

# 自治系统间的安全路由协议 GesBGP

李 琦<sup>1)</sup> 吴建平<sup>1)</sup> 徐明伟<sup>1)</sup> 徐 恪<sup>1)</sup> 张新文<sup>2)</sup>

<sup>1)</sup>(清华大学计算机科学与技术系 北京 100084)

<sup>2)</sup>(Samsung Information Systems America, San Jose, CA, USA)

**摘 要** 域间路由协议 BGP 的安全性直接影响着互联网路由的可用性. 虽然现有很多改进的 BGP 安全方案可以解决这些安全问题, 但这类方案存在很多设计缺陷(例如, 路由资源消耗问题). 在文中, 作者充分考虑了安全 BGP 的目标并提出了一个 Good-Enough-Security BGP (GesBGP) 协议. GesBGP 在可信计算技术的基础上使用基于身份的密钥(IFS)算法确保 BGP 协议中身份的真实性. IFS 算法的引入有效地消除了传统安全 BGP 协议中部署集中公钥基础设施(PKI)以及公钥证书的分发和储存问题. 此外, GesBGP 不单纯依赖于安全密钥算法, 基于可信计算技术的 BGP 可信服务从路由器系统本身防止了系统配置的非篡改, 消除了路由消息的多重累积签名. 在提出的优化 GesBGP 协议中, 通过部署 BGP 的安全规则建立 AS 之间强制信任关系, 进一步消除了 BGP 通告消息中的累积签名. 安全分析和性能评价表明, 优化的 GesBGP 在确保 BGP 安全性的同时有效地改进了 GesBGP 的性能.

**关键词** 域间路由协议; BGP; 安全 BGP; GesBGP

**中图法分类号** TP393 **DOI 号:** 10.3724/SP.J.1016.2009.00506

## GesBGP: A Good-Enough-Security BGP

LI Qi<sup>1)</sup> WU Jian-Ping<sup>1)</sup> XU Ming-Wei<sup>1)</sup> XU Ke<sup>1)</sup> ZHANG Xin-Wen<sup>2)</sup>

<sup>1)</sup>(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)

<sup>2)</sup>(Samsung Information Systems America, San Jose, CA, USA)

**Abstract** Inter-domain routing (BGP) directly influences availability of Internet routing which may be disrupted by misconfigured or malicious BGP updates. Although several secure solutions have been proposed to resolve the BGP security problem, they have many design drawbacks (e. g., large router resource consumption). Considered the design and performance of secure BGP, this paper proposes a Good-Enough-Security BGP (GesBGP). Identity-based signature (IBS) algorithm presented in GesBGP guarantees the authenticity of BGP routes in the help of Trusted Computing (TC) technology. The presented IBS can effectively eliminate the centralized public key infrastructure (PKI) and resolve the problem of public key certificate distribution and restoration. Furthermore, GesBGP does not only rely on cryptography functions provided by IBS. BGP attestation service integrated in GesBGP prevents router from malicious change radically and thus builds strong trust relationship between different routers. In the optimized GesBGP, BGP security rules are enforced and the cumulated signature in original GesBGP is eliminated. The security analysis and performance study show that the optimized GesBGP improves the performance of GesBGP while achieving the goal of BGP security at the same time.

**Keywords** inter-domain routing; BGP; secure BGP; GesBGP

收稿日期: 2008-09-20; 最终修改稿收到日期: 2009-01-14. 本课题得到国家自然科学基金(90604024)、国家“八六三”高技术研究发展计划项目基金(2007AA01Z2A2)、教育部科学技术研究重点项目(106012)以及新世纪优秀人才计划的资助. 李 琦, 男, 1979 年生, 博士研究生, 主要研究方向为计算机网络体系和协议、网络与系统安全. E-mail: liqi@csnet1.cs.tsinghua.edu.cn. 吴建平, 男, 1953 年生, 博士, 教授, 博士生导师, 主要研究领域为互联网体系结构、网络协议测试. 徐明伟(通信作者), 男, 1971 年生, 博士, 教授, 博士生导师, 主要研究领域为计算机网络体系结构、高速路由器体系结构、互联网路由. E-mail: xmw@csnet1.cs.tsinghua.edu.cn. 徐 恪, 男, 1974 年生, 博士, 副教授, 博士生导师, 主要研究领域为路由器软件体系结构. 张新文, 1974 年生, 博士, 主要研究方向为网络与系统安全.

## 1 引言

域间路由协议(BGP)是连接不同 IP 网络(自治域)形成互联网的一个重要路由协议,但是由于 BGP 协议本身的设计缺陷,BGP 存在很多安全漏洞,这些问题到目前为止还没有得到很好的解决。在 BGP 协议中,每个自治域(AS)申明自己的路由信息,而邻居 AS 收到这些路由信息后无法验证收到的路由消息的有效性而仅仅进一步传播这些路由信息。BGP 基于这个依赖关系建立了整个互联网的信任关系,但实践证明这个层次的信任关系无法得到保障。这个脆弱的信任机制使得很多伪造的路由申明在互联网中传播,并且导致数据分组将沿着不准确(错误)的路径传播,进而引入了很多互联网路由的安全问题,例如伪造路由。

BGP 安全的关键问题在于 BGP 中无法验证 AS 是否有权利申明一个 IP 前缀的路由,而伪造的路由直接导致了互联网的安全问题。伪造的路由可能是由于错误的配置或者恶意的攻击引起的,而伪造的路由可以直接引起严重的网络问题。例如,巴基斯坦电信公司发布的一条错误的路由导致了全球的 YouTube 服务意外中断。在很多情况下,伪造的路由产生于对一些目标服务的恶意攻击,通过让路由器产生 IP 前缀的伪造路由,攻击者可以探测或者丢弃这个前缀的分组以实现拒绝服务攻击或者中间人攻击等。

为了提高 BGP 的安全性并且有效防御恶意的路由通告,近年来提出了很多安全的 BGP 方案,其中包括安全保护<sup>[1-2]</sup>和异常检测<sup>[3-5]</sup>。典型的 BGP 安全保护方案有使用集中的路由权威机构和公钥基础设施的 SBGP<sup>[1]</sup>和 SoBGP<sup>[2]</sup>。这些算法需要消耗很多路由器的资源来存储各种可信信息,因此很难得到规模部署。异常检测的方案通过在 BGP 更新消息中添加前缀信息和 AS 的绑定<sup>[3]</sup>、比较路由更新和带外消息<sup>[4]</sup>以及查询第三方服务<sup>[5]</sup>以检测伪造路由。但这些方案不仅会消耗很多宝贵的路由器资源,而且可能会引入错误检测故障而影响正常的数据转发。

