doi:10.3969/j.issn.1000-436x.2014.10.018

穿越自治系统联盟的域间路由安全机制

孔令晶，曾华燊，窦军，李耀
(西南交通大学 信息科学与技术学院，四川 成都 610031)

摘 要：通过对 SE-BGP (security enhanced BGP)的研究与分析，发现此方案不仅无法认证动态变化的跨联盟 AS (autonomous system)，也无法抵御其自身所发起的主动攻击。为了解决 SE-BGP 存在的安全问题，设计了二层跨联盟等级结构 CAHS (cross-alliance hierarchical structure)，基于 CAHS 结构，借鉴护照签证思想，利用递增散列——AdHASH (additive hash)的特性提出了一种跨联盟安全机制 SCA-BGP(secure crossing alliance for BGP)。该机制具有更高的安全性，可以有效地认证跨联盟 AS 的身份及行为授权，还可对其所携带的信息进行安全验证。实验分析表明，SCA-BGP 可以有效地减少所需证书的规模和额外的时间开销，具有更好的可扩展性和网络收敛性能。

关键词：SE-BGP；SCA-BGP；跨联盟 AS；递增散列
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)10-0155-10

Inter-domain routing security mechanism for crossing autonomous system alliance

KONG Ling-jing, ZENG Hua-xin, DOU Jun, LI Yao
(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: Through studying and analyzing SE-BGP (security enhanced BGP), it was found that it couldn't validate the cross-alliance AS (autonomous system) and defense the self-launched active attack. To solve the security problems, two-layer cross-alliance hierarchical structure CAHS (cross-alliance hierarchical structure) was designed. Based on CAHS, using the idea of passport visa and the features of AdHASH (additive hash), a cross-alliance BGP security mechanism SCA-BGP (secure crossing alliance for BGP) was proposed. The mechanism has higher security, which is able to effectively validate the identities and behavior authorization of the cross-alliance AS as well as the message carried by them. The experiment results show that SCA-BGP can effectively reduce the certificate scale and extra time overhead to get better scalability and convergence performance.

Key words: SE-BGP; SCA-BGP; cross-alliance AS; AdHASH

1 引言

边界网关协议 BGP(border gateway protocol)[1]实现了自治系统 AS(autonomous system)之间路由信息的转发和交换，在整个网络中承担了重要的角色。然而，在 BGP 设计之初，并没有考虑其安全因素，所以 BGP 机制本身的漏洞和弱点很容易被攻击者利用进而实施攻击，导致局部网络或整个网络陷入瘫痪。一个典型案例是 2008 年巴基斯坦发生的 YouTube 错误路由事件。此次事件致使该网站在全球完全瘫痪了一个小时，直到 2 小时后才得以恢复通信。类似的事件表明，BGP 存在的安全问题给网络带来的危机绝对不可小视。

BGP 存在的安全问题主要集中在 2 个方面。1）会话的安全性：BGP 是一种基于 TCP 的协议，由于因特网中缺少独立的会话层，因此 BGP 对等

收稿日期：2013-07-17；**修回日期**：2013-09-10
基金项目：国家自然科学基金资助项目(60773102)；国家自然科学基金与中国工程院联合基金资助项目（U0970122）
Foundation Items: The National Natural Science Foundation of China (60773102); Chinese Academy of Engineering and the National Natural Science Foundation of China (U0970122)

体之间的会话直接利用 TCP 来连接，而 TCP 连接有可能遭受第三方的篡夺，进而窃听或篡改连接内的信息；2）路由信息的安全性：BGP 通过 Update 消息传递可达信息，无论是内部攻击者和还是外部攻击者都可以通过篡改地址前缀或路径属性达到改变路由信息，引发黑洞或达到拒绝服务的目的。

近些年来，针对 BGP 的安全性问题，业界人士提出了多种解决方案，主体上可以分为 2 大类：基于密码学的主动解决方案和基于路由检测的被动解决方案。第一类解决方案的典型代表是 S-BGP(secure BGP)[2]，它通过“集中式”的 PKI 下发认证证书，使用“洋葱模式”的签名方式保证路由信息的安全性，但是额外的性能开销、较差的可扩展性和难以实施的方案部署都使此方案在可行性方面大打折扣。soBGP(secure origin BGP)[3]及 psBGP(pretty secure BGP)[4]都试图在安全性和可行性方面寻找到平衡点。soBGP 采用忽略了可信锚(信任的起点)的“信任网”认证模式和仅仅基于可行路径的路径验证方式，而 psBGP 通过引入评估机制来实现地址前缀的验证。这些方式都给方案带来了不可小觑的安全隐患。并且，迄今为止，这些方案均未能解决 S-BGP 的可扩展性及部署问题。就在 2008 年，SE-BGP (security enhanced BGP)[5]解决方案在降低了传统方案性能开销的同时，很好地弥补了可扩展性和方案部署方面所存在的不足，但此方案却存在一定的安全漏洞(详见 3.2 节)。SA-BGP(secure aggregation BGP)[6]是基于 SE-BGP 的研究成果，却不能对所有跨联盟 AS 的身份以及动态跨联盟行为的合法性进行识别。第二类解决方案通过检测路由信息的异常从而确保 BGP 的安全性，其中较为典型的 PGP(pretty good BGP)[7]利用延迟转发所接收到的路由更新信息来检测信息的合法性，最终保证 BGP 的安全。此外，Listen and Whisper[8]和 RRVT(remote routing validation tool)[9]也属于此类解决方案。但是与基于密码学的主动型解决方案相比，就其安全性方面处于劣势。

综上所述，第一类解决方案一直以来都是 BGP 安全研究工作的主流，本文同样从密码学角度出发，全面研究 SE-BGP 的不足，提出了跨联盟安全机制 SCA-BGP(secure crossing alliance for BGP)，用于解决 SE-BGP 所存在的安全漏洞，并通过实验证明此方案具有更好的可扩展性和网络性能。

2 SE-BGP 的结构与信任模型

2.1 整体结构

整个互联网是由无数个 AS 组成的，每个 AS 之间存在着商业关系——“提供商-客户”关系、“对等”关系和“兄弟”关系[10]。这种 AS 级网络的拓扑关系可以看作是一个无向连接图，每个 AS 为无向图中的节点，AS 之间的关系为无向图中的边。文献[11]发现 AS 拓扑存在着 rich-club 现象，即少数具有大量连接的节点彼此相互连接，也就是说网络中的节点总是聚集成不同的集合，而这些集合通过少数的高度数节点与集合外的节点相互连接，这些少数节点称之为 rich 节点，rich 节点是网络拓扑结构中 rich-club[11]现象的“核心层”(core tier)节点。

