Science in China Series F: Information Sciences

© 2008 SCIENCE IN CHINA PRESS

www.scichina.com
info.scichina.com

Building a next generation Internet with source address validation architecture

WU JianPing[1,3†], REN Gang[1,3] & LI Xing[2,3]

[1] Department of Computer Science, Tsinghua University, Beijing 100084, China;
[2] Department of Electronic Engineering, Tsinghua University, Beijing 100084, China;
[3] Tsinghua National Laboratory for Information Science and Technology (TNList), Beijing 100084, China

The IP packet forwarding of current Internet is mainly destination based. In the forwarding process, the source IP address is not checked in most cases.This causes serious security, management and accounting problems. Based on the drastically increased IPv6 address space, a "source address validation architecture" (SAVA) is proposed in this paper, which can guarantee that every packet received and forwarded holds an authenticated source IP address. The design goals of the architecture are lightweight, loose coupling, "multi-fence support" and incremental deployment. This paper discusses the design and implementation for the architecture, including inter-AS, intra-AS and local subnet. The performance and scalability of SAVA are described. This architecture is deployed into the CNGI-CERNET2 infrastructure — a large-scale native IPv6 backbone network of the China Next Generation Internet project. We believe that the SAVA will help the transition to a new, more secure and dependable Internet.

IP source address validation, network architecture, network security

1 Introduction

The packet forwarding of current Internet is mainly destination based. In the forwarding process, the source IP address is not checked in most cases. This makes it very easy to spoof the source address of the IP packet. Attackers commonly forge source IP addresses to evade responsibility for their malicious packets. It has been recognized that packet source IP address validation is one of the most important challenges for Internet.

There have been many efforts in the research and engineering community to design mechanisms related to the validation of source IP addresses, such as cryptographic authentication based methods, traceback based methods, and filtering based methods. However, these mechanisms are

Received June 3, 2008; accepted July 30, 2008
doi: 10.1007/s11432-008-0142-x

†Corresponding author (email: jianping@cernet.edu.cn)

Supported by the National Natural Science Foundation of China (Grant No. 90704001), and the National Basic Research Program of China (973 Program) (Grant No. 2003CB314800)

not widely deployed in the Internet due to two reasons: the incremental deployment is not well supported and the incentive for ISPs to deploy these mechanisms is relatively low.

In this paper, we propose a "source address validation architecture" (SAVA) to provide a transparent network service to ensure that every packet received and forwarded must hold an "authenticated source IP address".

For the purposes of SAVA, the meaning of "authenticated source IP address" can be described as follows:

- Authorized. The address must be authorized by Internet address authorization organization and not be forged.
- Unique. The source IP address is globally unique except for the cases where global uniqueness is specifically excluded.
- Traceable. The packet is traceable to its origin using the source IP address. That is, information about the address's location and ownership is verifiable and correct.

This architecture would be very valuable for the following two main requirements. Firstly, the traffic in network can be traced back accurately. For every packet received and forwarded, not only where it goes to, but also where it comes from can be verified. Secondly, the packets that do not hold an authenticated source address will not be forwarded in network. Therefore, it is impossible to launch network attacks with spoofed source addresses.

There are many additional benefits if the authenticity and global uniqueness of the source IP addresses are ensured.

- Network management and accounting can be achieved with fine granularity. Because it is easy to map users or their applications to authenticated IPv6 addresses, network management systems can easily bill users based on their end-to-end usage, as is the case with telephony.
- The authentication of the application can be simplified. Traditional authentication mostly uses cryptographic methods. If the SAVA is supported, the authentication can be divided simply into two steps. First, identity of the entity can be mapped to an IPv6 address. Second, in packet forwarding, the authenticated IPv6 address represents the identity of the sending entity.
- New Internet applications, such as P2P applications and other large scale multimedia applications (for example VoIP using SIP), can be accelerated in deployment and improved in performance by using globally unique authenticated IPv6 addresses.

While SAVA is applicable for IPv4 networks, it is designed for IPv6 networks for the following two reasons. First, the current Internet addressing architecture using IPv4 has been in operation for many years, therefore, it is quite difficult and not cost-effective to deploy SAVA in the current Internet. Second, NAT is wildly used in current Internet because of the limited IPv4 address space. The large address space of IPv6 makes it possible for every end host to have a globally unique authenticated IP address.