在本文中,我们提出了一个 Good-Enough-Security BGP(GesBGP),路由系统以最少的计算代价获得足够安全的路由消息。在 GesBGP 中,我们引入了身份密钥签名算法(IFS)验证申明前缀和路由的有效性以及 BGP 可信服务,确保路由申明的完整

性。在不减弱 BGP 验证的安全性的情况下,GesBGP 不仅消除了传统的基于 RSA/DSA 的公钥密码算法验证路由所需要的公钥证书的管理,而且大大减少了由于安全密钥算法的多重累积签名所消耗的路由器资源。在 GesBGP 中,可信计算为 BGP 的可信验证服务提供的基本支持,彻底消除了由于人为配置或者路由劫持等攻击产生伪造路由的可能性。此外,为了减少由于多次签名引入的额外的计算代码并且优化 GesBGP 的性能,我们在路由可信验证服务中实现了路由有效性和可信性的检测。在路由可信服务中,通过验证路由器中输入和输出路由是否满足路由的安全策略规则以确保输出路由通告的安全可信。由我们的安全分析和性能评价可知,优化的 GesBGP 在确保 BGP 安全性的同时进一步优化了 GesBGP 的性能。

本文第 2 节简要介绍安全 BGP 的一些重要工作;第 3 节简要介绍本文的背景知识;第 4 节提出我们的 GesBGP 基本协议和 GesBGP 的改进协议;第 5 节分析协议的安全性以及 GesBGP 的性能;第 6 节总结全文。

## 2 问题阐述

我们首先回顾了 BGP 的安全性问题,并且分析和总结了目前已有的安全 BGP 方案。

### 2.1 BGP 的安全性问题

目前 BGP 协议主要面临 BGP 通告者和 BGP 会话的攻击,例如,一个恶意的或者错误配置的 BGP 通告者以及一个被截获或者未授权的 BGP 会话都会引起 BGP 路由异常。这些攻击一般分成两类:一是前缀劫持,另外一类是无效路径攻击。由于 BGP 中路由器无法验证收到通告消息中的 AS 源,一个 BGP 路由器可以通告任意前缀,包括那些根本不属于该 AS 的前缀,这类攻击我们称为前缀劫持。类似地,由于 BGP 路由器无法验证一个更新消息中的路由路径的有效性,所以被通告的路由可能是无效的并且将导致数据流量到达一个错误的目的地,这类攻击我们称为无效路由攻击。

前缀劫持包括了完整前缀劫持和部分前缀劫持。完整前缀劫持比较容易实现而且很难检测,例如,一个 AS 中的任意路由器都可以通告一个不属于该 AS 的前缀。一般来说,BGP 的过滤器可以过滤从邻居发送过来的不希望收到的前缀通告,但由于 AS 无法维护一个实时更新的过滤器,所以这种攻

击很难被检测到. 在部分前缀劫持中, 恶意的路由器可以通告部分更细化的 IP 前缀, 将部分的流量重定向到敌手, 而其他的流量将正常到达目的地. 由于路由器实现了最长路由匹配, 所以通过通告一个细化的前缀可以欺骗所有的 AS 使用伪造的路由.

无效路由攻击指 BGP 通告的路径中包含违反 BGP 策略或者无效的 AS 号. 由于 BGP 是策略路由, 所以 AS 无法检测其他 AS 之间的连接关系, 所以这类攻击也是很难检测的. 具体来说, 无效路由攻击可以分为伪造最短路径攻击、路由重分布攻击和 AS 号伪造攻击. 伪造最短路径攻击是违反策略强制减少从源 AS 到敌手所在 AS 路径中 AS 的数量; 路由重分布攻击指 BGP 路由输出了从服务网络或对端网络学习到的路由; AS 伪造是在输出路由前将伪造的 AS 号放入到通告的路径中.

## 2.2 安全 BGP 方案

为了有效解决 2.1 节中的 BGP 安全问题, 人们提出了很多的安全 BGP 算法. 一般来说, 安全 BGP 算法可以分为两类, 一类是通过安全算法实现的 BGP 攻击避免, 典型的算法有 SBGP<sup>[1]</sup>、SoBGP<sup>[2]</sup>、psBGP<sup>[3]</sup>等, 另外一类是通过部署 BGP 无效路由检测攻击, 典型的算法有 IRV<sup>[5]</sup>、Whisper<sup>[6]</sup>和 PGBGP<sup>[7]</sup>等.

SBGP(Secure BGP)是最早的一个安全 BGP 方案<sup>[1]</sup>, 通过使用公钥基础设施(PKI)颁发 AS 证书和前缀证书以提供前缀源认证以及路径认证. 在 SBGP 中使用了累计签名以确保使用的 BGP 通告消息安全可靠. 但是, 这个方案存在很多问题, 例如消耗计算代价和庞大的空间代价等. 为了解决 BGP 的问题, SoBGP(Secure Origin BGP)引入了分散的信任模型<sup>[2]</sup>. SoBGP 增加了额外的 BGP 消息传送证书, 但这个方案无法防御 AS 路径攻击. 一般来说, 这类方案中的安全算法都涉及比较大的运算代价, 无法满足现在 BGP 运行的真实场景.

IRV(Interdomain Route Validation)方案使用了一个额外的路由验证服务<sup>[5]</sup>, 通过查询第三方的路由验证服务来验证 BGP 消息的真实性, 但这个方案无法解决伪造 AS 的攻击. psBGP(Pretty Secure BGP)在每个 AS 中使用前缀认证列表验证消息真实性, 但这个方案不能满足 BGP 的现实运用场景<sup>[3]</sup>. Whisper(Listen and Whisper)算法通过监视路由器中的所有交换路由更新的标识位来检测异常

路由, 但无法提供足够的安全性<sup>[6]</sup>. 另外, PGBGP (Pretty Good BGP)通过减缓伪造路由的传播让网络管理员来阻止大规模的攻击<sup>[7]</sup>. 类似地, 这类算法不能快速检测 BGP 攻击, 并且可能存在故障的误报. 此外, 这类算法都无法避免无效路由通告而引起的路由器资源消耗.

## 3 背景知识

本节将介绍我们方案所涉及到的关键技术: 基于身份的签名算法和可信计算技术. 这两种技术为我们的 GesBGP 算法提供了基本的安全保障.

