中国科学: 信息科学 2021 年 第 51 卷 第 9 期: 1540–1558
SCIENTIA SINICA Informationis
论文

基于自治域协同的域间路由信誉模型

陈迪[1,2,3], 邱菡[1,2*], 祝凯捷[2], 王清贤[1,2], 朱俊虎[1,2]

1. 信息工程大学网络空间安全学院, 郑州 450002
2. 数学工程与先进计算国家重点实验室, 郑州 450002
3. 电子信息系统复杂电磁环境效应国家重点实验室, 洛阳 471003
* 通信作者. E-mail: qiuhan410@aliyun.com

收稿日期: 2020–07–05; 修回日期: 2020–10–08; 接受日期: 2021–02–10; 网络出版日期: 2021–09–14

国家自然科学基金 (批准号: 61502528, 61902447) 资助项目

摘要 域间路由系统自治域间的交互缺乏可信认证, 建立针对自治域行为模式的信誉模型可为域间路由管理提供约束与激励, 提高整体安全水平. 由于域间路由系统分布自治、局部路由信息不完整, 现有信誉评价方法无法从全局视角感知自治域行为, 难以准确反映自治域可信程度及其变化. 本文提出一种基于自治域协同的域间路由信誉模型. 首先通过分析自治域路由行为统计特征, 建立基于贝叶斯 (Bayes) 后验概率分析的自治域信誉量化指标, 用于对目标自治域进行本地信誉评价; 然后通过研究自治域属性与本地路由信息完整程度的关系, 设计信誉加权聚合算法, 采用多域协同方式计算目标自治域的全局信誉评价; 最后设计信誉动态更新方法, 以对连续恶意行为的自治域进行惩罚. 基于真实安全事件的实验结果表明, 该模型能够有效聚合各自治域本地信誉评价, 捕捉自治域行为在不同时间阶段的细微变化, 可为域间路由系统中异常路由抑制、安全事件溯源和供应商选取提供参考.

关键词 域间路由安全, 自治域行为, 信誉模型, 贝叶斯估计

1 引言

互联网上的各种应用与服务严重依赖路由系统基础服务的安全可靠运行, 作为互联网基础设施, 域间路由系统的安全性和稳定性对互联网运行至关重要 [1]. 各自治域 (autonomous system, AS) 分别受独立管理机构控制, 由边界网关协议 BGP (border gateway protocol) 负责互联互通. 每个自治域向邻居宣告本地拥有的网络地址范围或可达网络, 同时根据邻居宣告的路由信息和本地路由策略决定将数据包发往何处. 因此, 域间路由系统是一个信誉系统, 几乎完全依赖自治域 (运营商) 之间的信任与协作. 然而自治域间具有错综复杂的商业关系 [2] 和不尽相同的利益驱动 [3], 自治域出于商业利益等因素可能存在转发不符合商业规则的路由、宣告非法前缀、伪造 AS 路径等异常行为 [4]. 由于 BGP 缺

引用格式: 陈迪, 邱菡, 祝凯捷, 等. 基于自治域协同的域间路由信誉模型. 中国科学: 信息科学, 2021, 51: 1540–1558, doi: 10.1360/SSI-2020-0215
Chen D, Qiu H, Zhu K J, et al. An inter-domain routing reputation model based on autonomous domain collaboration (in Chinese). Sci Sin Inform, 2021, 51: 1540–1558, doi: 10.1360/SSI-2020-0215

乏路由真实性验证 [5], 任意一个自治域的异常行为会影响其他 AS 行为决策, 影响互联网的稳定运行. 近年来发生的多起域间路由安全事件[1)2)] 均是由个别自治域引发.

现行互联网域间信任关系一般基于自治域管理机构的线下关系, 许多骨干 AS 的管理机构会成立相关组织, 通过管理员论坛、电子邮件以及定期举办线下会议的方式加强彼此的信任关系, 如北美网络运营商集团 NANOG[3)]、国际互联网协会[4)] 等. 其余自治域之间只能遵循 BGP "盲信任" (blind trust) 策略来交互路由可达信息. 作为缓解措施, 自治域通常利用本地异常检测机制抑制非法路由的影响. 然而现有本地异常检测本质上均为事件驱动的响应式 (reactive) 解决方案, 且各自治域本地路由数据具有局限性. 在 2019 年互联网测量会议 IMC 上发表的工作 [6] 通过分析近 5 年的 NANOG 网络管理员邮件列表与 BGP 路由数据, 得出自治域行为模式具有一定规律性, 且自治域恶意行为在时间上具有连续特性. 建立针对自治域行为模式的信誉量化评价机制可提供前摄性 (proactive) 的安全状态感知, 可用于路由决策判断、上游供应商选择, 还可作为域间路由协同防御方案 [7,8] 激励机制的输入, 有助于提高域间路由系统的整体安全水平.

信誉机制 [9] 对分布式网络节点具有激励作用, 可抑制虚假信息传播和不可信交互, 在无线通信、物联网等领域得到广泛的研究与应用 [10~12]. 分布式信誉技术与域间路由系统分布式自治的本质相契合, 可用于激励自治域积极协同、惩罚恶意行为、实现 "软安全". 基于该思想, Chang 等 [13,14] 提出一种基于历史 BGP 路由数据统计分析的自治域行为可信程度量化指标与自治域异常行为检测机制; 该方案依赖于输入路由数据集的完备性, 而现行域间路由系统现网数据受限于采集点分布与数据发布时延. 一些工作 [15~18] 借鉴分布式信誉机制的思想, 采用自治域自组织协同方式获取目标自治域行为信息, 完成信誉评价的聚合. 然而, 现有研究工作中的信誉量化方法主要用于甄别恶意自治域, 难以反映自治域在不同时间阶段行为的动态变化, 以对自治域运营商形成良好的约束与激励; 且现有协同式自治域信誉聚合方法未充分考虑域间路由系统与其他系统之间的差异性, 如网络拓扑、动态演化、商业关系等, 难以保证对目标自治域信誉聚合的准确性.

本文提出一种基于自治域协同的域间路由信誉模型 (AS cooperative inter-domain reputation model, ASCIR). 首先, 在各自治域本地综合目标自治域行为统计特征和宣告前缀有效时长, 采用贝叶斯 (Bayes) 后验概率分析的方法, 对自治域行为可信程度进行量化评估; 然后, 将自治域连接度数作为其评价的影响力权重, 通过协同共享完成多域信誉量化评估结果的聚合; 最后, 各自治域综合目标自治域的历史信誉评价和实时状态动态更新其当前信誉值, 引入时间衰减函数对自治域的连续异常行为进行 "惩罚", 使其信誉值在异常期遵循分布式信誉系统中 "慢升快降" 的原则更新. ASCIR 与 BGP 控制平面完全分离, 不改变现行 BGP 协议和 BGP 通告的数据包格式, 且可从大规模自治域开始逐步展开增量部署. 自治域可根据本地意愿加入信誉系统, 支持利用本地检测工具从更多维度 (如商业规则或路由策略符合性) 计算本地信誉评价.

本文第 2 节介绍相关研究工作, 第 3 节给出 ASCIR 概述, 第 4 节介绍自治域信誉量化指标, 第 5 节介绍自治域全局信誉计算方法, 第 6 节是仿真实验及结果分析, 第 7 节讨论若干相关问题, 第 8 节总结全文.

1) BGPmon Blog. BGP leak causing Internet outages in Japan and beyond. 2017. https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/.

2) BGPmon Blog. Large scale BGP hijack out of India. 2015. https://bgpmon.net/large-scale-bgp-hijack-out-of-india/.

3) The North American Network Operators' Group. http://www.nanog.org.

4) Internet Society. http://www.internetsociety.org.

2 相关工作

针对域间路由系统的信誉技术研究主要分为两类, 一类为基于现网数据分析的集中式方法, 另一类为基于自治域信任覆盖网络的分布式方法.

集中式的自治域信誉机制是利用 Routeview, RIPE 等机构提供的现网数据, 基于机器学习等方法对自治域的历史行为进行量化评估. Chang 等 [13] 提出了 AS-TRUST 机制, 以量化自治域通告行为的可信程度 (准确、稳定、符合路由策略), 基于对域间路由现网历史数据的统计分析, 计算各自治域的信誉值; 文献 [14] 提出了 AS-CRED, 针对自治域的前缀行为进行可信程度量化评估并给出自治域异常行为预测方法. ASwatch [4] 从历史现网数据中提取了自治域重连、BGP 路由动态和自治域 IP 地址碎片化 3 类特征, 使用随机森林算法训练分类器, 计算自治域的历史信誉度, 以甄别恶意自治域. 文献 [19] 提出一种用于识别异常 BGP 路径的动态信誉系统 B-secure, 基于历史 BGP 更新数据计算路径加权编辑距离与偏差概率, 以量化 BGP 路径的可信度. Arouna 等 [20] 提出一种 BGP 链路信誉评估算法, 基于由 BGPstream 采集的 BGP 历史数据, 通过综合每个 AS-path 的链路稳定度、恶意链路数量及链路敏感度 3 项指标计算 BGP 链路的信誉值, 并使用 BGPPlayJS 进行了可视化. 集中式域间路由信誉机制可提供基于自治域历史行为的信誉度量, 但其信誉量化方法主要目标为识别恶意自治域节点或链路而并非刻画自治域行为动态变化. 此外, 现网数据的全面性受到采集点的局限, 实际中本地自治域并不能获取真正的全局数据; 现网数据的更新发布具有一定时延, 信誉更新的实时性也难以保证.