基于 rich-club 现象，文献[5]提出了 AS 联盟。所谓 AS 联盟，就是一组 AS 节点的集合，集合中的节点通过少数的 rich 节点与集合外的节点相连，而这些少数 rich 节点又称为关键节点。具体的生成算法是：首先从 rich 节点中确立关键节点，将关键节点作为一个 AS 联盟中的第 1 个节点；然后将属于这个关键节点的所有其他非关键节点的客户节点加入到 AS 联盟中，如果加入的客户节点还有其他非关键节点的客户节点，则继续加入，直到所有非关键节点的客户节点加完为止。实际操作中，会考虑对 AS 联盟范围的调整。SE-BGP 将建立了 PKI 的 AS 联盟称为“安全 AS 联盟”，记为 SA，如图 1 所示。

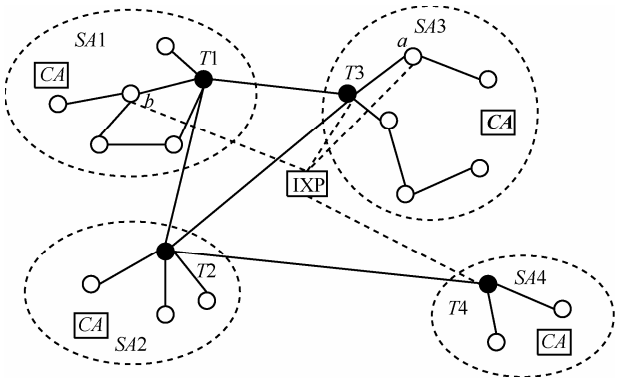


图 1 AS 联盟

图 1 中，*SA*1、*SA*2、*SA*3、*SA*4 为 AS 联盟，*T*1、*T*2、*T*3、*T*4 是关键节点，*CA* 是每个联盟内部的证书签发机构。

2.2 转换者信任模型 TTM

SE-BGP 方案中，不同联盟的 *CA* 之间并不互

相认证证书，联盟之间的信息认证完全依赖于互相连接的关键节点。如图 1 所示，关键节点 *T*1 和 *T*3 同时拥有来自 *SA*1 和 *SA*3 的 2 套证书，同一个 *CA* 所颁发的私钥和相对应的公钥证书为一套证书。

TTM 模型的原理如下：如果 *SA*3 的节点 *a* 欲将信息 *m* 发布至 *SA*1 的节点 *b*，*T*3 接收到来自节点 *a* 的信息 *m* 后，使用 *SA*3 中的 *CA* 分配的公钥进行验证，如果验证成功，使用 *SA*1 中的 *CA* 分配的私钥对信息内容 m_{a-T3} 进行签名，得到 $S_{T3}(m_{a-T3})$。当 *T*1 接收到信息后，使用 *T*3 在 *SA*1 中的公钥证书验证 $S_{T3}(m_{a-T3})$，如果验证成功，则用 *SA*1 中的 *CA* 所分配的私钥进行签名，记为 $S_{T1}(m_{a-T1})$。节点 *b* 收到信息明文 *m*'、$S_{T3}(m_{a-T3})$、$S_{T1}(m_{a-T1})$，验证签名，根据验证结果与信息明文 *m*' 的一致性来决定是否接受此信息，从而实现对路由信息的验证。

3　SE-BGP 安全性分析

3.1　IXP 概述

Internet 交换点(IXP, Internet exchange point)[12] 在不同组织的 AS 之间提供通信服务，这些 AS 之间通过 IXP 建立了公共对等关系 PUP(public peering)，不用借助提供商节点(ISP 节点)的转发而可直接与其他 AS 节点进行通信。PUP 减少了提供商节点的通信负担，最重要的是使 AS 节点可以直接转发路由信息，避免选择更长更昂贵的路径。根据文献[13]，目前因特网大约有 380 多个 IXP，每个 IXP 的成员也在不断增加，有的甚至可以达到成百上千个。

3.2　SE-BGP 安全漏洞

分析表明，SE-BGP 存在以下 3 点安全漏洞。

1) AS 联盟的关键节点，即 rich 节点，来源于 AS 网络中的核心层(主要由 Tier-1ISP 和 Tier-2 ISP 组成[8])，AS 联盟内部的非关键节点都是此联盟关键节点的客户节点，关键节点之间也有可能是“客户-提供商”的关系(即 Tier-2 ISP 也是 Tier-1ISP 的客户节点)。SE-BGP 认为 AS 联盟之间路由信息的转发必须要通过 rich 节点，即关键节点，跨联盟的信息只需要通过关键节点的认证即可。但是联盟之间的路由转发却出现了以下 2 种特殊情况：非关键节点并不一定仅仅通过与关键节点的“客户-提供商”连接，也可以通过 IXP 提供的 PUP 将路由信息转发至另一个联盟内部；关键节点不一定仅仅通过现有的“关键节点-关键节点”连接，也可以通过 IXP 提供的 PUP 跳过某一个或几个关键节点将路由信息转发至另一个联盟内部。如图 1 所示，*SA*3 的节点 *a* 可以通过 IXP 直接与 *SA*1 的节点 *b* 进行通信；*SA*4 的关键节点 *T*4 可以通过 IXP 直接与 *SA*3 的关键节点 *T*3 进行通信。并且近些年的分析 [12,14,15]表明，越来越多的 AS 选择了建立 PUP 转发信息，而不是必须将路由信息通过“提供商”节点再进行转发。那么越来越多绕过“关键节点-关键节点”连接而直接通过 PUP 关系转发的跨联盟路由信息就会因为无法认证其合法性和真实性被丢弃，从而引起“路由黑洞”现象。

2) 随着网络规模的扩大，越来越多的 AS 节点通过 IXP 建立 PUP 转发路由信息，同时也会出现某些 AS 节点取消 PUP 的情况，由此跨联盟参与者的数量也会随之变化，而不仅仅只限于关键节点。SE-BGP 方案中的关键节点，面对动态变化，很难实现动态认证。