### 3.1 基于身份的签名算法

不同于传统基于公钥证书的公钥密钥算法, 基于身份的密钥算法(IBC)使用用户的身份信息(例如, e-mail 地址等)作为公钥信息. 这个算法由 Shamir 最早提出, 解决了公钥证书方案的密钥存储和管理问题<sup>[8]</sup>. 基于身份的密钥算法中的私钥由一个可信的授权结构 PKG(Private Key Generator)产生, PKG 负责产生与身份信息对应的私钥.

基于身份的密钥算法包括了基于身份的加密(IBE)和基于身份的签名(IBS)算法<sup>[8]</sup>. 在本文中, 我们使用 IBS 算法来签名和验证前缀和 AS\_PAH. 具体来说, IBS 算法包括了 4 个主要过程: Setup 算法产生可公开的系统参数和私密的主密钥; Extract 算法根据一个给定的公钥(比如 e-mail 地址)产生一个私钥, 这个算法需要系统参数、主密钥和身份 ID 作为输入参数; Sign 算法使用系统参数和密钥和原消息作为输入, 并输出消息的签名; Verify 算法使用系统参数和身份(ID)检测签名是否有效.

举例来说, 我们假设 Alice 希望发送一个消息给 Bob, 而 Bob 需要验证收到消息的有效性. 首先, Alice 需要获得 IBS 的系统参数和她的私钥, 这些信息通过使用她的 ID 可以在 PKG 中产生并且获得. 同样, Bob 需要获得 PKG 中的系统参数(系统参数可以在 Bob 获取私钥的时候取得). 当 Bob 收到从 Alice 的消息后, Bob 不需要再次获取 Alice 的公钥, 可以直接使用 Alice 的 ID 验证 Alice 消息中的有效性. 在 GesBGP 方案中, 验证路由申明签名的 ID 信息(IP 前缀和 AS 号)可直接在申明消息中获得, 从而有效消除了传统 SBGP 方案中证书管理和存储的问题.

### 3.2 可信计算

可信计算组织(TCG)定义了一系列可信计算(TC)的硬件和软件规范<sup>①</sup>. TCG体系的关键技术核心是可信平台模块(TPM), TPM提供了安全密钥算法和安全存储功能,在TPM芯片中提供了一系列的安全密钥来标识一个可信平台,例如EK(Endorsement Key)和AIK(Attestation Identity Key). 硬件和软件的状态信息通过使用160位的散列值确保计算机平台的完整性,这些散列值存储在TPM中提供的PCR(Platform Configuration Registers)中.

一般来说,可信系统通过核心的测量信任基(CRTM)和TPM提供了一个可信的启动过程,这个是确保平台真实可信的基础. 当所有的启动组件经过测量确认组件完整性以后相关的散列值传递到PCR中. 当验证代理组件被验证并且启动以后,它将负责验证其他应用层的程序,例如,在路由系统中每个路由协议在启动前必须确保协议软件没有被篡改以及本文所提出的BGP可信服务以及安全规则能被正确执行. 本文不详细介绍具体路由器系统具体的可信启动机制. 为了便于说明,本文中提出的路由可信服务主要关注验证影响路由协议软件的完整性以及路由消息的完整性.

此外,TPM还提供了安全存储功能,例如可信的消息封存功能. 可信消息的封存功能(TPM\_Seal)确保了在特定PCR状态下封存的消息只能在相同的PCR的状态下才能解开. 在我们的方案中,TPM封存了路由器中的各种密钥,例如对应于AS号的密钥和对应于AS所拥有前缀的密钥. 一旦路由器被攻破或者运行了非法程序,这些密码都无法获得,因此也无法对BGP消息进行正常的签名操作.

## 4 安全的域间路由系统

在本节中,我们将首先分析和阐述安全BGP协议所需要实现的目标以及我们的Good-Enough-Security BGP(GesBGP)算法的基本思路,然后展开说明GesBGP中的安全策略规则的实现以及安全路由选择算法.

### 4.1 安全路由协议的目标

安全BGP协议的目标是在存在敌手攻击的情况下,BGP路由器能够有效防御各种攻击,并且能确保路由的有效性以保证数据的正常转发. 为了实现这个安全BGP协议的目标,具体来说,我们的

GesBGP需要满足以下几个安全目标<sup>[3]</sup>:

(1) AS号授权. 安全BGP协议中必须可以验证路由器是否使用它合法拥有的AS号 $s_i$ ,在一个AS中只有授权的BGP路由器才可以拥有 $s_i$ .

(2) BGP通告者授权. 安全BGP协议中BGP的通告者也必须是可验证的,这样确保一个BGP通告者是和一个AS号 $s_i$ 相关联的.

(3) AS路径认证. 安全BGP协议中,一个BGP路由 $m$ 中的AS\_PAH( $p_k = [s_1, s_2, \dots, s_k]$ )也必须是可验证的,确保这条路由是沿着路由 $m$ 所通告的AS路径传递,例如路由 $m$ 是沿着 $s_1, s_2, \dots, s_k$ 顺序传递.

(4) 前缀源认证. 安全BGP协议中,一个AS所产生的IP前缀也必须是可验证的,只有当满足以下3个条件的IP前缀 $f_1$ 才是有效的IP前缀:① $f_1$ 是 $s_1$ 所拥有的;② $s_1$ 经过 $f_1$ 的拥有者授权;③ $s_1$ 被分配到一个前缀集合 $F_1$ 中, $s_1$ 已经收到一个前缀集合 $F_2$ ,而且 $f_1$ 是 $F_1$ 或者 $F_2$ 的聚合的前缀路由,可表示为 $\forall f_x \subseteq f_1, f_x \subseteq F_1 \cup F_2$ .

### 4.2 基本思想

我们的Good-Enough-Security BGP(GesBGP)的目标是在满足4.1节所讨论的安全BGP协议的需求基础上,以最小的计算和部署复杂度提供足够安全的BGP方案. 也就是说,我们的GesBGP协议需要实现的最终目标是,以最小的路由器代价,比如路由器的存储空间和计算资源等,获得可确保的BGP安全性,防止由于用户误操作或者敌手攻击而引起的伪造BGP路由的问题.

GesBGP协议的核心思想是采用IBS算法验证前缀源和AS路径. 首先我们假设支持GesBGP的路由器已经提供了TPM硬件的协处理器<sup>②</sup>. 具体来说,我们的GesBGP主要通过3个核心的组件来确保BGP的安全性:BGP协议密钥可信存储、BGP通告消息的签名/验证和BGP协议可信服务.