分布式自治域信誉机制通过各自治域协同共享信息的方式获取自治域的行为信誉评价. 文献 [15] 指出自治域网络运营商之间的信任关系可为提高 BGP 安全提供有力支持, 作者借鉴 P2P 网络在线信誉系统设计了分布式自治域信誉协议, 在信誉覆盖网络中加权多自治域的信誉投票评分, 但没有给出信誉评分的具体量化方法. 胡宁等 [16] 提出了域间路由安全管理信誉机制 AIRS, 基于历史路由行为有效性统计结果, 通过邻居自治域投票获取自治域路由行为的可信度, 但其信誉量化方法仅依据自治域行为肯定/否定次数计算得出, 无法刻画自治域行为细节信息, 且聚合信誉评价时采用的就近原则, 使距离目标自治域较远的节点难以获取全面评价, 分布式全局信誉收敛性难以保证; 文献 [17] 提出了一种面向社交网络的在线信誉传播机制 ReMSA, 综合节点拓扑位置、交易频率等多方面要素, 将各节点的本地评价聚合为目标节点的信誉评价. 虽然 ReMSA 将域间路由系统作为应用背景开展了仿真实验, 但 ReMSA 并非针对域间路由系统设计, 其信誉值更新由节点间交易事件驱动, 即每收到一个更新事件就启动一次信誉更新, 应用于每日平均更新事件 200000 次的域间路由系统[5] 中需要过多资源消耗, 难以实现. 夏怒等 [18] 提出一种面向域间路由系统的信任模型 TMIRS, 通过综合邻居节点对目标节点的本地评价以实现目标自治域信任量化, 并设计了信任推荐激励机制. TMIRS 模型的信任计算方法需要根据不同自治域本地评价与被评估自治域路由通告行为的偏差设置权重, 根据节点本地信息完整程度分配信任聚合中的意见权重, 而实际中非对等自治域节点无法获取目标自治域的真实路由通告行为 [21], 该方案难以应用.

综上, 现有域间路由信誉技术在两个方面存在局限性: (1) 缺乏能够反映自治域行为动态变化的信誉评价指标以作为域间路由管理的约束与激励; (2) 针对域间路由系统各自治域的信息不对称性的全局信誉聚合算法准确性难以保证.

5) Huston G. BGP in 2019 - BGP Churn. http://blog.apnic.net/2020/01/15/bgp-in-2019-bgp-churn/.

3 ASCIR 概述

3.1 问题描述

自治域行为有效信誉量化指标的缺失和自治域本地路由信息的不完整性导致网络管理者难以通过已有信誉机制捕捉自治域行为模式的细微变化 (如自治域在某前缀劫持事件的不同阶段中发出路由更新频率, 前缀被宣告为有效的时长变化), 从而无法感知自治域安全状态, 预测其行为可信程度. 由此, 域间路由信誉技术要解决的关键问题是: (1) 如何建立从更新频率、前缀分布、有效时长等多个方面刻画自治域行为可信趋势的信誉量化指标? (2) 如何在本地路由信息有限情况下获取更接近全局视角的自治域信誉评价?

为解决上述问题, 本文使用信誉的概念对自治域行为进行量化. 分布式环境下, 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 [9]. 在域间路由系统中, 自治域可根据本地意愿与其他自治域建立逻辑连接, 共同组成协同共享信誉评价的覆盖网络. 将自治域节点之间更新报文的发送与接收过程视为节点间的交互事件, 任意自治域可作为评价节点, 也可作为被评价节点. 评价节点使用信誉指标来刻画被评价节点安全实时状态和行为可信程度, 量化与被评价节点之间的信任关系. 本文针对自治域发出路由通告的行为进行研究, 将通告前缀的合法性作为评价自治域行为信誉的依据.

具体地, 将自治域信誉协同网络表示为由参与自治域构成的无向图 $G=(A,E)$, A 代表参与自治域节点集合, E 代表参与自治域节点间建立的逻辑连接关系. 设 $a\in A$ 为被评价自治域, $e\in A$ 为评价自治域. 在每个观察时间周期 T 中, e 需依据本地接收到的来自于 a 的更新报文数据, 量化评价 a 在时间周期 T 的行为信誉, 即本地信誉评价 $\mathrm{Eval}(e,a)$. 由于受到拓扑位置、路由策略等影响, e 基于本地积累的交互数据得到的 $\mathrm{Eval}(e,a)$ 具有局限性. 因此, e 需问询其邻居节点对 a 的本地直接评价, 当邻居节点在反馈问询信息时为投票节点, 投票节点可继续向自己邻居节点问询其对 a 的信誉评价, 直到将多个信誉反馈加权综合后得到的全局信誉值收敛到 R_{ea} 时停止, R_{ea} 即为自治域 e 在时间周期 T 对自治域 a 行为的可信任程度的量化结果. 为了避免在时间周期 T 中 a 发出更新行为较少的情况并捕捉 a 在时间上的行为动态变化, e 需结合在本时间周期 T 得到的 R_{ea} 与 T 之前 a 已建立的信誉评价对其实时信誉评价进行更新.

本文第 4 与 5 节分别对上述两个关键问题进行阐述.

3.2 ASCIR 逻辑框架

本文提出的基于自治域协同的域间路由信誉模型 ASCIR 的逻辑框架如图 1 所示. ASCIR 逻辑上主要分为两个部分: 本地信誉量化与全局信誉计算.

本地信誉量化部分对应本文第 4 节, 自治域基于建立的自治域信誉量化指标对目标自治域进行本地信誉量化评价. 本地信誉量化分为训练阶段与操作阶段. 在训练阶段, 自治域基于本地历史路由数据与 Routeviews IP 前缀归属集提取自治域行为统计特征向量并进行正常/异常标签化. 将标签化的自治域行为统计特征向量作为训练集, 使用随机森林分类算法进行有监督学习, 生成自治域更新事件正常/异常分类器; 在操作阶段, 自治域基于本地接收到的实时路由数据, 提取目标自治域行为的统计特征向量, 将其输入自治域更新事件正常/异常分类器, 得到当前观察时间周期中的自治域更新事件正常/异常分类结果, 进而融合更新事件有效时间比率进行加权贝叶斯统计, 得到目标自治域的本地信誉量化评价.

全局信誉计算部分对应本文第 5 节, 自治域基于全局信誉聚合算法协同共享对目标自治域的本地

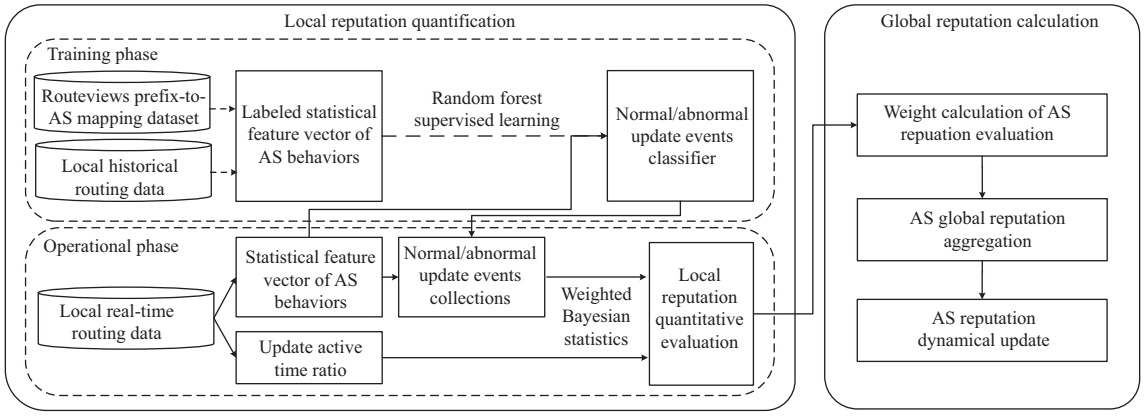

图 1　ASCIR 逻辑框架

Figure 1　Logical framework of ASCIR

信誉评价, 并综合目标已建立的历史信誉对其当前信誉值进行动态更新. 首先将自治域在域间路由系统中的连接度数作为信誉评价反馈的权重要素, 为自治域信誉评价分配权重; 然后向邻居节点问询针对目标自治域的本地信誉评价, 邻居节点继续迭代地收集毗邻自治域节点的本地评价, 并将反馈信息返回给评估节点, 进行信誉加权聚合, 得到目标自治域在当前观察时间周期的全局信誉值; 最后通过叠加时间衰减函数, 综合目标自治域已建立的信誉值和实时信誉聚合结果, 动态更新目标自治域信誉.

4　自治域信誉量化指标

自治域信誉量化指标需建立在评价方与被评价方之间路由行为交互累积的基础上, 且能够反映自治域历史行为变化与未来行为可信程度的预期. 为此将基于现网自治域行为特征的路由行为分类结果作为信誉量化的输入, 采用贝叶斯后验概率分析方法, 引入更新事件有效时间比率的概念以融合自治域路由行为的发出频率、有效时长等因素建立自治域信誉量化指标, 用于自治域间的信誉评价.

4.1　自治域行为特征

常规 BGP 异常检测驱动的特征指标基于全网 BGP 更新路由数据提取, 以反映整个域间路由系统的安全状态 [22], 并非针对单个自治域路由行为进行刻画. 本小节通过分析 BGP 事件前后自治域路由行为在更新数量、间隔时长等方面的变化, 提取能够反映单个自治域发出正常/异常 BGP 宣告 (announce) 和撤回 (withdraw) 行为模式差异的统计特征. 例如, 恶意自治域为了避免被列入黑名单, 会在短时间内周期性地宣告某些前缀, 造成攻击 IP 地址空间碎片化及扰动; 而合法自治域的宣告和撤回行为主要是由正常网络操作 (如流量负载均衡、本地策略更改) 驱动的, 在宣告前缀数量、更新时间间隔等方面会表现出不同于恶意自治域的行为特征 [6].

