基于分治策略的 BGP 安全机制

王滨[1,2,3]，安金梁[4]，吴春明[1]，兰巨龙[3]

（1. 浙江大学 计算机科学与技术学院，浙江 杭州 310027；2. 浙江工商大学 信息与电子工程学院，浙江 杭州 310018；
3. 国家数字交换系统工程技术研究中心，河南 郑州 450002； 4. 河南科技学院 信息工程学院，河南 新乡 453003）

摘 要：研究了 SE-BGP 的安全性，通过分析发现该机制存在安全漏洞，无法抵御合法用户发起的主动攻击。为了克服 SE-BGP 存在的安全漏洞， 基于 AS 联盟的思想，使用基于 RSA 的聚合签名算法设计了一种新的 BGP 安全机制:SA-BGP，该机制具有更高的安全性，可以有效地验证 AS 宣告的网络层可达信息(NLRI)的正确性和 AS 宣告的路径属性的真实性，还可以大规模地减少网络证书规模和单个节点存储的证书数量，通过仿真实验得到 SA-BGP 和同级别的安全机制相比对网络的影响较小，收敛速度更快。

关键词：BGP 安全；AS 联盟；聚合签名；RAS

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)05-0091-08

Study of BGP secure scheme based on divide and conquer strategy

WANG Bin[1,2,3], AN Jin-liang[4], WU Chun-ming[1], LAN Ju-long[3]

(1. Computer Science College, Zhejiang University, Hangzhou 310027 , China;
2. College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China;
3. National Digital Switching System Engineering&Technological R&D Center, Zhengzhou 450002,China;
4. College of Information Technology, Henan Institute of Science and Technology, Xinxiang 453003,China)

Abstract: A new approach was studied for BGP security: SE-BGP. By analyzing the security of SE-BGP, was found it had some secure leaks which couldnt resist active attack. To solve these secure problems of SE-BGP, an AS-alliance-based secure BGP scheme : SA-BGP was proposed, which used the aggregate signatures algorithm based on RSA. The SA-BGP has strong ability of security that can effectively verify the propriety of IP prefix origination and verifies the validity of an AS to announce network layer reachability information (NLRI). SA-BGP can large-scale reduced the number of the used certificates. Performance evaluation results that SA-BGP can be implemented efficiently and the incurred overhead, in terms of time and space, ptable in practice.

Key words: border gateway protocol security; autonomous system alliance; aggregate signatures; RSA

1 引言

域间路由系统作为整个互联网的支柱，其安全性具有重要的战略意义。作为目前互联网唯一的域间路由协议——BGP(border gateway protocol)协议[1]在设计当初并没有考虑到任何安全因素。由于 BGP

收稿日期：2010-08-23；**修回日期**：2010-12-22

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2008AA01A323, 2009AA01A334, 2008AA01A325）；国家重点基础研究发展计划（“973”计划）基金资助项目（2007CB307102）；国家科技支撑计划基金资助项目（2008BAH37B02）；国家自然科学基金资助项目（60773182, 61070157）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2008AA01A323, 2009AA01A334, 2008AA01A325); The National Basic Research Program of China (973 Program) (2007CB307102); The National Key Technology R&D Program of China (2008BAH37B02); The National Natural Science Foundation of China (60773182, 61070157)

本身存在着巨大的安全隐患[2]，近年来，很多的域间路由安全事件都是由 BGP 的安全脆弱性引起的。因此，提高 BGP 协议的安全性是解决域间路由安全的重要途径，也一直是人们研究的热点问题。

目前，针对 BGP 的脆弱性已有不少公司和个人提出一些安全扩展方案。这些方案各有优劣，大体可以分为以下 2 类。

1) 与 PKI 相关的方案，即在 BGP 的基础上结合 PKI 来对平台中的每一个实体提供授权声明和身份认证，其安全能力相对比较强，但实现开销太大、部署困难，如 S-BGP[3]和 psBGP[4]等。

2) 与 PKI 无关的方案，如 soBGP[5]和 Listen and Whisper 机制[6]等，这些安全机制的安全性相对而言较弱，但易于在实际环境中部署。

本文在研究了文献[7]中作者提出的一种新的 BGP 安全机制：SE-BGP。通过对该机制进行形式化描述后进行分析，发现 SE-BGP 存在明显的安全漏洞。为了克服 SE-BGP 存在的安全问题，本文提出了一种基于 RSA 顺序聚合签名的算法，该算法可以有效抵抗重放攻击。最后，使用该签名算法和基于 AS 联盟的思想设计了一种新的 BGP 安全机制：SA-BGP，该方案可以大规模地降低单个节点的证书存储规模，减少路由器处理负载和传输的信息量，并且该机制能够有效地验证 AS 宣告的 NLRI 的正确性和 AS 宣告的路径属性的真实性。