(1) 密码可信存储直接使用了TPM提供的可信封装功能,即当运行在内存中BGP系统没有被篡改过,相关的前缀和AS的密钥才能被BGP协议可信服务所获取. 一般来说,TPM封存(TPM\_Seal)该路由器所在的AS号对应的私钥以及这个AS所拥

① Trusted Computing Group, <https://www.trustedcomputinggroup.org/>

② 目前TCG组织已经在嵌入式平台(包括手机)等硬件上提出了TPM的规范和标准,所以路由器上提供TPM的假设是合理的.

有的前缀的对应私钥  $sQ_{ID}$ 。在本文中我们假设路由器已获得相关的密钥,并且已封存到了 TPM 中,如图 1 所示,当路由器从 PKG 获得对应的后直接封存到 TPM 中,这个过程需要在路由器部署网络配置时完成。只有当路由器的 PCR 处于正常状态时,所有的私钥信息才会从 TPM 中获取,确保了私钥的安全性。PCR 处于正常状态意味着此时 PCR 的值与初始私钥保存时的 PCR 状态一致,所有路由器的 BGP 进程和相关的运行环境都没有被篡改。

Notation;  
 $ID_{AS}$ : AS number  
 $MK$ : The master key of PKG  
 $Q_i$ : A string generated and kept in PKG  
 $params$ : The parameters known to all GesBGP routers  
 $sQ_{ID}$ : The private key corresponding to ID  
 $SK(m)$ : The ciphertext of message  $m$

IBS setup at PKGs;  
 1. PKGs:  $(Q_i, sQ_{ID}) = Keygen(ID, MK, params)$ ;  
 2. PKGs  $\rightarrow$  Routers:  $SK(sQ_{ID}, params)$ ;  
 3. Routers  $\rightarrow$  TPMs:  $TPM\_Seal(sQ_{ID})$ ;

Route Update;  
 4. Router A:  $\rho = Sign(Updates | params | sQ_{ID})$ ;  
 5. Router A  $\rightarrow$  Router B:  $(Updates | \rho)$   
 6. Router B:  $Verify(\rho | params | ID_{AS_A})$

图 1 IBS 算法流程

(2) BGP 通告消息的签名/验证提供了 BGP 路由器对将要通告的消息的签名,其中包括了对 IP 前缀和 AS\_PATH 的消息的独立签名以及对收到的通告消息的签名进行验证。这个过程通过使用 IBS 签名算法实现。IBS 在 GesBGP 中的概要算法流程如图 1 所示,路由器 A 用前缀或者 AS 号对应的私钥对路由通告消息签名,路由器 B 收到通告消息以后用对应的前缀标识符或者 AS 的标识符以及系统参数对签名消息验证。如果签名消息验证不通过,路由器将直接丢弃这个通告消息。

(3) BGP 协议可信服务提供了基本的 BGP 通告消息验证服务的接口,即在路由器处理接收到路由通告消息或者发送自己的路由选择前路由由申明将需要经过 BGP 协议可信服务组件的检测。可信服务属于 BGP 程序的一部分,可信计算技术最终确保服务的强制实施以消除由于人为配置或者路由劫持等攻击产生的伪造路由。在 GesBGP 协议中,可信服务包括了 3 部分算法,分别是可信服务的初始化以及 BGP 的入口 filter 和出口 filter 上验证和检测算法,具体的接口信息如图 2 所示。

#### Interface of BGP Attestation Service

0. Initialization: evaluated by core root of trust  
 input: BGP systems including programs and BGP policies,  
 output: IBS private keys including prefix keys and AS keys;
1. IN filter: incoming BGP updates  
 input BGP updates (prefix|AS\_PATH),  
 input BGP attributes in updates including update signature,  
 output true or false? //accept or reject BGP update;
2. OUT filter: outgoing BGP updates  
 input BGP updates (prefix|AS\_PATH),  
 output true or false? //continue or drop BGP update,  
 //if update legal sign prefix and AS\_PATH,  
 //else drop.

图 2 GesBGP 协议可信服务算法接口

图 2 中可信服务算法包括了 3 个过程,分别是初始化过程、入口 filter 和出口 filter。初始化过程在路由器开启的过程中执行。这个过程由路由器系统调用启动,并且由 CTRM 验证后的路由器系统验证服务验证 BGP 协议可信服务的可靠性和完整性。这个过程传入的参数是 BGP 路由软件和 BGP 策略,如果这些参数没有被篡改,则 BGP 路由软件可以正常启动,否则将直接退出。当 BGP 进程正常启动完成以后,这些输入参数的散列值将实时报告到 PCR 中。如果此时 PCR 散列值与私钥封存时的 PCR 散列值一致,则协议的可信服务可以成功获得前缀和 AS 的私钥。

可信服务中所在的入口和出口 filter 的位置和目前 BGP 协议的 filter 位置是一致的,即在收到 BGP 通告消息和发送 BGP 消息前。当 BGP 路由器收到路由通告消息,则 BGP 可信服务在入口 filter 上使用在路由申明获得的 AS 号标识和 IP 前缀标识使用 IBS 的 verify 算法依次进行验证。当验证过程中任何一个签名无效时,这个通告消息将直接丢弃。如果收到的通告消息有效,则验证服务将保存这些通告消息以及(/或者)路由通告的签名,以发送后续的路由通告消息。当 BGP 路由器完成更新消息计算以后,通告消息将在出口 filter 上检测。出口 filter 将调用可信服务接口,检测计算完的消息是否符合 BGP 安全规则。如果通告消息符合安全规则,则用前缀或者 AS 号的私钥对 BGP 通告消息进行签名。

### 4.3 GesBGP 的核心算法

由 4.2 节的分析我们可知,确保 GesBGP 安全性的核心组件是 BGP 的可信服务。在这一节中,我们将详细介绍 GesBGP 中可信服务的算法如何有效提供路由由安全性以消除潜在的伪造路由通告,从而确保 BGP 路由器的安全性。在这里我们将重点介绍在入口 filter 上和出口 filter 上的可信服务所需

要完成的路由验证工作。

当路由器收到一个 BGP 通告消息后将在入口 filter 上调用 BGP 可信服务接口,并按如图 3 所示的算法检测和校验通告消息。首先,可信服务将验证 AS\_PAH 消息的有效性,然后按着有效的 AS\_PATH 消息依次验证前缀的签名并对前缀本身进行验证。如果以上签名消息都有效,则把收到的签名消息压入可信服务列表。具体算法流程如图 3 所示。

