基于特征融合相似度的域间路由系统安全威胁感知方法

郭毅^{1,2}, 段海新^{1*}, 张连成², 邱菡²

1. 清华大学网络科学与网络空间研究院, 北京 100084

2. 解放军信息工程大学, 郑州 450001

* 通信作者. E-mail: duanhx@tsinghua.edu.cn

收稿日期: 2016–11–01; 接受日期: 2016–12–12; 网络出版日期: 2017–03–22

国家自然科学基金 (批准号: 61402525, 61472215, 61402526, 61502528) 资助项目

摘要 针对域间路由系统的网络攻击技术日益复杂, 尤其是近年出现的基于大规模 LDoS (low-rate denial of service) 的跨平面攻击, 其造成的危害远大于传统网络攻击. 已有域间路由系统安全技术主要研究如何解决 BGP (border gateway protocol) 协议缺乏路由真实性验证机制的问题, 而针对域间路由系统的大规模 LDoS 攻击利用的是 BGP 协议自适应机制的特性, 且用于 LDoS 攻击的流量与许多真实数据流的特征类似, 使得现有很多方法难以有效应对. 本文提出一种基于加权相似度的域间路由系统安全威胁感知方法, 利用多个特征融合描述域间路由系统的安全状态, 并结合网络流量的自相似特性, 运用加权相似度计算方法量化实时特征值与正常态特征值的偏差, 由此评估域间路由系统的安全状态. 进一步, 通过跟踪安全特征的实时变化情况, 即可推断域间路由系统遭受攻击的类型. 实验结果表明, 该方法能够实现对域间路由系统安全状态的有效评估, 在遭受控制平面攻击或数据平面攻击的初期阶段即能感知威胁, 为网络管理员及时制定有效的应对策略提供可靠参考.

关键词 域间路由, 数据平面攻击, 威胁感知, 加权相似度, 特征偏差

1 引言

作为互联网的关键基础设施, 基于 BGP (border gateway protocol) 的域间路由系统位于整个网络的控制平面, 是不同自治域互连及交换网络可达信息的主要机制, 其安全对整个互联网具有重要影响^[1,2]. 然而由于 BGP 协议存在设计缺陷, 致使域间路由系统安全问题日益突出^[3~7], 尤其是近年来针对域间路由系统的攻击技术越来越复杂, 造成的危害也远大于传统网络攻击^[8~10]. 如 Zhang 等^[9]提出的 ZMW (Zhang Mao Wang) 可以延长网络收敛时间并引起 BGP 会话重置; Schuchard 等^[10]在

引用格式: 郭毅, 段海新, 张连成, 等. 基于特征融合相似度的域间路由系统安全威胁感知方法. 中国科学: 信息科学, 2017, 47: 878–890, doi: 10.1360/N112016-00160

Guo Y, Duan H X, Zhang L C, et al. A threat perception method for inter-domain routing systems based on weighted similarity (in Chinese). Sci Sin Inform, 2017, 47: 878–890, doi: 10.1360/N112016-00160

ZMW 攻击的基础上提出了 CXPST (coordinated cross plane session termination) 攻击, 并通过仿真实验说明了这种攻击可使整个互联网瘫痪数小时且目前尚无有效防范措施.

已有域间路由安全技术主要研究如何解决 BGP 协议缺乏路由真实性验证机制的问题, 如 S-BGP^[11]、RPKI^[12,13] 和 PHAS^[14] 等. 但由于针对域间路由系统的大规模 LDoS 攻击是通过对网络数据平面发起大规模流量攻击的, 使网络路由器间的互连链路反复拥塞, 引发域间路由节点或邻接的大范围级联失效, 由此影响控制平面并将攻击造成的影响扩大到全局网络. 它们利用的是 BGP 协议自适应机制的特性, 且用于 LDoS 攻击的流量与许多真实数据流的特征类似, 使得现有很多方法难以有效应对.

态势感知技术支持在动态复杂的环境中获取当前系统的连续变化状况, 在交通监管、医疗应急调度等领域被广泛应用和研究. 如果将态势感知技术用于对域间路由系统运行状况的实时评估, 就能从全局上分析域间路由系统的安全状态, 一旦发现状态异常, 如路由振荡严重、大规模 BGP 路由器失效等, 就可初步判定面临安全威胁, 进而再通过分析 BGP 更新报文等路由信息, 对安全威胁进行识别和定位. 尤其对基于 LDoS 的跨平面攻击, 通过态势感知技术实时评估域间路由系统的安全状态, 即可在遭受攻击的初期阶段感知威胁. LIU 等^[15] 提出一种基于 BGP 异常路由的域间路由系统安全态势评估模型, 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. 该方法依赖于异常路由集的完备性, 且不能有效评估域间路由系统在遭受跨平面攻击时的安全状态.

目前关于域间路由系统安全态势感知的研究成果较少, 尤其缺乏能够有效感知跨平面攻击的域间路由系统安全态势感知方法. 针对上述问题, 本文提出一种基于加权相似度的威胁感知方法 (threat perception method based on weighted similarity, WS-TPM), 利用多个特征融合描述域间路由系统的安全状态, 并结合网络流量的自相似特性, 以加权相似度为参数, 度量融合特征在各个时刻与正常状态时的偏差, 由此评估域间路由系统的安全状态, 在攻击的初期阶段感知威胁. 进一步, 根据发生威胁时各个安全特征的实时变化情况, 判定威胁的类型.

