Efficient Information Propagation in Service Routing for Next Generation Network

David Lai and Zhongwei Zhang

University of Southern Queensland
Toowoomba, Queensland, 4350
lai, zhongwei@usq.edu.au
http://www.usq.edu.au/

Abstract. Service routing across multiple network domains often requires redirection of service requests. Service request redirection can be achieved with multiple single hop redirection as in Session Initiation Protocol (SIP) or as a single redirection of multiple hops as in Service Network Graph (SNG). For efficiency and manageability, it is desirable to hold all the redirection information and knowledge for service routing in a single entity during redirection of individual service. In this paper, we propose the use of Service Path (SPath) to store and communicate the redirection information and knowledge for better performance. We also discussed how SPath can be applied to access a shared service and perform authentication in a multi-hop inter-domain service routing context using SNG as an example for illustration.

1 Introduction

Many Internet services provided by the next generation network are shared by users from different network domains. Inter-domain service routing is critical for the success of next generation network. One of the major issues for service routing is redirection of service requests. Various models and architectures are proposed. For instance, Semantic Overlay Based Service Routing [1] maps network service to service ontology, and index structure of service routing is set up for service routing across different access network domains.

Service request redirection is commonly used in heterogeneous networks with multiple servers. For example, Session Initiation Protocol (SIP) [2] using Extended Header Field for Service Route Discovery During Registration [3] allows redirection of an INVITE request to another server which can further redirect the request to other servers. Thus service routing can be accomplished with multiple redirections of only one hop each.

Another example of using service request redirection is Service Network Graph (SNG). In SNG, service requests may undergo single redirection via multiple hops. Apart from server path information, redirection may need other information and knowledge pertaining to the request. Obtaining those related information and knowledge on-demand may pose tough requirements on availability, connectivity and security of the network devices. Thus it is desirable to put all the server path and service request information and knowledge into one place, the Service Path (SPath) for efficient and effective communication.

In this paper, we will discuss the concept of Service Path and explore how it can facilitate information propagation as applied to Service Network Graph, SNG. The service access and authentication processes in SNG will be used as examples of SPath application. This paper is organized into five sections. In Section 2, we summarize the basic concepts of SNG and SPath. In Section 3, we present the method to retrieve path information during user authentication and service access. Finally, we sum up our work in Section 4 and list some of our work in future.

2 Service Network Graph (SNG) and Service Path SPath

Authentication and security have always been one of the major issues for service sharing. Despite various efforts in the past such as the use of X.509 certificates [4], trust recommendations [5–8], trust establishment [9–13] and Kerberos [14], this problem has not been resolved. Service Network Graph (SNG) [15–19] was proposed in 2005, which precisely empowers heterogeneous networks to share their services.

The approach SNG takes is to allow the linking of heterogenous networks in an ad hoc manner to form a Service Network Graph. Users can get authenticated and access services via any network within the SNG without revealing any authentication information to the intermediate networks. Among the technologies used, the main technology is Service Path.

Independent heterogeneous networks have different authentication policies, schemes and platforms. For example, to log in for services, the authentication credentials required by network N_1 may be substantially different from that required by network N_2. Traditionally, the way to authenticate a register user of N_1 while he is in N_2 is to share the user identity information with N_2, and the user has to provide the set of credential to N_2 whenever he logs in for services. The user is effectively registered with N_2 also. The amount of data to be shared and the complex issues of privacy and security make this approach formidable.

Service Network Graph (SNG) can eliminate the need to share user identity information among networks. SNG requires the authentication server AS_1 of N_1 to share a secrete key K_{12} with the authentication server AS_2 of N_2. The secrete key K_{12} will be used to establish a self-authenticating [20] encrypted channel between AS_1 and AS_2. Then authenticated users of N_1 can now use the services from N_2.

In the following subsections, we will explain the procedure of how users of N_1 uses the services available on N_2 when he is located in his home network N_1 or in come other foreign network N_3 in the same SNG.

2.1 Joining an SNG

Suppose network N_2 is a member of an SNG. Network N_1 wishes to join the SNG. To participate in the SNG, as shown in Figure 1, the authentication server AS_1 of network N_1 is required to share a secret key with the authentication server AS_2 of network N_2. The shared key will be used to set up an encryption channel between AS_1 and AS_2. The encrypted channel established when joining an SNG is self-authenticating [20]. The self-authenticating properties of the encrypted channels in an SNG can prevent

