

基于局部联系的无线传感网络异常入侵检测

范荣真

(浙江商业职业技术学院, 浙江 杭州 310053)

摘 要: 提出一种局部联系对比搜索算法. 通过把节点刷新定位过程, 与其相邻的小范围分布网络的均值特征节点做比较, 利用局部无线网络节点最优信息, 检测异常入侵节点信息, 避免了传统集中式方法对全部节点搜索的耗时. 实验证明, 这种局部联系对比定位算法能够有效利用网络信息, 对异常节点实现准确入侵检测, 缩短了检测时间.

关键词: 无线网络; 局部联系; 入侵检测

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2012)03-0113-04

Based on Local Contact the Wireless Sensor Networks Abnormal Intrusion Detection

FAN Rong-zhen

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

Abstract: Put forward a kind of contact local contrast search algorithm. The node localization process through refresh, and its neighbors small areas of the distribution network of the mean value of feature nodes for comparison, the use of local wireless network node, the optimum information detection abnormal invasion node, avoid the traditional centralized information to all nodes of the search method in it. Experiments show that the algorithm can contact local contrast effective use of network information, abnormal node to realize accurate intrusion detection, shorten testing time.

Key words: wireless sensor networks; local contrast; intrusion detection

1 引言

随着无线传感网络的深入发展, 推出了消耗低的无线传感网络技术^[1-2], 其广泛应用于环境监测、军事国防、战场监视等特殊领域. 其通过预先在监控的地区装备大量的无线传感节点, 组成一个网状结构, 也就是无线传感网络. 由于无线传感网络通常应用于和人民生活相关的领域, 这样对无线网络节点的安全性提出了很高的要求^[3], 快速的检测出一些异常情况对无线网络节点的入侵, 实时保证无线网络的安全, 成为研究的目标.

2 无线网络异常入侵检测原理

无线网络节点入侵检测也被称节点异常检测, 常规方法根据节点自身的某些特性与标准节点来进行对照, 根据对照的结果判断节点是否遭到入侵^[4]. 通过在正常情况和被入侵的情况下, 根据节点某些特征变化, 完成对节点入侵的检测. 步骤如下:

(1) 建立无线传感网络节点的网状模型, 提取出正常情况下节点的某些特性 $Q(x, y)$;

(2) 利用节点在正常情况下的特征, 提取出节点中与其他节点特性相关性较小的数据作为待检测节点的原始信息, 方法如下:

$$\begin{cases} \frac{Q(x,y)-\bar{S}_{eqi}}{\ln(\bar{S}_{eqi})} < 0.5, & \bar{S}_{eqi} \text{ 节点正常信息} \\ \frac{Q(x,y)-\bar{S}_{eqi}}{\ln(\bar{S}_{eqi})} > 0.5, & \bar{S}_{eqi} \text{ 节点非正常信息} \end{cases} \quad (1)$$

式中,可作为对比识别的节点信息 $\bar{S} = (\bar{S}_{eq1}, \bar{S}_{eq2}, \dots, \bar{S}_{eqr})$, r 即为待检测的有效节点个数。

(3) 利用得到的节点有效信息与所有节点进行信息特征对比之前,需要对信息进行加权优化训练。设训练结果值 $D(k)$, 计算如下:

$$D(k) = \frac{1}{\cos w} \sum_{i=1}^r \ln(\bar{S}_{eqi}) \quad (2)$$

通过将正常节点的训练值 $D(k)$ 与无线网络内所有节点进行比较,确定节点是否正常:

$$\begin{cases} D(k) < \lambda, & \text{异常行为} \\ D(k) \geq \lambda, & \text{正常行为} \end{cases} \quad (3)$$

根据以上原理可知,提取节点信息时,获取的关乎入侵检测的信息特征越多,加权训练判决值 $D(k)$ 越准确,大规模的节点对比就会越准确,反之检测结果准确性相对较低,检测准确性的计算公式为:

$$\begin{aligned} L &= \frac{(D(k) - \Omega_d) \times r}{\sum_{i=1}^r \bar{S}_{eqi}} \\ &= \frac{\left[\frac{1}{w} \sum_{i=k-w+1}^k \ln(\bar{S}_{eqi}) - \Omega_d \right] \times r}{\sum_{i=1}^r \bar{S}_{eqi}} \end{aligned} \quad (4)$$