2 域间路由系统安全威胁分析

域间路由系统由大量以 BGP 为通信协议的自治域组成, 从逻辑功能上可以分为控制平面和数据平面. 其中, 控制平面负责交换域间路由信息、管控路由设备, 数据平面则负责转发数据报文. 下面以所处平面为分类依据, 对域间路由系统面临的主要安全威胁进行讨论.

2.1 基于路由信息的控制平面攻击

根据 BGP 协议的运行机理, BGP 邻居之间主要通过更新报文 (UPDATE) 交互路由信息. 从邻居路由器接收的所有路由都会被直接加入 RIB (routing information base), 路由选择进程再进一步从中选出前往各个网络的最佳路由并添加至 FIB (forwarding information base). 但在交互域间路由信息的过程中, BGP 路由器对来自邻居的路由信息的真实性并不进行验证. 恶意节点可以利用该缺陷, 随意伪造并宣告虚假或不符合路由策略的域间路由信息. 这些恶意路由一旦在域间路由系统内大范围扩散, 必将严重影响整个网络的安全稳定. 源自控制平面的安全威胁主要有 3 种.

(1) 前缀劫持 (prefix hijacking): 由于 BGP 路由器对来自邻居的 BGP 报文中的网络层可达性信息 NLRI (network layer reachability information) 不进行任何验证, 恶意 AS 就可以对外宣告任意一个

图 1 部分节点失效的级联传播

Figure 1 The propagation of cascading failure

非本 AS (autonomous system) 持有的前缀, 在该路由通告被大范围传播后, 网络中以受害前缀为目的地址的部分甚至全部数据包将被劫持到这个恶意 AS.

(2) 伪造路径攻击 (ASPATH tampering): ASPATH 是 BGP 协议公认强制的路径属性, 它用一组 AS 序列描述到达 NLRI 所属自治域的路径. 由于 BGP 协议没有验证 ASPATH 属性真实性的相关机制, 恶意 AS 就可以通过宣告含有伪造 ASPATH 属性的路由, 截获或丢弃路由到受害 AS 的流量, 造成网络不可达、流量窃听或流量黑洞 [16].

(3) 路由泄漏 (route leakage): 这是一种能够造成 BGP 路由发生严重错误、进而导致互联网部分中断的重要威胁 [4,17,18]. Dickson [17] 对路由泄漏进行了详细分析, 指出其具有以下 3 个特点: 第一, 泄露的路由通常是合法路由; 第二, 泄露的路由违反自治域间的路由策略; 第三, 路由泄露容易造成流量重定向.

2.2 基于大规模流量的数据平面攻击

基于大规模流量的数据平面攻击 (如 CXPST 攻击 [10]) 利用的是 BGP 协议自适应机制的特性, 通过对网络数据平面发起大规模流量攻击, 使网络路由器间的互连链路反复拥塞, 间歇、周期性地出现路由失效继而可用的情况, 使 BGP 路由器之间需要频繁地交换和更新路由.

对基于 BGP 协议的域间路由系统, 如果有路由节点失效, 它的邻居节点将向各自的邻居发送更新报文, 撤销与失效节点相关的所有路由. 当路由节点恢复服务时, 它会与所有邻居节点重新建立 BGP 会话并宣告前缀, 而它的邻居节点也会向各自的邻居发送更新报文, 由此将又开始新一轮的更新路由扩散. 一旦被攻击的路由节点达到一定数量时, 这种频繁、周期性地路由失效继而可用的情况, 会在域间路由系统中产生大量的更新报文, 而多数 BGP 路由器会因为需要处理这些更新报文而失效. 随着节点失效的快速级联传播 (如图 1 所示), 最终造成全局网络的更大范围瘫痪.

3 相似度与域间路由系统安全威胁感知

相似性是存在于任意两个对象之间的一种普遍关系, 而相似度作为相似性的定量表示, 通常被用于度量两个对象之间的差异程度. 本节首先介绍相似度的基本概念以及常用计算方法, 进而分析域间路由系统遭受攻击与正常运行时在一些特征属性上表现出的差异, 由此说明利用相似度评估域间路由系统安全状态并感知威胁的可行性.

3.1 相似度介绍

相似度是一个数学概念,用于计算两个数据样本之间的差异程度.目前,关于相似度的计算主要是基于向量距离的方法,下面给出基于距离的相似度的数学描述^[19].

对于 N 维样本空间 S 中的任意两个数据 X_i 和 X_j , 如果函数 $d_{ij} = d(X_i, X_j)$ 满足下列条件: (1) 对于所有 $X_i, X_j, d_{ij} \geq 0$, 当且仅当 $X_i = X_j$ 时, $d_{ij} = 0$; (2) $d_{ij} = d_{ji}$; (3) 对于任意 X_i, X_j 和 X_k , $d_{ij} \leq d_{ik} + d_{jk}$, 则称 d_{ij} 为数据 X_i 和 X_j 之间的距离. 相似度 $\text{sim}(X_i, X_j)$ 则用 X_i 和 X_j 的距离 d_{ij} 的倒数来表示, 即 $\text{sim}(X_i, X_j) = 1/d_{ij}$. 可以看出, 距离 d_{ij} 越大, 参与判断的数据样本 X_i 和 X_j 之间的相似度越小; 反之, 距离 d_{ij} 越小, X_i 和 X_j 的相似度越大.