The rest of this paper is organized as follows. In section 2, we briefly survey related works. The design principles and the hierarchical architecture of SAVA are presented in section 3. The protocol designs of Inter-AS SAVA and scalability analysis are given in section 4. In section 5, as a case study, we describe the deployment of SAVA, in CNGI-CERNET2 infrastructure, a large-scale native IPv6 backbone of the China Next Generation Internet project. In section 6, we summarize the paper and comment on the future work.

2 Related works

The related works used to validate source addresses can be divided into three categories: cryptographic authentication, proactive filtering and reactive traceback.

Cryptographic authentication is a valid solution. Examples include IPSec[1] and SPM[2]. IPSec is an end-to-end solution, and its large-scale deployment depends on global PKI. SPM is an AS to AS solution, and a unique temporal key is associated with each ordered pair of source and destination networks for filtering. With these approaches the spoofed source address can only be validated at destination.

Filtering is a proactive solution. It filters forged packets at the router, based on filtering rules for valid source addresses. Examples include Ingress Filtering[3], DPF[4], SAVE[5] and HCF[6]. Ingress filtering is deployed at the edge network, but it needs full-scale deployment to be effective. DPF extends the deployment position from edge to core network, and supports partial deployment, but it only has AS level granularity. SAVE has a new protocol to propagate valid source address information from the source location to all destinations, allowing each router along the route to build an incoming table which associates each incoming interface of the router with a set of valid source IP address blocks, but it is not layered. There are problems in deployment and scalability. All the filtering methods have a disadvantage that they cannot handle IP address spoofing in a subnet where the network prefix is correct.

Traceback is a reactive solution. It records the path information when the packet is forwarded, and traces back to the source of the forged packets from their destinations. Works include SPIE[7], iTrace[8], iTrace-CP[9], PPM[10], and DPM[11]. SPIE records path information at routers. ITrace and iTrace-CP use ICMP message to reserve path information. PPM and DPM directly use IP packet to record path information. Reactive nature of the solution, complexity of traceback algorithms and dependence on the sensitivity of IDS are the disadvantages of this class of mechanisms.

These methods deal with part of the validation of source addresses. However, there are no feasible systemic solutions with the current addressing architecture. We proposed a Source Address Validation Architecture (SAVA)[12] and submitted this work to the Internet Engineering Task Force (IETF). One RFC on SAVA testbed[13] has been published, and several Internet Drafts have been submitted on the topic of solution[14], framework[15], and problem statement[16]. These will be described in detail in the rest of this paper.

3 Source address validation architecture

3.1 Design principles

In the design of SAVA, the following design principles should be considered.

- Performance. Deployment of SAVA should not place unreasonable stress on network infrastructure components.
- Scaling. SAVA must be capable of scaling to the size of the global Internet.
- Multiple-fence solution. SAVA should support hierarchical multi-fence solutions to provide different granularities of authenticity of source IP address.
- Loose components coupling. SAVA should allow for different providers to use different solutions, and the coupling of components at different levels of granularity of authenticity should be loose enough to allow component substitution.

- Incrementally deployable. SAVA should show its benefit even if it is deployed only in part of the Internet. If there is no benefit for partial deployment, it is hard to start.
- Benefit to operator. The mechanism should have direct benefit to the party who makes investment on the deployment of the mechanism. Otherwise there is not enough incentive for the global deployment.

3.2 Hierarchical architecture

It is not to be expected that there will be a single mechanism applied at a single "level" that can solve the source address spoofing problem in the Internet at large. Since the Internet is organized as a hierarchical architecture, it is natural to consider organizing the SAVA mechanisms in a hierarchical way, too. Therefore we divided SAVA into three levels: first-hop, local subnet source address validation, intra-AS source address validation, and inter-AS source address validation, as in Figure 1.

Different levels of SAVA get different granularities of the authenticity of source address. At each level in the hierarchical architecture, one or more mechanisms are defined to address the problem of source address validation at that level. This particular hierarchy is chosen as a balance between allowing as much choices as possible for implementers and providers and keeping the architecture as simple as possible.