传统的无线网络节点入侵检测方法是以节点的正常特征信息作为对比数据源,当恶意入侵发生的时候,很难找到哪个节点被入侵,因此需要用正常节点信息与网络中所有节点进行对比识别,进而检测出哪些节点被入侵。但是,在一个大型无线传感网络中,大规模的节点对比十分耗时,这也给检测过程带来了麻烦。因此如何快速检测被入侵的节点,成为一个难题,本文将着重对此问题进行研究。

3 局部节点联系入侵检测

3.1 大规模无线传感网络区域模型建立

在进行节点异常检测之前,需要对网络建立区域模型,把大型的网络细分为几个小型网络,在单个网络中,各个传感器的配置是相同的,相互之间能够正常的通信。根据节点相似个数的不同,划分无线网络区域的大小也不同,假设一个无线网络区域中的

节点有 m 个,记作 $A_1, A_2, \dots, A_m$, 节点之间的距离记作 $X_1, X_2, \dots, X_n$, 节点之间距离不等。在入侵检测的无线传感网络中,承担入侵特征采集和对比数据转发的是区域无线网络节点。数目不同的节点组成了区域化的小型无线传感网络,而这些小系统又组成了一个庞大的无线网络系统,构成了各种实际应用的基础支撑平台。每一个区域无线网络中的单个节点都具有数据信息对比和发送两种功能。在完成无线传感网络入侵检测的过程中,需要完成以下 2 个功能:

(1) 实现节点自身特征数据的采集和对比。在硬件设计中,主要是通过节点特征信息传感器对节点异常数据特征进行采集,并对采集到的数据特征进行加权化处理。在一些大规模信息采集的过程中,为了传输简单,可能还需要运用压缩算法,因此区域网络节点必须具有快速处理数据的功能。

(2) 实现异常节点信息的传输和路由。区域节点能够发送本身对比后的信息,并接收和转发来自其他节点发送的数据,主动转发接到的信息,最终发送给终端系统。由于结构监测所要发送的数据量大,而且要反应快速,因此要求转发信息稳定可靠。这也对无线网络的性能提出了很高的要求。

运用区域划分的方法,以相邻节点的位置信息为基础,对大型无线网络进行小型化处理。根据划分后的小节点,进行区域节点单次多点对比,进行区域节点局部联系:首先根据区域节点中选出正常信息,然后让选出的标准节点与相邻节点进行信息对比,对比是根据位置信息为基础的,位置的半径大小选择合适的适配值。通过设计一个合适的选择算子,提高节点定位的准确性。

3.2 异常节点的区域对比识别

对比的方法是采用节点异常特征提取的方法,假设采集到节点的异常特征用 n 维向量表示,记作 $x = (x_1, \dots, x_n)^T$, 用 $\bar{x} = E[x]$, 区域矩阵 $R_x = E[xx^T]$, 特征差异矩阵记作 $C_x = E[(x - \bar{x})(x - \bar{x})^T]$ 。计算节点异常的过程可以表示,为运用 x 区域特征与异常的 y 区域特征 $y = (y_1, \dots, y_n)^T$ 对比识别的过程。计算方法如下:

$$y = U^T x = (u_1, u_2, \dots, u_n)^T x = \begin{pmatrix} u_1^T \\ u_2^T \\ \vdots \\ u_n^T \end{pmatrix} x$$

其中, $y_i = u_i^T x$, $i=1, 2, \dots, n$. x 可以表示为:

$$x = (U^T)^{-1} y = U_y y = U^T x = (U^T)^{-1} y = U_y$$

对节点的特征对加权优化处理, 以方便进一步对比识别, 加权过程如下所示:

$$\begin{aligned} \hat{x} &= \sum_{i=1}^m y_i u_i + \sum_{i=m+1}^n b_i u_i \\ \text{节点特征提取误差计算如下:} \\ \epsilon^2(m) &= E[(x - \hat{x})^T (x - \hat{x})] \\ &= \sum_{i=m+1}^n E[(y_i - b_i)^2] \end{aligned} \quad (5)$$

通过数学的知识, 可以得出: 当 $b_i = E[y_i] = u_i^T E[x] = u_i^T \bar{x}$ 时, 节点特征提取的误差最小. 由此可得:

$$\epsilon^2(m) = \sum_{i=m+1}^n E[(y_i - b_i)^2] = \sum_{i=m+1}^n u_i^T C_x u_i$$

为了使得计算的误差最小, $\epsilon^2(m)$ 的值也要最小, 通过以上的条件, 由

$$\frac{\partial J}{\partial u_i} = 0$$

其中

$$J = \sum_{i=m+1}^n [u_i^T C_x u_i - \lambda_i (u_i^T u_i - 1)] \quad (6)$$

得出:

$$C_x u_i = \lambda_i u_i, i=m+1, \dots, n$$

其中, λ_i 表示的是特征协方差矩阵的特征值, u_i 为对应的特征向量.

