基于信誉的域间路由选择机制的研究与实现

赵仕祺，黄小红，钟志港
（北京邮电大学计算机学院，北京 100876）

摘 要：为了解决边界网关协议（BGP）缺乏对路由更新消息验证的问题，提出一种由信誉评估机制和基于信誉的 BGP 路由选择算法两部分组成的域间路由选择机制。信誉评估机制采用分布式自治系统（AS）联盟架构，详细划分节点路由行为，以服务域和观测权重为指标量化节点行为带来的影响，通过设计反馈机制让信誉不仅能反映节点善恶，还能反映节点对恶意攻击的抵抗能力；基于信誉的 BGP 路由选择算法在现有路由选择算法中加入一条“安全”策略：过滤包含低信誉节点的路由，并从高信誉的路由中选择最佳路由。实验结果表明，所提机制不仅抑制非法路由传播，还避开易受污染的路径，相比于现有的信誉评估机制更适用于域间路由系统，提供更加安全的域间路由环境。

关键词：边界网关协议；信誉机制；路由选择机制；网络安全
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023114

Research and implementation of reputation-based inter-domain routing selection mechanism

ZHAO Shiqi, HUANG Xiaohong, ZHONG Zhigang
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: To solve the problem of lack of validation for exchanging messages in BGP, a inter-domain routing mechanism, which consisted of a reputation evaluation mechanism and a reputation-based BGP optimal routing algorithm, was proposed.The reputation evaluation mechanism used a distributed autonomous system (AS) alliance architecture, which divided node routing behavior in detail. The service domain and observation weight were used as indicators to quantify the impact of node behavior. By designing a feedback mechanism, the reputation value not only reflected the good and bad of nodes, but also reflected the node’s resistance to malicious attacks. The reputation-based BGP routing selection algorithm adds a “security” policy to the existing routing selection algorithm by filtering routes containing low-reputation nodes and selecting the best route among high reputation routes. The experimental results show that the proposed mechanism outperform most existing reputation mechanisms by avoiding routes with vulnerable nodes and restraining the propagation of illegal routes, thereby providing a more secure inter-domain routing environment.

Keywords: border gateway protocol, reputation mechanism, routing selection mechanism, network security

0 引言

边界网关协议（BGP, border gateway protocol）作为域间路由的标准协议，可为自治系统（AS, autonomous system）和自治域间提供网络可达信息，避免路由环路[1]。然而，BGP 在设计上存在巨大的安全漏洞：BGP 默认接收对等实体的全部通告，但缺乏对通告内容的认证机制[2]。这种设计上的缺陷使攻击者可以恶意篡改通告内容，发动路由劫持攻击，将受害者流量重新定向，造成路由黑洞和网络

收稿日期：2023−03−08；**修回日期：**2023−06−05
基金项目：国家重点研发计划基金资助项目（No.2018YFB1800404）
Foundation Item: The National Key Research and Development Program of China (No.2018YFB1800404)

中断，或通过被劫持的前缀发动域名系统（DNS）攻击[3]、分布式拒绝服务（DDoS）攻击[4]、中间人攻击[5]等，对网络性能与可靠性造成严重威胁。

基于此，相关研究人员和标准组织推出一系列安全机制来增强 BGP 的安全性，一类是通过认证机制保证源路由可信的 RPKI（resource public key infrastructure）[6]以及路径可信的 S-BGP（secure BGP）[7-10]。这类认证机制通过仿真实验[11]和网络测量[12]等方式表现出对恶意行为有良好的抵御效果，但由于部署成本和收益的不平衡，在实际网络环境中的部署规模并不乐观（目前仅有 20%的前缀通过 RPKI 实现源认证[13]）。另一类防御手段是借助路由注册，注册数据包括路由起源和路由策略等，通过设置路由过滤器[14-15]过滤掉不匹配注册数据的路由。但路由注册在实际运营中存在数据库内容不完整、不可靠、更新不及时的问题，这影响了它实际的使用效果[16]。相较于认证机制的部署瓶颈和路由过滤的信息滞后，将信誉机制引入域间路由系统不失为一种轻量、高效，同时兼顾时效性的防御手段。

信誉是根据一个实体的历史行为衡量其执行特定任务可能性的定量指标[17]。在域间路由环境下，节点（即 AS）可以通过考察对方的信誉调整路由策略，避开恶意节点，抑制虚假信息传播，从而提升网络安全性。文献[18]提出了一种基于贝叶斯预测的信誉评估机制，将节点收到真实路由或非法路由作为一个二项式事件。然而实际环境中网络节点的行为是复杂的，合法与非法的二分类无法刻画节点行为细节。文献[19]提出了域间路由安全管理信誉机制，以节点的历史路由行为作为指标，通过邻居节点投票的方式为节点可信度赋值。文献[20]提出了一种信誉传播机制 ReMSA（reputation management for social agent），以节点信息交互频次和节点所处网络位置作为主要考虑因素，通过仿真验证其局部及全局信誉计算方案。文献[21]提出了面向域间路由系统的信任模型 TMRIS（trust model for inter-domain routing system），该模型将节点信誉分为 3 个部分：节点本地评估结果、节点历史路由通告偏差和信息完整程度，并设计了一种激励机制来激励节点间交互信誉。文献[22]考虑了域间路由的特点，对文献[20]提出的 ReMSA 进行了改进：局部信誉由目标节点的行为结果通过贝叶斯预测算出，全局信誉由节点的信誉经节点的度数加权平均得到。文献[23]提出了 ASwatch 机制，依靠控制平面信息设置 AS 信誉指标，包括宣告稳定度、前缀可达性和连接稳定性，监测低信誉的 AS。上述方案缺乏对节点转发非法路由行为的惩罚机制，转发节点对非法路由的传播和扩散起到推波助澜的作用，而现有机制并未将这种行为反馈到信誉上。此外，以上方案的防御措施较被动，通常是在发现路由中出现低信誉节点后才采用路由过滤措施抑制非法路由传播，而非选择更安全的路由来预防恶意行为的发生。

