标准模型下可证明安全的BGP路由属性保护机制

李道丰[1),3)] 王高才[1),3)] 王志伟[2)] 钟 诚[1),3)] 李陶深[1),3)]

[1)](广西大学计算机与电子信息学院 南宁 530004)

[2)](南京邮电大学计算机学院 南京 210003)

[3)](广西高校并行分布式计算技术重点实验室 南宁 530004)

摘 要 BGP路由协议是目前大多数网络基础设施所采用的重要协议之一.随着网络攻击技术的发展,如何构造安全且容易部署的BGP协议保护机制,仍然是安全路由协议研究中的热点问题.文中提出标准模型下可证明安全的BGP协议的路由属性保护机制——Identity-based Sanitizable Signature Path Verification(简称IDSPV).IDSPV机制采用基于身份的密码学思想以及可净化签名方案的优点.并结合BGP路由协议特征,在无需证书的条件下,仅需将自己的更新报文签名后再添加到AS_PATH路径中,为BGP路由属性完整性和真实性提供保护.避免证书存储和管理开销.另外,文中给出保护AS_PATH路由属性的安全模型,利用规约技术,在标准模型下给出IDSPV机制的安全证明.通过安全性和性能方面的分析可知,与现有方案相比,IDSPV机制更易于在实际网络中部署.

关键词 标准模型;边界网关协议;可证明安全;路由属性保护;可净化签名

中图法分类号 TP393 **DOI号** 10.3724/SP.J.1016.2015.00859

Provable Secure Mechanism for BGP Path Protection in the Standard Model

LI Dao-Feng[1),3)] WANG Gao-Cai[1),3)] WANG Zhi-Wei[2)] ZHONG Cheng[1),3)] LI Tao-Shen[1),2)]

[1)](*School of Computer and Electronics Information, Guangxi University, Nanning* 530004)

[2)](*School of Computer, Nanjing University of Posts and Telecommunications, Nanjing* 210003)

[3)](*Guangxi Colleges and University Key Laboratory of Parallel and Distributed Computing Technology, Nanning* 530004)

Abstract In current, the BGP is one of the important routing protocols that are adopted by most network infrastructures. With the development of network attack technology, how to construct a protected mechanism which is secure and easy to be deployed for BGP is still a hot topic in the research of secure routing protocols. In this paper, based on identity-based cryptography and sanitizable signature scheme, a provable secure path attributes protection mechanism — Identity-based Sanitizable Signature Path Verification (IDSPV) for the BGP in the standard model is proposed. Combines with the features of the BGP, the IDSPV only needs to update messages and add the updated messages to AS_PATH without certification. The protection in the integrity and authenticity for the BGP attribute is proved in the IDSPV. Furthermore the storage space and management overhead for the certification is avoided. In addition, the security model for the AS_PATH attribute is presented and the security proof for the IDSPV mechanism is given by using the reduction method in the standard model. The analysis and experiment results show that the proposed IDSPV mechanism is more feasible and effective than the existing schemes mentioned in the analysis of security and performance.

收稿日期:2014-02-16;最终修改稿收到日期:2014-10-31.本课题得到国家自然科学基金(61262003,61373006,61362010)、广西自然科学基金项目(2011GXNSFA018152)、广西教育厅基金(YB2014008,2013YB007)、广西大学自然科学基金(XBZ110905)资助.**李道丰**,男,1974年生,博士,副教授,主要研究方向为密码学与信息安全.E-mail:ldf_0123@163.com.**王高才**,男,1976年生,博士,教授,博士生导师,主要研究领域为系统性能评价、计算机网络技术等.**王志伟**,男,1976年生,博士,副教授,主要研究方向为密码学与信息安全.**钟 诚**,男,1964年生,博士,教授,博士生导师,主要研究领域为并行计算、生物计算、可信计算等.**李陶深**,男,1957年生,博士,教授,博士生导师,主要研究领域为网络计算和信息安全等.

Keywords standard model; border gateway protocol (BGP); provable secure; path attribute protection; sanitizable signature

1 引 言

BGP 路由协议①是当前唯一使用的域间路由协议,而构建安全的 BGP 协议一直是近十多年以来互联网研究的热点问题. 随着互联网技术的发展和网络攻击技术的提高,BGP 协议的安全问题日益凸出,严重影响着网络的正常运营[1],阻碍到互联网的进一步发展. 目前 BGP 路由协议所存在的安全问题是源地址真实性问题和更新报文 AS_PATH 路由属性的安全问题[2]. 源地址真实性问题是指路由信息发起者 AS(Autonomous System,AS)是否真正拥有所声称的 IP 地址前缀;AS_PATH 路由属性安全问题则是 AS 所更新的报文 AS_PATH 是否具有完整性和真实性,亦即是否被篡改. 具体而言,所有参与路由的 AS 是否诚实地传播 AS_PATH 并正确地添加相应的路由信息到 AS_PATH 中. 这两个安全问题将引起非法的路由攻击. 前缀劫持就是由于上述安全问题而导致的破坏性巨大的一种攻击方式,而且 BGP 路由器能够自主地宣告任意错误/恶意路由信息,同时这些路由信息不加任何检测措施就传播到整个互联网,造成全球网络不稳定,甚至瘫痪. 因此,在可信可控可管的网络基础设施课题研究中,BGP 路由协议的安全问题仍然是不可回避的研究课题[3-4].

BGP 路由协议的安全问题主要包括 BGP 会话安全、前缀源地址认证和 AS_PATH 路由属性信息的真实性和完整性认证等问题. AS_PATH 路由属性是 BGP 最重要的属性之一,其主要任务是按顺序记录一条 BGP 路由从源 AS 到目的 AS 所经过的路径,且可以用于避免环路,提供选路标准. 若 AS_PATH 路由属性信息未得到安全保护,将会遭到篡改攻击而引起路由欺骗、窃取秘密信息和流量以及路由黑洞等危及网络空间安全的严重安全事件. 因此,AS_PATH 路由属性的保护是 BGP 安全研究中首先需要解决的关键问题之一.

在 AS_PATH 路由属性信息保护的研究过程中,首先要认识到在 BGP 上部署任何安全机制都会对其工作性能造成影响这个事实. 因此,所研究的 AS_PATH 路由属性信息保护机制需满足容易部署且能提供安全保护的功能. 所谓容易部署是指要求所部署的安全机制能尽量减少对 BGP 工作性能的影响,如能考虑到存储和资源开销、路由收敛时间影响以及可扩展性等;安全保护要求所部署的安全机制确实能保护 AS_PATH 路由属性信息的完整性和真实性. 针对 BGP 存在更新报文 AS_PATH 路由属性的安全问题的研究,目前已有很多研究成果,大致可分为基于密码学技术的保护机制[5-10]、非基于密码学技术的保护机制[11-16]以及这两种机制的整合机制[17]. 尽管这些方案具有很高的理论研究价值和实际意义,但在现有的众多方案中,容易部署的安全方案未能很好的解决 BGP 路由安全问题;安全强度高的方案又因计算能力和存储资源等问题而难以部署于互联网中. 如路由检测方案[11],虽然引入了异常检测机制,但检测结果本身存在一定的不确定性,因而很难得到更准确的安全保证;而 S-BGP 协议[5]利用基于证书和数字签名机制给出了 AS_PATH 路由属性的保护方案,提供了很好的完整性和真实性保护功能,但其所用的部分密码组件运算较为复杂,且增加证书管理负担和存储开销. 另外,现有的方案均未给出在标准模型或随机预言机模型下的安全证明. 因此,研究既易于部署又能提供很好安全保护的可证明安全的 BGP 协议 AS_PATH 路由属性安全机制具有重要的理论价值和实际意义,这也是路由协议安全方面的一个研究方向.

密码学理论具有保护信息完整性和真实性的良好属性. 同时,根据不同的应用场合和需求,利用密码学理论可以构造出满足不同应用需求的轻量型的密码方案[8,18-19]. 由于目前用于保护 BGP 协议安全的公钥密码保护方案大都是基于 PKI 证书的设计方案(如 S-BGP 等),PKI 体系是集中式的架构,但 BGP 是分布式的工作架构,若采用基于证书的方案,不仅需要承担证书存储开销,而且使得 BGP 的部署难以扩展. 为此,我们采用基于身份的思想,能够避免证书的使用,从而能使我们的设计方案无需承担证书存储开销. 同时,可净化签名方案的优点是具有允许签名的文档可以指定被授权者不需与消息签名者进行交互即可修改文档指定的部分,且修改后的文档的签名仍然有效的属性. 因此,在 BGP 协议中,我们采用可净化签名方案,在更新报文过程中,路由属性更新者(AS)不需要与路由前缀拥有者

① Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, 2006. https://tools.ietf.org/html/rfc4271

以及上一跳的路由属性更新者进行交互，就可以生成更新部分的有效路由属性证明，并直接添加到原来的路由属性证明中，无需重新对整个 AS_PATH 路由属性进行签名. 因此，本文采用基于身份的可净化签名，在标准模型下提出了一种可证明安全的保护 BGP AS_PATH 路由属性的安全机制——IDSPV 机制（Identity-based Sanitizable Signature Path Verification）. IDSPV 机制利用 AS 的身份作为 AS 的公开密钥，运用可净化签名的特点，允许被授权的 AS 在更新 AS_PATH 报文时，仅需对自己更新的部分进行签名，生成 AS_PATH 路由属性证明，同时能确保更新后的 AS_PATH 路由属性证明仍然有效. 另外，我们在标准模型下给出了 IDSPV 机制的安全证明. IDSPV 机制的优点有：(1) IDSPV 机制无需证书部署，从而避免证书存储和管理开销；(2) 在更新报文时，IDSPV 机制无需重新对整个 AS_PATH 路由属性进行签名；(3) IDSPV 机制是一种标准模型下可证明安全的机制. 目前已有的 BGP 路由保护安全机制和方案均不是标准模型下可证明安全的机制和方案.

