

## 一种轻量化的边界网关协议路径验证机制

赵宸<sup>\*①③</sup> 孙斌<sup>①②</sup> 杨义先<sup>①③</sup> 杨焱<sup>②</sup>

<sup>①</sup>(北京邮电大学信息安全中心 北京 100876)

<sup>②</sup>(北京交通大学轨道交通控制与安全国家重点实验室 北京 100044)

<sup>③</sup>(北京邮电大学灾备技术国家工程实验室 北京 100876)

**摘要:** 由于边界网关协议(Border Gateway Protocol, BGP)存在安全问题, 路径信息(AS\_PATH 属性)易遭受各种攻击。已有的路径验证方案中, 过程复杂和开销巨大严重阻碍了方案的实际部署。基于对 AS\_PATH 属性的分析, 该文提出一种轻量化的 BGP 路径验证机制—FTAPV(First-Two-AS based Path Verification)。FTAPV 中, 更新报文只需要携带 AS\_PATH 中前两个 AS 的签名信息就可以有效地为路径信息提供保护。安全分析和性能评估表明, 与已有方案相比, 该机制在保证安全能力的同时, 有效地减少了路由资源的消耗和所需证书的规模, 具有良好的可扩展性。

**关键词:** 信息安全; 边界网关协议(BGP); 路径验证; First-Two-AS

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1009-5896(2012)09-2167-07

**DOI:** 10.3724/SP.J.1146.2012.00285

## A Lightweight Mechanism for Border Gateway Protocol Path Verification

Zhao Chen<sup>①③</sup> Sun Bin<sup>①②</sup> Yang Yi-xian<sup>①③</sup> Yang Yan<sup>②</sup>

<sup>①</sup>(Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

<sup>②</sup>(State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China)

<sup>③</sup>(National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

**Abstract:** Since BGP (Border Gateway Protocol) possesses many security vulnerabilities, BGP Autonomous System PATH information (AS\_PATH attribute) is vulnerable to various attacks. In proposed BGP path verification mechanisms at present, the high computational overhead and complex process severely block security solutions from being implemented and deployed in real world. A lightweight method is designed for BGP path verification named First-Two-AS based Path Verification (FTAPV). Based on analysis of AS\_PATH attribute, FTAPV can protect path information effectively through carrying signatures of first two ASes in the AS\_PATH of UPDATES. Security analysis and performance evaluation demonstrate this mechanism can reduce the route resource expense and the number of used certificates with strong ability of security and good scalability compared with existing method.

**Key words:** Information security; Border Gateway Protocol (BGP); Path verification; First-Two-AS

### 1 引言

边界网关协议(Border Gateway Protocol, BGP)<sup>[1]</sup>通过 UPDATE 更新报文在自治系统(Autonomous System, AS)之间交换网络可达性信息。作为目前唯一的域间路由协议, BGP 拥有丰富的路径属性, 其中最重要的两个属性就是网络可达

性信息(Network Layer Reachable Information, NLRI)和 AS\_PATH 属性。NLRI 用于列出可到达目的地的集合; AS\_PATH 顺序记录了一条 BGP 路由从源 AS 到目的 AS 所经过的路径。

BGP 的安全是 Internet 路由安全的关键, 但 BGP 在设计之初是建立在网络高度可信的基础之上, 没有考虑任何安全因素, 本身存在的安全问题主要有以下 3 点<sup>[2]</sup>: (1)BGP 会话的安全; (2)前缀地址的起源认证; (3)路径属性信息的完整性和真实性认证。近年来, 许多的域间路由安全事件都是由 BGP 的脆弱性引起的<sup>[3-5]</sup>, 严重影响了网络的可信、

2012-03-20 收到, 2012-06-06 改回

国家自然科学基金(61121061), 国家重大科技专项(2011ZX03002-005-01)和轨道交通控制与安全国家重点实验室(北京交通大学)开放课题基金(2010K010)资助课题

\*通信作者: 赵宸 sdqdzhaochen@163.com

可控和可管。

路径信息(AS\_PATH属性)的保护作为BGP安全所要解决的首要问题之一,引起了学者们的广泛关注,提出了多种路径验证方案<sup>[6-8]</sup>,但大量的签名验证操作和过多的证书存储开销制约了方案的部署实现。如何降低路由资源的消耗,提高路径验证的性能成为安全方案能够部署的关键。本文根据对AS\_PATH属性的分析,参考了人类社会中的现象,提出了一种轻量化的BGP路径验证机制——FTAPV(First-Two-AS based Path Verification)。该机制中,每个UPDATE消息携带AS\_PATH属性中前两个AS的签名信息,通过这两个签名的验证为路径信息提供保护。与已有的方案相比,FTAPV在不降低安全能力的同时,有效地减少了签名的数量,签名信息不会随着路径的增加而积累,同时显著降低了认证所需的证书规模,具有良好的可扩展性。本文的重点在于路径信息的保护,有关BGP其他方面的安全问题超出了本文的讨论范围。

