中国科学 : 信息科学　2014 年　第 44 卷　第 4 期 : 527–536
www.scichina.com　info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论　文

基于多特征的域间路由节点安全状态评估方法

郭毅[①②*], 朱俊虎[①②], 王振兴[①②], 程东年[①]

① 解放军信息工程大学, 郑州　450001
② 数学工程与先进计算国家重点实验室, 郑州　450001
* 通信作者. E-mail: guoyi2006@yeah.net

收稿日期: 2013–04–25; 接受日期: 2013–06–28
国家重点基础研究发展计划 (批准号: 2012CB315901, 2007CB307102) 资助项目

摘要　域间路由节点安全状态评估能够实现对 BGP 节点安全状态的直观、实时描述, 可为制定合理的安全策略, 及时定位、抑制异常路由事件提供数据参考. 然而由于完整的异常域间路由集难以获取, 使得传统基于数据融合的状态评估方法不再适用. 分析 BGP 节点间交互路由过程中存在的统计特征以及这些特征与域间路由节点安全状态的关系, 进而提出一种基于多特征的安全状态评估方法. 以平均路径长度和路由事件发生频率等属性为安全特征, 并借鉴云模型理论转换定量特征为定性概念的思想, 构建域间路由安全特征云, 将正常态下的多属性综合安全特征转换为安全正常态, 然后通过度量安全特征偏离正常态的程度来计算节点偏离正常态的程度, 由此得到域间路由节点面临安全威胁的概率. 实验结果表明, 该方法能够实现对域间路由节点安全状态的评估, 准确性高、实时性强, 可为域间路由系统的安全稳定运行提供有力支撑.

关键词　BGP　状态评估　云模型　路径长度　威胁概率

1　引言

基于 BGP(border gateway protocol) 的域间路由系统是互联网的核心基础设施, 其主要功能是进行自治系统或自治域 AS(autonomous system) 间网络可达性信息交换、路由策略配置和管理. 然而, BGP 缺乏安全机制, 使得域间路由系统存在诸多安全缺陷而易遭受网络攻击, 由此引发的安全事件对互联网的性能和安全造成了严重危害 [1~3]. 为此, 针对域间路由系统的安全方案不断被提出, 依据不同技术思路已有解决方案可分为 BGP 协议安全扩展和域间路由安全监测两种类型. 其中, BGP 协议安全扩展就是对原有 BGP 协议进行修改、扩展, 通过加入验证机制提高协议的安全性, 如: S-BGP(secure BGP)[4]、soBGP(secure origin BGP)[5] 和 Listen & Whisper[6] 等. 域间路由安全监测技术则通过增量式部署的监测节点, 被动采集域间路由信息, 然后对采集到的路由信息进行集中分析或通过监测节点之间的协同验证, 发现进而应对域间路由安全事件, 达到提高域间路由系统安全性的目的 [7~11]. 相比 BGP 协议安全扩展方案, 域间路由安全监测技术不需要部署覆盖全网的密钥管理基础设施及修改路由协议和路由器, 只需增量式布置所需监测节点即可大幅提高域间路由节点及全网的安全性, 因而受到广泛重视.

引用格式: 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, doi: 10.1360/N112013-00029

Lad 等 [8] 针对前缀劫持问题开发了 PHAS 系统, 其对 RouteViews(或 RIPE) 提供的 BGP 路由数据进行分析, 实时生成用户前缀的使用状态报告, 若有其它 AS 未经授权宣告用户前缀则向用户发送告警通知, 帮助网络管理员监测前缀劫持事件.

文献 [9] 分析了域间路由系统的层次特性, 提出基于 BGP 异常路由的安全评估模型. 该方法通过构造路由状态树刻画各路由实体之间的层次关系、存储和表达每个实体的路由安全状态, 并根据所检测的异常路由对各实体的安全状态进行量化. 该方法需要以完整的异常路由集为输入, 才能够保证评估结果的准确性, 从而降低了其可用性.

当前的域间路由安全监测技术主要用于为用户分析并提供所关注路由信息 (前缀、AS 号等) 的使用状况, 或者用于检测特征明显的异常域间路由 (如: 非法 AS 号 BGP 路由、环路 BGP 路由等), 之后将监测结果直接呈现给网络管理员. 这就可能让管理员陷于大量的细节信息, 而忽略监测结果所体现或内含的一些重要情况. 实际上, 对于各 AS 的管理员, 他们更希望安全监测系统能够直观呈现本自治域所处安全状态的定量或定性描述, 只在发现了重大异常后才去进一步关注细节信息. 针对已有解决方案难于有效评估域间路由节点的安全状态, 本文提出一种基于多特征的安全状态评估方法, 以平均路径长度和路由事件发生频率等属性为安全特征, 进而借鉴云模型理论转换定量特征为定性概念的思想, 构建域间路由安全特征云, 将正常态下的多属性安全特征转换为安全正常态, 从而通过度量安全特征偏离正常态的程度来判断运行状态下节点偏离正常态的程度, 以此计算域间路由节点的安全威胁概率.

