ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.3, March 2010, pp.505−515
doi: 10.3724/SP.J.1001.2010.03479

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于信誉机制的域间路由安全协同管理方法*

胡 宁+, 邹 鹏, 朱培栋

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Reputation-Based Collaborative Management Method for Inter-Domain Routing Security

HU Ning+, ZOU Peng, ZHU Pei-Dong

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: ning_hu@163.com, http://www.nudt.edu.cn

Hu N, Zou P, Zhu PD. Reputation-Based collaborative management method for inter-domain routing security. *Journal of Software*, 2010,21(3):505−515. http://www.jos.org.cn/1000-9825/3479.htm

Abstract: The main topic of inter-domain routing security management is how to suppress the propagation of untrustworthy routes and malicious routing behaviors. Supervising and evaluating autonomous system's (AS) routing behaviors is a key technology in this topic. This paper designs a distributed collaborative reputation mechanism of trustworthiness evaluation for AS's routing behaviors. The mechanism takes in the statistical results on routing trustworthiness published by AS, uses a self-organizing method, employs posterior probability analysis, and finally calculates a reputation score for a particular AS. The score will be used as a metric on the trustworthiness of the routing information that AS propagates or announces afterwards. In simulations, this reputation mechanism has been shown to effectively contain AS's bad behaviors, and hence improve the overall security of the inter-domain system. The reputation mechanism designed in this research supplies a reference to evaluation and analysis of AS's routing behaviors. It has the following features: It supports incremental deployment. It needn't modify the BGP protocol, so it is easy to be implemented.

Key words: inter-domain routing; security management; reputation; collaborative; self-organize

摘 要: 如何抑制虚假路由的传播和恶意路由行为的发生,是域间路由安全管理的重要研究内容,对自治系统路由行为进行可信性评价和监督是其中的关键技术.设计了一种用于评价自治系统路由行为可信性的分布式协同信誉机制.该机制基于历史路由的有效性统计结果,采用后验概率分析的方法,由多个自治系统按照自组织协同的方式完成对目标自治系统的信誉计算,并将信誉计算结果作为度量该自治系统路由行为可信性的依据.实验结果表明,该机制能够抑制不良路由行为,有效提高域间路由系统的总体安全性,还能够为路由可信性分析和故障诊断提供依据,支持渐进式部署,无须修改 BGP 协议,具有良好的可实施性.

关键词: 域间路由;安全管理;信誉;协同;自组织

中图法分类号: TP393 **文献标识码**: A

* Supported by the National High-Tech Research and Development Plan of China under Grant No.2008AA01A325 (国家高技术研究发展计划(863)); the National Natural Science Foundation of China Grant No.60873214 (国家自然科学基金)

Received 2007-12-07; Accepted 2008-10-06; Published online 2009-04-23

域间路由系统是 Internet 的基础设施,由多个自治系统(autonomous system,简称 AS)互联组成,自治系统是由特定机构独立管理的网络系统,包括若干网络和一组路由器.自治系统之间通过域间路由协议交换网络的路由信息.BGP[1]是目前域间路由协议的事实标准.自治系统通过 BGP 协议能够自由宣告和转发去往不同地址前缀的路由信息,Internet 的连通性在很大程度上依赖于路由系统的安全,因此,域间路由的安全管理显得尤为重要,提高路由可信性是域间路由安全管理的主要研究内容.路由可信性主要包括路由信息可信性以及路由行为可信性.路由信息可信性是指 ISP 传递的路由信息(包括网络前缀和 AS-Path 等路由属性)与实际网络物理拓扑是否一致,常见的路由信息不可信现象有前缀劫持、虚假路由[2].配置错误、恶意攻击和软件故障都可能引起路由信息的不可信.路由行为的不可信是指 ISP 为了维护自身商业利益,在网络流量转发控制中可能存在违背商业合同、不履行流量转发约定或者违背预定流量工程规划等自私行为.含谷底路由、路径延长、热土豆路由等问题都源于 ISP 的自私行为[3].近年来发生的多起路由安全事件[4−6],严重地影响了互联网的可信、可控和可管能力.

现有的研究工作大多通过完善路由协议的安全机制和加强对路由信息的诊断及监测来提高域间路由系统的安全能力,这些工作虽然可以有效地提高单个自治系统的抗路由欺骗的能力,但是没有形成良好的约束和激励机制,对抑制不可信路由的产生和传播缺乏明显的效果.文献[7]的研究结果表明,信誉(reputation)机制具有激励作用,能够有效降低虚假信息的传播速度并抑制欺骗行为,提高系统的整体安全性.从 NANOG[8]近期的会议情况来看,虽然加强自治系统协同已经成为众多运营商的共识,但在现实的网络运营过程中,运营商之间的协同能力较弱,主要的协同方式还局限于管理员论坛、电子邮件、人为会议等,在协同监测、协同管理等方面有待加强.另外,管理信息的共享是制约自治系统之间协同的主要障碍.为了保护商业利益,自治系统的路由策略和路由分析结果往往不便于对外透露,信誉机制为自治系统之间实现信息共享提供了手段.

本文设计了一种用于评价自治系统路由行为可信性的分布式协同信誉机制.该机制基于历史路由的有效性统计结果,采用后验概率分析的方法,由多个自治系统按照自组织协同的方式完成对目标自治系统的信誉计算,并将信誉计算结果作为度量该自治系统路由行为可信性的依据.实验结果表明,该机制能够抑制不良路由行为,有效提高域间路由系统的总体安全性.该机制能够为路由可信性分析和故障诊断提供依据,支持渐进式部署,无须修改 BGP 协议,不依赖 PKI 设施,具有良好的可实施性.

本文第 1 节介绍相关研究工作.第 2 节描述信誉机制的重要概念和关键算法.第 3 节针对域间路由安全管理中的两个典型问题——前缀劫持和虚假路径给出基于信誉机制的协同管理方法.第 4 节是仿真实验及结果分析.第 5 节讨论一些相关问题.最后总结全文.