本文第2节分析了对AS\_PATH的各种攻击。第3节总结了当前的相关研究工作,并分析其中的不足。第4节阐述了FTAPV的工作机制。第5节和第6节分别对机制进行了安全能力分析和性能评估。第7节分析了该机制的证书规模。最后总结全文。

## 2 AS\_PATH攻击分析

AS\_PATH路径属性可以用来避免环路,其长度也是BGP协议的第2选路标准<sup>[1]</sup>(越短的AS\_PATH越被优选)。对AS\_PATH的攻击主要分为以下3类。本文以图1为例描述这3种攻击,AS<sub>1</sub>通告其拥有的前缀信息( $f, \{1\}$ ),根据BGP路由传播规则和各AS的本地策略,最终AS<sub>8</sub>将分别收到来自AS<sub>6</sub>和AS<sub>7</sub>的两条UPDATE消息( $f, \{6,4,2,1\}$ )和( $f, \{7,5,3,1\}$ )。

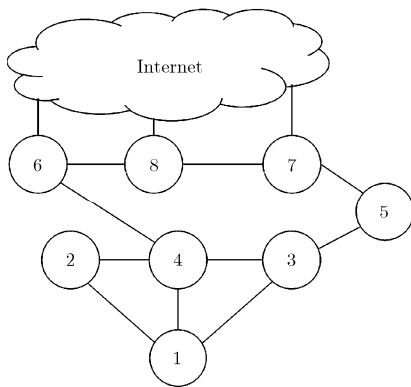


图1 网络拓扑示意图

### 2.1 填充攻击

出于自私等原因,节点可以通过增加AS\_PATH的长度使其避免被优选为最佳路由。例如,图1中,自私节点AS<sub>7</sub>向AS<sub>8</sub>通告虚假路由( $f, \{7,5,3,4,2,1\}$ ),通过增加AS\_PATH的长度欺骗AS<sub>8</sub>使其优选AS<sub>6</sub>为路由的下一跳。

### 2.2 删减攻击

攻击节点可以通过减少AS\_PATH的长度使其被优选为最佳路由。以图1为例,设恶意节点AS<sub>6</sub>向AS<sub>8</sub>通告伪造的路由信息( $f, \{6,4,1\}$ ),使AS<sub>8</sub>优选其作为路由的下一跳。这样AS<sub>6</sub>可以获得更多来自AS<sub>8</sub>去往AS<sub>1</sub>的流量,进行流量分析或者窃取更多的私密信息等。

### 2.3 修改攻击

恶意节点可以修改AS\_PATH中的AS号,产生黑洞路由,导致路由信息丢失。假如AS<sub>6</sub>为坏节点,修改AS<sub>2</sub>为AS<sub>8</sub>,向AS<sub>8</sub>通告修改过的路由信息( $f, \{6,4,8,1\}$ )让AS<sub>8</sub>误认为产生了环路而丢弃路由消息,即形成路由黑洞,造成路由缺失。

## 3 相关研究

目前,针对BGP面临的AS\_PATH篡改攻击,现有的安全方案可以分为3类:

第1类为主动保护方案,比较著名的有:S-BGP(Secure BGP)<sup>[6]</sup>和soBGP(secure origin BGP)<sup>[7]</sup>。S-BGP基于公钥基础设施(PKI)颁发的AS证书,使用累计签名的方式确保BGP路径信息真实可靠,但过于庞大的计算和空间开销导致无法部署。soBGP使用拓扑数据库对路径进行认证,但不能验证该更新报文是否确实经过AS\_PATH所含的自治系统以及抵抗AS\_PATH填充攻击。基于身份的路径验证方案IDPV<sup>[8]</sup>在S-BGP基础上,简化了PKI的结构,但过多的签名验证操作还是带来了较多的负担。近年来提出的psBGP<sup>[9]</sup>与SE-BGP<sup>[10]</sup>等弱安全机制以降低安全能力为代价,大量削减协议开销,但这些方案也未被广泛接受。

第2类为被动保护方案即路由监测方案<sup>[11, 12]</sup>,通过监测BGP路由信息和事件来发现和抑制虚假路由行为,但是监测方案只是一种被动解决方案,它需要具备对虚假路由强有力的识别能力及快速响应机制的配合才能达到快速有效阻断攻击、降低攻击影响的目的。

第3类为延迟更新方案:PGBGP(Pretty Good BGP)<sup>[13]</sup>延迟所有新路由的使用直至确定该路由是合法的,但因为延迟合法新路由的使用,PGBGP中路由的收敛时间显著长于BGP。