2 SE-BGP 概述

文献[7]中给出了一种新的 BGP 安全机制：SE-BGP，该机制根据网络中 AS 节点总是聚集成不同的集合，集合中的节点通过少数高度数节点与集合外的节点相连，并且高度数节点之间具有很高的聚集度的特点，生成 AS 联盟并确立联盟中的关键节点，且每个 AS 联盟内都有一个认证中心 CA，安全 AS 联盟中关键节点相连的其他安全 AS 联盟中关键节点也需要在这个安全 AS 联盟中进行认证。本节将对 SE-BGP 机制中的认证算法进行简单地描述。

2.1 TTM 模型

TTM 基于分布式的 PKI 结构。与传统的网状结构不同，每个 CA 之间并不相互认证证书，其信任关系的传递是通过关键节点的特殊能力实现的。在如图 1 所示的网络中假设 AS 联盟和关键节点都已经生成完毕，具体如图 1 所示。关键节点 T_1、T_2 同时拥有 2 套公钥证书，即 T_1、T_2 都具有 SA_1 和 SA_2 中的公钥证书。其中，$S_k(m)$ 表示节点 k 对其发布的信息 m 进行签名，$V_k(S)$ 表示用节点 k 的公钥对签名 S 进行验证。

假设 SA_2 中的节点 c 需发布信息 M 到 SA_1 中的节点 b。当 T_2 收到 c 的信息，通过认证后，用 SA_1 中的 CA 分配的密钥对 M 进行签名，签名的内容记为 M_{c-T_2}。当 T_1 收到 T_2 传递的信息时，用对应的公钥验证 M，其用 T_2 在 SA_1 中的公钥验证 $M=V_{T_2}[S_{T_2}(M_{c-T_2})]$，若通过验证，则对 M 用自己在 SA_1 中的私钥进行签名，签名的内容记为 M_{c-T_1}。当节点 b 收到明文 M' 和 2 个签名 $S_{T_1}(M_{c-T_1})$、$S_{T_2}(M_{c-T_2})$ 后，节点 b 接受发布信息 M 的条件为 $M'=V_{T_1}[S_{T_1}(M_{c-T_1})]=V_{T_2}[S_{T_2}(M_{c-T_2})]$。

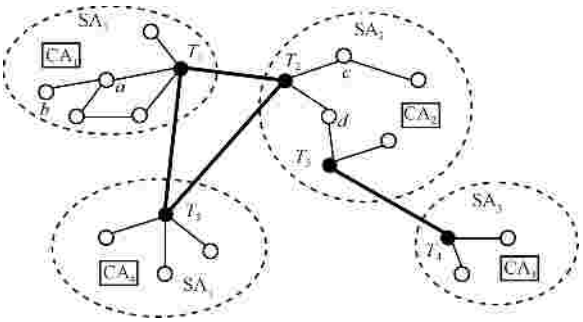

图 1 AS 联盟连接

2.2 SE-BGP 新增的属性

SE-BGP 需要增加 2 个属性。

1) AS_Security_Source 用于地址源认证，用来存放源节点以及关键节点对于地址源信息的签名，其中最多包含 2 个签名，只有源节点和关键节点才会更新 AS_Security_Source。

2) AS_Security_Path 用于路径认证，用来存放任何节点对于路径信息的签名，其需要签名的路径信息包括已经过的路径(含本身)、下一节点和时间等其他需签名的信息，任何节点都会更新 AS_Security_Path。

2.3 SE-BGP 认证和更新算法

SE-BGP 主要解决对于不同 AS 联盟之间，如何通过关键节点来进行认证。对于关键节点，由于其拥有 2 套以上的公钥证书，因此其使用的原则为：用来源节点的 AS 联盟内的公钥证书进行认证，用目的 AS 节点联盟内的私钥签名。

当某节点需要发布一条 UPDATE 信息时，它需要同时修改 AS_Security_Source 和 AS_Security_Path 属性。当节点收到一条 UPDATE 信息时，首先对

源地址信息和路径信息进行认证，然后对 AS_Security_Source 和 AS_Security_Path 属性做相应的修改，并向下传递。具体描述如下。

1) 查找 AS 联盟内的完整路径，检查其状态，若不正确，则抛弃该路径，并结束算法。

2) 对地址源信息进行认证和更新。

① 地址源认证：若 AS_Security_Source 中只有一个签名(源节点签名)，则检查证书；若 AS_Security_Source 中只有 2 个签名(含源节点签名)，则验证签名是否一致并检查证书；若 AS_Security_Source 中只有 2 个签名(不含源节点签名)，则验证签名是否一致。

② 地址源认证签名更新：若目的 AS 和来源 AS 节点不在同一个 AS 联盟内，则 AS_Security_Source 中的签名队列前移，并将自己对于验证后的地址源信息签名加入到队列中；否则，若签名队列为 1，则队列前移，并将自己对于验证后的地址源信息签名加入到队列尾；若签名队列为 2，则将自己对于验证后的地址源信息签名替换队列尾；

3) 对路径信息进行认证和更新。

① 对 AS_Security_Path 中的签名进行认证，如果不正确，则退出算法。

② 若目的来源 AS 为相邻安全 AS 联盟的关键节点，且目的节点为本 AS 联盟内节点，则将 AS_Security_Source 中的签名队列清空，只保留最后一个元素，将自己对于验证后的地址源信息签名并加入到队列中；否则，将自己对于验证后的地址源信息签名并加入到队列中。对于非关键节点，由于只有本安全 AS 联盟内的证书和密钥，因此只需处理本 AS 联盟内节点和相邻 AS 联盟的关键节点的认证信息。