1 相关研究

目前,针对域间路由安全管理问题的相关研究工作主要分布在控制平面和管理平面.控制平面的研究工作,通过加强 BGP 协议的安全机制来提高路由协议的抗攻击能力,主要的研究成果有 soBGP[9],psBGP[10]和 SBGP[11]等,其中最完整也最有代表性的工作是 SBGP 协议.SBGP 路由信息的传输基于 IPSec,路由会话的保护采用 TCP MD5 等签名机制.路由内容的可信性使用公钥证书和数字签名来验证.上述安全路由协议依赖 PKI 技术来保证信息的可信性,具有良好的计算安全性,但是在具体部署时容易受到性能问题、政治问题等因素的影响[12].同时,由于需要修改 BGP 协议,难以得到众多设备厂商的支持,因此目前并没有得到广泛的应用.管理平面的工作,主要包括对各种分析、诊断、验证和监督技术的研究.文献[13]基于互联网路由注册中心(IRR)提供的路由注册信息和某些已知的全局路由信息对自治系统的路由表进行异常和错误分析,MIT 开发的 RCC 采用多视图的方法检查单自治系统内部的 BGP 配置错误[14].文献[15,16]基于多自治系统协同的思想,提出了对路由信息可信性进行验证和评估的方法.文献[17,18]通过对路由信息进行安全监测来保证域间路由系统的安全.在管理平面的研究成果为建立域间路由系统的信誉机制提供了基础和可行性保障.信誉机制被广泛应用于电子商务[19]、网格[20]、P2P[21]、AD-Hoc[22]等领域,对抑制恶意行为的重复发生和虚假信息的传播扩散具有良好的效果.上述工作为建立适合域间路由系统自身特点的信誉机制提供了参考依据和设计标准.文献[23]提出了一种

通过多自治系统投票来验证路由信息是否可信的方法,该思想具有整体安全性高、易于部署等特点,但是对投票主体的重要性并未加以区分,没有充分挖掘域间路由系统的特色信息,如自治系统规模、商业关系等因素对路由可信性的影响,也没有考虑如何抑制恶意投票等行为.

2 自治系统信誉机制

BGP 是一种策略型路由协议,在路由策略的控制下实施路由信息的宣告、传递和选择.自治系统在配置路由策略时主要考虑彼此的商业关系和商业合同的约束,缺乏评价路由是否可信的依据,因此,难以抑制不可信路由的传播.路由诊断与监测系统虽然能够从现有的路由信息中检测出不可信路由,但是检测结果不能对未来路由选择策略提供指导,也无法阻止不可信路由的宣告者再次宣告新的不可信路由.另外,由于缺乏有效的信息共享手段,即使自治系统的不良行为被发现,其他不了解情况的自治系统仍然可能受到伤害.建立信誉机制有助于解决上述问题:首先,信誉机制根据历史经验信息计算自治系统的信誉,并且用信誉评估其未来路由行为的可信性,这就为制定路由策略提供了参考依据,管理员在配置路由策略时,可以在不违背商业合同的前提下,根据自治系统的信誉来调整路由选择策略,优先选择由高信誉自治系统宣告的路由,过滤或抑制低信誉自治系统宣告的路由,从而达到抑制恶意自治系统的目的;其次,路由攻击行为往往具有一定的连续性,信誉机制具有反馈性,攻击者连续宣告不可信路由会导致其信誉迅速下降,其后续宣告的路由将遭到其他自治系统的拒绝和抑制,从而避免造成不良影响;另外,信誉的计算需要多个自治系统进行协同和交互,不同的信誉评价体现了各自治系统对路由可信性诊断和分析的结果,实现了一种隐式信息共享,有助于提高域间路由系统的整体安全能力;最后,域间路由系统具备建立信誉机制的条件[7],例如:自治系统路由策略的制定受到商业利益的驱动,具有显著的社会行为特征;自治系统作为构成信誉系统的成员,能够长期稳定存在;路由信息是否可信不仅是可以通过路由诊断和监测系统进行判定的客观事实,也是能够表征其宣告者未来路由行为是否可信的评估指标.

2.1 自治系统信誉

信誉在现实社会中用于表达个体在群体心目中的诚信程度,文献[7]对信誉的描述是:某实体的信誉是指在给定时刻和上下文环境下,根据其他实体的观察或该实体历史行为的信息对其未来行为的预期.该定义强调了信誉的上下文相关性,指出信誉的形成来源,同时也说明了计算实体信誉的目的在于根据其历史行为信息预测其未来的行为.根据上述理解,我们结合域间路由系统自身特点和路由安全管理的需求,给出了自治系统信誉的定义和约束说明.

定义 1(直接评价). 自治系统 A 对 B 的直接评价是指 A 根据对 B 历史路由行为的直接观察经验,对 B 未来路由行为可信程度的预期.

在本文中,自治系统 A 对 B 历史路由行为的直接观察经验主要是指在 A 收到来自 B 的历史路由信息中真实路由和虚假路由的统计结果,该统计结果由 A 自己产生.由于在域间路由系统中,只有具备某种商业邻居关系的自治系统之间才会彼此交换路由,因此,直接评价只存在于具有商业邻居关系的自治系统之间.

定义 2(信誉评价). 信誉评价是信誉被量化的结果,自治系统 A 对 B 的信誉评价是指 A 在综合多个自治系统对 B 的直接评价的基础上得到的对 B 未来路由行为可信程度的预期.

直接信誉评价是最终形成信誉评价的要素,而信誉评价则是多项直接评价的综合结果.在本文中,直接评价和信誉评价的取值被映射到实数区间[0,1]:自治系统的评价值为 1 表示评价值提供者认为由该自治系统宣告的路由完全可信;反之,则表示完全不可信;评价值介于 0 和 1 之间则表示可信的程度.

定义 3(评价咨询和评价推荐). 评价咨询是指自治系统从其他自治系统处获取对目标自治系统的直接评价或信誉评价的询问行为.评价推荐是指自治系统在收到评价咨询后,对咨询予以应答的行为.