3) SE-BGP 安全机制中，由于对关键节点的充分信赖，致使忽略了其本身自发的主动攻击。一旦关键节点本身成为了恶意节点，对路径信息进行伪造或肆意篡改，对整个网络所带来的损害将会更大，而 SE-BGP 对此没有提供任何相关的安全防范措施。

4　SCA-BGP 安全机制

根据 SE-BGP 体系结构中 AS 节点的不同功能特性，本文将 AS 联盟的结构纵向扩展为二层跨联盟等级结构 CAHS (cross-alliance hierarchical structure)，如图 2 所示。CAHS 结构将各个 AS 节点分而治之，每个层实现自己相应的功能，更易于管理和实现。基于 CAHS 结构，针对 SE-BGP 所存在的安全漏洞，提出一种全新的跨联盟安全机制——SCA-BGP。方案中将跨越联盟的 AS(包括 SE-BGP 中的关键节点)统称为跨联盟者 CAA(cross-alliance AS)，并假定网络中的 AS 节点不会进行“合谋”。

4.1　CAHS 等级结构

由图 2 可以看出，CAHS 等级结构分为 2 层：1) 第一层 $Layer_1$——宏-跨联盟层 MARO-CA；2) 第二层 $Layer_2$——联盟内部层(IA, internal alliance)。

定义 1　MARO-CA

MARO-CA 是指通过跨联盟连接(CAL, cross alliance link)聚集在一起的 AS 节点。此处的 CAL 是一个抽象概念，将所有 2 个跨联盟 AS 之间的会话连接均看作端到端的 CAL 连接，它是不同联盟

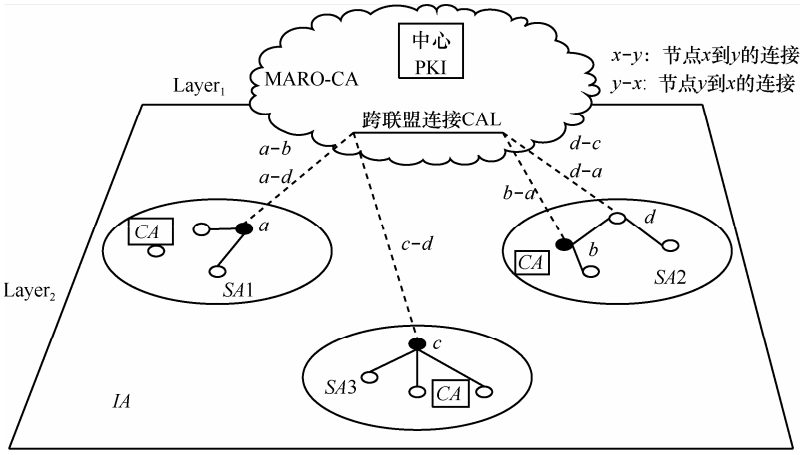


图 2 CHAS 等级结构

之间的通信桥梁。CAL 连接不仅包括 AS 节点之间的直接连接，也包括 2 个节点通过 IXP 建立的连接(此时 IXP 节点可看作一条 BGP 会话连接)。

IA 层只需使用本联盟内部的 CA 签发的证书验证信息，不会涉及到联盟之间的交互。MARO-CA 层位于 IA 的上一层，能够宏观地控制各个 AS 联盟之间的认证交互。

定义 2 中心 PKI

中心 PKI 为合法的 CAA 颁发护照证书，每个 CAA 以及 CAA 的邻居都可以在中心 PKI 中查询其他 CAA 的护照证书。中心 PKI 与各个联盟内 CA 所颁发的证书均是基于 X.509 证书的扩展证书，具有相同的格式。

定义 3 AS_Security_Mark 属性

AS_Security_Mark 属性存储途经所有 AS 节点对路径信息的数字签名，此属性添加于 BGP 可选属性中。

4.2 护照证书认证

在 MARO-CA 层，CAA 通过 CAL 连接完成护照证书的签证实现 CAA 的动态认证，并通过通信密钥的生成来识别 CAA 的身份及行为授权的合法性。

4.2.1 相关标记

护照签证模型中主要标记的含义如表 1 所示。

4.2.2 签证过程

1) 请求签证

本地联盟的 $\mathrm{CAA_{HA}}$ 持有中心 PKI 下发的护照证书，可证实其身份的合法性。为了能够获得异地联盟的授权，$\mathrm{CAA_{HA}}$ 通过 CAL 连接向异地联盟的 $\mathrm{CAA_{FA}}$ 提出签证申请 $Passport^{\mathrm{HA}}_{\mathrm{CAA_{HA}}}$，见式(1)。签证过程中，使用 Diffie-Hellman[16]密钥交换算法实现 $\mathrm{CAA_{HA}}$ 与 $\mathrm{CAA_{FA}}$ 共享密钥的协商。$\mathrm{CAA_{HA}}$ 预先产生一对 Diffie-Hellman 公/私密钥($PUK_{\mathrm{CAA_{HA}}}$，$PRK_{\mathrm{CAA_{HA}}}$)，利用 $\mathrm{CAA_{HA}}$ 自身的公钥 $PK_{\mathrm{CAA_{HA}}}$ 对其标识符 $id_{\mathrm{CAA_{HA}}}$ 和 $PUK_{\mathrm{CAA_{HA}}}$ 进行加密，并使用自身的私钥对护照号 $PassPort_{No}$，有效期 $expiry$，本地联盟标识 id_{HA} 连同加密信息一起签名，发送至异地联盟的 $\mathrm{CAA_{FA}}$。

表 1 签证相关标记

符号	描述
HA	本地联盟——发起跨联盟路由信息的 AS 联盟
$\mathrm{CAA_{HA}}$	HA 的跨联盟者
$PassPort_{No}$	护照号
$expiry$	护照或签证有效期
$Passport^{\mathrm{HA}}_{\mathrm{CAA_{HA}}}$	本地联盟 CAA 的护照
$SK_{\mathrm{A\text{-}B}}$	A 与 B 的共享密钥
$PassKey$	通行密钥
FA	异地联盟——接收 HA 跨联盟路由信息的 AS 联盟
$\mathrm{CAA_{FA}}$	FA 的跨联盟者($\mathrm{CAA_{HA}}$ 的通信方)
$Visa_{No}$	签证号
id_{A}	实体 A 的标识符
$Visa^{\mathrm{FA}}_{\mathrm{CAA_{HA}}}$	异地联盟对 CAA 发放的签证
$h(x)$	单向散列函数

$$Passport^{\mathrm{HA}}_{\mathrm{CAA_{HA}}}=\{\mathrm{Sig}_{\mathrm{CAA_{HA}}}(PassPort_{No},expiry,\ id_{\mathrm{HA}},PK_{\mathrm{CAA_{HA}}}(id_{\mathrm{CAA_{HA}}},PUK_{\mathrm{CAA_{HA}}}))\} \quad (1)$$