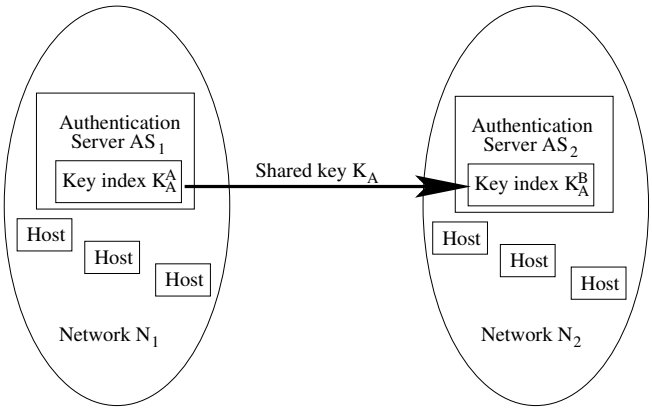

Fig. 1. Network 1 joins Network 2 in an SNG

spoofing. As shown in Figure 2, an SNG topology diagram depicts how networks within an SNG are linked logically using encrypted channels. In an one-way joining, N_2 will share its services with N_2. In a two-way joining, both N_1 and N_2 will share services with each other. The services shared are announced to the other network in the form of SPaths.

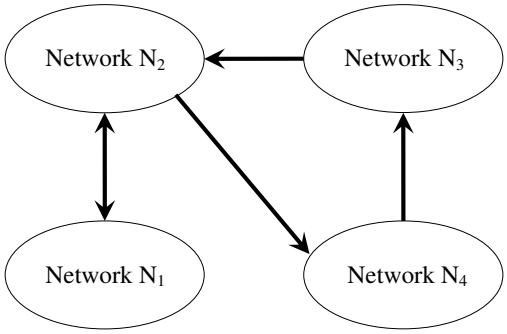

Fig. 2. Graphical representation of an SNG

2.2 Service Network Path

When N_2 shares its services with other networks, it has to specify which service, which server that provides the service, the access path, cost and the condition of sharing. Ser-

vice Path (SPath) was defined [16, 17] as shown below. Note that the SAPath starts from the home network.

```
<ShareOption:SAPath/SverN/SviceN>:<Cost>
```

where

ShareOption specifies the condition of sharing, such as free (F) to share with other networks or restricted (R) for further sharing.
SAPath is the path from the home network AS to the service providing server.
SverN is the name of the service providing server.
SviceN is the name of the requested service.
cost is the cost for using this service.

2.3 Authentication Delegation

In this subsection, we will illustrate what is Authentication Delegation. By Authentication Delegation, we mean that one network can delegate the authentication authority to another . For instance, by sharing services with N_1, N_2 has delegated the authentication authority to N_1. When N_1 declare a user as authenticated and has the right to use the services it provides, N_2 will also provide the shared services to the user as if the user was authenticate by N_2 also.

Further more, if the shared services have the option of free sharing, N_1 can share the services provided and shared by N_2 with another network N_3. The chain of authentication delegation is shown in the SAPath in an SPath. Using the example in Section 2.2, the SPath at N_3 when the service in N_1 is further shared with N_3 and AS_3 is located at `200.200.3.2` will look like:

```
<F:200.200.3.2/200.200.1.2/200.200.2.2/AS1/time>:<4>
```

The chain of authentication delegation is `200.200.2.2` (N_2) to `200.200.1.2` (N_1) and finally to `200.200.3.2` (N_3).

2.4 Authentication Propagation

Authentication Propagation is the relay of authentication request/reply of a user from a foreign network to the home network. If both the foreign and home networks are members of the same SNG, then Authentication Propagation is applicable.

For example, if a user from N_3 are now located in N_4 and he wishes to access the service

```
<F:200.200.3.2/200.200.1.2/200.200.2.2/AS1/time>:<4>
```

AS_4 in N_4 will pass the authentication and service request to the home authentication server of the user which is AS_3. AS_4 cannot get any path information for this message relay from the SPath. So AS_4 has to rely on the SNG topology file which was built and updated by individual networks when a new network joins the SNG. The SNG topology file will indicate the next hop where the message should be passed to just like a routing table in a router.

3 Accessing Shared Services using Service Path

In this section, we will discuss how SPath is used in the processes of sharing a service including Authentication Delegation, Authentication Propagation and Service Access within an SNG. The SNG shown in Figure 2 will be used as an example in our discussion.

It is quite common for large networks to have independent service providing servers and authentication servers. Some smaller networks may have a single server which authenticates users and provides services at the same time. We will take the small network approach of having one server for both authentication and service providing.

