传感器网络定位中节点攻击类型的分布式识别算法

王夙喆, 李勇, 程伟, 王道平

(西北工业大学 电子信息学院, 陕西 西安 710072)

摘 要:针对无线传感器网络在定位过程中的外部攻击节点的类型识别问题,提出了一种交替方向-L_p 范数支持向量机(ADM-PSVM)分布式识别算法。该算法基于线性支持向量机分类模型,首先引入了 L_p 范数约束形式,通过选择不同的范数值 p 以增强分类算法对数据集的适应能力;继而根据交替方向乘子方法推导出了算法的分布式形式,实现了节点根据剩余能量将识别的计算任务分布于不同节点之间进行;最后将算法对各类型的恶意节点数据进行了训练及识别仿真,并讨论了范数约束值以及惩罚因子取值的不同对识别精确率的影响。仿真结果表明,该算法对于恶意外部攻击节点数据具有较好的识别精确度及更高的计算效率。

关 键 词:分布式;支持向量机;传感器网络;p 范数;定位;识别

中图分类号:TP393; TP181 **文献标志码**:A **文章编号**:1000-2758(2016)01-0085-07

在无线传感器网络(wireless sensors network, WSN)中,节点的位置信息无论对于环境监测和预报、目标跟踪等实际应用领域,还是基于地理位置的拓扑结构控制、路由算法等协议都起着重要的作用。但在实际应用中,传感器节点通常被布置于无人维护或者维护较困难的物理环境下,节点的定位过程容易受到来自内部或是外部的攻击,导致 WSN 产生错误或无效的定位结果[1]。

网络节点受到攻击的形式可以分为内部、外部攻击 2 种。内部攻击是攻击者通过俘获节点来获得信息密钥等信息,可以通过数据加密等方式进行防范;外部攻击是指恶意节点通过在物理和链路层上采用阻挡、反射等手段对信号进行干扰,或者在网络层采用重放、篡改报文的方式制造假象,典型的攻击方式有移位、重放、阻塞、虫洞攻击等,而常规的基于加密或变频等安全机制难以防御上述类型的攻击[2]。近年来,研究者提出了许多节点安全定位及恶意节点的检测算法,见文献[3]。然而,这些方法只是将恶意节点造成的影响降低或是检出后剔除,并没有对其攻击的类型进行后续的分析及识别,从而为以后有针对性地处理位置攻击事件,有效保障网络安全带来了不利影响。

支持向量机(support vector machine, SVM)是一种基于统计学习理论的分类算法,由于在分类问题的良好表现,已被应用于无线传感器网络领域的识别和检测问题。文献[4]基于 SVM 提出了一种入侵检测算法,该系统把网络拓扑分成簇头、簇成员和 Sink 3 层结构,每层均能根据 SVM 的训练结果进行入侵检测的判断。文献[5]利用 SVM 算法能够在高维空间对非线性样本进行分类的优点,通过各传感器节点估测其与锚点间的距离作为特征向量,最终对未知节点所属立方体空间进行分类来实现定位未知节点。以上算法都是集中式求解的,如果应用于能量与计算能力均受到限制的传感器网络,会出现大批节点的能量耗尽并失效;而且基于传统向量机分类器,对于不同数据的适应性较差。因此,研究具有高效识别能力,并能根据数据特征灵活改变的分布式算法具有重要的现实意义。

本文设计了一种分布式的交替方向-L_p 范数支持向量机(ADM-PSVM)定位攻击类型识别算法。该算法将 p 范数支持向量机作为识别的核心算法,通过引入分布式计算中的交替方向乘子法,将其计

收稿日期:2015-10-09 **基金项目**:国家自然科学基金(61401360)、陕西省自然科学基础研究计划(2014JQ2-6033)与中央高校基本科研业务费专项资金(3102014JCQ01055)资助

作者简介:王夙喆(1985—),西北工业大学博士研究生,主要从事无线传感器网络研究。

算过程分布于网络的不同检测节点,再利用邻居节点的位置、能量信息将迭代过程进行传递。由于该算法充分利用了支持向量机分类器优良的分类特性,同时也利用了 ADMM 迭代快速的特性,因此能在分布式的网络环境中对定位中的攻击行为进行准确而快速的识别。

1 WSN 定位攻击识别模型构造

1.1 WSN 定位攻击特点分析

假设网络中存在 n 个未知节点 $S_1,S_2,\cdots,S_n$,每个节点的实际位置表示为(x_{Si},y_{Si}),$i=1,2,\cdots,n$;另外有 m 个锚节点 $B_1,B_2,\cdots,B_m$,每个锚节点的位置表示为(x_{Bj},y_{Bj}),$j=1,2,\cdots,m$。未受到攻击时,某一未知节点 S_1 在通信范围内共存在未知节点 p 个,锚点 q 个,因此计算出 S_1 到未知节点及锚点之间的距离估计值分别为 $d_i,i=1,2,\cdots,p,d_j,j=1,2,\cdots,q$。

