

校园网络安全中异常入侵快速定位方法研究

王 慧

(浙江商业职业技术学院, 浙江 杭州 310053)

摘 要: 研究了校园网络中快速确定异常入侵位置的方法, 提出区域入侵关联概率检测方法. 以网络节点间的相互关系为基础, 根据被入侵区域与其附近区域互相依存的关联程度, 估计被异常入侵区域的关联概率. 运用概率决策思维迭代锁定被入侵区域. 实验证明, 该方法能够提高获取校园网络中异常入侵位置的效率, 从而保证了校园网络的安全.

关键词: 校园网络; 异常入侵; 入侵关联概率

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)03-0159-04

Campus Network Security Abnormal Invasion of Quick Location Methods Research

WANG Hui

(Zhejiang Vocational College of Commerce, Hangzhou 310053, China)

Abstract: Study in campus network quickly determined the position of abnormal invasion method. This paper puts forward area associated probability detection method invasion. Network node in the relationship between as the foundation, according to the area and its surrounding area was invaded our interdependence on each other, the connection degree is estimated to be abnormal invasion of the region associated probability. Use probability decision thought iteration lock was invaded area. The experiment shows that, by using the method can improve the campus network for the efficiency of the abnormal invasion position, so as to ensure the security of campus network.

Key words: campus network; abnormal invasion; invasion associated probability

1 引言

在校园网络中, 网络终端设备是校园网络节点, 如果校园网络安全遭受破坏, 那么这些节点就会变成异常入侵, 影响信息安全, 需要利用快速、准确的方式获取异常入侵的位置才能保证校园网络安全^[1]. 所以, 异常入侵快速定位校园网络方法是校园网络安全的核心内容. 当前的检测异常入侵区域的方法, 必须选择一个典型的节点, 将其作为一个衡量的标准, 然后将需要进行判断的节点用此节点作为标准进行衡量, 如果二者差异较大, 则视为是异常入侵, 如果二者比较接近, 则视为是正常节点^[2-3]. 使用这种方式确定异常入侵在校园网络中的位置, 步骤比较繁复, 耗时也比较长, 不能快速准确获取异常入

侵在校园网络中的具体位置^[4-5].

为了避免上述问题, 提出区域入侵关联概率检测方法. 该方法依据节点间相互关系, 通过获取的异常入侵与其附近节点传输信息的情况, 迭代计算最大被入侵概率的区域, 迅速检测异常入侵所在区域.

2 异常入侵定位原理

网络异常定位方法获取校园网络中异常入侵位置时, 通过获取的异常入侵区域节点网络相关特征与典型节点的差异, 从而判断异常入侵大致区域, 再通过细微比较定位, 获取异常入侵在校园网络中的准确位置^[6]. 使用这种方法获取异常入侵位置, 能够保障了校园网络的安全. 具体步骤如下:

(1) 通过获取的异常入侵传输信息情况得到此

区域相关参数与典型节点的差异,相关参数值计算方法如下:

$$g(b_{jk}) = N \ln(q(b_j) \cdot q(b_k)) \quad (1)$$

在上述表达式中, $g(b_{jk})$ 是异常入侵相关参数值, $q(b_j)$ 与 $q(b_k)$ 是相邻节点数据参数, N 是路径参数。

(2) 根据上述表达式获取异常入侵相关参数值集合, 获取其精确位置, 计算方式如下:

$$G(a, b) = \ln N / \sum_k (g(b_{0j}) + g(b_{0j+1}) + \dots + g(b_{09})) \quad (2)$$

使用上面阐述的方法能够获取异常入侵在校园网络中的位置。但是这种方式需要使用到一个典型节点, 作为校园网络中节点是否异常的衡量标准, 这就导致在判断一个节点是否是异常入侵的时候, 必须将此节点与衡量标准进行逐个对比分析, 维护整个校园网络安全的步骤过于复杂, 衡量标准使用频率过高, 不能时刻保证校园网络的安全检测的效率, 效率衡量标准计算方法如下:

$$R = \ln N \cdot [(g(b_{0j}) - g(b_{1j-1}) - \dots - g(b_{j0}))] \quad (3)$$

通过上述公式计算结果能够得知, 能够检测到的异常入侵的节点数目与节点的使用频率成正比例关系。利用传统方式定位校园网络中异常入侵位置的效率计算表达式如下:

$$T = R \cdot \ln(g(b_{0j})) \quad (4)$$

利用传统方式定位校园网络中异常入侵位置的效率系数与衡量标准使用频率密切相关, 并且二者成反比例关系。因此传统定位方法与衡量标准的关系过于密切, 获取异常入侵的步骤过于繁杂, 导致使用传统方式定位校园网络中异常入侵位置效率比较低, 不能实时保证校园网络的安全。