3　SE-BGP 安全性分析

本节将给出 SE-BGP 的形式化描述，并基于此形式化描述对其进行安全性分析。

3.1　SE-BGP 形式化描述

文献[7]作者给出的基于 TTM 模型的认证和更新算法的形式化描述如下。假设关键节点 T_1 所在的联盟中的节点 C 需要发送一个 SE-BGP 数据分组给关键节点 T_4 所在的联盟中的节点 D，数据分组需要依次经过关键节点 T_1、T_2、T_3、T_4，4 个关键节点呈串接关系。则每个关键节点分别拥有其相邻关键节点所在 AS 联盟内的认证中心 CA 颁发的证书。另外，形式化描述不考虑联盟内的认证，仅仅考虑关键节点间的认证。

相关符号说明如下。$path$：数据分组经过的路径；$time$：发送数据分组时的时间；k_{CAi-T}：联盟 i 的 CA 为用户 T 颁发证书的公钥；k_{CAi-T}^{-1}：联盟 i 的 CA 为用户 T 颁发证书的私钥；$[M]k$：表示对消息 M 用密钥 k 进行加密或签名运算；Crt_U：用户 U 的数字证书。

算法的形式化描述如下。

$1) T_1 \rightarrow T_2 : \{[M]k_{CA1-S}^{-1}, [M_{C-T1}]k_{CA2-T1}^{-1}\},$

$\{[path, T_2, time_1]k_{CA2-T1}^{-1}\}, M$。

$2) T_2 \rightarrow T_3 : \{[M]k_{CA1-S}^{-1}, [M]k_{CA3-T2}^{-1}\},$

$\{[path^{+}, T_3, time_2]k_{CA3-T2}^{-1}\}, M$。

$3) T_3 \rightarrow T_4 : \{[M]k_{CA1-S}^{-1}, [M]k_{CA4-T3}^{-1}\},$

$\{[path^{++}, T_4, time_3]k_{CA4-T3}^{-1}\}, M$。

3.2　SE-BGP 的安全性分析

SE-BGP 存在以下的安全问题。

1) 设计的算法中存在冗余。按照文献中认证和更新算法的描述 *AS_Security_Source* 中的 2 个签名，其中第一个签名：源节点所在的联盟中的关键节点对信源地址的签名，将一直不被替换，但是该签名在第二跳以后就不具有任何的认证作用了，因为节点 T_3 不和 T_1 相连，所以 T_3 得不到用户 C 的证书，故无法验证这个签名，所以第二跳以后第一个签名就成为一个冗余。

2) 算法基于对关键节点的完全信任，所以无法抵御主动攻击敌手发起的伪造攻击。

①任何传输路径上的关键节点都可以篡改或伪造路径信息；算法协议中 T_2 发送给 T_3 的消息应该是 $\{[M]k_{CA1-S}^{-1}, [M]k_{CA3-T_2}^{-1}\}$、明文消息 M 和 $\{[path^{+}, T_3, time_2]k_{CA3-T_2}^{-1}\}$，但是如果 T_2 是一个主动攻击者，那么可以随意地修改路径信息并对修改后的信息进行签名得到 $\{[M]k_{CA1-S}^{-1}, [M']k_{CA3-T_2}^{-1}\}$，$\{[path', T_3, time_2]k_{CA3-T_2}^{-1}\}$，由于该签名的生成者是内部攻击者，其拥有合法的证书，并且下一跳节点无法验证 $[M]k_{CA1-S}^{-1}$，所以下一跳节点将接受该签名。

②每个关键节点都可以任意伪造并发布虚假的关于非本 AS 联盟内节点的 UPDATE 消息；例如图 1 中的关键节点 T_3 可以任意伪造关于非 SA_3 内节点的虚假的 UPDATE 消息，进行签名后发送出去，但是其下一跳节点假设为 T_4，由于它对节点 T_3 是完

全信任的，所以只要验证这个消息是不是节点T_3的签名，如果是，就会接受并转发出去。

3.3 总结

通过上面对作者提出的算法的安全性分析，可以看到，BGP 协议中使用作者提出的安全机制后和没有添加安全机制的协议安全性大致相同，SE-BGP 仅仅比 BGP 协议增加了当发现虚假 UPDATE 消息后可以进行追查是哪个节点发送了虚假信息的功能。但是，就危害程度而言，SE-BGP 比不添加任何安全机制的 BGP 更大，因为主动攻击对协议来说具有更大的危险性，在网络环境下，当通信各方彼此信赖时，这种攻击对协议的威胁就显得更为严重，因为攻击者是一个合法用户。通过以上的分析可以看到，TTM 模型不适合用来设计安全域间路由协议。