2) 签证

$\mathrm{CAA_{FA}}$ 接收签证申请后，从中心 PKI 查询有关

CAA_{HA} 护照信息的数字证书，使用证书中的公钥验证签名，并解开加密信息，识别 $id_{CAA_{HA}}$，保留 $PUK_{CAA_{HA}}$ 用于共享密钥的计算。如果护照信息验证无误，将对此护照进行签证，授予 CAA_{HA} 跨联盟的权利，见式(2)。CAA_{FA} 利用自身的公钥 $PK_{CAA_{FA}}$ 对标识符 $id_{CAA_{FA}}$ 和自产生的 Diffie-Hellman 公钥 $PUK_{CAA_{FA}}$ 进行加密，并利用自身的私钥对护照号 $PassPort_{No}$，签证号 $Visa_{No}$，有效期 *expiry*，连同加密信息一起进行签名，发送至本地联盟的 CAA_{HA}。

$$Visa_{CAA_{HA}}^{FA}=\{\mathrm{Sig}_{CAA_{FA}}(PassPort_{No},Visa_{No},expiry,\ PK_{CAA_{FA}}(id_{CAA_{FA}},PUK_{CAA_{FA}})\} \quad (2)$$

3) 计算共享密钥

CAA_{HA} 和 CAA_{FA} 分别接收到对方产生的 Diffie-Hellman 公钥 $PUK_{CAA_{HA}}$，$PUK_{CAA_{FA}}$，根据 Diffie-Hellman 算法，计算它们之间的共享密钥 $SK_{CAA_{HA}\text{-}CAA_{FA}}$ 和 $SK_{CAA_{FA}\text{-}CAA_{HA}}$，且

$$SK_{CAA_{HA}\text{-}CAA_{FA}}=SK_{CAA_{FA}\text{-}CAA_{HA}}$$

p 为系统公开的参数，且为素数，则

$$SK_{CAA_{HA}\text{-}CAA_{FA}}=PUK_{CAA_{FA}}^{PRK_{CAA_{HA}}} \bmod p$$

$$SK_{CAA_{FA}\text{-}CAA_{HA}}=PUK_{CAA_{HA}}^{PRK_{CAA_{FA}}} \bmod p$$

4) 通行密钥 *PassKey*

如果签证成功，CAA_{HA} 和 CAA_{FA} 分别计算通行密钥 *PassKey*，见式(3)。在有效期 *expiry* 内，CAA_{HA} 可以使用 *PassKey* 对跨联盟信息“盖章”生成 *Stamp* 值，只有 CAA_{FA} 能识别并验证 *Stamp*，从而有效保证跨联盟者身份及行为授权的合法性。

$$PassKey=h(SK_{CAA_{HA}\text{-}CAA_{FA}},Visa_{No},PassPort_{No}) \quad (3)$$

4.3 主动攻击防御机制

SE-BGP 方案中，联盟内部的每个 AS 通过 CA 下发的证书对接收到的信息进行验证，如果成功，则转发给下一跳。联盟之间的交互完全依赖于 CAA，只要本地联盟的 CAA_{HA} 能够证明信息的正确性，异地联盟的 CAA_{FA} 不需要再次证明，而只需要确定 CAA_{HA} 的身份即可。这种情况只适宜于 CAA 是完全可信的，然而 CAA 很有可能已经遭受攻击者的侵入或控制而本身成为了恶意节点，进而对网络发起主动攻击。单单验证对方的身份根本无法检测出对方的行为是否可信，因为从身份角度来说它本身就是合法的。如果本地联盟的 CAA_{HA} 对路径信息进行伪造和篡改，异地联盟的 CAA_{FA} 根本无法察觉。SCA-BGP 方案对于源地址的认证方式与 SE-BGP 相似，针对路径信息，提出了基于递增散列函数 AdHASH 的主动攻击防御机制(AAD, active attack defense)，有效地防止 CAA 本身发起的主动攻击，解决了 SE-BGP 所存在的安全漏洞。

4.3.1 AdHASH

图 3 为 AdHASH 的原理图。

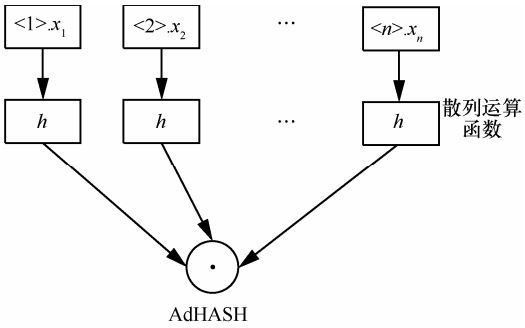


图 3　AdHASH 原理

AdHASH[17]其实是通过一系列模加运算来计算有限集合的散列值，将有限集合中的每个元素经过散列运算后，再将结果相结合进行取模运算，记为 *AH*，见式(4)。

$$AH_n=\{((h(<1>.x_1)+h(<2>.x_2))\bmod M +\cdots+h(<n>.x_n))\bmod M\} \quad (4)$$

h 是标准散列函数(MD5 或 SHA)，M 是足够大的 k 比特整数，$<i>$ 是信息集合中每个元素 x_i 的序列号，可以保证它们与每条信息的串接在整个集合中的唯一性。AH 算法具有以下几点性质。

1) 有效性

AH 的计算在标准散列运算的基础上进行模加运算，每增加一个元素，计算开销仅为一次加法和一次取模运算，有效性基本等同于标准散列运算。

2) 压缩性

AH 通过模运算可以将输入压缩为 k bit 的数据块，每个节点只需要很小的空间来存储递增的散列值。

3) 递增性

较大集合 *AH* 值总是可以由它的子集通过递增计算得出。如果增加一个元素，新的 *AH* 值可以通过先前的 *AH* 值计算得到。

$$AH_n=\{(AH_{n-1}+h<n>.\{AS_n\})\bmod M\}$$

4) 无碰撞性

想要找到或者伪造另一组元素集而得到相同

的 AH 值在计算上是不可行的，并已证明它的困难程度等同于加权背包问题，属于 NP-hard 问题。

4.3.2 AAD 基本思想

1) 节点信息检测(NT)