定义 4(评价者、被评价者和评价推荐者). 评价者、被评价者和评价推荐者是指自治系统在信誉评价计算过程中可能担任的 3 种角色:当自治系统在计算或者进行评价咨询时,它的角色是评价者;当自治系统成为被评价目标时,它的角色是被评价者;当自治系统在进行评价推荐时,它的角色是评价推荐者.

在图 1 中,自治系统 A,C,D 与 B 有邻居关系,设它们对 B 的直接评价分别为 $D\_E_{A\to B}$,$D\_E_{C\to B}$,$D\_E_{D\to B}$,自治

系统 A 在计算对 B 的信誉评价($R\_E_{A\to B}$)时,向 C 和 D 咨询 $D\_E_{C\to B}$ 和 $D\_E_{D\to B}$,A 综合 $D\_E_{A\to B}$,$D\_E_{C\to B}$,$D\_E_{D\to B}$ 得到 $R\_E_{A\to B}$,记为 $R\_E_{A\to B}=D\_E_{A\to B}\oplus D\_E_{C\to B}\oplus D\_E_{D\to B}$.自治系统 F 在计算对 B 的信誉评价($R\_E_{F\to B}$)时,由于 F 和 B 之间没有邻居关系,所以 $R\_E_{F\to B}=D\_E_{C\to B}\oplus D\_E_{D\to B}$.自治系统 E 在计算对 B 的信誉评价时,因为信任 A,为了降低计算和通信开销,E 直接询问 A 对 B 的信誉计算结果,此时,$R\_E_{E\to B}=R\_E_{A\to B}$.在计算 $R\_E_{A\to B}$ 和 $R\_E_{F\to B}$ 的过程中,A,C,D 和 F 的角色是评价者,B 是被评价者;当 A 向 C 和 D 咨询时,C 和 D 还承担了评价推荐者的角色.在计算 $R\_E_{E\to B}$ 时,E 是评价者,B 是被评价者,A 则是评价推荐者.

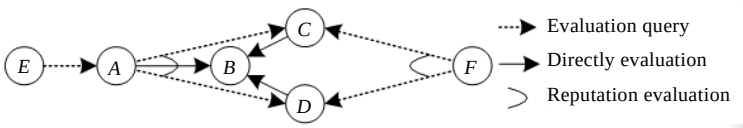


Fig.1 Illustration of reputation evaluation

图 1 信誉评价计算示意图

2.2 直接评价

根据对无效路由的分析[24]以及 NANOG 提供的管理员邮件列表(operator mail list)[8]中对路由错误的调查情况来看,不可信路由的出现具有随机性,一旦出现又会表现出一定的连续性.例如,某 ISP 的管理员在配置路由策略时可能出现错误,这种配置错误的发生是一个随机事件,但是如果发生了,在未来的一段时间内都可能由于管理员的原因导致新的配置错误的发生.鉴于此,我们将某自治系统是否宣告了一条真实路由视为一个二项事件,如果真实,则称为肯定事件,否则,称为否定事件.根据二项事件的后验概率分布服从 Beta 分布的特性[25],在已知肯定事件次数和否定事件次数的情况下,可以计算出该自治系统下一次宣告真实路由的概率,并以此方法计算评价者对被评价者的直接评价[26].令 r_t 和 s_t 分别表示在过去 t 时间里自治系统 B 产生的肯定事件次数和否定事件次数,p 表示自治系统 B 下一次产生肯定事件的概率,则 p 的概率密度函数可以用伽玛函数(Γ)表示为

$$\varphi(p\mid r_t,s_t)=(\Gamma(r_t+s_t+2)/(\Gamma(r_t+1)\times\Gamma(s_t+1)))\times p^{r_t}\times(1-p)^{s_t},\ 0\le p\le 1,r_t\ge 0,s_t\ge 0 \tag{1}$$

我们采用 p 的期望值作为自治系统 A 对 B 的直接评价($D\_E_{A\to B}$):

$$D\_E_{A\to B}=E(\varphi(p\mid r_t,s_t))=(r_t+1)/(r_t+s_t+2) \tag{2}$$

鉴于对路由有效性的监测与诊断研究工作已经取得了良好的结果[13,14,17,24],本文假设在计算直接评价时能够通过路由监测系统获得自治系统发布不真实路由的列表和统计情况.在统计 r_t 和 s_t 时,仅统计过去 t 时间内的情况,这样做的好处是,使得直接评价方法具有一定的时间遗忘效应,发生在 t 时间以前的否定事件将不被引入计数.通过时间遗忘效应,自治系统的信誉评价不会因为偶然的错误配置而长期受到影响.

直接评价的准确性与对不真实路由的统计结果相关,而信誉评价的最终形成又依赖直接评价,为了向直接评价的使用者提供一个能够反映出本次直接评价结果准确性的指标,我们引入直接评价可采纳度(τ).

定义 5(直接评价可采纳度). 直接评价提供者对本次直接评价准确程度的评估.直接评价可采纳度(τ)的取值范围是[0,1]区间,当直接评价可采纳度为 0 时,表示本次评价值不值得采纳;为 1 时,表示本次评价值可以完全采纳;介于 0 和 1 之间表示在采纳该值时,需要进行一定比例的衰减.

由公式(2)可知,直接评价依赖肯定事件计数(r_t)和否定事件计数(s_t)的取值,而路由监测系统是否能够提供准确的路由检测结果又与 IRR 路由注册信息、自治系统路由表采样等数据是否准确和全面有关.为了体现这种差异,将直接评价可采纳度的计算函数定义为一个与路由检测结果准确度相关的函数.我们假设路由监测系统能够提供路由检测结果的准确度评估值,则直接评价可采纳度公式定义如下:

$$\tau=\begin{cases}1-\alpha^{(\theta-\mu)}, & 0\le\alpha\le 1,\mu\le\theta\le 100\\ 0, & 0\le\theta\le\mu\end{cases} \tag{3}$$

式(3)中,θ表示路由检测结果的准确度评估值,取值范围是[0,100],μ为最低阈值,α为衰减因子.当θ低于μ时,本次的直接评价将被丢弃;当θ高于μ时,τ越趋近于 1,则表示直接评价值越准确.

