基于关键节点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，成都 610031）

摘 要：BGP 作为 Internet 域间路由的基本协议，其安全问题一直受到学界的关注，特别是安全性与实现难度之间的折中。针对传统解决方案 S-BGP（secure BGP）的不足，在定义关键节点 KN（key node）的基础上，利用 KN 对路由信息安全验证的特殊功能，提出了更加轻量级的解决方案——基于关键节点的域间路由安全机制 SR-KN（secure routing based on key node）。通过对比分析表明，SR-KN 在保证 BGP 安全的前提下，减少了全网证书规模及存储量，且具有更好的收敛性能。

关键词：边界网关协议；域间路由安全；S-BGP；SR-KN；关键节点
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2013)12-3753-05
doi:10.3969/j.issn.1001-3695.2013.12.061

Secured inter-domain routing mechanism based on key node

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

Abstract: As the basic inter-domain routing protocol, security issues of BGP (border gateway protocol) have drawn much attention from academic community, especially the trade-off between security and difficulty in implementation. Having pinned down the inadequacy of the traditional solution S-BGP, on the basis of the definition of KN, this paper utilized KN's special function of routing security validation and put forward a lightweight scheme-secured inter-domain routing mechanism SR-KN. As a result, under the premise of the security of BGP, the results of analysis and comparison show that for the whole network, the scale of certification and the storage are reduced and the convergence performance is improved.

Key words: BGP; inter-domain routing security; S-BGP; SR-KN; key node

0 引言

全球性的互联网实质上是由多个称为自治系统（autonomous system，AS）自主管理的网络互连而成的。每个 AS 使用同种或多种内部网关协议（interior gateway protocol，IGP）交换路由选择信息，如路由信息协议（routing information protocol，RIP）、开放式最短路径优先 OSPF（open shortest path first）以及 IS-IS（intermediate system to intermediate system routing protocol）等。AS 之间的路由信息选择和交换则毫无例外地使用边界网关协议 BGP。BGP 虽几经修订，即使是目前的最新版本 BGP-4[1]，其安全性问题仍未得到很好的解决。BGP 的安全问题给整个网络所带来的灾难不可轻视，2008 年，巴基斯坦电信在试图限制本国用户访问视频网络 You Tube 时无意间将错误的路由信息传播到整个网络，使 You Tube 网络瘫痪了一个小时。分析表明[2]，出现类似不安全问题，除了人为因素外，BGP 的隐含假设——“每一个 BGP 网关都是可信的”是其根本的原因。文献[2]详细列出了 BGP 中所存在的几个根本性的弱点：

a）BGP 缺乏相应的措施来保证消息的完整性、新鲜性以及内容的真实性。

b）BGP 没有相应的机制证明某个 AS 系统已授予宣告某个真实存在的 IP 地址前缀的权利。

c）BGP 不能够保证 AS 路径属性的真实性。

进一步分析表明，BGP 所面临的安全性问题集中体现在以下两方面：

a）会话的安全性。BGP 是基于 TCP 之上的路由信息交换协议，BGP 发言者之间的会话连接控制权可能被第三方篡夺，进而任意地窜改该会话连接的路由信息。这种攻击是以窃听和会话权篡夺为代表的主动攻击形式。IPSec[3] 和 TCPMD5[4] 是用来解决会话安全性的典型技术。

b）路由信息的安全性。BGP 通过 UPDATE 消息宣告或者转发 AS 之间的路由信息，因此，前缀劫持和路径属性窜改成为异常/敌意节点最典型的攻击手段。除了配置错误可能会引起路由信息的错误以外，攻击者可以假冒成合法的 AS 系统宣告非法的前缀地址，进而对路由网络进行破坏。攻击者还可以肆意窜改 AS_PATH 路径属性，从而改变路由信息的选择和转发，最终引发窃听、黑洞等攻击。

业界人士对路径信息安全性问题提出过多种解决方案，这类方案大体可归入两类：基于密码学的 BGP 保护法和基于路由信息检测的路由信息安全保护。迄今为止，基于密码学的方法一直扮演着重要的角色。S-BGP[5] 便是基于密码学方法的

收稿日期：2013-03-12；**修回日期**：2013-05-06 **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）

作者简介：孔令晶（1983-），女，甘肃兰州人，博士，主要研究方向为下一代计算机网络、网络安全（kafeishunzi@163.com）；曾华燊（1945-），男，四川成都人，博导，主要研究方向为下一代网络体系结构、高速交换技术、网络测试技术；窦军（1963-），男，四川成都人，副教授，博士研究生，主要研究方向为网络体系结构、网络安全；李耀（1985-），男，四川南充人，博士研究生，主要研究方向为安全苛求系统软件可靠性与安全性.