基于上述的优点，在低端设备的存储能力和计算能力不断提高的背景下，与现有的 BGP 保护机制和方案相比，IDSPV 机制更具有重要的理论意义和应用价值.

本文第 2 节讨论 BGP 协议安全保护机制的相关研究工作；第 3 节介绍基于身份的可净化签名模型，提出一种采用基于身份的可净化签名机制保护 BGP 协议 AS_PATH 路由属性安全的机制；在第 4 节中给出机制的安全证明；第 5 节中给出机制的效率分析；最后在第 6 节中总结全文并给出进一步的工作展望.

2　相关研究工作

目前，面向 BGP 协议在更新报文 AS_PATH 路由属性方面容易部署且安全强度高的保护机制的研究工作仍在不断的探索之中，尚未出现成熟且系统化的方案，已有相关领域的研究工作概括如下：

自从 BGP 协议提出以后，其安全问题得到了广泛地关注. 首先，Kent 等人在 2000 年提出 S-BGP 协议[5]，其思想是采用 PKI 技术来确保网络地址前缀和 AS_PATH 路由属性的真实性和完整性，通过 4 种“证书”来解决路由信息的安全保护，但未能给出安全证明，而且路由资源开销较大. 随后，各种基于证书和密码技术的保护方案相继提出. Kranankis 等人[6]在 S-BGP 优点的基础上提出了 psBGP，它主要利用集中式的信任模型来认证 AS 号码，并利用分布式的信任模型来验证 IP 地址前缀的所有权. 在网络地址前缀信任方面，通过邻居 AS 的信誉评价程度来刻画，但是由于网络规模很大，若采用证书机制来确保信任，将严重影响路由协议的正常运行，同时证书的管理也是一个很刺手的问题，难于部署. 胡湘江等提出的 SE-BGP[20]，结合 PKI 认证中心，建立“安全 AS 联盟（Secure AS Alliance）”，以 AS 联盟为单位建立 PKI 认证中心，设计一种新的 BGP 安全协议机制，该机制采用基于 AS 联盟的安全体系架构. 并提出一种分布式的转换者信任模型（Translator Trust Model，TTM），只需局部信息就可进行全局认证，在很大程度上简化了证书的管理. 王娜等人[7]提出的基于身份的域间路由协议安全机制，进一步简化证书使用和管理工作. 赵宸等人[8]提出的一种轻量化的边界网关协议路径验证机制 FTAPV（First-Two-AS based Path Verification），主要借助人类社会中排直线队列的思想，通过验证 AS_PATH 中前两个 AS 的签名信息的有效性来确认路径信息的真实性. Raimagia 等人[9]提出了采用对称密码学技术对 BGP 路由信息进行加密以确保 BGP 路由信息的安全，其核心思想是在对等 BGP 实体建立连接时，采用一种循环移位算法来产生加密密钥，并用 SHA-1 算法对密钥求 Hash 值，再将密钥的 Hash 值通过 open 消息发给邻居对等 BGP 实体. 其邻居对等 BGP 实体收到密钥 Hash 值后，也利用相同的循环移位算法产生密钥并生成新的密钥 Hash 值，再与接收到的密钥 Hash 值进行比较，若匹配则建立安全连接，否则中断. 该方案能减少签名操作次数和密钥存储需求，但经常出现未能成功连接的情况. 最近 Boldyreva 等人[10]借鉴密码学中可证明安全理论和方法，提出了路径向量路由协议的安全模型，通过规约的方法给出 S-BGP 的安全证明，指出 S-BGP 未能完全满足其所提出的安全模型中定义的三个安全目标，并对 S-BGP 进行改进，是开展 BGP 协议安全机制研究的关键和突破点.

3　IDSPV 的 BGP 协议路径属性保护机制

3.1　预备知识

设阶均为 q 的加法群 G_1 和乘法群 G_2，g 为 G_1 的生成元，存在映射 $e: G_1 \times G_1 \rightarrow G_2$，具有以下性质：

(1) 双线性. 对于 $\forall a, b \in Z_q$，$P, Q \in G_1$，有

$e(P^a,Q^b)=e(P,Q)^{ab}$；

(2)非退化性. 存在$P,Q\in G_1$，使得$e(P,Q)\neq 1$；

(3)可计算性. $\forall P,Q\in G_1$，存在计算$e(P,Q)$的有效算法.

定义 1. 计算 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题：已知有限的加法群G_1，给定元素$g,g^a,g^b\in G_1$，其中$a,b\in\mathbb{Z}_q^*$，且a,b未知，求g^{ab}.

定义 2. (ε,t)-CDH 假定. 若不存在任何概率多项式算法能在时间t内，以至少概率为ε解决群G_1上的 CDH 问题，则称群G_1上的(ε,t)-CDH 假定成立.

可知，在 Diffie-Hellman 的假设下，CDH 问题是一个非常困难的问题[21].

3.2 基于身份的可净化签名模型

基于身份的可净化签名方案[19](IDSSA)具有对披露文档进行认证的功能，主要由 4 个参与者参与操作：私钥生成器(PKG)、签名者(signer)、可净化者(sanitizer)和验证者(verifier). 一个 IDSSA 方案主要由 5 个步骤组成：系统参数建立(Setup)、密钥抽取(Extract)、签名(Sign)、净化签名(Sanitize)和验证(Verify).

设$ID=(ID_1,ID_2,\cdots,ID_n)\in\{0,1\}^\lambda$，$M=(M_1,M_2,\cdots,M_n)\in\{0,1\}^\lambda$，给出算法定义如下：

(1)系统参数建立(Setup). 给定一个安全参数k，私钥生成器(PKG)生成系统参数$params$和主密钥msk，其中$params$公开，msk保密.

(2)密钥抽取(Extract). 给定一个身份ID，PKG 利用主密钥msk计算ID的私有密钥d_{ID}，并将d_{ID}通过安全信道秘密发送给用户ID.

(3)签名运算(Sign). 给定系统参数$params$，签名者身份ID，消息M以及签名者的私钥d_{ID}，签名者输出签名σ以及秘密信息ψ.

(4)净化运算(Sanitize). 给定系统参数$params$，签名者身份ID，秘密信息ψ以及消息M的签名σ. 净化者输出新的消息M'及其签名σ'.

(5)验证运算(Verify). 给定系统参数$params$，签名者身份ID_i，以及消息/签名(M_i',σ_i')和(M_i,σ_i)，利用签名验证算法进行验证，输出有效“True”或无效“False”.

3.3 安全模型

针对目前 AS_PATH 路由属性已有的攻击方式，我们给出安全模型. 在所给的安全模型中，假定攻击者拥有很强的攻击条件和能力，既能知道网络N的拓扑，同时能根据自己的攻击需要来腐化除了攻击对象之外的任意 AS. 而且攻击者能代表已被腐化的 AS 执行任意攻击行为，可以修改路由宣告中的 AS_PATH 路径属性，例如在 AS_PATH 路由属性中增减 AS. 在攻击过程中，假定挑战者 C 和攻击者 A 之间进行如下的交互游戏：

(1)参数建立. 给定一个安全参数k，挑战者 C 利用私钥生成器(PKG)生成系统参数$params$和主密钥msk. 并将$params$发送给攻击者 A，msk保密.

(2)请求. 攻击者 A 进行有界多项式次数的请求，而且每次请求都是有记忆、自适应的. 具体如下：

①密钥抽取请求. 攻击者 A 指定一个身份为ID的 AS，挑战者 C 运行密钥抽取算法得到身份为ID的 AS 的私钥d_{ID}，并将d_{ID}发送给攻击者 A；

②签名请求. 攻击者 A 指定一个身份为ID的 AS 以及路由属性消息M以及签名者的私钥d_{ID}，挑战者 C 运行密钥抽取算法和签名算法得到(ID,M)的签名σ并发给攻击者 A.

(3)伪造. 攻击者 A 能成功宣告关于一个身份为ID'的 AS′对自己更新的路由信息 AS_PATH 路由属性$(IP_1,AS_1,AS_2,\cdots,AS_i,AS')$及其签名$\sigma'$，使得

①攻击者 A 未进行过关于身份为ID'的 AS′私钥抽取请求；

②攻击者 A 未对 AS_PATH 路由属性$(IP_1,AS_1,AS_2,\cdots,AS_i,AS')$进行过签名请求；

③攻击者 A 所宣告的 AS_PATH 路由属性$(IP_1,AS_1,AS_2,\cdots,AS_i,AS')$及其签名$\sigma'$有效，即使得未腐化的 AS 接收到该路由属性时认为是有效的路径.

若攻击者 A 成功伪造有效的 AS_PATH 路由属性证明，则其可以解决 CDH 问题的实例.