2.3 信誉评价

信誉评价是对直接评价的融合,利用了互联网拓扑结构的丰富连接特性(richly connected topology),能够发挥自治系统协同管理的优势,实现了隐式信息共享,有效避免了单点欺骗.其次,不同自治系统之间的路由策略受商业关系的约束,有些无效路由可能被路由过滤器(route filter)所屏蔽,无法被路由监测系统发现,此时,单个自治系统提供的直接信誉评价可能无法准确反映被评价者路由行为的可信性.最后,没有邻居关系的自治系统之间由于没有路由交换,无法对对方做出直接评价.本节阐述信誉机制需要解决的 3 个问题:直接评价推荐者的选择、恶意评价的预防和筛选以及直接评价的融合.

2.3.1 构造推荐者集合

推荐者集合构造算法应该具备随机性、反馈性和收敛性.随机性是指同等条件的自治系统被选为推荐者的可能性基本相同,反馈性是指自治系统被选为推荐者的可能性随着其恶意推荐行为的增加而减少,收敛性是指算法应该在多项式时间内完成推荐者集合的构造.为了防止和抑制合谋欺骗或恶意评价,评价者为每个推荐者维护一个恶意推荐行为计数器(σ)用于记录推荐者曾经发生的恶意推荐行为次数.关于恶意推荐行为的检测方法将在第 2.3.2 节介绍.我们假设自治系统能够通过互联网路由注册中心(IRR)提供的路由注册信息产生整个网络的拓扑结构图[27].在此基础上,直接评价推荐者集合的构造算法设计如下:

Step 1:根据网络拓扑图生成满足如下约束条件的被评价者邻居节点列表(L):

1) L 中所有元素的σ均小于恶意推荐行为计数上限($\sigma_{\max}$);

2) L 按σ作升序排列;

Step 2:若 L 为空,则跳转至 Step 6;

Step 3:将推荐者集合(RS)初始化为空集$\varnothing$;

Step 4:若RS最大容纳元素个数(S_{RS})大于L元素个数(S_L),则将L全部节点加入RS,跳转至Step 6;

Step 5:抽取 L 中前 S_{RS} 个元素加入到 RS 中(若存在两个σ值相同的元素,则从中随机选取一个);

Step 6:返回 RS,算法结束.

上述算法中,当推荐者集合为空或元素过少时可以通过降低$\sigma_{\max}$的取值来增加推荐者集合元素的个数.

2.3.2 直接评价综合

为了防止不准确或恶意评价对信誉计算造成的影响,需要对推荐者返回的直接评价进行筛选.对历史路由的监测是否完全会影响直接评价的准确度,例如:自治系统之间的路由策略受彼此商业关系的影响,某些推荐者可能没有收到被评价者发布的无效路由,从而对被评价者给出较高的直接评价.恶意评价是指自治系统为了特定目标故意提供偏低或者偏高的直接评价值.为了标识恶意评价,在数据筛选时,采用索要证据的方法对评价值的有效性进行确认.根据第 2.2 节介绍的直接评价计算方法可知,在计算被评价者的直接评价时,需要使用被评价者的否定事件计数(s_t).由于假设了路由监测系统在提供否定事件计数时,还提供与否定事件相关的具体路由,该路由称之为证据.显然,当 $s_t>0$ 时,一定存在相关的证据.由于评价咨询者在获取了评价推荐者提供的证据后,可以通过咨询确认等有效技术手段对该证据的有效性进行检验,因此对于恶意评价者而言,制造这种证据是困难的.基于大多数自治系统都是诚实的这一假设,本文使用聚类分析的方法来确定离群点,对于评价偏高的离群点直接丢弃,对于评价偏低的离群点则向提供者索取证据.基于上述分析,本文设计数据筛选算法如下:

Step 1:将直接评价集合(S_{DE})初始化为空集$\varnothing$;

Step 2:将可采纳度(τ)大于或等于$\tau_{\min}$的直接评价加入直接评价集合(S_{DE});

Step 3:标识直接评价集合(S_{DE})中的离群点,如果没有发现离群点则跳转 Step 5;

Step 4:对于 S_{DE} 中所有的离群点(x)作如下处理:

1) 若x是偏低的离群点,则向提供该值的推荐者发送证据获取请求,若未收到有效证据,则视x为恶意推荐,将x从S_{DE}中剔除且推荐者的σ加1;

2) 若x是偏高的离群点,则直接从S_{DE}中剔除;

Step 5:返回 S_{DE},算法结束.

在完成对数据的筛选处理后,使用加权求和的方法对直接评价进行综合,计算公式如下:

$$R\_E_{A\to B}=\sum_{i=1}^{n}\left(D\_E_{i\to B}\times\left(\varpi_i\Big/\sum_{i=1}^{n}\varpi_i\right)\right) \tag{4}$$

上式中,采用推荐者的邻居节点数在所有推荐者邻居节点数总和的比例作为权重因子,ϖ_i 表示第 i 个推荐者的邻居节点数.这样做是基于如下考虑:(1) 邻居节点越多的节点,其收到的路由数量也越多,这就为路由监测系统提供了更为完全的检测样本;(2) 连接度数越大的节点成为推荐者的次数也会越多,如果该节点能够被第 2.3.1 节的推荐者集合构造算法选中,表示其进行恶意推荐的可能性很少,因此应该获得较高的权值;(3) 连接度数大的节点往往是服务供应商节点,这些节点的网络管理水平较高,对不可信路由的检测能力也很强,而且为了争取更多的用户市场,这些节点会努力维护自身的可信形象,因此更值得信赖.