4 SA-BGP 认证算法

虽然通过第 3 节的分析可以看到，文献[7]中给出的 SE-BGP 存在明显的安全漏洞，但是并不意味着利用 AS 结构的 Rich-Club 特性生成 AS 联盟的不能设计出具有较高安全性和减少证书规模的 BGP 安全机制，本节将利用 AS 结构的 Rich-Club 特性生成 AS 联盟，并设计一种新的 BGP 安全机制? ? SA-BGP (secure aggregation BGP)。

4.1 SA-BGP 概述

SA-BGP 机制利用文献[7]中提出的 AS 联盟生成算法，将网络中的 AS 分成若干的联盟，整个网络拥有一个管理所有关键节点的中心 CA，相关定义如下。

定义 1 AS 联盟：所谓 AS 联盟指的是一组 AS 节点，这组 AS 节点只通过少数的节点与组外其他节点相连和转发流量；这些少数的节点也称为“关键节点”，每个 AS 联盟内有一个独立的 PKI 系统，可以为该联盟内的节点颁发证书，每一个关键节点除了拥有自己联盟颁发的证书外还拥有中心 CA 颁发的数字证书。

定义 2 中心 CA：为所有的关键节点颁发证书，所有的关键节点都可以在其上查询到其他关键节点的证书。

定义 3 *AS_Security_Path*（*ASP*）属性：用于地址源认证和路径认证，用来存放所有经过路径上关键节点相关信息的签名，关键节点需要签名的信息包括关键节点的身份信息、下一节点和时间戳信息。

4.2 基于 RSA 算法的聚合签名算法

S-BGP 和 SE-BGP 均使用 DSA 算法作为签名算法，主要原因是 DSA 算法产生的签名短，但是其验证签名速度慢，而且还需要进行多步骤的运算，所以 DSA 算法不适用于本来收敛速度就缓慢的 BGP 类协议，故 SA-BGP 使用认证速度很快 RSA 算法作为基本签名算法。

聚合签名[8]就是一种能够将 N 个不同的用户对 N 个不同的信息进行的签名聚合成一个短签名的数字签名算法。目前，已经有许多的学者提出了各种不同的聚合签名算法[8~10]，其中还有学者将聚合签名算法应用于安全路由[11]。但是这些聚合签名算法大都是基于双线性映射，由于双线性映射要使用对运算[12~14]速度较慢，且理论研究还不是很成熟，所以文献[15]给出了一种基于 RSA 算法的多签名算法，但是其存在安全问题：无法抵御重放攻击，下面给出一个可抵御重放攻击的基于 RSA 算法的聚合签名算法。

在基于 RSA 签名算法中，假设每个用户 U 拥有数字证书 Crt_U 和其对应的公钥和私钥(k_U，k_U^{-1})，算法分为签名和验证 2 部分，具体运算过程如下。

1) 聚合签名：假设用户 T_1, T_2, L, T_n 分别对 m_1, m_2, L, m_n 进行签名，且假设信息的发送过程是从用户 T_1 到 T_n，按序号依次进行，用户 T_1 为初始签名者，其首先计算 $h_1 = H(m_1, r_1)$ 和 $s_1 = [h_1]k_{T_1}^{-1}$（其中，r_1 为用户生成的时间戳），并将(s_1, m_1, r_1)发送给 T_2，下面的用户对应的聚合签名过程为：当用户 T_i 收到前面用户发送来的 s_{i-1} 和 $r_1, m_1, m_2, \text{L}, m_{i-1}$ 时，计算 $h_i = H(r_1, m_1, m_2, \text{L}, m_i)$ 和 $s_i = [h_i + s_{i-1}]k_i^{-1}$，然后将 $\{s_i, (m_1, m_2, \text{L}, m_i)\ m_1, r_1\}$ 发送给用户 T_{i+1}。

2) 聚合签名验证：当用户 T_{i+1} 收到前面用户发送来的 s_i 和 $r_1, m_1, m_2, \text{L}, m_i$ 时，首先验证时间戳 r_1 的新鲜性，如果是新鲜的那么接着计算 $h_i = H(r_1, m_1, m_2, \text{L}, m_i)$，然后计算 $s_{i-1} = h_i + [s_i]k_i$，依次计算 h_{i-1}、s_{i-2}、L、h_1、s_1，验证计算得到的 h_1 是否等于 $[s_1]k_1$，如果相等则接受签名，否则拒绝该签名。

该算法在基于 RSA 问题的困难性假设下，可以证明方案在随机预言(RO，random oracle)模型[16]下是安全的，并且可以有效地抵御重放攻击。

4.3 SA-BGP 的认证算法

SA-BGP 的认证算法分为联盟内节点间的认证和关键节点间的认证，假设 UPDATE 数据分组为关键节点 T_1 所在的 AS 联盟中的节点 N_1 产生，发送到关键节点 T_n 所在的 AS 联盟中的节点 N'_1，数据分组需要依次经过 T_1 所在的 AS 联盟内的 N_2, L, N_m

到达关键节点T_1，然后数据分组需要经过关键节点$T_2, \perp, T_{n-1}$到达目的关键节点T_n，数据分组需要在关键节点T_n所在的 AS 联盟内依次经过$N'_1, \perp, N'_{l-1}$到达目的节点N'_l。