解决方案之一。尽管此方法具有很强的安全保护能力,却存在网络收敛速度慢、证书规模及存储量大等问题,使得 S-BGP 至今一直处于不断的探索中。本文就 S-BGP 基础上提出了基于关键节点的域间路由安全解决方案——SR-KN。通过关键节点 KN 的引入,简化复杂的验证过程,减少全网证书规模和存储量需求,并提高了网络收敛速度。

1 相关工作

1.1 研究状况

正是由于 BGP 安全的重要性,在近十几年的发展中,它的研究从未间断过。在各类解决方案中,基于密码学的方法一直都是整个研究方向的领头军。继 2000 年 S-BGP 问世之后,Cisco 所提出的 soBGP (secure origin BGP)[6] 试图在安全性和可行性方面寻求到平衡支点,但方案中并没有详述安全锚(信任的起点)[7] 的问题,且 AS_PATH 路径验证问题也只是建立在可行路径的基础之上,从而在安全性方面大打折扣。PsBGP (pretty secure BGP)[8] 也是试图解决 S-BGP 在可行性方面的相关问题,它在验证地址前缀的真实性中引入了评估机制,但是由此却增加了不必要的复杂性。后续还有一些方案试图从密码学算法的角度出发来实现保护 BGP 安全的目的,诸如 SE-BGP[9]、SA-BGP[10] 等。另外一些方案希望通过检测异常路由信息来保证路由系统的安全。例如 IRV(Internet routing validation)[11] 试图在每个 AS 内部建立一个验证者 IRV(Internet routing validator),在每一次验证过程中,通过它询问其他 AS 内部的验证者 IRV 来获得相关信息从而最终判断路由信息的真实性。但是方案中没有考虑询问与响应过程的安全性,也没有考虑每一次询问/响应过程所带来的额外开销以及网络收敛性的问题。PGP(pretty good BGP)[12]、listen and whisper[13] 等也都是基于非法路由检测而设计的解决方案。然而上述方案都存在着不足之处,BGP 的安全问题一直都没有得到根本上的解决。S-BGP 作为最早提出的经典解决方案,近年来一直都是本领域研究的热点。本文通过借鉴 S-BGP 严格的安全保护措施,提出了更为轻量级的解决方案——SR-KN 安全机制。

1.2 S-BGP

S-BGP 安全措施主要由两个 PKI(public key infrastructure)、X.509 证书以及确认(attestation)所组成。两个 PKI 都是基于 X.509 证书发放授权信息的。其中一个 PKI 用于指定 IP 地址前缀的分配,另一个 PKI 用于指定 AS 号以及 BGP 发言者与其所属 AS 的关系。

确认分为两种类型,即地址确认(address attestation,AA)和路由确认(route attestation,RA)。AA 是由一个组织(ARIN、ISP 等)授予某个 AS 宣告合法 IP 地址前缀的权利,该 AS 使用专有的私钥对该宣告信息进行数字签名;RA 则是证实通过此路由的每个中转 AS 都被先前的 AS 授权转发此路由,签名确认后转发给下一个指定的 AS。AA 可以防止 AS 内部的配置错误或不合法的地址前缀宣告,RA 可以防止路由信息在转发过程中不被恶意窜改。

每一个接收到 UPDATE 路由信息的 S-BGP 发言者需要验证 AA 和 RA。在验证之前从证书数据库中获取 PKI 发放的 X.509 证书,此证书中包含了与数字签名相对应的公钥。S-BGP 发言者使用相对应的公钥对 AA 和 RA 进行验证。每一个 S-BGP 发言者将进行一次 AA 验证和与 AS_PATH 长度相等次数的 RA 验证,如图 1 所示。

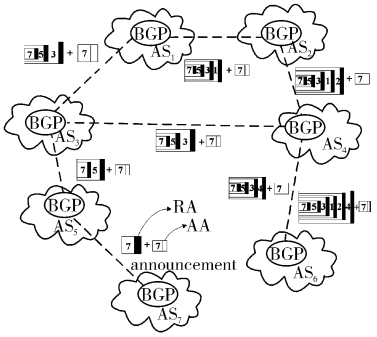

图 1 S-BGP 验证过程

然而 S-BGP 的验证过程却暴露了以下几个重要的问题:

a)验证 RA 之前 S-BGP 发言者必须获取与 AS_PATH 所包含的每个 AS 内部的 S-BGP 发言者相对应的公钥证书;验证 AA 之前 S-BGP 发言者也必须获取地址分配证书。证书处理程序较复杂,且需求量大。

b)接收到 UPDATE 消息的每一个 S-BGP 发言者必须执行对同一个 AA 的安全验证,重复性的操作带来了不必要的额外开销。

c)接收到 UPDATE 消息的每一个 S-BGP 发言者必须验证先前所经过的所有 AS 的 RA,随着 AS_PATH 的增大,带来的计算开销也随之增大。

d)从 AS 网络连接的特性可以看出,某些 AS 节点与大量的 peering 连接,尤其是 IXP 的 peering 数目有可能达到几百个,在一定时间内接收到的大量 UPDATE 信息给验证处理工作带来了不可低估的计算负担。