2.4 AS信誉联盟

采用分布式体系结构建立信誉系统虽然具有很好的健壮性,但是对单个自治系统节点要求较高,各个节点需维护大量评价信息,多次重复计算引起的存储和通信开销较大.为了弥补这一不足,我们基于自组织思想提出一种构建 AS 信誉联盟以及基于 AS 信誉联盟来实现信誉评价的共享方法.通过 AS 信誉联盟这种组织形态将众多自治系统组织成多个小群体,通过盟主节点在盟员节点之间实现信誉评价共享.对于盟员节点来说,加入信誉联盟能够有效降低自身被询问直接评价的次数;对于盟主节点来说,能够聚集更多的自治系统,扩大自己的客户范围,是一种双赢的形式.在基于信誉联盟的信誉计算过程中,信誉评价的传递只经历一跳,盟主节点在众多盟员节点的监督下实施信誉评价推荐,具有很好的安全性.

定义 6(AS 信誉联盟). AS 信誉联盟是一组彼此存在可达路由的 AS 节点按照自组织方式形成的一个集合体,每个集合体有一个盟主节点,盟主节点负责计算和存储本联盟内成员(简称盟员)的信誉评价,同时还负责响应来自其他自治系统的信誉评价咨询.

图 2 给出了 AS 信誉联盟的结构示意图, 图 2(a)是未建立信誉联盟时的网络拓扑结构图,在图 2(b)中自治系统形成了 *AA*1,*AA*2 和 *AA*3 等 3 个联盟,每个联盟由盟主节点负责创建,盟员按照自愿的原则加入或退出联盟,盟员可以同时属于多个联盟.通常情况下,盟主节点由一些枢纽节点担任.

Step 1:若评价者是盟主节点:

1) 若被评价者属于自己管理的联盟,则跳转 Step 3;
2) 以广播方式询问所有盟主节点,确定被评价者所属联盟;若被评价者不属于任何联盟则跳转 Step 3;
3) 从被评价者所属联盟的盟主节点处获取被评价者的信誉;跳转 Step 4;

Step 2:若评价者是盟员节点:

1) 若评价者属于某联盟,则向其所属联盟的盟主节点询问被评价者的信誉;跳转 Step 4;
2) 若评价者不属于任何联盟,则跳转 Step 3;

Step 3:按第 2.3 节的方法计算被评价者信誉;

Step 4:返回结果,算法结束.

信誉联盟的构建方法描述如下:

Step 1:盟主节点将盟员节点集合(AA)初始化为空集∅;

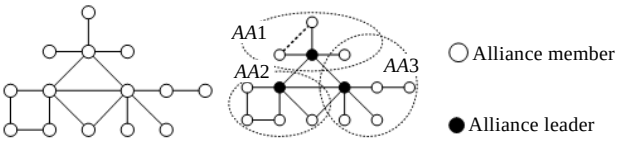
Step 2:盟主节点根据本地 BGP 路由表,选择与自己 *AS_PATH* 距离小于阈值 *n* 的自治系统,并向其发出加盟邀请;

Step 3:收到邀请的自治系统通过计算兴趣函数 $Ins{:}s\times r\times d\to\{0,1\}$来决定是否接受加盟邀请.函数返回 0 表示拒绝邀请,返回 1 表示接受邀请.s 表示邀请者规模,当邀请者的 BGP 邻居数小于自己的 BGP 邻居数时返回 0,否则返回 1;r 表示邀请者的推荐信誉,当邀请者的恶意行为推荐计数大于阈值(δmax)时返回 0,否则返回 1;d 表示去往邀请者的优选 BGP 路由的 AS_PATH 距离,若大于指定阈值则返回 0,否则返回 1.

Step 4:若盟主节点收到接受加盟邀请应答后,将应答者加入到联盟成员名单中.

上述算法具有自组织特性,自治系统会选择值得信赖的联盟加入,有相同利益的自治系统会被组织在一起,

信誉联盟能够随着自治系统之间商业关系的变化进行自我调整,具有良好的自我成长、自主演化能力.



(a) AS topology (b) AS reputation alliance
(a) AS 拓扑结构 (b) AS 信誉联盟划分

Fig.2 AS topology and alliance division

图 2 AS 拓扑结构与信誉联盟划分

2.5 性能分析

基于信誉联盟这种组织形态实现信誉评价的计算和存储,能够有效降低单个自治系统在计算所有其他自治系统信誉评价时引起的存储开销,以及所有自治系统在计算同一自治系统信誉评价时引起的通信开销.为了便于分析,表 1 给出了分析过程需要用到的变量及符号说明.

Table 1 Definition and description of variables

表 1 变量定义及说明

$SCost.DE$	Storage cost for a direct evaluation and belief discounting
$SCost.RE$	Storage cost for a reputation evaluation
$SCost.\sigma$	Storage cost for a counter of malicious recommendation
$CCost.DE$	Communication cost for a direct evaluation query which includes query and acknowledge, evidence requirement and evidence acknowledge
$AvgD$	Average count of neighbors
n	The total number of AS

当不使用 AS 信誉联盟时,存储和通信开销为

$$TSCost.RE=(AvgD\times(SCost.DE+SCost.\sigma)+SCost.RE)\times(n-1) \tag{5}$$

$$TCCost.RE=(AvgD\times CCost.DE)\times(n-1) \tag{6}$$

使用 AS 信誉联盟时(假设只有一个信誉联盟),盟主节点和盟员节点的存储开销分别为

$$TSCost.RE=(AvgD\times(SCost.DE+SCost.\sigma)+SCostRE)\times(n-1) \tag{7}$$

$$TSCost.RE=SCostRE\times(n-1) \tag{8}$$

在使用 AS 信誉联盟时,盟员节点的通信开销为

$$TCCost.RE=(AvgD\times CCost.DE)+(n-1)\times CCost.DE \tag{9}$$

据 AS65000 提供的统计数据[28],截止 2008 年 8 月 26 日,域间路由系统的自治系统总数为 29 167 个,平均每个自治系统的连接度数为 3.2.设每个变量占用存储空间为 4 字节,则式(5)的计算结果为 1 166 640 字节,而式(8)的计算结果为 116 664 字节,存储开销降低了 90%.式(6)的计算结果为 349 992 次,而式(9)的计算结果为 29 178 次,通信开销降低了 91.6%.式(7)的结果虽然和式(5)一样,但这是在假设只有一个信誉联盟的情况下,随着信誉联盟数的增加,这部分存储开销将被分散到多个盟主节点承担.