根据信息的“输出=输入+自产生”原则，每个 AS 输出的信息应该等于输入与自产生的信息和。即

$$Message_{\text{out}}=Message_{\text{in}}+Message_{\text{local}}$$

$$AH(Message_{\text{out}})=\text{AH}(Message_{\text{in}})+\text{AH}(Message_{\text{local}})$$

如果某个节点 AS_i 在路径属性 AS_PATH 中添加的信息是虚假的，那么

$$AH_i \neq AH_{i-1}+AH_{\text{local}_i} \tag{5}$$

其中，$AH_{\text{local}_i}=h(<i>.m_i)\bmod M$，是 AS_i 自产生的信息，除了第一个节点 AS_1 自产生的信息为 $m_1=\{f,AS_1\}$,其他节点通过依次添加如下自产生信息：$m_2=\{AS_2\}$，$m_3=\{AS_3\}$，…，$m_i=\{AS_i\}$，最终得到新的路径信息。为了检测 AS_i 所添加信息的正确性和真实性，基于式(5)提出 NT 检测算法，具体算法流程如下。

Notation:

$\text{Sig}_{k_i^-}(AH_i)$: the signature of AH_i by AS_i, denoted by S_i

$\text{Ver}_{k_i^+}(S_i)$: the verification of S_i

$|AS\_PATH|$: the length of AS_PATH

Input: AS_PATH, S_i, S_{i-1}

Output: true: the self-generated message by AS_i in the AS_PATH is correct

false: the self-generated message by AS_i in the AS_PATH is false

```
if Ver_{k_i^+}(S_i) is success
    AH_i = Ver_{k_i^+}(S_i);
    if |AS_PATH| == 1
        AH_0 = 0;
    else if |AS_PATH| > 1 && Ver_{k_{i-1}^+}(S_{i-1}) is success
        AH_{i-1} = Ver_{k_{i-1}^+}(S_{i-1});
    m_i = get(AS_PATH[0]); /* 得到AS_PATH的第一个元素 */
    if AH_i = {(AH_{i-1} + <i>.m_i) mod M is true
        return true;
    else
        return false;
else
    return false;
```

2) 路径信息检测(PT)

AH 值是路径信息经过的每个 AS 节点计算的摘要信息累加值，如果 AS_i 对本节点前的路径信息进行了伪造、篡改，则

$$AH_{i-1}\neq\{((h(<1>.m_1)+h(<2>.m_2))\bmod M +\cdots+h(<i-1>.m_{i-1}))\bmod M\} \tag{6}$$

为了检测第 i 个节点前的路径信息是否遭受攻击，基于提出了 PT 算法，具体算法流程如下。

Input: f, AH_{i-1}, AS_PATH, NT

Output: true: AS_PATH has not been attacked

false: AS_PATH has been attacked

```
if NT is correct
    m_{i-1} = get(AS_PATH[1]);
    m_{i-2} = get(AS_PATH[2]);
    …
    m_1 = f + get(AS_PATH[i-1]);
    if {AH_{i-1} = {((h(<1>.m_1) + h(<2>.m_2)) mod M
            + … + h(<i-1>.m_{i-1})) mod M} is true
        return true;
    else
        return false;
else
    return false;
```

4.3.3 AAD 原理

1) 初始阶段

每个 AS 联盟内部成员获得来自 CA 的数字证书和相对应的公钥/私钥 (k_i^+,k_i^-)，私钥 k_i^- 用来对信息进行签名，而公钥 k_i^+,用来验证签名，并且每个 AS 获得与其相邻 2 跳的数字证书。

2) 联盟内部认证算法

① 联盟内的 AS_i 接收到来自 AS_{i-1} 的 Update_{i-1} 信息后，将会执行 Validate 验证算法，如下所示。

Input: $AS\_PATH=\{AS_{i-1}, AS_{i-2},\cdots, AS_1\}$

output: true: Update will be processed

false: Update will be dropped

```
if |AS_PATH| == 1
    if NT is correct
        return true;
```

else
return false;
if $|AS\_PATH|>1$
if NT is correct && PT is correct
return true;
else
return false;

AS_i 首先验证 AS_{i-1} 携带的信息(包括验证数字签名和 NT 检测算法是否成功)，如果验证成功，将会执行路由更新处理；如果失败，丢弃 Update_{i-1}。

② 如果 AS_i 执行验证算法 Validate 的结果是正确的，证明 AS_{i-1} 转发的信息真实可信，则执行路由更新算法，算法具体流程如下。

Input : Validate_i
if Validate_i is correct
$S_i = \text{Sig}_{k_i^-}(\text{AH}_i)$
Delete(AS_Security_Mark[1])
/*删除AS_Security_Mark队列的尾元素*/
Move(AS_Security_Mark[0],AS_Security_Mark[1])
/*将AS_Security_Mark队列的首元素移至尾部*/
ADD(S_i,AS_Security_Mark[0])
/*添加S_i至AS_Security_Mark队列的首部*/
ADD(AS_i, AS_PATH[0])
/*添加AS_i至AS_PATH队列的首部*/
else
drop Update_{i-1}

AS_i 完成更新算法后，将 Update_{i-1} 转发至下一节点 AS_{i+1}，…，直至 AS_{n-1} 将更新消息 Update_{n-1} 转发至本地联盟的跨联盟者 CAA_{HA} ——第 n 跳节点。

3) 联盟之间认证算法

CAA_{HA} 执行验证算法 Validate，如果结果正确，执行路由更新算法，并“盖章”生成 $Stamp = h(PassKey + AH_n)$ 追加在 Update 信息尾部，跨入 Layer_1，通过 CAL 连接转发至 CAA_{HA} 的对等体 CAA_{FA}。如果 CAA_{FA} 执行 Validate 正确，验证 *Stamp* 值，*Stamp* 如果也正确，可以有效地证明 CAA_{HA} 是合法的跨联盟者，其行为已被 CAA_{FA} 授权，且携带的信息真实可信，允许将 Update_n 进入异地联盟 FA。如果 CAA_{FA} 将跨联盟信息转发至下一个联盟，CAA_{FA} 将成为新的 CAA_{HA}，执行与上述相同的程序，直到信息转发至异地联盟内部。