基于密码学等技术的主动安全方案虽然修改了 BGP 协议，增加了路由器的处理负担，但是我们仍然重点研究了主动安全方案，因为攻击检测方案始终都是一种被动的处理方法，只有主动解决方案才能有效地阻止攻击的发生，也为设计下一代可信网络的安全域间路由架构打下了良好的基础。

## 4 FTAPV 体系结构和工作机制

### 4.1 相关知识

**定义 1** First-Two-AS: 本文中, First-Two-AS 指的是 AS\_PATH 中最前两个 AS。例如, 设  $AS_i$  收到路径信息为  $\{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$ , First-Two-AS 为  $AS_{i-1}$  和  $AS_{i-2}$ 。

### 4.2 AS\_PATH 属性分析

AS\_PATH 属性列出了路由在传递过程中经历了哪些 AS, 路径验证实际上就是判断上一跳 AS 是否存在破坏 AS\_PATH 的行为, 这有点类似于人类社会中的排队列。人们在排队列时, 其实并不需要从头开始对齐, 而只需验证是否与前两个人处于同一条直线上即可。如果队列中的每个人都能准确地做到这一点, 则这个队列最终会是一条直线。FTAPV 利用这种特性, 通过 AS\_PATH 中前两个 AS 的签名就可以对路径进行验证, 确保路径信息的安全。

### 4.3 证书结构

FTAPV 采用一个两级层次的 PKI 进行安全认证, 主要有 AS 证书和 BGP 路由器证书, 解决 AS 的身份和 BGP 路由器的身份验证问题。

(1)AS 证书(ASCert): 某组织  $A$  向地区注册机构 RIR(Regional Internet Registry)申请 AS 号码, 提供自己的公钥、已分配的地址空间和相关的私有信息。RIR 对组织  $A$  所提供的信息进行合法性检查, 检查通过后除为  $A$  分配一个 AS 号码外, 还将颁布包含上述信息的签名证书给申请者。

(2)BGP 路由器证书(BSCert): 在一个 AS 中, 所有的 BGP 路由器都将得到由 AS 签名的证书, 共用一对公私钥对, 并且和 AS 证书的公私钥对相一致<sup>[9]</sup>。这样 BGP 路由器可以代替 AS 进行签名或者验证签名, AS 之间也只需要获得其余 AS 的 ASCert 证书就可以达到相互认证的目的。

证书不能作为 UPDATE 消息的一部分来传递, 因为这样不但消耗了有限的带宽, 而且 UPDATE 消息最大只有 4096 byte<sup>[1]</sup>, 这对证书来说是不够的。本文采用更为合理的带外传输的方式, 相对来说, 证书的更新频率不高, 带外传输的方式比较节省带宽和储存空间及大量的签名验证过程。

### 4.4 路由证据(route evidence)属性

为了保护 AS\_PATH 属性不被恶意篡改, 本文增加了一种新的、可传递的属性——路由证据属性。通过验证其正确性来保证 AS\_PATH 的真实性与完整性。路由证据属性携带了 AS\_PATH 中最前两个 AS 的签名信息。不失一般性, 设  $AS_0$  为路由的起始者, 经路由传播,  $AS_i$  收到的路径信息为  $(\{AS_{i-1}, AS_{i-2}, \dots, AS_0\})$ , 其中  $i \geq 1$ ,  $AS_i$  向  $AS_{i+1}$  通告路由信息所携带的路由证据属性的具体格式如图 2 所示。其中“首”签名  $Signature_n = \{AS_{i-1}, AS_{i-2}, \dots, AS_0\}_{k_{i-1}}$  为离路由接收者 2 跳距离的 AS 对路径的签名信息;“尾”签名  $Signature_i = \{AS_i, AS_{i-1}, \dots, AS_0\}_{k_i}$  为路由发送者对路径的签名信息,  $k_{i-1}$  为  $AS_{i-1}$  的私钥,  $k_i$  为  $AS_i$  的私钥。“首”与“尾”签名形成一条“签名链”为 AS\_PATH 提供保护。特别地, 路由起始者的  $Signature_n$  为  $\emptyset$ 。

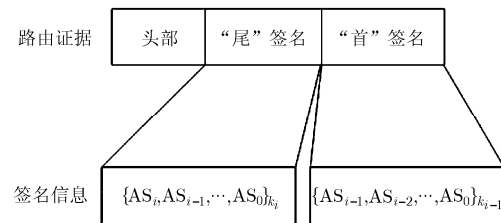


图 2 路由证据属性格式

### 4.5 FTAPV 工作流程

首先定义 3 个函数:

- (1)  $S_{k_i}(m)$  表示  $AS_i$  使用私钥  $k_i$  对信息  $m$  进行签名。
- (2)  $V_{p_i}(S)$  表示  $AS_i$  使用公钥  $p_i$  对签名  $S$  进行验证。