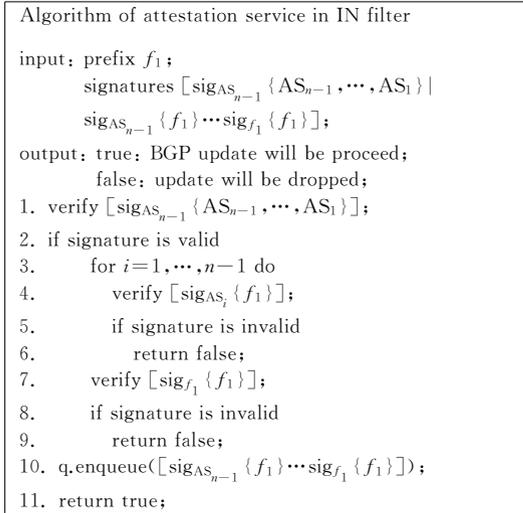


图 3 GesBGP 协议入口 filter 算法

类似地,当路由器计算完路由选择后产生 BGP 通告消息,则通告消息将在出口 filter 上进行检测,算法流程如图 4 所示。在出口 filter 上我们首先判断该前缀是否是本地 AS 所有,如果是本地 AS 所有,则需要用本地所有的前缀私钥签名;如果签名失败,则说明该前缀不是 AS 合法拥有。如果前缀不是 AS 所有,则 AS 用对应的私钥分别对前缀  $f_1$  和 AS\_PATH 进行签名操作得到 S1 和 S2。最后可信

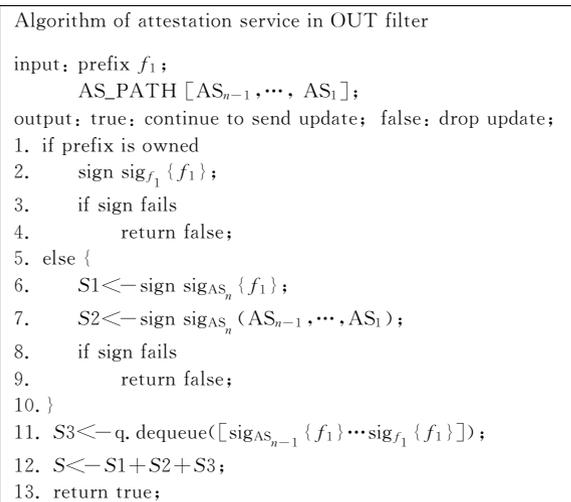


图 4 GesBGP 协议出口 filter 算法

服务将从列表中取得在入口 filter 中保存的 S3 累积作为一个完整 BGP 通告消息的签名。在这个算法中,BGP 的可信服务在入口 filter 和出口 filter 对收到和本地签名的 AS 信息进行签名累积,有效消除了 SBGP 中路由签名的多重累积签名。

下面我们通过例子介绍 GesBGP 的基本机制。我们通过图 5 所示的 AS 拓扑关系说明 GesBGP 的协议是如何确保 BGP 协议的消息的有效性。图 5 中的  $AS_1 \sim AS_6$  标识自治系统号码分别是 1~6 的自治系统。为了便于说明问题,我们假设每个自治系统只有一个边界路由器,由字母 A~F 标识,并且每个路由中都获得签名所需要的系统参数和私钥;自治系统所有的 IP 前缀用  $f_1 \sim f_2$  表示;各个圆圈间的连接标识了各个自治系统间的 BGP 会话,这些会话包括了 provider-customer 关系和 peer-peer 关系;各个圆圈所标识的消息标识了各个自治域/路由器将要通告的 BGP 更新消息以及附属于该更新消息的签名。

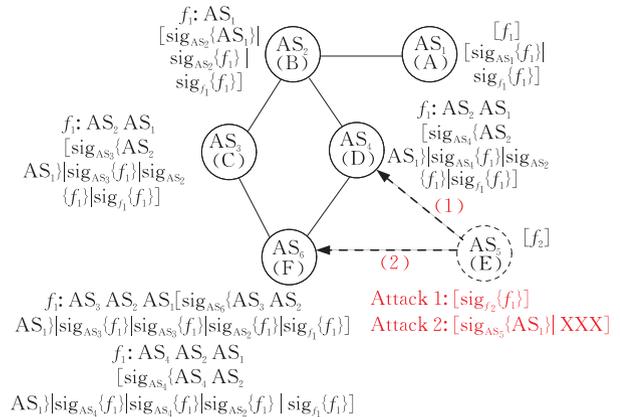


图 5 GesBGP 协议的实例分析

图 5 中  $AS_1$  的路由器 A 向  $AS_2$  的路由器 B 通告自己的一个前缀  $f_1$ ,并且在通告消息中放入通告消息的签名  $[\text{sig}_{AS_1}\{f_1\} | \text{sig}_{f_1}\{f_1\}]$ 。 $AS_2$  收到这个消息后路由器直接使用 AS 号的标识符  $AS_1$  和 IP 前缀的标识符  $f_1$  验证这个消息的有效性。有别于传统的 SBGP 等方案需要实现取得公钥证书以后才能验证 BGP 通告消息,GesBGP 并不需要预取任何公钥证书。如果收到的 BGP 通告有效,即前缀  $f_1$  属于  $AS_1$  并且路由器 A 没有修改消息,则  $AS_2$  计算自己的路由消息,并将  $f_1$  的 BGP 通告发送给  $AS_3$  和  $AS_4$ ,同时将消息的签名  $[\text{sig}_{AS_2}\{AS_2\} | \text{sig}_{AS_2}\{f_1\} | \text{sig}_{f_1}\{f_1\}]$  作为通告的一部分(属性)也同时发送出去。类似地,当  $AS_3$ 、 $AS_4$  和  $AS_6$  等自治域收到通告消息以后完成类似的操作继续通告这条路由。

现在我们考虑存在敌手的情况,如图 5 所示,我们假设  $AS_5$  中的路由器 E 由一个恶意的管理员或者被攻破. 路由器 E 通告  $AS_4$  自己是前缀  $f_1$  的所有者,但是路由器 E 无法获得前缀  $f_1$  的私钥,所以路由器 E 发送通告无法使用  $f_1$  的私钥进行签名. 当  $AS_4$  收到这个通告消息用前缀标识符  $f_1$  无法验证这个通告的有效性,则直接丢弃这个通告消息. 这种是前缀源攻击的一个实例. 另外,我们考虑 E 向  $AS_6$  发送到前缀  $f_1$  的伪造  $AS\_PAH\{AS_1\}$ ,同时通告中的消息签名为  $[\text{sig}_{AS_5}\{AS_1\}]$ . 由于  $AS_6$  无法在 BGP 更新消息中出示前缀  $f_1$  的签名,所以本次的 BGP 路由通告也不会被  $AS_6$  采纳.