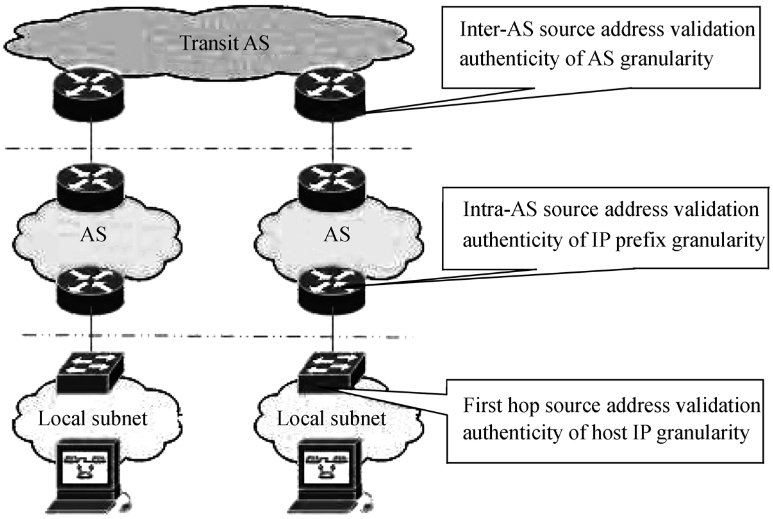

Transit AS
Inter-AS source address validation
authenticity of AS granularity
AS
AS
Intra-AS source address validation
authenticity of IP prefix granularity
Local subnet
Local subnet
First hop source address validation
authenticity of host IP granularity

Figure 1 Source address validation architecture.

(1) First-hop, local subnet source address validation. It is an important part of the architecture to achieve an authenticity of host IP granularity. If there is no special consideration of source validation of this fine granularity, one host can still spoof source address by sending packet with the "legal" IP address of another host with the same IP prefix.

It has the following characteristics:

- All the network devices are under the same administrative authority.
- The solution is in compliance with the address allocation and management policy of the local subnet.
- The solution is in compliance with the way that end host access the Internet.

For the instance that many end host access the Internet through switches, the main idea of the proposed solution is based on creating a dynamic binding between a switch port and valid source IP address, or a binding between MAC address, source IP address and switch port.

Mobility is one of the main characters of the next generation Internet. For the mobile nodes which access the Internet using Mobile IPv6 protocol, sometimes the Home Address and the Care of Address cannot match the source address validation rule in the same time. This instance must be taken into consideration. The packet should not be simply dropped, and it should be carefully handled for different types of connection.

(2) Intra-AS source address validation. It is a simple part of the architecture. The goal is to achieve an authenticity of IP address prefix granularity. It has the characteristic that all the network devices are under the same administrative authority.

The main idea of the proposed solution is to build a filtering table that associates each incoming interface of the router with a set of valid source address blocks. Because the AS is under the same administrative authority, this filtering only needs to be deployed in the access router near the subscriber's network. Ingress filtering is proposed as a solution.

(3) Inter-AS source address validation. It is the most complex part of the architecture. The goal is to achieve an authenticity of AS level granularity.

It has the following characteristics:

- It should cooperate among different ASs with different administrative authorities and different interests.
- It should be lightweight to support high throughput and not to influence forwarding efficiency.

The proposed solution and protocol design of Inter-AS source address validation are described in detail in section 4.

Thus the problem of source address validation has been divided into three parts. Different parts get different granularities of the authenticity of source address. In the edge network, fine granularity source address validation is deployed, while in the core network, only AS granularity source address validation is deployed. These avoid the source address validation mechanism to become a bottleneck of the network.

3.3 Architecture of SAVA-compliant network node

SAVA is implemented by the deployment of solutions in the network nodes. The network nodes can be switches, routers and gateways. Figure 2 shows the architecture of SAVA-compliant network node, which contains the following major logical parts.

- Forwarding information database. This database contains packet forwarding information.
- Source validating information database. This database contains source validating information.
- Routing/switching protocols. This module exchanges forwarding information among network nodes and updates forwarding information database.
- SAVA protocols. This module exchanges source address validating information among network nodes and updates source validating information database.
- Forwarding engine. This module forwards data packets according to forwarding information database.
- Source validating engine. This module filters incoming data packets according to source validating information database and transfers legal packets to packet forwarding engine.