验证签名信息通过的条件就是  $V_{p_i}(S_{k_i}(m))=m$ 。

- (3)  $U_i(AS\_PATH)$  表示 AS\_PATH 中从第  $i$  个 AS 号开始到路由起始 AS 为止的一个 AS\_PATH 的子集。例如, 假设  $AS\_PATH = \{AS_i, AS_{i-1}, \dots, AS_0\}$ , 那么  $U_2(AS\_PATH) = \{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$ 。特别地, 当  $i=1$  时, 有  $U_1(AS\_PATH) = AS\_PATH$ 。

具体的工作流程如下:

- (1)初始: 在初始阶段, 每个 AS 获得属于自己的 ASCert, 每个路由器获得相应的证书 BSCert。通过带外传输机制, 每个 AS 获得相邻 2 跳距离内 AS 的 ASCert 证书以便验证使用。

- (2)路由更新: 不失一般性, 设  $AS_i$  (其中  $i \geq 0$ , e.g., 0,1,2,…) 的路由更新算法如表 1 (路由更新之前需对收到的路由信息进行验证, 若验证失败, 丢弃虚假的路由信息) 所示。

表1 路由更新算法

```

算法1 路由更新
输入: 收到的 AS_PATH 属性和路由证据属性。
输出: 新的 AS_PATH 属性和路由证据属性。
if (|AS_PATH| == 0) /*路由起始者*/
    Add(localAS,AS_PATH); /*将本地 AS 号加入到 AS_PATH 中*/
     $S_{k_i}(AS\_PATH) \rightarrow Signature_t$ ; /*签名当前的路径信息, 填入到  $Signature_t$  中*/
else if (|AS_PATH| == 1) /*路由的第1个接收者*/
     $Signature_h = Signature_t$ ; /*将  $Signature_t$  移动到  $Signature_h$  的位置*/
    Add(localAS,AS_PATH);
     $S_{k_i}(AS\_PATH) \rightarrow Signature_t$ ;
else /*路径上其他节点*/
    Delete  $Signature_h$ ; /*从 Route Evidence 中删除  $Signature_h$ */
     $Signature_h = Signature_t$ ; /*将  $Signature_t$  移动到  $Signature_h$  的位置*/
    Add(localAS,AS_PATH);
     $S_{k_i}(AS\_PATH) \rightarrow Signature_t$ ;
end

```

在签名转发路由的过程中, UPDATE 消息始终只携带路径信息中最前面两个 AS 的签名信息。如果 AS 为路由的起始者, 只签名路径信息; 如果 AS 为路由的第 1 个接收者, 在验证收到的路由信息后, 将“尾”签名移动到“首”签名的位置, 再将包含本地 AS 号的 AS\_PATH 进行签名, 签名信息直接加入到路由证据中; 如果 AS\_PATH 长度大于 1, 在验证路由信息后, 删除“首”签名信息, 将“尾”签名移动到“首”签名的位置, 然后对加上本地 AS 号的 AS\_PATH 进行签名, 将新的“尾”签名加入到路由证据中, 完成通告过程。当然, 路径上最后一个节点不需要转发路由, 也就不需要进行路由更新算法。

(3)验证过程: 对于某条路径信息的验证, 主要是针对路由更新中携带的路由证据属性的验证, 若通过表示路由真实可靠, 否则立即丢弃虚假路由。路由接收者  $AS_i$  对收到的路径信息 ( $\{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$ , 其中  $i \geq 1$ ) 和携带的路由证据属性的验证算法如表 2 所示。

验证算法中, 路由更新的第 1 个接收者, 验证起始者的  $Signature_t$  签名; 路径上其他节点需要验证“首”与“尾”两个签名。另外, 路由的起始者不需要进行路径验证。

图 3 举例说明了 FTAPV 的一次工作流程以及 AS\_PATH 和路由证据属性的处理过程。 $AS_1$  通告路由信息 ( $f, \{1\}$ ),  $f$  为其拥有的地址前缀。 $AS_1$  签名

表2 验证算法

```

算法2 验证算法
输入: 收到的 AS_PATH 属性和携带的路由证据属性。
输出: True or False。
if (|AS_PATH| == 1) /*路由的第1个接收者*/
    if ( $V_{p_i}(Signature_t) == AS\_PATH$ ) /*验证路由起始者的签名*/
        return True;
    else
        return False;
    end
else /*路径上其他节点*/
    if ( $V_{p_i}(Signature_h) == U_2(AS\_PATH) \& \& V_{p_i}(Signature_t) == AS\_PATH$ ) /*验证“首”和“尾”两个签名*/
        return True;
    else
        return False;
    end
end