为了将多源冲突和子前缀劫持等多种情况考虑在内, 我们将自治域与声明前缀 (AS-prefix) 的组合视为一个更新事件进行分析. 例如由自治域 a 声明的前缀 p 及其子前缀 p' 被视为 (a,p) 和 (a,p') 两个更新事件对象进行特征提取与分类. 我们选取了 7 个自治域行为特征指标, 并从 BGPmon 提供的 BGP 事件报告中选取已知域间路由安全事件对应时间段的路由更新数据进行测量 (如图 2 所示), 以说明自治域行为特征提取的合理性, 具体如下.

- 宣告更新数量 (announcement number, Anum) 指自治域对某目的前缀进行宣告的数量. 图 2(a)

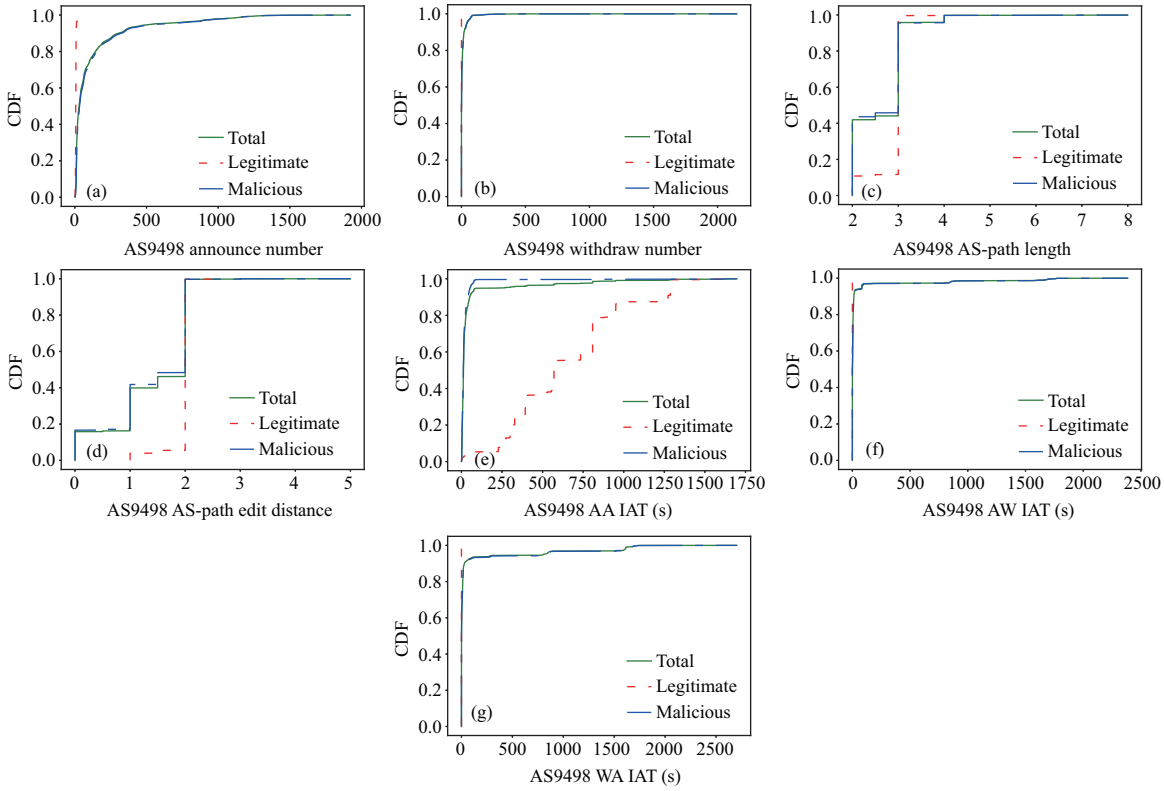

图 2 (网络版彩图) AS9498 行为特征统计 (2015.11.06 10:00∼11:00UTC). (a) 宣告更新数量; (b) 撤回更新数量; (c) 宣告路径长度; (d) 路径编辑距离; (e) 重复宣告间隔; (f) 宣告撤回间隔; (g) 撤回宣告间隔

Figure 2 (Color online) AS9498 behavior feature statistic (2015.11.06 10:00∼11:00UTC). (a) Anum; (b) Wnum; (c) APL; (d) APED; (e) AA IAT; (f) AW IAT; (g) WA IAT

为 AS9498 在异常行为期对所有前缀发出宣告的数量, 可以看到该时段 AS9498 发出的大部分宣告为非法前缀宣告.

• 撤回更新数量 (withdrawal number, Wnum) 指自治域对某目的前缀进行撤回的数量. 图 2(b) 为 AS9498 在异常行为期对所有前缀发出撤回的数量, 可以看到该时段 AS9498 没有对合法前缀进行撤回, 但撤回了少量非法前缀.

• 宣告路径长度 (AS-path length, APL) 指自治域对某目的前缀进行宣告的路径长度, 可反映相应前缀的可见性. 图 2(c) 展示了 AS9498 在异常行为期所有前缀宣告的平均路径长度, 可观察到 AS9498 宣告非法前缀对应的路径长度更长.

• 宣告路径编辑距离 (AS-path edit distance, APED) 是自治域对某目的前缀宣告的路径差异程度的量化, 用于反映自治域发出更新事件的路径稳定性 [19, 23]. 宣告路径编辑距离借鉴度量字符序列差异的字符串度量标准 (Levenshtein distance). 例如 ASa 分别在 t 时刻与 $t+1$ 时刻声明了通往属于 ASd 的某目的前缀的两条路径 $r_t = [a, b, c, d]$ 及 $r_{t+1} = [a, b, d]$, 则 APED$(r_t, r_{t+1}) = 1$. 图 2(d) 展示了 AS9498 在异常行为期宣告的所有前缀对应的路径编辑距离, 可观察到 AS9498 宣告非法前缀对应的更新事件的路径编辑距离变化范围更广.

• 重复宣告间隔 (announce-announce inter-arrival time, AA IAT) 是自治域对同一目的前缀重复宣告行为的时间间隔, 用于刻画自治域宣告行为模式的动态特征 [4]. 图 2(e) 展示了 AS9498 在异常行为

期对所有前缀进行重复宣告行为的平均时间间隔, 可观察到相较于合法前缀, 对非法前缀的重复宣告间隔更短.

• 宣告撤回间隔 (announce-withdraw inter-arrival time, AW IAT) 是自治域对同一目的前缀宣告后再撤回的时间间隔, 代表自治域通往某目的前缀的可达时间 [4]. 图 2(f) 展示了 AS9498 在异常行为期对所有前缀的平均宣告撤回时间间隔, 可观察到 AS9498 仅对部分非法前缀进行了宣告撤回操作.

• 撤回宣告间隔 (withdraw-announce inter-arrival time, WA IAT) 是自治域对同一目的前缀撤回后再宣告的时间间隔, 代表自治域通往某目的前缀的恢复时间 [4]. 图 2(g) 为 AS9498 在异常行为期对所有前缀的平均撤回宣告间隔, 可观察到 AS9498 仅对部分非法前缀进行了撤回宣告操作.

根据上述分析, 提取的自治域在通告数量、路径长度、时间间隔方面的行为特征在正常模式与异常模式中差异显著. 由于自治域在观察时间周期内通常会对同一前缀发出多个更新事件, 难以用单一的数值特征来刻画. 为此除宣告/撤回更新数量两个特征外, 对其余特征将自治域声明每个前缀统计值的概率分布用 3 个特征值表示: 第 5 百分位、第 95 百分位和中位数. 将这 3 个值包括在整个特征向量中, 构成统计特征向量. 因此, 共计提取 17 个特征值构成特征向量用于描述针对每个前缀的自治域行为安全特征向量.

基于以上自治域行为特征, 将 RIPE 项目提供的 BGP 路由现网数据[6)] 中各自治域发出的历史路由行为划分为正常/异常集合, 作为自治域信誉计算的输入. 我们将 RouteViews BGP monitors 提供的 IP 归属数据集[7)] 作为依据, 对已知 BGP 安全事件期间的路由更新数据进行标签化, 构成训练集, 进而从 2015 年 11 月全采集点的 BGP 路由更新数据中提取每个自治域行为的统计特征向量作为分类对象. 通过比较多种分类算法, 发现随机森林算法能够适应自治域行为统计特征向量的多维度与重尾特性, 具有更高的分类结果准确率, 且已较好地用于现有自治域行为分类工作中 [4, 6]. 因此选取随机森林 (random forest, RF) 算法 [24] 对训练集进行学习生成分类器, 进而基于本文自治域行为特征统计向量对更新事件进行分类, 其结果准确率为 0.9872. 在 ASCIR 自治域信誉评价计算时, 我们以上述历史更新事件分类结果作为输入, 实际应用部署中, 参与自治域可依据本地检测方法对被评价自治域行为的判别结果计算本地信誉评价.

4.2 贝叶斯统计信誉计算

本小节提出一种基于贝叶斯后验概率分析的信誉量化指标 BQR (Bayesian-estimation-based quantitative reputation), 用于刻画自治域在更新频率、有效时长等方面的行为可信趋势.

文献 [16] 指出, 自治域是否宣告一个正常路由更新可视为二分类结果的随机事件, 其后验概率分布服从 Beta 分布 [25] 的特性. Beta 分布是一种连续性概率密度分布, 随机变量 X 服从参数 α, β 的 Beta 分布通常表示为 $X \sim \mathrm{Beta}(\alpha, \beta)$, 由两个形状参数 α, β 决定 [25], 一般被用于建模伯努利试验 (Bernoulli experiment) 事件成功概率的概率分布. Beta 分布的概率密度函数可用伽玛函数 Γ 表示为

$$f(x|\alpha,\beta)=\frac{x^{\alpha-1}(1-x)^{\beta-1}}{\int_0^1 t^{\alpha-1}(1-t)^{\beta-1}\mathrm{d}t}=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1},\qquad 0\leqslant x\leqslant 1,\ \alpha{>}0,\ \beta{>}0, \tag{1}$$

且 Beta 分布的概率期望值为 $\mathrm{E}(x)=\frac{\alpha}{\alpha+\beta}$. 文献 [16] 将已知自治域发出更新正常/异常次数作为 Beta 函数的形状参数, 计算后验概率的期望值 (即该自治域下一次宣告合法路由的概率) 作为该自治域的信誉评价.