本文以未知节点 S_1 定位过程中,受到 4 种外部攻击而成为恶意节点 A_1 为例,逐类分析其节点间距离以及邻居节点信息的变化。① 重放攻击时,恶意节点 A_1 将锚节点 B_1 发往未知节点 S_2、S_3 的位置数据截取之后,随后重新发给它们,误让 S_2、S_3 认为 A_1 是锚节点 B_1,而原来节点 S_1 的 ID 信息不广播,其他邻居节点将不再发现 S_1。② 在虫洞攻击中,攻击方在距离 S_1 较远的某一个位置通过一个低延迟的连接接收锚节点以及未知节点发来的位置与距离信息,并在 A_1 处重放它们,此时 A_1 增加的距离信息分别为 $d_i,i=p+1,p+2,\cdots,p+u,d_j,j=q+1,q+2,\cdots q+v$。③ 阻塞攻击时,在节点 A_1 周围通过阻挡等手段削弱锚节点 B_j 发送至其他节点 S_2、S_3 的信号强度,使 B_1 到锚节点之间的距离 d_j 增加,并使 A_1 与其相邻所有节点的信号强度减弱或是消失。④ 移位攻击即攻击者重新放置未知节点 S_1,导致 S_1 的距离信息 $d_i,i=1,2,\cdots,p,d_j,j=1,2,\cdots,q$ 的取值重新改变。

经上述分析可知各种攻击类型对于未知节点 S_1 与其他未知节点或是锚节点的距离均会产生一定程度影响。将这些含有攻击特征的数据投射到一个二维平面后,如果能找到几条直线可以将这几类数据分开,那么这些直线就相当于最优分类平面,攻击类型识别问题进而可以转化为求解多个受约束的凸二次规划问题。本文根据以上分析,基于支持向量机和分布式迭代算法,研究在 WSN 网络环境下,根据数据类型的不同且依赖相邻节点间相互协作的分布式识别攻击类型的方法。

1.2 基于线性支持向量机的分类模型

在一个有限空间 $\mathbf{R}^n$ 里,假定有 n 个已标记的训练样本,其样本集表示为$\{\boldsymbol{x}_i,y_i\}$,其中$\boldsymbol{x}_i\in\mathbf{R}^N,y_i\in\{1,-1\},i=1,2,\cdots,n$。在线性可分情况下,SVM 的目的就是找到一个最优超平面,能将数据集中的 2 类样本完全分开并使 2 类数据点到超平面的间隔最大,寻找该最优分类面的问题可转化为以下最优问题[6]:

$$\begin{aligned}&\underset{\boldsymbol{w},b,|\xi_i|}{\operatorname{argmin}}\ \frac{1}{2}\|\boldsymbol{w}\|^2+C\sum_{i=1}^{N}\zeta_i\\&\text{s.t.}\quad y_i(\boldsymbol{w}_i^{\mathrm{T}}\boldsymbol{x}_i+b_i)\geqslant 1-\xi_i\quad i=1,\cdots,N\\&\xi_i\geqslant 0\quad i=1,\cdots,N\end{aligned}\tag{1}$$

式中,C 是惩罚因子,ξ_i 为松弛系数,引入 Lagrange 乘子 α_i,并将原问题(1)式转化为如下的凸二次规划的对偶形式:

$$\begin{aligned}&\max\sum_{i=1}^{n}\alpha_i-\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\alpha_j y_i y_j(x_i x_j)\\&\text{s.t.}\quad\sum_{i=1}^{n}\alpha_i y_i=0\\&0\leqslant\alpha_i\leqslant C,\ i=1,2,\cdots,n\end{aligned}\tag{2}$$

1.3 分布式交替方向乘子迭代算法

对于具有可分结构的凸规划问题,其模型如下:

$$\begin{aligned}&\min\quad F(\boldsymbol{w})+g(\boldsymbol{z})\\&\text{s.t.}\quad\boldsymbol{w}-\boldsymbol{z}=0,\ \boldsymbol{w}\in\mathbf{R}^n,\boldsymbol{z}\in\mathbf{R}^n\end{aligned}\tag{3}$$

交替方向乘子法按照如下顺序依次更新变量 $\boldsymbol{w}$、$\boldsymbol{z}$ 以及乘子 u,第 k 次的各个变量迭代更新步骤为[7]:

$$\boldsymbol{w}^{t+1}=\operatorname{argmin}\left(f(\boldsymbol{w})+<\boldsymbol{u}^t,\boldsymbol{w}-\boldsymbol{z}^t>+\frac{\eta}{2}\|\boldsymbol{w}-\boldsymbol{z}^t\|_2^2\right)\tag{4}$$

$$\boldsymbol{z}^{t+1}=\operatorname{argmin}\left(g(\boldsymbol{w})+<\boldsymbol{u}^t,\boldsymbol{w}^{t+1}-\boldsymbol{z}>+\frac{\eta}{2}\|\boldsymbol{w}^{t+1}-\boldsymbol{z}\|_2^2\right)\tag{5}$$

$$\boldsymbol{u}^{t+1}=\boldsymbol{u}^t+\eta(\boldsymbol{w}^{t+1}-\boldsymbol{z}^{t+1})\tag{6}$$

