A New NSIS Application for LSP Setup with Security Features

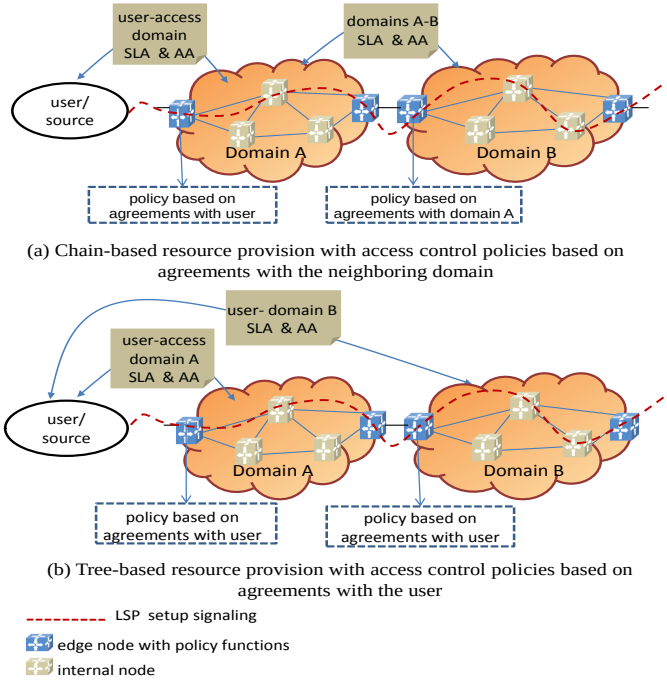
Silvana Greco Polito, Dennis Gebbers, Mohit Chamania and Admela Jukan
Technische Universität Carolo-Wilhelmina zu Braunschweig
Email: greco, gebbers, chamania, jukan@ida.ing.tu-bs.de

***Abstract*—Connection-oriented path setup is becoming one of the key features of the next-generation Internet with the Multi-Protocol Label Switched (MPLS) framework and its generalized version GMPLS addressing the automated label switched path (LSP) setup. Despite the significant technological progress in various LSP implementations, the integration of robust security features for authentication and authorization for global path setup remains an open issue. However, security is becoming essential for carrier-grade operations as it directly translates to inter-carrier's service level agreements and user's satisfaction with quality of the services purchased. In this paper, we propose to study the applicability of NSIS (Next Step Signaling Protocol) for LSP setup signaling with security features; NSIS is a generic protocol for configuring network nodes that supports multiple existing transport and security protocols. We design an NSIS application called NSIS-LSP which takes advantage of the NSIS transport security features and has own features for application layer authentication. Unlike the existing path setup protocols that refer to security mechanisms between neighboring domains for resource provisioning, NSIS-LSP also allows mutual authentication between source and remote provisioning domains. We use an open-source NSIS testbed and simulations to obtain the performance results, which show that the NSIS-LSP application carries significant potential for future implementations.**

***Index Terms*—LSP Setup, NSIS, Authentication, Security.**

I. Introduction

Efforts are underway to develop standards for constraint-based path provisioning within the GMPLS-TE [1] framework that encompasses packet, time-division, wavelength and spatial switching, and refers to the RSVP-TE (Resource Reservation Protocol-Traffic Engineering) [2] protocol as main solution for LSP setup. This protocol allows setup of paths along heterogeneous networks with different technologies, but does not include robust security features suitable for the next generation multi-domain infrastructures. It refers to IPsec that requires shared keys between neighboring nodes as transport layer security solution and includes application layer AA (authentication and authorization) features for chain-based service provisioning models in which, as shown in Figure 1.a, secure service provisioning is guaranteed through bilateral SLAs between neighboring domains and access policies at ingress edge nodes are configured on the basis of the authorization right of upstream domains. What is still missing are robust AA security features for resource provisioning based on direct SLAs between source and and any provisioning domain, according to the tree-based service provisioning approach. In such an approach, as shown in Figure 1.b, provisioning domains enforce access policies to incoming resource requests



(a) Chain-based resource provision with access control policies based on agreements with the neighboring domain

(b) Tree-based resource provision with access control policies based on agreements with the user

Fig. 1. Chain and tree based models for LSP setup

on the basis of QoS agreements with the source and therefore models for source authentication and authorization are required. Although the use of the tree-based service provisioning carries scalability challenges due to the need to establish SLAs with multiple provisioning domains, it is now being widely re-evaluated by multiple projects, such as IPSphere [3], because of its powerful capability to guarantee end-to-end QoS. In the chain model, end-to-end QoS cannot be guaranteed as it depends on SLAs between any pair of remote domains, which is out of control of the source domain. In this paper, we contend that chain and tree-based models will co-exist in the next generation service infrastructure and that new signaling solutions for LSP setup in both the models are required that allow secure access to the resource.