3.4 IDSPV 保护机制

3.4.1 IDSPV 机制原理

本文提出的 IDSPV 机制和 S-BGP 的目标一样，主要用于保护 AS_PATH 路由属性的完整性和真实性以及前缀地址的真实性. 我们利用上面提到的基于身份的可净化签名方案模型，提出了一种简称为 IDSPV 的 BGP 路由协议 AS_PATH 路由属性保护机制. IDSPV 机制的工作流程如下：

(1)系统初始化. 包括系统参数建立和每个 AS 及其相应的 BGP 路由器密钥的生成阶段.

(2)路由更新. 更新过程包括添加路由、路由属性证明生成、路由属性证明验证 3 个主要操作，具体操作流程如图 1 所示. 在路由更新过程中，主要分如下两种情况来实现：

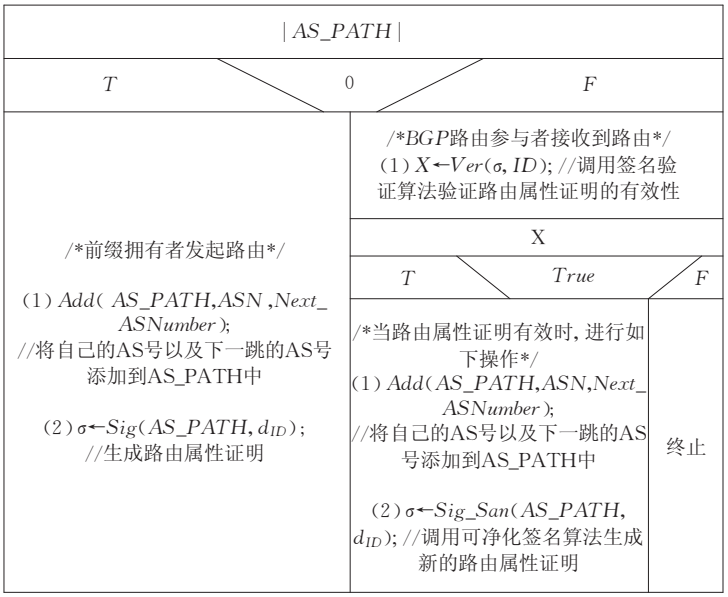

图 1　IDSPV 机制工作流程

当$|AS_PATH|=0$时，意味着由拥有 IP 地址前缀的 AS 发起路由宣告. 首先将自己的 AS 号(AS Number，ASN)以及下一跳的 AS 号添加到 AS_PATH 中；其次利用自己的私钥 d_{ID} 对 AS_PATH 路由信息进行签名，生成路由属性证明. 并将生成的 AS_PATH 路由信息和路由属性证明传递给下一跳信任的邻居 AS.

当$|AS_PATH|\geq 1$时，表明 AS 收到上一跳 AS 发来的 AS_PATH 路由信息. 在收到路由消息后，AS 首先利用上一跳 AS 的公钥来验证路由属性证明的真实性和有效性；其次，添加下一跳的 AS 号到 AS_PATH 中；最后，利用可净化签名算法对更新后的 AS_PATH 路由信息进行签名，生成新的路由属性证明. 再将新的 AS_PATH 路由信息及其路由属性证明发送给下一跳信任的邻居 AS.

图 1 中$|AS_PATH|$表示 AS_PATH 的长度. 所涉及的函数描述如下：

(1) $Add(AS\_PATH, ASN, Next\_ASNumber)$. 表示某个 AS 将自己的 AS 号 ASN 以及它所信任的下一跳 AS 号 $Next\_ASNumber$ 添加到 AS_PATH 中.

(2) $Sig(AS\_PATH, d_{ID})$. 表示某个 AS 利用自己的私钥 d_{ID} 对要宣告的 AS_PATH 进行签名生成路由属性证明.

(3) $Sig\_San(AS\_PATH, d_{ID})$. 表示某个 AS 利用自己的私钥 d_{ID} 对更新后的 AS_PATH 进行可净化签名生成新的路由属性证明.

(4) $Ver(\sigma, ID)$. 表示某个 AS 利用公钥 ID 对路由属性证明 σ 的真实性和有效性进行验证.

3.4.2　IDSPV 机制实现

在本节中主要给出 IDSPV 机制中每个操作的具体实现方法.

(1) 系统初始化

在系统初始化阶段中，主要建立 IDSPV 机制的系统，包括系统参数建立和系统中每个 AS 及其相应的 BGP 路由器密钥生成.

(1) 系统参数建立. 给定安全参数 k，PKG 选取阶为 q 的两个群 G_1 和 G_2，一个生成元 g 以及可允许的双线性配对 $e: G_1\times G_1\rightarrow G_2$. 而后随机选取整数 $\alpha\in\mathbb{Z}_q^*$，计算 $g_1=g^\alpha$ 并选取 $g_2\in G_1$. PKG 选择两个元素 $u', m'\in G_1$ 以及两个含有 n 个元素的向量 $\boldsymbol{U}=(u_i)$，$\boldsymbol{V}=(v_i)$，其中向量的元素均随机取自于群 G_1. 从而得到系统参数为

$$params=(G_1, G_2, e, q, g, g_1, g_2, u', m', \boldsymbol{U}, \boldsymbol{V}),$$

以及系统主密钥为 g_2^α.

(2) BGP 路由器密钥生成. 每个路由器将自己的身份信息 $ID_i=Hash(IP_{R(i)}\,\|\,AS_i\,\|\,t_i)$ 做为自己的公钥，将 ID_i 表示为 $ID_i=\{ID_i^1, ID_i^2, \cdots, ID_i^n\}$，并发给 PKG，其中 $IP_{R(i)}$ 为 AS_i 中第 i 个边界路由器的 IP 地址或 MAC 地址，AS_i 为第 i 个边界路由器所属的第 i 个 AS 域；t_i 为 BGP 路由器公钥的有效期. 其私钥 d_{ID_i} 生成如下：PKG 随机选取一个整数 r_{ID_i}，并按式(1)计算：

$$d_{ID_i}=(d_{ID_i}^{(1)}, d_{ID_i}^{(2)})=\left(g_2^\alpha\left(u'\prod_{j=1}^{n}u_j^{ID_i^j}\right)^{r_{ID_i}}, g^{r_{ID_i}}\right) \quad (1)$$

其中 $j=1, 2, \cdots, n$. 此步中包括宣告前缀消息签名

AS 的公钥、宣告前缀消息签名 AS 的私钥、更新 AS_PATH 的 AS 公钥以及更新 AS_PATH 的 AS 私钥的生成. 限于篇幅,我们这里不做详细地说明.

(2)路由更新

在路由更新阶段中,主要给出路由属性证明生成、路由属性证明验证的 3 个操作:$Sig(AS\_PATH, d_{ID})$、$Sig\_San(AS\_PATH, d_{ID})$、$Ver(\sigma, ID)$ 的实现.

① 源路由宣告的属性证明生成 $Sig(AS\_PATH, d_{ID})$ 函数实现,即生成路由属性证明(AS_PATH 路径签名,文后涉及到的签名均指路由属性证明). 假定源路由宣告(前缀)的发起者为 AS_1,其发布路由通告信息 $NLRI(IP_1)$,并通过其路由器将该信息发送给其信任的邻居 AS,这样的 AS 可能有很多个. 为了方便描述,我们仅讨论一个 AS 的情形,同时不对 AS 和它下面负责宣告路由信息的 BGP 路由器作区分,也可将负责宣告路由的 BGP 路由器看作其所在的 AS. 设邻居 AS 为 AS_2,并生成 AS_PATH 路径属性(IP_1, AS_1, AS_2),同时计算:$H_1 = Hash(d_{ID_1} \| IP_1 \| AS_1 \| ID_1)$;$h_1 = Hash(H_1 \| AS_2 \| ID_2)$,并将 h_1 分成 n 份,表示为$h_1 = \{h_1^1, h_1^2, \cdots, h_1^n\}$,其中$Hash(\ )$ 为 Hash 函数.

AS_1 随机选取一个整数 $\bar{r}_{ID_1}, r'_{ID_1} \in \mathbb{Z}_q^*$,按式(2)计算 AS_PATH 路由属性证明:

$$\sigma_1 = d_{ID_1}^{(1)} \left(v' \prod_{i=1}^{n} v_i^{h_1^i}\right)^{r'_{ID_1}} = g_2^{\alpha} \left(u' \prod_{i=1}^{n} u_i^{ID_1^i}\right)^{\bar{r}_{ID_1}} \left(v' \prod_{i=1}^{n} v_i^{h_1^i}\right)^{r'_{ID_1}}$$
$$\sigma_2 = d_{ID_1}^{(2)} = g^{\bar{r}_{ID_1}},\ \sigma_3 = g^{r'_{ID_1}} \tag{2}$$

并可将 $NLRI(IP_1)$、AS_PATH 属性(IP_1, AS_1, AS_2)、路由属性证明 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ 以及 H_1 一起发给信任的邻居 AS_2.

② 更新路由的属性证明生成 $Sig\_San(AS\_PATH, d_{ID})$ 函数实现,即下一个 AS 进行的 AS_PATH 路由属性证明. 在实现过程中,我们采用可净化签名技术,将更新的路由信息部分直接添加到原来的路由属性证明 σ 中,生成新的路由属性证明,而且保持新的路由属性证明有效,同时起到聚合签名的作用. 以下给出具体实现过程.