2 分布式 p 范数支持向量机分类算法

本文在(2)式和(5)~(7)式的基础上进行改

进,首先加入 L_p 范式约束, 其中 $0 < p \leqslant 2$;同时考虑到后续的分布式分类计算,将原问题乘常数 2,使其依然等价于问题(1)。从而提出的 p 范数 ADMM-SVM 分类算法的目标函数和约束条件改写为如下形式

$$\begin{aligned}&\min F(w) = \min_{\{w_i,b_i,\xi_i\}} \frac{1}{2}\sum_{n=1}^{2} \| w_n \|_p^p + C\sum_{i=1}^{N}\sum_{n=1}^{2}\zeta_{in}\\ &\text{s.t.}\quad y_{in}(\boldsymbol{w}_n^{\mathrm{T}} x_{in} + b_n) \geqslant 1 - \xi_{in}\quad i = 1,\cdots,N\\ &\qquad \xi_{in} \geqslant 0\quad i = 1,\cdots,N\\ &\qquad w_1 = w_2, b_1 = b_2 \end{aligned} \tag{7}$$

改写之后,问题(7)将可以用 2 个节点求解,因为等式约束保证了任何一个节点优化得到的可行解与另外一个节点的解一致。因此,将其中的一项进行改写后,得到

$$\begin{aligned}&\min F(\boldsymbol{w}) = \min_{\{w_i,b_i,\xi_{in}\}} \frac{1}{2}\| \boldsymbol{w}_1 \|_p^p +\\ &\quad \frac{1}{2}(\| \boldsymbol{w}_2 \|^p)^{1/p} + C\sum_{i=1}^{N}\sum_{n=1}^{2}\zeta_{in} =\\ &\quad \min_{\{w_i,b_i,\xi_{in}\}} \frac{1}{2}\| \boldsymbol{w}_1 \|_p^p + C\sum_{i=1}^{N}\zeta_{i1} +\\ &\quad \frac{1}{2}a(\| \boldsymbol{v}_2 \|^p)^{\frac{1}{p}} + C\sum_{i=1}^{N}\zeta_{i2} = f(w_1) + f(av_2)\\ &\text{s.t.}\quad y_{in}(\boldsymbol{w}_n^{\mathrm{T}}\boldsymbol{x}_{in} + b_n) \geqslant 1 - \xi_{in}\quad i = 1,\cdots,N\\ &\qquad \xi_{in} \geqslant 0\quad i = 1,\cdots,N\\ &\qquad w_1 - av_2 = 0 \end{aligned} \tag{8}$$

依据交替方向乘子法,第 k 次迭代步更替步骤可以写为:

$$\{\boldsymbol{w}_1(k+1),\xi_{i1}(k+1)\} = \operatorname{argmin} L'(\boldsymbol{w}_1(k),\xi_{i1}(k),a\boldsymbol{v}_2(k),\alpha(k)) \tag{9}$$

$$\{\boldsymbol{v}_2(k+1),\xi_{i2}(k+1)\} = \operatorname{argmin} L''(a\boldsymbol{v}_2(k),\xi_{i2}(k),\boldsymbol{w}_1(k+1),\alpha(k)) \tag{10}$$

$$\alpha(k+1) = \alpha(k) + \eta(a\boldsymbol{v}_2(k+1) - \boldsymbol{w}_1(k+1)) \tag{11}$$

如同在集中式 SVM 的情况下,问题(8)将通过其对偶问题解决,为了达到这个目标,引进拉格朗日乘子 $\alpha(k)$,并根据文献[8],(9) 对应的增广拉格朗日函数为

$$\begin{aligned}&L'(\{\boldsymbol{w}_1(k)\},\{\xi_{i1}(k)\},\{a\boldsymbol{v}_2(k)\}\{\alpha(k)\})\\ &\quad = \frac{1}{2}\| \boldsymbol{w}_1(k) \|_p^p + C\sum_{i=1}^{N} 1_{i1}\zeta_{i1}(k) +\\ &\quad \alpha(k)(\boldsymbol{w}_1(k) - a\boldsymbol{v}_2(k)) +\\ &\quad \frac{\eta}{2}\| \boldsymbol{w}_1(k) - a\boldsymbol{v}_2(k) \|^2 +\\ &\quad \sum_{i=1}^{N}\sigma_{i1}[1 - y_{i1}(\boldsymbol{x}_{i1}\boldsymbol{w}_1(k)^{\mathrm{T}} - b_{i1}) - \xi_{i1}(k)] -\\ &\quad \sum_{i=1}^{N}\boldsymbol{u}_{i1}^{\mathrm{T}}\xi_{i1}(k) \end{aligned} \tag{12}$$