将信誉机制引入域间路由系统还需要高效合理的信誉评估架构。信誉评估机制的结果要实时、准确，这要求评估所需的观测数据在满足低滞后、高覆盖（涉及全局信誉评估）的同时，还要实现高效的信誉计算。集中式架构难以保证数据源的实时性和全面性，而分布式架构在局部信誉存储和全局信誉聚合过程中带来庞大的重复存储和通信开销，降低信誉评估效率。综上所述，针对现有的信誉评估机制的不足，本文提出一种基于 AS 联盟（AA, AS alliance）的分布式信誉评估机制，并基于该信誉评估机制设计 BGP 路由选择算法。本文的主要研究工作如下。

1) 引入 AS 联盟，每个 AS 联盟有一个主节点，负责联盟内的通信、信誉计算和信息存储维护。基于域间路由的特殊环境为节点行为模式分类，以服务域和观测权重为指标量化节点行为带来的影响。依据节点行为和影响设计不同的信誉反馈机制。

2) 对现有 BGP 路由选择算法进行改进和扩展：通过路由过滤舍弃包含低信誉节点路由；将路由上节点的信誉聚合为路由的信誉，结合 BGP 的默认路由选择策略，从高信誉的路由中选出最佳路由。

3) 仿真结果表明，本文提出的信誉评估机制能够有效地区分节点类型，而路由选择方案能有效抑制恶意路由，降低受感染路径比例。与现有的信誉评估机制相比，本文提出的信誉评估机制更具有效性。

1 基于信誉的域间路由选择机制

本文提出了一种基于信誉的域间路由选择机制，由信誉评估机制和路由选择算法两部分组成。接下来，本节从信誉评估机制、信誉计算和路由选择算法 3 个方面进行介绍。

1.1 信誉评估机制

1.1.1 基于 AS 联盟的分布式信誉评估机制架构

AS 联盟是由一组连通性高的 AS 按照共同的目标组成的一个局部协同集合体，每个 AS 联盟中有一个主节点，负责联盟内的重要事务，以及联盟间

的信息传递。图 1 是 AS 联盟示意，共有 AA100 和 AA300 这 2 个联盟，AS100 和 AS300 分别是这 2 个联盟的主节点。联盟中每个节点均可作为数据采集点为信誉评估提供源数据，如AS101通过与AS2261和 AS204 建立对等实体连接可获取来自联盟外邻居节点的路由消息。

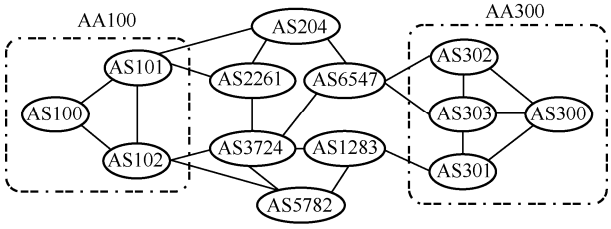

图 1　AS 联盟示意

AS 联盟是分布式信誉评估的基本单元。在联盟内部，各节点依据其特定的连接关系与路由策略采集路由数据，交由主节点评估各节点局部信誉。联盟主节点间相互通信，将节点局部信誉聚合成全局信誉，为路由选择提供重要参照。图 2 展示了基于信誉的路由选择机制，并给出了基于信誉的 BGP 路由选择算法、基于 AS 联盟的分布式信誉评估机制和 AS 联盟三者之间的关系。

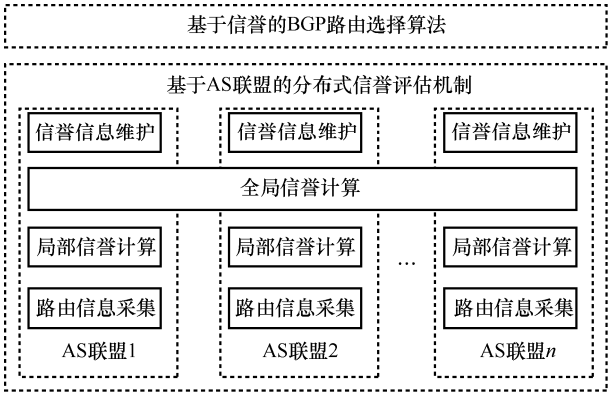

图 2　基于信誉的路由选择机制

AS 联盟由有紧密合作关系的自治域构成，并推举出联盟主节点，由于 BGP 自身带有维护自治域间连接的属性，联盟一经建立，如果主节点不改变将不会给联盟的更新和维护带来额外开销。

AS 联盟建立以后，路由更新信息的采集和计算由联盟内的观测点执行，并将统计结果上传至联盟主节点；主节点计算所有可观测到的节点的局部信誉，并通过节点之间的交互计算目标节点的全局信誉。由于观测点和主节点以及主节点之间的通信仅交互统计和计算结果，并且交互频率不高，因此通信开销较小；同时主节点的计算、存储和维护任务都在本地设备上进行，不会给通信设备带来额外的计算开销。因此这种信誉评估架构能够在保证观测全面、准确的同时，兼顾集中式和分布式的优势，对通信网络性能的影响较小。

分布式信誉评估机制可通过软件定义网络（SDN）实现：每个 AS 联盟作为一个 SDN 控制域，控制域中的 SDN 控制器担任联盟主节点的角色，控制器依据该控制域的局部观测结果计算并存储可观测到的节点的局部信誉信息，而节点的全局信誉则通过不同 SDN 控制器之间的相互通信进行信誉聚合求得。