从以上的实例分析可以看出, GesBGP 协议中的每个路由器都可以有效验证 BGP 更新消息的有效性,防止 BGP 更新消息的伪造. 但是,这个基本协议解决了传统安全 BGP 协议(例如, SBGP 和 SoBGP 等协议)需要消耗很多路由器资源的问题,比如公钥证书获取和存储的代价等. 在 GesBGP 中,所有的相关 IP 前缀私钥和 AS 私钥可以由 ICANN、IANA 等机构以及他们的可信代理机构的 PKG 产生. 由于验证路由的公钥信息都在路由申明中标注(例如 IP 前缀以及 AS 号),路由器可以直接利用这些信息直接验证收到的路由申明. PKG 不需要额外集中/非集中的基础设施分发的公钥信息,有效消除了由于传统 PKI 所引入的公钥证书管理和存储. 此外,通过使用 BGP 可信服务, GesBGP 不需要改动 BGP 协议路由选择过程,所以具备了比较好的可部署性. 在 GesBGP 协议中,虽然 GesBGP 消除了 AS 路径的多重累积签名,把传统 SBGP 中  $O(n^2)$  的消息签名/验证的计算复杂度下降到了  $O(n)$ . 但是, GesBGP 协议中还存在对前缀和 AS 路径累积签名的计算代价,这仍然给路由器增加很多额外的计算开销.

#### 4.4 优化 GesBGP 的算法

GesBGP 路由器提供了以 TPM 为安全核心的安全可信机制,可以有效防御由于管理员恶意行为或者路由器被攻破导致的伪造路由发布. 由于 BGP 协议中的通告信息具有规律,即所有的路由通告都有触发源<sup>[9]</sup>. 所以,我们可以在 BGP 可信服务上为不同的路由器实施安全 BGP 规则,利用这些安全 BGP 规则可以建立 AS/BGP 路由器之间的信任关系. 通过这个信任关系, GesBGP 可以消除对通告消息的重复/累积签名. 同时,利用路由可信服务中实施的安全策略规则在 BGP 的 filter 中过滤无效/伪

造的路由通告.

在优化的 GesBGP 协议中,每个路由器的出口 filter 上根据路由消息规则强制检测路由通告的有效性,确保发送的路由通告消息有效. BGP 可信服务确保只有经过安全规则检测的通告才能获得私钥签名. 通过这种基于路由信任服务的强制信任关系,路由器仅需要验证邻居路由器的身份即可信任邻居的路由通告有效性. 因此,路由器无需检测和验证收到的路由通告中 AS 路径的每一跳的有效性,即路由源用前缀验证、路由后续经过的其他 AS 的 AS 号验证等. 通过这种方式, GesBGP 可以有效消除路由通告的累积签名从而有效提高安全 BGP 的性能. 在本节中,我们将详细讨论路由通告的安全规则. 在给出具体的规则定义前,我们给出规则定义中涉及到符号定义,如表 1 所示.

表 1 规则符号表

$f_1, f_2$	IP 前缀
$N, n$	当前的 AS 号, 路由器 ID
$\varphi f_1[AS]$	收到通告消息中 $f_1$ 的 AS_PATH
$\hat{\varphi} f_1[AS]$	发送通告消息中 $f_1$ 的 AS_PATH
$Update(f_1, f_1[AS])$	BGP 路由申明消息
$Withdraw(f_1)$	前缀 $f_1$ 的路由撤销消息
$Peer(n)$	路由器 $n$ 的邻居路由器
$Time(f_1)$	路由器 $n$ 撤销/通告前缀 $f_1$ 的时间
$A(AS)$	AS 合法拥有者前缀列表

**定义 1.** 申明消息规则. 当一个路由器  $n$  允许发送一个有效 BGP 新路由的通告消息  $Update(f_1, f_1[AS])$ , 当且仅当满足下面 3 个条件之一:

- (1)  $f_1 \subseteq A(AS) \wedge \varphi f_1[AS] = \emptyset$ ;
- (2)  $(\{N\} \cup \varphi f_2[AS] = \hat{\varphi} f_1[AS]) \wedge f_2 \supseteq f_1$ ;
- (3)  $Withdraw(m, f_1) \wedge Time(n, f_2) - Time(m, f_1) < \tau \wedge \forall m \in Peers(n) \wedge f_1 \supseteq f_2$ .

这个规则说明 Update 消息有效当且仅当  $f_1$  是  $AS_N$  的所有者,或者是先前收到的路由申明的重新申明,或者是先前收到一条已撤销的消息后的再路由重新申明. 需要注意的是,我们的规则考虑了由于地址聚集引起的路由更新. 另外,定义 1 中的第 3 条规则是在路由器  $n$  收到邻居路由器  $m$  的路由撤销消息时,路由器决策选择的时间在  $\tau$  时间内完成. 也就是说, BGP 可信服务在检测和比较收到的撤销消息和将要发送的通告消息必须在  $\tau$  时间内完成<sup>①</sup>. 类似地,我们可以得到撤销消息规则的定义.

**定义 2.** 撤销消息规则. 当一个路由器  $n$  允许

① 为了有效消除误报,在我们的模拟中我们取  $\tau$  为 30s.

发送一个有效的路由撤销消息  $Withdraw(f_1)$ , 当且仅当满足下面的条件:

$$Withdraw(m, f_1) \wedge Time(n, f_2) -$$

$$Time(m, f_1) < \tau \wedge \forall m \in Peers(n) \wedge f_2 \supseteq f_1.$$

BGP 的可信服务中所执行申明消息规则和撤销消息规则确保了 GesBGP 中所有路由消息的可靠性, 而 TPM 最终确保了可信服务的正确执行. 当路由器成功验证收到的路由申明, 这个过程说明了发送该路由申明的路由器已实施了安全规则并且已成功验证了申明的合法性. 因此, 路由器可以采纳该路由申明. 通过在不同 AS 的路由器执行安全规则以及路由申明的签名和验证过程, 不同 AS 之间建立了基于 IP 前缀的可传递的强路由信任关系. 由此可知, 改进的 GesBGP 可以有效防御任何位置的 AS/路由器由于管理员配置错误或者敌手攻击引起的伪造路由. 因此, 我们可以得到定理 1, 具体的定理证明在本文中省略.