注意到上述目标函数中含有 $\| \boldsymbol{w} \|_p^p$,所以为了顺利求得其对偶问题,必须保证在每一次迭代中 $\boldsymbol{w}(k)$ 值的有效性。因此引入向量 $\boldsymbol{V}$ 来表示 $\| \boldsymbol{w} \|_p^p$,得:

$$\begin{aligned}&L'(\{\boldsymbol{w}_1(k)\},\{\xi_{i1}(k)\},\{a\boldsymbol{v}_2(k)\}\{\alpha(k)\})\\ &\quad = \frac{1}{2}\boldsymbol{w}_1^{\mathrm{T}}(k)\boldsymbol{V}\boldsymbol{w}_1(k) + C\sum_{i=1}^{N} 1_{i1}\xi_{i1}(k) +\\ &\quad \alpha(k)[\boldsymbol{w}_1(k) - a\boldsymbol{v}_2(k)] +\\ &\quad \frac{\eta}{2}\| \boldsymbol{w}_1(k) - a\boldsymbol{v}_2(k) \|^2 + \sum_{i=1}^{N}\sigma_{i1} -\\ &\quad \sum_{i=1}^{N}\boldsymbol{\sigma}_1^{\mathrm{T}}\mathrm{diag}\{y\}\boldsymbol{X}\boldsymbol{w}_1(k) + \sum_{i=1}^{N}\sigma_{i1}y_{i1}b -\\ &\quad \sum_{i=1}^{N}\sigma_{i1}\xi_{i1}(k) - \sum_{i=1}^{N}\boldsymbol{u}_{i1}^{\mathrm{T}}\xi_{i1}(k)\\ &\boldsymbol{V} = |\ \boldsymbol{w}_1(k)\ |^{p-2}\\ &\boldsymbol{\sigma}_1^{\mathrm{T}} = [\sigma_{11},\cdots,\sigma_{N1}]^{\mathrm{T}}\\ &\boldsymbol{X} = [x_1,\cdots,x_N]^{\mathrm{T}} \end{aligned} \tag{13}$$

在算法实现过程中,一旦解出 $\boldsymbol{w}_1(k-1)$,即将 $\boldsymbol{V} = |\ \boldsymbol{w}_1(k-1)\ |^{p-2}$ 作为下一次迭代的目标函数中 $\boldsymbol{V} = |\ \boldsymbol{w}_1(k)\ |^{p-2}$ 的近似值代替,这样每一次迭代依然是标准的二范数 SVM 优化问题,而在初次迭代中,任意置一个初值或由二范数 SVM 作为 $w_1(0)$ 的初值;另外,由于 $0 < p \leqslant 2$,则 $p - 2 < 0$,为了保证 w_1 为正,在计算过程中将负号提取出来,完成后再将负号加上。

根据 KKT 条件,得到

$$\begin{aligned}&\frac{\partial L'}{\partial w_1} = \boldsymbol{w}_1^{\mathrm{T}}(k+1)\boldsymbol{V} - \boldsymbol{\sigma}_1^{\mathrm{T}}\mathrm{diag}\{y\}\boldsymbol{X} +\\ &\qquad \alpha(k) + \eta\boldsymbol{w}_1(k+1) = 0\\ &\boldsymbol{w}_1(k+1) = (\boldsymbol{\sigma}_1^{\mathrm{T}}\,\mathrm{diag}\{\boldsymbol{y}\}\boldsymbol{X} - \alpha(k))(\boldsymbol{V} + \eta)^{-1}\\ &\frac{\partial L'}{\partial \xi_{i1}} = C - \sigma_{i1} - \boldsymbol{u}_{i1}^{\mathrm{T}} = 0\\ &\frac{\partial L'}{\partial b} = \boldsymbol{y}^{\mathrm{T}}\sigma_{i1} = 0 \end{aligned} \tag{14}$$

把上述条件代入 $L'(\{w_1(k)\},\{\xi_{in}(k)\},\{av_2(k)\}\{\alpha_1(k)\})$,其对应的对偶问题可以表

示为：

$$\sigma_{i1}(k+1)=\operatorname{argmax}-\frac{1}{2}[\sigma_1^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k)]\cdot(V+\eta)^{-1}[\sigma_1\operatorname{diag}\{y\}X^{\mathrm{T}}-\alpha(k)]+(1+(\sigma_1^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k))(V+\eta)^{-1}(2\alpha(k)-\eta(w_1(k)-av_2(k))))\sigma_1^{\mathrm{T}}$$

$$\text{s.t.}\quad\sum_{i=1}^{N}y^{\mathrm{T}}\sigma_{i1}=0,\sigma_{i1}\geqslant 0,u_{i1}\geqslant 0,\ i=1,2,\cdots,N \tag{15}$$