1.1.2　信誉评估机制的组成

信誉评估机制分为局部信誉评估与全局信誉评估 2 个步骤。局部信誉评估应用于 AS 联盟内部，由行为划分、影响量化和反馈 3 个部分组成，如图 3 所示。全局信誉评估是聚合局部信誉的过程，应用于 AS 联盟之间，依据各联盟的观测权重为节点赋予全局信誉，如图 4 所示。

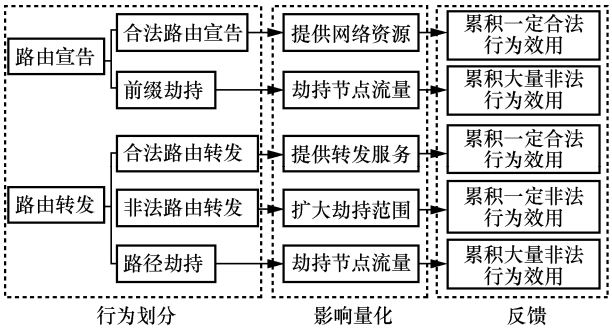

图 3　局部信誉评估

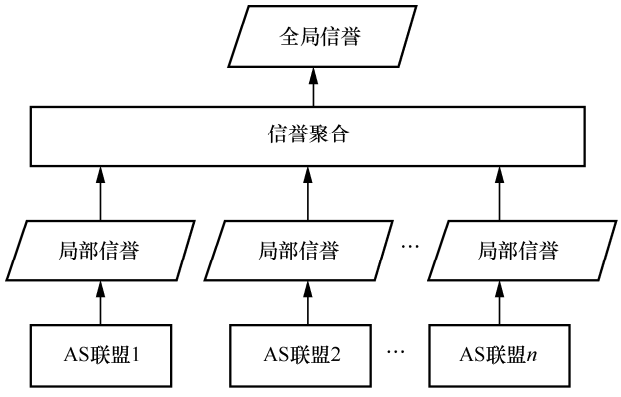

图 4　全局信誉评估

1.1.3　节点行为模式划分

节点行为合法、非法的二元划分方式缺乏对域间路由行为细节的刻画。本文将细化这 2 种行为模

式：合法行为细分为合法路由宣告和合法路由转发，其中合法路由宣告表示节点拥有的网络资源，合法路由转发描述节点转发能力；非法行为除前缀劫持、路径劫持这两类常见攻击行为外，增加非法路由转发行为，用来刻画节点对恶意攻击的抵抗能力。表 1 给出了域间路由节点行为模式划分。

表 1　域间路由节点行为模式划分

行为模式	定义
合法路由宣告	节点宣告了属于本自治域的前缀
前缀劫持	节点宣告了不属于本自治域的前缀
路径劫持	节点通过篡改路由更新报文的 AS_PATH 属性伪造了路由，并将伪造的路由转发给了其他节点
非法路由转发	节点转发了来自攻击者的路由，如转发了被劫持前缀的路由，或转发了伪造的路由
合法路由转发	节点进行了路由转发，且路由并不来自攻击者

1.1.4　节点行为影响分析

节点行为带来的影响需要统一指标量化，为信誉计算和反馈设计设立标准。本文采用服务域和节点权重这 2 个指标评估节点行为所产生的影响。

服务域定义为网络节点的集合，假设网络节点 P 发起对某个前缀 prefix 的访问，流量经由节点 N 转发或被其接收，则称 P 在 N 的服务域 $z(N,p)$ 内。考虑 2 种合法路由行为：如果 N 是前缀 prefix 的合法宣告者，那么 $z(N,p)$ 代表所有可访问前缀 prefix 的网络节点集合；如果 N 是前缀 prefix 的合法路由转发者，那么 $z(N,p)$ 中节点访问前缀 prefix 都需要由 N 转发。因此服务域能够刻画网络节点合法行为的影响范围。同理，如果 N 是前缀劫持、路径劫持的发起者或是非法路由的转发者，那么访问前缀 prefix 的流量都将流经 N，其中，$z(N,p)$ 表示所有受非法行为感染的节点集合，服务域便能准确刻画节点非法行为的影响范围。

服务域定义了节点行为的影响范围，即节点数量。而不同节点因其内部用户数量、承载业务、网络位置的不同呈现不同的规模，在定义影响范围的同时，也要考虑节点规模的大小。本文为网络中的每一个节点 P 设定一个权重 $W(P)$，反映节点 P 的内部规模，节点 P 规模越大，则权重 $W(P)$ 越大。

1.1.5　反馈机制设计

节点不同行为的后果要合理地反馈到节点信誉上，首先考虑 2 种合法路由行为。无论是合法的路由宣告还是路由转发，都是健康的商业行为，它们对节点的信誉有正向作用。

在前缀劫持和路径劫持里，攻击者通过宣告虚假路由信息，恶意吸引攻击者服务域内所有节点的流量。反馈机制要对这种行为施以惩罚，降低攻击者信誉，惩罚力度由影响范围决定。

非法路由转发节点并不是恶意行为的发起者，相反它们位于攻击者的服务域内。虽未发起恶意攻击，但这类节点通过接收和转发非法路由扩大了恶意行为的影响范围，对劫持事件的扩散推波助澜，因此需施以一定程度的惩罚。惩罚的力度从 2 个方面考虑：服务域规模和距离攻击者的位置。节点服务域规模越大，散播范围越大，造成的影响越严重，因此要对节点予以大力度惩罚。转发节点距离攻击者越近，及时阻止非法路由的传播便能有效抑制事件扩散；转发节点距离攻击者较远，这意味着上游节点均未能有效抑制非法路由的传播，转发节点不负有主要责任，惩罚力度不宜过大。