5 SCA-BGP 方案分析

5.1 安全性

定理 1 跨联盟者 CAA 及联盟内部每个 AS 节点的身份均不可伪造。

证明 CAA 及联盟内部每个 AS 节点的私钥只有其本身持有，并存储在防串扰的硬件内部，攻击者很难获得私钥。而通过计算得到私钥的困难性等同于求解离散对数的困难性，所以攻击者想要伪造 CAA 和其他 AS 节点的身份几乎不可能。

定理 2 实现了跨联盟的行为授权，且授权不可伪造。

证明 跨联盟的行为是基于护照/签证的基础上得以授权的。其思想借鉴了出国签证的思想，先申请得到护照证书，再经过签证获得盖章后才有资格出国，SCA-BGP 中“盖章”体现在 *Stamp* 值,所以是合理且可行的。在签证过程中双方都持有证明身份的私钥，只有合法的跨联盟者才有权利申请签证或者对其执行签证。通过 2 个联盟 CAA 间的交互，协商并计算了通行密钥 *PassKey*。即便在信息交互过程中，被第三方窃取，它只能得到护照和签证的相关信息，却很难计算出通行密钥 *PassKey*。所以,伪造 *Stamp* 很困难，从而有效地保证了跨联盟行为授权的安全性。

定理 3 跨联盟者 CAA 携带的路径信息不可伪造，不可肆意篡改。

证明 假设本地联盟的 CAA_{HA} 所携带的信息为 $\{f, \text{CAA}_{\text{HA}}, AS_{n-1}, \cdots, AS_1\}$，AS_Security_Mark 队列中首签名为 S_n 尾签名为 S_{n-1}，如果 CAA_{HA} 想要伪造路由信息，必须要伪造 AH_{n-1} 和 S_{n-1}，否则通过 NT 算法—— $AH_n \neq AH_{n-1} + AH_{\text{local}_n}$ 很容易检测出来。然而 CAA_{HA} 很难获得 AS_{n-1} 的私钥，所以只能伪造另一个 $AH'_{n-1} = AH_{n-1}$。根据 AdHASH 的无碰撞性，想要伪造另外一个 AH'_{n-1} 与 AH_{n-1} 在计算上并不可行。CAA_{FA} 使用从中心 PKI 获得证书中的 AS_{n-1} 公钥验证签名得出：$\text{Ver}_{k_{n-1}^+}(S_{n-1}) \neq AH'_{n-1}$，则认为 CAA_{HA} 所携带的路径信息并不真实可信，并将其丢弃。由此得知，跨联盟所携带的路由信息不可伪造，一旦伪造，就会被检测出，并将其丢弃。

如果 CAA_{HA} 想要篡改路径信息 $m=\{f, \text{CAA}_{\text{HA}},$

$AS_{n-1},\cdots,AS_i,AS_{i-1},\cdots,AS_1\}$, 则

填充 X 得到

$$m'=\{f,\mathrm{CAA}_{\mathrm{HA}},AS_{n-1},\cdots,AS_i,X,AS_{i-1},\cdots,AS_1\}$$

删减 AS_{i-1} 得到

$$m''=\{f,\mathrm{CAA}_{\mathrm{HA}},AS_{n-1},\cdots,AS_i,AS_{i-2},\cdots,AS_1\}$$

修改 AS_{i-1} 为 Q 得到

$$m'''=\{f,\mathrm{CAA}_{\mathrm{HA}},AS_{n-1},\cdots,AS_i,Q,\cdots,AS_1\}$$

$\mathrm{CAA}_{\mathrm{FA}}$ 对篡改后的信息 m',m'' ,m''' 计算 AH 值分别得到 AH'，AH''，AH'''，并验证 $\mathrm{Ver}_{k_{n-1}^+}(S_{n-1})\neq'\ AH'\neq AH''\neq AH'''$，由此来证明路径信息是否已被篡改。

定理 4　路径信息在 AS 联盟内部传输的完整性和真实性。

证明　在 AS 联盟内部，如果路径信息在传输过程中遭受到外部攻击者的破坏，由于外部攻击者无法获得合法节点的私钥，所以验证 $\mathrm{Ver}_{k_i^+}(S_i)$ 和 $\mathrm{Ver}_{k_{i-1}^+}(S_{i-1})$ 的结果将不正确；如果遭受了内部攻击者自发的攻击，虽然签名验证成功，但是却导致 NT 或 PT 检测的失败，由此可以有效地验证路径信息在 AS 联盟内部传输的完整性和真实性。

5.2　可扩展性

假设每个 AS 持有一个证书，重点考虑 2 个指标：全网证书规模 C 和单点证书规模 C_s。假设整个网络中 AS 的节点数目为 N，rich 节点的范围为 $\beta\%$，rich 节点的连接概率为 p，建立 PUP 连接的 CAA 数目为 Num_{CAA}，PUP 成员的节点范围为 $\alpha\%$，PUP 成员节点的连接概率为 p'，则 AS 联盟内关键节点的数目为 $K=N\beta\%=N\dfrac{\beta}{100}$，每个联盟内部的 AS 数目为 $n=\dfrac{N}{N\beta\%}=\dfrac{100}{\beta}$，$Num_{\mathrm{CAA}}=\alpha\%N$。

AS 联盟内部每个节点需要相邻两跳 AS 的证书，假设每个 AS 的邻居数目平均为 $avgL$，那么相邻一跳 AS 节点数目为 $avgL$，相邻两跳的节点数目则为 avg^2L，则

AS 联盟内部节点的证书规模为

$$\begin{aligned}C_n&=n(avgL+avg^2L)K\\&=N(avgL+avg^2L)\end{aligned}$$

CAA 所需的证书规模为

$$\begin{aligned}C_{\mathrm{CAA}}=&p'Num_{\mathrm{CAA}}(1+avgL)Num_{\mathrm{CAA}}+\\&pK(1+avgL)K\end{aligned}$$

总的证书规模为

$$\begin{aligned}C&=C_n+C_{CAA}\\&=N(avgL+avg^2L)+\\&\quad(p'Num_{\mathrm{CAA}}{}^2+pK^2)(1+avgL)\end{aligned}$$