同理，(10)式对应的拉格朗日函数为

$$\begin{aligned}L''(av_2(k),\xi_{i2}(k),w_1(k+1),\alpha(k))&=\frac{1}{2}av_2^{\mathrm{T}}(k)Uv_2(k)+C\sum_{i=1}^{N}1_{i1}\xi_{i1}(k)+\alpha(k)[w_1(k+1)-av_2(k)]+\\&\frac{\eta}{2}\|w_1(k+1)-av_2(k)\|^2+\sum_{i=1}^{N}\sigma_{i2}-\sum_{i=1}^{N}\sigma_2^{\mathrm{T}}\operatorname{diag}\{y\}Xav_2(k)+\\&\sum_{i=1}^{N}\sigma_{i2}\gamma_{i1}b-\sum_{i=1}^{N}\sigma_{i2}\xi_{i1}(k)-\sum_{i=1}^{N}u_{i1}^{\mathrm{T}}\xi_{i1}(k)\end{aligned}$$

$$U=|v_2|^{p-2} \tag{16}$$

$$v_2(k+1)=(\sigma_2^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k))(U-\eta)^{-1}$$

其对偶问题可以表示为：

$$\sigma_{i2}(k+1)=\operatorname{argmax}-\frac{1}{2}[\sigma_2^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k)]\cdot(U-\eta)^{-1}[\sigma_2\operatorname{diag}\{y\}X^{\mathrm{T}}-\alpha(k)]+(1+(\sigma_2^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k))(U-\eta)^{-1}(2\alpha(k)-\eta(w_1(k+1)-av_2(k))))\sigma_2^{\mathrm{T}}$$

$$\text{s.t.}\quad\sum_{i=1}^{N}y^{\mathrm{T}}\sigma_{i2}=0,\sigma_{i2}\geqslant 0,u_{i1}\geqslant 0,\ i=1,2,\cdots,N \tag{17}$$

基于 p 范数的 ADMM 算法的支持向量机迭代步骤(9)~(11)被为归纳为算法 1，在相邻的节点中执行的示意图如图 1 所示。进行迭代的 2 个相邻节点自身的能量都大于设定的阈值，并已知惩罚因子 C 和参数 η，然后分别依次设定初始的 $\sigma_{i1}(0)$、$\sigma_{i2}(0)$、$w_1(0)$、$v_2(0)$、$\alpha(0)$，2 个节点首先开始计算第 k 次迭代的矩阵 $N_j\times N_j$ 维的矩阵 $[\sigma_1^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k)](V+\eta)^{-1}[\sigma_1\operatorname{diag}\{y\}X^{\mathrm{T}}-\alpha(k)]$ 及 $[\sigma_2^{\mathrm{T}}\operatorname{diag}\{y\}X-\alpha(k)](U-\eta)^{-1}[\sigma_2\operatorname{diag}\{y\}X^{\mathrm{T}}-\alpha(k)]$，然后 2 个节点与输入的样本训练集 $\{x_i,y_i\}$ 更新其对偶问题的 $\sigma_{i1}(k)$、$\sigma_{i2}(k)$ 值，继续再计算 $w_1(k)$、$v_2(k)$ 的值，当计算完成后，将 $\sigma_{i1}(k)$、$w_1(k)$ 赋值于节点 2，最后更新出 $\alpha(k+1)$。这时根据转发规则，如果 2 个节点的剩余能量都大于其初始能量比较的阈值时，其继续进行 $k+1$ 轮迭代，否则，将选择一个距离低于能量阈值节点距离更近且具有更高能量水平的邻居节点，向其传递 $\sigma_{i2}(k)$、$v_2(k)$、$\alpha(k+1)$ 值，同时，原来的第2个节点就变成了第1个节点，负责迭代计算 $\sigma_{i1}(k+1)$、$w_1(k+1)$。

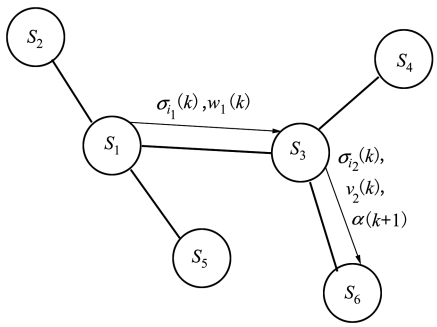


图 1 节点迭代计算示意图

3 实验仿真与结果分析

3.1 仿真设置及训练、测试样本获取

为检验 ADM-PSVM 算法的有效性，在 MATLAB 里对了定位攻击场景进行模拟。假设将 600 个未知节点以及 150 个信标节点随机部署点到 300 m×300 m 的区域，每个节点的剩余能量分配为随机值，通信半径设置为 20 m，其定位机制采用文献[9]提出的非测距 MDS-MAP 算法。按照以下步骤产生识别所需的训练及测试数据集：