1.2　信誉计算

依据 1.1 节提出的量化指标和反馈机制，本节给出局部信誉和全局信誉的计算式。

1.2.1　局部信誉的计算

定义 1　$U^t_{u,A}(N)$、$U^f_{u,A}(N)$ 分别是 AS 联盟 u 观测到节点 N 的合法路由宣告、非法路由宣告所累积的效用，可以表示为

$$U^t_{u,A}(N)=\sum_{A^t_u(N)}\sum_{P\in z(A^t_u((N))}\gamma W(P) \tag{1}$$

$$U^f_{u,A}(N)=\sum_{A^f_u(N)}\sum_{P\in z(A^f_u(N))}2^t\rho W(P) \tag{2}$$

其中，A^t_u和A^f_u是联盟 u 观测到节点 N 的一次合法路由宣告和一次非法路由宣告，$z(A^t_u)$和$z(A^f_u)$分别对应其服务域，2 个求和号统计了联盟 u 观测到的所有合法路由宣告和所有非法路由宣告，$W(P)$是节点 P 的权重，t 是节点 N 近期非法行为的次数，γ 和 ρ 是可调参数。

定义 2　$U^t_{u,E}(N)$和$U^f_{u,E}(N)$ 分别为 AS 联盟 u 观测到节点 N 的合法路由转发和非法路由转发所累积的效用，可以表示为

$$U^t_{u,E}(N)=\sum_{E^t_u(N)}\sum_{P\in z(E^t_u(N))}\omega W(P) \tag{3}$$

$$U^f_{u,E}(N)=\sum_{E^f_u(N)}\sum_{P\in z(E^f_u(N))}((1-\kappa)D(N)\omega W(P)+\kappa 2^t W(P)) \tag{4}$$

其中，E_u^t和E_u^f分别为联盟u观测到节点N的一次合法路由转发和一次非法路由转发，$z(E_u^t)$和$z(E_u^f)$分别为上述 2 种路由转发的服务域；ω为可调参数；如果N是路径劫持行为的发起者，κ=1，否则N只是转发了非法路由，κ=0；$D(N)$是对非法路由转发行为的惩罚系数，N与攻击者之间的跳数越少，$D(N)$越大。

定义 3　$R_{u,A}(N)$和$R_{u,E}(N)$分别为 AS 联盟u观测到的节点N的路由宣告信誉和路由转发信誉所产生的效用，可表示为

$$R_{u,A}(N)=\frac{U_{u,A}^t(N)-U_{u,A}^f(N)}{U_{u,A}^t(N)+U_{u,A}^f(N)} \tag{5}$$

$$R_{u,E}(N)=\frac{U_{u,E}^t(N)-U_{u,E}^f(N)}{U_{u,E}^t(N)+U_{u,E}^f(N)} \tag{6}$$

定义 4　AS 联盟u对节点N的局部信誉评估结果$R_u(N)$为节点的宣告信誉$R_{u,A}(N)$与路由转发信誉$R_{u,E}(N)$的加权平均和，计算式为

$$R_u(N)=\alpha R_{u,A}(N)+\beta R_{u,E}(N) \tag{7}$$

其中，α与β为可调参数，满足$\alpha>0,\beta>0$，$\alpha+\beta=1$。

1.2.2　观测权重的计算

通过 1.2.1 节可知，局部信誉计算的基础单元是联盟内部观测到目标节点路由行为的统计次数，而局部信誉反映的是联盟内各节点信誉的相对大小关系。不同联盟内部观测点数量不同、网络拓扑各异，加之路由策略限制，导致不同联盟在观测规模、观测角度上有较大差异。这要求局部信誉聚合为全局信誉时要充分考虑各联盟的观测权重。

通常认为如果一个网络节点在拓扑中度数越高，或与一个高度数高节点相连，那么它在网络拓扑中的可见度就越高，即大部分节点可观测到该点。然而并不是所有节点都具有高可见度，大部分节点属于区域可见。如果目标节点在某个联盟内部的可见度越高，则该联盟观测到的信息越丰富，其局部信誉权重越大。因此观测规模是各联盟观测权重的重要指标。观测规模是指联盟内所有能观测到目标节点路由行为的节点数量，可用目标节点的服务域表示。

根据反馈机制的设计原则，节点的非法行为会拉低其信誉。当联盟观测到某个恶意节点时，节点局部信誉会降低。为使这种影响更大程度地反映在全局信誉上，需提高该联盟观测权重，而提高的程度和非法行为次数有关：非法行为次数越多，观测权重越大。据此提出以下定义。

定义 5　$w_u(N)$为 AS 联盟u计算得到的对节点N的观测权重，计算式为

$$w_u(N)=\sum_{P\in z(A_u^t(N))}W(P)+\sum_{P\in z(E_u^t(N))}W(P)+t\left(\sum_{P\in z(A_u^f(N))}W(P)+\sum_{P\in z(E_u^f(N))}W(P)\right) \tag{8}$$

1.2.3　全局信誉的计算

定义 6　节点N的全局信誉$R_g(N)$为所有 AS 联盟对节点N的局部信誉的加权平均和，计算式为

$$R_g(N)=\frac{\sum_u w_u(N)R_u(N)}{\sum_u w_u(N)} \tag{9}$$

信誉计算是周期性的，为保证信誉的实时性，计算结果应反映出短时间内路由行为对各个节点信誉的影响。为此本文引入评估周期，每一轮信誉计算涵盖了评估周期内所有的路由行为。需要指出的是，路由行为是持续且动态变化的，时刻越近的路由行为对当前信誉影响越大，即便它们不在当前评估周期内。本文引入时间衰减系数σ来体现这种依赖关系。