本文所提出的轻量级的方案——SR-KN 很好地解决了以上所存在的问题。

2 SR-KN 框架、关键节点 KN 与 BGP 信息验证

在介绍 SR-KN 的框架结构之前,首先介绍 SR-KN 的重要组件——关键节点 KN。KN 是对特定 AS 的抽象,它是在 AS 网络的层次结构选出的具有特定功能、持有特殊证书的节点(AS)。换言之,不是所有的 AS 都可以被抽象为 KN。

2.1 关键节点

用数学方式,一个网络图可以表达为 $G=(V, E)$。其中:V 是所有 AS 节点的集合,E 代表 AS 与 AS 之间的边集合。为了量化一个 AS(节点)与其他 AS(节点)间的连接关系数量(即边数 E)的大小,用节点度 d 来定义,即具有 n 个边的节点,其度数(d)为 n。从 AS 网络地理分布的角度来看,AS 之间的关系呈现出幂律分布[14] 的特点,即少数 AS 具有高节点度而大多数 AS 却具有低节点度的特性。除了 AS 地理分布的关系,AS 之间还存在着另一种关系——商业关系。如图 2 所示,文献[15]列举了这四种关系:provider-customer(P2C)、customer-provider(C2P)、peering-peering(P2P)以及 sibling-sibling(S2S)。P2C 或者 C2P 关系在整个 AS 网络中基本达到了 90% 以上。在这两种关系中,provider 的节点度大于 customer 的节点度,并且 customer 通过向 provider 付费的方式连接到其他网络。在 P2P 关系中,两个 AS 通过达成共同的协议免费传递对方的 customer 路由信息。基于 AS 之间的地理关系和商业关系,文

献[16]提出了层次等级结构,如图 2 所示。

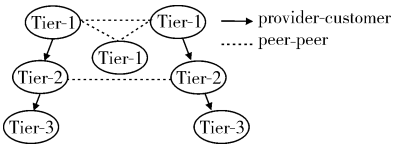

图 2　AS 网络层次结构及商业关系

a)Tier-1 AS 是一系列无 provider 的节点,它们可以通过与其他所有 Tier-1 AS 的全连接将路由信息转送到网络中的其他任何地方,无须支付任何费用。

b)Tier-2 通过向 Tier-1 付费的方式将地方级 AS 的路由信息转送到网络的其他地方。

c)从 Tier-2 依次往下划分:Tier-3 是 Tier-2 的 customer,Tier-4 是 Tier-3 的 customer…。

文献[16]还提出了一条重要的准则——valley-free,这条准则决定了 AS 路径转发的方向,即 AS 路径经过一条 P2C 或者 P2P 边之后,不允许经过 C2P 边,并且一条路径中只能经过 P2P 边一次。形象化地描述,就是 AS 路径就如爬山一样,从较低的节点至顶点后再向下传递,或者从较低的节点至较高节点后经过 P2P 边后再向下传递,不能够从顶点向下传递后再从下至上传递。根据以上理论基础,将阐述三个关键论述,此论述所需的数据来自于 Route Views[17](Route Views 的数据集通过 BGP table 采集并已广泛应用于各种研究机构)。

a)根据 2012 年 Route Views 的数据,现有的网络中大约共有 43 000 多个 ASes, 其中大约 85% 都是 stub AS(仅与一个其他 AS 相连)。这些 AS 不具有中转的作用,简单地来说,它只能够扮演 customer 的角色,并且分布在除了 Tier-1 的各个层中。剩余的少部分 transit AS 在路由信息转发中担任了中转的角色,这些 transit AS 在层次结构中表示为 Tier-1 provider, Tier-2 provider…。80% 以上的 customer 都属于 Tier-1 provider 和 Tier-2 provider,呈现了幂律分布的特点。通过 Route Views 的数据分析, 大约99% 的 AS 节点在5 hops(前三层)之内就可以到达目的地,即 Tier-2、Tier-1、Tier-1、Tier-2。作为节点度最高的两个层之一的 Tier-2 provider 在路由转发中起到了桥梁的作用,将路由信息通过顶级 Tier-1 转送到网络的其他地方。

b)Tier-2 从 Tier-1 购买中转信息的服务,再将这些服务转卖给它的 customer,然而这样的方式需要偿付更高的费用。由此越来越多的 AS 都选择绕过 Tier-1,直接通过 Tier-2 以 private peering 或者 public peering 的方式转发路由信息。由此,Tier-2 成为了最能吸引流量的节点。

c)因特网交换点 IXP(NAP 是它的前身)为 Tier-2 provider 之间提供了 public-peering 的连接。从 2011 年 sFlow 采样的最大规模之一的 IXP 数据分析[18],将近 80% 的成员是 Tier-2 provider,其他成员仅占了很小部分,如图 3 所示。并且近乎 90% 的流量都来自于 Tier-2 provider,也就是说 Tier-2 provider 主导了 IXP 的流量。目前有大约 300 多个 IXP[19],IXP 的 peering 成员的数目也在不断增加,有的可以达到 1 000 个以上,这样的数目是惊人的,同时也给 IXP 的信息验证带来了巨大的负担。