本文第 2 节分析域间路由节点安全状态评估方法面临的关键问题和难点, 第 3 节分析域间路由相关属性与域间路由节点安全状态的关系, 第 4 节详细说明了基于多特征的域间路由节点安全状态评估方法, 重点描述基于云模型理论的安全状态评估算法, 第 5 节对该方法的应用和有效性进行实验说明, 结果表明该方法能够实现对域间路由节点安全状态的评估, 准确性高、实时性强, 最后, 对全文进行总结并指出进一步的研究方向.

2 问题分析

随着互联网规模的扩展和商业化进程的加速, 域间路由系统日渐表现出开放复杂巨系统特征, 如节点数量庞大、系统结构复杂、节点行为自治多变, 由此导致通过 BGP 协议交互的路由信息的频率和次数都大大增加, 从而加剧了域间路由信息规模的膨胀. 在这种环境下, 如何对各节点相关的海量域间路由信息进行分析、处理、归纳, 进而实时、准确地评估它们所处的安全状态是研究域间路由节点安全状态评估方法面临的关键问题和难点.

(1) 实时性

域间路由节点安全状态评估方法应该具备能够在较短时间内得到 BGP 节点安全状态的能力, 只有达到该要求才能为管理员或用户及时制定安全策略提供数据参考. 将这种能力称为安全状态评估方法的实时能力, 定义如下:

$$\begin{cases} (T_j^i - T_i) \leqslant \Delta T, \mathrm{cap}_{\mathrm{realtime}} = 1, \\ (T_j^i - T_i) > \Delta T, \mathrm{cap}_{\mathrm{realtime}} = 0. \end{cases} \tag{1}$$

式中 T_i 为待评估安全状态的时刻; T_j^i 为得到 T_i 安全状态的时刻; $\Delta T \geqslant 0$ 为允许的最大延迟时间, 若延迟时间小于或等于 ΔT, 说明评估方法具备实时能力, 表示为 $\mathrm{cap}_{\mathrm{realtime}} = 1$, 否则说明达不到实时评估的要求, 表示为 $\mathrm{cap}_{\mathrm{realtime}} = 0$.

(2) 准确性

同样, 域间路由节点安全状态评估方法应该能够准确反映 BGP 节点的安全状态, 从而为管理员或用户制定合理的安全策略提供可靠的数据依据. 用准确度来描述安全状态评估方法所得结果与实际安全状态的吻合程度, 定义如下:

$$\begin{cases} \left|\mathrm{Threat}_i' - \mathrm{Threat}_i\right| \leqslant \delta, \mathrm{cap}_{\mathrm{accurate}} = 1, \\ \left|\mathrm{Threat}_i' - \mathrm{Threat}_i\right| > \delta, \mathrm{cap}_{\mathrm{accurate}} = 0. \end{cases} \tag{2}$$

式中 Threat_i' 为评估方法所得的域间路由节点安全状态的量化值; Threat_i 为实际的安全状态; $\delta \geqslant 0$ 为允许的最大误差, 若误差小于或等于 δ, 说明评估方法的准确度达到要求, 表示为 $\mathrm{cap}_{\mathrm{accurate}} = 1$, 否则说明该评估方法的准确度达不到要求, 表示为 $\mathrm{cap}_{\mathrm{accurate}} = 0$.

针对 BGP 节点安全状态评估的研究成果相对较少, 其解决思路都是以检测出的异常域间路由集为输入, 采用相关理论或方法对其进行融合处理, 从而得到 BGP 节点的安全状态. 这类方法需要已知异常域间路由集而很少被实际采用, 主要原因为: ①通过 BGP 协议传输的域间路由数量巨大, 已有方法难以在合理时间范围内高效 (高正确检测率、低误报率) 检测出具有异常特征的域间路由, 从而降低了状态评估结果的时效性; ②针对某些类型的异常路由 (如: 伪造路径类型的异常域间路由), 目前尚无有效的检测方法, 也就是说异常路由集的完整性无法保证, 由此降低了状态评估结果的准确性.

3 域间路由节点安全特征

如上所述, 异常域间路由集的完整性难以保证, 使得传统基于数据融合的状态评估方法不适用于评估域间路由节点的安全状态. 本节研究 BGP 节点间交互路由过程中存在的统计特征, 如: BGP 报文更新频率、AS_PATH 平均长度等, 从中选取能够反映 BGP 节点安全状况的特征, 进而研究基于特征的节点安全状态评估方法. AS_PATH 为更新报文的公认必选属性, 它用 AS 号的顺序来描述 AS 间的路径或到 NLRI 所明确的目的地的路由. AS_PATH 可以描述所有它经过的自治域, 以最近的 AS 开始, 以发起者的 AS 结束, 是反映域间路由系统运行状况及特性的关键信息. 为此以更新报文的 AS_PATH 属性为研究对象, 分析其相关表象特征 (如: 路径长度、编辑距离) 与域间路由节点安全状态的关系.