当邻居 AS_i 接收 AS_{i-1} 发来的信息$(\sigma_1, \sigma_2, \sigma_3)$以及 H_{i-1} 时,进行如下操作:

(i)首先根据 AS_PATH 信息以及自己的身份 ID_i 来验证路由路径证明$(\sigma_1, \sigma_2, \sigma_3)$的有效性,验证方法详见路由属性证明验证 $Ver(\sigma, ID)$ 函数的实现,若路由证明无效,则丢弃该路由信息. 否则进入下一步;

(ii)指定要更新的路由属性以及下一跳信任的 AS. AS_i 在自己的信任邻居列表中选取信任的 AS,记为 AS_{i+1},以及该域的身份 ID_{i+1},并计算:

$$H_i = Hash(d_{ID_i} \| AS_i \| ID_i),$$
$$h_i = Hash(H_i \| AS_{i+1} \| ID_{i+1});$$

并将 h_i 表示为 $h_i = \{h_i^1, h_i^2, \cdots, h_i^n\}$;

(iii)AS_i 更新自己要宣告的 AS_PATH 路由属性为$(IP_1, AS_1, AS_2, \cdots, AS_i, AS_{i+1})$,随机选取两个整数 $\bar{r}_{ID_i}, r'_{ID_i} \in \mathbb{Z}_q^*$,并按式(3)进行可净化签名运算:

$$\sigma_1 = \sigma_1 \left(u' \prod_{j=1}^{n} u_j^{ID_i^j}\right)^{\bar{r}_{ID_i}} \left(v' \prod_{j=1}^{n} v_j^{h_i^j}\right)^{r'_{ID_i}},$$
$$\sigma_2 = \sigma_2 g^{\bar{r}_{ID_i}},\ \sigma_3 = \sigma_3 g^{r'_{ID_i}} \tag{3}$$

将 $NLRI(IP_1)$、AS_PATH 属性$(IP_1, AS_1, AS_2, \cdots, AS_i, AS_{i+1})$、路由属性证明 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ 以及 H_i 一起发给下一个信任的邻居 AS_{i+1}.

如步骤(iii)中所示,AS_i 仅需将要宣告的 AS_PATH 路由属性中的更新部分的路由属性证明按式(3)添加至原来的路由属性证明中,无需重新对整个 AS_PATH 路由属性进行签名.

(3)路由属性证明验证 $Ver(\sigma, ID)$ 函数的实现. 当邻居 AS_i 接收 AS_{i-1} 发来的信息 $NLRI(IP_1)$、AS_PATH 路由属性$(IP_1, AS_1, AS_2, \cdots, AS_i)$、路由属性证明 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ 以及 H_{k-1} 时,进行如下计算:

① 对于每一个 AS_k,其中 $k \in \{1, 2, \cdots, i\}$,计算 Hash 值:$h_k = Hash(H_{k-1} \| AS_k \| ID_k)$,并将 h_k 表示为 $h_k = \{h_k^1, h_k^2, \cdots, h_k^n\}$;

② 对于 $k \in \{1, 2, \cdots, i\}$,判断式(4)是否成立:

$$e(\sigma_1, g) = e(g_1, g_2) \prod_{k=1}^{i} e\left(u' \prod_{j=1}^{n} u_j^{ID_k^j}, \sigma_2\right) \prod_{k=1}^{i} e\left(v' \prod_{j=1}^{n} v_j^{h_k^j}, \sigma_3\right) \tag{4}$$

若式(4)成立,意味着接收到的路由信息有效.

正确性分析:由式(4)的左边等式有

$$\begin{aligned} e(\sigma_1, g) &= e\Big(\sigma_1 \left(u' \prod_{j=1}^{n} u_j^{ID_2^j}\right)^{\bar{r}_{ID_2}} \left(v' \prod_{j=1}^{n} v_j^{h_2^j}\right)^{r'_{ID_2}} \cdots \\ &\quad \left(u' \prod_{j=1}^{n} u_j^{ID_i^j}\right)^{\bar{r}_{ID_i}} \left(v' \prod_{j=1}^{n} v_j^{h_i^j}\right)^{r'_{ID_i}}, g\Big) \\ &= e\Big(g_2^{\alpha} \left(u' \prod_{j=1}^{n} u_j^{ID_1^j}\right)^{\bar{r}_{ID_1}} \left(v' \prod_{j=1}^{n} v_j^{h_1^j}\right)^{r'_{ID_1}} \cdots \\ &\quad \left(u' \prod_{j=1}^{n} u_j^{ID_i^j}\right)^{\bar{r}_{ID_i}} \left(v' \prod_{j=1}^{n} v_j^{h_i^j}\right)^{r'_{ID_i}}, g\Big) \\ &= e\Big(g_2^{\alpha} \Big(\prod_{k=1}^{i} \left(u' \prod_{j=1}^{n} u_j^{ID_k^j}\right)^{\bar{r}_{ID_i}}\Big) \cdot \end{aligned}$$

$$\left(\prod_{k=1}^{i}\left(v'\prod_{j=1}^{n}v_j^{h_k^j}\right)^{r'_{ID_i}}\right),g\Big)$$

$$=e(g_2,g^a)e\left(\prod_{k=1}^{i}\left(u'\prod_{j=1}^{n}u_j^{ID_k^j}\right)^{r_{ID_i}},g\right)\cdot$$

$$e\left(\prod_{k=1}^{i}\left(v'\prod_{j=1}^{n}v_j^{h_k^j}\right)^{r'_{ID_i}},g\right)$$

$$=e(g_1,g_2)\prod_{k=1}^{i}e\left(\left(u'\prod_{j=1}^{n}u_j^{ID_k^j}\right)^{r_{ID_i}},g\right)\cdot$$

$$\prod_{k=1}^{i}e\left(\left(v'\prod_{j=1}^{n}v_j^{h_k^j}\right)^{r'_{ID_i}},g\right),$$

$\sigma_2=g^{\sum_{k=1}^{i}r_{ID_k}}$，$\sigma_3=g^{\sum_{k=1}^{i}r'_{ID_k}}$.

因此，只要 BGP 协议遵循上述保护机制，即可保证 AS_PATH 路由属性的完整性和真实性.

4　安全性分析

本节主要对 IDSPV 机制的安全性进行分析. 我们利用密码学中的规约技术和可证明安全的方法，给出 IDSPV 机制在标准模型下的安全证明.

定义 3.　假设网络 I 中的 AS 规模大小为 N，称攻击者 A 是一个具有(t,q_e,q_s,ε)能力的攻击者：在 IDSPV 机制中，A 可以进行 q_e次私钥抽取请求和 q_s次的签名请求，在运行时间为 t 内能以不可忽略的优势 ε 成功伪造有效的 AS_PATH 路由属性.

定义 4.　若 IDSPV 机制能抵御定义了的攻击，则称 IDSPV 机制为(t,q_e,q_s,ε)安全.

定理 1.　如果(ε',t')-CDH 假定成立，上述的 IDSPV 机制是(t,q_e,q_s,ε)安全.

证明.　假定 IDSPV 机制不是(t,q_e,q_s,ε)安全，则存在一个攻击者 A，A 进行 q_e次私钥抽取请求和 q_s次的签名请求，在运行时间为 t 内能以 ε 的优势根据 IDSPV 机制的步骤能成功伪造有效的 AS_PATH 路由属性. 在这样的假定下，给定群 G_1 和它的生成元 g，则存在一个求解算法 B 能在运行时间 t' 内以ε'的优势解决 CDH 问题的一个实例，即在收到 g^a、g^b后，能用算法 B 求解 g^{ab}，其中

$$t'=t+O(5q_e+(2N+4)q_s)t_{G_1},$$

$$\varepsilon'=\frac{\varepsilon}{16q_s(q_e+q_s)(N+1)^2},$$

其中 t_{G_1} 为群 G_1 中指数运算所花的总时间.

对于给定运行 IDSPV 机制的网络 I，而且网络 I 中的 AS 域的个数$|AS|=N>2$，在攻击过程中，算法 B 充当挑战者的角色与攻击者 A 进行交互，两者掌握共同的资源，在攻击者 A 能攻击 IDSPV 机制成功伪造合法的 AS_PATH 路由属性时，算法 B 也能成功求解攻击场景中涉及到的具体 CDH 问题的一个实例. 具体攻击步骤如下：

首先，算法 B 构造用于求解 CDH 问题实例的部分数据和系统参数. 随机选取以下整数和参数：

整数 r_u和 r_m，其中要求 $0<r_u<q$，$0<r_m<q$；

整数 s_u和 s_m，其中要求

$0<s_u<n$，$0<s_m<n(r_u(n+1)<q$，$r_m(n+1)<q)$；

令 $r_u=2(q_e+q_s)$，$r_m=2q_s$.