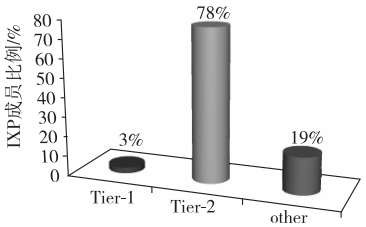

图 3　IXP 成员比例

综上所述,Tier-2 provider 作为路由转发的中转节点,IXP 的主导者,吸引了所有节点中最多的网络流量,并成为 90% 以上路由必经的中转节点。将其视为关键节点 KN,拥有权威机构所授予的能够证明其身份的特殊证书,并发挥对路由信息认证的处理能力及与其他 KN 的安全交互能力。

2.2　功能组件

SR-KN 的三个主要组件是关键节点、密钥产生器(key generator,KG)以及认证资源存储库(validation resource storage, VRS)。

KN 已经在 2.1 节详细介绍,此处不再重复。

KG 是置于每个 AS 中,产生用于确认和验证路由信息的随机密钥对(k_i^+,k_i^-)。

VRS 是置于每个 KN 中,存储已验证的属于 KN 的 customer 的地址前缀信息,这些信息从资源 PKI(RPKI)的存储库系统中导出[20],详细内容见 2.4.1 节。

本文假设 KN 没有受到恶意攻击者的入侵,其本身是安全可信的。

2.3　路径属性验证

阶段 1[21]　BGP 发言者宣告一条 UPDATE 信息,置于 AS_1 内部的 KG 首先产生一对密钥对(k_i^+,k_i^-),其中 k_0^- 用于下一个 BGP 发言者执行 RA 的私钥,k_0^+ 用于验证下一个 RA 的公钥。每个发起者使用自己所持有的私钥 Ik_0^- 确认路由信息并传送给 AS_2。与每一个 S-BGP 发言者一样,Ik_0^- 来自 PKI 的预分配,且与宣告者证书中的公钥相对应。每个 AS 确认的路由信息包括 IP 地址前缀、AS_PATH、下一个指定的 AS 以及产生的公钥 k_0^+。KG 产生的私钥 k_0^- 一般通过 IPSec 传送给下一个 BGP 发言者。

接收到 UPDATE 消息的 AS_2 的 BGP 发言者从证书数据库中获取宣告者的证书,使用证书中的公钥 Ik_0^+(与 Ik_0^- 相对应)验证 RA,并在需要确认的路由信息的 AS_PATH 项添加此 BGP 发言者所属 AS 号,使用来自上游 AS 的私钥 k_0^- 执行 RA。除此之外,清除 k_0^-,将所有的 RA 和置于本 AS 的 KG 产生的私钥 k_1^- 一起传送给下一个指定的 AS_3。

$$AS_0 \rightarrow AS_1 : \{ IP; AS_0; AS_1; k_0^+ \}_{Ik_0^-}, k_0^-$$

$$AS_1 \rightarrow AS_2 : \{ IP; AS_0; AS_1; k_0^+ \}_{Ik_0^-}$$

$$\{ IP; AS_1, AS_0, AS_2; k_1^+ \}_{k_0^-}, k_1^-$$

$$\cdots$$

$$AS_{i-1} \rightarrow AS_i : \{ IP; AS_0, AS_1; k_0^+ \}_{Ik_0^-}$$

$$\cdots$$

$$\{ IP; AS_{i-1} \cdots AS_0; AS_i; k_{i-1}^+ \}_{k_{i-2}^-}, k_{i-1}^-$$

每个 AS 使用 KG 自产生的密钥对(k_i^+,k_i^-)执行 RA 以及 RA 的验证,仅仅获取了一次证书中的公钥,减少了证书的需求量,节省了证书的存储量,提高了执行速度。并且从安全角度来说,每一次随机产生的密钥对得到了实时更新,减轻了密钥管理的负担。

阶段 2　当 KN_1 内部的 BGP 发言者接收到 UPDATE 消息,验证路由经过的每一个 AS 所作的 RA。如果成功,清空 RA 队列,并使用自身持有的私钥 Ik_{KN}^-(Ik_{KN}^-来自于 PKI 的预分配)执行 RA_{KN_1};否则停止转发路由信息。RA_{KN_1} 的信息内容如图 4 所示。