```

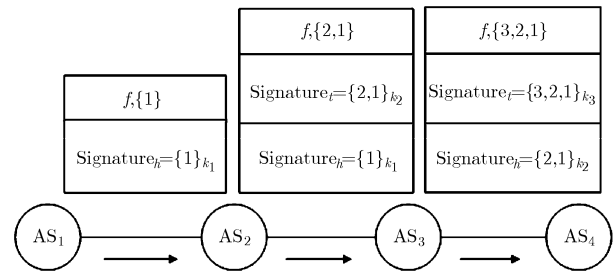


图3 FTAPV 工作示例

路径信息生成  $Signature_t = \{1\}_{k_1}$  加入到路由证据属性中, 发送给  $AS_2$ 。 $AS_2$  验证路由证据属性后, 将  $Signature_t$  移动到  $Signature_h$  的位置, 然后签名路径信息  $Signature_t = \{2,1\}_{k_2}$  加入到路由证据属性中, 发送给  $AS_3$ 。 $AS_3$  验证后, 删除  $Signature_h$  项, 将  $Signature_t$  移动到  $Signature_h$  的位置, 然后签名路径信息  $Signature_t = \{3,2,1\}_{k_3}$  前置到路由证据属性中, 发送给  $AS_4$ 。

## 5 安全能力分析

### 5.1 FTAPV 方案的正确性

**定理1** FTAPV 方案是正确可行的。

本文提出的 FTAPV 方案, 是借鉴了人类社会中的排队列的思想, 即只要每个人都与前面两个人对齐, 就可以保证队列最后是一条直线。利用这一思想, 在路径验证中, 只需要前两跳 AS 的签名, 即可验证路径信息是否真实可信。所以, FTAPV 方案是正确可行的。

## 5.2 FTAPV 方案的安全性

FTAPV 方案在签名验证上采用 DSA(Digital Signature Algorithm)签名技术, DSA 签名技术是基于整数有限域上离散对数难题的。本文的重点在于 FTAPV 方案如何为路径信息提供安全保护, 抵御各种攻击。

不失一般性, 我们以路径  $AS_{i-1} \rightarrow AS_i \rightarrow AS_{i+1}$  为例, 对本方案中路径信息的安全性进行详细分析, 假设  $AS_i$  为恶意节点, 其收到来自  $AS_{i-1}$  的路径信息为  $\{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$  和路由证据属性中携带的两个签名,  $AS_{i+1}$  为验证者。

实际上,  $AS_{i+1}$  对  $AS_i$  发送的路径信息的验证分为两部分, 即  $\{AS_i, AS_{i-1}\}$  和  $\{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$ 。(1) 由于  $AS_i$  无法获得  $AS_{i-1}$  的私钥, 也就无法模拟  $AS_{i-1}$  的签名, 所以  $AS_i$  无法修改路径信息  $\{AS_{i-1}, AS_{i-2}, \dots, AS_0\}$ , 所以这部分路径信息是安全的。(2) 由于  $AS_i$  与  $AS_{i+1}$  为直连邻居, 邻居间的 AS 号在邻居建立时已互相通告<sup>[1]</sup>, 所以  $AS_i$  只能对  $AS_i$  后面的路径进行篡改, 同时  $AS_i$  由于无法获得其他 AS 的私钥, 无法模拟其他 AS 的签名, 所以保证了  $AS_i$  无法对  $\{AS_i, AS_{i-1}\}$  之间进行任何的添加、删除或者修改, 所以这部分路径信息也是安全的。

FTAPV 方案能够为路径信息提供强有力的保护, 我们以第 2 节所描述的对路径信息的攻击为例, 对方案抵御攻击的能力进行分析。

(1) 抵御填充攻击: 若  $AS_i$  在  $AS_{i-1}$  之后增加任意的 AS 号  $AS_j$ , 设虚假的路径信息为  $\{AS_i, AS_{i-1}, AS_j, \dots, AS_0\}$ , 由于  $AS_i$  无法得到其余 AS 的私钥, 那么  $AS_{i+1}$  在验证  $AS_{i-1}$  的签名时就会发现伪造路径; 若攻击节点在  $AS_i$  与  $AS_{i-1}$  之间增加任意的 AS 号  $AS_j$ , 设虚假的路径信息为  $\{AS_i, AS_j, AS_{i-1}, \dots, AS_0\}$ , 由于  $AS_i$  得不到其余 AS 的私钥,  $AS_{i+1}$  在验证  $AS_j$  的签名时就会发现路径信息为伪造的。

(2) 抵御删减攻击: 若删除的 AS 号码中包含  $AS_{i-1}$ , 设伪造的路径信息为  $\{AS_i, AS_{i-2}, \dots, AS_0\}$ , 因为  $AS_i$  无法得到  $AS_{i-2}$  的私钥来模拟其签名, 所以  $AS_{i+1}$  通过验证签名会发现路径虚假; 若删除的 AS 号中不包含  $AS_{i-1}$ , 设伪造的路径信息为  $\{AS_i, AS_{i-1}, AS_{i-3}, \dots, AS_0\}$ , 同样, 在  $AS_{i+1}$  验证  $AS_{i-1}$  的签名信息时会发现虚假路径。