3.1 平均路径长度

定义 1 路径长度 (AS_PATH length, APL) 描述更新报文 AS_PATH 属性所指定的目的 AS 与源 AS 间的路径的长度, 即从源 AS 到达目的 AS 所需经历的 AS 个数, 用 $\mathrm{APL}(\mathrm{AS_{Sour}}, \mathrm{AS_{Destn}})$ 表示. 另外, 定义平均路径长度 $\bar{l}_i = \frac{1}{(M-1)} \sum_{j \neq i} \mathrm{APL}(i,j)$ 为 ASi 到系统其它节点的路径长度的平均值.

较长时间的域间路由不稳定会导致部分路由失效或者某些特定目的地不可达. 这种情况下, BGP 路由器需要撤销已失效路由 (包括含有不可达节点的路由), 并启用存储于转发表的备份路由, 直至接收到其它节点提供的更优路由. 尽管 BGP 是一种基于策略的路由选择协议, BGP 在确定最佳路径时考虑的不是速度, 而是让 AS 能够根据多种 BGP 属性来控制数据流的传输, 但据统计分析, 多数情况下备份路由的路径长度仍大于原有路由给出的路径的长度 [11]. 正常状态时, BGP 路由器的任一邻居节点 (路由器) 向其宣告的到达同一目的节点的路由的路径长度与平均值的偏差都很小, 描述为

$$\forall j \in \Gamma_i, \left|[\mathrm{APL}(j,k)+1] - \bar{l}(i,k)\right| \leqslant \varepsilon, \tag{3}$$

式中 Γ_i 为节点 i 所有邻居节点的集合, $\bar{l}(i,k)$ 为节点 i 接收的到节点 k 的所有路由的平均路径长度.

文献 [11] 对 Slammer 蠕虫爆发时位于 AS513 的路由器所接收到的路由消息的路径长度分布情况进行了分析, 结果见文献 [11] 的图 2 所示, 该图虚线左半部分显示尚未遭受攻击 (正常状态) 时的分布, 右半部分则为蠕虫开始破坏后的分布情况. 显然, 受到攻击后, 路径长度大于正常状态平均值的路由消息数量大幅增加, 表明路径长度的变化与域间路由节点的安全状态具有紧密联系.

3.2 路径编辑距离

定义 2 AS_PATH 编辑距离 APED (AS_PATH edit distance) 借鉴字符串操作的编辑距离 (levenshtein/edit distance) 度量, 用于衡量不同时刻节点之间路径的差异程度. 假设 t 时刻 AS2 到 AS6 的路径为 r_t=[5,1,3,4,6], k 时刻 AS2 与 AS6 的路径变为 r_k=[5,4,6], 则 APED(r_t, r_k)=APED(r_k, r_t) = 2. 定义平均编辑距离 $\overline{d} = \frac{1}{(M-1)} \sum_{j \neq i} \mathrm{APED}\left(r_t(i,j), r_k(i,j)\right)$, 用于刻画 t 时刻相对于 k 时刻的路由波动程度.

Slammer 蠕虫爆发前后共 5 个小时内, 位于 AS513 的路由器所接收到的路由消息的 APED 变化情况如文献 [11] 的图 3 所示, 该图虚线左半部分为尚未遭受攻击时的情况, 右半部分则为蠕虫开始破坏后的情况. 显然, 受到攻击后, 路由编辑距离大于正常状态平均值的路由消息数量大幅增加. 由此说明, 路由编辑距离的变化与域间路由节点的安全状态具有紧密联系.

3.3 路由事件发生频率

定义 3 路由事件发生频率 (frequency of routing events) 用于衡量路由事件在某一阶段内发生的频繁程度, 表示为 $f = C_{\mathrm{RE}}/t$, 其中 C_{RE} 为路由事件数量. 一般以天为路由事件发生频率的时间单位, 也就是说, 每天的更新报文数量即为本天的路由事件发生频率, 所以下面所涉及到的更新报文数量特征等同于路由事件发生频率特征.

Wang 等 [12] 根据 (prefix, peer) 二元组将 BGP Update 报文分成 8 种, 路由表初始化交换、抖动、NADA、一般性新声明、重复声明、SPATH 隐式撤销、DPATH 隐式撤销、源撤销和重复撤销. 前 6 种均为声明报文, 后两种为撤销报文. 相应的, 将路由事件分为两类, 拓扑不稳定、策略变化. 其中, 拓扑不稳定反应网络拓扑的变化, 如部分 AS 失效或频繁重启, 这些可能导致其它 AS 路由器大量消耗控制层资源, 或产生大量无效报文, 从而影响 BGP 的收敛; 策略变化反映路由策略的变化, 如: 选择其它 AS 作为 Provider, 可能导致大量无用报文的产生, 降低网络性能. 一旦有节点失效或更优路由路径被宣告, 在域间路由系统内将产生大量的相关 BGP 更新报文. 所以路由事件发生频率直接反映路由的稳定状况, 单位时间内更新报文越多, 即路由事件发生频率越高, 路由就越倾向于不稳定状态, 相关域间路由节点的安全状态就越差.