2.6 部署与实施

域间路由安全管理信誉机制(AIRS)在具体部署实施时如图 3 所示.

在图 3 中,AIRS 由部署在多个自治系统上的信誉评价代理(RA)组成,RA 彼此独立运行,负责实现信誉计算以及与其他自治系统代理之间的协同.RA 之间的通信协议建立在应用层 TCP 协议之上,各自治系统的路由监测系统 M 通过侦听 BGP 的 Update 消息来收集路由信息.当发现虚假路由时,形成虚假路由名单提交给 RA,RA 在收到新的虚假路由名单时,重新计算对相应自治系统的直接评价.直接评价的计算与信誉评价的计算彼此独立进行.以图 3 为例,当自治系统 A 需要计算对自治系统 B 的信誉评价时,处理过程如下:

Step 1:RA_A 获取对 B 的最新直接评价($D\_E_{A\to B}$);

Step 2:RA_A 向 RA_C 发送直接评价咨询,获取 C 对 B 的最新直接评价($D\_E_{C\to B}$);

Step 3:RA_C 收到咨询请求后,向 RA_A 返回对 B 的最新直接评价值($D\_E_{C\to B}$);

Step 4:RA_A 收到 $D\_E_{C\to B}$ 后,按照第 2.3 节的算法计算 $R\_E_{A\to B}$,处理结束.

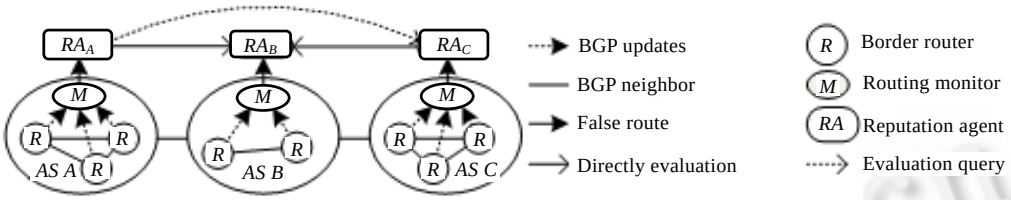


Fig.3 Architecture of AIRS

图 3 AIRS 系统结构

3 域间路由安全管理应用

网络地址前缀起源保护(prefix origin protection)和 BGP 路径保护(BGP path protection)[12]是域间路由安全管理的两个核心问题,前缀劫持和虚假路由是这两个问题的典型代表.目前的路由监测工具虽然能够识别前缀劫持和虚假路由,但是没有考虑如何抑制和预防这类行为的再发生.本节基于信誉机制提出一种方法,用于预防和抑制同一自治系统多次实施前缀劫持和虚假路由攻击.

3.1 前缀劫持

前缀劫持是指恶意自治系统通过宣告不属于自己的地址前缀路由来破坏网络连通性的攻击行为.这种行为往往具有一定的连续性和重复性,将信誉机制与路由前缀劫持监测工具相结合,能够实现对前缀劫持行为的预防和抑制.基于信誉机制的前缀劫持防御方法描述如下:

Step 1:当前缀劫持监测工具检测到某邻居有前缀劫持行为时,向信誉评价代理提交虚假路由报告;

Step 2:信誉评价代理重新计算对该邻居的直接评价;

Step 3:当自治系统收到来自邻居自治系统的路由宣告消息时,按照如下规则处理:

1) 若发生地址前缀冲突(MOAS),则由信誉评价高的自治系统宣告的路由被优先选择;

2) 若自治系统的信誉评价值低于可信任阈值,则抑制该路由的传播,直到该路由被确认可信.

实施前缀劫持攻击的恶意节点如果连续实施前缀劫持,将导致自己的信誉评价迅速下降,其发布的地址前缀将被拒绝;如果该恶意节点企图通过减少前缀劫持的次数,甚至发布正确的路由信息来提高自己的信誉评价,又会增加自己的攻击开销,延长了攻击时间.

3.2 虚假路由

虚假路由是指 *AS_PATH* 属性与真实的网络拓扑结构不一致的路由,路由信息在传播过程中,如果 *AS_PATH* 属性被篡改,会导致虚假路由的产生.当自治系统收到虚假路由时,由于缺乏参考信息,往往不能马上识别出来,为路由选择和转发带来困难.利用信誉评价信息能够帮助自治系统识别和抑制虚假路由的传播.由第 2 节提出的信誉计算方法可知,有过路径伪造行为的自治系统其信誉值会有所降低,因此,可以利用信誉评价来指导路由选择和转发,处理方法描述如下:

Step 1:自治系统 A 收到来自 AS_1 的 *AS_PATH* 为{AS_1,…,AS_n}的路由;

Step 2:依次计算 *AS_PATH* 包含的自治系统的信誉评价值{E_R_1,…,E_R_n};

Step 3:若 Min(E_R_1,…,E_R_n)低于可信任阈值,则抑制该路由传播,直到该路由被确认有效为止;

Step 4:否则,接受该路由.

4 仿真及结果分析

为验证本文所提机制的合理性,我们设计了一个与实际应用相近的网络拓扑结构,在此拓扑结构下进行了模拟实验,本实验需要验证的结果与具体的自治系统无关,因此并不使用真实的自治系统编号.