6) https://www.ripe.net/analyse/internet-measuments/routing-information-service-ris.

7) http://data.caida.org/datasets/routing/routeviews-prefix2as/2015/11/.

然而 BGP 在通过更新报文传播可达信息时, 每个更新事件中的前缀有效时间通常是分散的 [6], 更新事件的有效时间与自治域发出通告行为的数量、频率、影响程度均相关. 在计算自治域行为信誉评价量化指标时, 不仅需要考虑自治域发出正常/异常更新事件的数量, 还需将更新事件对应的前缀有效时间作为衡量自治域行为状态的重要因素. 因此我们引入更新事件有效时间比率及更新事件加权次数的概念, 作为贝叶斯统计权重, 用于刻画每个更新事件发生的频率及产生的影响.

自治域发起的更新事件的有效时间指该事件对应前缀的可达时间, 代表该更新事件的影响程度. 更新事件有效时间与观察时间周期的比率可作为贝叶斯统计的权重. 下面给出更新事件有效时间比率 (update active time ratio, UAT) 的定义.

定义1 更新事件有效时间比率:

$$\mathrm{UAT}(u,T)=\frac{\sum_{t_u\in T}\mathrm{AA\ IAT}(u)+\mathrm{AW\ IAT}(u)}{T}, \tag{2}$$

其中 T 为时间周期, u 为在时间周期 T 内目标自治域发起的更新事件, 对应该自治域与更新事件 u 声明前缀的组合 (AS-prefix). AA IAT(u) 为更新事件 u 被重复宣告的时间间隔, AW IAT(u) 为更新事件 u 在宣告后被撤回的时间间隔. 将更新事件 u 在时间周期 T 内每一次被重复宣告与宣告后撤回的时间间隔求和得到更新事件 u 在时间周期 T 内的有效时间, 其与时间周期 T 的比值即为更新事件 u 在时间周期 T 的有效时间比率, 记为 UAT(u,T).

在进行自治域信誉量化时, 将目标自治域在时间周期 T 发出的正常/异常行为分为两个集合, 分别对每个集合中的更新事件以其有效时间比率作为权重进行加权累计求和, 作为贝叶斯统计信誉计算的输入. 下面给出在时间周期 T 中自治域类别为 X 的更新事件加权累计次数 $\langle U_T^X\rangle$ 的定义.

定义2 更新事件加权累计次数:

$$\langle U_T^X\rangle=\sum_{u\in U_T^X}\mathrm{UAT}(u,T),\quad X\in\{G,B\}, \tag{3}$$

其中 X 表示更新事件所属集合的类型, G 代表正常更新事件集合, B 代表异常更新事件集合, U_T^X 代表在观察时间周期 T 内类型为 X 的更新事件集合, UAT(u,T) 为在观察时间周期 T 中更新事件 u 的有效时间比率. 将 U_T^X 集合中的每个更新事件的有效时间比率作为权重, 对集合中所有更新事件加权求和, 得到在时间周期 T 中所有 X 类型更新事件的加权累计次数, 记为 $\langle U_T^X\rangle$.

基于 4.1 小节的自治域行为分析, 可将目标自治域在观察时间周期内发出的更新事件分为正常更新事件集合 U_T^G 与异常更新事件集合 U_T^B, 并分别统计每个集合对应的加权累计次数 $\langle U_T^G\rangle$ 和 $\langle U_T^B\rangle$. 基于对目标自治域在已有观察时间周期内行为的观察, 我们将用于刻画该自治域下一次发出正常更新事件的概率密度函数 Beta(α,β) 的形状参数 α 与 β 设置如下:

$$\alpha=\langle U_T^G\rangle+1;\quad \beta=\langle U_T^B\rangle+1,\qquad \langle U_T^G\rangle,\ \langle U_T^B\rangle\geqslant 0. \tag{4}$$

令 p 表示目标自治域下一次发出正常更新事件的概率, 根据式 (1) 与 (4), 目标自治域的信誉函数可用 p 的 Beta 概率密度函数表示为

$$\phi\left(p|\langle U_T^G\rangle\ \langle U_T^B\rangle\right)=\frac{\Gamma(\langle U_T^G\rangle+\langle U_T^B\rangle+2)}{\Gamma(\langle U_T^G\rangle+1)\Gamma(\langle U_T^B\rangle+1)}p^{\langle U_T^G\rangle}(1-p)^{\langle U_T^B\rangle},\qquad 0\leqslant p\leqslant 1,\ \langle U_T^G\rangle\geqslant 0,\ \langle U_T^B\rangle\geqslant 0. \tag{5}$$

自治域下一次发出正常更新事件概率的期望可代表其量化信誉值 [25], 即计算式 (5) 的期望. 下面具体给出 ASCIR 中的自治域信誉量化指标的定义.

定义3 (自治域信誉量化指标) 令 $\langle U_T^G \rangle$ 和 $\langle U_T^B \rangle$ 分别表示在时间周期 T 中评价自治域 e 在本地收到被评价自治域 a 发出的正常更新事件的加权累计次数与异常更新事件的加权累计次数, 自治域 a 的信誉函数表示为 $\phi(p|\langle U_T^G \rangle \langle U_T^B \rangle)$. 评价自治域 e 对被评价自治域 a 的量化信誉评价值为

$$\mathrm{Eval}(e,a) = \mathrm{E}\left(\phi\left(p|\left\langle U_T^G\right\rangle \left\langle U_T^B\right\rangle\right)\right) = \frac{\langle U_T^G \rangle + 1}{\langle U_T^G \rangle + \langle U_T^B \rangle + 2}. \tag{6}$$

采用上述方法, 自治域可依据本地接收到的路由通告数据, 对各被评价的目标自治域分别计算本地信誉评价量化指标. 上述自治域信誉量化指标建立在评价自治域与被评价自治域之间累积路由信息交互的基础上, 融合了自治域通告行为频率、通告前缀有效时长等多方面因素, 能够细粒度地捕捉自治域的行为模式.

5 自治域全局信誉计算

在域间路由系统中, 每个自治域都只能以局部视角获取部分信息, 因此基于本地路由数据得到的被评价自治域信誉具有一定局限性. 域间路由自治域间通过协同共享本地信誉评价, 可以对被评价自治域行为获取更全面的信誉评价. 为了保证全局信誉聚合结果的准确性, 通过研究自治域属性与本地信息完整程度的关系, 设置能够反映域间路由自治域节点重要度的权重, 加权聚合多自治域节点对被评价自治域的本地评价; 为了捕捉自治域在时间上的行为连续性, 设置时间衰减函数, 综合其历史信誉与当前反馈, 对信誉进行动态更新.

5.1 自治域评价权重

本地自治域获取信息的全面性和准确性受限于其拓扑位置及信息来源 [6]. 为了获取被评价自治域行为更全面的信誉评价, 评价自治域需聚合其他自治域的本地信誉评价, 对每个参与自治域的本地信誉评价设置聚合权重对最终全局聚合结果的准确性至关重要. 节点权重的设置需符合域间路由系统的实际, 反映参与自治域在网络中的节点重要程度和信息全面程度.

在针对域间路由系统中自治域节点重要度的研究中, 自治域的下游客户个数 (customer cone)、可达子网数量 (IP space) 和连接度数 (degree) 普遍被认为是反映节点重要度的属性 [26]. 但尚没有相关工作针对自治域本地信息全面程度进行分析, 且自治域本地信息完整程度的概念并不明确. 为了分析自治域节点本地信息的全面程度与其相关属性之间的关系, 我们对 2015 年 11 月的路由数据进行测量分析. 首先统计每个时间窗口中所有接收到 AS9498 发出通告的自治域本地视角下的 AS9498 行为特征 (AS9498 发出更新报文中 AS-path 上的其他 AS 为接收 AS), 这里时间窗口设置为 RIPE 提供 BGP 数据的时间间隔, 即 5 min; 然后基于 AS9498 发出的所有更新数据提取 AS9498 行为特征并计算其与各接收 AS 本地行为特征的欧式距离, 简称为特征距离 (feature distance); 最后分析各接收 AS 本地特征距离与下面 3 个属性之间的相关性.