Forwarding information database, routing/switching protocols, and forwarding engine are the modules of the current forwarding function. Source validating information database, SAVA protocols and source validating engine are the modules of new source validation function.

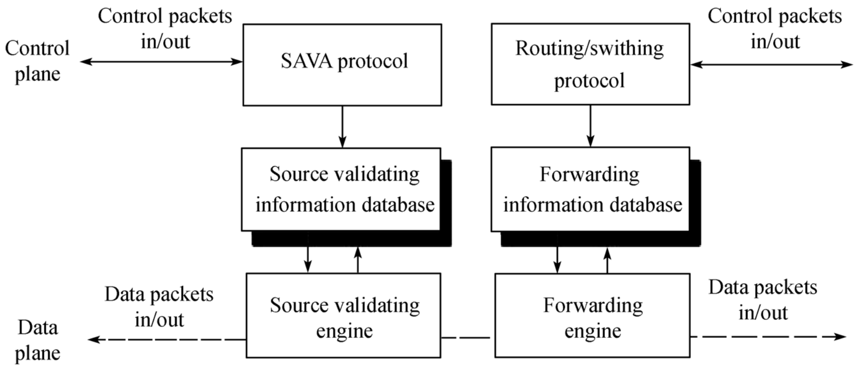


Figure 2 Architecture of SAVA-compliant network node.

The module of SAVA protocols is a control plane component. Control plane components in general have the advantage of being able to be implemented in software, either in the control planes of existing network forwarding elements or in servers external to existing network elements. The module of source validating engine is a data plane component. Data plane components typically need to be implemented in hardware (or at least in microcode) on line cards.

4 Inter-AS source address validation

4.1 Overview

All the SAVA-compliant ASs form a trust alliance (TA). The inter-AS level of SAVA can be classified into two sub-cases:

- Two SAVA-compliant ASs exchanging traffic are directly connected.
- Two SAVA-compliant ASs are separated by one or more intervening, SAVA-non-compliant providers.

To generate inter-AS validation rules (VR) of the source validating information database in network nodes some information should be exchanged among network nodes. According to the types of information exchanged among network nodes, the mechanisms can be classified into two categories:

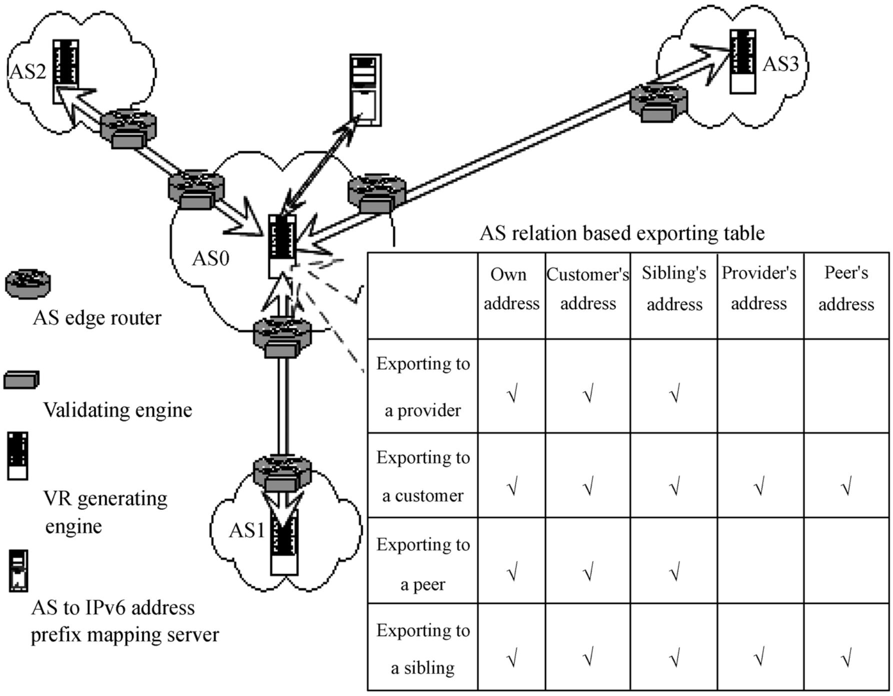
- Path/route based mechanisms. The VR is derived from the path that the packet is transmitted along or from the routing information base. The advantage of this mechanism is that the VR is directly in the form of IP prefix. The disadvantage of this mechanism is the network nodes generating the VR must be neighboring with each other.
- Mark/signature based mechanisms. Such mechanisms rely on some additional information (e.g. Mark/Signature) to check the authenticity of the source address. The advantage of this mechanism is that the network nodes generating the VR are not required to be neighboring with each other. The disadvantage of this mechanism is the overhead to negotiate mark/signature for each peer, if the total number of peers is relatively large.