4.1 网络拓扑与实验设计

如图 4 所示,*A*~*F* 分别代表不同的自治系统,它们之间的商业关系在图中已标出.*B* 是一个恶意节点,它希望劫持 *E* 的地址前缀,随着 *E* 不断宣告新的地址前缀路由,*B* 也不断向 *A* 宣告相同的地址前缀路由.根据第 3.1 节介绍的方法,*A* 需要计算 *B* 和 *E* 的信誉评价.*F* 是一个多宿主(multi-homing)节点,*E* 和 *G* 在争夺 *F* 成为它们的客户,*G* 为了自己的利益,对 *E* 有恶意推荐行为.*B* 向 *A* 宣告的劫持路由不向 *D* 宣告.在上述情况下,我们分别从 *B* 和 *E* 注入路由,在初始状态下,所有节点的信誉评价和直接评价缺省值为 1,*A*,*C*,*D*,*F*,*G* 的路由表中各有 1 000 条路由, *E* 和 *B* 每次宣告 50 条新的地址前缀路由,其中 *E* 宣告的路由为真实路由,*B* 宣告的路由为虚假路由.我们假设 *B* 宣告的虚假路由能够被路由监测系统发现,经过 20 次路由更新后,观察 *A* 对 *B* 和 *E* 的信誉评价的变化.

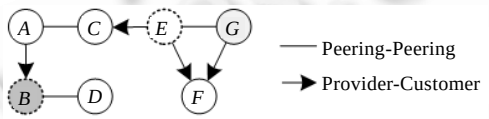


Fig.4 AS topology and relationship of simulation environment

图 4 仿真实验拓扑结构图

4.2 结果分析

从图 5 所示的实验结果可以看出,随着 *AS B* 不断向 *A* 宣告不可信路由,*A* 对 *B* 的直接评价开始下降,由于 *B* 没有向 *D* 宣告不可信路由,*D* 对 *B* 的直接评价没有发生变化,这表明评价者在构造评价推荐者集合时,应该尽可能地公平和全面,以免受到主动或者被动恶意推荐行为的影响.另外,虽然在开始阶段 *A* 对 *B* 的信誉评价值高于对 *E* 的信誉评价值,但是随着 *B* 不断向 *A* 发布不可信路由,*A* 对 *B* 的信誉评价开始迅速下降并且低于对 *E* 的信誉评价,此时,当 *A* 再次收到来自 *B* 的前缀路由信息时,将抑制或者拒绝接受,通过信誉机制使得路由选择策略具备了自学习的能力.从实验结果中我们还注意到,虽然 *G* 对 *E* 实施了恶意推荐,但是由于 *E* 另外的邻居节点 *C* 和 *F* 能够为其提供公正的评价,因此能够保证自治系统 *E* 的信誉评价值维持在一个较高的水平.在本实验中,我们没有启动恶意推荐行为检测机制,事实上,如果启动恶意推荐行为检测机制,自治系统 *E* 的信誉评价会更高,*A* 对 *B* 的抑制会更加提前.信誉评价值在辅助自治系统选择路由时,不仅可以帮助自治系统直接拒绝和抑制来自信誉低的自治系统的路由,也可用于多个信誉相当的自治系统间的路由的比较和选择.

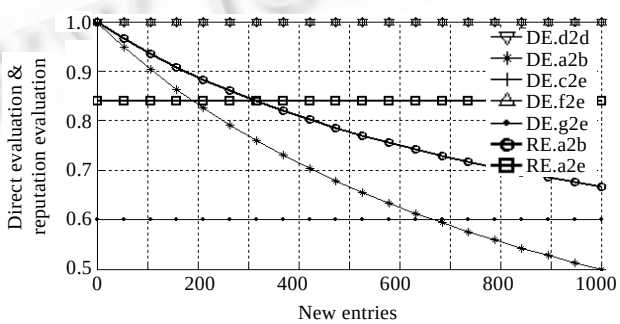


Fig.5 Directly and reputation evaluation curves from *AS B* to *E*

图 5 *AS B* 和 *E* 的直接评价和信誉评价变化曲线

5 讨 论

5.1 评价更新

路由监测系统对虚假路由统计分析结果的更新会导致直接评价的更新,而路由监测系统的统计分析又会受到 IRR 路由注册信息、BGP 路由、自治系统商业关系、网络拓扑等因素变化频率的影响.因此,直接评价的更新独立于信誉评价的计算,在更新后不主动广播,以免造成震荡.信誉评价采用按需更新.当自治系统需使用路由发布者的信誉评估路由信息的可信性时,会触发信誉计算.从 AS65000 BGP 路由表的统计结果来看,平均每小时会有 2 368.022 条路由表项被更新,其中包括 215.091 条新表项、86.844 条撤销表项和 2 066.087 条更新表项[28].显然,如果分析每条路由表项都重新计算自治系统的信誉会引起较大的通信开销.为提高性能,每个自治系统的信誉评价值具有一定的有效期,在有效期内的信誉评价只更新一次.

5.2 恶意评估监测

ISP 之间是一种竞争型合作关系,在计算信誉评价时可能存在恶意评价行为.本文在抗恶意评价机制方面主要从构造推荐者集合、设置直接评价可采纳度、设置恶意推荐行为记数器、索取评价证据以及采用加权求和的方式抑制单点欺骗等机制来防御和抑制恶意评价行为.除此以外,通过使用一些新的数理统计模型或分析方法,如聚类分析等也可以提高信誉评价的准确值.尽管如此,并不能彻底杜绝恶意评价行为的发生,尤其是在多个自治系统合谋攻击的情况下.为此,还应该加强除信誉机制以外的其他协同管理技术的研究.

5.3 信誉机制与可信路由

基于信誉机制实现域间路由的安全管理是一种采用非加密技术解决路由安全问题的方法,虽然不具备绝对可信性,但是这种方法能够有效促进域间路由系统向更为健康的方向演化.域间路由系统以 ISP 作为基本的行为实体,ISP 之间的信任关系是可信域间路由信息传递的保证,是域间路由系统健康运行与和谐演化的基础.域间路由系统的信誉机制不但为 ISP 之间实现信息共享、进行有效的协同管理和联合安全防护提供有效的支持,还有利于规范 ISP 的行为、避免单边控制和恶意行为,实施全局优化的协同流量工程.