Current RSVP-based mechanisms for authentication and authorization in chain based architectures have been discussed in [4], while a mechanism for remote authorization of users with RSVP is proposed in [5]. This mechanism propose to include AA (authentication and authorization) tokens asserting identity and authorization right of a user to get resources in the RSVP reservation request. With this token-based model remote domains cannot authenticate with the source, as a consequence the user cannot have guarantees about the integrity

of the domain chain used for provisioning. A mechanism for negotiation of services between source and resource providers is introduced in [6], which proposes extensions to the RSVP-TE protocol to include proof of the negotiated services. This mechanism does not address security issues rising from the hop-by-hop transfer of the negotiated service proof and assumes trusted interactions between carriers. Another proposal [7] refers to the PCE (Path Computation Element) protocol that implements path computation functions to verify which are the optimal paths satisfying users QoS constraints before activation of resource reservation. It proposes a model for authentication between source and remote domains during path computation and a mechanism to make access control policies on resource reservation requests dependent on AA performed during path computation. This effort is restricted for scenarios in which the PCE framework is supported.

In this paper, we propose to rethink the path setup protocol requirements to comprehensively address the security issues arising in connection-oriented path setup, especially in the context of multi-domain networking. To this end, we study the applicability of the NSIS (Next Steps in Signaling) protocol [8] for LSP setup. NSIS is a recent IETF protocol for setup of state in network nodes for multiple purposes such as NAT/firewall traversal, resource reservation and metering. NSIS was designed as generic protocol for control of network nodes states with security as main objective. The NSIS protocol designed for the transport service is called GIST (General Internet Signaling Transport) [9] and can be used with multiple existing standard transport and security protocols such as TCP, UDP, IPsec and TLS. The inherent NSIS security features coupled with its extensible architecture make it ideal for the design of a secure path setup application. Therefore we design and implement a new NSIS application for LSP setup with security features called NSIS-LSP. The application is designed based on the existing requirements for the RSVP-TE protocol, and it additionally includes features for mutual authentication between source and provisioning domains. The authentication model proposed supports both symmetric and asymmetric key-based mechanisms. We provide results obtained from a test-bed implementing the NSIS-LSP application to verify their cost in terms of setup delay and signaling overload. We also show with simulation results how the model scales with the increasing size of the network.

The paper is organized as follows. In section II, we introduce the basic features of the NSIS-LSP application, its signaling structure and components for label switching path setup. In section III, we describe the NSIS-LSP security features for symmetric and asymmetric authentication. In Section IV we provide a critical discussion about the proposed solution for LSP setup, while in Section V we introduce performance results.

II. NSIS Label Switching Path Application

To design the NSIS-LSP application we use existing objects for establishing of LSP with route constraints which are the LabelQuery [1] , Label [1] and ERO (Explicit Route Object) [2] objects describing label request, label, and the set of nodes along the path that the source wants to be crossed, respectively. We define five NSIS-LSP messages, namely the Query, Reserve, Response, Error, and Release messages. To describe these messages and their processing rules in the NSIS-LSP nodes, we refer to the example in Figure 2, where node A represents the source and node B and C are two nodes to which LSP setup is requested.