The case where the two SAVA-compliant ASs are directly connected is our main focus of the design. An AS relation based mechanism is proposed for neighboring SAVA-compliant ASs. This is a path/route based mechanism. For the integrality of the system, a lightweight tag based mechanism is proposed for non-neighboring SAVA-compliant ASs.

4.2 System design of neighboring ASs

An AS relation based mechanism is proposed for neighboring SAVA-compliant ASs. The basic ideas of this AS-relation based mechanism are as follows. It builds a VR table that associates each incoming interface of the router with a set of valid source address blocks, and then uses it to filter spoofed packets. The VR is generated from the AS relation of neighboring SAVA-compliant ASs. The AS relations determine the inter-AS routing polices. The inter-AS routing polices determine the BGP routing, and the BGP routing table is the primary information to generate the inter-AS forwarding table. Using AS relations to create VR has a very low overhead and is simple to implement in routers. It does not directly rely on routing information and the AS relation is relatively stable. Consequently, it is not affected by the dynamics of route changes and route flaps.

There are three major components in the system: the validation rule generating engine (VRGE), the validation engine (VE) and the AS-IPv6 prefix mapping server (AIMS). Validation rules (VR) that are generated by the VRGE are expressed as IPv6 address prefixes. They are shown in Figure 3.



AS relation based exporting table

	Own address	Customer's address	Sibling's address	Provider's address	Peer's address
Exporting to a provider	√	√	√		
Exporting to a customer	√	√	√	√	√
Exporting to a peer	√	√	√		
Exporting to a sibling	√	√	√	√	√

Figure 3 AS relation based inter-AS source address validation.

- The VRGE generates validation rules, and every SAVA-compliant AS has a VRGE. It communicates with VRGEs in other AS to exchange VR information. It communicates with all VEs of the local AS to configure the VR information.

- The VE loads VR generated by VRGE to filter packets passed between SAVA-compliant ASs.

- The AIMS maintains the IP prefix ownership information of all SAVA-compliant ASs. It should support both mapping from IP prefix to AS number and mapping from AS number to all

IP prefixes owned (by an ISP).

There are four kinds of AS relation: customer-to-provider relation, provider-to-customer relation, peer-to-peer relation and sibling-to-sibling relation, as described in ref. [17].

For an AS, VRO, VRC, VRS, VRP and VRE are defined to be VR sets from the local AS, customer AS, sibling AS, provider AS and peer AS. EVRC, EVRS, EVRP and EVRE are defined to be VR sets exported to customer AS, sibling AS, provider AS and peer AS.

- EVRC=VRO∪VRC∪VRS∪VRP∪VRE,
- EVRP=VRO∪VRC∪VRS,
- EVRS=VRO∪VRC∪VRS∪VRP∪VRE,
- EVRE=VRO∪VRC∪VRS.

Different ASs exchange VR information using this AS-relation-based exporting table in the VRGE. This is shown in Figure 3. An AS exports the address prefixes of its own, its customers, providers, siblings and peers to its customers and siblings as valid prefixes, while it only exports the address prefixes of its own, its customers and siblings to its providers and peers as valid prefixes.

With the support of AIMS, only AS numbers of valid IP address prefixes are transferred between ASs and the AS number is mapped to address prefixes at the VRGE. The overhead of communication between AS members should be relatively low. Only changes of AS relation and changes of IP address prefixes belonging to an AS require the generation of VR updates.