整数 $x'\in\mathbb{Z}_{r_u}$，$y'\in\mathbb{Z}_{r_m}$，$z'\in\mathbb{Z}_q$，$w'\in\mathbb{Z}_q$；

n 维向量$(x_1,x_2,\cdots,x_n)$，其中 $x_i\in\mathbb{Z}_{r_u}$；

n 维向量$(y_1,y_2,\cdots,y_n)$，其中 $y_i\in\mathbb{Z}_{r_m}$；

n 维向量$(z_1,z_2,\cdots,z_n)$，其中 $z_i\in\mathbb{Z}_q$；

n 维向量$(w_1,w_2,\cdots,w_n)$，其中 $w_i\in\mathbb{Z}_q$；

同时，对于网络 I 中的任意身份为 ID^* 的 AS*，将其身份表示为 $ID^*=\{ID_1^*,ID_2^*,\cdots,ID_n^*\}$，并构造与身份为 ID^* 的 AS* 相关的 AS_PATH 路由信息 $AS^*\|ID^*$，$h^*=Hash(AS^*\|ID^*)$，表示为 $h^*=\{h_1^*,h_2^*,\cdots,h_n^*\}$. 利用这些信息构造如下 4 个函数：

$$F(ID^*)=x'+\sum_{i=1}^{n}x_iID_i^*-r_us_u;$$

$$J(ID^*)=z'+\sum_{i=1}^{n}z_iID_i^*;$$

$$K(h^*)=y'+\sum_{i=1}^{n}y_ih_i^*-r_ms_m;$$

$$J(h^*)=w'+\sum_{i=1}^{n}w_ih_i^*;$$

并构造以下系统参数：

$$g_1=g^a,\ g_2=g^b;$$

$$u'=g_2^{-r_us_u+x'}g^{z'},\ u_i=g_2^{x_i}g^{z_i},\ 1\le i\le n;$$

$$u'=g_2^{-r_ms_m+y'}g^{w'},\ v_i=g_2^{y_i}g^{w_i},\ 1\le i\le n;$$

且有

$$u'\prod_{i=1}^{n}u_i^{ID_i}=g_2^{F(ID)}g^{J(ID)},\ v'\prod_{i=1}^{n}v_i^{h_i^*}=g_2^{K(h^*)}g^{L(h^*)}.$$

然后将网络 I 以及上面的信息发给攻击者 A.

其次，在攻击 IDSPV 机制过程中，当攻击者 A 在任何时间内进行询问 AS 私钥抽取 oracle 和 AS_PATH 签名 oracle 时，算法 B 给以如下响应：

(1) 私钥抽取请求. 当攻击者 A 向算法 B 提交关于身份为 ID^* 的 AS* 的私钥抽取请求时，算法 B 进行如下操作：

① 若 $F(ID^*)=0 \bmod(r_u)$，则算法 B 终止并输出“失败”；

② 若 $F(ID^*)\neq 0 \bmod(r_u)$，则算法 B 随机选取一个整数 $r_{ID^*}\in\mathbb{Z}_q^*$ 并按式(5)计算私钥：

$$d_{ID^*}=(d_{ID^*}^{(1)},d_{ID^*}^{(2)})$$
$$=(g_1^{-\frac{J(ID^*)}{F(ID^*)}}(g_2^{F(ID^*)}g^{J(ID)})^{r_{ID^*}},g_1^{-\frac{1}{F(ID^*)}}g^{r_{ID^*}}) \quad (5)$$

并将身份为 ID^* 的 AS^* 的私钥$(d_{ID^*}^{(1)},d_{ID^*}^{(2)})$发给攻击者.

由于

$$d_{ID^*}^{(1)}=g_1^{-\frac{J(ID^*)}{F(ID^*)}}(g_2^{F(ID^*)}g^{J(ID^*)})^{r_{ID^*}}$$
$$=g_2^a(g_2^{F(ID^*)}g^{J(ID^*)})^{\frac{-a}{F(ID^*)}}(g_2^{F(ID^*)}g^{J(ID^*)})^{r_{ID^*}}$$
$$=g_2^a(g_2^{F(ID^*)}g^{J(ID^*)})^{r_{ID^*}-\frac{-a}{F(ID^*)}}$$
$$=g_2^a\left(u'\prod_{i=1}^{n}u_i^{ID_i^*}\right)^{r_{ID^*}},$$
$$d_{ID^*}^{(2)}=g_1^{-\frac{1}{F(ID^*)}}g^{r_{ID^*}}=g^{-\frac{a}{F(ID^*)}}g^{r_{ID^*}}$$
$$=g^{r_{ID^*}-\frac{a}{F(ID^*)}}=g^{\boldsymbol{r}_{ID^*}},$$

其中 $\boldsymbol{r}_{ID^*}=r_{ID^*}-\dfrac{a}{F(ID^*)}$.

因此所构造的私钥(d_1,d_2)是有效的.

(2) AS_PATH 路由属性证明(签名)请求. 当攻击者 A 向签名 oracles 提出关于身份为 ID^* 的 AS^* 生成的 AS_PATH 路由属性证明，即对自己更新的路由属性的签名. 自己更新的路由信息就是所信任的下一跳的 AS 域及其身份 ID，记为 $AS'\|ID'$. 算法 B 操作如下：

① 若 $F(ID^*)\neq 0 \bmod(r_u)$，算法 B 调用前面给出的私钥抽取请求来构造身份为 ID^* 的 AS^* 的私钥，再用私钥对更新的 AS_PATH 信息进行签名即可；

② 若$F(ID^*)=0 \bmod(r_u)$且$K(h^*)\neq 0 \bmod(r_m)$，则算法 B 选取 $r',r''\in\mathbb{Z}_q^*$，并按式(6)计算得到签名：

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)$$
$$=\left(\left(u'\prod_{i=1}^{n}u_i^{ID_i^*}\right)^{r'}g_1^{-\frac{L(h^*)}{K(h^*)}}\left(v'\prod_{i=1}^{n}v_i^{h_i^*}\right)^{r''},g^{r'},g_1^{-\frac{1}{K(h^*)}}g^{r''}\right) \quad (6)$$

③ 若$F(ID^*)=0 \bmod(r_u)$且$K(h^*)=0 \bmod(r_m)$，则算法 B 终止并输出“失败”.

(3) AS_PATH 路由属性证明(签名)伪造. 倘若算法 B 在求解过程中未终止，则攻击者 A 能成功输出一个身份为 ID' 的 AS' 生成的路由属性证明 $\sigma'=(\sigma_1',\sigma_2',\sigma_3')$，从而能成功伪造有效的 AS_PATH 路由属性$(IP_1,AS_1,AS_2,\cdots,AS_i,AS')$.

最后，算法 B 对 CDH 问题实例进行求解. 若 $F(ID')\neq 0 \bmod(q)$且 $K(h')\neq 0 \bmod(q)$，算法 B 终止操作. 否则，若 $F(ID')=0 \bmod(q)$且 $K(h')=0 \bmod(q)$，那么算法 B 可求出 CDH 问题的实例的一个解为

$$g^{ab}=\frac{\sigma_1'}{(\sigma_2')^{J(ID')}(\sigma_3')^{L(h')}}.$$

为了确保算法 B 能以至少 ε' 的概率成功解决 CDH 问题实例，算法 B 需在同时满足如下 3 个事件的条件下进行：

① Evt1. 当攻击者 A 进行 AS^* 私钥抽取请求时算法 B 不会终止，即要求 $F(ID^*)\neq 0 \bmod(r_u)$；

② Evt2. 攻击者 A 能生成身份为 ID' 的 AS' 对自己更新的路由信息的一个有效的路由属性证明(签名)$\sigma'=(\sigma_1',\sigma_2',\sigma_3')$；即至少要求 $K(h^*)\neq 0 \bmod(r_m)$；

③ Evt3. 路由属性证明伪造成功，同时要求 $F(ID')=0 \bmod(q)$ 且 $K(h')=0 \bmod(q)$，其中 $1\leq i\leq n$.

为了便于计算，定义 U_i：$F(ID^*)\neq 0 \bmod(r_u)$；U^*：$F(ID')=0 \bmod(q)$；V_j：$K(h^*)\neq 0 \bmod(r_m)$；V^*：$K(h')=0 \bmod(q)$. 则算法 B 成功的概率等价于

$$Pr[B_{\text{succ}}]\geq Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\wedge U^*\wedge\bigcap_{j=1}^{q_s}V_j\wedge V^*\right]$$
$$=Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\wedge U^*\right]\wedge Pr\left[\bigcap_{j=1}^{q_s}V_j\wedge V^*\right] \quad (7)$$
$$=Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\right]\wedge Pr[U^*]\wedge Pr\left[\bigcap_{j=1}^{q_s}V_j\right]\wedge Pr[V^*] \quad (8)$$

式(7)、(8)均由 U_i、U^*、V_j、V_j 相互独立而得到，其中 $Pr[U^*]$以及 $Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\right]$分别计算如下：

$$Pr[U^*]=Pr[F(ID')=0 \bmod(q)\wedge F(ID')=0 \bmod(r_u)]$$
$$=Pr[F(ID')=0 \bmod(r_u)]\times Pr[F(ID')$$
$$=0 \bmod(q)]\,|\,Pr[F(ID')=0 \bmod(r_u)]$$
$$=\frac{1}{r_u}\times\frac{1}{N+1},$$
$$Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\right]=1-Pr\left[\bigcup_{i=1}^{q_e+q_s}\neg U_i\right]\geq 1-\frac{q_e+q_s}{N}.$$

因此，我们得到

$$Pr\left[\bigcap_{i=1}^{q_e+q_s}U_i\wedge U^*\right]\geq\left(\frac{1}{r_u}\times\frac{1}{N+1}\right)\times\left(1-\frac{q_e+q_s}{r_u}\right)$$
$$\geq\frac{1}{4(q_e+q_s)(N+1)},$$

同理可得

$$Pr\left[\bigcap_{j=1}^{q_s}V_j\wedge V^*\right]\geq\frac{1}{4q_s(N+1)},$$

从而有

$$Pr[B_{\text{succ}}]\geq\frac{1}{16q_s(q_e+q_s)(N+1)^2},$$

得到 ε' 的值为

$$\varepsilon'=\frac{\varepsilon}{16q_s(q_e+q_s)(N+1)^2}.$$

算法 B 的运行时间为攻击者 A 的运行时间加上 q_E 次私钥询问以及 q_S 次签名询问的响应时间，且将攻击者 A 的伪造签名转化为解决 CDH 问题的时间. 在攻击游戏中，每次私钥抽取询问中，总共进行了 5 次群 G_1 中的指数运算；每次签名询问中进行了 $(2N+4)$ 次群 G_1 中的指数运算. 因此总的运行时间有如下关系：

$$t'=t+O(5q_e+(2N+4)q_s)t_{G_1},$$

其中，t_{G_1} 是群 G_1 中指数运算所花的总时间.