3.4 综合安全特征

定义 4 综合安全特征 (integrated security characteristic) 指的是用于描述域间路由节点安全状态实时变化的属性的集合, 记为 S_{ISC}. 例如, 以域间路由平均路径长度、域间路由编辑距离和路由事件发生频率为安全状态特征, 则 $S_{\mathrm{ISC}} = \{c_l, c_d, c_f\}$, 其中 c_l, c_d, c_f 分别表示平均路径长度特征、编辑距离特征和路由事件发生频率特征.

综合安全特征提供了一种将域间路由安全特征与 BGP 节点活动整合关联的方法. 通过对综合安全特征的监测, 可以实现对 BGP 节点安全状态的实时评估, 即通过评估综合安全特征偏离其正常态

的程度来量化 BGP 节点的安全状态.

4 基于云模型理论的安全状态评估模型

在确定域间路由安全特征之后, 还需将采集或统计得到的特征数据转换为对节点安全状态的定量和定性描述. 借鉴云模型实现定性概念与其数值表示之间不确定性转换的思想, 提出一种域间路由节点安全状态评估模型 CSSAM, 将正常态下的综合安全特征转换为节点的安全正常态, 构建域间路由安全特征云, 进而通过计算综合安全特征偏离其正常态的程度来量化域间路由节点面临威胁的概率.

4.1 二维正态云模型介绍 [13~15]

云模型由李德毅院士提出, 以随机数学和模糊数学为基础, 用于描述语言值的随机性、模糊性及两者的关联性. 云模型的主要特点是能够实现语言表述的定性概念与其定量数值描述之间的不确定性转换. 用 U 代表论域空间, C 是论域空间 U 上的定性概念, 如果某一定量值 $x \in U$ 是 C 的一次随机实现, x 对 C 的确定度 $\mu(\mathrm{x}) \in [0,1]$, $\mu : U \to [0,1]$,$\forall x \in U, x \to \mu(x)$, 则 x 在论域 U 上的分布称为云, 表示为 $C(X)$. 每一个 x 称为一个云滴, 其定量值由标准正态分布函数决定, 而云滴的确定度或隶属度函数则采用模糊集合论中广泛使用的正态隶属函数. 因此, 正态云模型结合了概率论和模糊集合论的特点, 也就是说, 兼具概率论的随机性和模糊集合论的模糊性特点.

在云模型中, 通过大量的定量数值及其确定度的二元组形式 $\langle x, \mu \rangle$ 来表达其所要描述的定性概念. 定性概念在云模型中具体由 3 个数字特征期望 Ex、熵En和超熵He来反映. 利用正向云算法和逆向云算法可以实现定性概念与定量数值间的不确定性转换. 其中, 正向云算法用于将定性概念的整体特征转换为定量数值的表示, 实现概念空间到数值空间的转换. 逆向云算法则用于实现定量值到定性概念的转换. 如果一个复杂的定性概念是由两个或多个定性子概念组成, 那么可以用二维 (或多维) 的数字特征构建二维 (或多维) 云模型, 用于描述复杂的定性与定量间的相互转换.

4.2 域间路由节点安全特征云

除了路径长度、编辑距离和路由事件发生频率这 3 种特征之外, 能够反映 BGP 节点安全状态的特征还有很多, 且选择的特征越多, 构成的多维云模型越能精确反映节点安全状态的变化. 但是, 随着云模型维数的增大, 云模型的构造也将变得更加复杂, 偏离正常态程度的计算复杂度也就越高, 评估效率将相应降低 [13,14]. 另外, 由于路由编辑距离和路由事件发生频率都是反映域间路由波动程度的特征, 但是与路由事件发生频率特征相关的信息较容易获取且更易于量化, 所以仅选择路由事件发生频率与平均路径长度两个特征, 共同构建二维云模型, 进行安全状态的评估.

定义 5 域间路由安全特征云指的是用云模型表示的域间路由安全特征的定性概念, 是对一维正态云的拓展, 由若干云滴 $\overline{x_i} = (x_{li}, x_{fi})$ 组成, 其中 x_{li} 为云滴 $\overline{x_i}$ 的路由路径长度特征分量, x_{fi} 为云滴 $\overline{x_i}$ 的路由事件发生频率特征分量.

