local management and utilizes the interfaces exposed by our O&M at the PLC. The federation mechanism implemented using SFA, while the operation and management is according to our O&M framework.

Using the control framework defined by SFA and implemented by the PlanetLab, we utilized the provided interfaces for the control messages. For the data exchange, we used an overlay data plane on top of control plane. Management of the project is mostly by the local O&M modules, which gather operational and performance data and in return send control messages. In both scenarios, peer to peer mechanism is used; however, the global management functions, data translation and operations are handled by the O&M at the PlanetLab side. In comparison to the second scenario, the first scenario shows less flexibility and more delay, which is due the wrapper implementation and abstraction at the Panlab. While in the second scenario, as the underlying federation framework is same, therefore, the O&M mechanism is more robust.

Although, the case studies could not involve a thorough analysis of the whole system, but they helped us in

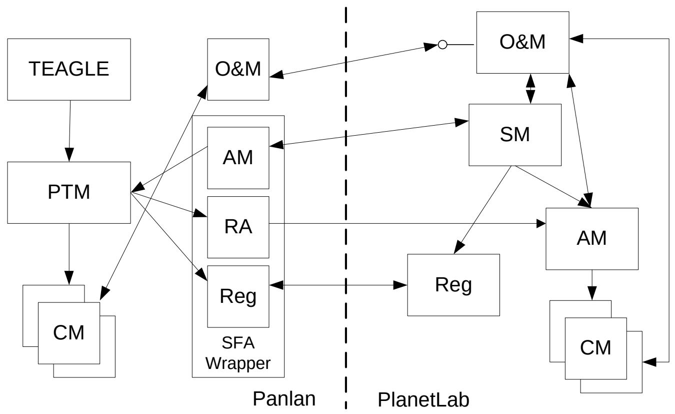

Figure 7. Federation Scenario for Panlab and PlanetLab.

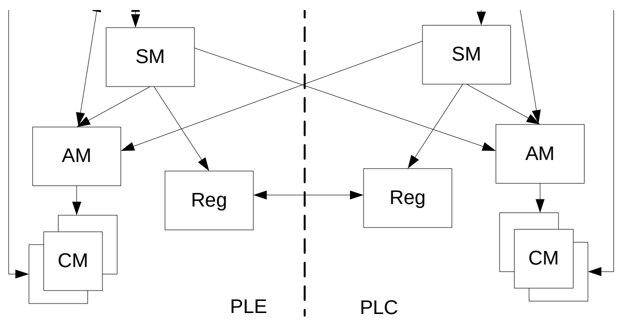

Figure 8. Federation Scenario for PlanetLab Central and PlanetLab European.

5. Related Work

In the scope of GENI, the effort towards developing a federation mechanism is described in the SFA draft document [14]. SFA is a control framework architecture. The draft document presents federation scenario within GENI and also with other organizations. It represents a rough consensus among principals of the GENI control frameworks, and defines the minimal set of interfaces and data types that permit a federation of slice-based network substrates to interoperate. However, it leaves many crucial aspects of the control framework unspecified. FIRE federation mechanism, given in [13] and [15], uses two mechanisms for federation. The first concept is to give control to a centralized authority, such as Teagle [28], which controls the domains involved in the federation. The other concept is to give partial control to both the domain managers by using domain wrappers and adapters, which is good for known domains. However, challenges are expected when moving to arbitrary resources and services. Also, trust, policy and operational issues are not addressed. In [16], a federation mechanism is presented for DETER, which are Emulab based testbeds. As DETER testbeds have similar underlying resource and allocation models, hence, this federation mechanism cannot be adopted for heterogeneous networks and organizations.

In EU, FEDERICA infrastructure [17] is being developed to include virtualization and control and monitor more than one network. FEDERICA defines a service interface in order to federate resources with other projects such as FP7 project OnaLab2 or even GENI in the future. FEDERICA's federation solution is based on the service oriented architecture (SOA).