- 下游客户数量指自治域作为服务提供商 (Internet service provider, ISP) 与其他自治域建立连接的个数. 下游客户数量代表了自治域在域间路由系统中提供网络可达服务的能力, 通常用于自治域排序 (AS-ranking). 图 3(a) 展示了评价自治域的特征距离与相应的下游客户个数, 可观察到相较于自治域平均客户数量, 下游客户数量较少和较多的评价自治域本地特征距离较小.
- 可达子网数量指自治域拥有的可声明的地址空间. 文献 [27] 分析指出自治域可达子网数量可作为衡量自治域在域间路由系统中经转流量的重要度指标. 图 3(b) 展示了评价自治域特征距离与相应

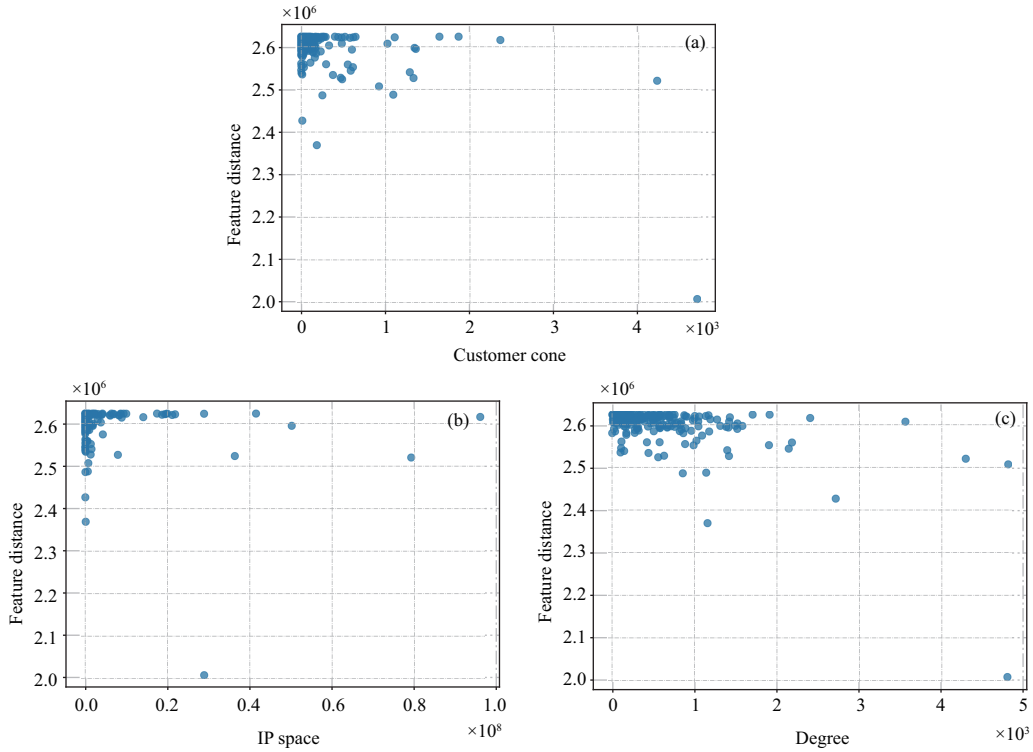

图 3 (网络版彩图) 自治域本地特征距离与其网络属性的相关性. (a) 自治域客户数量与特征距离; (b) 自治域 IP 子网数量与特征距离; (c) 自治域度数与特征距离

Figure 3 (Color online) The correlation between AS local feature distance and its network properties. (a) AS customer cone and feature distance; (b) AS IP subnets and feature distance; (c) AS degree and feature distance

的可达子网数量, 可观察到本地特征距离较小的评价自治域所对应的可达子网数量相对于平均子网数量较少或较多.

- 连接度数指自治域在域间路由系统中与其他自治域建立逻辑连接的个数, 为自治域节点的网络拓扑属性. 在复杂系统中, 节点度数为衡量节点重要度的通用指标. 图 3(c) 展示了评价自治域本地特征距离与相应的连接度数, 可观察到自治域连接度数越大的节点对应的本地特征距离越小.

由上述分析可知, 自治域本地信息全面程度与其在域间路由系统中的连接度数呈正相关关系. 此外, 大部分自治域的本地信息完整程度相差不大, 本地信息非常完整或非常匮乏的自治域所占的比例很少. 这也说明自治域协同共享信息的重要性. 根据上述测量结果, 我们在 ASCIR 全局信誉聚合算法中, 选用自治域节点的度数作为其评价的权重要素, 以此反映自治域在信息共享中的重要程度. 下面分别给出本地评价权重和邻居评价权重的定义.

定义4 本地评价权重:

$$\alpha_e = \frac{\mathrm{Degree}_e}{\max_{a_m \in A} \{\mathrm{Degree}_{a_m}\}}, \tag{7}$$

其中 A 为所有自治域组成的集合, a_m 为 A 集合中连接度数最大的自治域节点, Degree_{a_m} 为 a_m 的连接度数, Degree_e 为评价自治域 e 的连接度数, 本地评价权重 α_e 代表了评价自治域节点 e 的评价意见在信誉网络中的重要程度.

定义5 邻居评价权重:

$$\beta_{ev} = \frac{\text{Degree}_v}{\sum_{k \in N_e} \text{Degree}_k}, \tag{8}$$

其中 N_e 为评价自治域 e 邻居节点中参与评价的投票自治域集合, Degree_v 为投票自治域 v 的连接度数, k 为 N_e 集合中的投票自治域, Degree_k 为 k 的连接度数, β_{ev} 代表了 e 视角下投票自治域 v 反馈的信誉评价的相对重要程度.

5.2 全局信誉聚合算法

ASCIR 的自治域全局信誉算法聚合算法针对域间路由实际, 在 P2P 网络中经典的信誉聚合算法 EigenTrust [28] 的基础上进行改进. 不同于 P2P 网络中的文件下载行为, 自治域发出路由行为相对独立, 且信息相对完整的参与节点通常集中分布在少数路径上, 为此设计了自治域全局信誉聚合算法 (global reputation aggregate algorithm, GRA), 面向域间路由系统实际改进了 EigenTrust 分布式信誉机制中的权重设置与收敛判断部分, 以保证全局信誉值的准确性. 在信誉聚合过程中, 评价自治域可根据本地对聚合信誉全面性的需求指定聚合轮次阈值, 然后问询信誉协同网络中与本地相邻的节点关于被评价自治域的信誉评价反馈, 从中选取与被评价自治域具有交互历史的节点构成投票自治域集合. 投票自治域可继续向自己的邻居节点收集信誉评价反馈, 直到达到指定聚合轮次阈值且所有信誉评价反馈经加权综合后收敛为止.

具体地, 全局信誉反馈聚合算法如算法 1 所示. 算法输入包括自治域信誉协同网络 $G(A, E)$, 评价自治域 e, 被评价自治域 a 以及由 e 指定的聚合轮次阈值 K. 首先初始化除 e 和 a 以外的所有在信誉协同网络 G 中的自治域节点是否投票属性和初始全局信誉评价, 将 e 的投票属性标记为 True 并把其初始全局信誉评价赋为本地评价 $\text{Eval}(e, a)$ (1~3 行); 然后初始化投票自治域队列 Q 并将 e 入队, 初始化聚合轮次 k (4~7 行); 接着, 开始信誉聚合, 每轮次聚合中从投票自治域队列 Q 中出队的自治域节点作为信誉评价的问询方, 扫描该节点的邻接链表, 将与本地相邻且与 a 具有交互历史的自治域节点纳入本轮次投票集合, 加权综合其最新信誉评价, 根据反馈信誉评价更新本地信誉评价值 (8~17 行). 最后, 在每次聚合后评价自治域 e 根据本地投票自治域集合中节点的最新信誉评价计算对 a 的全局信誉评价, 当聚合轮次达到指定阈值且全局信誉评价收敛后返回 e 获取的全局信誉评价 (18~26 行).

将与被评价自治域 a 具有交互的投票自治域节点集合表示为 V, 投票节点之间的连接关系集合表示为 E_V. 算法 1 在初始化后, 不会再给任何参与节点的投票属性标记为 False, 因此每个参与节点入队次数与出队次数最多仅为一次, 且入队和出队的时间均为 $O(1)$. 考虑需遍历所有与 a 具有交互历史的投票自治域节点 V 的最坏情况, 对队列进行操作的总时间为 $O(V)$. 算法只在一个节点出队时才对其邻接链表进行扫描, 因此每个邻接链表最多只扫描一次. 由于所有投票节点的邻接链表长度之和为 $\Theta(E_V)$, 用于聚合邻居节点信誉评价的总时间为 $O(E_V)$. 因此算法 1 的运行复杂度在最坏情况下为 $O(V + E_V)$. 值得注意的是, 我们基于 BGP 现网数据对超过 20000 个自治域发出路由通告的接收自治域数量进行了统计, 90% 自治域路由通告行为的接收自治域数量均在 200 个以内, 最多没有超过 300 个接收自治域, 说明实际中全局信誉聚合并不需过多计算就能够返回信誉评价反馈. 将每轮次中的 α 值记为常数 c, 则第 k 轮次的投票自治域反馈的信誉评价在聚合结果中的权重为 $c(1-c)^k$, 且 $0 < c < 1$, 因此最终得到的信誉评价聚合结果是收敛的. 文献 [28] 中使用马尔科夫链 (Markov chain) 稳态分布的概率解释证明了算法返回信誉聚合结果的收敛性.

算法 1 AS global reputation aggregate algorithm

Input: AS reputation cooperative network $G(A, E)$, evaluating AS e, evaluated AS a, aggregate round threshold K;
Output: Global reputation evaluation R_{ea};

for $n \in G.A - \{e, a\}$ **do**
  n.voted $\Leftarrow$ False, $n.R(n, a) \Leftarrow \text{Eval}(n, a)$;
end for
e.voted $\Leftarrow$ True, $e.R(e, a) \Leftarrow \text{Eval}(e, a)$;
Initialize voting AS queue $Q \Leftarrow \emptyset$;
ENQUEUE(Q, e);
Initialize aggregate round $k \Leftarrow 0$;
while $Q \neq \emptyset$ **do**
  $v \Leftarrow$ DEQUEUE(Q);
  Initialize reputation evaluation feedback list of current round FeedbackList $\Leftarrow \emptyset$;
  for $u \in G$.neibor(v) **do**
    if u.voted = False **and** u and a have interaction history **then**
      FeedbackList.append$(\beta_{vu} u.R(u, a))$;
      ENQUEUE(Q, u);
    end if
  end for
  $v.R(v, a)^{(k+1)} = \alpha_v v.R(v, a)^{(k)} + (1 - \alpha_v) \sum_{f \in \text{FeedbackList}} f$;
  $e.R(e, a)^{(k+1)} = \alpha_e e.R(e, a)^{(k)} + (1 - \alpha_e) \sum_{m \in G.\text{neibor}(e)} \beta_{em} m.R(m, a)^{(k+1)}$;
  Calculate $\delta = \left| e.R(e, a)^{(k+1)} - e.R(e, a)^{(k)} \right|$;
  if $\delta < \varepsilon$ **and** $k > K$ **then**
    return $e.R(e, a)^{(k+1)}$;
    break;
  end if
  $k \Leftarrow k + 1$;
end while
return $e.R(e, a)^{(k)}$.