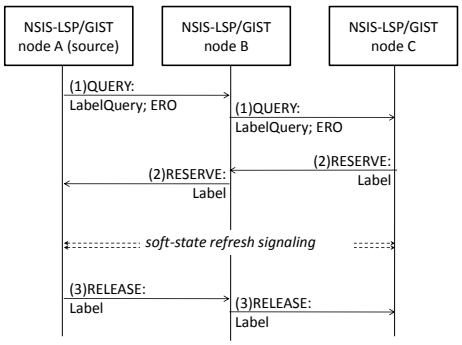


Fig. 2. NSIS-LSP messaging for label switched path setup

a) NSIS-LSP Query message processing. The source issues a Query message (1) to ask for establishing an LSP. The LabelQuery object is used to describe the LSP request. If the source wants to force constraints about the route of the path, it includes the ERO object in the Query message. The Query message is forwarded till the destination. The NSIS-LSP application in each node, source included, provides the lower layer GIST protocol responsible of the transport of the message with the identifier of the destination node of the path or the next hop described in the ERO object, if this is present in the message. The application can also force the GIST protocol to use a specific transport layer solution. Each node, on receiving the Label Query, verifies if the request can be accepted before forwarding it.

b) NSIS-LSP Reserve message processing and periodic refresh. The destination node, on receiving the request, issues the Reserve message (2) with the Label Object describing the label and sends it to the upstream node. This process is repeated by each upstream node till when the message arrives to the source with the GIST protocol responsible of its transport along the same path of the Query. At this step the LSP is established and Reserve messages have to be sent periodically to keep active the path. A Release message can be used for explicit release of the path (3).

c) NSIS-LSP Error and Response messages processing. Both Error and Response messages are not present in the example of Figure 2 as they are used only when special events happen. Responses are used by nodes to provide answers that do not imply resource provisioning. In the next section we will show how they can be used to provide authentication information. The Error message is used to notify the source that a Query service request cannot be processed because it does not satisfy one or more requirements. A node that triggers the error event, sends the error message upstream toward the source and does not forward the received Query downstream.

III. NSIS Label Switching Path Application with Security Features

In this section, we introduce the components and signaling mechanisms of the NSIS-LSP application for mutual authentication between a source requesting a path spanning multiple domains, and the domains involved. The application provides both symmetric and asymmetric authentication mechanisms and is based on extensions to the basic signaling flow introduced in the previous section to include authentication requests/responses between source and provisioning domains. More into details, we assume that the edge nodes implement the authentication functions for their domains as they are responsible for access policy. As a consequence, authentication is between source and the ingress edge node of each domain along a path request. The authentication functions can also be implemented in an authentication server communicating with the edge nodes.

To describe the model proposed, we will refer to the example of Figure 3.a , in which we assume that the source node A wants to establish a path that crosses two domains with ingress edge nodes B and C respectively. For simplicity of the description, we do not show the internal nodes of each domain that are not involved in the authentication procedures.

The example shows how service provisioning with mutual authentication requires a first Query message (1) that includes an authentication request with a challenging nonce from the source to the edge nodes. The edge nodes B and C provide their authentication response in a Response message (2) along with a challenging nonce for source authentication. The source then has to send a new Query message (3) with information that allows the edge nodes to authenticate it before getting the service. To describe authentication requests and responses carried by NSIS-LSP messages, we define a new NSIS object called AuthObject. As shown in Figure 3.c, the AuthObject has a type-length-value format and includes a flag in its header that specifies the authentication method, i.e., symmetric or asymmetric. The value of the AuthObject depends on the message described. We will now describe the AuthObjet in detail while introducing the processing rules of NSIS-LSP signaling carrying the authentication requests and responses.