对于域间路由安全特征云, 每个云滴包括两个特征分量, 相应的, 其特征向量表示为 $C((Ex_l, Ex_f), (En_l, En_f), (He_l, He_f))$. 期望 E$x$ 是定性概念量化的最典型样本. 对于域间路由安全特征云, 若已知 M 个代表平均路径长度特征和路由事件发生频率特征的云滴$\{(x_{l1}, x_{f1}), (x_{l2}, x_{f2}), \ldots, (x_{lM}, x_{fM})\}$,

则 $\mathrm{E}x_l$ 的估计值 $\widehat{\mathrm{E}x_l}=\overline{X_l}$, $\mathrm{E}x_f$ 的估计值 $\widehat{\mathrm{E}x_f}=\overline{X_f}$, 其中 $\overline{X_l}$ 和 $\overline{X_f}$ 分别表示 x_l, x_f 的样本均值,

$$\overline{X_l}=\frac{1}{M}\sum_{i=1}^{M}x_{li},\quad \overline{X_f}=\frac{1}{M}\sum_{i=1}^{M}x_{fi}. \tag{4}$$

熵 En 由定性概念的随机性和模糊性决定, 用于描述定性概念的可度量粒度和不确定度. 也就是说, En 既可反映能够代表定性概念的所有云滴的离散程度, 又可反映能够被概念接受的云滴的取值范围. 对于 M 个域间路由安全特征云的云滴, En_l 和En_f 的估计值分别为

$$\widehat{En_l}=\sqrt{\frac{\pi}{2}}\times\frac{1}{M}\sum_{i=1}^{M}\left|x_{li}-\widehat{Ex_l}\right|,\quad \widehat{En_f}=\sqrt{\frac{\pi}{2}}\times\frac{1}{M}\sum_{i=1}^{M}\left|x_{fi}-\widehat{Ex_f}\right|. \tag{5}$$

超熵 He 用于度量熵的不确定性, 是对模糊性和随机性之间的关联的描述. 根据此概念, 可分别计算平均路径长度特征的超熵估计值 $\widehat{He_l}=\sqrt{S_l^2-\widehat{En_l}^2}$, 路由事件发生频率的超熵估计值 $\widehat{He_f}=\sqrt{S_f^2-\widehat{En_f}^2}$, 其中 S_l^2 和 S_f^2 分别为 2 个安全特征的样本方差,

$$S_l^2=\frac{1}{M-1}\sum_{i=1}^{M}\left(x_{li}-\overline{X}_l\right)^2,\quad S_f^2=\frac{1}{M-1}\sum_{i=1}^{M}\left(x_{fi}-\overline{X}_f\right)^2. \tag{6}$$

4.3 安全威胁概率的计算

在云模型中, 用云滴隶属度描述由路径长度特征和路由事件发生频率特征构成的云滴隶属于域间路由安全特征云模型所代表的正常行为概念的程度. 论域 $U'=\{\overline{x_i}|\overline{x_i}=(x_{li},x_{fi}),i\in\mathbb{N}\}$ 及其模糊集合 $\widetilde{A}$, 对于任意元素 $\overline{x_i}=(x_{li},x_{fi})$, 都存在一个有稳定倾向的随机数 $\mu\widetilde{A}(x_l,x_f)$, 即 (x_l,x_f) 对 $\widetilde{A}$ 的隶属度或确定度.

获取域间路由安全特征 (x_l, x_f) 之后, 将其作为云滴坐标输入到域间路由安全特征云模型, 根据期望值 ($\mathrm{E}x_l$, $\mathrm{E}x_f$)、熵 (En_l, En_f) 和超熵 (He_l, He_f), 计算此云滴所代表的安全状态隶属于云模型所代表正常行为概念的程度.

$$y=\exp^{-\frac{(x_l-\mathrm{E}x_l)^2}{2\cdot\left(En_l'\right)^2}-\frac{\left(x_f-\mathrm{E}x_f\right)^2}{2\cdot\left(En_f'\right)^2}}, \tag{7}$$

式中 En_l' 和 En_d' 分别为区间 $[En_l-He_l,\ En_l+He_l]$ 和 $[En_f-He_f,\ En_f+He_f]$ 上生成的正态随机数; y 为 (x_l, x_f) 隶属于域间路由安全特征正常态概念的确定度, 也就是云滴的隶属度; $\{(x_l,\ x_f),\ y\}$则反映此次定量与定性的不确定性转换. 进而计算节点面临安全威胁的概率 P_{threat}, 显然 $P_{\mathrm{threat}}=1-y_i$. 一旦计算得到的威胁概率超出阈值, 立即发出警报; 相反, 若概率没有超出阈值, 则利用新加入的云滴数据对域间路由安全特征云进行更新调整. 为了避免积累的数据过多而影响运行效率, 可以采取先进先出方式 [13] 向云滴集合$\{(x_{l1},\ x_{f1}),\ (x_{l2},\ x_{f2}),\ \ldots,\ (x_{lM},\ x_{fM})\}$添加新云滴 $(x_l,\ x_f)$, 并重新生成域间路由安全特征云. 采用这种方法, 云模型就能够根据域间路由节点运行状况的动态变化不断更新、调整, 自适应地感知域间路由安全特征的新特点.