5.3 信誉评价动态更新

为了使自治域信誉评价能够反映其历史行为与实时状态, 在得到当前时间窗口的被评估自治域信誉评价后, 需要将其与历史已经建立的信誉评价进行综合, 动态更新被评估自治域的信誉评价. 信誉评价动态更新使得评估自治域在被评估自治域没有发出行为或连续发出异常更新行为的情况下仍然可通过其信誉值预测其未来行为的可信性.

信誉系统中的更新机制主要为了捕捉信誉在时间上的连续特性, 赋予新的信誉反馈更多的权重, 逐渐减少旧反馈的影响 [17, 25, 29], 但已有信誉更新方法并未针对自治域行为特性设计. 实际域间路由系统中, 不同因素导致的自治域异常行为在时间维度上会表现出不同的行为模式 [6]. 恶意攻击自治域会在攻击期间频繁宣告大量前缀, 但在攻击后的较长时间中不发出任何更新报文; 合法自治域即使因为误配置等偶然因素在短期内具有异常行为, 但在较长时间范围中的更新行为都较为稳定. 针对自治域行为在时间维度上的不同行为模式, ASCIR 的信誉评价动态更新需依据以下实际需求设计: (1) 在自治域行为中断期间仍能够基于其历史行为更新当前信誉值; (2) 针对自治域连续异常行为适度惩罚; (3) 针对自治域由偶然因素引发的异常行为具备一定时间遗忘效应. 为此, ASCIR 在更新信誉评价时引入时间衰减函数, 使自治域发出异常行为后的信誉值遵循社交网络中实体信誉值快速下降、慢速上升的规律变化; 并通过设置时间遗忘阈值, 逐步减小前期异常行为对当前信誉值的影响, 避免自治域

信誉评价受到误配置等偶然事件的持续影响. ASCIR 的信誉动态更新时间衰减函数定义如下.

定义6 时间衰减函数:

$$D(t)=\mathrm{e}^{-\frac{c}{(t-t_e^i)|\mathrm{th}}},\qquad t\in\left[t_e^i,t_e^{i+1}\right),\ c<T, \tag{9}$$

其中 $D(t)$ 为在 t 时刻计算信誉更新的时间衰减函数, t_e^i 为 t 时刻前最后一次检测出发生异常事件的时刻, t_e^{i+1} 为 t 时刻后的首次异常事件时刻, c 为小于时间周期 T 的常数, th 为时间遗忘阈值.

信誉值动态更新函数计算如下:

$$R_{ea}=D(t)R_{ea}^{t-T}+(1-D(t))R_{ea}^{t}, \tag{10}$$

其中 $D(t)$ 为时间衰减函数, R_{ea}^{t-T} 为上一时间周期结束时评价自治域 e 对被评价自治域 a 建立的信誉评价值, R_{ea}^{t} 为在当前时间周期结束的 t 时刻, e 通过全局信誉聚合算法得到对 a 的信誉评价反馈值, R_{ea} 为更新的信誉值, 信誉值动态更新后的最终结果是已建立的信誉与当前信誉值反馈的加权和.

上述信誉动态更新方法使得信誉评价能够随着自治域间交易累积和时间推移综合自治域实时行为与历史信誉, 反映其未来行为正常的趋势, 从而对自治域连续异常行为进行适度惩罚, 使评价自治域能够针对其他自治域异常行为提前规划相应防御措施, 抑制自治域连续异常行为的进一步传播.

6 仿真实验

本节通过构建域间路由仿真网络拓扑并基于真实 BGP 事件开展实验, 分别对 ASCIR 信誉模型中信誉量化指标、全局信誉聚合算法和信誉动态更新方法的有效性进行分析.

6.1 网络拓扑与实验设计

基于 CAIDA 域间路由拓扑数据和 RIPE 项目提供的 BGP 路由数据, 构建了一个节点个数为 51779, 边个数为 219733 的仿真网络拓扑. 实际域间路由系统中有 63100 个自治域, 包括 9000 个中转自治域 (transit AS) 和 54100 个底层自治域 (stub AS). 只有 20000 ~ 40000 个自治域生成大部分的 BGP 更新报文, 其余自治域极少参与转发更新报文. 为了保证仿真网络拓扑中的节点均出现在 BGP 更新报文中, 并可依据现网数据获取节点相关属性以在信誉聚合时分配相应权重, 我们首先从不同时段的 BGP 路由数据中提取语义信息, 提取 AS-path 中出现的高频 AS 构成集合一; 然后从 CAIDA 提供的域间路由拓扑数据集[8]、AS 关系数据集[9] 以及 RouteView BGP monitors 提供的路由信息表 RIB 数据集[10] 中提取信息完整的 AS 构成集合二; 最后将两个集合取交集构成仿真网络拓扑中的节点集合. 仿真实验以发生于 2015 年 11 月 6 日的 AS9498 (BHARTI Airtel Ltd.) BGP 劫持事件为背景, 基于 RouteViews 和 RIPE RIS 提供的历史真实 BGP 更新报文数据对 AS9498 的安全状态进行分析, 量化评估其信誉度变化以及其他节点对其信誉的本地评价与全局聚合结果, 分别对自治域信誉量化指标与全局信誉模型的有效性进行验证.

6.2 信誉量化指标有效性分析

为了评估 ASCIR 中贝叶斯信誉量化指标 BQR 的有效性, 我们对 2015 年 11 月 6 日全天数据进行分析. AS9498 劫持事件时间约持续 10 个小时, 为了细粒度地刻画 AS9498 在事件不同阶段行为的

8) http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml.
9) http://www.caida.org/data/active/as-relationships/.
10) https://www.ripe.net/analyse/internet-measuments/routing-information-service-ris.

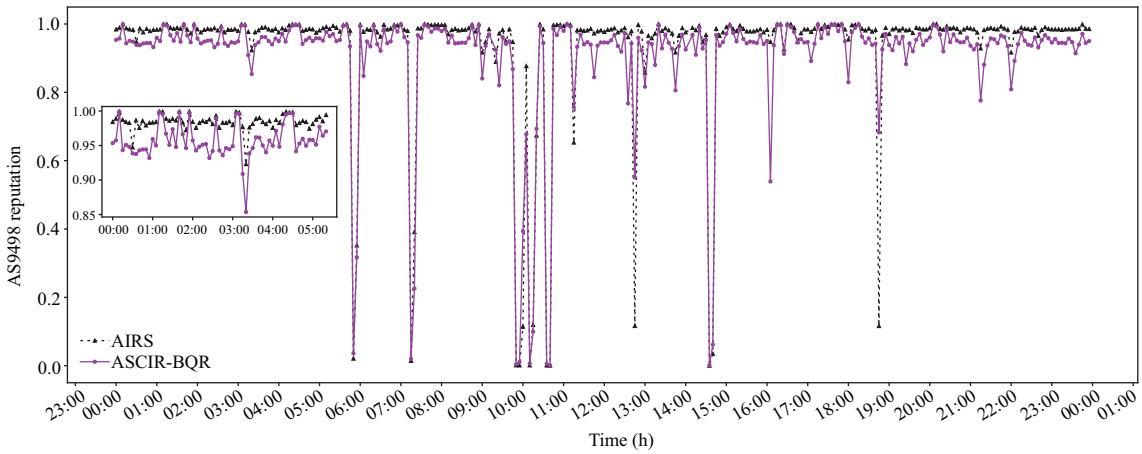

图 4 (网络版彩图) AS9498 的信誉量化评价 (2015.11.06)

Figure 4 (Color online) Quantitative evaluation of AS9498 reputation (2015.11.06)

变化, 设置信誉评价时间窗口为 5 min. 我们分别采用 4.2 小节中的贝叶斯信誉量化方法与 AIRS [16] 中的信誉计算方法对 AS9498 的行为可信度进行量化并进行比较, 如图 4 所示.

从图 4 可看出, 根据 BGP 现网更新数据计算的 AS9498 在 2015 年 11 月 6 日事件当天的信誉值首次急剧降低于 05 : 50 UTC 左右, 接着在 07 : 10, 10 : 00∼11 : 00, 12 : 40 和 14 : 40 UTC 存在数次信誉值急剧降低的情况, 最后的信誉值急剧下降时间为 14 : 40 UTC, 之后没有信誉值低于 0.5 的情况. 根据 BGPmon 给出的 2015 年 11 月 6 日 AS9498 (BHARTI Airtel Ltd.) BGP 劫持的事件报告, 当天 05 : 52 UTC, AS9498 开始宣告大量不属于本地的前缀, 然后在接下来的数个小时中持续间歇性的宣告异常前缀, 直到 14 : 40 UTC 清除最后一个异常宣告. 图 4 中 ASCIR 的信誉量化指标 BQR 的变化趋势与事件报告中吻合, 这表明 ASCIR 的信誉量化方法可以反映自治域在事件不同阶段的行为可信程度变化.