为了解决上述问题, 提出区域入侵关联概率检测方法, 通过计算相关区域被感染的概率, 从而最终迭代计算获取异常入侵在校园网络中具体位置。运用该方法能够快速、准确地确定异常入侵在校园网络中的位置, 从而实时保证校园节点安全。实验证明, 使用相关探索确定位置方法能够提高获取校园网络中异常入侵位置的效率, 从而保证了校园网络的安全。

3 区域入侵关联概率检测方法

3.1 构造校园网络模型

算法的第一步是构造校园网络模型, 在这个校

园网络模型中, 所有节点都可以互相传递数据。设校园网络模型覆盖范围半径是 S , 在校园网络模型覆盖范围中选择一些已经确定具体位置的节点, 设为 $B_1, B_2, \dots, B_n$, 这些节点的临近节点设为 $Y_1, Y_2, \dots, Y_n$, 二者的距离用 e_j 表示。具体步骤如下: 首先, 获取节点的相关信息集合; 其次, 使用测取节点间距离的数学方法获取节点间的大致距离。假设获取的距离取值小于节点相关信息集合中的距离, 则将此取值放入内部存储器, 内部存储器中为最近获取的距离值, 代表了更新节点的结果。假设临近节点数据传输过程中, 路径上包含的节点数目超过路径负载极大值, 那么将获取的距离取值与之前存储器中的距离取值相加, 然后将节点相关数据参数放入节点相关信息参数集合中, 并对其位置进行估计。假设 Y_j 的估计位置用 (a, b) 表示, 那么通过此节点的相关参数, 计算临近节点距离极小值:

$$G = \sum_{j=0} \sqrt{(a+a_j)^2 - (b+b_j)^2} / e_j \quad (5)$$

在上面计算临近节点距离极小值表达式中, (a_j, b_j) 代表临近节点相互位置关系。通过临近节点相互位置关系特性得知, 利用相关探索确定位置方法获取异常入侵在校园网络中的具体位置, 需要先依据节点相关数据集合中的位置参数, 获取异常入侵的大致位置, 然后使节点间相互传输数据, 获取临近节点距离极小值, 建立相关概率关系统计。

3.2 选取合理临近节点

将节点的相关信息数据集合中的数据作为获取异常入侵位置的数据基础, 假设相关节点连线趋近于相邻区域, 那么通过数据方式获取距离结果偏差较大, 不能够将其忽略不计。假设相关节点平均分布在此节点临近位置, 则获取的距离取值偏差较小, 能够准确获取异常入侵在校园网络中的位置。相关探索确定位置方法需要根据区域特性, 选取临近相关节点, 在相关区域多个顶点处选取临近节点, 使相关区域变成校园网络覆盖区域, 从而平均分布校园网络中的节点, 最终减少获取异常入侵的计算步骤, 缩短获取异常入侵的计算时间, 精确定义异常入侵在校园网络中的位置, 保证校园网络安全。图 1 是利用三角形特性选取节点的示意图。

通过图 1 能够得知, 图中三角形是一个三个边长相等的特殊三角形, 复合最佳状态下节点分布位置, 三角形三个顶点连线趋近于直线。根据图 1 可以知道, 假设三角形三个顶点连线趋近于直线, 则三角形中最小内角角度趋近于 0° 。例如在三角形 CDF