5 实验与评估

为了验证域间路由节点安全状态评估方法 CSSAM 的有效性, 以 RouteViews 提供的 BGP 路由信息为实验数据, 用于评估域间路由节点的安全状态. 利用我们先前开发的 BGP ISS 对 AS65000(APINC)

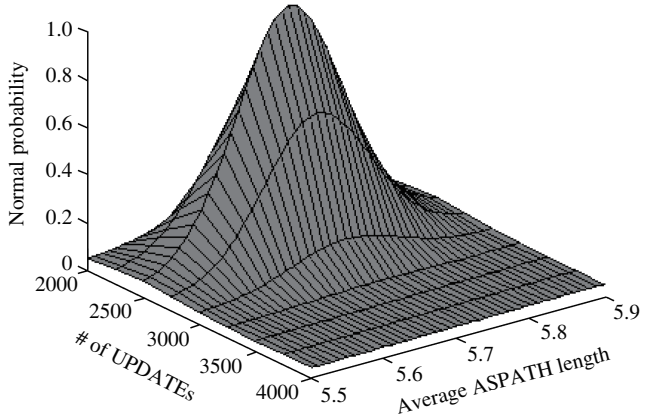

图 1 域间路由安全特征云模型

Figure 1 The security characteristic cloud model for inter-domain routing system

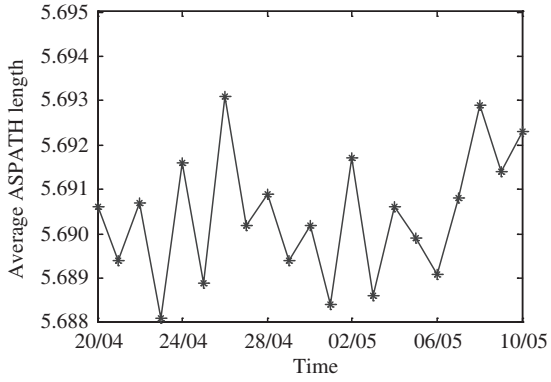

图 2 平均路径长度特征

Figure 2 The average AS_PATH length characteristic

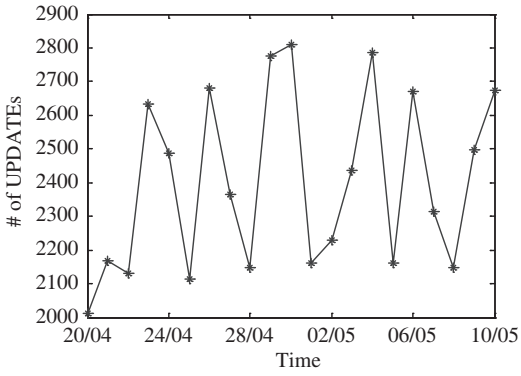

图 3 UPDATE 报文数量特征

Figure 3 The number of UPDATE packets characteristic

的路由数据进行分析, 可得到能直接用于模型所需的域间路由安全特征信息. 下面以 2011 年 4 月 20 日至 2011 年 5 月 10 日的路由数据为例, 进行安全状态评估的应用说明, 分析该段时间内节点安全状态的变化.

5.1 CSSAM 方法的评估能力

根据采集得到的 300 个正常路由数据, 利用逆向云生成算法, 分别计算域间路由安全特征二维正态云的数字特征值: 期望 ($\mathrm{E}x_l$, $\mathrm{E}x_f$)、熵 (En_l, En_f) 和超熵 (He_l, He_f). 若当天自治域运行正常, 则该天的域间路由平均路径长度 x_l 和路由事件频度 x_f 共同构成一个正常数据 (x_l, x_f). 由上述数字特征值构造的云模型如图 1.

图 1 中 x 轴为平均路径长度特征, y 轴为路由事件频度特征, z 轴为自治域安全状态隶属于正常情况的确定度.

对 2011 年 4 月 20 日至 2011 年 5 月 10 日期间 AS65000 的域间路由数据进行分析, 可得该段时间平均路径长度特征和更新报文数量特征的变化趋势, 如图 2 和图 3 所示.

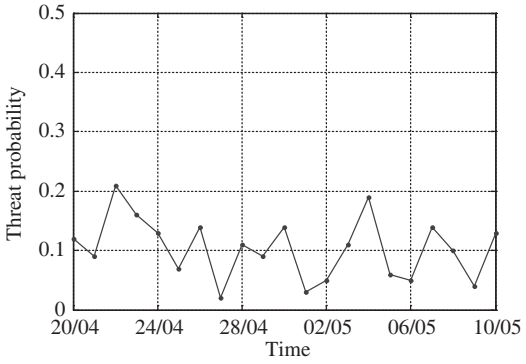

图 4　域间路由安全威胁云模型所得的威胁概率

Figure 4　The threat probability between 20/04/2011 to 10/05/2011 according to the cloud model