当然，在算法 B 的模拟过程中，若事件 X_i：$F(ID^*)=0 \bmod(r_u)$ 或者事件 Y_j：$F(ID^*)=0 \bmod(r_u)$ 且 $K(h^*)=0 \bmod(r_m)$ 发生，则会导致攻击失败而终止. 易知，攻击失败的概率为

$$\begin{aligned}Pr[\bigcup_{i=1}^{q_e}X_i\vee\bigcup_{j=1}^{q_s}Y_j]&=Pr[\bigcup_{i=1}^{q_e}X_i]+Pr[\bigcup_{j=1}^{q_s}Y_j] \quad (9)\\&=\sum_{i=1}^{q_e}Pr[X_i]+\sum_{j=1}^{q_s}Pr[Y_j]\\&=\frac{1}{N+1}\left(\frac{q_e}{r_u}+\frac{q_s}{r_m}\right)\\&=\frac{1}{N+1}\times\frac{3q_s}{4(q_e+q_s)} \quad (10)\\&\leq\frac{1}{N+1}\times\frac{q_s}{(q_e+q_s)},\end{aligned}$$

其中式(9)的结果由 X_i、Y_j 相互独立得到，式(10)根据前面的参数设置得到.

若 N、q_e 和 q_s 都很大时，攻击者 A 攻击失败的概率一定程度上不影响我们模拟攻击的完成. 证毕.

假定在参与路由宣告过程中的 AS 既是签名者又是可净化签名者，实际上在 IDSPV 机制中就是如此. 任何 AS 均不能修改前面 AS 所更新的路由属性. 具体地，若攻击者 A 已攻陷了自治域 AS_i，攻击者 A 能篡改 AS_i 接收到的路由属性 $(IP_1, AS_1, AS_2, \cdots, AS_i)$，则意味着我们的保护机制未能达到存在不可伪造签名安全. 因此得出如下结论.

定理 2.　假定存在有界多项式攻击者 A 能在时间 t 内经过至多 q_e 次的密钥提取询问和 q_s 次的签名询问后以优势 ε 来攻破 IDSPV 机制中 AS_PATH 路由属性的不可改变性，则存在一个算法 B 能在时间 t'' 内以优势 ε'' 来产生一个有效的签名.

证明.　AS_PATH 路由属性的不可改变性是指即使攻击者 A 未能合法地将路由属性 $(IP_1, AS_1, AS_2, \cdots, AS_i)$ 修改为 $(IP_1, AS_1, AS_2, \cdots, AS_i^*)$，即将 AS_i 替换为 AS_i^*，其中 AS_i^* 为未授权的自治域. 若攻击者 A 将接收到的路由属性中插入路由信息如 AS_i^*，则更改为 $(IP_1, AS_1, AS_2, \cdots, AS_i^*)$，而且更改后的路由属性有效，意味着算法 B 可以产生一个有效的路由属性证明(签名). 具体分析如下：

(1) 参数建立. 攻击者 A 在游戏中与算法 B 及其挑战者 C 进行如下交互：

① 算法 B 向挑战者 C 提交一个请求，挑战者 C 给算法 B 返回系统的参数如下 $(G_1, G_2, e, q, g, g_1, g_2, u', v', u_1, \cdots, u_n, v_1, \cdots, v_n)$；

② 对于 $i=1, \cdots, n$，算法 B 选择 $t_i\in\mathbb{Z}_q^*$，并令 $u_i=g^{t_i}$，并添加到发给算法 B 的系统参数之中；

③ 对于 $i=1, \cdots, n$，算法 B 选择 $s_i\in\mathbb{Z}_q^*$，并令 $v_i=g^{s_i}$，并添加到发给算法 B 的系统参数之中.

(2) 私钥抽取请求. 攻击者 A 向算法 B 提交关于身份为 ID_i 的 AS_i 的私钥，算法 B 如下响应：

① 算法 B 向挑战者 C 请求身份为 ID_{i-1} 的 AS_{i-1} 的私钥，并获得私钥 $(d_{ID_{i-1}}^{(1)}, d_{ID_{i-1}}^{(2)})$；

② 算法 B 令 $\boldsymbol{d}_{ID_i}^{(1)}=d_{ID_{i-1}}^{(1)}\cdot(d_{ID_{i-1}}^{(2)})^{ID_it_i}$ 且 $\boldsymbol{d}_{ID_i}^{(2)}=d_{ID_{i-1}}^{(2)}$，并将 $(\boldsymbol{d}_{ID_i}^{(1)}, \boldsymbol{d}_{ID_i}^{(2)})$ 发送给攻击者 A.

(3) 路由属性证明(签名)请求. 当攻击者 A 向算法 B 提交关于身份 ID_i 的 AS_i 对路由信息 $AS_{i+1}\|ID_{i+1}$ 的路由属性证明(签名)询问时，算法 B 进行如下操作：

① 算法 B 计算 $H_i=Hash(\boldsymbol{d}_{ID_i}\|AS_i\|ID_i)$，$h=Hash(H_i\|AS_{i+1}\|ID_{i+1})$，并将 h 表示为 $h=\{h^1, h^2, \cdots, h^n\}$；

② 算法 B 向挑战者 C 询问关于身份 ID_{i-1} 的 AS_{i-1} 对路由信息 $AS_i\|ID_i$ 的路由属性证明，并得到 $(\sigma_1, \sigma_2, \sigma_3)$；

③ 算法 B 令 $\boldsymbol{\sigma}_1=\sigma_1\cdot\sigma_2^{ID_it_i}\prod_{j=1}^{n}\sigma_3^{h^js_i}$，$\boldsymbol{\sigma}_2=\sigma_2$，$\boldsymbol{\sigma}_3=\sigma_3$；

④ 算法 B 将 $(\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \boldsymbol{\sigma}_3)\cup(\sigma_3^{h^1s_i}, \cdots, \sigma_3^{h^ns_i})$ 发给攻击者 A.

(4) 路由属性证明(签名)伪造. 假定攻击者 A 能输出一个由身份 $I\hat{D}$ 的 $A\hat{S}$ 对相关的 AS_PATH 路由信息 $AS\|ID$ 的一个有效路由属性证明 $(\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3)$，则算法 B 在攻击者 A 伪造的签名的基础上也能获得一个有效路由属性证明，具体如下：

① 攻击者 A 将路由相关信息 $AS\|ID$ 及其路

由属性证明$(\hat{\sigma}_1,\hat{\sigma}_2,\hat{\sigma}_3)$发给算法 B,其中 $AS\|ID$ 不是 AS_i 指定的合法消息.

② B 构造身份为 ID^* 的 AS_i^* 对相关的 AS_PATH 路由信息 $AS^*\|ID^*$ 的有效路由属性证明,其中 $AS^*\|ID^*$ 不是 AS_i 指定的合法消息.具体计算如下:

$$\sigma_1^*=\frac{\hat{\sigma}_1}{(\hat{\sigma}_2)^{\widehat{ID}\cdot\hat{t}_i}\cdot\prod_{j=1}^{n}\hat{\sigma}_3^{h^j s_i}},$$

$$\sigma_2^*=\hat{\sigma}_2,\ \sigma_3^*=\hat{\sigma}_3.$$

很容易验证,$\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$是身份为 ID^* 的 AS_i^* 对相关的 AS_PATH 路由信息 $AS^*\|ID^*$ 的有效路由属性证明.从定理 1 的证明可知,算法 B 能求解 CDH 问题的一个实例.

显然,算法 B 成功伪造有效路由属性证明的前提条件是攻击者 A 能改变了 IDSPV 机制的 AS_PATH 路由属性的不可改变性,因此 B 成功的概率 $\varepsilon''\geq\varepsilon$.

同时,算法 B 运行的时间 t'' 等于攻击者 A 运行的时间 t 再加上它响应 q_e 次的密钥提取询问和 q_s 次的签名询问所花的时间.而每次密钥抽取询问需要算法 B 在群 G_1 中进行 n 次的指数运算;每次签名询问需要算法 B 在群 G_1 中进行 $2n$ 次的指数运算.假定群 G_1 中进行指数运算所花的时间为 t_e,则有 $t''=t+(n\cdot q_e+2n\cdot q_s)$. 证毕.