于是, 进行差异对比检测方法如下

$$\begin{cases} \epsilon^2(m) = \sum_{i=m+1}^n \lambda_i \\ E[(y_i - \bar{y}_i)^2] = \lambda_i \\ C_y = E[(y_i - y)(y_i - y)^T] \\ = U^T C_x U = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 \cdots & \\ & & \lambda_n \end{bmatrix} \end{cases}$$

因此, 通过解出以上的方程组能够实现节点特征对比, 能够把节点异常特征值分量比较完整的保存下来, 在简化运算量的同时, 又尽可能的保存了大量的原有信息. 很好的实现异常特征和正常特征的检测.

3.3 分区域异常节点定位算法实现

在小区域无线网络中, 根据节点的位置信息对其进行划分, 但是为了保证对比的准确性, 区域内节点的数目不能小于三个. 当相邻节点收到标准节点验证信息的时候, 如果验证无误, 会把标准信息传递

给其他及节点. 最终找到小区域内与标准节点存在异常的节点位置. 如果选择同时参与节点验证的节点数目大于3个, 可利用最优选择算子, 选择出最优的多个通信节点. 然后使用估计算法获得节点的初始位置解, 得到节点区域的公共范围, 如图1所示.

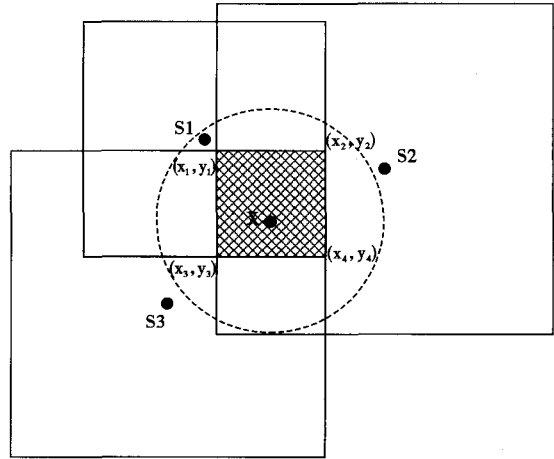


图1 多节点同时验证区域

如果上图中多个节点的区域可以分别表示为 (x_1, y_1) 、 (x_2, y_2) 、 (x_3, y_3) 、 (x_4, y_4) , 这样接可搜索得到标准节点的位置信息 (x, y) :

$$(x, y) = ((x_2 - x_1)/2, (y_3 - y_1)/2) \quad (7)$$

节点异常特征搜索算法中, 会出现特征误差的情形, 并且其误差通常是随着区域的临近会发生波动, 考虑到这种波动会得到最优计算节点, 但是得到的结果只是小区域网络节点的结果, 而不是整个网络中的结果, 因此根据小区域结果对大区域进行优化计算, 具体优化的公式为:

$$P_i(S_{\text{cur}} \rightarrow S_i) = \begin{cases} 1, & F(S_{\text{cur}}) \geq F(S_i) \\ \exp(-(F(S_{\text{cur}}) - F(S_i))/T_k), & F(S_{\text{cur}}) < F(S_i) \end{cases} \quad (8)$$

式(8)将相邻无线网络区域节点特征信息进行优化, 使计算出全局网络节点中的最优解. 通过与各区域各个节点的迭代计算, 使得受到入侵的节点的位置信息被逐步缩小, 最后获取最精确的定位信息. 这样通过相邻区域内, 公共节点通信获取异常节点特征信息, 并通过通信信息对节点进行位置精确定位, 避免了整理网络节点大范围对比造成网络负载过大, 定位不准的问题.