(3) 抵御修改攻击: 若修改的 AS 号码中包含  $AS_{i-1}$ , 设仿造的路径信息为  $\{AS_i, AS_j, \dots, AS_0\}$ 。因为  $AS_i$  无法模仿其余 AS 的签名, 所以  $AS_{i+1}$  会通过验证签名检测出路径被恶意修改。若修改的 AS 号码不包含  $AS_{i-1}$ , 设修改  $AS_{i-2}$  为  $AS_j$ , 虚假的路径信息为  $\{AS_i, AS_{i-1}, AS_j, \dots, AS_0\}$ , 同样,  $AS_{i+1}$  验证

$AS_{i-1}$  的签名信息时会检测出虚假路径。

通过上述分析我们可以看出, 本方案能够有效地抵御对路径信息的各种攻击, 为路径信息提供强有力的保护。

## 6 性能评估

FTAPV 采用 DSA 数字签名方案, 签名的长度采用 320 bit(即 40 byte), 并采用 OpenSSL<sup>[14]</sup>库实现。基于 Ubuntu11.04 操作系统, 模拟结果表明, 在 2.4 GHz 的处理器上, DSA 算法的验证时间约为 2.6 ms, 签名时间约为 2.1 ms。

### 6.1 通信开销

新增加的路由证据属性中携带两个签名, 其长度大约为 81 byte, 即  $\Delta_{\text{FTAPV(DSA)}} = 81(l > 1)$  byte。而在 S-BGP 与 IDPV 方案中, 更新报文增加的大小分别为  $\Delta_{\text{S-BGP(DSA)}} = 42 \times l + 4$  和  $\Delta_{\text{IDPV}} = 50 \times l + 4$ <sup>[8]</sup>,  $\Delta$  表示通信开销的增量,  $l$  为路径长度。

图 4 显示了 FTAPV, IDPV 与 S-BGP 更新报文长度的增量大小, 虽然增加了一个新的属性, 但 FTAPV 消除了路径验证中签名的累积, 其更新报文的增量显著小于 IDPV 和 S-BGP 方案, 并且增量保持不变。

### 6.2 收敛时间

在 FTAPV 中, 影响收敛时间的关键取决于签名技术带来的 CPU 额外的处理时间。表 3 给出了 FTAPV 和 S-BGP 在签名验证方面 CPU 的时间开销,  $l$  为路径长度,  $t_s$  为签名的时间,  $t_v$  代表验证花费的时间。当路径大于 2 时, FTAPV 在处理签名验证的时间开销明显小于 S-BGP, 而且并不伴随着路径的增加而增长。

表 3 FTAPV/S-BGP 路由器签名和验证 UPDATE 消息的时间开销

路由器	签名和验证时间开销
FTAPV	$l \times t_v + t_s (l < 1), 2 \times t_v + t_s (l > 1)$
S-BGP	$l \times t_v + t_s$

我们使用基于离散事件驱动的 NS2<sup>[15]</sup>仿真工具考察机制性能, 采用 BRITE 拓扑生成器生成网络拓扑<sup>[16]</sup>。仿真参数设置如下: 最小路由通告间隔 (MRAI)  $M=30$  s, 链路延迟  $ld=0.1$  ms。假设每个 AS 只有 1 台 BGP 路由器, 每个 AS 通告 2 条路由信息。图 5 表明, FTAPV 的收敛时间对 BGP 的收敛时间影响很小。

当前 Internet 中, 绝大多数 BGP 路由器, 平均每秒只处理一次 UPDATE 消息<sup>[10]</sup>。在 200 MHz 的 CPU 的条件下(接近真实的路由器)<sup>[17]</sup>, DSA 算法的

验证时间为 31 ms, 签名时间为 25.5 ms。FTAPV 处理一次 UPDATE 消息进行 1 次签名操作和 2 次验证操作, 时间约为 87.5 ms。即使遇到路由器重启等特殊情况, 峰值扩大 10 倍, 签名验证花费的时间总和约为 875 ms, 对收敛时间造成的影响很小, 而且随着 CPU 的升级, 签名与验证消耗的时间也会越来越小。

结果表明, 该方法减少了对路由资源的消耗, 就目前的条件看, 完全可以满足 FTAPV 方案所带来的额外的开销。

### 7 可扩展性分析

为了统一分析, 我们假设每个 AS 拥有一个证书(不考虑 BGP 路由器证书), 同时我们考虑 2 个指标: 全网的证书规模  $C$  和单个节点证书规模  $C_n$ 。设整个 Internet 中总的 AS 的节点规模为  $N$ , 平均每个 AS 拥有  $avgP$  个邻居。则对于任意 AS, 直连邻居的数目  $\alpha_1 = avgP$ , 相邻  $k$  跳距离的节点数为  $\alpha_k = avgP^k$ ,  $k$  跳距离以内的邻居节点数目为  $V_k = \alpha_1 + \alpha_2 + \dots + \alpha_k = \frac{avgP \times (1 - avgP^k)}{1 - avgP}$ 。