5 效率分析

针对第 3 节提出的 IDSPV 保护机制,本节给出了存储和平均收敛时间两个指标的效率分析.在存储方面,我们主要考虑保护机制中更新路由信息的大小增量以及证书存储开销;在平均收敛时间方面,主要考虑更新路由信息总数、签名运算次数及所花的时间以及签名验证运算次数及所花的时间.在测试过程中,所采用的测试网络场景参数是:假定有 m 个 AS,每个 AS 均有 a 个 AS speaker,且与 b 个 AS 对等链接,同时每个 AS speaker 发布 c 个前缀信息,该信息传播到整个网络,在传播过程中接收到宣告信息的 AS 进行更新,直至路由稳定收敛.

5.1 存储增量

在考察存储增量中,主要考虑 IDSPV 机制和 S-BGP 中的报文长度分别比 BGP 更新报文长度的增加量.由于 IDSPV 机制采用了可净化签名方案,在更新报文中增加了路由属性证明$(\sigma_1,\sigma_2,\sigma_3)$属性,因此 IDSPV 机制中的更新报文长度比 BGP 协议的更新报文长度约增加 92.6 字节.若在有限域 $F_{3^{97}}$ 上进行,则 IDSPV 机制中更新报文的大小增量为 $\Delta_{Update\_IDSPV}=92.6(L\geq1)$.而采用 1024 比特的 RSA 算法的 S-BGP 中更新报文的大小增量为 $\Delta_{Update\_RSA}=128L$,FTAPV 机制中更新报文的大小增量为 $\Delta_{Update\_FTAPV}=81(L\geq1)$,其中 L 为 BGP 中 AS_PATH 的长度.图 2 所示的结果是随着 AS_PATH 长度 L 不断增加,IDSPV 机制、FTAPV 机制以及采用 1024 比特的 RSA 机制的 S-BGP 中更新报文长度增量的变化.

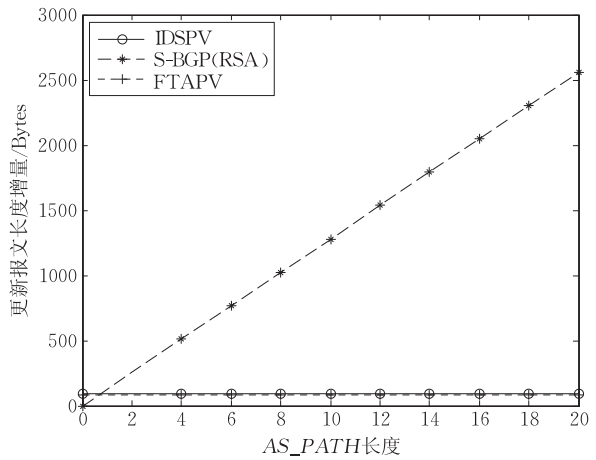

图 2 IDSPV、S-BGP 和 FTAPV 更新报文长度增量

我们从图 2 观察到:S-BGP 机制的更新报文长度增量随着 AS_PATH 长度 L 不断增加而增加,而 IDSPV 机制和 FTAPV 机制并未发生变化.尽管 IDSPV 机制中更新报文新增加了一个属性,相当于 3 个签名长度,但在每次生成路由属性证明过程中采用可净化签名技术,只需按照 3.4.2 节的式(4)对更新的报文进行聚合添加,起到了聚合签名作用,占用较少的存储空间,而且增量未随着 AS_PATH 长度 L 的变化而改变.因此采用 IDSPV 机制的路由更新报文增加的长度比采用 RSA 机制的 S-BGP 的路由更新报文增加的长度小;对于 FTAPV 机制,IDSPV 机制报文长度增量略高,但如下面表 1 所示,IDSPV 机制不需要存储证书.

从存储开销方面来说,由于 IDSPV 机制主要基于身份的可净化签名方案,避免了使用证书,因此不需承担证书存储开销,仅需承担系统参数和更新报文长度增量的存储开销.但目前基于密码学的 BGP 路由属性保护方案多数采用了证书,比如在 S-BGP 中,总证书规模为 N^2,单个 BGP 路由器的证书规模为 N;在 IDPV[7] 中,总证书规模为 $0.027N^2$,单个

节点证书规模为 $0.027N$；其中 N 是网络拓扑 I 中的 AS 规模；FTAPV[8] 中，总证书规模为 $\bar{O}\times(1+\bar{O})$，单个节点证书规模为 $\bar{O}\times(1+\bar{O})\times N$，其中 $\bar{O}=avg\_p\times(1+avg\_p)$，$avg\_p$ 为每个 AS 拥有的平均邻居数目. X.509 证书的大小约为 600 byte[22]，若 N 很大时，如 CIDR Report① 数据给出，2014 年 2 月 14 日在 Internet 中约有 46 351 个 AS，会导致每个 BGP 路由器承担的证书存储开销很大，再加上承担系统参数和更新报文长度增量的存储开销，将会占用很多的路由器存储空间，因而影响 BGP 路由器的工作性能. 表 1 给出各方案采用证书的规模.

表 1　各方案证书规模

方案	每个路由器需存储的证书规模	全网需存储的证书规模
IDSPV	—	—
FTAPV	$\bar{O}\times(1+\bar{O})$	$\bar{O}\times(1+\bar{O})\times N$
IDPV	$0.027N$	$0.027N^2$
S-BGP	N	N^2

表 1 中给出了 IDSPV、FTAPV、IDPV 以及 S-BGP 等方案中需要存储的证书规模. 从表中可知，IDSPV 机制由于采用了基于身份的密码学，不再需要证书机制. 因此，在证书方面 IDSPV 机制比其他方案更优.

5.2　平均收敛时间

我们所考虑的路由平均收敛时间与产生的更新报文总数 $\sharp Update$、生成路由属性证明运算次数 $\sharp Sign$ 及所耗时间 t_{Sign}、路由属性证明验证次数 $\sharp Verif$ 及所耗时间 t_{Verif} 等因素有关，当然还与 CPU 处理信息的能力、所采用的路由属性证明生成算法等有关. 根据前面的实验场景和参数设置，获得更新报文的总数为 $\sharp Update=m\times a\times b\times c$. 由于在更新的报文中，AS 仅选择与自己的路由策略相符合的报文，因此在签名验证时，并不是对所有接收到的更新报文进行验证，而是仅对自己所选择的报文的合法性和完整性进行验证. 类似的，AS 也仅对所选择的更新报文进行更新并生成路由属性证明. 由于 AS 都是自治域，均可自主地根据自己的路由策略来选取路由，因此对更新报文的选择、路由属性证明生成和路由属性证明验证均具有一定的概率性. 在相同的最小路由宣告间隔（MRAI）下，假定每个 AS 选择更新报文的概率均为 $Pr\{\text{AS\_PATH preferred}\}$，则给出路由收敛时间增量模型如下：

$$\Delta_{\text{Time\_Conver}}=Pr\{\text{AS\_PATH preferred}\}\times\sharp Update\times(b\times\sharp Sign\times t_{Sign}+L\times\sharp Verif\times t_{Verif}),$$

其中参数 $\Delta_{\text{Time\_Conver}}$ 表示路由收敛时间增量，其余参数已由上面给出.

我们在测试中采用 SSFNet② 生成网络拓扑，根据 SSFNet 生成的网络拓扑，搭建了 60 个 AS 域，总共 120 台 BGP 路由器. 我们的 IDSPV 机制是基于 2.4 GHz 的处理器及 Ubuntu11.04 操作系统，采用 PBC Library③ 来实现. 在我们的原型系统中每个 AS 有 1 个 speaker，且有 12 个邻居，同时每个 speaker 生成 2 个前缀，即 $a=1$，$b=12$，$c=2$. 具体参数如下设置：最小路由宣告间隔（MRAI）为 30 s，链路延迟为 0.1 ms，$L=16$，$Pr\{\text{AS\_PATH preferred}\}=0.8$. 根据文献[23-24]，1024 比特的 RSA 的签名所花时间为 50 ms，签名验证所花的时间为 2.5 ms；而有限域 $F_{3^{97}}$ 上的配对运算所花时间为 43 ms；主要考察随着 AS 规模大小的变化，采用 IDSPV 机制的 BGP 协议、采用 RSA 机制的 S-BGP 协议以及未采用任何安全机制的 BGP 协议的路由平均收敛时间，实验结果如图 3 所示.

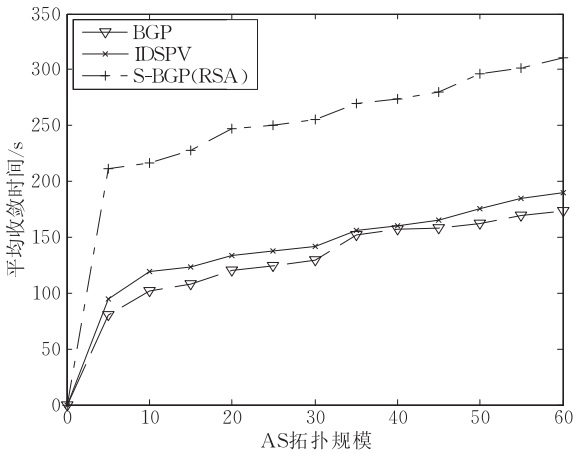

图 3　平均收敛时间

图 3 中表明，采用 IDSPV 机制的 BGP 协议的路由平均收敛时间比采用 S-BGP 的 BGP 协议的路由平均收敛时间少，而与 BGP 协议的路由平均收敛时间略多. 目前互联网中绝大多数的 BGP 路由器处理一次 UPDATE 消息平均需要的时间为 1 s，在 200 MHz 的 CPU（接近目前路由器的计算能力）中，实现有限域 $F_{3^{97}}$ 的配对运算中所需的时间是 43 ms，而 IDSPV 机制中进行了 1 次签名操作和 1 次验证操作，总耗时为 86 ms. 若遇到高峰期，峰值扩大 10 倍，也仅耗时 860 ms. 因此，IDSPV 机制对 BGP 路

① CIDR report. http://www.cidr-report.org/as2.0，2014
② Ogielski A T，Cowie J H. SSFNet：Scalable simulation framework—Network models. http://www.ssfnet.org
③ PBC Library. http://crypto.stanford.edu/pbc/download.html

由的平均收敛时间不造成太大影响.