4.3.1　联盟内节点之间的认证

在同一个安全 AS 联盟内，联盟内有可信的认证中心 CA，所以联盟内的任何节点都可以获取其他节点的地址证书和公钥，具体认证过程如下。

1) N_1产生 UPDATE 报文向N_2通告路由，此时将自己的 AS 号码AS_{N1}加入到路由的路径属性中，这时$AS_PATH=\{\mathrm{AS}_{N1}\}$，并同时生成一个时间戳$r_1$，计算$h_1=H(r_1,\mathrm{AS}_{N1})$和$s_1=[h_1]k_{N1}^{-1}$，修改$ASP=\{r_1,s_1\}$，然后发送给下一跳关键节点$N_2$。

2) N_2收到N_1的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，如果不新鲜则丢弃该数据分组，否则依据计算AS_PATH中的消息查找到其中节点AS_{N1}的证书，并计算$h_1=H(\mathrm{AS}_{N1},r_1)$，和$[s_1]k_1$，看 2 个值是否相同，如果不相同拒绝签名，否则接受签名并使用自己的 AS 号AS_{N2}计算$h_2=H(r_1,\mathrm{AS}_{N1},\mathrm{AS}_{N2})$和$s_2=[s_1+h_2]k_{T2}^{-1}$，然后修改$AS_PATH=\{\mathrm{AS}_{N1},\mathrm{AS}_{N2}\}$，$ASP=\{r_1,s_2\}$，并将修改后的路由通告发送给下一跳节点$N_3$。

$\perp$

$i+1$) N_{i+1}收到N_i的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，如果不新鲜则丢弃该数据分组，否则依据AS_PATH中的消息查找到其中节点$\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Ni}$的证书，并计算$h_i=H(r_1,\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Ni})$，然后计算$s_{i-1}=h_i+[s_i]k_i$，然后依次计算得到$h_{i-1}$、$s_{i-2}$、$\perp$、$h_1$、$s_1$，验证计算得到的$h_1$是否等于$[s_1]k_1$，如果不相等则拒绝该签名，否则接受签名并计算$h_{i+1}=H(r_1,\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Ni+1})$，$s_{i+1}=[h_{i+1}+s_i]k_{i+1}^{-1}$，然后修改$ASP=\{r_1,s_{i+1}\}$，$AS\_PATH=\{\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Ni+1}\}$，并将修改后的路由通告发送给下一跳节点$N_{i+2}$；

$\perp$

$m+1$) T_1收到N_m的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，并依据计算AS_PATH中的消息查找到其中节点$\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Nm}$的证书，并按照聚合签名验证算法的步骤验证签名的正确性，如果正确，那么T_1开始执行关键节点之间的认证算法。

4.3.2　关键节点之间的认证

1) T_1向T_2通告路由，此时将自己的 AS 号码AS_{T1}加入到路由的路径属性中，这时修改路径属性为$AS_PATH=\{path,\mathrm{AS}_{T1}\}$，其中，$path$为数据分组在联盟内所走的路径，计算路径$h'_1=H(path,\mathrm{AS}_{T1},r_1)$和$s'_1=[h_1']k_{T1}^{-1}$，修改$ASP=\{r_1,s'_1,s_1\}$，然后发送给下一跳关键节点$T_2$。

2) T_2收到T_1的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，并依据计算AS_PATH中的消息查找到其中关键节点AS_{T1}和N_1的证书，并按照签名验证算法验证 2 个签名，如果通过验证计算$h'_2=H(path,r_1,\mathrm{AS}_{T1},\mathrm{AS}_{T2})$和$s'_2=[s'_1+h'_2]k_{T2}^{-1}$，修改$AS_PATH=\{path,\mathrm{AS}_{T1},\mathrm{AS}_{T2}\}$，$ASP=\{r_1,s'_2\}$，并将修改后的路由通告发送给下一跳节点$T_3$；

$\perp$

$i+1$) T_{i+1}收到T_i的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，并依据AS_PATH中的消息查找到对应关键节点的证书，按照签名验证算法验证签名，如果通过验证计算$h'_{i+1}=H(path,r_1,\mathrm{AS}_{T1},\mathrm{AS}_{T2},\perp,\mathrm{AS}_{Ti+1})$和$s'_{i+1}=[h'_{i+1}+s'_i]k_{i+1}^{-1}$，修改$ASP=\{r_1,s'_{i+1}\}$，$AS\_PATH=\{path,\mathrm{AS}_{T1},\mathrm{AS}_{T2},\perp,\mathrm{AS}_{Ti+1}\}$，并将修改后的路由通告发送给下一跳节点$T_{i+2}$；

$\perp$

n) T_n收到T_{n-1}的通告路由消息后，检查 ASP 属性中时间戳r_1的新鲜性，并依据计算AS_PATH中的消息查找到其中节点$\mathrm{AS}_{N1},\mathrm{AS}_{N2},\perp,\mathrm{AS}_{Nm}$的证书，并按照聚合签名验证算法的步骤验证签名的正确性，如果正确，那么T_n开始执行联盟内节点之间的认证算法，只是此时的$AS_PATH=\{path,path^+,\mathrm{AS}_{Tn}\}$，其中，$path$为数据分组在关键节点之间所走的路径。