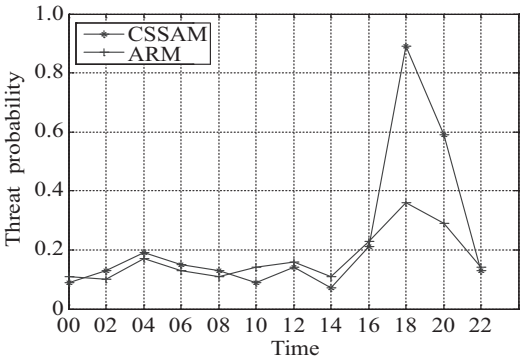

图 5　域间路由系统安全威胁概率

Figure 5　The threat probability of inter-domain routing system according to CSSAM and ARM

将各时间段的 (x_l, x_f) 作为云滴坐标输入到云模型, 根据数字特征期望 $(\mathrm{E}x_l, \mathrm{E}x_f)$、熵 (En_l, En_f) 和超熵 (He_l, He_f), 计算云滴隶属于云模型代表正常行为概念的程度 (云滴隶属度). 之后, 获取不同时刻自治域面临威胁的概率, 概率越高说明自治域的安全状况越差, 结果见图 4. 可以看出, 该段时间内自治域的安全态势存在一定波动, 但其威胁概率均小于或略大于 0.2, 表明该段时间自治域的安全状态良好.

5.2　与其他方法的比较

为了更好地验证 CSSAM 方法对域间路由节点安全状态评估的实际效果, 下面以 2008 年 2 月 24 日各时间段的域间路由信息为输入数据, 计算不同时刻自治域面临安全威胁的概率. 当天, 巴基斯坦电信 (AS17557) 劫持了 YouTube(AS36561) 的前缀, 使得 YouTube 网站在 2 月 24 日的 18 点至 21 点停止对外提供服务 2 个多小时. 由于评估的单位时间为小时, 对 UPDATE 报文数量的统计也要求以小时为单位, 这与前面的更新报文数量特征的单位时间不一致, 所以在计算每个时刻的威胁概率时需要对 UPDATE 报文数量进行相应处理, 采取等比例放大的方法, 即 $x'_f = 24 * x_f$, 也就是说, 输入的云滴数据 (x'_l, x'_f) 为 $(x_l, 24 * x_f)$. 图 5 同时给出基于多特征的安全状态评估方法 (CSSAM) 和基于异常路由的模型 (ARM) 所得的当天安全态势.

从图中可以看出, 基于异常路由的模型给出的安全态势较为平稳, 仅在 20 点左右有微小的波动. 相比之下, CSSAM 所得的 18 点至 20 点前后的安全威胁概率值都要远远大于 50%, 直观、准确地反映了该时间段自治域的安全态势. 另一方面, 基于异常路由的模型需要以完整的异常路由数据集为输入, 才能准确计算出自治域的安全状态. 而获取异常路由数据集本身就是一个很复杂的问题, 不仅时间开销大, 且检测结果的准确性难以保证. CSSAM 仅需要对各时刻的 UPDATE 报文进行统计分析, 获取平均路径长度值和 UPDATE 报文数量, 即可利用基于云模型的状态评估算法得到各个时刻的安全威胁概率.

6　结论

域间路由节点安全状态评估能够实现对 BGP 节点安全状态的直观、实时描述, 可为自治域或全网的管理人员制定合理的安全策略, 及时定位、抑制异常路由事件提供数据参考, 是目前提高域间路

由系统整体安全性较为有效且可行的方法之一. 然而由于完整的异常域间路由集难以获取, 使得传统基于数据融合的状态评估方法不再适用. 本文提出一种基于多特征的 BGP 节点安全状态评估方法, 以平均路径长度、路由事件发生频率为安全特征, 进而借鉴云模型实现定量特征与定性概念相互转换的思想, 构建域间路由节点安全特征云, 通过评估安全特征偏离其正常态的程度来评估节点的安全状态. 实验结果表明, CSSAM 方法能够实现对域间路由节点安全状态的感知, 准确性高、实时性强, 且克服了其它方法不能同时定量定性分析节点安全状态的不足. 另外, 采用 CSSAM 评估域间路由节点的安全状态, 需要构建并不断更新域间路由节点安全特征云, 计算云的 3 个数字特征和云滴隶属度, 这些过程都需要花费一定的计算资源. 也就是说, 相比于其它方法, CSSAM 需要耗费更多的计算资源, 以精确量化域间路由节点的安全状态. 为此, 改进域间路由节点安全特征云生成和更新算法, 降低整个方法的计算复杂度, 是下一步需要重点研究的问题.