6 结 论

BGP 路由协议中 AS_PATH 路由属性的认证问题是 BGP 路由协议安全的一个重要课题,研究资源开销少、易部署的 AS_PATH 路由属性安全保护方案仍是重要的研究方向.基于此,本文提出了一种标准模型下可证明安全的 BGP 路由属性保护机制——IDSPV 机制,采用基于身份的可净化签名技术来保护 BGP 路由属性完整性和合法性的安全机制,同时在标准模型下给出了 IDSPV 机制的安全证明.在文中详细讨论了 IDSPV 机制的安全性和性能,与现有方案相比,IDSPV 机制更易于在实际中部署实现.由于所采用的可净化签名方案是一种轻量型的签名方案,该机制是可以结合 BGP 自身的路由策略来决定将路由信息转发给更信任的下一个 AS 域,从安全性和负载均衡方面来说,具有一定的灵活性和可扩展性.今后的研究工作将进一步研究如何结合 BGP 自身的路由策略来确定和刻画 AS 域的信任度,以便更好地确保新机制的有效性.

致 谢 审稿人提出的修改意见对提高论文水平有很大的帮助,在此表示感谢!

参 考 文 献

[1] Huston G, Rossi M, Armitage G. Security BGP-A literature survey. IEEE Communications Surveys and Tutorials, 2011, 13(2): 199-222

[2] Butler K, Farley T, McDaniel P. A survey of BGP security issues and solutions. Proceedings of the IEEE, 2010, 98(1): 100-122

[3] Goldberg S, Schapira M, Hummon P, Rexford J. How secure are secure interdomain routing protocols?//Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication (SIGCOMM). New Delhi, India, 2010: 87-98

[4] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭雪海. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)

[5] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

[6] Kranankis E, Wan T, Oorschot P C. On interdomain routing security and pretty secure BGP(psBGP). ACM Transactions on Information and System Security, 2007, 10(3): 11-25

[7] Wang Na, Zhi Ying-Jian, Zhang Jian-Hui, Cheng Dong-Nian, Wang Bin-Qiang. Identity-based security inter-domain routing protocol. Journal of Software, 2009, 20(12): 3223-3239(in Chinese)
(王娜, 智英建, 张建辉, 程东年, 汪斌强. 一种基于身份的安全域间路由协议. 软件学报, 2009, 20(12): 3223-3239)

[8] Zhao Chen, Sun Bin, Yang Yi-Xian, Yang Yan. A light-weight mechanism for border gateway protocol path verification. Journal of Electronics & Information Technology, 2012, 34(9): 2167-2173(in Chinese)
(赵宸, 孙斌, 杨义先, 杨焱. 一种轻量化的边界网关协议路径验证机制. 电子与信息学报, 2012, 34(9): 2167-2173)

[9] Raimagia D, Singh S, Zafar S. A novel approach for secure routing through BGP using symmetric key. International Journal of Network Security & Its Applications (IJNSA), 2013, 5(5): 153-165

[10] Boldyreva A, Lychev R. Provable security of (S-BGP) and other path vector protocols: Model, analysis, and extensions//Proceedings of the 19th ACM Conference on Computer and Communications Security, Sheraton Raleigh Hotel. Raleigh, USA, 2012: 541-552

[11] Cazenave I O, Kosluk E, Ganiz M C. An anomaly detection framework for BGP//Proceedings of the 2011 International Symposium on Innovations in Intelligent Systems and Applications (INISTA). Istanbul, Turkey, 2011: 107-111

[12] Israr J, Guennoun M, Mouftah H T. Analysis of impact of trust on secure border gateway protocol. Proceedings of the 16th IEEE Symposium on Computers and Communications. Kerkyra, Corfu, Greece, 2011: 1099-1104

[13] Suchara M, Fabrikant A, Rexford J. BGP safety with spurious updates//Proceedings of the Infocom. Shanghai, China, 2011: 2966-2974

[14] Fabrikant A, Syed U, Rexford J. There is something about MRAI: Timing diversity may exponentially worsen BGP convergence//Proceedings of the Infocom. Shanghai, China, 2011: 2975-2983

[15] Gill P, Schapira M, Goldberg S. Let the market drive deployment: A strategy for transitionning to BGP security//Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication (SIGCOMM). Toronto, Canada, 2011: 14-25

[16] Sundaresan S, Lychev R, Vytautas V. Preventing attacks on BGP policies: One bit is enough. Institute of Technology, Georgia: Technical Report GT-CS-11-07, 2011

[17] Li Qi, Wu Jian-Ping, Xu Ming-Wei, et al. GesBGP: A good-enough-security BGP. Chinese Journal of Computers, 2009, 32(3): 506-515(in Chinese)
(李琦, 吴建平, 徐明伟等. 自治系统间的安全路由协议 GesBGP. 计算机学报, 2009, 32(3): 506-515)

[18] Zhou You-Sheng, Sun Yan-Bin, Qing Si-Han, Yang Yi-Xian. An efficient ID-based verifiably encrypted signature scheme. Journal of Computer Research and Development, 2011, 48(8): 1350-1356(in Chinese)
(周由胜，孙艳宾，卿斯汉，杨义先. 一种高效的基于身份的可验证加密签名方案. 计算机研究与发展，2011，48(8)：1350-1356)

[19] Yang Ming, Shen Xiaoqin, Peng Yamian. Identity-based sanitizable signature scheme in the standard model//Proceedings of the International Conference on Information Computing and Applications, Part I, CCIS 105. Berlin: Springer-Verlag, 2010: 9-16

[20] Hu Xiang-Jiang, Zhu Pei-Dong, Gong Zheng-Hu. SE-BGP: An approach for BGP security. Journal of Software, 2008, 19(1): 167-176(in Chinese)
(胡湘江，朱培栋，龚正虎. SE-BGP:一种 BGP 安全机制. 软件学报，2008，19(1)：167-176)

[21] Waters B. Efficient identity-based encryption without random oracles//Advances in Cryptology-Proceedings of the EUROCRYPT 2005. Aarhus, Denmark, 2005: 114-127

[22] Zhao M, Smith S W, Nicol D. Evaluating the performance impact of PKI on BGP Security//Proceedings of the 4th Annual PKI Research and Development Workshop. Gaithersburg, Maryland, 2005: 144-148

[23] Granger R, Page D, Stam M. On small characteristic algebraic Tori in pairing-based cryptography. LMS Journal of Computation and Mathematics, 2006, 9(13): 64-85

[24] Zhao M, Smith S W, Nicol D. Aggregated path authentication for efficient BGP security//Proceedings of the 12th ACM Conference on Computer and Communications Security. Alexandria, USA, 2005: 128-138

LI Dao-Feng, born in 1974, Ph. D., associate professor. His current research interests include cryptography and information security.

WANG Gao-Cai, born in 1976, Ph. D., professor, Ph. D. supervisor. His current research interests include computer networks, performance evaluation.

WANG Zhi-Wei, born in 1976, Ph. D., associate professor. His current research interests include cryptography and information security.

ZHONG Cheng, born in 1964, Ph. D., professor, Ph. D. supervisor. His current research interests include parallel and distributed computing, computational biology, and trusted computing.

LI Tao-Shen, born in 1957, Ph. D., professor, Ph. D. supervisor. His current research interests include network computing and information security.

Background

This work described in this paper is supported by the National Natural Science Foundation of China (Nos. 61262003, 61373006, 61362010), Foundation of Guangxi Educational Committee (Nos. YB2014008, 2013YB007) and the Talents Foundation of GXU (No. XBZ110905).

The Border Gateway Protocol (BGP) is a distributed routing protocol that establishes how Internet traffic is routed between autonomous systems(ASes). The BGP lacks security, since BGP relies on hearsay information to update routing tables. And the malicious routers have a chance to insert false information into the forged messages they send. The major vulnerabilities are the lack of authenticity of the information conveyed in messages and the lack of authorization for BGP routes to represent certain ASes.

There are lots of proposals to provide route authentication for BGP in the reference, but when they come to deployment, they are faced to two main obstacles: time problem and space problem.

Aiming at these problems, in this paper the authors proposed a new path authentication scheme for authenticating path information in BGP route announcements. The main idea is to combine the identity-based cryptography and sanitizable signature scheme. This scheme only needs to update messages and add the updated messages to AS_PATH without certification, so that the integrity and the authenticity for the AS_PATH attribute are protected, which reduces the route resource expense. Furthermore, the security of the scheme is proved by using the reduction method in the standard model.