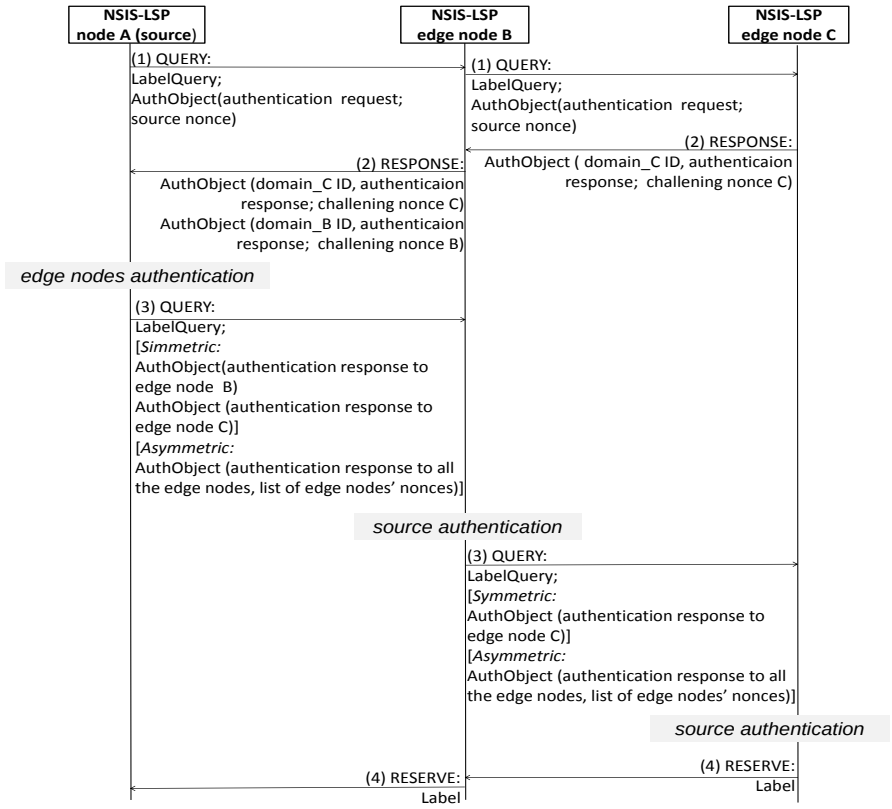
a) Query message with edge node authentication request: The source, on issuing the Query (1) includes the AuthObject embedding an authentication request. This authentication request is addressed to all the edge nodes along the path. It specifies the authentication mechanism requested by the source (symmetric or asymmetric) and includes a pseudo-random nonce to challenge the other parties for authentication. The source also provides a session identifier (session ID) associated with the LabelQuery in the Query message. The session ID will be used to couple authentication with the specific path request. The query message propagates till the destination and each domain edge node in the path extracts the source nonce and the session ID.

b) Response message with edge nodes authentication responses and source authentication requests: The destination edge node issues a Response message (2) that propagates to the source. In this message, each edge node includes a new AuthObject that encodes the identifier of its domain, the authentication response to the source authentication request and a new challenging nonce for authentication of the source. As shown in Figure 3.b, the authentication response depends on the authentication mechanism used. If symmetric key-based authentication was requested, the authentication response is a hash computed on a content that includes the symmetric key shared with the source, the source nonce and the session ID. If asymmetric key-based authentication was requested, digital signatures are used instead of hashes for authentication. Each node computes a digital signature on a content that includes the source nonce and the session ID. This way the source, on receiving the Response message, can authenticate all the edge nodes along the path through verification of the received hashes or digital signatures. In both hashes and signatures the embedded nonce guarantees the freshness of the response, while the session ID allows to couple the authentication response to the specific path request.

c) Query message with source authentication response: If all the domains are successfully authenticated, the source sends a new Query message (3) in which it includes information for the authentication of the source by the edge nodes. If symmetric authentication is required, the source issues an independent authentication response for each edge node. This response has the same format of the response from the edge nodes and is composed of an hash computed on the key shared with the edge node, the nonce received from it and the session ID. In this case, the source includes an AuthObject for each edge node in the Query message. If the authentication mechanism is asymmetric a signature is used for authentication. As secret information is not required for authentication, we propose that the source issues a single authentication response for all the requests from the different edge nodes. This response is a signature on a content that includes all the nonces received by all the edge nodes and is encoded in a single AuthObject. The AuthObject also includes the list of nonces received by the source as edge nodes need to know it to verify the signature. The use of a single signature allows to reduce the computational cost that is higher for asymmetric than for symmetric encryption. All edge nodes verify the identity of the source through the authentication response addressed to them before forwarding the new Query request. For symmetric authentication they can delete their AuthObject from the Query before forwarding. If authentication at any edge node is not successful, an error message is sent, otherwise a Reserve message (4) is initialized at the destination and propagated towards the source.