5　SA-BGP 的安全性分析

SA-BGP 具有了以下的安全性质。

定理 1　签名是可认证的。

证明　要证明签名是可认证的，就是证明签名算法必须要保证合法用户的正确签名能够被验证者认证通过，即当用户收到未经篡改的$ASP=\{r,s_i\}$和$AS_PATH=\{\mathrm{AS}_1,\mathrm{AS}_2,\perp,\mathrm{AS}_i\}$，那么通过按照聚合签名认证算法就可以计算得到$h_1$$[s_1]k_1$。

计算过程如下。

1) 计算 $h_i = H(r, \mathrm{AS}_1, \mathrm{AS}_2, \mathrm{L}, \mathrm{AS}_i)$，计算得到 $[s_i]k_i = s_{i-1} + h_i$，可得 s_{i-1}，然后进行下面的计算。

2) 计算 $h_{i-1} = H(r, AS_1, AS_2, \mathrm{L}, AS_{i-1})$，然后可以得到

$s_{i-2} = h_{i-1} + [s_{i-1}]k_{i-1}$；

L；

i-1) 计算 $h_2 = H(r, AS_1, AS_2)$，可得 $s_2 = h_2 + [s_3]k_3$；

i) 计算 $h_1 = H(r, AS_1)$，$s_1 = h_1 + [s_2]k_2$，然后验证 $[s_1]k_1$ 是否等于 h_1。

此时，只要用户接收到数据未经修改，那么最后一定可以得到 $h_1 = [s_1]k_1$。

综上所述，每一个收到正确签名的用户都可以通过对签名进行认证。

定理 2 实现对数据源的安全认证。

证明 实现对数据源的安全认证，主要是要确认宣告地址前缀的源 AS 是否真正拥有该地址前缀，由于 AS 所拥有的数字证书对 AS 的组织号和所拥有的 IP 地址前缀进行了绑定，而私钥是只有合法的 AS 组织独自拥有的，在联盟内传输时，当路由通告到达关键节点时只有通过了关键节点的认证它才会将该路由通告在关键节点之间传输，而签名能够被验证通过意味着该路由通告的发起者拥有其对应的私钥，这也就证明了 AS 的组织号是所拥有该 IP 地址前缀的合法用户，从而实现了对数据源的安全认证。

定理 3 实现对 AS_PATH 的真实性和完整性的安全认证。

证明 要证明对 AS_PATH 的真实性和完整性的安全认证，即是要证明经过恶意的节点修改或伪造的 AS_PATH，都是不能被下一跳节点安全认证。假设某个恶意 *ASi* 将 $AS\_PATH = \{\mathrm{AS}_1, \mathrm{AS}_2, \mathrm{L}, \mathrm{AS}_i\}$ 修改为 $AS\_PATH = \{\mathrm{AS}_1, \mathrm{L}, \mathrm{AS}'_l, \mathrm{L}, \mathrm{AS}_i\}(l < i)$，那么无论其进行签名时使用的是修改过的还是没有修改过的 *AS_PATH*，其签名均无法被下一跳的节点安全认证。

假设恶意的节点签名使用的是没有修改过的 *AS_PATH*，此时用户接收到如下的签名消息为 $ASP = \{r, s_i\}$，经过修改的路经属性为 $AS\_PATH = \{\mathrm{AS}_1, \mathrm{L}, \mathrm{AS}'_l, \mathrm{L}, \mathrm{AS}_i\}(l < i)$，下面用户做如下的验证。

计算 $h'_i = H(r, \mathrm{AS}_1, \mathrm{L}, \mathrm{AS}'_l, \mathrm{L}, \mathrm{AS}_i)$，此时 s'_{i-1} 为 $h'_i + [s_i]k_i = h'_i + h_i + s_{i-1}$，由于 $h'_i \neq h_i$，所以 $s'_{i-1} \neq s_{i-1}$，那么用户在余下的步骤中计算得到 $s'_{i-2} \neq s_{i-2}$、L、$s'_1 \neq s_1$，最后计算得到 $h_1 = [s_1]k_1$，显然有 $h_1 \neq [s'_1]k_1$，从而该签名无法通过认证，说明有人伪造了签名或者修改了路径属性，故拒绝该签名。从而实现了对 AS_PATH 的真实性和完整性的安全认证。

上面证明了消息无论在关键节点之间还是在非关键节点之间的传递都是可以保证 AS_PATH 的真实性和完整性的安全认证，下面考虑消息在第一个关键节点和第二个关键节点之间进行传递时，第一个关键节点是否能够篡改或伪造消息。

T_1 向 T_2 通告路由时，传输的消息为 $ASP = \{r_1, s'_1, s_1\}$，其中 $h'_1 = H(path, \mathrm{AS}_{T1}, r_1)$，$s'_1 = [h_1']k_{T1}^{-1}$，此时 T_2 可以验证 s'_1 和 s_1，如果其中一个无法通过验证那么将会拒绝该消息，再由签名的安全性保证了一旦认证通过那么消息是真实的和有效的。