AS 联盟内部的单点证书规模为

$$C_{s_n}=avgL+avg^2L$$

CAA 的单点证书规模为

$$C_{s_{\mathrm{CAA}}}=(p'Num_{\mathrm{CAA}}+pK)(1+avgL)$$

对于传统模型 S-BGP，$C=N^2,C_s=N$

SE-BGP[5]模型为

$$C=\frac{100}{\beta}N+\frac{2\beta p}{100}N^2$$

$$C_{s_{\mathrm{CAA}}}=pN,C_{s_n}=100+0.003N$$

根据 2013 年 4 月 17 日 RouteViews[18]数据分析，目前互联网 AS 的数目大约为 44 167，连接数目为 92 893，每个 AS 的平均邻居数目大约为 4.2；从 peering DB[13]数据可知，PUP 的参与成员大约为 4 617，共建立 PUP 14 786。那么，$avgL$=4.2，p'=0.000 7，$\alpha\%$=0.1，且取 $\beta=1$，$p=0.3$ [5]。

就目前的网络规模，表 2 对已有的方案与本方案从全网证书规模与单点证书规模进行了对比。

从表 2 可以看出，SCA-BGP 的全网证书规模与单点证书规模均小于其他 2 种安全解决方案。随着网络规模的扩大，证书的规模也随之变化，图 4 和图 5 对全网证书规模以及单点证书规模的发展趋势进行了对比。

表 2　　**证书规模对比**

N	C			C_s				
	S-BGP	SE-BGP	SCA-BGP	S-BGP	SE-BGP		SCA-BGP	
					CAA	Normal Nodes	CAA	Normal Nodes
44 167	1.95×10^9	1.61×10^7	1.35×10^6	44 167	13 250	233	705	22

从图 4 和图 5 可以看出，就全网证书规模，SCA-BGP 均小于 S-BGP 和 SE-BGP；就单点证书规模，SCA-BGP 普通节点的证书规模远小于其他 2 种方案，CAA 的单点证书规模也小于 SE-BGP。由此可以得出，SCA-BGP 有效地减少了证书所需数量，具有更好的可扩展性，同时也减少了证书管理所带来的额外开销。

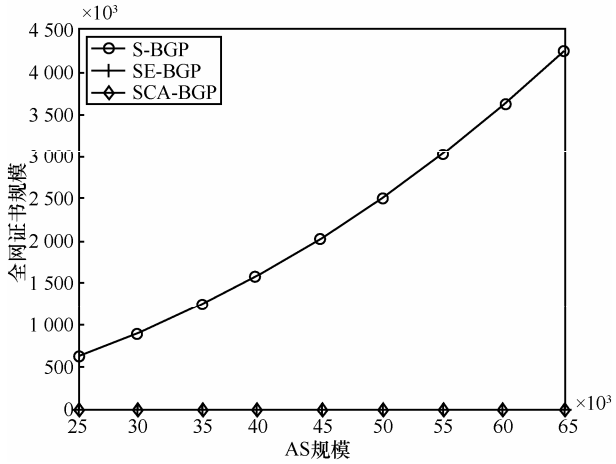


图 4　全网证书规模

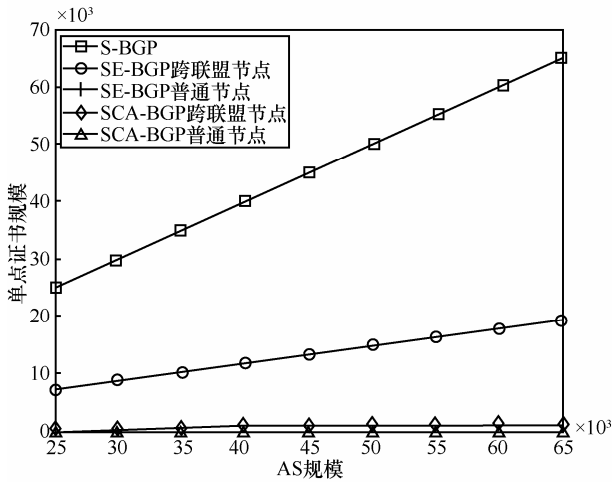


图 5　单点证书规模

5.3　网络收敛性

跨联盟的签证都是预先完成的，并不会影响网络的性能。而本方案提出的 AAD 机制，是基于 AdHASH 所设计的，路由更新算法中 *AH* 值的计算仅仅是在标准散列运算基础上增加一次加法和取模运算，从运算速度方面来说，与标准散列运算基本是一样的。Validate 算法中 RT 的检测会涉及到几次散列运算的加法和取模运算。与 SE-BGP 一样，SCA-BGP 也采用 DSA 签名和验证算法，散列运算采用 SHA-1 算法，SHA-1 的输入仅仅是 16 bit 的 AS 号，所以运算时间仅仅需要几 μs 的时间[19]。从最新的数据分析[18]，有 98%的路由信息在 4 跳之内就可以到达目的地，通常 RT 最多会涉及到 3 次散列运算的加法与取模，所以也不会影响到网络的收敛时间。

那么，网络的收敛性能则主要取决于数字签名和验证所带来的时间开销，DSA 算法的签名时间约为 25.5 ms,验证时间约为 31.0 ms[19]。在实验中，选取 AS 规模分别为 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60，使用 SSFNET[20]做仿真实验，假设每个 AS 内部只有一台 BGP 路由器，最小路由通告间隔 *MRAI*=30 s，选取一个节点度为 1 的 Stub AS 宣告一条 Update 消息，仿真网络平均收敛时间，如图 6 所示。