参考文献

1 Deng W P, Zhu P D, Lu X C, et al. On evaluating BGP routing stress attack. J commun, 2010, 5: 13–22

2 Deshpande S, Thottan M, Ho T K, et al. An online mechanism for BGP instability detection and analysis. IEEE Trans Comput, 2009, 58: 1470–1484

3 Guo Y, Wang Z X. An immune-theory-based model for monitoring inter-domain routing system. Sci China Inf Sci, 2012, 55: 2358–2368

4 Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE J Sel Area Comm, 2000, 18: 582–592

5 White R. Securing BGP through secure origin BGP. Internet Protoc J, 2003, 6: 15–22

6 Subramanian L, Roth V, Stoica I, et al. Listen and whisper: security mechanisms for BGP. In: Proceedings of 1st Symposium on Networked Systems Design and Implementation, San Francisco, 2004. 127–140

7 Hu N, Zhu P D, Zou P. Information sharing mechanism for inter-domain routing cooperative monitoring. J Softw, 2011, 22: 481–494 [胡宁, 朱培栋, 邹鹏. 域间路由协同监测中的信息共享机. 软件学报, 2011, 22: 481–494]

8 Lad M, Massey D, Pei D, et al. PHAS: a prefix hijack alert system. In: Proceedings of the 15th USENIX Security Symposium, Vancouver, 2006. 153–166

9 Liu X, Wang X Q, Zhu P D, et al. Security evaluation for interdomain routing system in the Internet. J Comput Res Dev, 2009, 46: 1669–1677 [刘欣, 王小强, 朱培栋, 等. 互联网域间路由系统安全态势评估. 计算机研究与发展, 2009, 46: 1669–1677]

10 Goodell G, Aiello W, Griffin T, et al. Working around BGP: an incremental approach to improving security and accuracy of inter-domain routing. In: Proceedings of the ISOC NDSS 2003, San Diego, 2003. 75–85

11 Deshpande S, Thottan M, Ho T K, et al. An online mechanism for BGP instability detection and analysis. IEEE Trans Comput, 2009, 58: 1470–1484

12 Wang L, Zhao X, Pei D, et al. Protecting BGP routes to top-level DNS servers. IEEE Trans Parall Distr Syst, 2003, 14: 851–860

13 Zhang H B, Pei Q Q, Ma J F. An algorithm for sensing insider threat based on cloud model. Chin J Comput, 2009, 32: 784–792 [张红斌, 裴庆祺, 马建峰. 内部威胁云模型感知算法. 计算机学报, 2009, 32: 784–792]

14 Li D Y, Liu C Y. Study on the universality of the normal cloud model. Eng Sci, 2004, 6: 28–33 [李德毅, 刘常昱. 论正态云模型的普适性. 中国工程科学, 2004, 6: 28–33]

15 Liu Y, Li D Y, Zhang G W, et al. Atomized feature in cloud based evolutionary algorithm. Acta Electron Sin, 2009, 37: 1651–1658 [刘禹, 李德毅, 张光卫, 等. 云模型雾化特性及在进化算法中应用. 电子学报, 2009, 37: 1651–1658]

A multi-characteristics-based method for evaluating the security situation of inter-domain routing nodes

GUO Yi[1,2*], ZHU JunHu[1,2], WANG ZhenXing[1,2] & CHENG DongNian[1]

1 *PLA Information engineering University, Zhengzhou* 450001*, China;*
2 *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450001*, China*
*E-mail: guoyi2006@yeah.net

Abstract The administrators of the AS(autonomous system) can develop a more rational strategy with the help of evaluating the secure state of the BGP(border gateway protocol) nodes. However, the existing fusion-based method is inapplicable because it needs an integrated set of abnormal inter-domain routes to ensure accurate results. In this paper, we first analyze the statistical characteristics existing in the process of exchanging routes between BGP nodes and the relationships between these characteristics, taking into account the security situation of a node. We then propose a multi-characteristics-based method for evaluating the security situation of inter-domain routing nodes that selects the average length of the routing path and the frequency of routing events as security characteristics, borrowing an idea from Cloud Model theory in transforming the values of quantitative characteristics to a qualitative concept. CSSAM, a security state awareness model, is proposed. It constructs a cloud model with a mass of numerical values of the security characteristics in the normal state, and then computes the threat probability for the system, by measuring the degree of deviation of the security characteristics from their norms. The experimental results show that the method is capable of sensing the security situation of BGP nodes.

Keywords BGP, situation evaluation, cloud model, length of routing path, threat probability

GUO Yi was born in 1984. He received his Ph.D. in Computer Application Technology from the PLA Information and Engineering University, Zhengzhou City, in 2012. Currently, he is a lecturer at the PLA Information and Engineering University. His research interests include internet routing, routing security and complex networks.

ZHU JunHu received his M.S. degree from the PLA Information Engineering University at which he is currently an affiliated Associate Professor. His current research interests include network security, modeling and evaluation of network performance.

WANG ZhenXing is a Professor affiliated to the PLA Information Engineering University. He received his M.S. from Xi'an Jiaotong University and Ph.D. from Nanjing University of Science and Technology. His current research interests include network security, traffic analysis, and the next-generation internet. He has served as a member of the editorial boards of several journals.

CHENG DongNian CHENG DongNian is a Professor affiliated to the Digital Switching System Engineering and Technological R&D Center. He received his Ph.D. at Xidian University in 2000. His research interests include high-performance computer networks, network security protocols, architectures of next-generation networks, modeling and evaluation of network performance.