Signer:签名实体的标志符(通常是 IP 地址)
Signature:确认所使用的哈希函数和签名算法
Expiry 确认的有效期
Date: 具体日期
A-bit: 用来标志路径聚合
RASC:1 RA 序列中所包含 RA 的数目
EXPPA 数字签名信息规范化版本
Prefix: 发起者宣告的地址前缀
AS_PATH: AS 路径(AS_{TN}...)
Target: 指定的下一跳 AS
自产生的公钥
Footprint: ID 与密钥的哈希值

图 4 KN 的具体 RA 信息

KN 路由确认的内容与其他普通 AS 不同的是增加了 Footprint 字段。Footprint 是 KN_1 的足迹,处于下游的 KN_2 可以通过 Footprint 值辨别上游 KN_1 的真实存在性和可靠性。Footprint 采用单向哈希函数 H 对 KN_1 的 ID 以及 KN_1 与 KN_2 的密钥进行哈希运算得到:

$$\text{Footprint} = H(\text{ID}_1 + \text{key}(\text{KN}_1, \text{KN}_2))$$

其中:$\text{key}(\text{KN}_1, \text{KN}_2)$是权威机构预先通过 IPSec 或离线方式分配给每两个 KN 之间的共享密钥。带密钥的单向哈希运算可以有效地防止第三者的窜改和伪造,以保证足迹的真实性和可靠性。

最后,KN_1 将 RA_{KN_1}和自产生的私钥 k_{TN}^-传送给下一个指定的 AS——AS_{KN+1}。

2.4 地址前缀验证

2.4.1 VRS

VRS 存储了已验证的属于 KN 的 customer 的 IP 地址前缀和 AS 标志符的映射关系。它的数据集来源于资源 PKI—RPKI[20]。

RPKI 将用于 IP 地址前缀分配的 PKI 与 AS 标志符分配的 PKI 合并为同一个 PKI,X.509 证书通过扩展指定了地址前缀与 AS 标志符的映射关系,此类证书被称之为资源证书。RPKI 还建立了以地址前缀和 AS 标志符作为资源的形式化验证的数据库。它的主要组件如下:

a)一个包含有资源证书的 PKI;

b)一系列经过数字化签名的路由对象;

c)用来存储这些对象的分布式库系统。

所谓的数字化签名的路由对象其实就是权威机构已经授予某 AS 宣告某 IP 地址前缀的权利,将此 AS 标志符与 IP 地址前缀块的相互关联信息经过数字签名所表示的对象集合。库系统以分布式的方式通过 IANA、RIRs 以及 ISPs 存储路由对象。

VRS 是从分布式库系统中复制属于 KN customer 的数字化签名对象集合,连同资源证书一起存入 KN 的本地数据库。

2.4.2 VRS 存储与匹配

VRS 的数据以 $m = \text{map}\langle P, \text{AN}\rangle$的形式存储,其中以地址前缀 P_{VRS}/[prefix. min. length, prefix. max. length] 为 key, 相对应的 AS 号 AN 作为 value 进行存储。当接收到 UPDATE 信息时,提取出路由信息中的地址前缀 P_{update}和 AN_{update}与 VRS 中的数据进行匹配,结果有三种可能:valid、invalid、not found。具体描述和流程(图 5)如下:

a)当 P_{update}被 P_{VRS}所覆盖,并且 AN_{update}也可以与 p 相对应的 AN 集合中的元素相对应,则认为是 valid。

b)当 P_{VRS}被 P_{update}所覆盖或者与 P_{update}无匹配项,则为 not found。

c)当 P_{update}被 P_{VRS}所覆盖,但是 AN_{update}不能与 P 相对应的 AN 集合中的元素相对应,则认为是 invalid。

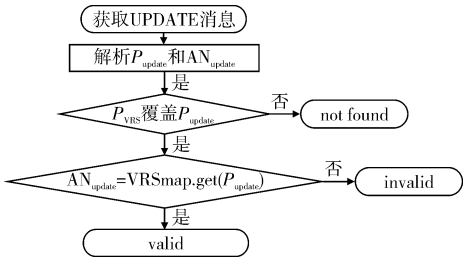

图 5 VRS 匹配流程

2.4.3 地址前缀防护

阶段 1 BGP 发言者在宣告新的地址前缀信息的同时,使用了与地址分配证书内公钥相对应的私钥执行 AA。与 RA 所不同的是,如图 4 所示,在 Target 字段中,不再描述指定的下一跳 AS,而是描述了一个或多个发起宣告的 AS 号。当下一个 AS 接收到 UPDATE 信息时,从存储库中获取预先处理好的宣告者的地址分配证书,使用证书中与发起 AS 私钥相对应的公钥验证 AA。路由信息经过的每一个 AS,验证一次宣告者的 AA,直到 KN_1 接收到 UPDATE 消息。