对比分析图 4 中分别使用 ASCIR 与 AIRS [16] 中的信誉量化方法计算得到的 AS9498 信誉评价, 可在左边的局部放大子图中观察到在 00 : 00 ∼ 05 : 00 UTC 事件发生前的正常行为期, 相较于 AIRS 信誉指标, ASCIR 的信誉指标 BQR 的变化幅度更大, 能够更清晰地反映自治域在正常期的细微行为变化; 在 05 : 00 ∼ 15 : 00 UTC 的异常行为期, 两者均在同时刻出现骤降, 但 ASCIR-BQR 信誉指标在骤降前会表现小幅的下降趋势; 在 15 : 00 UTC 后的事件发生后期, ASCIR-BQR 信誉指标的下降均未低于 0.5, 能与事件期间的异常行为信誉值波动加以区分, 而 AIRS 信誉值下降幅度较大, 易与事件期间的信誉值下降混淆. 由上述分析可知, ASCIR 中的信誉量化指标 BQR 能够更加准确地对目标自治域处于非行为密集期的正常时段及劫持事件不同阶段的行为进行刻画.

6.3 全局信誉计算有效性分析

为了评估 ASCIR 中对全局信誉计算的有效性, 我们选取 AS9498 作为被评价自治域, 选取 AS6762 作为评价自治域, 针对 AS9498 在 2015 年 11 月 6 日 03 : 00 ∼ 16 : 00 UTC 的路由行为进行信誉评价、聚合与更新, 分别对 ASCIR 中全局信誉聚合算法 GRA 与信誉动态更新方法进行验证.

为了评估 ASCIR 的全局信誉聚合算法 GRA 的有效性, 我们对比分析了 AS6762 在 2015 年 11 月 6 日 03 : 00 ∼ 16 : 00 UTC 每个时间片中采用 ASCIR-GRA 算法与 AIRS [16] 和 ReMSA [17] 中的信誉聚合算法得到的 AS9498 信誉评价, 如图 5 所示. 图 5 中 Global view 对应的曲线为基于全网数

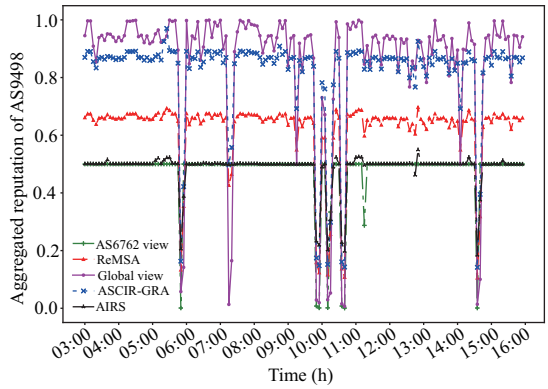

图 5 (网络版彩图) 自治域信誉聚合算法有效性分析

Figure 5 (Color online) Efficacy analysis of reputation aggregate algorithms

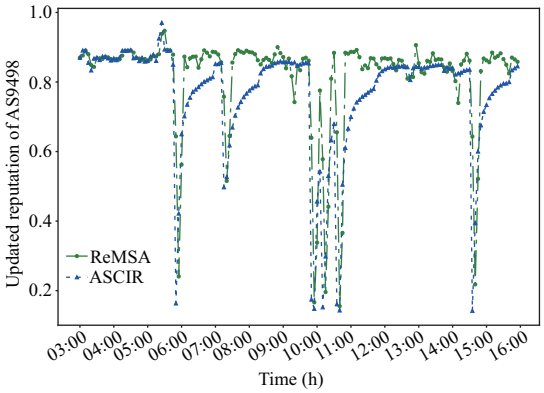

图 6 (网络版彩图) 自治域信誉更新方法有效性分析

Figure 6 (Color online) Efficacy analysis of reputation update methods

据分析 AS9498 在每个观察时间周期中的路由通告行为得到的信誉值, AS6762 view 对应的曲线为分析 AS6762 作为接收 AS 收到的 AS9498 路由通告行为得到的信誉值, 可观察到两者相差较大, 每个时间周期中对 AS9498 的本地信誉评价与全局视角 AS9498 信誉值的平均差值为 0.4039, 说明 AS6762 仅通过本地数据无法获取 AS9498 的真实信誉状态. 分别使用 AIRS 和 ReMSA 中的信誉聚合算法计算 AS6762 作为评价自治域对 AS9498 信誉评价进行聚合的结果并计算与 AS9498 全局信誉值的差值. AIRS 和 ReMSA 对 AS9498 的信誉聚合值在每个时间周期中与全局视角 AS9498 信誉值平均差值分别为 0.4065 与 0.2600. ASCIR-GRA 对应曲线为采用 ASCIR 的全局信誉聚合算法 GRA 在每个时间周期中得到的聚合信誉值, 与全局视角信誉评价平均差值为 0.0811. ASCIR-GRA 信誉聚合结果与全局信誉的差值分别比使用 REMSA, AIRS 中的信誉聚合算法的差值减少了 80% 和 68%. 可以看出, 利用 ASCIR 全局信誉聚合算法得到的信誉值与分析全数据得到的 Global view 信誉值平均差距最小, 相较于已有算法, 本文的全局信誉聚合算法能够使评价自治域得到相对更全面的信誉评价.

为了评估信誉动态更新方法的有效性, 我们将 AS6762 作为评价自治域对 AS9498 在 2015 年 11 月 6 日 03 : 00 ∼ 16 : 00 UTC 期间每个观察时间周期的信誉评价聚合结果按时间顺序推移计算其动态更新后的信誉值, 并与 ReMSA [17] 中的信誉更新方法进行比较, 如图 6 所示.

图 6 展示了在 AS6762 视角下分别采用 ReMSA 和 ASCIR 的信誉更新方法对 AS9498 的信誉评价进行更新的计算结果 (这里 ASCIR 的遗忘时间阈值设置为 1 h). 可观察到 ReMSA 的信誉更新结果与 AS9498 在每个时间窗口中的信誉计算结果几乎相同, 这是因为 ReMSA 中的时间衰减函数仅将事件频率作为影响因素, 并未考虑自治域异常行为的连续特性. 观察 ASCIR 的信誉更新结果, 在 03 : 00 ∼ 05 : 00 UTC 的正常期与 ReMSA 的更新结果相同, 当 AS9498 在 05 : 52 出现异常行为后, 评价自治域对 AS9498 的信誉更新值遵循快降慢升的趋势变化, 并在达到时间遗忘阈值时减小前期异常行为对当前信誉值的影响, 对自治域连续异常行为进行适度惩罚.

从被评价自治域的角度看, 域间路由系统自治域节点的准入门槛较高, 自治域连续恶意行为将使其信誉持续受到惩罚, 从而付出高昂的代价. 因为一旦被公认为不可靠的自治域, 就很难重新正常运营; 从评价自治域的角度, 动态建立基于被评价自治域历史表现和实时状态的信誉评价, 能够帮助本地网络管理员及时更改路由选路策略, 更谨慎地与信誉较低的自治域建立商业关系, 从而抑制异常路由通告在域间路由系统中的不断传播.

7 讨论

7.1 部署激励问题

鉴于自治域独立管理和运维, 如何激励自治域部署域间路由信誉模型是一个具有挑战性的问题. 在域间路由系统中, 各自治域间具有竞争与合作并存的博弈关系, 一方面客户自治域依赖于运营商自治域提供的流量传输服务, 另一方面运营商自治域会互相竞争更多的客户自治域以获取更多的经济收益. 大多数自治域都具有维护安全稳定网络环境、孤立恶意自治域的动机. ASCIR 域间路由信誉模型通过参与自治域协同实现局部路由监测信息和知识的隐式共享. 对于客户自治域, 信誉模型能够帮助其克服本地信息局限性, 为其选取上游运营商、过滤异常路由、感知安全状态提供有效参考. 对于高层的运营商自治域, 信誉模型能够激励本地网络管理员谨慎操作, 降低误配置概率, 为本地服务安全性提供有效证明. 因此, 即使在没有额外激励机制的情况下, 自治域也具有一定的参与动机. 此外, 信誉系统领域的经济激励机制的研究成果 [30] 可为 ASCIR 的部署激励提供参考.

7.2 评价修正问题

实际域间路由运行中, 自治域某些异常路由宣告行为可能是为了满足特定商业目的或者流量工程, 由此导致自治域信誉评级下降. 如何对上述情况引发的自治域信誉下降进行快速修正是域间路由信誉模型在实际应用中需要考虑的问题. 根据文献 [6] 提供的测量结果, 不同因素导致的自治域异常行为在时间维度上会表现出不同的行为模式. 恶意攻击自治域会在攻击期间频繁宣告大量前缀, 但会在攻击后的较长时间中不发出任何更新报文; 合法自治域即使因为流量工程等偶然因素在短期内具有异常行为, 但在其他时间段中的更新行为都较为稳定. 因此, ASCIR 中的信誉动态更新方法中连续异常惩罚机制与时间遗忘阈值设置能够使不同类型自治域异常行为导致的自治域信誉变化呈现不同的变化趋势, 便于区分正常自治域与恶意自治域, 一定程度上修正由流量工程、误配置等偶然因素引起的信誉值降低.

7.3 恶意评价问题

域间路由系统中存在竞争关系的运营商可能会对竞争对手自治域提供恶意评价, 如何采信和避免恶意评价是决定域间路由信誉模型是否实用的重要因素. 在分布式信誉系统研究领域中, 研究者针对参与者的不诚实评价、恶意伪装、恶意合谋等攻击 [30] 提出了 EigenTrust++ [31], GroupTrust [32] 等方案. 这些方法引入基于节点直接信誉评价相似度的节点信誉评价可采信度评估、设置信誉传播阈值控制信誉聚合传播等措施, 以阻止不合理的信誉传播. 域间路由信誉模型的参与自治域逻辑上构成了协同共享信誉评价的覆盖网络, 与上述研究的适用情景具有共通性, 因此 EigenTrust++ 等方案中的恶意评价检测方法也适用于域间路由信誉模型. 此外, 近年来区块链以其去中心化、防篡改、可追溯的优势同时受到了域间路由安全 [8] 和分布式信誉系统领域 [33] 的关注. ASCIR 域间路由信誉模型也可结合区块链技术, 约束参与自治域的恶意评价行为, 实现自治域信誉的可靠传播.