**定理 1.** 在改进的 GesBGP 中, 基于强制的可信服务建立的邻居 AS/路由器之间的信任关系在确保 BGP 安全性的同时, 可以有效消除 BGP 通告消息的累积签名.

由于改进的 GesBGP 协议在仅在可信服务中增加了执行定义 1 和定义 2 中规则的策略检查从而减少了签名的次数以及签名的复杂度, 即在每个路由器上仅执行一次签名并获得一个签名消息(并不是聚集签名消息). 在入口 filter 上 GesBGP 不需要保存收到路由申明的签名, 在出口 filter 上 GesBGP 仅进行路由安全规则检测和一次路由签名. 因此, 这个算法并没有增加计算的复杂性, 具体流程和 4.3 节算法类似, 这里省略. 如图 6 所示, 各个 AS/路由器在发布路由通告时候仅产生一个签名消息, 例如前缀拥有者仅用前缀  $f_1$  的对应私钥对前缀消息进行签名, 而其他的 AS 对 AS\_PATH 进行签名. 由于 BGP 的安全规则在可信服务中的执行, 其他伪造的消息

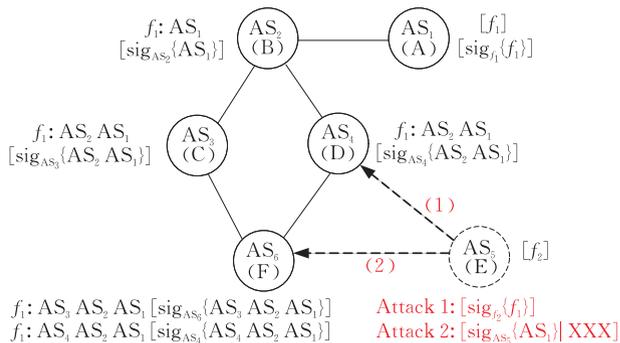


图 6 优化的 GesBGP 协议实例

无法在路由器被成功的发送出来, 例如, 图 6 中所示的攻击 1 和攻击 2 都无法将攻击的伪造路由发送到  $AS_4$  和  $AS_5$ . 所以, 通过在每个路由器执行强制的安全规则, 优化 GesBGP 可以提供和 SBGP 等同等级的安全性. 具体的安全性我们将在第 5 节中进行详细分析和评价.

## 5 安全性分析以及性能评价

在本节中, 我们首先分析和证明 GesBGP 是否可以实现 BGP 安全的目标以及 GesBGP 是否可以有效防御 BGP 攻击. 接着, 我们对 GesBGP 的性能进行了分析和评价.

### 5.1 安全性分析

本节我们将分析优化的 GesBGP 是否满足 4.1 节所提出的安全 BGP 的目标. 由于篇幅关系, 我们仅给出相应的命题和简化的证明过程.

**命题 1.** GesBGP 提供了 AS 号认证, 防止 AS 号伪造(目标 1).

证明. 在 GesBGP 中, 每一个 AS 号  $s$  都有对应的 IBS 私钥  $sQ_{ID}$ . 由于  $sQ_{ID}$  是由可信的私钥产生中心(PKG)产生, 任何不合法的 AS 路由器都无法获得 AS 号对应的  $sQ_{ID}$ . 任何路由器都可以用 AS 号  $s$  来验证  $sQ_{ID}$  签名消息的有效性. 也就是说, 通过 PKG 所提供的  $(s, sQ_{ID})$  绑定可以验证 AS 号的真实性.

**命题 2.** GesBGP 提供了 BGP 通告者认证(目标 2).

证明. 对于一个合法的 BGP 通告路由器来说, GesBGP 确保只有  $AS_s$  中的路由器才能拥有合法的  $AS_s$  和前缀  $f_1$  所对应的私钥  $sQ_{ID1}$  和  $sQ_{ID2}$ . 所以, 无论是前缀源或者是 AS 的路径通告都是基于  $(s, sQ_{ID1})$  或者  $(f_1, sQ_{ID2})$  的绑定来验证  $AS_s$  中路由器通告者的身份.

**命题 3.** GesBGP 提供了 AS\_Path 的认证(目标 3).

证明. 假设  $m_k = (f_1, [AS_1, AS_2, \dots, AS_n])$  是一条 BGP 路由, 并且  $AS_1$  是  $f_1$  的通告源. 为了方便证明, 我们假设在一个 AS 中仅有一个 BGP 通告者, 并且这个 BGP 通告者代表了 this AS 的行为. 在 GesBGP 中,  $m_k$  的完整性意味着  $m_k$  已经穿越了  $AS_1, AS_2, \dots, AS_n$ . 当 AS\_PATH 仅为 1, 即  $n=1$  时, GesBGP 提供了基于前缀源的认证, 确保第一跳 AS 的可信性. 当  $n=2$  时, 在每个 GesBGP 路由器

中的出口 filter 验证  $AS_2$  和  $AS_3$  之间路径  $(f_1, [AS_1])$  和  $(f_1, [AS_1, AS_2])$  的关联关系, 确保路由  $(f_1, [AS_1, AS_2])$  是路由  $(f_1, [AS_1])$  的可信的延续, 即存在有效前缀  $f_1$  源  $AS_1$  到  $AS_2$  的信任链. 因此, 当  $AS_3$  收到路由  $(f_1, [AS_1, AS_2])$  后,  $AS_3$  仅需要验证  $(f_1, [AS_1, AS_2])$  中  $AS\_PATH$  的签名消息即可验证通告消息的前缀以及路径的有效性. 依次类推, 基于出口 Filter 上的可信服务服务建立的基于前缀  $f_1$  的邻居强制信任关系,  $AS\_PATH([AS_1, AS_2, \dots, AS_n])$  的认证可以通过直接验证邻居  $AS$ /路由器的真实性而获得.

**命题 4.** GesBGP 提供了前缀源认证(目标 4).

证明. 在 GesBGP 中, 前缀  $f_1$  和私钥的绑定  $(f_1, s_{Q_{11}})$  确保了源认证的真实性. BGP 验证服务支持前缀的聚集, 确保所有  $AS$  所通告的前缀都有可信的认证源.

通过以上 4 个命题, 我们可以得到定理 2.

**定理 2**(GesBGP 的安全属性). GesBGP 满足以下 4 个安全目标:  $AS$  号认证(目标 1)、BGP 通告者认证(目标 2)、 $AS\_PATH$  的认证(目标 3)和前缀源认证(目标 4).

## 5.2 性能评价

第 4.3 节介绍的基本 GesBGP 协议的时间和空间复杂度都比较高, 而我们优化的 GesBGP 协议在提供同等安全性的基础上改进了性能, 所以我们将评价 GesBGP 在增加了通信开销以及处理开销的情况下对 BGP 性能的影响. 类似于其他 BGP 评价和模拟方法, 我们同样采用网路模拟器 SSFNet. SSFNet 是一个离散事件驱动的模拟器, 并且提供了一个基本的 BGP 操作模型. 在模拟中, 我们采用了 3 种规模的网络拓扑: 10 个自治系统的 Net10、29 个自治系统的 Net29 和 110 个自治系统的 Net110, 其中后面两种网络拓扑都是基于互联网路由表生成. 在 3 种拓扑中, 每个自治系统都只由一个边界路由器构成.