阶段 2 KN_1 接收到 UPDATE 信息,提取地址确认中的地址前缀和 Target 中的 AS 号与 VRS 中的数据进行匹配。如果结果为 valid,则认为源地址的宣告合法并继续转送给下一个指定的 AS,反之则不合法。后续的 AS 将不再对源地址信息进行认证,直到下一个 KN_2 收到 UPDATE 消息。

整个验证过程如图 6 所示。

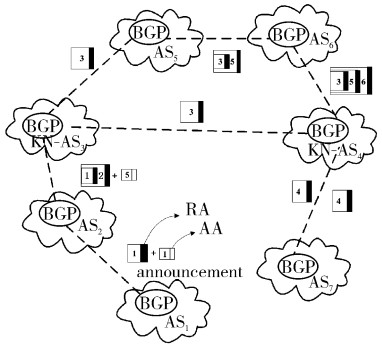

图 6 SR-KN 验证过程

3 对比分析

3.1 安全性分析

SR-KN 可实现以下安全目标:

a)宣告者和 KN 的身份不可伪造。只有合法的宣告者和 KN 才能持有专属于它们的私钥。通常私钥会被安全保存,假设攻击者很难窃取私钥,通过计算获取私钥并实现身份伪造是不可能的。

b)源数据—IP 地址前缀真实可信。PKI 下发的所有数字证书能够将源 AS 宣告的 IP 地址前缀与 AS 标志符绑定,只有合法的源 AS 才持有其专属的私钥。在传输过程中,其他普通 AS 通过数字证书中的公钥验证源 AS 的 AA。如果验证成功,则证明源 AS 宣告的 IP 地址前缀与证书中绑定的信息一致,即真实可信。KN 通过与 VRS 所存储的资源证书中已验证的 AS 标志符与 IP 地址前缀相互关联关系来验证源数据。资源证书是已经被签名的证书,非合法成员无法获得 X.509 证书扩展部分的信息。由此,KN 通过权威机构的资源库来确保源数据的真实性。

c)保证了 AS 路径的真实性和完整性。每一个 AS 的 BGP 发言者都预先建立了下一跳列表,并将列表分发给其他 AS。假设 AS 之间不会发生合谋现象,就算 AS 路径验证的过程中某个确认私钥被盗取,由于 RA 中包含了 Target 字段,验证过程保证了 Target 字段与下一跳列表的一致性,使得敌人无法肆意窜改 AS 路径,保证了普通节点与 KN 之间 AS 路径的真实性和完整性。

d)提供 KN 之间的相互信赖。PKI 授予了 KN 特殊的证书以证明其身份的合法性。每个 KN 的 RA 添加了 Footprint 字段。Footprint 字段使用单向哈希函数来保证不被窜改和伪造,并使得处于下游的 KN 辨别上游 KN 是否真实存在,由此判断它对信息验证处理的真实性。为了防止 KN 遭受攻击者的入侵,需要在 KN 部署其他附加的安全机制,这部分并不属于本文研究的内容。在本文中,假设 KN 并未受到攻击者的入侵。

3.2　收敛性能

SR-KN 使用与 S-BGP 相同的算法 DSA,执行一次签名确认需消耗 0.038 s,验证一次签名则为 0.046 s。KG 自产生的密钥对已在离线状态准备完成,它的开销可以忽略不记。S-BGP 与 SR-KN 的安全机制带来了额外的开销,由此影响了网络的收敛性。为了评估在不同机制下网络收敛的性能,使用网络模拟器 SSFNet 进行仿真实验。在实验中,采用了 110 个自治系统 AS 的网络规模,每个 AS 内部只有一个边界路由器,将节点度最高且相互连接的节点视为 Tier-1, 与 Tier-1 直接相连并连接其他低级节点的视为 Tier-2 provider。分别对 BGP、S-BGP 以及 SR-KN 进行了模拟,若将 Tier-1 断开之后再次连接,三种机制收敛性能的比较如图 7 所示。

很明显地看出,与 S-BGP 相比,SR-KN 的网络收敛时大约减少了一半。

3.3　IXP 的计算开销

值得注意的是,IXP 的 peering 数目使得 S-BGP 在这个特殊的节点面临了巨大的挑战。根据 2.1 节的分析,IXP 80% 的成员是由 KN 组成的,而这 80% 的 KN 占据了总流量的 90%。如果一个 KN 所携带的 UPDATE 消息包含了大约 2 ~ 3 个 AS 的验证信息,而 IXP 的 peering 数目达到 800 时,每秒钟平均大约接收 13 个 UPDATE 消息,那么每秒钟将会产生大约26 ~ 30 个 RA,将这些 RA 交付给 IXP 来验证所带来的负担是不可言喻的。SR-KN 的每个 KN 可以将每个 UPDATE 消息中 RA 的验证数目降为 1,AA 的验证数目降为 0,那么很明显可以看出,每秒钟需要处理的 RA 将至少降低 50%,随之网络收敛速度也会得到很大的提高。