Federation between different testbeds is a key objective of OneLab [18], which allows the mutual sharing of their resources. The OneLab federation of resources is based on virtualization, slicing and a straightforward business model. OneLab's flagship testbed PlanetLab Europe is already federated with the PlanetLab Central, EmanicsLab, PlanetLab Japan and PPK testbeds. Federation projects such as OneLab1, OneLab2, Networking innovations Over Virtualized Infrastructures (NOVI), and FIREworks are OneLab's collaborations as testbed federator with different Future Internet projects. OneLab works as a federation platform by providing codebase for each federating testbeds and a reference API for developing a common code base. It also supports a web user interface for the end users.

GENI's Operation, Management, Integration and Security working group has developed GENI Meta-Operation Center (GMOC) [19]. GMOC is responsible to design and craft the protocols and processes needed to bring consistency and repeatability to GENI's federated infrastructure. GMOC is aimed to collaboratively define the core operational dataset needed for successful operation and integration of GENI aggregates. The GMOC will also work with Control Framework Clusters to develop the appropriate format and protocol for data sharing and provide basic operational functions. However, the management aspects for the federation mechanism are not yet addressed by the GENI OMIS WG.

We performed analysis of our framework using a partial implementation of the interfaces as API reference, and for checking the compatibility of the data translation module. We adopted the GeniApi functions, and PlanetLab interfaces for the SLA support. We believe that although our proposed framework does not support a control or data plane, however, by adopting the SLA reference control framework for the federation, our proposed O&M is good solution for the operation and management problem. It is light weight as it is not based on service oriented architecture but uses low-level interfaces for data gathering and operations. It provides a feasible data model, a translation mechanism for data variations and an event-notification mechanism. However, there are many aspects which are needed to be addressed within the framework such as, data model to cover more detailed parameters, scheduling, improvement of real-time communication, etc.

6. Conclusion

In this paper, we have performed a study on state-of-the-art Future Internet architectures and experimental facilities, the concept of federation and the current research trends. After analyzing the current research efforts, we have identified the problems and proposed an operation and management framework for federation among heterogeneous projects and organizations. Our framework exploits GENI's SFA and defines exposed interfaces for data exchange, operational data gathering and management and control functions. We have also provided a common data model, an event notification mechanism and a compatible scheme for different XML schemas for data and control exchange. We performed case studies for analyzing our framework's consistency and compatibility. In future, we put our efforts towards the implementation of our framework and its enhancements.

References

[1]. Anja Feldmann, "Internet Clean-Slate Design: What and Why?" ACM SIGCOMM Computer Review, vol. 37, num. 3, pp. 59-64, July 2007.
[2]. D. Clark, "The Internet is Broken" in Technology Review, December 2005/January 2006
[3]. A. Gavras et al. "Future Internet Research and Experimentation: The FIRE Initiative" ACM SIGCOMM Computer Review, vol. 37, Is. 3, pp. 59-64, July 2007.
[4]. CORDIS, "Future Internet Research and Experimentation: An Overview of the European FIRE Initiative and Its Projects," Sept. 1, 2008; http://cordis.europa.eu/fp7/ict/fire/
[5]. L. Peterson et al "GENI design principles," IEEE Computer Magazine, vol. 3, Is. 9, pp. 102-105, Sep 2006
[6]. "Future INternet Design (FIND)." http://www.nsf.gov/pubs/2007/nsf07507/nsf07507.htm
[7]. J. Rexford and L. Peterson, "VINI: Virtual network infrastructure." http://www.geni.net/dev VINI.txt.
[8]. Peterson, L. and Roscoe, T: The Design Principles of PlanetLab. SIGOPS Oper. Syst. Rev. 40, 1, 11-16 (2006)
[9]. AKARI: Architecture Design Project for New Generation Network. http://akari-project.nict.go.jp/eng/index2.htm.