计算相似度的常见方法有 4 种, (1) Minkowsky (明氏) 距离: $d(x, y) = (\sum_{i=1}^N |x_i - y_i|^m)^{1/m}$; (2) Euclidean (欧几里德) 距离: $d(x, y) = (\sum_{i=1}^N |x_i - y_i|^2)^{1/2}$; (3) Manhattan (曼哈顿) 距离: $d(x, y) = \sum_{i=1}^N |x_i - y_i|$; (4) Canberra 距离: $d(x, y) = \sum_{i=1}^N \left| \frac{x_i - y_i}{x_i + y_i} \right|$.

在上述 4 种计算方法中, Euclidean 距离和 Manhattan 距离是 Minkowsky 距离的特殊形式. 相比而言, Manhattan 距离的运算较为简单, 向量中各元素的误差对整体距离的影响权重都相同. Canberra 距离将元素误差占本身的比重也进行了考虑, 做了自身的标准化, 一般应用于对高度偏倚数据的处理. 而 Euclidean 距离则对较大元素误差在距离计算中的作用进行了放大, 这种计算方式的应用最为广泛. 由于在评估不同时刻域间路由系统安全状态的差异时, 强表征性特征具有更大的影响, 所以本文在计算相似度时采用 Euclidean 距离计算方式.

3.2 相似度与安全威胁感知

作为度量不同对象差异程度的主要方法, 相似度在信息检索、数据挖掘和人工智能等领域都有具体应用. 例如, 在信息检索中, 相似度反映文本与用户查询在词义上的符合程度; 在数据挖掘中, 相似度通常用于刻画不同数据样本的关联程度; 在基于人工智能的自动问答系统中, 相似度用于对问题和答案匹配程度的定量描述.

如第 1 节分析, 基于路由信息的控制平面攻击的本质是向其他域间路由节点宣告无效路由信息, 主要是伪造路径和非自有前缀. 当某个恶意节点向其他路由节点宣告伪造路径或非自有前缀时, 由于 BGP 协议没有验证路由信息真实性的相关机制, 根据路由选择算法的择优特性, 接收到更新报文的路由器会将路由表中的原有路由替换为路径较短的伪造路由, 同时向对等节点发送更新报文以宣告重新计算得到的较优路由. 可以看出, 当域间路由系统遭受基于路由信息的控制平面攻击时, 不仅 BGP 消息的数量会增加, 平均路径长度等属性也会发生较大变化, 而且特征变化越大说明攻击造成的危害就越严重. 也就是说, 遭受攻击时和正常运行时在某些特征属性上的相似度会有明显下降.

另外, 当域间路由系统遭受基于 LDoS 的数据平面攻击时, 初期阶段会有部分链路被间歇式地反复拥塞, 而链路的反复失效继而可用必然会导致 BGP 邻居之间需要通过 BGP 报文频繁交换和更新路由. 当这种路由不稳定在更大范围扩散后, 就会有更多的路由节点相继失效, 那么在域间路由系统中就会产生更大规模的 BGP 报文. 可见, 受到这种类型的攻击时, UPDATE 和 OPEN 等 BGP 消息的数量会急剧增加, 且攻击规模越大, 整个域间路由系统内的 BGP 消息总量变化就越大. 即, 域间路由系统遭受数据平面攻击和正常运行时在一些特征的相似度上会有所下降.

通过分析域间路由系统遭受攻击与正常运行时在一些特征属性上表现出的差异, 充分说明了利用相似度评估域间路由系统安全状态进而感知威胁的可行性. 因此, 本文提出一种基于多特征融合相似度的安全威胁感知方法, 用于评估域间路由系统的安全状态.

4 基于加权融合相似度的域间路由系统安全威胁感知方法

为了保证态势评估和威胁感知的有效性, 需要从宏观、全局上对域间路由事件和信息进行分析, 选取多个具有强表征性的属性作为域间路由安全特征, 融合描述域间路由系统的安全状态, 之后即可通过计算安全特征在各个时段与正常状态的相似度, 实现对域间路由系统安全状态的定量描述。

4.1 域间路由系统安全状态特征

本节分析域间路由系统中以 BGP 为通信协议的各个自治域在路由信息交互过程中存在的统计特征, 从中选取对域间路由系统安全状态具有强表征性的特征, 加入域间路由安全特征集合, 由此提供一种将域间路由安全特征与域间路由系统活动进行整合关联的方法。

4.1.1 更新消息数量特征

在 BGP 协议的 4 种消息中, 更新消息是核心内容. AS 间的路由信息交换主要通过更新消息实现, 包括增加新路由 (ANNOUNCE 消息) 和撤消旧路由 (WITHDRAW 消息). 一旦域间路由系统出现异常, 如拓扑不稳定或某些 AS 路由策略发生变化, 都会产生大量的更新消息, 所以更新消息的数量直接反映域间路由系统的稳定状况. 由于 ANNOUNCE 消息和 WITHDRAW 消息能够表征域间路由系统面临不同安全威胁时的状态差异, 为此将 ANNOUNCE 消息数量 (Number of ANNOUNCE, NOA) 和 WITHDRAW 消息 (Number of WITHDRAW, NOW) 作为评估域间路由系统运行状态的特征。

下面分析域间路由系统遭受不同类型攻击时 NOA 和 NOW 的变化。

(1) 基于路由信息的控制平面攻击是通过可控 BGP 路由器向其他 AS 的 BGP 路由器宣告错误路由信息. 其中, 前缀劫持和伪造路径攻击都是宣告虚假但一般较优的路由, 根据 BGP 路由选择算法的择优特性, 这些虚假路由将会通过 ANNOUNCE 消息的级联宣告在域间路由系统中大范围扩散. 显然, 发生这种情况时, NOA 值会变大, 且无效路由信息的规模越大或攻击者的层次越高, NOA 的增长幅度就越明显. 同样, 对于路由泄露, 泄露的路由也会通过 ANNOUNCE 消息的级联宣告在域间路由系统中大范围扩散, 所以发生这种情况时, NOA 值会变大, 且泄露路由的规模越大或层次越高, NOA 的增长幅度就越明显。