1)将网络探测区域划分成边长为 60 m 的网格单元，使每个网格平均覆盖 2~3 跳范围内的节点。

2)未受攻击条件下，利用最短路径法分别计算网格内部各未知节点间以及未知节点与信标间的相异性矩阵 $\boldsymbol{B}_1$、$\boldsymbol{B}_2$，相异性矩阵定义为 $\boldsymbol{B}=-\boldsymbol{J}\boldsymbol{D}^2\boldsymbol{J}/2$，其中 $\boldsymbol{D}$ 为各节点间平方距离矩阵，$\boldsymbol{J}=\boldsymbol{E}-N^{-1}g\boldsymbol{I}$，$E$ 为 N 阶单位矩阵，$\boldsymbol{g}=\boldsymbol{I}^{\mathrm{T}}$，$\boldsymbol{I}$ 为 N 阶全一矩阵。每个节点依序号取 $\boldsymbol{B}_1$、$\boldsymbol{B}_2$ 中对应的一行共同构成向量 $\boldsymbol{X}_{\mathrm{nor}}$。

3) 从未知节点中取 120 个节点作为恶意节点，划分为移位、重放、阻塞、虫洞攻击 4 种类型并实施攻击，在干扰环境下重新计算相异性矩阵，并将节点

得到的新一组向量定义为 $\boldsymbol{X}_{\text{att}}$。

4) 以2种环境下产生的相异性矩阵的差的绝对值 $\boldsymbol{X}_{\text{test}} = | \boldsymbol{X}_{\text{nor}} - \boldsymbol{X}_{\text{att}} |$ 形成一组训练特征向量。

5) 重复步骤 1 ~ 4,将形成的向量作为测试样本。

实验中,将上述数据集生成步骤重复 5 次,总共产生 6 000 组样本,其中训练样本和测试样本各占 50%。为了将本算法应用到多类型攻击识别问题,本文采用目前应用比较广泛的 1-v-1-SVM 多类识别结构[1]。惩罚因子 $C=1$,$\eta=1$,而范数值 p 对于各类型攻击识别时,从初值 0.2,终值 2,以等差增加 0.2 的方式,依次进行测试。

3.2　实验结果与分析

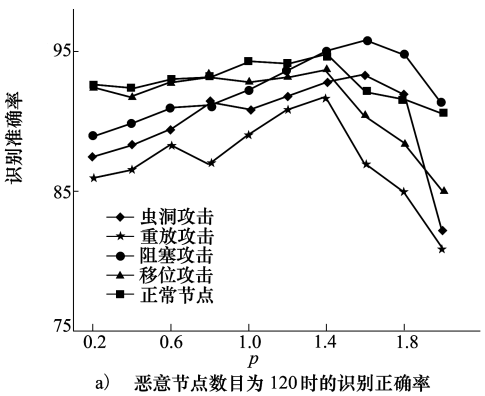
ADM-PSVM 算法和 C-SVM 算法对训练集测试样本的识别结果如表 1 所示,其中 ADM-PSVM 的识别率取所有范数 p 值下正确识别样本数与测试样本数之比之中的最大值。由表 1 可以看出,本文提出的算法比传统的标准 C-SVM 算法具有更好的识别精度。由于本文方法采用范数作为约束条件,不但控制了最优化问题解的稀疏性,也有效选择了与相应攻击类型标签高度相关的特征向量,减小了识别错误率;同时对目标函数使用较低阶次的范数约束,降低了原优化问题对异常值的敏感性,相比起传统的 SVM 方法,ADM-PSVM 避免了个别测距噪声的影响,具有更优优越的性能;在算法训练时间方面,本文提出的算法明显少于 C-SVM 的训练数据,尤其是当训练数据量较大时,使用 ADM-PSVM 有明显优势。对于 2 种算法均在识别过程中出现误差,经分析有以下影响因素:(1)网络测距误差。识别结果中有很多随机产生的无规律识别错误,这些都是由于在估计每对节点距离时,其采用的是最短路径算法,导致在节点分布不均匀的网络中测量距离与实际距离的偏差较大,所引起的相异性矩阵误差所导致。(2)特征样本采集不全。某一种攻击类型被识别为另一种是由于在训练样本获取阶段,网格的划分隔离了某些攻击类型的影响区域,特征向量无法完全获取所有遭受攻击的节点的数据。