3.4　证书规模及存储量

1)证书规模

S-BGP 方案中验证 AA 和 RA 都需要 PKI 发布的证书来完成验证。SR-KN 方案中只有 AS 节点处于发起者或 KN 节点的下游时 RA 的验证才需要证书;只要处于 KN 下游,AA 的验证则无须执行。针对两种方案,图 8 就发放证书的规模进行了比较。

可以看出,SR-KN 证书规模明显地减少了,不仅仅消除了存储量的顾虑,同时也减少了证书管理所带来的额外开销。

2)存储量

存储量的需求主要考虑两个方面:a)证书的存储,2.4.1 节详述了有关问题;b)存储重复的 AA 和 RA 以减少验证 AA 和 RA 带来的计算开销。

a)与 S-BGP 不同的是,已验证的 AA 只存储于 KN 中,并且存储的只是 KN 的 customer 的相关验证信息,不同的 KN 可以分摊 AA 验证的存储负担。

b)S-BGP 方案中,每个 AS 存储重复 RA 的空间是 20 MB,对于一般的 AS 来说,只有 2 ~ 3 个 peer,不会产生大的影响,但是在 IXP 点,如果存在几百个 peer, 存储量的需求量就很难处理了。SR-KN 方案中 KN 所交付给 IXP 的 RA 已经减少了 50%,对于 IXP 来说无须投入更大的成本来增加额外的存储空间。

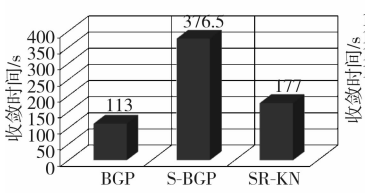

图 7　收敛性能比较

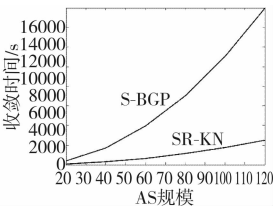

图 8　S-BGP 与 SR-KN 证书规模比较

4　结束语

域间路由安全问题一直是全球所关注的问题,虽然在近些年的研究过程中取得了很大的发展,但至今为止并没有一个完善的解决方案。本文在分析了经典解决方案 S-BGP 的基础上提出 SR-KN 方案。此方案在保证了域间路由通信安全的前提下,降低了执行的复杂度,减少了证书规模和存储量需求,同时提高了网络收敛性能,并解决了 IXP 所面临的计算负担和存储问题,最后经过实验证明此方案是有效可行的。但是本文还存在一些不完善的地方,SR-KN 是在假设关键节点本身可信的情况下设计的,在今后的工作中将会深入研究关键节点的可信模型,进一步对此方案进行完善。

参考文献:

[1] REKHTER Y, LI T, HARES S. RFC 4271, A border gateway protocol 4 (BGP-4) [S]. 2006.

[2] MURPHY S. RFC 4272, BGP security vulnerabilities analysis [S]. 2006.

[3] KENT S, SEO K. RFC 4301, Security architecture for the Internet protocol [S]. 2005.

[4] HEFFERNAN A. RFC 2385, Protection of BGP sessions via the TCP MD5 signature option [S]. 1998.

[5] 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.

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

[7] HUSTON G, ROSSI M, ARMITAGE G. Securing BGP: a literature survey [J]. IEEE Communications Surveys & Tutorials, 2011, 13(2):199-222.

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

[9] 胡湘江,朱培栋,龚正龙. SE-BGP:一种 BGP 安全机制[J]. 软件学报, 2008,19(1):167-176.

[10] 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.

(下转第 3782 页)

3 仿真测试及结果分析

仿真实验采用的是经过 FFMPEG 转换后为 8 位 128 kbps 的 WMA 格式音频信号作为原始载体语音采样信号，如图 6 所示。图 7 是含水印的数字音频信号。采用图像作为水印，如图 8 所示。从仿真实验可以看出，比较原始数字音频信号和含水印的数字音频信号的波形图，两者之间失真几乎不存在，嵌入水印后信噪比 SNR = 37.26 dB，说明嵌入水印后的音频已经具有良好的音频效果，从而证明了采用 FFMPEG 转换格式后的原始音频文件在利用本算法嵌入水印后的透明性有很好的效果。

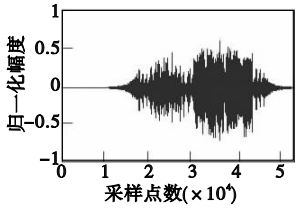

图6 原始载体语音采样信号波形图

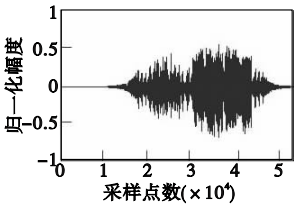

图7 嵌入水印后的数字音频波形图

为了检测经过格式转换后的音频水印文件的稳健性，对其分别进行下面的处理：a）音频压缩，压缩至 128 kbps；b）低通滤波，截止频率为 10 kHz；c）加入高斯白噪声（均值为 0，均方差为 0.01）。图 9（a）～（c）分别为经过以上处理后提取的水印，归一化相关系数分别为 0.68、0.75、0.82。从图 9 中可以得出，经过该算法处理后的提取水印与原始水印具有很强的视觉相似性，所以对数字音频信号的版权具有很好的保护性。