4.3 System design of non-neighboring AS

A lightweight tag based mechanism is proposed for non-neighboring SAVA-compliant ASs. The basic ideas of this lightweight tag based mechanism are as follows. For every two SAVA-compliant ASs, there is a pair of unique temporary tags. All SAVA-compliant ASs form SAVA AS Alliance. When a packet is leaving its own AS, if the destination IP address belongs to an AS in the SAVA AS Alliance, the edge router of this AS looks up for the tag based on the destination AS number, and tags a tag to the packet. When a packet is arriving at the destination AS, if the source address of the packet belongs to an AS in the SAVA AS Alliance, the edge router of the destination AS looks up for the tag based on the source AS number, and the tag carried in the packet is verified and removed.

There are three major components in the system: the Registration Server (REG), the AS Control Server (ACS), and the AS Edge Router (AER). They are shown in Figure 4.

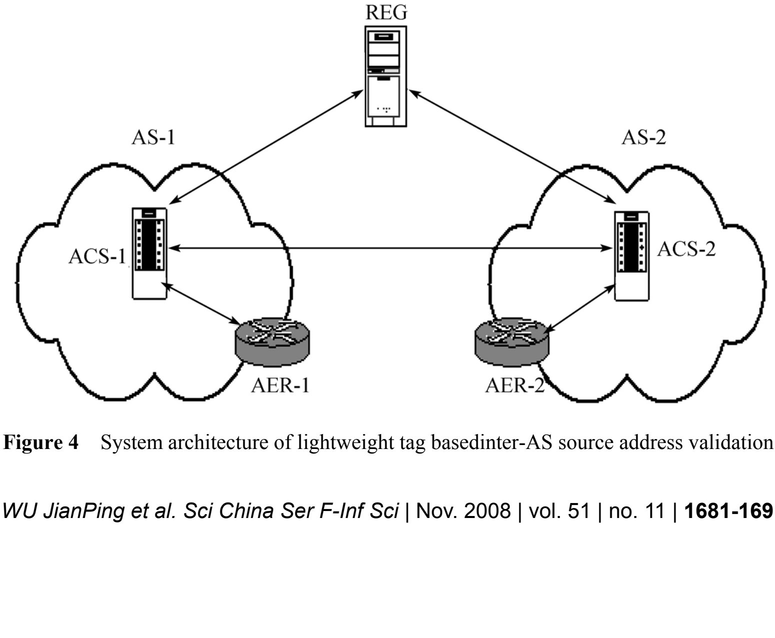


Figure 4 System architecture of lightweight tag basedinter-AS source address validation.

● The Registration Server maintains a member list for the SAVA AS Alliance. It processes requests from the AS Control Server to get the member list for the SAVA AS Alliance. When the member list is changed, it notifies each AS Control Server.

● Every AS deploying this mechanism should have an AS Control Server. It communicates with the Registration Server to obtain the up-to-date member list of SAVA AS Alliance. It communicates with the AS Control Server in other AS to exchange updates of IP prefix ownership information and to exchange tags. It communicates with all edge routers of the local AS to configure the tags information.

● The AS Edge Router does the work of adding tag to the packet at the sending AS and the work of verifying and removing the tag at the destination AS.

For every packer forwarded, the tag can be put in an IPv6 extension header. Figure 5 shows the format of the extension header.

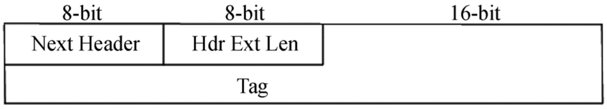


Figure 5 IPv6 extension header for lightweight tag based inter-AS source address validation.

The tag in the incoming packet is removed after AER validates the packet. Under the assumption that it is hard for an attacker to sniff the backbone network between ASs, the method for guessing the tag between two AS members is described in ref. [2]. It is relatively difficult and we can increase the difficulty of guess by increasing the length of the tag. Here we can use a 128-bit shared random number as the tag, instead of using cryptographic method to generate the tag. During the period of tag refresh, after having negotiated a new tag, the old tag should be set to be invalid after a period of time. The length of this period is a parameter that will control how long the old tag will be valid after the new tag has been assigned. In the experiment, we used five seconds and get no packets dropped by mistake.