(2) 基于大规模流量的数据平面攻击利用 DoS 攻击网络数据平面, 使 BGP 路由器间的互连链路反复拥塞, 间歇、周期性地造成某些路由失效继而可用, 这个过程必然会有大量新路由的宣告和不可用路由的撤消, 具体定量反应就是 NOA 和 NOW 的值变大, 而且攻击越剧烈有效, NOA 和 NOW 的增长幅度就越明显。

4.1.2 路由路径特征

作为更新消息的公认必选属性, ASPATH 是 AS 间要交换的路由信息的主要内容, 用带有顺序的 AS 号序列来描述 AS 间的路径或到某个具体 NLRI 的路径. BGP 路由器向邻居发送更新消息的主要目的就是告知邻居某条路径现在可行或不可行, 所以无论是拓扑变化, 还是某些 AS 路由策略发生变化, 都会产生大量含有不同 ASPATH 的更新消息. 如果将某个时刻所有 AS 间的 ASPATH 综合起来, 就是域间路由系统在该时刻的拓扑结构. 所以, 通过比较不同时刻域间路由系统全部路由的 ASPATH 属性的差异程度, 可以衡量域间路由系统的拓扑波动幅度. 为此借鉴字符串差异性度量技术, 引入平均路径长度 (average path length, APL) 衡量不同时刻 ASPATH 的差异程度。

下面分析域间路由系统遭受不同类型攻击时 APL 的变化。

表 1 面临不同安全威胁时各个安全特征的变化情况
Table 1 Changes of security feature in different security threats

Security threat	Feature		
	NOA	NOW	APL
Prefix hijacking	↗	—	
Path tampering	↗	—	↘
Route leakage	↗	—	↗
Cross plane attack	↗	↗	↗

(1) 对于控制平面攻击中的前缀劫持和伪造路径攻击, 它们利用的是 BGP 协议的路由择优策略, 发布较优 (ASPATH 较短或前缀较长) 但不符合实际的路由, 这些虚假路由都要明显优于已有的实际路由, 一旦这些虚假路由在域间路由系统大范围传播, APL 将发生明显变化, 且攻击造成的影响越严重, 它相对于正常状态时的差异就越大. 而对于路由泄露, 这种威胁造成的是 BGP 路由发生严重错误、进而导致互联网部分中断, 由此造成原有路径不可行, 这种情况下 APL 的值也将发生明显变化. 且路由泄露越严重, APL 的变化幅度就越大.

(2) 数据平面攻击通过阻塞网络关键链路, 使得大量 BGP 路由器无法对外提供服务, 这种情况会造成许多原有较优路径不可行而被撤消, 而替代以宣告的大量较差路由, 此时的 APL 要大于正常状态时的值, 且攻击越严重, APL 相比于正常状态时的差异就越大.

表 1 给出域间路由系统在发生不同类型异常时各个特征的变化情况, 其中 “↗” 表示明显增大, “↘” 表示明显减小, “|” 表示明显变化 (可能是增大也可能是减小), “—” 表示变化不明显.

4.2 基于多特征融合的相似度计算方法

能够反映域间路由系统安全状态的特征有很多, 且采用的特征越多, 越能全面、准确地描述域间路由系统的安全状态. 但是, 特征越多就意味着安全状态的计算越复杂, 所以考虑到域间路由系统安全态势感知在实时性方面的要求, 本文只采用 ANNOUNCE 消息特征 NOA、WITHDRAW 消息特征 NOW 和平均路径长度特征 APL 等 3 个特征.

定义1 域间路由安全特征实时矩阵 I 为 $m \times 3$ 矩阵, 用于存储各个采集节点实时采集到的域间路由系统安全特征的值, 表示为

$$I = \begin{bmatrix} I_{11} & I_{12} & I_{13} \\ I_{21} & I_{22} & I_{23} \\ \cdots & \cdots & \cdots \\ I_{m1} & I_{m2} & I_{m3} \end{bmatrix}, \tag{1}$$

式中 I_{ij} 为该时段第 i 个采集节点采集到的第 j 个特征的值 (第 1 个特征为 NOA, 第 2 个特征为 NOW, 第 3 个特征为 APL). 若某个时段域间路由系统运行正常, 则将该时段对应的 I_t , 即由各个采集节点的路由数据 (包括 ANNOUNCE 消息数量 NOA、WITHDRAW 消息数量 NOW 和平均路径长度 APL) 构成的二维矩阵, 称为正常态数据.

定义2 域间路由安全特征标准矩阵 S 是对域间路由系统处于正常状态时各个安全特征的定量描述. 与实时矩阵 I 一样, 矩阵 S 也为 $m \times 3$ 矩阵, m 为采集节点的个数. 域间路由系统是一个动态变化的复杂系统, 为了保证标准矩阵 S 对域间路由系统运行状态的实时表征性, 需要在每采集到 1 个正常态数据时即对其进行更新, 更新方式为 $S(n+1) = \frac{S(n) \times n + I}{n+1}$, 式中 n 为更新次数.