在 S-BGP<sup>[6]</sup>中, 总证书规模  $C_{S-BGP} = N^2$ , 单个节点证书规模为  $C_{n_{S-BGP}} = N$ 。

在 IDPV<sup>[8]</sup>中, 总证书规模  $C_{IDPV} = 0.027 N^2$ , 单个节点证书规模  $C_{n_{IDPV}} = 0.027 N$ 。

在 SE-BGP<sup>[10]</sup>中, 总证书规模  $C_{SE-BGP} = 100N +$

$0.006 N^2$ , 单个节点规模  $C_{n_{SE-BGP}} = 100 + 0.006 N$ 。

在 FTAPV 中, 总的证书规模为  $C_{FTAPV} = V_2 \times N$ , 单个节点  $C_{n_{FTAPV}} = V_2 = avgP \times (1 + avgP)$ 。

X.509 证书大约有 600 byte 大小<sup>[17]</sup>。基于 2012 年 2 月 13 日的 CIDR Report<sup>[18]</sup>数据, 当前 Internet 中, 大约有 40200 个 AS。整个互联网中, AS 拥有的平均邻居数  $avgP = 5.4$ <sup>[19]</sup>, 表 4 对比了 FTAPV 与已有安全方案的证书规模和单个节点证书存储开销  $Sc$ 。

表 4 证书规模和存储开销

方案	$C$	$C_n$	$Sc(\text{Mbyte})$
FTAPV	$1.69 \times 10^6$	42	0.02
S-BGP	$1.62 \times 10^9$	40200	23.00
IDPV	$4.37 \times 10^7$	1086	0.62
SE-BGP	$1.37 \times 10^7$	341	0.20

FTAPV 单个节点的证书规模只有 S-BGP 的 0.1%, IDPV 的 3.9% 和 SE-BGP 的 12.3%。这是由于 FTAPV 进行路径验证时只需 2 跳距离内邻居的证书, 消除了签名信息的累积, 节约了路由设备并不宽裕的存储空间。图 6, 图 7 说明了网络规模扩展时证书规模的发展趋势。

随着网络的发展, FTAPV 的证书规模发展趋势远小于 IDPV, S-BGP 与 SE-BGP。因此, FTAPV 具有良好的可扩展性。

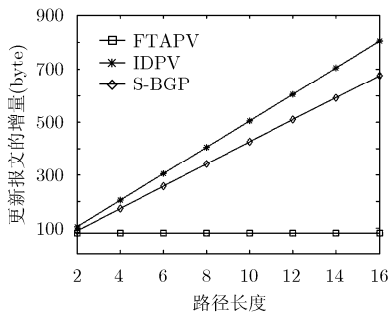


图 4 FTAPV, IDPV 和 S-BGP 方案更新报文的增量

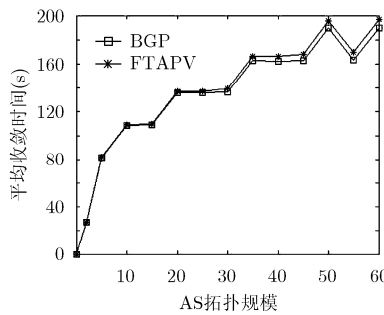


图 5 平均收敛时间

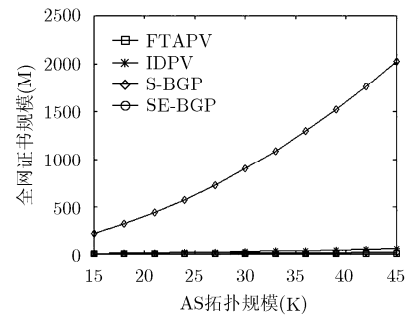


图 6 全网证书规模

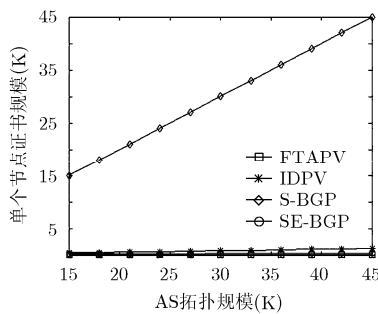


图 7 单个节点证书规模

### 8 结束语

BGP 作为域间路由协议, 在 Internet 路由系统中起到至关重要的作用。虽然 BGP 比较圆满地完成了路由的工作, 但是缺乏任何安全机制的 BGP 协议也为日后网络埋下了极大的隐患。路径验证是 BGP 安全的一个重要方面, 关于路径验证已提出了很多解决方案, 但是 PKI 管理复杂, 路由资源过多的消耗使得方案难以实现。基于此, FTAPV 作为一种轻量化的方案, 通过验证 AS\_PATH 中最前面两个