表 1　ADMM-SVM 和 SVM 分类器准确率和训练时间比较

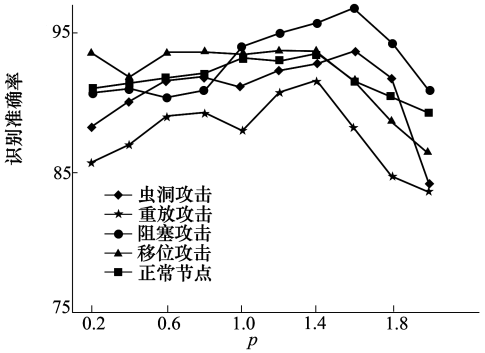
数据集 目标类	训练集数/ 测试集数	ADM-PSVM		C-SVM	
		训练时间/ 测试时间	识别率/(%)	训练时间/ 测试时间	识别率/(%)
虫洞	600/600	5.47/0.32	93.35	21.38/3.33	83.33
重放	600/600	4.90/0.21	91.62	20.45/2.26	81.67
阻塞攻击	600/600	4.12/0.30	95.00	22.24/4.45	88.33
移位攻击	600/600	5.07/0.20	93.71	21.11/2.38	85.00
正常节点	3600/3600	8.24/0.62	94.84	36.84/5.47	90.63

图 2 分别给出了恶意节点数目从 120 增加至 180 时,各范数 p 值对应的所有类型节点的识别准确率。从图 2a)、b) 显示的结果可以看出,从整体上,对于不同数目恶意节点的攻击环境下,ADM-PSVM 算法在 $p \in [0.2, 1.4]$ 或 $p \in [0.2, 1.6]$ 时,对于各类型节点的识别准确率随着 p 值的增加而逐渐升高;而在其余的范围内,均出现一定幅度下降,在 $p=2$ 时,其下降幅度最大。以图 2a) 中的重放攻击识别为例,算法从 0.2 增加到 0.8 时,其识别率仅仅增长了 2%,在 $p=1.4$ 时,识别率增长到最大值 91.67%,原因是较低的范数值降低了目标函数对测试集中异常值的敏感性,避免了类似测距误差的影响。但是当范数值选取过大时,当 $p=2$,目标函数选择了所有特征,包含了其他无关的特征以及噪声,导致识别的准确率下降到 80%。另外从图 2b) 可以看出,在节点总数不变的情况下,当恶意节点的数目增加到 180 时,各个类型的训练样本数目也相应增加,使分类器获得了更多的判别信息,提高了分类器的整体识别准确率。

图 3 分别给出 2 个范数值 p 约束下,带有不同惩罚因子 η 的 ADM-PSVM 算法对于虫洞攻击训练样本的经验风险误差的影响,恶意节点数目为 120。从图 3 各子图可以看出:2 幅图的误差收敛曲线趋势相似,并且当范数值 $p=1.6$ 时,ADM-PSVM 算法

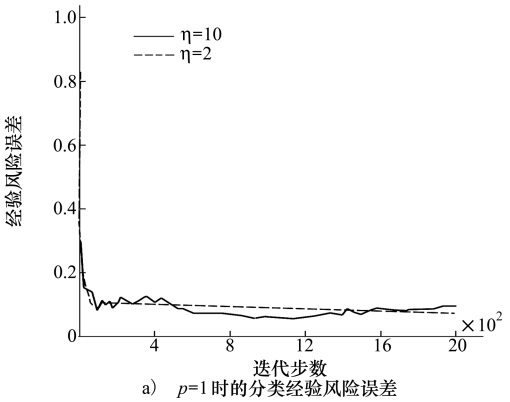


a) 恶意节点数目为 120 时的识别正确率

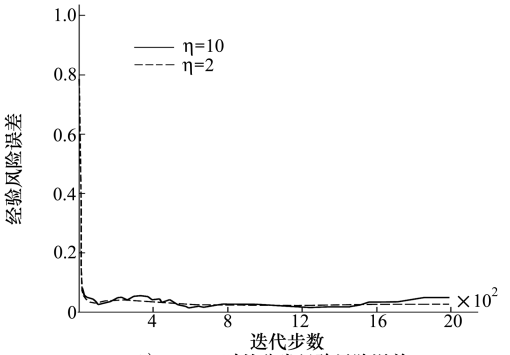


b) 恶意节点数目为 180 时的识别正确率

图 2 范数约束值 p 对识别正确率的影响



a) p=1 时的分类经验风险误差



b) p=1.6 时的分类经验风险误差

图 3 惩罚因子 η 对经验风险误差的影响

的分类经验风险误差较 $p=1$ 时有所下降;其次,算法在 $\eta=2$ 时,经过了一小段迭代后,分类器的经验风险误差开始逐渐趋于平稳。但是当 η 值过大时,不仅经验风险误差有所上升,且收敛迭代过程不平稳,迭代曲线出现了明显波动,这表示分类器出现了过度拟合训练数据的现象。虽然 ADM-PSVM 算法对于 η 的所有取值均会收敛,但是过大的 η 值阻碍了收敛速率,因此不同的参数值 η 会对分类器的训练结果造成一定的影响。