考虑到 3 个安全特征的取值范围差异较大, 而它们取值范围的不一致性显然会导致处理结果更偏向于取值范围较大的特征. 为了平衡取值范围不一致的特征, 需要对 3 个特征全部进行归一化处理, 将特征取值归一化到 $[0, 1]$ 区间. 由于 3 个安全特征的量化值分布都不具有明显的概率分布特性, 为此本文采用线性函数归一化 (Min-Max scaling) 方法, 将原始数据线性化地转换到 $[0, 1]$ 的范围, 实现对原始数据的等比例缩放, 具体归一化方式为 $x_{\text{norm}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$, 其中 x_{norm} 为归一化后的数据, x 为原始数据, $x_{\max}$ 和 $x_{\min}$ 分别为原始数据集的最大值和最小值.

由此, 即可计算 t 时段实时矩阵和标准矩阵的 Euclidean 距离 $D_e(I, S) = \sqrt{\sum_{i=1}^m \sum_{j=1}^3 (I_{ij} - S_{ij})^2}$, 然后求两者的相似度 $\text{Sim}(I, S) = 1/D_e(I, S)$. 进一步, 对上式得到的相似度进行归一化处理, $\text{Sim}(I, S) = \frac{\text{Sim}(I, S)}{1 + \text{Sim}(I, S)} = \frac{1}{1 + D_e(I, S)}$, 由此将相似度的取值范围限制于 $(0, 1)$, 其值越接近于 1, 说明相似度越高.

4.3 增加权重的多特征相似度计算方法

通过 2.1 小节的分析可知, 对于不同类型的域间路由系统异常, 其引起各个特征的变化程度不尽相同. 或者说, 各个特征对不同类型异常的表征性存在差异. 例如, 发生基于 LDoS 的数据平面攻击时, 由于出现大量的链路或节点失效, 会产生大量的 BGP 消息报文, 尤其是 WITHDRAW 消息的数量相对于正常态时会急剧增长, 所以 NOW 特征的变化非常明显; 发生基于路由信息的控制平面攻击时, 会有大量伪造的较优路由被宣告到域间路由系统, 这种情况下的 APL 就会明显小于正常态时的 APL. 所以, 在计算多特征融合相似度时, 引入特征权重对方法进行改进.

定义3 安全特征权重矩阵 λ 描述各个安全特征在域间路由系统态势感知过程中的重要性. 本文采用三个属性为域间路由安全特征, 所以 λ 应该为 1×3 矩阵, $\lambda = [\lambda_1 \ \lambda_2 \ \lambda_3]$, 且 $\lambda_1 + \lambda_2 + \lambda_3 = 1$, 式中 λ_i 为第 i 个特征的权重, 其值可以通过训练数据进行估计和修正. 由此, 基于权重的多特征融合相似度的计算公式为

$$\text{Sim}(I, S) = \frac{1}{1 + D_e(I, S)} = \frac{1}{1 + \sqrt{\sum_{i=1}^m \sum_{j=1}^3 \lambda_j (I_{ij} - S_{ij})^2}}. \quad (2)$$

在 3 个安全特征中, 无论发生哪种异常, NOA 的值都会明显变大, 所以在初始化时, 可以取 $\lambda_1 = 0.4$, $\lambda_2 = 0.3$, $\lambda_3 = 0.3$. 后续可以根据先验数据对权重进行动态调整, 例如近期发生的异常主要为数据平面攻击, 则 $\lambda_1 = \lambda_1 - \Delta/2$, $\lambda_2 = \lambda_2 + \Delta$, $\lambda_3 = \lambda_3 - \Delta/2$; 如果近期发生的异常主要为基于路由信息的控制平面攻击, 则 $\lambda_1 = \lambda_1 + \Delta$, $\lambda_2 = \lambda_2 - \Delta/2$, $\lambda_3 = \lambda_3 - \Delta/2$. 注: $\Delta < \min(\lambda_1, \lambda_2, \lambda_3)$, 且为了保证各个特征权重平滑调整, Δ 取值不可过大, 如 $\Delta = 0.05$.

在得到多特征融合相似度之后, 计算特征偏差 $\text{Dev}_t = 1 - \text{Sim}_t$, 并判断偏差是否低于阈值, 即判断 $\text{Dev}_t(I, S) < \varepsilon_t$ ($\varepsilon \in (0, 1]$) 是否成立. 如果成立, 说明当前运行正常, 这时需要对标准矩阵进行更新; 如果不成立, 也就是说融合特征偏差高于阈值, 说明域间路由系统的安全状态较差, 向管理员发送异常报警. 阈值 ε 根据实际需要确定, 如果管理员对网络发生异常较为敏感, 可以取较小阈值, 如 $\varepsilon = 0.3$; 如果管理员只想关注较大规模的异常, 则可以选取较大阈值, 如 $\varepsilon = 0.5$.

图 2 (网络版彩图) NOA 和 NOW 特征的变化

Figure 2 (Color online) Changes of NOA and NOW

图 3 APL 特征的变化

Figure 3 Changes of APL

进一步, 由于域间路由系统在遭受不同类型攻击时, 各个安全特征的变化趋势存在差异. 因此, 在利用 WS-TPM 方法初步判断域间路由系统状态异常后, 可以通过跟踪 3 个特征的变化趋势并与表 1 进行比对, 从而确定域间路由系统遭受攻击的类型, 为后续制定合理的应对策略提供参考.

5 实验与分析

本节首先利用 RouteViews 项目提供的 BGP 路由数据评估 WS-TPM 方法在感知现实环境中的控制平面威胁的有效性, 进一步, 考虑到针对域间路由系统的大规模 LDoS 攻击不适于在现实环境中实施, 本文通过仿真实验, 验证 WS-TPM 方法在域间路由系统遭受基于 LDoS 的数据平面攻击时的有效性.