4 实验结果及分析

选定一个 $500\text{m} \times 500\text{m}$ 的无线网络区域, 并通

本文的方法把大区域分成 5 个小区,在无线网络监测区域内,建立 5 组具有相同结构的节点. 设定 10 个随机感应器节点为入侵节点,分别用传统的集中式定位搜索算法和本文的算法对这些被入侵的异常节点进行检测,记录两种方法的耗时,并利用下面公式计算平均误差:

$$E_{\text{error}} = \frac{\sum_{i=1}^m \|x_{\text{real}}^i - x_{\text{est}}^i\|}{mR} \quad (9)$$

平均误差是用估计待检测位置信息与被入侵节点实际的位置信息之间的欧式距离来表示的,距离越大误差越大. 计算两种节点异常检测方法的平均误差,并记录两种方法完成被入侵节点检测的耗时,两组数据的对比结果如表 1 所示. 图 2 为两种算法的平均误差趋势图.

表 1 两种方法定位数据对比

定位方法	定位耗时	平均误差
传统集中式	9.1 s	26.2%
本文算法	4.2 s	6.3%

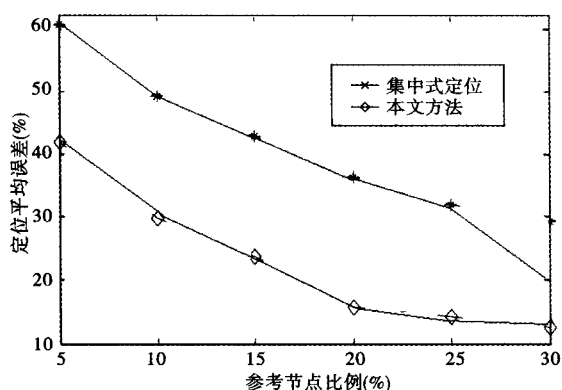


图 2 平均误差趋势图

(上接第 112 页)

以及连接产生的候选集规模也就较小,所以改进的算法效率优势就不那么明显.

总体上,可以得出,在候选集相同的情况下,改进的算法的执行效率明显优于传统算法.

5 结束语

本文的主要内容是对基于关联规则数据挖掘算法进行了分析研究,先详细描述了算法的步骤,再结合实际例子进行应用,然后分析了算法的缺点,针对它的缺点,提出了改进的算法. 改进的算法是通过减少连接判断次数,以及在生成候选集前对 L_k 进行了裁枝,产生新的频繁集 L'_k ,然后连接产生新的候选

由上述实验结果可以看出,本文的方法不仅缩短了定位耗时而且具有较高的定位准确率,满足了无线传感网络中对异常节点定位实时性的要求.

5 结束语

本文提出了一种区域联系的异常节点定位检测方法. 通过把大的无线网络分成小的区域,进而运用寻优算法,把定位过程分布到各个小网络中相关节点上,利用小区域相关节点中的正常信息,与局部节点信息进行比较,完成一次多节点比较,避免了传统集中式方法大规模比较的弊端,最终实现了无线传感网络入侵的快速定位.

参考文献:

- [1] 孙佩刚,赵海,张文波,等. 普适计算中定位服务的参考点布置及选择算法[J]. 电子学报, 2006, 34: 1456-1463.
- [2] Koutsonikolas D, Das S M, Hu Y C. Path planning of mobile landmarks for localization in wireless sensor networks[C]//Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops. Amsterdam, The Netherlands: IEEE, 2006: 80-86.
- [3] 姜华,袁晓兵,付耀先,等. 无线传感器网络中信道仿真模型的研究[J]. 计算机仿真, 2006(11): 129-132.
- [4] 王伟. 多信息源的实时入侵检测方法研究[M]. 西安: 西安交通大学出版社, 2005.

作者简介:

范荣真 男, (1974—), 硕士, 高级工程师. 研究方向为网络安全、电子商务安全.

集. 最后实验也证实了改进的算法的优越性.

参考文献:

- [1] 朱元忠. 入侵检测系统发展研究[J]. 北京工业职业技术学院学报, 2006(1): 8-11.
- [2] 陶剑文. 一种分布式 Web 日志挖掘系统的设计与实现[J]. 计算机仿真, 2006(10): 122-123.
- [3] 刘兵. Web 数据挖掘[M]. 北京: 清华大学出版社, 2009.

作者简介:

张翔 女, (1973—), 硕士, 讲师. 研究方向为图像处理、数据库技术.

陈胜勇 男, (1973—), 博士, 教授, 博士生导师. 研究方向为计算机视觉、图像分析与处理、机器人智能技术.