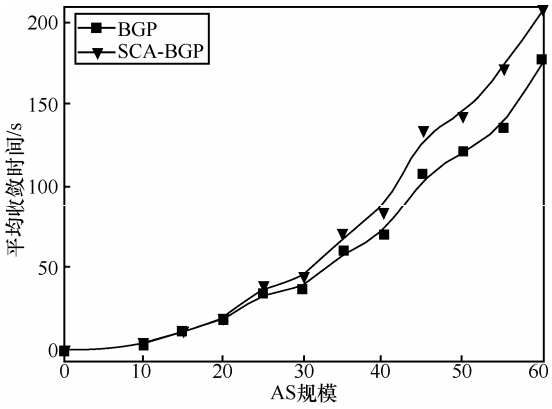


图 6　平均收敛时间

由图 6 可以看出，AS 规模从 10 增长到 60 时，收敛延迟仅仅为原 BGP 的 18%。随着 AS 规模的扩大，当 AS 规模达到 110 时，传统经典方案 S-BGP 的收敛延迟大约为 230%[19]，基于 AS 联盟的 SA-BGP 的收敛延迟大约为 30%[6]，而 SCA-BGP 的收敛延迟大约仍为 18%。从 AS 节点抵制自发攻击的角度来看，S-BGP、SA-BGP 与 SCA-BGP 具有同样的安全级别，但是 SCA-BGP 的收敛性能较前 2 种方案得到了很大的改善。由此，SCA-BGP 在保证安全性的同时，获得了接近于原始 BGP 的良好网络性能。

6　结束语

本文对基于 AS 联盟的 BGP 安全机制 SE-BGP 进行了深入研究，对 SE-BGP 的安全模型和现有 AS 网络拓扑特性进行了全面剖析，发现了 SE-BGP 存

在的几个安全漏洞，即无法认证 CAA 的身份和行为授权，也无法抵御 CAA 自身发起的内部攻击，这些给 BGP 安全造成了致命的威胁。由此，本文通过纵向拓展 AS 联盟结构，提出了一种全新的跨联盟安全机制——SCA-BGP。SCA-BGP 借鉴护照签证的思想，实现了动态 CAA 的安全认证以及行为授权，并利用递增散列运算的 AdHASH 设计出 NT 和 RT 检测算法，将检测算法与数字签名相结合，最终实现了抵御主动自身发起的内部攻击。SCA-BGP 不仅仅实现了每个联盟内部 Update 信息的安全交互，更重要的是保证了 CAA 携带的跨联盟信息的真实性和完整性。实验结果表明，SCA-BGP 具有高安全性的同时，还具有更好的可扩展性和网络性能。

参考文献：

[1] REKHTER Y, LI T, HARES S. A Border Gateway Protocol 4(BGP-4) [EB/OL]. http://datatracker.ietf.org /doc/rfc4271/. 2006.

[2] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592.

[3] WHITE R. Securing BGP through secure origin BGP (soBGP)[J]. The Internet Protocol Journal, 2003, 6(3):15-22.

[4] OORSCHOT P C, WAN T, KRANAKIS E. On inter-domain routing security and pretty secure BGP (psBGP)[J]. ACM Transactions on Information and System Security (TISSEC), 2007, 10(3): 11.

[5] 胡湘江，朱培栋，龚正虎. SE-BGP:一种 BGP 安全机制[J].软件学报, 2008,19 (1):167-176.
HU X J, ZHU P D, GONG Z H. SE—BGP：An approach for BGP security[J]. Journal of Software, 2008, 19 (1):167-176.

[6] 王滨, 安金梁, 吴春明等. 基于分治策略的 BGP 安全机制[J]. 通信学报, 2012,33(5):91-98.
WANG B, AN J L, WU C M, *et al*. Study of BGP secure scheme based on divide and conquer strategy[J]. Journal on Communications, 2012. 33(5): 91-98.

[7] KARLIN J, FORREST S, REXFORD J. Pretty good BGP: improving BGP by cautiously adopting routes[A]. Proceedings of the 2006 IEEE International Conference on Network Protocols[C]. Washingdon, DC, USA, 2006.290-299.

[8] SUBRAMANIAN L, ROTH V, STOICA I, *et al*. Listen and whisper: Security mechanisms for BGP[A]. Symposium on Networked Systems Design and Implementation (NSDI 2004)[C]. 2004. 29-31.

[9] YUN J K, BYUN C H, KIM Y. Architecture of the remote routing validation tool for BGP anomaly detection[A]. Proceedings of the 2012 ACM Research in Applied Computation Symposium[C]. CA, USA, 2012. 232-236.

[10] GAO L. On inferring autonomous system relationships in the Internet[J]. IEEE/ACM Transactions on Networking, 2001, 9(6):733-745.

[11] ZHOU S, MONDRAGON R J. The rich-club phenomenon in the Internet topology [J]. IEEE Communications Letters, 2004, 8(3): 180-182.

[12] AGER B, CHATZIS N, FELDMANN A, *et al*. Anatomy of a large European IXP[A]. Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication[C]. 2012. 163-174.

[13] PeeringDB [EB/OL]. https://www.peeringdb.com/. 2013.

[14] GIOTSAS V, ZHOU S. Valley-free violation in Internet routing—analysis based on BGP community data[A]. IEEE International Conference on Communications (ICC)[C]. 2012.1193-1197.

[15] ORSINI C, GREGORI E, LENZINI L, *et al*. Evolution of the Internet k-dense structure[J]. arXiv preprint arXiv:1301.5938.2013.

[16] LIU X, LI A, YANG X, *et al*. Passport: secure and adoptable source authentication[A]. Proceedings of the 5th USTNIX Symposium on Networked Systems Design and Implementation[C]. 2008.365-378.

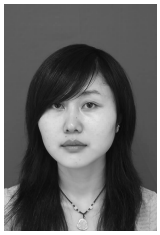
[17] ZHANG Y, YANG J, LI W, *et al*. An authentication scheme for locating compromised sensor nodes in WSNs[J]. Journal of Network and Computer Applications, 2010, 33(1): 50-62.

[18] University of Oregon Route Views Project[EB/OL]. http://www.routeviews.org/.2013.

[19] ZHAO M, SMITH S W, NICOL D M. Evaluating the performance impact of PKI on BGP security[A]. 4th Annual PKI R&D Workshop[C]. Gaithersburg, MD, 2005.42-48.

[20] The SSFNET Project [EB/OL]. http://www.ssfnet.org. 2013.

作者简介：



孔令晶（1983-），女，甘肃兰州人，西南交通大学博士生，主要研究方向为网络体系架构及路由安全。

曾华燊（1945-），男，四川成都人，博士，西南交通大学教授、博士生导师，主要研究方向为网络测试技术、网络体系架构和高速交换技术。

窦军（1963-），男，四川成都人，博士，西南交通大学副教授，主要研究方向为网络体系架构、网络安全。

李耀（1985-），男，四川南充人，西南交通大学博士生，主要研究方向为系统建模与验证。