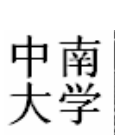

图8 插入的水印图片

图9 提取的水印图像

4 结束语

本文首先通过 FFMPEG 开源程序实现了音频文件的格式转换，比第三方软件具有更强的嵌入性和灵活性，省去了因为格式导致实际的水印嵌入复杂的繁琐过程，音频格式转换前后的失真情况几乎为零。对于本文所提出的基于改进的分段 DCT 域水印算法是根据不同的水印攻击、透明性的需要以及置乱极化操作和量化等方法和原理上研究出来的。实验结果表明，此方案在水印透明性方面有很好的成果，能抵御大多数的水印攻击，稳健性强、计算时间短、可行性很高。由于现在对音频文件的水印攻击没有一套完整的标准，文中得到的攻击数据只是在实验基础上主观得到的，而且文中提到的四个嵌入位置也不一定是水印嵌入的最佳位置，这些将是下一步研究的重点。

参考文献：

[1] 王颖，肖俊，王蕴红. 数字水印原理与技术[M]. 北京：科学出版社，2007.

[2] PODILCHUK C I, DELP E J. Digital watermarking: algorithms and applications[J]. IEEE Signal Processing Magazine, 2001, 18(4): 33-46.

[3] PAINTER T, SPANISAS A. Perceptual coding of digital audio[J]. Proc of the IEEE, 2000, 88(4): 451-515.

[4] VOYATZIS G, PITAS I. The use of watermark in the protection of digital multimedia product[J]. Proc of the IEEE, 1999, 87(7): 1197-1207.

[5] 温泉，王树勋，年桂君. DCT 域音频水印：水印算法和不可感知性测度[J]. 电子学报，2007，35(9)：1702-1705.

[6] 李跃强. DCT 域音频水印透明健壮算法[J]. 计算机工程与应用，2010，46(3)：84-86.

[7] 马翼平，韩纪庆. DCT 域音频水印：嵌入对策和算法[J]. 电子学报，2006，34(7)：1260-1264.

[8] 张金燕，赵占杰. 基于快速独立分量分析的音频盲数字水印算法[J]. 北京石油化工学院学报，2009，17(1)：28-31.

[9] 暴晋飞，柏森，朱桂斌，等. 基于能量比的小波域音频水印算法[J]. 计算机应用研究，2010，27(3)：1035-1038.

[10] 孙见青，汪荣贵，李守毅. 基于 DC 分量和 AC 分量相结合的数字水印技术[J]. 合肥工业大学学报：自然科学版，2007，30(7)：825-828.

[11] 黄雄华，王宏霞. 一种 DCT 域自适应音频水印算法[J]. 计算机应用研究，2009，26(8)：2989-2991.

（上接第 3757 页）

[11] GOODELL G, AIELLO W, GRIFFIN T, *et al*. Working around BGP: an incremental approach to improving security and accuracy of interdomain routing[C]//Proc of the Network and Distributed System Security Symposium. 2003: 75-85.

[12] KARLIN J, FORREST S, REXFORD J. Pretty good BGP: improving BGP by cautiously adopting routes[C]//Proc of IEEE International Conference on Network Protocols. 2006: 290-299.

[13] SUBRAMANIAN L, ROTH V, STOICA I, *et al*. Listen and whisper: security mechanisms for BGP[C]//Proc of Symposium on Networked Systems Design and Implementation. 2004: 29-31.

[14] SIGANOS G, FALOUTSOS M, FALOUTSOS P, *et al*. Power laws and the AS-Level Internet topology[J]. IEEE/ACM Trans on Networking, 2003, 11(4): 514-524.

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

[16] GE Zi-hui, FIGUEIREDO D, JAISWAL S, *et al*. On the hierarchical structure of the logical Internet graph[C]//Proc of SPIE ITCom. 2001: 208-222.

[17] University of Oregon route views project[EB/OL]. http://www.routeviews.org/.

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

[19] PeeringDB [EB/OL]. [2013-04-20]. https://www.peeringdb.com/private/index.php.

[20] MOHAPATRA P, SCUDDER J, WARD D, *et al*. RFC 6811, BGP prefix origin validation [S]. 2013.

[21] KONG Ling-jing, ZENG Hua-xin. Use of distributed trustworthy node to secure AS_PATH[C]//Proc of International Conference on Multimedia Information Networking and Security. 2012: 35-38.