AS 的签名信息, 保证了路径信息的真实性与完整性。本文详细讨论了机制的安全性和性能, 与已有的方案相比, FTAPV 在保证安全能力的同时, 明显减少了签名验证的开销, 对 BGP 收敛时间的影响很小, 显著降低了证书的规模, 可扩展性良好, 为 BGP 路径验证提供了一种可操作性强的方法, 易于在实际中部署实现。

### 参 考 文 献

- [1] Rekhter Y, Li T, and Hares S. A Border Gateway Protocol 4 (BGP-4)[S]. RFC 4271, 2006.
  - [2] Butler K, Farley T, and McDaniel P. A survey of BGP security issues and solutions[J]. *Proceedings of IEEE*, 2010, 98(1): 100-122.
  - [3] Huston G, Rossi M, and Armitage G. Security BGP-A literature survey[J]. *IEEE Communications Surveys and Tutorials*, 2011, 13(2): 199-222.
  - [4] 吕高锋, 孙志刚, 卢锡成. 域间 IP 欺骗防御服务增强机制[J]. *软件学报*, 2010, 21(7): 1704-1716.  
Lü G F, Sun Z G, and Lu X C. Enhancing the ability of inter-domain IP spoofing prevention[J]. *Journal of Software*, 2010, 21(7): 1704-1716.
  - [5] 刘欣, 朱培栋, 彭宇行. Co-Monitor: 检测前缀劫持的协作监测机制[J]. *软件学报*, 2010, 21(10): 2584-2598.  
Liu X, Zhu P D, and Peng Y X. Co-Monitor: collaborative monitoring mechanism for detecting prefix hijacks[J]. *Journal of Software*, 2010, 21(10): 2584-2598.
  - [6] Kent S, Lynn C, and Seo K. Secure Border Gateway Protocol(S-BGP)[J]. *IEEE Journal on Selected Areas in Communications*, 2000, 18(4): 582-592.
  - [7] White R. Securing BGP through secure origin BGP[J]. *Internet Protocol Journal*, 2003, 6(3): 15-22.
  - [8] 王娜, 顾纯祥, 汪斌强. 基于身份的 BGP 路径验证机制[J]. *计算机工程*, 2007, 33(17): 34-36.  
Wang N, Gu C X, and Wang B Q. BGP path verification mechanism based on ID[J]. *Journal of Computer Engineering*, 2007, 33(17): 34-36.
  - [9] Kranankis E, Wan T, and Oorschot P C. On interdomain routing security and pretty secure BGP(psBGP)[J]. *ACM Transactions on Information and System Security*, 2007, 10(3): 1-41.
  - [10] 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, and Gong Z H. SE-BGP: an approach for BGP security[J]. *Journal of Software*, 2008, 19(1): 167-176.
  - [11] Cazenave I O, Kosluk E, and Ganiz M C. An anomaly detection framework for BGP[C]. *Innovations in Intelligent Systems and Applications (INISTA)*, Istanbul, Turkey, 2011: 107-111.
  - [12] 胡宁, 邹鹏, 朱培栋. 基于信誉机制的域间路由安全协同管理方法[J]. *软件学报*, 2010, 21(3): 505-515.  
Hu N, Zou P, and Zhu P D. Reputation-based collaborative management method for inter-domain routing security[J]. *Journal of Software*, 2010, 21(3): 505-515.
  - [13] Karlin J, Forrest S, and Rexford J. Pretty good BGP: improving BGP by cautiously adopting routes[C]. *Proceedings of the IEEE International Conference on Network Protocols*, Santa Barbara, California, USA, 2006: 290-299.
  - [14] OpenSSL: the open source toolkit for SSL/TLS[EB/OL]. <http://www.openssl.org/>, 2012.
  - [15] The network simulator-ns2[EB/OL]. <http://www.isi.edu/nsnam/ns/>, 2012.
  - [16] BRITE [EB/OL]. <http://www.cs.bu.edu/brite/>, 2012.
  - [17] Zhao M, Smith S W, and Nicol D. Evaluating the performance impact of PKI on BGP security[C]. *4th Annual PKI Research and Development Workshop*, Gaithersburg, MD, April 2005.
  - [18] CIDR report[EB/OL]. <http://www.cidr-report.org/as2.0>, 2012.
  - [19] Internet topology at router- and AS-levels, and the dual router+AS Internet topology generator[EB/OL]. <http://www.caida.org/research/topology/generator/>, 2012.
- 赵 宸: 男, 1985 年生, 博士生, 研究方向为网络安全与路由技术。  
孙 斌: 女, 1967 年生, 副教授, 研究方向为媒体通信、计算机网络与网络安全。  
杨义先: 男, 1961 年生, 教授, 研究方向为编码密码学、网络与信息安全。