定义 7　节点N在第$k+1$轮的全局信誉为$R_g^{k+1}(N)$，计算式为

$$R_g^{k+1}(N)=\sigma R_g^k(N)+(1-\sigma)R_g(N) \tag{10}$$

1.3　路由选择算法

本文提出的信誉评估机制不仅能体现节点的善恶程度，还能反映出节点面对恶意行为的抵抗能力，这为路由选择提供了重要参考。基于信誉的路由选择机制是在 BGP 路由选择机制上增加一个“安全”策略：通过路由过滤舍弃包含低信誉节点的路由；将路由上节点的信誉聚合为路由的信誉，结合 BGP 的默认路由选择策略，从高信誉的路由中选出最佳路由。这一过程仅在传统路由选择中增加了简单的过滤和筛选操作，不会给节点的路由设备带来过多开销，因此域间代价可控。

定义 8　路由r的路由信誉为R_r，计算式为

$$R_r = \frac{\sum_{N_i \in r} k_i R_g(N_i)}{\sum_{N_i \in r} k_i} \tag{11}$$

其中，N_i 是路由 r 上的节点，$R_g(N_i)$ 是节点 N_i 的全局信誉，k_i 是可调参数。

安全策略首先遍历所有可选路由，如果可选路由中存在信誉低于 μ 的节点，则将这条路由从可选路由中排除；然后根据式(11)计算剩余所有可选路由的聚合信誉，并根据信誉大小排序，选择和最高信誉相差不超过 χ 的路由作为最佳路由的候选集合；如果候选集合中只存在一条路由，则选择其为最佳路由，否则将根据默认的路由选择策略从候选集合中选出最佳路由。基于信誉的 BGP 路由选择算法如算法 1 所示。

算法 1 基于信誉的 BGP 路由选择算法

定义 goodroute = [] 为最佳路由候选集合，给定节点信誉和路由信誉的阈值参数 μ 和 χ

输入 所有可选路由的集合 routes，路由上节点的全局信誉 $R(N_i)$，其中，N_i 代表第 i 个路由节点

输出 bestroute

1) 遍历 routes 中每条路由 r；
2) 遍历 r 上所有节点；
3) 如果全局信誉 $R(N_i) < \mu$；
4) 从 routes 中剔除 r；
5) 否则根据式(11)为路由 r 赋值；
6) routes 遍历结束；
7) 根据 routereputation 对 routes 从大到小排序；
8) 遍历 routes 中每条路由 r；
9) 如果 routereputation[r] ≥ routereputation[1] − χ；
10) r 添加到 goodroute；
11) routes 遍历结束；
12) 如果 goodroute 唯一；
13) 输出 goodroute；
14) 否则根据默认路由选择策略从 goodroute 中选出 bestroute；

节点（BGP 路由器）选择路径后，对数据包的转发可借助分段路由技术实现：通过配置分段路由策略（SRP, segment routing policy）引导数据包沿着该路径通过网络，具体做法是在数据包报头中插入带顺序的 Segment 列表，以指示接收到这些数据包的节点如何处理和转发这些数据包。Segment 指令列表实例化基于信誉的路由选择结果，并通过 BGP 在网络中分发 BGP Segment 信息[24]。

2 仿真实验结果与分析

为验证本文所提方案的有效性，将其与基于贝叶斯预测（记作 Bayesian）[18]、基于信任模型 TRIMS（记作 TRIMS）[21]以及改进的信誉传播机制 ReMSA（记作 ReMSA）[22]进行对比。仿真平台选择 SimBGP，为满足实验需要进行了二次开发，部署了本文以及上述提到的机制，并实现前缀劫持、路径劫持、源路由认证、路径认证的模拟。

仿真实验拓扑如图 5 所示，共有 AA9 和 AA10 这 2 个 AS 联盟，AA9 包含 AS4、AS8、AS9、AS12 这 4 个节点，AA10 包含 AS3、AS6、AS10 这 3 个节点，其中，AS9 和 AS10 分别是这 2 个联盟的主节点。

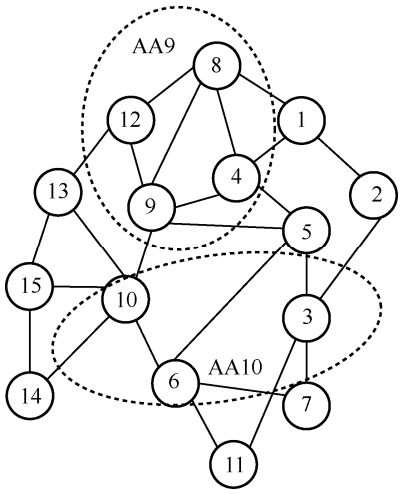

图 5 仿真实验拓扑

信誉评估机制中的可调参数及取值如表 2 所示。

表 2 信誉评估机制中的可调参数及取值

参数	值
α	0.5
β	0.5
γ	1.0
ρ	2.0
ω	1.0
τ	1.0
σ	0.367 9
初始全局信誉	0.800 0

2.1　信誉评估机制仿真分析

为了评估本文提出的信誉评估机制（记作RepBGP）的有效性，仿真实验分析 Bayesian 和 RepBGP 对域间路由系统中呈现不同行为模式的节点得到的信誉评价。根据 1.1.3 节中提出的节点行为模式的划分方式，实验设计了 4 类路由节点。