5.1 WS-TPM 方法的有效性

利用先前开发的 BGP ISS^[20] 对 RouteViews 各个采集节点采集到的路由数据进行分析, 可得到能直接用于 WS-TPM 方法所需的域间路由安全特征数据. 下面以 2015 年 3 月 10 日至 2015 年 3 月 12 日的路由数据为例, 进行安全威胁感知的应用说明, 分析该段时间内域间路由系统安全状态的变化.

首先根据 2015 年 3 月 1 日到 9 日期间采集得到的 300 个正常态路由数据 $\{I^1, I^2, \dots, I^{3000}\}$, 构建标准矩阵 S . 若某个时段域间路由系统运行正常, 则该时段各个采集节点的 3 个安全特征的对应值 x_{NOA} , x_{NOW} 和 x_{APL} 共同构成一个正常态数据. 然后对 10 日至 12 日的域间路由数据进行统计分析, 可得这 3 天内各个采集节点的安全特征 NOA, NOW 和 APL 的值, 由此构建各个时段的实时矩阵. 图 2 和 3 给出采集节点 route-views2.oregon-ix.net 在 10 日至 12 日期间 3 个安全特征 NOA, NOW 和 APL 的变化趋势. 可见, 在 21 日 09:00 至 10:00 期间, 域间路由系统中出现了大量的 ANNOUNCE 消息, APL 的值也明显大于其他时段, NOW 的变化则不明显.

将各个时段对应的实时矩阵 I_t 作为输入数据, 计算 I_t 与代表正常状态的标准矩阵 S 的相似度 $\text{Sim}(I_t, S)$. 之后, 计算特征偏差 $\text{Dev}_t = 1 - \text{Sim}_t(I_t, S)$, 并判断特征偏差是否在允许范围之内, 偏差越大说明域间路由系统的安全状况越差, 具体结果见图 4, 从而获取不同时段域间路由系统的安全状态. 显然, 在 12 日 9:00 至 10:00 期间, 域间路由系统相对于正常状态时的偏差明显高于 0.6, 表明该时间

图4 WS-TPM 方法的安全态势评估结果 (3/10~3/12)

Figure 4 Assess the security situation of inter domain routing system from March 10th to March 12th by WS-TPM

图5 DRL-TPM 方法的检测结果 (3/10~3/12)

Figure 5 Assess the security situation of inter domain routing system from March 10th to March 12th by DRL-TPM

段域间路由系统的安全状态较差. 进一步分析 3 个特征的变化趋势, NOA 明显增大、NOW 变化不明显、APL 明显增大, 由此可以判断异常类型为路由泄露. 根据 BGPmon.net 的报告显示, 在当天 08:58, 由于 Airtel 和 Hathway 的大量 BGP 路由泄露, 造成部分欧洲用户无法接入 Google 服务. 可见, 利用 WS-TPM 方法得到的结果与实际情况一致.

为了说明 WS-TPM 相对于其他 BGP 安全威胁感知方法的特点, 本文同样以 3/10/2015 至 3/12/2015 各时间段的域间路由信息为输入数据, 利用其他方法进行检测结果比较. 由于这是一次路由泄露事件, 所以选用文献 [18] 提出的基于路由循环检测的威胁感知方法 (threat perceive method based on detecting routing loops, DRL-TPM). 该方法同样支持以 Route Views 项目提供的路由信息为输入, 通过检测路由循环来识别路由泄露事件, 并以一个三元组表示一条路由泄露记录, 记录数量的多少则说明了路由泄露事件的严重性.

从图 5 可以看出, 在该时间阶段, DPL-TPM 方法检测出的路由泄露记录数量变化趋势较为平稳, 在 12 日 9:00 至 10:00 期间有涨幅, 但幅度不是很明显. 而且这种对异常路由进行简单记数的方式很容易让网络管理员陷于大量的细节信息, 实际上他们更希望威胁感知系统能够将域间路由系统的实时安全状态直观、定性地呈现出来, 只有在发现了重大异常后才去进一步关注细节信息. 另外, 虽然本文方法和 DPL-TPM 方法都是以路由信息为处理数据, 但是 DPL-TPM 方法需要分析每条路由并判断是否满足路由循环条件, 如图 2 所示, 仅 RouteViews 项目采集到的路由宣告已经达到每小时 10^6 的规模, 对数量如此巨大的路由进行逐条分析和判断所需的时间开销必然很大, 而本文方法仅对路由信息进行数量上的统计, 其时间开销要远小于 DRL-TPM 方法. 在实际测试中, 如果以小时为处理单位, 那么从安全特征的统计 (去除路由数据文件的下载时间) 到最后计算出该小时的安全状态偏差所需的时间通常都少于 2 分钟, 即 $t_{\text{total}} < 2 \text{ min}$.

5.2 WS-TPM 方法对数据平面威胁的感知能力

由于在现实网络环境中, 尚没有发生过且也不适于发起针对域间路由系统的大规模 LDoS 攻击, 所以无法采集到这种攻击真实场景的域间路由安全特征数据. 下面将通过一个仿真实验, 说明 WS-TPM

图 6 面临数据平面攻击时的安全态势感知结果

Figure 6 Security situation of inter domain routing system when suffering from data plane attack

方法在域间路由系统面临基于 LDoS 的数据平面攻击时的有效性. 鉴于仿真效率的考虑, 以及数据平面攻击主要针对 transit AS 的特点, 本文在实验中并没有采用全网完整拓扑, 而是根据 CAIDA 项目提供的 BGP AS links 数据, 从中选取那些有为其他 AS 提供转发服务的 AS, 以这些 AS 和它们之间的连接为拓扑数据 (1829 个 transit AS 以及它们之间的 13000 条链路), 利用 OPNET 软件构建域间路由系统仿真环境.

