Authentication, Authorization and Resource Allocation Policies in Dynamic Circuit Network

Tananun Orawiwattanakul, Hideki Otsuki, Eiji Kawai, Shinji Shimojo

National Institute of Information and Communications Technology
KDDI Building, 1-8-1 Otemachi, Chiyoda-ku, Tokyo, 100-0004
{tananun, eiji, eiji-ka, sshinji}@nict.go.jp

1. Introduction

This paper and the submitted poster present an on-going research of dynamic circuit network (DCN) in Japan Gigabit Network eXtreme (JGN-X), the Japanese Future Internet testbed. This research proposes attribute-based resource allocation policies (RAPs) and Shibboleth inter-operability in On-demand Secure Circuits and Advance Reservation System (OSCARS) [1].

DCN is an on-demand virtual circuit (VC) service in which authenticated and authorized users, i.e., humans and applications, request a VC via a Web page or an application service interface (API). Currently, JGN-X utilizes OSCARS for providing a DCN service. OSCARS was developed by the Energy Sciences Network (ESnet) and it supports advance reservation for VCs at layer 2 (Ethernet) and layer 3 (IP).

Most of human users in DCN request a VC via a Web page and three main authentication/attribute provisioning methods can be done:

1. Authentication at a DCN own authentication system: OSCARS has its own authentication/attribute management.
2. Authentication at the Centralized authentication and authorization (AA): the Centralized AA provides both authentication and attribute-provisioning services. It may maintain its own authentication and user directories or connect to the external authentication and attribute provisioning services. Currently, there is no centralized AA system in JGN-X. The example of the Centralized AA utilized by a bandwidth on demand service was developed in GEANT networks [2].
3. Authentication at an identity provider (IdP) by utilizing single-sign-on (SSO) technologies, such as Shibboleth [3]. Shibboleth consists of two main software; Shibboleth IdP (installed at an IdP) and Shibboleth SP (installed at OSCARS). Note that Shibboleth IdP does not act as either an authentication provider or an attribute provider. The user authenticates with the IdP. Then, user attributes from the IdP and the VOMS are aggregated by Shibboleth IdP. Shibboleth IdP releases user attributes to OSCARS through the Shibboleth SP. OSCARS determines users attributes for authorization.

After the user is authenticated and authorized, the user requests for a VC via a Web page. Resource computation determines whether the network has sufficient resources that satisfy constraints for a request. Resource Allocation Policies (RAPs) defines how resources should be managed in resource computation. The conventional OSCARS provides authorization and quality of service (QoS) regarding resource computation, such as, maximum requested bandwidth and time. However, existing mechanisms do not efficiently manage resources, because the path computation elements (PCEs) cannot differentiate requests. Since a PCE is an entity, e.g., a software component, which determines resources and allocates the path according to a network graph algorithm and constraints, several QoS mechanisms, e.g., bandwidth allocation policy (BAP) and preemption, proposed in literature cannot be implemented.

The resources for a VC may be required from multiple domains, and RAPs in each individual domain are independent. A service definition (SD) is defined in a network service interface (NSI) framework as a machine readable textural document (an XML file) that identifies each attribute of the service and its permitted range of values. The SD of OSCARS/DCN can be described as SD = (the Source (S), the Destination (D), an amount of bandwidth (BW), the Start time (t^{Start}), the End time (t^{End})). The inter-domain requests can contain only an SD. However, if QoS is required, QoS attributes are included in a request. In addition, priority assignment sometimes should be determined according to the user profile because resources are limited in some domains for certain projects and users, or an agreement for resource allocation is done between a user IdP and a corresponding domain. Consequently, the inter-domain requests may contain not only an SD but also QoS and/or user attributes. Each domain independently determines this information for selecting corresponding local RAPs. Note that the format of QoS and user attributes must be agreed among domains in advance so that a corresponding domain understands what service level it should deliver.

2. Resource Provisioning based on the Authorization Policies

The goals of this research are to extend the third party authentication capability and to develop QoS mechanisms for a DCN service in JGN-X. A graphical user interface (GUI) is developed for the network administrator to efficiently manage the QoS-attribute assignment. Two main contributions will be developed in OSCARS version (v.) 6.

(1) Third party authentication capability: This research proposes architecture and software development of OSCARS to compile with the technical specification and policies of Shibboleth/virtual organization management service (VOMS)-based federation. Utilizing external authentication/user-attribute providers reduces workload for DCN administrators to manage user accounts and the users do not need to have many accounts. In our proposal, Web interface users can select to authenticate with the OSCARS authentication system or with their IdP. We select Shibboleth/VOMS for OSCARS development because GakuNin (the Japanese academic federation) utilizes these technologies, and GakuNin is the most potential authentication and user-attribute providers for JGN-X.