综上所述，SA-BGP 可以保证对 AS_PATH 的真实性和完整性的安全认证。

定理 4 AS 的身份不能被冒充，签名不可伪造。

证明 攻击者要想冒充合法 AS 的身份或伪造其签名，就必须要获得合法 AS 的私钥。假设攻击者无法窃取到用户私钥，那么攻击者要计算获得用户的私钥这个问题等价于计算大素数分解问题的难解性问题。

定理 5 恶意节点无法进行各种重放攻击。

证明 由于每个合法的用户在做签名时都有时间戳 r 的参与，如果某恶意节点想要冒充用户 T_{i+1}，利用一个先前的签名信息 $ASP = \{r, s_i\}$ 和 $AS\_PATH = \{\mathrm{AS}_1, \mathrm{AS}_2, \mathrm{L}, \mathrm{AS}_i\}$ 发起重放攻击，那么由于下一跳节点在收到该签名信息后首先要验证时间戳 r 的新鲜性，因为攻击者必须要将原来的时间戳 r 修改为当前的时间戳 r'，但是签名 s_i 是用时间戳 r 计算得到的，所以下一跳节点会通过验证算法最终拒绝该签名，从而导致重放攻击失败。

另外，在时间戳的有效时间范围内，如果恶意节点发起重放攻击， 由于恶意节点无法对时间戳及对应的消息进行修改(若修改，则修改后的签名无法通过验证)，所以当接受消息的节点收到之前已经收到了带有相同时间戳的消息(所有的时间戳都是不会相同的)，那么节点将会忽略这条消息，由此可见这样的攻击不会对网络造成危害。

表 1　SA-BGP 、SE-BGP 和 S-BGP 的证书规模

N	C			C_S				
	S-BGP	SE-BGP	SA-BGP	S-BGP	SE-BGP		SA-BGP	
					Key	Nomal	Key	Nomal
23 000	5.29×10^8	5.54×10^6	7.59×10^6	23 000	169	100	330	100
48 000	2.304×10^9	1.86×10^7	2.76×10^7	48 000	244	100	580	100
64 000	4.096×10^9	3×10^7	4.74×10^7	64 000	292	292	100	740

综上所述，恶意节点无法进行重放攻击。

6　可扩展性分析

本节从使用 SA-BGP 将会给网络中路由器需要的证书存储规模和处理 UPDATE 成本 2 个方面来考察 SA-BGP 的可扩展性。

6.1　路由器需要的证书存储规模

对路由器需要的证书存储空间的分析，主要考虑 3 个指标：全网的证书规模 C、单个 AS 节点所需的证书规模 C_s 以及一个证书改变时所影响的 AS 范围 $\overline{C}$。假设互联网中总的 AS 节点的规模为 N，rich 节点的范围为 ß%。对于传统的信任模型，有：$C=N^2$，$C_s=N$，$\overline{C}=N$。

表 1 对比了 SA-BGP、SE-BGP 和 S-BGP 的证书规模。

通过表 1 看出，随着网络中 AS 数目的增多，采用 SA-BGP 比采用 S-BGP 将减少网络中证书的规模，而且其证书规模和 SE-BGP 的证书规模几乎相等。最关键的是采用 SA-BGP 将会大规模地降低单个节点存储的证书数量，证书规模的减小不仅有利于规模的可扩展性，而且会在很大程度上降低由于带外控制而带来的管理开销。

6.2　仿真实验

本节使用 SSFNet 模拟器[17]在相同的网络拓扑、相同的 BGP 行为设置的情况下来评估采用各种安全机制给网络带来的时延和网络的收敛时间[18]。在模拟中，采用了 110 个自治系统的网络拓扑，每个自治系统都只有一个边界路由器构成。每一个 BGP 发言者宣告 2 个前缀，网络拓扑是基于互联网路由表生成[19]。因为 IBSAS 是基于聚合算法的，S-BGP 基于数字证书的，而 SA-BGP 是采用基于数字证书的聚合签名算法的，所以实验中分别模拟 IBSAS、S-BGP 和 SA-BGP 3 种安全机制。

基于相同的安全性仿真实验显示，由于 SA-BGP 随着参与签名的节点数目的增加，SA-BGP 对网络的延时影响最小，当有 6 个节点签名时，SA-BGP 密码操作带来的网络延时仅为 S-BGP 的 1/3，IBSAS 的 1/5。

图 2 中比较了网络中最大连接数节点从网络中断开，然后再重新连接到网络中，网络所需的平均收敛时间。

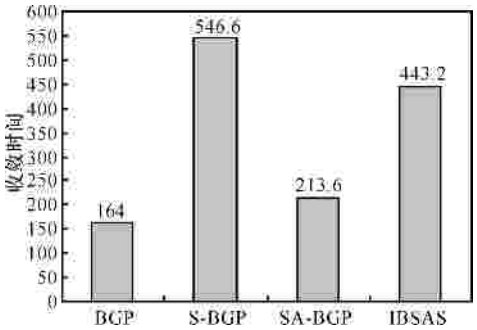

图 2　收敛时间

从以上的分析可以看出，随着互联网 AS 规模的不断扩展，SA-BGP 的全网证书规模、单个 AS 节点所需的证书规模、造成的延时、处理开销以及收敛时间都小于现有的相同安全级别的安全机制。因此，SA-BGP 具有良好的规模可扩展性。