[10]."FIF: Future Internet Forum", http://fif.kr/
[11].Jinho Hahm, Bongtae Kim, and Kyungpyo Jeon, "The study of Future Internet platform in ETRI", The Magazine of the IEEK, Vol.36, No.3, March, 2009.
[12].CNGI-CERNET2, http://www.cernet2.edu.cn/index_en.htm
[13].L. Peterson, R. Ricci, A Falk, and J. Chase "Slice Federation Architecture" http://groups.geni.net/geni/wiki/SliceFedArch
[14].S. Wahle, T. Magedanz, and A. Gavras, "Conceptual Design and Use Cases for a FIRE Resource Federation Framework,"Towards the Future Internet - Emerging Trends from European Research, pp. 51-62, April 2010.
[15].S. Wahle and A. Gavras "Federation Interoperability - Dealing With Heterogeneity," NSF/FIRE Workshop on Federating Computing Resources, May 2010
[16].T. Faber, J. Wroclawski, K. Lahey, A DETER Federation Architecture, in: Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test, August 2007.
[17].M. Campanella, "FEDERICA: Federated E-Infrastructure Dedicated to European Researchers Innovating in Computing Network Architectures," Future Internet Conf., Apr. 2, 2008; http://www.fp7-federica.eu/
[18].Onelab – Federated Testbeds, http://www.onelab.eu/index.php/testbeds/federated-testbeds.html.
[19].J.-P. Herron, "GENI Meta-Operation Center," IEEE Fourth International Conference on eScience, pp.384-385, Dec 2008.
[20].GENI Project Office, ProtoGENI Control Framework Overview, GENI-SE-CF-PGO-01.4 (2009)
[21].Chase, J et al.: Beyond Virtual Data Centers: Toward an Open Resource Control Architecture, Selected Papers from the International Conference on the Virtual Computing Initiative (ACM Digital Library) (2007)
[22].Ott, M et al.: ORBIT Testbed Software Architecture: Supporting Experiments as a Service, Proceedings of IEEE Tridentcom 2005 (2005)
[23].Asia-Pacific Advanced Network initiative website: http://www.apan.net/
[24].Maoke Chen, Sue Moon, and Akihiro Nakao. Goals and Blueprint for PlanetLab CJK. Presentation at Conference for Future Internet 2008 PlanetLab BoF, June 19th, 2008, Seoul, Korea.
[25].Asia Future Internet Forum website: http://www.asiafi.net/
[26].Thomas Magedanz and Sebastian Wahle. Control Framework Design for Future Internet Testbeds. e & i Elektrotechnik und Informationstechnik, 126(07/08):274-279, July 2009.
[27].Website of Panlab and PII European projects, supported by the European Commission in its both framework programs FP6 (2001-2006) and FP7 (2007-2013): http://www.panlab.net
[28].TEAGLE portal website: http://www.fire-teagle.org

[ACKNOWLEDGEMENT]

This work was supported by the IT R&D program of MKE/KEIT. [10M14710, Future Internet Testbed Construction for International Federation and Collaboration] Dr. CS Hong is the corresponding author.

Muhammad Shoaib Siddiqui

2004 University of Karachi, Pakistan, BS in Computer Science

2004 ~ 2006 InfiniLogic, Software Engineer

2008 Kyung Hee University, MS in Computer Engineering

2008 ~ Now Kyung Hee University, PhD in Computer Engineering

<Research Interests> Network Management, Autonomous Management in WSN, Wireless Mesh Networks

Choong Seon Hong

1983 Kyung Hee University, BS in Computer Engineering

1985 Kyung Hee University, MS in Computer Engineering

1988 ~ 1993 Korean Telecom

1993 ~ 1997 Keio University, Japan, PhD in Computer Engineering

1997 ~ 1999 Telecommunications Network Lab, KT

1999 ~ Now Professor, Department of Computer Engineering, Kyung Hee University.

<Research Interests> Ubiquitous Networks, Future Internet, Mobile Computing, Wireless Sensor Networks, Network Security, And Network Management.

Han Sol Park

2002 Pusan National University, MS in Computer Science

2005 ~ Now Electronics and Telecommunications Research Institute(ETRI)

2010 ~ Now Chungnam National University, Ph.D. course in Computer Engineering

<Research Interests> Ubiquitous Computing, Network Management, Future Internet, Wireless Sensor Networks

Sun Hee Yang

1984 KyungBook National University, BS in Electronics

1986 KAIST, MS.in Electric and Electronics

1986~1988 Research Staff , Communications Lab, KAIST

1988~Now, Director, ETRI

<Research Interests> High Speed Delivery Network Architecture, Network Control, Future Internet and Media-aware Network