4.4 Scalability analysis

The inter-AS source address validation solutions have fine scalability. When the number of the ASs that joins the Trust Alliance increases, the solutions can still work well. This section analyzes the scalability of the solutions.

The Internet can be abstracted as an undirected graph G (W; N; F). W is the set of nodes and every node represent an AS. N is the set of SAVA-compliant ASs. $N \in W$. N is just the set of Trust Alliance. F is the set of edge. Every edge represents a direct connection between two ASs.

We make the following set.

● n is the number of elements which needs to negotiate the tag in the Trust Alliance.

● t is the total number of transit AS in G.

● a is the total number of AS in G.

● v is a new AS joining the Trust Alliance.

● if □$v_i \in N$, and edge $vv_i \in F$, deploy AS relation based source address validation mechanism between v and v_i. Here v and v_i combine to a new element, and negotiate the tag with other elements in the Trust Alliance.

Lemma 1. $n \leqslant$ the independence number of G.

Proof. From the former setting, we know that n is the number of elements that needs to negotiate the tag in the Trust Alliance. If □$v_i \in N$, and edge $vv_{\mathrm{i}} \in F$, deploy AS relation based source address validation mechanism between v and v_i. Here v and v_i combine to a new element, and negotiate the tag with other elements in the Trust Alliance.

Thus from the definition of independence number in Graph Theory, we can make a conclusion: $n \leqslant$ the independence number of G.

Lemma 2. The set of transit AS nodes of G is the minimum dominating set of G.

Proof. For an AS node of G, it is either a transit AS, or a stub AS. A stub AS must connect to one or more transit AS.

From the definition of minimum dominating set in Graph Theory, the set of transit AS nodes of G is the minimum dominating set of G.

Theorem. $n \leqslant a-t$.

Proof. From Lemma 1, $n \leqslant$ the independence number of G.

From Lemma 2, t is the dominating number of G.

From a theorem of Graph Theory, the independence number + the dominating number = a.

Thus $n \leqslant a-t$.

With the incremental deployment of SAVA, when n get the maximum $a-t$, any new AS join to N will lead to the decrease of n. When $N=W$, $n=1$. Only AS relation based source address validation is needed. Thus n is limited and the solutions have scalability.

5 Deployment

The prototypes of our solutions for SAVA are implemented and tested over CNGI-CERNET2. The deployment of SAVA has been carried out with the participation of network equipment manufacturers.

CERNET2 is one of the China next generation Internet (CNGI) backbones. CNGI-CERNET2 connects 25 core nodes distributed in 20 cities in China at speeds of 2.5—10 Gb/s. The CNGI-CERNET2 backbones are IPv6-only networks, not the mixed IPv4/IPv6 infrastructure. The CNGI-CERNET2 backbones, CNGI-CERNET2 CPNs, and CNGI-6IX all have globally unique AS numbers. Thus a multi-AS environment is provided.

The deployment is distributed across 12 universities connected to CERNET2, namely Tsinghua University, Beijing University, Beijing University of Post and Telecommunications, Shanghai Jiaotong University, Wuhan Polytechnic University, Southeast University in Nanjing, South China Polytechnic University in Guangzhou, Northeast University in Shenyang, Xi'an Jiaotong University, Shandong University in Jinan, University of Electronic Science and Technology of China in Chengdu, and Chongqing University. They are shown in Figure 6. Every deployment of the university is connected to the CERNET2 backbone network through a set of inter-AS SAVA mechanisms. The deployment at Tsinghua University has all the features with inter-AS, intra-AS and first hop solutions.

Tests on function, stability and performance have been carried out. Successful results were achieved. The details of the testbed and test result have been submitted to the Internet Engineering Task Force (IETF) and published as RFC5210[13].