Let us first assume that AS_1, AS_2, AS_3, and AS_4 are the authentication servers on network N_1, N_2, N_3, and N_4 respectively. We also give each server an IP address as follows:

1. AS_1 in N_1 has address `200.200.1.2`
2. AS_2 in N_2 has address `200.200.2.2`
3. AS_3 in N_3 has address `200.200.3.2`
4. AS_4 in N_4 has address `200.200.4.2`

3.1 Sharing a Service

According to the SPtah defined in Section 2.2, the basic form of an SPath is a local service. For instance, a local time service provided by AS_2 with a free sharing option is

```
<F:200.200.2.2/AS2/time>:<4>
```

If N_2 shares the service with N_1, the SPath (and its SAPath) used in N_2 remains the same, while the same service in N_1 will have the address of AS_1, `200.200.1.2` pre-pended to the SAPath in SPath:

```
<F:200.200.1.2/200.200.2.2/AS1/time>:<7>
```

Note that the cost for the service may have to be adjusted if N_1 imposes overhead cost to the service.

Only local service may have the Restricted (R) Sharing Option. Restricted services will not be shared with other networks and so will never appear in an SPath with composite SAPath.

3.2 SNG Topology

We can easily find out that SAPath of SPath provides some information of how networks are linked together for sharing in an SNG. For example, local services of N_2 when shared with N_3 will have the SAPath of `200.200.3.2/200.200.2.2/`. From this SAPath, N_3 can deduce that `200.200.2.2` (AS_2) is directly linked and can be reached as a next hop neighbor. When the service is again shared from N_3 to N_4, the SAPath becomes `200.200.4.2/200.200.3.2/200.200.2.2/`. From this SAPath N_4 knows that `200.200.3.2` (AS_3) is an immediate neighbor and is also the gateway for reaching `200.200.2.2` (AS_2).

No doubt that multiple paths to the same destination may be listed if the same service is shared through a different network path within the SNG. We can make choices base on the cost of using those paths or the number of hops required to reach the destination. In so doing we are optimizing the SNG Authentication Propagation paths.

With sufficient number of SPath, we can have a complete mapping of the networks in an SNG.

3.3 Authenticating a User

A user may log in from his home network, or from a foreign network. If the user logs in from his home network, it is a local log in. Otherwise, it is a remote log in.

Case 1: If the first network address in SAPath of an SPath matches with the current network AS address, authentication can be done locally.

Case 2: If the current network AS address is part of the SAPath but not the first one, then all we have to do is to pass the request to the address on the left of the current AS address in the SAPath.
We will use an example to illustrate how it works. Suppose a local service in N_4 has SAPath `200.200.4.2/`. When shared with N_2, the SAPath becomes `200.200.2.2/200.200.4.2/` in N_2. When the service is shared again with N_3, it becomes `200.200.3.2/200.200.2.2/200.200.4.2/`. Now if a N_3 registered user logs in at AS_4 on network N_4, the request will be passed from `200.200.4.2` to `200.200.2.2` and finally to `200.200.3.2`

Case 3: When the user log in at a network whose AS address does not appear in the SPath, the current AS will require the help of the SNG topology file. The SNG topology file is a listing of next hop address used to reach a network within the SNG. The format of a SNG topology file is as follows:

```
Network Address  Next Hop Address
```

The topology file for N_1 in our example is shown below:

```
200.200.2.2   200.200.2.2
200.200.3.2   200.200.2.2
200.200.4.2   200.200.2.2
```

Using the previous example, if an user on network N_3 now logs in at N_1, the network address of N_1 is `200.200.1.2` which is not part of the SAPath `200.200.3.2/200.200.2.2/200.200.4.2/`. Hence AS_1 will resolve the path to N_3 by looking up the N_1 topology file for the entry

```
200.200.3.2   200.200.2.2
```

which means that in order to pass the request to `200.200.3.2` (AS_3), we need to pass it to `200.200.2.2` (AS_2) first. Then AS_2 can work out the next hop from SPath.

Note that the first case is an example of Authentication Delegation while the last two cases are examples of authentication Propagation.

3.4 Accessing Service

After log in, AS in the home network will contact the service agent in the service providing network to start the service for the user.

As the home AS address is always the first address in SAPath, we need to pass the service request to the address on the right of the current AS address until we reach the server address. As an illustration, consider the SAPath `200.200.3.2/200.200.2.2/200.200.4.2/`. After authentication, the request is located in `200.200.3.2`; the request should be passed to `200.200.2.2` and subsequently to `200.200.4.2`.

Note that a service agent will start a service for a service using a set of parameters including the service port number, user ID, and the session key. The service requesting user must use the set of parameters in order to access the service. This feature enhances the security and privacy of SNG transactions.

4 Conclusion

In this paper, we have explained the SPath technology and how it can be applied in the context of a multi-hop service redirection, the SNG for efficient and effective information and knowledge communication.