8 结论

本文分析了域间路由系统分布自治、行为连续、信息不对称等特性, 提出了 ASCIR, 包括融合自治域路由行为更新频率、有效时长等多方面要素的自治域信誉量化指标, 以自治域连接度数作为权重要素的多域协同全局信誉聚合算法, 以及针对自治域连续异常行为的信誉更新方法. 实验结果表明,

ASCIR 的信誉量化指标能够反映自治域处于非行为密集期的正常时段及劫持事件不同阶段的行为变化; 能够实现在自治域本地信息受限情况下的全局信誉聚合, 并有效对发出连续异常行为的自治域信誉值进行惩罚. 下一步将针对域间路由信誉模型的激励部署策略与自治域恶意评价抑制开展进一步研究.

参考文献

1 Wang N, Du X H, Wang W J, et al. A survey of the border gateway protocol security. Chin J Comput, 2017, 40: 138–160 [王娜, 杜学绘, 王文娟, 等. 边界网关协议安全研究综述. 计算机学报, 2017, 40: 138–160]

2 Giotsas V, Luckie M, Huffaker B. Inferring complex as relationships. In: Proceedings of the 2014 Conference on Internet Measurement Conference, 2014. 23–30

3 Kuerbis B, Mueller M. Negotiating a new governance hierarchy: an analysis of the conflicting incentives to secure Internet routing. Commun Strategies, 2011, 1: 125–142

4 Konte M, Perdisci R, Feamster N. ASwatch: an AS reputation system to expose bulletproof hosting ASes. SIGCOMM Comput Commun Rev, 2015, 45: 625–638

5 Nordström O, Dovrolis C. Beware of BGP attacks. SIGCOMM Comput Commun Rev, 2004, 34: 1–8

6 Testart C, Philipp R, Alistair K, et al. Profiling BGP serial hijackers: capturing persistent misbehavior in the global routing table. In: Proceedings of the Internet Measurement Conference, 2019. 420–434

7 Chung T, Aben E, Bruijnzeels T, et al. RPKI is coming of age: a longitudinal study of RPKI deployment and invalid route origins. In: Proceedings of the Internet Measurement Conference, 2019. 406–419

8 Chen D, Qiu H, Zhu J H, et al. Research on blockchain-based interdomain security solutions. J Softw, 2020, 31: 208–227 [陈迪, 邱菡, 朱俊虎, 等. 区块链技术在域间路由安全领域的应用研究. 软件学报, 2020, 31: 208–227]

9 Resnick P, Kuwabara K, Zeckhauser R, et al. Reputation systems: facilitating trust in Internet interactions. Commun ACM, 2000, 43: 45–48

10 Ishmanov F, Zikria Y B. Trust mechanisms to secure routing in wireless sensor networks: current state of the research and open research issues. J Sens, 2017, 2017: 1–16

11 Sharma A, Pilli E S, Mazumdar A P, et al. Towards trustworthy Internet of Things: a survey on trust management applications and schemes. Comput Commun, 2020, 160: 475–493

12 Ge X H, Chen J Q, Wang C-X, et al. 5G green cellular networks considering power allocation schemes. Sci China Inf Sci, 2016, 59: 022308

13 Chang J, Venkatasubramanian K K, West A G, et al. AS-TRUST: a trust quantification scheme for autonomous systems in BGP. In: Proceedings of the Trust and Trustworthy Computing, 2011. 262–276

14 Chang J, Venkatasubramanian K K, West A G, et al. AS-CRED: reputation and alert service for interdomain routing. IEEE Syst J, 2013, 7: 396–409

15 Yu H, Rexford J, Felten E W. A distributed reputation approach to coopertive Internet routing protection. In: Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols, 2005. 73–78

16 Hu N, Zou P, Zhu P D. Reputation-based collaborative management method for inter-domain routing security. J Softw, 2010, 21: 505–515 [胡宁, 邹鹏, 朱培栋. 基于信誉机制的域间路由安全协同管理方法. 软件学报, 2010, 21: 505–515]

17 Lee J Y, Oh J C. A node-centric reputation computation algorithm on online social networks. In: Applications of Social Media and Social Network Analysis. Cham: Springer, 2015. 1–22

18 Xia N, Li W, Lu Y, et al. A trust model for the inter-domain routing system. J Comput Res Dev, 2016, 53: 845–860 [夏怒, 李伟, 陆悠, 等. 一种面向域间路由系统的信任模型. 计算机研究与发展, 2016, 53: 845–860]

19 Sankar A U P, Poornachandran P, Ashok A, et al. B-secure: a dynamic reputation system for identifying anomalous BGP paths. In: Advances in Intelligent Systems and Computing. Singapore: Springer, 2017. 515: 767–775

20 Arouna H A, Metongnon L, Lobelle M. Reputation rating algorithm for BGP links. In: Proceedings of International Conference on e-Infrastructure and e-Services for Developing Countries, 2017. 352–357

21 Gill P, Schapira M, Goldberg S. A survey of interdomain routing policies. SIGCOMM Comput Commun Rev, 2013, 44: 28–34

22 Zhang M W, Li J, Brooks S. I-seismograph: observing, measuring, and analyzing internet earthquakes. IEEE/ACM Trans Networking, 2017, 25: 3411–3426
23 Guo Y, Zhu J H, Wang Z X, et al. A multi-characteristics-based method for evaluating the security situation of interdomain routing nodes. Sci Sin Inform, 2014, 44: 527–536 [郭毅, 朱俊虎, 王振兴, 等. 基于多特征的域间路由节点安全状态评估方法. 中国科学: 信息科学. 2014, 44: 527–536]
24 Breiman L. Random forests. Mach Learn, 2001, 45: 5–32
25 Ismail R, Josang A. The beta reputation system. In: Proceedings of the Bled Econference, 2002. 41
26 Tozal M E. Autonomous system ranking by topological characteristics: a comparative study. In: Proceedings of the Annual IEEE International Systems Conference (SysCon), 2017. 1–8
27 Nur A Y, Tozal M E. Identifying critical autonomous systems in the Internet. J Supercomput, 2018, 74: 4965–4985
28 Kamvar S, Schlosser M, Garcia-molina H. The EigenTrust algorithm for reputation management in P2P networks. In: Proceedings of the 12th International Conference on World Wide Web, 2003. 640–651
29 Yashkina E, Pinigin A, Lee J Y, et al. Expressing trust with temporal frequency of user interaction in online communities. In: Proceedings of International Conference on Advanced Information Networking and Applications, 2019. 1133–1146
30 Fan X X, Liu L, Zhang R, et al. Decentralized trust management. ACM Comput Surv, 2020, 53: 1–33
31 Fan X X, Liu L, Li M C, et al. EigenTrust++: attack resilient trust management. In: Proceedings of the 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012. 416–425
32 Fan X X, Liu L, Li M C, et al. GroupTrust: dependable trust management. IEEE Trans Parallel Distrib Syst, 2017, 28: 1076–1090
33 Bellini E, Iraqi Y, Damiani E. Blockchain-based distributed trust and reputation management systems: a survey. IEEE Access, 2020, 8: 21127–21151

An inter-domain routing reputation model based on autonomous domain collaboration

Di CHEN[1,2,3], Han QIU[1,2*], Kaijie ZHU[2], Qingxian WANG[1,2] & Junhu ZHU[1,2]

1. *Institute of Cyberspace Security, Information Engineering University, Zhengzhou* 450002*, China*;
2. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450002*, China*;
3. *State Key Laboratory of Complex Electromagnetic Environment Effect on Electronic and Information System, Luoyang* 471003*, China*
* Corresponding author. E-mail: qiuhan410@aliyun.com

Abstract Interactions between autonomous systems (ASes) in inter-domain routing systems lack credibility authentication. Establishing a reputation model to evaluate AS behaviors can provide constraints and incentives for inter-domain routing management, thus improve the overall security. Due to the autonomous distributed nature and incomplete local routing information of inter-domain routing systems, existing reputation evaluation methods cannot perceive AS behaviors in a global perspective and reflect AS credibility dynamics accurately. We propose an inter-domain routing reputation model based on autonomous domain collaboration. We first analyze statistical characteristics of AS routing behaviors and establish a Bayesian-estimation-based AS reputation quantification index to evaluate local reputation of the target AS; Then, based on our investigation of relationships between AS properties and its local routing information integrity, we design a weighted reputation aggregation algorithm to compute global reputation of target AS in a multi-domain collaborative manner; Finally, we introduce a reputation updating method to penalize ASes with continuous malicious behaviors. Experimental results based on real incidents show that, the proposed model can effectively aggregate local reputation evaluations of participant ASes and capture AS behavior dynamics in different phases. The model can be used for abnormal routing suppression, security event source tracing, and provider selection in inter-domain routing systems.

Keywords inter-domain routing security, autonomous system behaviors, reputation model, Bayesian estimation

Di CHEN was born in 1992. She received her M.S. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 2015. She is currently a Ph.D. candidate at Information Engineering University. Her research interest is inter-domain routing security.

Han QIU was born in 1981. She received her Ph.D. degree in communication and information systems from Information Engineering University, Zhengzhou, China, in 2008. She is currently an associate professor at Information Engineering University. Her research interests include Internet routing security, modeling, and the evaluation of network security.

Kaijie ZHU was born in 1991. He received his M.S. degree in computer science and technology from China National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, China, in 2016. He is currently a Ph.D. candidate at State Key Laboratory of Mathematical Engineering and Advanced Computing. His research interest is network security.

Qingxian WANG was born in 1960. He received his M.S. degree in computer science and technology from Peking University, Beijing, China, in 1988. He is currently a professor at Information Engineering University. His research interests include network science and security.