(2) Attribute-based Resource Allocation Policies (RAPs) for both intra- and inter- domain communications: Since the conventional OSCARS can guarantee bandwidth by utilizing queuing, admission control, and input data rate limitation, several mechanisms, e.g., scheduling, were proposed to decrease request blocking probabilities (RBPs). However, when congestion finally occurs, QoS mechanisms, such as BAP and preemption, have been proposed in literature in order to ensure low RBPs for high-priority users. This research introduces an extension of the new PCE module, called the User Profile PCE (UP-PCE), in OSCARS v.6 to differentiate among requests. The UP-PCE determines two RAPs: (1) policy for control of available topology and (2) bandwidth allocation policy (BAP). In the control of available topology and BAP, certain links and amount of bandwidth are reserved to ensure low RBPs for high-priority users. In OSCARS, the resources are allocated and managed during the service request process; therefore, requests can be differentiated according to the attributes of the requesters. In our proposal, the DCN administrator defines RAPs as attributes called User-PCE attributes indicating the resource policy's name and the constraints for resources as follows.

- **User-PCE attributes for control of available topology**: *constraint-name* = "unauthz-linkid*" and *constraint-value* = a set of the port IDs that the user is not authorized to use.
- **User-PCE attributes for BAP**: *constraint-name* = "bandwith-policy*" and *constraint-value* = threshold of the reserved bandwidth ratio as a percentage of the ports that the user can utilize.

(A.) For intra-domain requests made by its administrative domain users: When creating a user account, the DCN administrator assigns the User-PCE attributes according to the user profile, and he/she can change the User-PCE attributes at any time though the Web page.

(B.) For inter-domain requests and requests made by the users who authenticated at an IdP: OSCARS will be extended to add user attributes and/or QoS attributes into the *OptionalConstraint* data type and send them to other domains. Each domain determines incoming information and selects the proper local RAPs. Our developed software will provide a GUI for the DCN administrator to flexibly define the rules (called attribute-mapping rules) that translate the attributes of inter-domain requests and those of requests of which a requester is authenticated with the IdP to the User-PCE attributes. The examples of attributes to be translated are user attributes (project name) and QoS parameters.

When the request is processed through the PCEs, each PCE prunes those network components that cannot satisfy its corresponding constraints, such as the user's requested bandwidth, from a network graph. The UP-PCE determines the User-PCE attributes contained in the request. It determines the attributes that have a constraint-name beginning with the term "unauthz-linkid" and "bandwith-policy" as the attributes for determining unauthorized ports and the threshold of the reserved bandwidth ratio, respectively. The UP-PCE determines elements (links, ports, and nodes) that the user is not authorized to utilize, or whose reserved bandwidth ratio exceeds the threshold, and it removes them from Topology.

Our proposal enables OSCARS to provide QoS mechanisms and a developed GUI for attribute-mapping mechanism introduces a flexible solution for priority assignment. Our developed GUI for attribute-mapping mechanism enables the network administrator to flexibly map incoming QoS parameters, user attributes and a corresponding domain name to the local User-PCE attributes. Consequently, the network administrator can simply assign users of a specific project, a service requested from a specific domain, and incoming QoS parameters, as high or low priority in our developed local RAPs.

3. Summary

The development in Section 2.2.A was developed and more details are described in [4]. Currently, we are in process of software development described in Sections 2.1 and 2.2.B. The poster presents our research including a design of proposed OSCARS software architecture.

References

[1] William Johnston, Chin P. Guok, and Evangelos Chaniotakis, "Motivation, Design, Deployment and Evolution of a Guaranteed Bandwidth Network Service," in Proceedings of the TERENA Networking Conference, 2011.

[2] G. Adam, C. Bouras, I. Kalligeros, K. Stamos, G. Zaoudis, "Security Aspects for Large Scale Distributed Environments," in Proceedings of the 6th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2012.

[3] Internet2 Shibboleth project, "Shibboleth 2 Documentation," https://spaces.internet2.edu/display/SHIB2

[4] Tananun Orawiwattanakul, Hideki Otsuki, Eiji Kawai, Shinji Shimojo, "Extension of Path Computation Element (PCE) Framework for Resource Provisioning based on User Profile in Dynamic Circuit Network," in Proceedings of the 5th International Conference on Advanced Infocomm Technology (ICAIT), 2012.