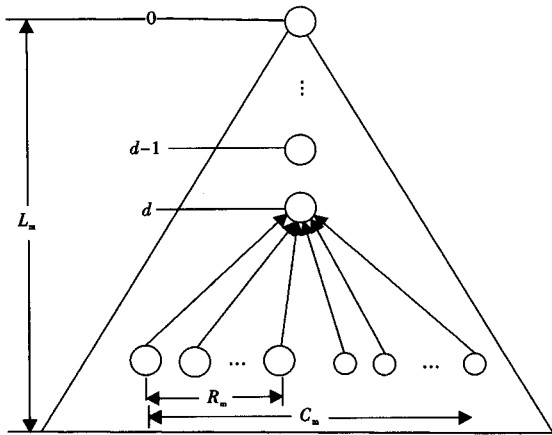


图1 利用三角形特性选取节点的示意图

中,假设将最小内角 $\angle CDF$ 的角度增大到 $\angle CDE$,那么依据三角形相关特性,三个顶点的分布更加平均.通过上面阐述得知,在选取临近节点时,优先选取三角形最小内角角度最大的节点,可以有效提高获取异常入侵在校园网络中具体位置的准确度.

根据三角形角度最小的内角小于 60° 的特性,以及三角形函数特性,相关三角函数可以作为选取临近节点的衡量尺度.首先需要确定获取异常入侵位置的衡量标准 F , r 代表最短边长, t 和 u 代表其它两条边,则通过下面表达式计算衡量尺度:

$$F = (\sin\beta + \cos\beta) / (s + t + u)^2 \quad (6)$$

充分考虑两节点连线长度极小值对获取异常入侵在校园网络中位置的影响,能够提高获取结果准确度.在长度极小值比较小时,衡量尺度可以通过下述表达式计算:

$$F' = (e_1 + e_2 + e_3)^2 / (r_{\min} \cdot F) \quad (7)$$

在上述衡量尺度表达式中, e_1 、 e_2 、 e_3 是选取的三个临近节点与异常入侵的长度,在传输信息的过程中,节点相关数据集合也随之传输,通过上述表达式能够得到合理的临近节点位置,然后获取异常入侵在校园网络中位置计算表达式如下:

$$G = (a_1^2 + a_2^2 + \dots + a_j^2) / (d_1 + d_2 + \dots + d_i) \quad (8)$$

3.3 获取异常入侵精确位置方法

通过上面阐述能够得知,传输节点相关信息数据集合后,假设数据集合中样本数量小于3,那么在临近节点获取新节点相关信息数据集合后,再进行校园网络数据传输,根据三角形特性选取临近节点.假设数据集合中样本数量不小于3,那么选择合理的临近节点,根据临近节点相关数据信息获取校园网络模型覆盖范围.如图2所示.

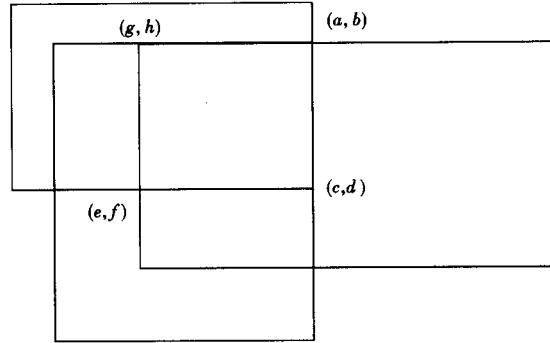


图2 校园网络模型覆盖范围

图2中三个覆盖范围的交点位置用 (a, b) 、 (c, d) 、 (e, f) 、 (g, h) 描述,可以利用下面表达式获取异常入侵大致位置 (m, n) 计算相关概率分布

$$P(m, n) = P((a - c)^2, (f - h)^2) \quad (9)$$

通过相关搜索确定位置方法获取的异常入侵在校园网络中位置并不平稳,趋近于衡量函数变小的取值,因此通过上面阐述的概率方法获取的位置是小范围中异常入侵的理想位置,而不是整个校园网络中异常入侵的理想位置.将全部结果通过迭代处理,才能获取校园网络中异常入侵精确位置.

通过迭代处理后的异常入侵位置是整个校园网络中最理想的异常入侵位置.假设异常入侵与邻近节点的大致位置不是整个校园网络中最理想的结果,那么继续进行迭代处理,直到获取结果达到标准为止.上述方法避免了传统方式获取异常入侵在校园网络中位置的衡量标准使用频率过高问题,缩短了计算时间,提高了获取校园网络中异常入侵位置的效率.