4 结 论

为了快速而准确地对传感器网络定位过程中进行攻击的恶意节点进行分类,本文提出了分布式 ADM-PSVM 节点定位攻击类型识别方法。不同于传统的集中式支持向量机分类器,该算法能将原有的识别问题分解为 2 个独立的子问题,并能够根据节点能量剩余情况转移迭代运算参数,从而将整体计算任务分配到了不同的节点上;而且 ADM-PSVM 还引入任意 p 范数约束的条件,在选择不同的范数 p 的,不仅在一定程度上选择了相关性更强的特征向量,也降低了由于噪声等干扰造成的影响,增强了分类器的识别性能及稳定性。通过在非测距定位机制下产生的攻击数据集的实验表明,本文提出的 ADM-PSVM 别算法取得了更优越的识别性能且降低了计算的时间复杂度。

参考文献:

[1] 刘华博, 崔建明, 戴鸿君. 基于多元分类的无线传感器网络恶意节点检测算法[J]. 传感技术学报, 2011, 24(5): 771-777

Liu Huabo, Cui Jianming, Dai Hongjun. Multivariate Classification-Based Malicious Node Detection for Wireless Sensor Network [J]. Chinese Journal of Sensor and Actuators, 2011, 24(5): 771-777 (in Chinese)

[2] Sun Bo, Shan Xuemei, Wu Kui, Yang Xiao. Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks[J]. IEEE Systems Journal, 2013, 7(1): 13-25

[3] Zeng Yingpei, Cao Jiannong, Xie Li. Secure Localization and Location Verification in Wireless Sensor Networks: A Survey[J]. Journal of Supercomputing, 2013, 64(3):685-701

[4] 汪淑丽. 基于支持向量机的无线传感器网络的入侵检测系统[J]. 传感器与微系统, 2012, 31(7): 73-76
Wang Shuli. Intrusion Detection System for WSNS Based on SVM[J]. Transducer and Microsystem Technologies, 2012, 31(7): 73-76 (in Chinese)

[5] 刘健, 沈海斌. 无线传感器网络的三维定位算法研究[J]. 传感器与微系统,2013,32(9): 66-71
Liu Jian, Shen Haibin. Study on 3D Localization Algorithm for WSNS[J]. Transducer and Microsystem Technologies, 2013, 32(9): 66-71 (in Chinese)

[6] Chen Jinhu, Takiguchi Tetsuya, Ariki Yasuo. A Robust SVM Classification Framework Using PSM for Multi-Class Recognition [J]. Eurasip Journal on Image and Video Processing, 2015, 1: 1-12

[7] Boley Daniel. Local Linear Convergence of the Alternating Direction Method of Multipliers on Quadratic or Linear Programs[J]. SIAM Journal on Optimization, 2013, 23(4): 2183-2207

[8] Xu M H, Wu T. A Class of Linearized Proximal Alternating Direction Methods[J]. Optimization Theory and Applications, 2011: 321-337

[9] Lu Xiaopei. MDS-Based Wormhole Detection Using Local Topology in Wireless Sensor Networks[J]. International Journal of Distributed Sensor Networks, 2012, 2012: 1-9

Distributed Localization Attack Type Recognition Algorithm for Malicious Nodes in Wireless Sensor Networks

Wang Suzhe, Li Yong, Cheng Wei, Wang Daoping

(Department of Electronics Engineering, Northwestern Polytechnical University, Xi′an 710072, China)

Abstract: The process of localization in wireless sensor networks is easily attacked by malicious nodes. In order to identify the types of those external attacks, an Alternating Direction Method of Multipliers-p-Norm Support Vector Machines(ADM-PSVM) algorithm is proposed. The proposed algorithm is based on classification model of the linear support vector machine. Firstly, by introducing a norm constraint into the classification algorithm, the adaptability of classifier for various types of dataset can be enhanced via selecting different value p. Then we derive distributed form of the algorithm according to Alternating Direction Method of Multipliers; this makes the classifier have the ability to distribute computing task among different nodes based on the residual energy of each node. Finally, the sample and testing dataset for each of four types of external malicious nodes are implemented in the training and testing processes of the proposed algorithm, and the influence on recognition accuracy performance in various p values and penalty factor η ones are discussed. The experimental results show that the proposed algorithm can achieve higher classification accuracy and better computational efficiency on the hostile external attack dataset.

Keywords: adaptive systems, classifiers, computational efficiency, eigenvalues and eigenfunctions, iterative methods, Lagrange multipliers, matrix algebra, mesh generation, sampling, support vector machines, vectors, wireless sensor networks; ADM-PSVM(Alternating Direction Method of Multipliers-p-Norm Support Vector Machines), attack type recognition, classification, distributed, localization, malicious, p-norm