A. Authentication with special conditions

The model proposed allows to combine symmetric and asymmetric authentication mechanisms, authenticate the source with a sub-set of edge nodes, and performing single way authentication of source with edge nodes. A combination of asymmetric and symmetric mechanisms can be useful when domains support different authentication models. To facilitate



	Authentication response with symmetric-key method	***Authentication response with asymmetric-key method***
edge nodes	Hash (symmetric key, source nonce, session ID)	Signature (source nonce, session ID)
source node	Hash* (symmetric key, edge node nonce, session ID) ** a different response per each node*	Signature *(list of the edge nodes' nonces, session ID) ** a cumulative response per each node*

(b)

Type	Flag: symmetric/ asymmetric	Length
Object content [domain ID] [source nonce] [hash] [signature] [certificate] [list of edge nodes' nonces]		

(c)

Fig. 3. (a) NSIS-LSP messaging for label switched path setup with authentication between source and edge nodes of domains along the path. (b) Authentication responses of source and edge nodes for symmetric and asymmetric models. (c) NSIS-LSP authentication object (AuthObject).

the same, each edge node specifies the authentication method to be used in its response message. If the source is interested in authenticating only a sub-set of domains along the path, it has to specify their identifier, i.e., their domain name, in the authentication request. Edge nodes, on receiving the request will answer to the authentication challenging only if the identifier of their domain is included in the message. When the source does not initialize the authentication procedures, edge nodes can force the source to authenticate with them sending an Error message specifying that authentication is required in response to a received reservation request. In this case the source has to send a new query with an AuthObject composed only of the header. This object does not include an authentication request as the source is not interested in it, but it allows the nodes along the chain to understand that someone is asking for authentication and a Response message is issued in stead of a Reserve one. In this Response message, each node interested in authenticating the source, can add its authentication request.

IV. Discussion

The proposed model for authentication with remote domains has the following main properties.

Robustness of the authentication mechanisms: Authentication is based on a four-way handshake between the source and each edge node with authentication requests and responses integrated in end-to-end LSP setup messages. Although the content for mutual authentication between source and generic edge node can be read by any other node along the path between them, the challenging/response mechanism assures freshness, data origin and integrity of received authentication responses. The challenging nonce guarantees protection against replay attacks as it allows to distinguish responses related to different authentication requests. Data origin is guaranteed by the signature or the keyed-hash, while integrity is guaranteed by the one-way property of the hash function. On the other hand, the model proposed does not provide guarantees against malicious path setup requests that aim to activate denial of service attacks (DoS) forcing edge nodes to process authentication requests. Edge nodes are required to deploy their own mechanisms for protection against DoS attacks.

Adaptability: The NSIS LSP security features allow to use both symmetric and asymmetric mechanisms for authentication of source with different domains for the same path request. This makes the model proposed suitable for multi-domain scenario in which different domains deploy different authentication models. The four-way signaling model integrated in the NSIS-LSP messaging can be extended to allow the parties to negotiate the cipher algorithms to use for authentication. More into details the source can include the list of supported cipher algorithms in its authentication request and edge nodes the algorithm selected from this list in their authentication

responses.

Authorization: One of the main purposes of the authentication model proposed is to allow edge nodes to authorize incoming path setup signaling on the basis of the identity of the issuer of the request. This means that our model addresses both authentication and authorization issues. We recall that while authentication is used to verify the identity of a subject, authorization is used to verify which services the subject is authorized to use. In our model, authorization is identity-based as edge nodes verify if users are allowed to get a requested service on the basis of their identity. Investigation about signaling extensions to provide *complex* authorization mechanisms is the object of our future work.

Guarantees about the route integrity: Although the existing path setup signaling protocols allow users to select the inter-domain chain along which establishing a path, they do not provide users with path integrity guarantees. The proposed NSIS-LSP application allows users to authenticate domains along the inter-domain path guaranteeing that malicious nodes do not force it along untrusted domains.

Authentication for chain-based resource provisioning: Although we focus on authentication mechanisms for tree-based resource provisioning models, the GIST hop-by-hop security features provide support for authentication for chain-based resource provisioning. In this case, authentication is handled in the GIST transport layer where the ingress edge nodes authenticate with the egress nodes of the upstream domain.

NSIS-LSP versus RSVP-TE: The soft-state mechanism with support of explicit connection release for the NSIS-LSP application makes the proposed solution close to RSVP-TE. The main difference between the two solutions comes from the transport layer service. Unlike RSVP-TE that runs on raw IP packets, and on top of UDP, NSIS-LSP/GIST can use either TCP or UDP for transport and IPsec or TLS for security. This means that the NSIS-LSP application can run on top of protocols with different security and reliability properties and that service providers can select dynamically the transport service to use according to service or networking security constraints. With NSIS different transport layer mechanisms can be used in different parts of the network although, as showed in [9], it requires higher but acceptable network layer protocol overhead and computation costs compared with RSVP.