恶意节点：主动进行前缀劫持和路径劫持攻击。

安全节点：部署防御机制，对前缀劫持和路径劫持攻击具有防御能力的节点。

正常节点：不会主动实施恶意攻击，但也未部署防御机制，对前缀劫持和路径劫持没有防御能力。

积极节点：最初等同于正常节点，经过一段时间后部署源路由认证机制，主动过滤非法的源路由宣告，再经过一段时间后部署路径认证机制，主动过滤包含路径劫持的路由宣告。

实验设计的思路是通过对比不同机制对节点的信誉评估验证其有效性，具体设置如下：评估周期为 10 s，总时长为 200 s，共进行 20 轮信誉评估；依照图 5 进行设计，每个节点宣告 30 条前缀，宣告间隔为 10 s；节点 4 和节点 6 为恶意节点，每个宣告间隔内随机发起两次前缀劫持和路径劫持；节点 10 为积极节点，在第 8 轮部署源路由认证机制，第 15 轮部署路径认证机制。

需要指出的是，在实验开始阶段，所有节点的初始信誉相同，而后续信誉的变化是基于不同联盟的观测点对每个节点的真实路由行为量化聚合得到的，因此信誉基本不会对全局信誉的鲁棒性有影响。

图 6 和图 7 分别记录了基于 Bayesian 和 RepBGP 的 4 类节点的全局信誉在 20 轮评估周期内的变化。从图 6 可以看出，Bayesian 通过信誉只能识别恶意节点，无法区分正常节点、积极节点和安全节点。Bayesian 的缺陷和多数信誉评估机制类似，即对节点行为进行简单的二分类，并未考虑节点在非法路由传播和抑制上的贡献，也缺乏相应机制反馈到信誉上，这就导致最终结果难以区分抵抗力差的正常节点和安全性高的安全节点、积极节点。

从图 7 可以看出，与 Bayesian 中恶意节点的信誉维持在相对较低数值不同，RepBGP 使恶意节点的信誉随评估周期迅速下跌至最低点。安全节点因其部署的防御机制能有效抵御前缀劫持和路径劫持，并抑制非法路由传播，因此信誉稳步升至最高。正常节点不是恶意行为的发起者，但由于缺乏防御机制，只能被动接收和转发非法路由，这对恶意行为的传播负有一定责任。信誉机制对这种行为给予适量惩罚，最终的信誉维持在 0.78，稍低于安全节点但远高于恶意节点。积极节点的信誉在启动防御机制前与正常节点一致，在第 8 轮和第 15 轮分别部署源路由认证和路径认证机制后，有效抑制了前缀劫持和路径劫持非法路由的传播，反馈机制鼓励这种行为，信誉也快速提升。可以看出，RepBGP 相较于 Bayesian 能有效区分节点类型并给出合理的信誉。

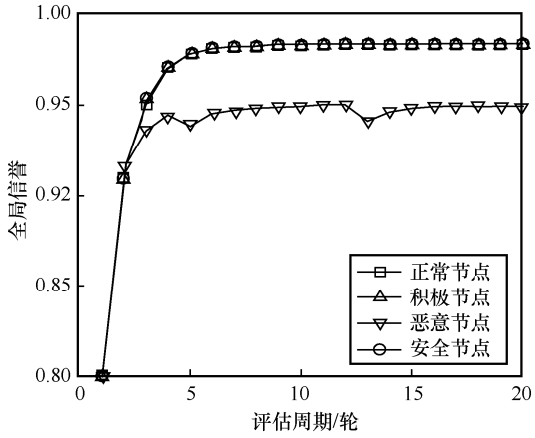

图 6　Bayesian 的信誉评估结果

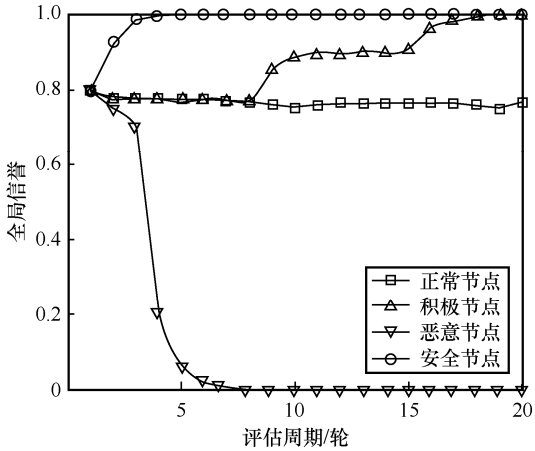

图 7　RepBGP 的信誉评估结果

为比较不同信誉评估机制对恶意节点的识别能力，本文统计了恶意节点 4 在不同信誉评估机制下的信誉变化情况，如图 8 所示。从图 8 可以看出，本文提出的机制使恶意节点的信誉显著下跌到最低；而在 Bayesian、TRIMS 和 ReMSA 这 3 种机制下，恶意节点的信誉稳定地维持在较高数值。这种

结果的产生和 RepBGP 的信誉评估机制有关：由于恶意节点 4 发起恶意行为的频率低、规模小，Bayesian、TRIMS 和 ReMSA 这 3 种机制对这种行为敏感度低，惩罚力度不够，导致信誉评估缺乏区分度；而 RepBGP 在发现节点恶意行为时会提高节点的观测权重，后续过程中如果恶意行为持续存在，会通过反馈机制不断加大惩罚力度。这些措施使 RepBGP 对节点的恶意行为敏感度极高，即便节点在发起恶意行为的同时也在进行合法行为（如宣告合法前缀、转发合法路由），但持续不断的恶意行为只会让节点逐渐失去信任，这也更符合实际网络情况。