4 实验结果及分析

实验环境中,确定一个纵向是300米,横向是600米的范围是校园模拟网络范围.在这个校园模拟网络覆盖范围中,选择200个构造方式相同的节点.假设其中20个点是异常入侵,分别使用传统方式和相关探索确定位置方式计算异常入侵在校园模拟网络中的位置,分别得到两种方法获取结果使用的时间,并且通过下面的表达式计算获取结果的偏差:

$$\delta = \sum_{j=0} (a_1^j + a_2^j)^2 / r_{\min} \quad (10)$$

在上述表达式中, δ 代表获取的异常入侵在校园网络中位置的偏差系数, a_1^j 代表节点 j 的真实位置, a_2^j 代表节点 j 的估计位置, $r_{\min}$ 代表校园模拟网络覆盖范围的最小半径.不同方法得到的结果统计

趋势如图 3 所示。

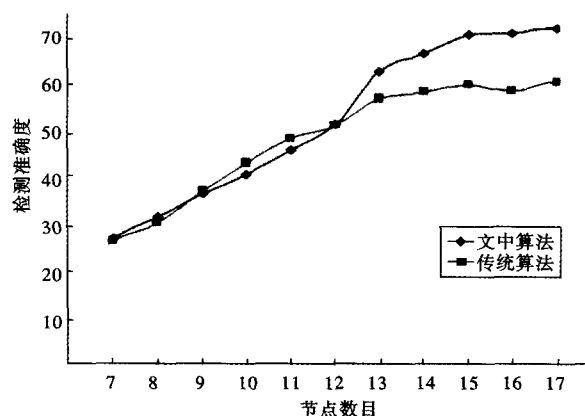


图 3 入侵定位趋势分布

通过运算获取两种方式获取异常入侵在校园模拟网络中的偏差系数,同时记录获取结果使用的时间,将两组数据进行对比分析,如表 1 所示。

表 1 两种方法定位数据对比

	时间	偏差
传统方法	10.7 s	29.7%
相关搜索确定位置方法	2.8 s	5.6%

通过上述实验结果能够得知,利用传统方式获取异常入侵在校园网络中的位置,计算步骤繁杂,使用时间比较长,获取结果的准确率较低,最终导致获取结果效率低。而相关探索确定位置方式获取异常入侵在校园网络中位置则避免了上述问题,符合了实时、准确确定校园网络中异常入侵位置的标准,保证了校园网络的安全。

5 结束语

本文使用相关探索确定位置方式获取异常入侵在校园网络中的位置,通过节点间的相互关系,平均分布临近节点位置,根据临近节点的相关数据集中的信息,及在传递数据过程中获取的局部节点参数,估计异常入侵位置,避免了传统方式获取校园网络中异常入侵位置时耗时长,准确率低等问题。实验证明,利用相关探索确定位置方式获取异常入侵在校园网络中的位置计算步骤少,耗时短,准确率高,能够准确、实时获取异常入侵在校园网络中的位置,从而保证校园网络的安全。

参考文献:

- [1] 张岳公, 范希骏, 李大兴. 计算机病毒入侵检测技术探讨[J]. 微电子学与计算机, 2005(11): 47-48.
- [2] 王涛, 余顺争. 无线自组织网络中多层有综合的节点行为异常检测方法[J]. 计算机科学, 2009(36): 246-247.
- [3] 刘涛, 肖汉. 基于目标定位的低功耗无限传感器网络节点设计[J]. 计算机测量与控制, 2009(11): 33-34.
- [4] 成汝震, 尚志恩, 袁军华. 校园网终端网络节点自治性的探讨[J]. 河北师范大学学报, 2003(5): 66-68.
- [5] Jan sen W. Intrusion detection with mobil agents[J]. Computer Communications, Special Issue on Intrusion Detection, 2002(25): 24-25.
- [6] Niculesce D, Nath B. Ad hoc positioning system (APS) using AoA[C]// Proc of the IEEE INFOCOM 2003. San Francisco: IEEE Computer and Communications societies, 2003: 1734-1743.

作者简介:

王 慧 男, (1980—), 硕士. 高级工程师研究方向为网络安全。