V. Numerical Results

To evaluate the performance of the proposed NSIS-LSP application with its authentication features, we have implemented it over the open source NSISFree code [10] version 0.6.0. The OpenSSL library [11] was used for the authentication functions with hash function SHA-1, 128 byte long keys and X509 certificates. Our testbed consisted of three NSIS-LSP nodes (source, transit and destination edge nodes) with each node running on a desktop machine with Intel Core 2 duo processor and Fedora core 8 running on VM with 512MB RAM. The testbed was used to measure the packet processing times at each node for NSIS-LSP application in scenarios with no-authentication, symmetric authentication and asymmetric authentication.

	Process	Delay (ms)	Load (Messages/sec)
No Authentication	Packet Forwarding	0.099	910
	Packet Processing(Conservative Estimate)	1.0	
Symmetric Authentication	Hash Computation	0.121	862
Asymmetric Authentication	Signature Computation	5.310	397
	Signature Verification	0.369	

Fig. 4. Delays of different processes in the signaling and the estimates capacity in Messages/sec for different authentication mechanisms

The measured times for different operations in the NSIS-LSP application are shown in Fig. 4. The measured packet processing times as observed on the testbed were largely dominated by the authentication mechanisms and the packet forwarding delays were observed to be very low (0.000099). However, in real systems, these delays would be significant as they would include configuration of the routers in specific signaling scenarios. Even when using a conservative maximum bound on the time required for other processes on a node as 1 ms, we observe that the packet processing time for asymmetric authentication is dominated by the signature computation process. We use these measurements to estimate the maximum connection rate that a router can support, which is also shown in Fig. 4. As seen here, the high signature computation delay can significantly increase the packet processing times of a node and can therefore support significantly lower loads, while the symmetric authentication mechanisms can still support high request loads. While the asymmetric authentication mechanisms can create a bottleneck during operations, symmetric authentication mechanisms require a pre-shared secret key between domains, and can therefore be a management bottleneck. Therefore, both mechanisms are necessary for operations in future networks.

To test the scalability of the proposed NSIS application we simulated networking scenario with increasing number of domains. We used the Generalized Linear Preference (GLP) model [12] to generate the network topologies and an event driven simulator to evaluate the performance metrics. The minimum distance unit was assumed to be 1000 km, and the nodes representing domains were placed inside a square of dimentions $(10,000Km, 10,000Km)$. The probability p of adding a link for the GLP model was set to 0.2 while the parameter $\beta = 0.64$. We studied the affect of increase in the number of nodes in a topology on the average signaling delay and the average load per link in the network.

The average delay for three scenarios, LSP setup with no authentication, with symmetric and asymmetric-key based authentication was evaluated and the results are shown in Figure 5. The average signaling delay in a topology was computed as the average of signaling delays measured across all possible source-destination pairs, while choosing the shortest hop route. For a given number of nodes, 50 random topologies were generated by the model and the final average delay was evaluated as the average measurement for all these topologies.

Figure 5 shows that the signaling delay increases linearly with the increase in number of nodes but not significantly. This is due to the average number of hops between source/destination pairs that does not change significantly for the topologies used having connectivity degree ranging from (2.5, 3). As introduced above, the gap between the delays measured for symmetric and asymmetric authentication depends on the high delay for signature computation.