在域间路由仿真系统运行过程中, 通过部署的监测节点实时采集路由数据 (包括更新报文和 BGP 路由表), 然后利用 BGP ISS 对路由数据进行分析, 得到能直接用于 WS-TPM 方法所需的域间路由安全特征数据. 域间路由仿真系统从 2015 年 6 月 12 日开始稳定运行, 各个采集器也从该时刻起采集数据. 当采集到的正常数据达到 300 个, 构建标准矩阵 S , 并于 6 月 16 日 18:50 对仿真系统发起大规模 LDoS 攻击. 基于 LDoS 的数据平面攻击就是选择然后堵塞关键链路, 使关键链路上的节点对外频繁失效重启. 所以, 在仿真域间路由系统遭受大规模 LDoS 攻击时, 本文采取一种简单的方法, 具体步骤为 (1) 统计所有 AS 的节点度, 并计算整体度平均值; (2) 从节点度大于平均值的 AS 中随机选取一定比例 (α) 的 AS, 加入到节点集 F_AS ; (3) 将 F_AS 所有节点之间的链路置为满负载, 间隔 t 秒后再将这些链路置为轻负载; (4) 重复步骤 (3) m 次. 根据文献 [9, 10, 20] 的分析, 在实验过程中, 对域间路由系统 1% (α) 的关键节点之间的链路发起间歇性的基于大规模流量的蓄意攻击, 每次攻击的间隔时间 $t = 3 \text{ min}$, 攻击次数 $m = 10$ 次.

将采集器实时采集到的 16 日至 18 日的域间路由数据进行统计分析, 然后将各时段的 I_t 作为输入, 利用 WS-TPM 方法获取域间路由系统在不同时段的运行状态与正常状态的偏差, 结果见图 6. 可以看出, 在 16 日 19:00 至 20:00 期间, 域间路由系统相对于正常状态的偏差高于 80%, 表明该段时间域间路由系统的安全状态很差. 进一步分析 3 个特征的变化趋势, NOA 明显增大、NOW 明显增大、APL 明显增大, 由此可以判断异常类型为跨平面攻击. 以上结论与域间路由仿真系统的实际运行状况相符合, 说明了 WS-TPM 方法在域间路由系统遭受大规模流量攻击时的有效性.

在面临这种安全威胁时, 采用基于异常路由的检测方法很难准确、及时感知到域间路由系统出现异常. 因为它们需要以完备的异常路由数据集为输入, 才能准确计算出域间路由系统的安全状态. 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, 且检测结果的可靠性难以保证, 更重要的是数据平面攻击并不是通过宣告异常路由信息发起的, 整个过程也不产生异常路由.

6 结论

利用态势感知技术对域间路由系统运行状况进行实时评估, 能够从全局上分析域间路由系统的安全状态, 一旦发现状态异常, 就可初步判定面临安全威胁, 进而再通过分析 BGP 更新报文等路由信息, 对安全威胁进行识别和定位. 本文提出一种基于特征融合相似度的安全威胁感知方法, 利用多个特征融合描述域间路由系统的安全状态, 然后考虑到各个特征对遭受不同类型攻击时的安全状态具有不同程度的表征性, 以加权相似度为参数度量融合特征在各个时刻与正常状态时的偏差, 由此评估域间路由系统的安全状态, 进而感知是否存在威胁及面临威胁的类型. 论文对 WS-TPM 的有效性进行了验证, 实验结果表明, 域间路由系统在遭受较大规模的传统控制平面攻击或跨平面攻击等数据平面攻击时, 本文方法都能在攻击发生的初期阶段有效评估并直观反映域间路由系统的整体安全态势. 在此基础上, 可以通过进一步跟踪安全特征的实时变化情况, 推断域间路由系统遭受攻击的类型. 而且, 由于域间路由系统一旦遭受攻击, 必然引起 ANNOUNCE 消息特征、WITHDRAW 消息特征和平均路径长度特征 APL 发生变化, 即遭受攻击与正常运行两种状态之间的相似度一定较低, 所以针对域间路由系统的多数攻击很难规避本文方法的检测. 当然, 如果攻击的影响范围很小, 其引起特征变化的幅度就会不明显, 计算得到的融合特征偏差值也就不会太大, 由此会影响对是否遭受攻击的判断的确定性.

对于 WS-TPM 方法, 安全特征量化值的准确性直接影响评估结果的可靠性. 另外, 采用 WS-TPM 评估域间路由系统的安全态势, 需要构建并不断更新域间路由安全特征标准矩阵, 动态修正各个安全特征的权重, 这些过程都需要花费一定的计算资源. 也就是说, 相比于其他方法, WS-TPM 需要耗费更多的计算资源, 以精确量化域间路由系统的安全状态. 而且, 路由数据采集节点的选取与部署对域间路由系统全局态势感知的准确性具有重要影响, 本文目前只是采用 RouteViews 项目提供的多个采集节点采集到的路由数据, 下一步会继续研究采集节点应该如何部署, 才能使采集到的路由数据更加全面、准确地反映域间路由系统的实时运行状况.