6 Conclusion and future work

We have proposed a “Source Address Validation Architecture” (SAVA) for IPv6 network to en-

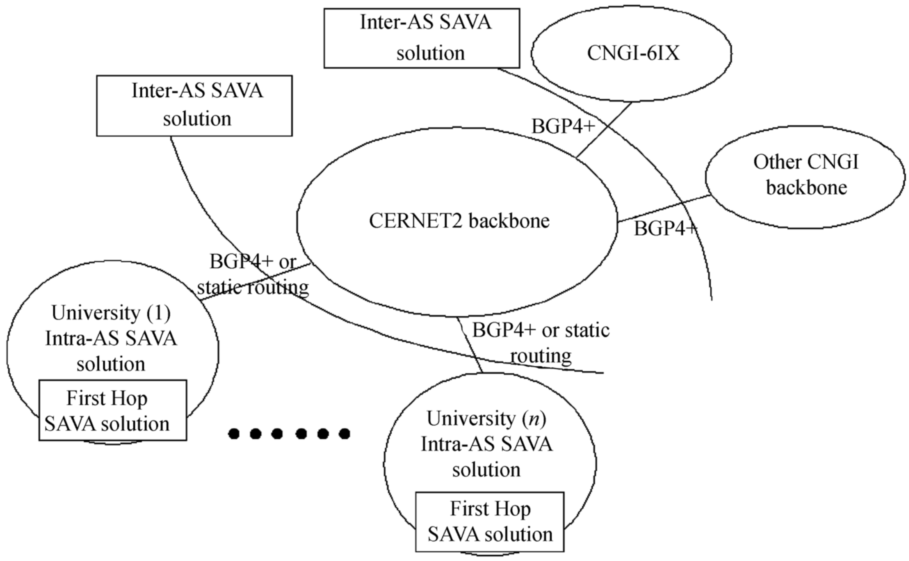


Figure 6 CNGI-CERNET2 SAVA deployment.

sure that every packet received and forwarded must hold an authenticated source IP address. The architecture divides the problem of source address validation into three parts: inter-AS, intra-AS, and first hop. The architecture and protocol design are described in detail. The architecture has the properties of being lightweight, loosely coupled, and providing “multi-fence support”. It supports incremental deployment and is beneficial even if deployed only in a single AS of the Internet. SAVA may greatly improve network security, management, accounting, and new applications. We believe that SAVA will support a new, more secure and dependable Internet.

Our future work will focus on building a related trust model for SAVA and improving the performance and protocol design of the multiple solutions for SAVA.

1 Kent S, Atkinson R. RFC2401. Security Architecture for the Internet Protocol. IETF, 1998
2 Bremler-Barr A, Levy H. Spoofing Prevention Method. IEEE INFOCOM, 2005
3 Ferguson P, Senie D. RFC2827. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. IETF, 2000
4 Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM, 2001
5 Li J, Mirkovic J, Wang M, et al. SAVE: Source address validity enforcement protocol. IEEE INFOCOM, 2002
6 Jin C, Wang H. Hop-count filtering: an effective defense against spoofed DDoS traffic. ACM CCS, 2003
7 Snoeren A, Partridge C, Sanchez L, et al. A Hash-based IP traceback. ACM SIGCOMM, 2001
8 Bellovin S, Leech M, Taylor T. ICMP traceback messages. IETF Internet Draft, draft-ietf-itrace-03, 2003
9 Lee H, Thing V, Xu Y, et al. ICMP traceback with cumulative path, an efficient solution for IP traceback. Information and Communications Security. LNCS, 2003. 124—135
10 Savage S, Wetherall D, Karlin A, et al. Practical network support for IP traceback. ACM SIGCOMM, 2000
11 Belenky A, Ansari N, IP traceback with deterministic packet marking. IEEE Commun Lett, 2003, 7(4): 162－164
12 Wu J, Ren G, Li X. Source address validation: Architecture and protocol design. ICNP, 2007
13 Wu J, Bi J, Li X, et al. RFC5210. A source address validation architecture (SAVA) testbed and deployment experience. IETF, 2008
14 Wu J, Ren G, Bi J, et al. A first-hop source address validation solution for SAVA. IETF Internet Draft, draft-wu-sava-solution-firsthop-eap-00, 2007
15 Wu J, Bi J, Ren G, et al. Source Address validation architecture (SAVA) framework. IETF Internet Draft, draft-wu-sava-framework-01, 2007
16 Wu J, Ferguson P, Bi J, et al. Source Address verification architecture problem statement. IETF Internet Draft, draft-sava-problem-statement-02, 2007
17 Gao L. On inferring autonomous system relationships in the Internet. IEEE/ACM Trans Network-Ing, 2001, 9(6): 733－745