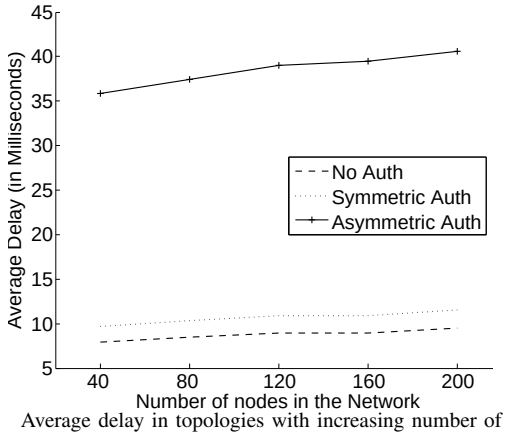


Fig. 5. Average delay in topologies with increasing number of nodes

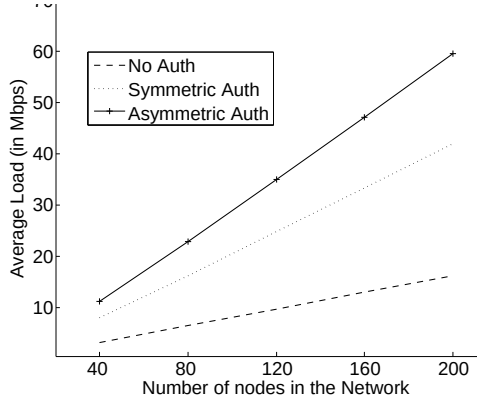


Fig. 6. Average load in topologies with increasing number of nodes

To evaluate the average signaling load we provided each node with an average arrival rate of 1 path request/sec, and destinations were uniformly distributed among all other nodes in the network. Figure 6 shows how the load increases with the increasing number of nodes in the network, with the increasing rate higher in asymmetric than symmetric authentication, and this one higher than the scenario without authentication. This is due to the size of the ERO and the AuthObject of the NSIS-LSP message that depends on the number of hops and the different size of the AuthObject for symmetric and asymmetric authentication. Note that the load for asymmetric authentication increases faster but always linearly. The delay and load information results confirm the higher cost of the asymmetric mechanism and suggest that for big networks symmetric authentication mechanisms should be used. However, given the high management cost for maintaining pre-shared keys in a large network, a combination of symmetric and asymmetric mechanisms inside the same signaling session is a more likely implementation for the future.

VI. Conclusion

In this paper we focused on security aspects of label switching path setup across multi-domain networks. We proposed a new signaling solution based on the NSIS protocol that supports both symmetric and asymmetric key-based mechanisms for mutual authentication between source and all provisioning domains. The domains provide resources on the base of identity of users and provide protection against attacks to the offered route of the path. The mutual authentication mechanism proposed is based on a four-way handshake between the parties that have to authenticate and its robustness does not depend on the hop-by-hop security chain between neighboring nodes. We also implemented the verification method and our simulations have shown that the model is scalable with the increased size of the network with the asymmetric authentication mechanism, while measuring higher delay and load overhead. Our future work will investigate the performances of the NSIS-LSP application while using different transport solutions supported by NSIS and extending the NSIS-LSP application for finer authorization with mechanisms that allow differentiation among multiple authorization profiles.

Acknowledgment

This work was partially supported by Deutsche Forschungsgemeinschaft (DFG) under support code JU2757/-1/1.

References

[1] L. Berger, *Generalized Multi-Protocol Label Switching(MPLS) Signaling Functional Description*, RFC 3471, January 2003.
[2] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan and G. Swallow, *RSVP-TE: Extensions to RSVP for LSP Tunnels*,RFC 3209, December 2001.
[3] *http://www.tmforum.org/ipsphere*.
[4] H. Tschofenig and R. Graveman, *RSVP Security Properties*, RFC 4230, December 2005.
[5] S. Herzog, *RSVP Extensions for Policy Control*, RFC 2750, January 2000.
[6] A. P. Bianzino, J.-L. Rougier, S. Secci, R. Casellas, R. Martinez, R. Munoz, N, Bachit, R. Douville and H. Pouyllau, *Testbed Implementation of Control Plane Extensions for Inter'Carrier GMPLS LSP Provisioning*, International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, Washington (USA), April 2008.
[7] S. Greco Polito, M. Chamania and A. Jukan, *Extending the Inter-domain PCE Framework for Authentication and Authorization in GMPLS Networks*, International Conference on Communications, Dresden, Germany, June 2009.
[8] R. Hancock, G. Karagiannis, J. Loughney and S. Van den Bosch, *Next Steps in Signaling (NSIS): Framework*, RFC 4080, June 2005.
[9] X. Gu, H. Schulzrinne, H. Tschofenig, C. Dickmann and D. Hogrefe, *Overhead and performance study of the general internet signaling transport (GIST) protocol*, IEEE/ACM Transactions on Networking , Volume 17 , Issue 1 , Pages 158-171, 2009.
[10] The Free Next Steps In Signaling (FreeNSIS) Implementation, *http://user.informatik.uni-goettingen.de/ nsis/download.html*.
[11] http://www.openssl.org/
[12] T. Bu and D. Towsley, *On distinguishing between Internet power law topology generators*, in Proceedings of IEEE Infocom 2002, New York, NY, Jun. 2002.