7　结束语

本文研究了文献[7]中提出的一种新的 BGP 安全机制：SE-BGP。该安全机制利用互联网的拓扑连接规律，采用局部 PKI 的认证机制，虽然 SE-BGP 避免了全局集中式认证所带来的负面影响，大规模地降低了网络中节点的证书存储规模，但是由于其提出的 TTM 模型存在安全缺陷，所以使用 TTM 模型设计的安全路由机制也存在明显的安全漏洞。

为了克服 SE-BGP 存在的安全漏洞，基于文献[7]中提出的 AS 联盟的思想，提出了一种基于 RSA 的聚合签名算法，并使用该算法设计了一种新的 BGP 安全机制：SA-BGP，通过分析可以看到，SA-BGP 导致的网络中节点存储的证书数量大致相

同，但是其可以有效地验证AS宣告的网络层可达信息(NLRI)的正确性和AS宣告的路径属性的真实性。最后通过仿真与现有的BGP安全机制IBSAS和S-BGP进行比较，可以看到SA-BGP给网络造成延时和传输信息量的增加比现有的安全机制都要小。

参考文献：

[1] REKHTER Y, LI T. A border gateway protocol 4 (BGP-4)[EB/OL]. http://datatracker.ietf.org/doc/rfc4271/,2006.

[2] MURPHY S. BGP security vulnerabilities analysis[EB/OL]. http://datatracker.ietf.org/doc/rfc4272/,2006.

[3] 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.

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

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

[6] SNBRAMANIAN L, ROTH V, STOICA L, *et al*.Listen and whisper: security mechanisms for BGP[A]. Proc of the 1st Symposium on Networked Systems Design and Implementation[C]. San Francisco, CA, USA,2004.

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

[8] BONEH D, GENTRY C, LYNN B, *et al*.Aggregate and verifiably encrypted signatures from bilinear maps[A]. EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science[C]. Springer-Verlag, 2003.416-423.

[9] GENTRY C, RAMZAN Z. Identity-based aggregate signatures[A]. PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography[C]. Springer-Verlag, 2006.257-273.

[10] LU S, OSTROVSKY R, SAHAI A, *et al*. Sequential aggregate signatures and multisignatures without random oracles[A]. EUROCRYPT 2006[C]. Springer-Verlag, 2006.465-485.

[11] BOLDYREVA A, GENTRY C, O'NEILL A, *et al*. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing[A]. ACM CCS 07: 14th Conference on Computer and Communications Security[C]. 2007.276-285.

[12] KERINS T, MARNANE W P, POPOVICI E M, *et al*. Efficient hardware for the Tate pairing calculation in characteristic three[A]. Workshop on Cryptographic Hardware and Embedded Systems 2005 (CHES 2005)[C]. Edinburgh, Scotland, 2005. 412-426.

[13] SCOTT M. Computing the tate pairing[A]. Proceedings of the RSA Conference: Topics in Cryptology-the Cryptographers' Track (CT-RSA 2005)[C]. Springer-Verlag, 2005.293-304.

[14] SCOTT M, BARRETO P S L M. Compressed pairings[A]. Proceedings of CRYPTO 2004[C]. Springer-Verlag, 2004.140-156.

[15] BONEH D, GENTRY C, LYNN B, *et al*. A survey of two signature aggregation techniques[J]. RSA Crypto Bytes, 2003, 6(2):1-10.

[16] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[A]. The 1st ACM Conference on Computer and Communications Security[C]. 1993.62-73.

[17] The SSFnet project[EB/OL]. http://www.ssfnet.org/homepage.html, 2006.

[18] **赵金晶**,**朱培栋**,**卢锡城**. BGP **收敛性及其对网络性能影响的定量分析**[J].**通信学报**, 2007,28(8):24-33.
ZHAO J J, ZHU P D, LU X C. Quantitative analysis of BGP convergence and its influence on network performance[J]. Journal on Communications, 2007,28(8):24-33.

[19] Multi-AS topologies from BGP routing tables[EB/OL]. http://www.ssfnet.org/Exchange/gallery/asgraph/index.html,2006.

作者简介：

王滨（1978-），男，山东泗水人，浙江大学博士后，主要研究方向为宽带信息网络技术、高性能路由、信息安全。

安金梁（1981-），男，河南郑州人，河南科技学院讲师，主要研究方向为智能计算及人工神经网络和信息安全。

吴春明（1967-），男，浙江萧山人，浙江大学教授、博士生导师，主要研究方向为网络服务质量、可重构网络、网络虚拟化。

兰巨龙（1962-），男，河北张家口人，国家数字交换系统工程技术研究中心教授、博士生导师、总工程师，主要研究方向为高速宽带信息网络技术、网络路由与交换技术、军事信息网络工程。