We use SPath for the service route. Service path and the associated cost are included in the SPath used in this paper. Other information and knowledge related to the service, such as the target user group and time when the service is available, can be included by extending the SPath.

When accessing a service, the address of the service providing server can be found from the SPath. Special care must be taken when traversing the SAPath specified in an SPath for authentication and for services access. In general, we have to move towards the start of the path for authentication and towards the end of the path for the service providing server.

When the service network aggregate grows, the SAPath in a SPath may get longer and longer thereby making it less efficient. We can optimize SPath [21] when applied to SNG so that it is scalable and efficient independent of the size of a service network aggregate. Our future work includes the investigation of optimizing the inter-domain service routing information, both automatically and on-demand.

References

1. Cao, C., Yang, J., Zhang, G.: Semantic Overlay Based Services Routing Between MPLS Domains. Proceedings of the 7th International Workshop on Distributed Computing, IWDC 2005, Kharagpur, India. (2005)
2. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC 3261, June, 2002. (2002)
3. Willis, D., Hoeneisen, B.: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts. RFC 3608, October, 2003. (2003)
4. X.509 (03/00). International Telecommunication Union ITU-T Recommendations X series. Sept 2003. http://www.itu.int/rec/recommendation.asp. (2003)

5. Rahman, A. A., Halles, S.: A Distributed Trust Model. Proceedings of the New Security Paradigms Workshops 1997. (1997)
6. Denning, D.: A new paradigm for trusted systems. Proceedings of 1992-1993 ACM SIGSAC New Security Paradigms Workshop. (1993)
7. Montaner, M., Lopez, B., Rosa, J. L.: Developing Trust in Recommender Agents. Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems. (2002)
8. Robles, S., Borrell, J., Bigham, J., Tokarchuk, L., Cuthbert, L.: Design of a Trust Model for a Secure Multi-Agent Marketplace. Proceedings of the Fifth International Conference on Autonomous Agents. (2001)
9. Beth, T., Borcherding, M., Klien, B.: Valuation of Trust in Open Networks. Proceedings of the Conference on Computer Security, 1994. (1994)
10. Reiter, M., Stubblebine, S.: Authentication Metric Analysis and Design. ACM Transactions on Information and System Security, Vol 2, number 2, January, 1999. (1999)
11. Rahman, A. A., Hailes, S.: Using Recommendations for Managing Trust in Distributed Systems. Proceedings of the IEEE Malaysia International Conference on Communication '97 (MICC'97), Kuala Lumpur, Malaysia. (1997)
12. Rahman, A. A., Hailes, S.: Supporting Trust in Virtual Communities. Proceedings of the Hawaii Int. Conference on System Sciences 33, Maui, Hawaii, January, 2000. (2000)
13. A. R. Au, A. R., Looi, M., Ashley, P.: Automated cross organisational trust establishment on extranets. Proceedings of the Workshop on Information Technology for Virtual Enterprises, 2001. Page 3-11, number 7, January, 2001. (2001)
14. IETF, IESG: The Kerberos Network Authentication Service (V5). Proposed Standard, RFC1510, Sept 1993. (1993)
15. Lai, D., Zhang, Z., Wang, H.: Towards an Authentication Protocol for Service Outsourcing Over IP Networks. Proceedings of the 2005 International Conference on Security and Management, number 7, June, 2005. (2005)
16. Lai, D., Zhang, Z.: An Infrastructure for Service Authentication and Authorization Revocation in a Dynamic Aggregation of Networks. WSEAS Transactions on Communications, Page 537-547, Number 8, Vol 4, August 2005. (2005)
17. Lai, D., Zhang, Z.: Network Service Sharing Infrastructure: Service Authentication and Authorization Revocation. Proceedings of the 9thWSEAS International Conference on Communications, July, 2005. (2005)
18. Lai, D., Zhang, Z., Shen, C.: Achieving Secure Service Sharing Over IP Networks. Proceedings of the ASEE Mid-Atlantic Section Spring 2006 Conference, April, 2006. (2006)
19. Lai, D., Zhang, Z.: Secure Service Sharing over Networks for Mobile Users Using Service Network Graphs. Proceedings of the Wireless Telecommunication Syposium 2006, April, 2006. (2006)
20. Lai, D., Zhang, Z.: Self-Authentication of Encrypted Channels in Service Network Graph. Proceedings of the IFIP International Conference on Network and Parallel Computing Workshops, NPC 2008, Page 163. (2008)
21. Lai, D., Zhang, Z.: Improving Efficiency and Scalability of Service Network Graph by Rerouting Service Routes. Proceedings of the First Asian Conference on Intelligent Information and Data Base Systems, 2009, Vietnam. (2009)