参考文献

- 1 Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). IETF RFC 4271, January 2006
- 2 Barbir A, Murphy S, Yang Y. Generic threats to routing protocols. IETF RFC 4593, October 2006
- 3 Deng W P, Zhu P D, Lu X C. On evaluating BGP routing stress attack. J Commun, 2010, 5: 13–22
- 4 Li S, Zhuge J W, Li X. Study on BGP security. Chin J Softw, 2013, 24: 121–138 [黎松, 诸葛建伟, 李星. BGP 安全研究. 软件学报, 2013, 24: 121–138]
- 5 Lychev R, Goldber S, Schapira M. BGP security in partial deployment: is the juice worth the squeeze? In: Proceedings of the ACM Conference on SIGCOMM, New York, 2013. 171–182
- 6 Butler K, Farley T R, McDaniel P, et al. A survey of BGP security issues and solutions. Proc IEEE, 2010, 98: 100–122
- 7 Li Q, Zhang X W, Zhang X, et al. Invalidating idealized BGP security proposals and countermeasures. IEEE Trans Dependable Secure Comput, 2015, 12: 298–311
- 8 Jiang J, Li W, Luo J Z, et al. A routing evidence based malicious AS detection mechanism for interdomain routing inconsist path. Chin J Comput, 2016, 39: 1147–1161 [蒋健, 李伟, 罗军舟, 等. 基于路由证据的域间路由不一致路径恶意自治系统检测机制. 计算机学报, 2016, 39: 1147–1161]
- 9 Zhang Y, Mao Z M, Wang J. Low-rate TCP-targeted DoS attack disrupts Internet routing. In: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, 2007
- 10 Schuchard M, Mohaisen A, Foo Kune D, et al. Losing control of the internet: using the data plane to attack the control plane. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, 2010. 726–728

- 11 Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). *IEEE J Sel Areas Commun*, 2000, 18: 582–592
- 12 Malhotra A, Goldberg S. RPKI vs ROVER comparing the risks of BGP security solutions. In: *Proceedings of the 2014 ACM Conference on SIGCOMM*, New York, 2014. 113–114
- 13 Cohen A, Gilad Y, Herzberg A, et al. One hop for RPKI, one giant leap for BGP security. In: *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, Philadelphia, 2015
- 14 Lad M, Massey D, Pei D. PHAS: a prefix hijack alert system. In: *Proceedings of the 15th USENIX Security Symposium (USENIX-SS'06)*, Vancouver, 2006. 108–119
- 15 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]
- 16 Butler K, McDaniel P, Aiello W. Optimizing BGP security by exploiting path stability. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, Alexandria, 2006. 298–310
- 17 Dickson B. Route leaks-definitions. Internet Draft, 2012. <http://tools.ietf.org/html/draft-dickson-sidr-route-leak-def-01>
- 18 Li S, Duan H X, Wang Z L, et al. Route leaks identification by detecting routing loops. In: *Proceedings of the 11th EAI International Conference on Security and Privacy in Communication Networks*, Dallas, 2015. 313–329
- 19 Sun J X. *Modern Pattern Recognition*. Changsha: National Defense Science and Technology University Press, 2002 [孙即祥. *现代模式识别*. 长沙: 国防科技大学出版社, 2002]
- 20 Guo Y, Wang Z X, Luo S P, et al. A cascading failure model for interdomain routing system. *Int J Commun Syst*, 2012, 25: 1068–1076

A threat perception method for inter-domain routing systems based on weighted similarity

Yi GUO^{1,2}, Haixin DUAN^{1*}, Liancheng ZHANG² & Han QIU²

1. *Institute for Network Science and Cyberspace, Tsinghua University, Beijing 100084, China;*

2. *PLA Information Engineering University, Zhengzhou 450001, China*

* Corresponding author. E-mail: duanhx@tsinghua.edu.cn

Abstract BGP (border gateway protocol) based inter-domain routing systems play an important role in the Internet. However, the BGP has certain design flaws, which result in many serious security problems for inter-domain routing systems. Compared to traditional attacks, such as prefix hijacking, large-scale LDoS attacks against inter-domain routing systems are extremely hard to detect, which is reflected in its attack traffic and reactions appearing to be legal. The concealment of such attacks makes existing security solutions insufficient. In this paper, we first analyze the feasibility of utilizing similarity theory for assessing the security situations in inter-domain routing systems. We then propose a similarity-theory-based method for evaluating the security situations in inter-domain routing systems. It uses multiple characteristics to describe the system security situation collectively and evaluates the security situation by measuring the deviation degree of the security characteristics to their norms. Because the ability of each characteristic to represent different attacks is not the same, we make use of weighted similarity to assess the deviation of the fusion characteristics from their normal state at various times. Experimental results show that our method can perceive threats in their early stages, regardless of an inter-domain routing system suffering from control plane attacks or data plane attacks.

Keywords inter-domain routing, data plane attack, threat perception, weighted similarity, characteristics deviation

Yi GUO was born in China in 1984. He received a Ph.D. degree from PLA Information and Engineering University, Zhengzhou in 2012. His current research interests include Internet routing, routing security, and complex networks.

Haixin DUAN is a professor at the Network Science and Cyberspace Institute of Tsinghua University. His current research interests include network security, traffic analysis, and Next Generation Internet.

Liancheng ZHANG received his Ph.D. degree in computer science and technology from PLA Information and Engineering University, Zhengzhou in 2011. His current research interests include Next Generation Internet and network traffic analysis.

Han QIU received her Ph.D. degree in computer science and technology from PLA Information and Engineering University, Zhengzhou in 2010. Her current research interests include routing security and network simulation.