GesBGP 协议需要额外消耗的路由器资源执行 IBS 的签名和验证的 CPU 资源, 在我们的实验中我们模拟了 512 位的 IBS 签名验证算法. 如图 7 所示, 基本的 GesBGP 协议引入了大量签名和验证的开销, 从而导致在 Net10、Net29 和 Net110 中收敛时间分别增加了 148%、186% 和 174%. 由于 GesBGP 消除了 SBGP 的多重累积签名, 获得了优于 SBGP 方案的收敛性能. 以 Net110 为例, SBGP 引入的收敛延迟为 230%<sup>[10]</sup>, GesBGP 仅引入了 186% 的收敛

延迟. 我们所提出的优化 GesBGP 减少了更新消息的累积签名和签名的计算复杂度, 获得进一步优化的收敛性能. 在 3 种拓扑中, 优化 GesBGP 的收敛性能分别提高了 124%、129% 和 119%, 收敛时间仅比原始 BGP 增加了 11%、25% 和 25%. 和 SBGP 的收敛性能相比, GesBGP 获得了超过 120% 的性能改进. 由此可见, 优化的 GesBGP 在确保 BGP 安全性的情况下可以获得了接近原始 BGP 的收敛性能.

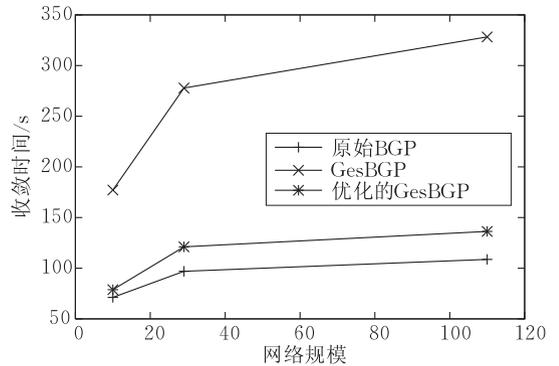


图 7 BGP 的收敛性能

## 6 结 论

本文提出了 GesBGP 协议以解决目前 BGP 的众多安全性问题, 例如前缀劫持和  $AS$  路径篡改. 在 GesBGP 协议中, 我们引入了基于身份的签名算法, 消除了传统公钥算法中的 PKI 部署以及证书分发和存储的问题. 同时, 我们使用可信计算解决了私钥的安全储存和路由器系统的完整性问题, 并且消除了路由申明的多重累积签名. 此外, 我们进一步优化了 GesBGP 的性能, 提出了基于可信计算技术建立路由器之间的强安全信任模型的方法, 即利用可信安全服务实施 BGP 的安全规则, 在确保 BGP 安全性的同时也优化了 GesBGP 的性能. 从我们的安全性分析和性能评价可以看出, GesBGP 在实现了 BGP 安全性的目标的同时也获得了较好的性能.

## 参 考 文 献

- [1] Kent S, Lynn C, Seo K. Secure border gateway protocol. IEEE JSAC, 2000, 18(4): 582-592
- [2] White R. Securing BGP through secure origin BGP. The Internet Protocol Journal, 2003, 6(3): 15-22
- [3] van Oorschot P C, Wan T, Kranakis E. On Inter-domain routing security and pretty secure BGP (psBGP). ACM TISSEC, 2007, 10(3): 1-41
- [4] Aiello W, Ioannidis J, McDaniel P. Origin authentication in

interdomain routing//Proceedings of the 10th ACM Conference Computer and Communications Security. Washington D. C. , USA, 2003: 165-178

- [5] Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing//Proceedings of the ISOC NDSS 2003. San Diego, California, USA, 2003
- [6] Subramanian L, Roth V, Stoica I, Shenker S, Katz R H. Listen and whisper: Security mechanisms for BGP//Proceedings of the 1st Symposium Networked System Design and Implementation. San Francisco, California, USA, 2004

- [7] Karlin J, Forrest S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes//Proceedings of the IEEE International Conference on Network Protocols. Santa Barbara, California, USA, 2006: 290-299
- [8] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the Crypto. Santa Barbara, California, USA, 2004: 47-53
- [9] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, 2006
- [10] Zhao M, Smith S, Nicol D. The performance impact of BGP security. IEEE Network, 2005, 19(6): 42-48



**LI Qi**, born in 1979, Ph. D. candidate. His research interests include network architecture and protocols, system and network security.

**WU Jian-Ping**, born in 1953, Ph. D. , professor, Ph. D. supervisor. His current research interests include computer network architecture, next generation Internet, and protocol testing and formal methods.

**XU Ming-Wei**, born in 1971, Ph. D. , professor, Ph. D.

supervisor. His research interests include computer network architecture, high-speed router architecture and Internet routing.

**XU Ke**, born in 1974, Ph. D. , associate professor, Ph. D. supervisor. His research interests include next generation Internet, switch and router architecture, P2P and overlay network.

**ZHANG Xin-Wen**, born in 1974, Ph. D. . His research interests include computer and system security models, security in distributed and mobile computing system, trusted computing and high assurance systems.

## Background

This critical Internet infrastructure has significant security vulnerabilities that are well studied but have been unresolved for many years. Prefix hijack and AS path spoofing attacks on BGP directly influence availability of Internet routing. Although several improved BGP security proposals have been proposed to mitigate or partly solve the problem, these proposals are unable to deploy in real networks because of their complexity or security weaknesses. In this paper, the authors propose a trusted routing attestation service which is used to verify and validate routes with the help of the identity-based signature (IBS) algorithm. IBS eliminates central PKI deployment and certificate distribution. Furthermore, optimized GesBGP fully utilizes the internal features of BGP

route selection with the help of trusted computing to improve GesBGP performance. The security analysis and performance study show that optimized GesBGP greatly improves the secure BGP performance without sacrificing BGP security. The GesBGP proposals and the built trust model cast light on design and development of secure Inter-domain routing in next generation Internet.

This research is supported in part by the National Natural Science Foundation (NSFC) of China under grant No. 90604024, the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z2A2, the Key Project of Chinese Ministry of Education under grant No. 106012.