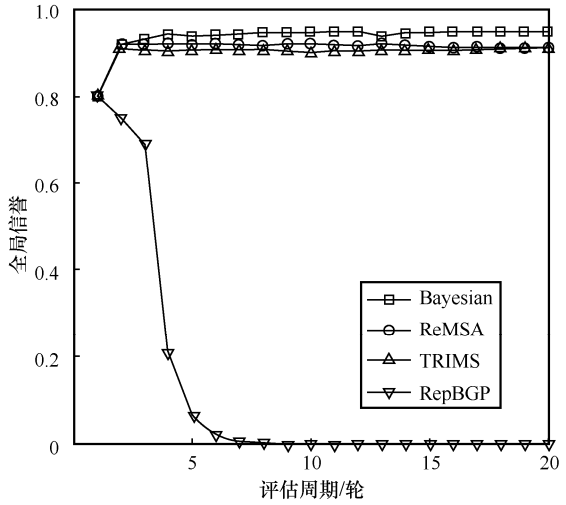

图 8 恶意节点 4 在不同信誉评估机制下的信誉变化情况

2.2 基于信誉的路由选择机制仿真分析

本文使用非法路由占比（RIR, ratio of invalid route）这一指标来评价不同路由选择机制。非法路由占比是指路由收敛后非法路由在全部路由中的占比，可表示为

$$\mathrm{RIR}=\frac{\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} r_f(s,d,p)}{\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} r_t(s,d,p)+\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} r_f(s,d,p)} \tag{12}$$

其中，S 是所有前缀的集合，p 是 S 中的一个前缀；R 是所有路由的集合，每条路由用三元组(s,d,p)表示，s 是路由的终点（流量的始发位置），d 是路由的起点（流量的最终流向）；$r_t(s,d,p)$ 和 $r_f(s,d,p)$ 分别表示由 d 发起最终流向 s 中 p 的合法路由和非法路由。

实验沿用图 5 拓扑，设定信誉评估周期为 20 s，共进行 10 轮信誉评估。每个节点宣告 30 条前缀，节点 4 和节点 6 为恶意节点，每个宣告间隔内随机发起一次前缀劫持和一次路径劫持。节点在每个评估周期内的路由选择策略都是基于上一轮信誉评估结果在一个周期结束时计算整个拓扑中非法路由占比。实验记录了在部署默认路由机制（记作 Default）、基于 TRIMS 的路由选择机制、基于改进的 ReMSA 的路由选择机制和本文提出的路由选择机制下非法路由占比随评估周期的变化情况，结果如图 9 所示。

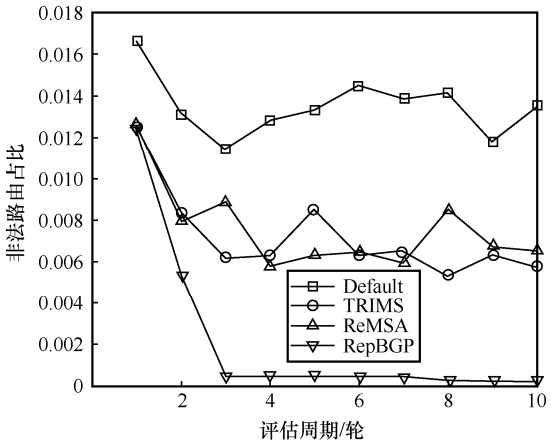

图 9 非法路由占比随评估周期的变化

从图 9 可以看出，部署了基于信誉的路由选择机制相较于默认路由机制能更有效地抑制非法路由占比，这得益于路由选择过程舍弃了低信誉路由，在一定程度上抑制了非法路由的传播，提高了整个网络的安全性。而本文的路由选择机制不仅阻断了非法路由的传播，还避开了容易受污染的路径，因此对非法路由的抑制效果更好。

由于附加损害[13]现象的存在，如果合法路由中的节点被污染，流量仍会通过被污染节点转发给攻击者。本文提出的“安全”策略可以解决这一问题：通过聚合路由上各个节点的信誉形成路由信誉，对所有可选路由排序；结合 BGP 默认的路由选择策略，从高信誉可选路由中选出最佳路由。为了验证这一策略的有效性，本文引入感染路径占比（RIP, ratio of infected path）这一指标，定义为路由收敛后流经感染节点的路径在全部路由中的占比，可表示为

$$\mathrm{RIP}=\frac{\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} P_f(s,d,p)}{\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} P_t(s,d,p)+\sum\limits_{p\in S}\sum\limits_{(s,d)\in R} P_f(s,d,p)} \tag{13}$$

其中，$P_t(s,d,p)$ 和 $P_f(s,d,p)$ 分别表示由 d 发起最终流向 s 中 p 的安全路径和感染路径。实验环境沿用上一个实验配置，对比双方是各节点在应用本文所提路由选择机制时是否部署了“安全”策略（未部署安全策略记为机制 1，部署安全策略记为机制 2）。经过 10 轮评估周期后，2 种路由选择机制下非法路由和感染路径占比如表 3 所示。可见增加这种“安全”策略能有效减少网络中的非法路由和感染路径。

表 3　2 种路由选择机制下非法路由和感染路径占比

路由选择机制	非法路由占比	感染路径占比
机制 1	3.075‰	8.543‰
机制 2	2.571‰	4.307‰

3　结束语

本文对基于信誉的域间路由选择机制进行了研究。考虑到现有方案判断节点行为单一、反馈机制不合理、量化方式未考虑域间路由场景特殊性等问题，本文提出了一种基于 AS 联盟的分布式信誉评估机制，更加细致地刻画了节点行为，特别是对恶意行为的传播，并对持续发起恶意行为的节点加大了惩罚力度，丰富了信誉的反馈机制，同时兼顾了集中式和分布式评估机制的优势。针对默认路由选择机制存在的附中损害现象，本文通过增加一个“安全”策略，避免选择包含恶意节点和易感染节点的路由，提升域间路由系统的安全性。仿真结果表明，本文机制能有效识别节点类型，信誉赋值更符合实际网络情况，路由选择更加安全。

参考文献：

[1] REKHTER Y, LI T, HARES S. A border gateway protocol 4(BGP-4)[S]. Internet Engineering Task Force (IETF) RFC 4271, 2006.