6 结论及工作展望

域间路由安全管理是目前的研究热点,ISP 协同是提高域间路由系统的整体安全能力的重要手段.本文借鉴开放网络和分布式系统安全问题的研究成果,结合域间路由系统安全管理的需求和特殊性,设计了一种面向域间路由安全协同管理的信誉机制.该机制兼顾了公平性、主观性、安全性、实时性等要求,能够有效地避免评估者的武断和不公平投票行为,支持评价者信任策略的实施,能够抵御合谋攻击,能够反映 ISP 行为表现的时间特性,所提出的 AS 信誉联盟能够有效降低通信和存储开销,具有良好的可扩展性.信誉机制为自治系统在进行路由选择和可信路由评估时提供了参考,使得现有的域间路由安全管理体系更为完善.如何设计更为健全的信誉评价体制、信任联盟管理方法以及如何利用信誉体制开发新的安全管理应用将是我们下一步的研究内容.

致谢 在此,我们向审稿老师严谨的评审以及对本文提出很多建设性的意见表示诚挚的感谢.对学报编辑老师的辛勤工作表示由衷的感谢.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol (BGP Version 4). IETF Internet RFC, RFC 4271. 2006.

[2] Butler K, Farley T, McDaniel P, Rexford J. A survey of BGP security. 2005. http://www.patrickmcdaniel.org/pubs/td-5ugj33.pdf

[3] Roughgarden T. Selfish routing [Ph.D. Thesis]. Cornell University, 2002.

[4] Bono VJ. 7007 explanation and apology. 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html

[5] Popescu AC, Premore BJ, Underwood T. Abstract: Anatomy of a leak: AS9121. 2005. http://www.nanog.org/mtg-0505/underwood.html

[6] Brown MA. Pakistan hijacks YouTube: A closer look. 2008. http://www.circleid.com/posts/82258_pakistan_hijacks_youtube_closer_look

[7] PResnick P, Zeckhauser R, Friedman E, Kuwabara K. Reputation systems: Facilitating trust in Internet interactions. Communications of the ACM, 2000,43(12):45−48.
[8] The North American Network Operators' Group. 2008. http://www.nanog.org/
[9] White R. Securing BGP through secure origin BGP (soBGP). The Internet Protocol Journal, 2003,6(3):15−22.
[10] Wan T, Kranakis E, Oorschot PCv. Pretty secure BGP (psBGP). ACM Trans. on Information and System Security (TISSEC), 2007, 10(3):1−41.
[11] Kent S, Lynn C, Mikkelson J, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000,18(4):582−592.
[12] Murphy S. BGP security vulnerabilities analysis. IETF Internet RFC, RFC 4272, 2006.
[13] Siganos G, Faloutsos M. Analyzing BGP policies: Methodology and tool. In: Li VOK, ed. Proc. of the 23rd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2004). Hong Kong: IEEE Press, 2004. 1640−1651.
[14] Feamster N, Balakrishnan H. Detecting BGP configuration faults with static analysis. In: Vahdat A, ed. Proc. of the 2nd Symp. on Networked Systems Design & Implementation (NSDI 2005). Boston: USENIX Press, 2005. 43−56.
[15] Goodell G, Aiello W, Griffin T. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Neuman C, ed. Proc. of the ISOC NDSS 2003. San Diego: National Security Agency Press, 2003. 75−85.
[16] Pei D, Lad M, Zhang B, Massey D, Zhang LX. Route diagnosis in path vector protocols. 2004. http://www.cs.colostate.edu/~massey/pubs/tr/massey_uclatr040039.pdf
[17] Lad M, Massey D, Pei D, Wu Y, Zhang B, Zhang LX. PHAS: A prefix hijack alert system. In: Keromytis AD, ed. Proc. of the 15th USENIX Security Symp. (Security 2006). Vancouver: USENIX Press, 2006. 153−166.
[18] The RIPE NCC MyASN service. 2008. http://www.ris.ripe.net/myasn.html
[19] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2007, 43(2):618−644.
[20] Silaghi GC, Arenas AE, Silva LM. Reputation-Based trust management systems and their applicability to grids. 2007. http://www.coregrid.net/mambo/images/stories/TechnicalReports/tr-0064.pdf
[21] Cornelli F, Damiani E, Vimercati SDCd. Choosing reputable servents in a P2P network. In: Lassner D, ed. Proc. of the 11th Int'l World Wide Web Conf. (WWW 2002). Hawaii: World Wide Web Conf. Committee Press, 2002. 376−386.
[22] Michiardi P, Molva R. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Blazic BJ, ed. Proc. of the Communications and Multimedia Security 2002. Portoroz: IFIP Press, 2002. 376−386.
[23] Yu H, Rexford J, Felten EW. A distributed reputation approach to cooperative Internet routing protection. In: Fahmy S, ed. Proc. of the Secure Network Protocols 2005. Boston: IEEE Press, 2005. 73−78.
[24] Mahajan R, Wetherall D, Anderson T. Understanding BGP misconfiguration. In: Steenkiste P, ed. Proc. of the ACM SIGCOMM 2002. ACM Press, 2002. 3−16.
[25] Heckerman D. A tutorial on learning with Bayesian networks. In: Jordan M, ed. Learning in Graphical Models. MIT Press, 1998.
[26] Jøsang A, Ismail R. The beta reputation system. In: Gricar J, ed. Proc. of the 15th Bled Electronic Commerce Conf. Bled, 2002. 1−14.
[27] Dimitropoulos XA, Krioukov DV, Riley GF. Revisiting Internet AS-level topology discovery. In: Dovrolis C, ed. Proc. of the PAM 2005. LNCS 3431, Heidelberg: Springer-Verlag, 2005. 177−188.
[28] AS65000 BGP routing table analysis report. 2008. http://bgp.potaroo.net/as1221/bgp-active.html

胡宁(1972－),男,湖南长沙人,博士生,主要研究领域为路由技术,网络安全技术.

朱培栋(1971－),男,博士,副教授,主要研究领域为路由技术,网络安全技术.

邹鹏(1957－),男,教授,博士生导师,主要研究领域为分布操作系统,分布式计算.