[2] 王娜, 杜学绘, 王文娟, 等. 边界网关协议安全研究综述[J]. 计算机学报, 2017, 40(7): 1626-1648.
WANG N, DU X H, WANG W J, et al. A survey of the border gateway protocol security[J]. Chinese Journal of Computers, 2017, 40(7): 1626-1648.

[3] HUDAIB A A Z, HUDAIB E A Z. DNS advanced attacks and analysis[J]. International Journal of Computer Science and Security (IJCSS), 2014, 8(2): 63.

[4] MIRKOVIC J, REIHER P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(2): 39-53.

[5] CONTI M, DRAGONI N, LESYK V. A survey of man in the middle attacks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2027-2051.

[6] HUSTON G, MICHAELSON G. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs)[S]. Internet Engineering Task Force (IETF) RFC 6483, 2012.

[7] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP)[C]//Proceedings of IEEE Journal on Selected Areas in Communications. Piscataway: IEEE Press, 2002: 582-592.

[8] WHITE R. Architecture and deployment considerations for secure origin BGP (soBGP)[R]. 2006.

[9] WHITE R. Securing BGP through secure origin BGP (soBGP)[J]. Business Communications Review, 2003, 33(5): 47.

[10] LEPINSKI M, SRIRAM K. BGPsec protocol specification[S]. Internet Engineering Task Force (IETF) RFC 8205, 2017.

[11] LYCHEV R, GOLDBERG S, SCHAPIRA M. BGP security in partial deployment[J]. ACM SIGCOMM Computer Communication Review, 2013, 43(4): 171-182.

[12] CHUNG T, ABEN E, BRUIJNZEELS T, et al. RPKI is coming of age: a longitudinal study of RPKI deployment and invalid route origins[C]//Proceedings of the Internet Measurement Conference. New York: ACM Press, 2019: 406-419.

[13] GILAD Y, COHEN A, HERZBERG A, et al. Are we there yet? on RPKI’s deployment and security[C]//Proceedings of 2017 Network and Distributed System Security Symposium. Reston: Internet Society, 2017: 1-16.

[14] BATTISTA G D, REFICE T, RIMONDINI M. How to extract BGP peering information from the Internet routing registry[C]//Proceedings of the 2006 SIGCOMM Workshop on Mining Network Data. New York: ACM Press, 2006: 317-322.

[15] GOODELL G, AIELLO W, GRIFFIN T, et al. Working around BGP: an incremental approach to improving security and accuracy in inter-domain routing[C]//Proceedings of the Network and Distributed System Security Symposium. Saarland: DBLP, 2003: 1-11.

[16] MITSEVA A, PANCHENKO A, ENGEL T. The state of affairs in BGP security: a survey of attacks and defenses[J]. Computer Communications, 2018, 124: 45-60.

[17] 刘湘辉, 殷建平, 唐乐乐, 等. 网络流量的有效测量方法分析[J]. 软件学报, 2003, 14(2): 300-304.
LIU X H, YIN J P, TANG L L, et al. Analysis of efficient monitoring method for the network flow[J]. Journal of Software, 2003, 14(2): 300-304.

[18] WANG N, WANG B Q. A reputation-based method to secure in-

ter-domain routing[C]//Proceedings of 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing. Piscataway: IEEE Press, 2014: 1424-1429.

[19] HU N, ZHU P D, ZOU P. Reputation mechanism for inter-domain routing security management[C]//Proceedings of 2009 Ninth IEEE International Conference on Computer and Information Technology. Piscataway: IEEE Press, 2009: 98-103.

[20] LEE J Y, OH J C. Applications of social media and social network analysis[M]. Germany: Springer International Publishing, 2015.

[21] NU X, WEI L, YOU L, et al. A trust model for the inter-domain routing system[J]. Journal of Computer Research and Development, 2016, 53(4): 845.

[22] 陈迪, 邱菡, 祝凯捷, 等. 基于自治域协同的域间路由信誉模型[J]. 中国科学(信息科学), 2021, 51(9): 1540-1558.
CHEN D, QIU H, ZHU K J, et al. An inter-domain routing reputation model based on autonomous domain collaboration[J]. Scientia Sinica (Informationis), 2021, 51(9): 1540-1558.

[23] KONTE M, PERDISCI R, FEAMSTER N. ASwatch: an AS reputation system to expose bulletproof hosting ASes[C]//Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication. New York: ACM Press, 2015: 625-638.

[24] FILSFILS C, MICHIELSEN K, TALAULIKAR K. Segment routing 详解 (第一卷)[M]. 苏远超, 蒋治春, 译. 北京: 人民邮电出版社, 2017.
FILSFILS C, MICHIELSEN K, TALAULIKAR K. Segment routing part I[M]. Translated by SU Y C, JIANG Z C. Beijing: Posts & Telecom Press, 2017.

[作者简介]

赵仕祺（1992– ），男，河南南阳人，北京邮电大学博士生，主要研究方向为域间路由异常检测、事件源定位等。

黄小红（1978– ），女，广东广州人，博士，北京邮电大学副教授，主要研究方向为互联网体系结构、网络管理与测量、网络安全等。

钟志港（1996– ），男，甘肃兰州人，北京邮电大学硕士生，主要研究方向为域间路由安全。