

IDE-SVM 算法及其在物联网物理层安全中的应用

王强¹, 朱晨鸣¹, 潘甦², 秦玉玺²

(1.中通服咨询设计研究院有限公司, 江苏 南京 210019; 2.南京邮电大学, 江苏 南京 210003)

摘 要:针对支持向量机(support vector machine, SVM)算法参数选择没有标准的问题,提出了一种基于综合改进差分进化算法(improve differential evolution, IDE)的参数优化选择方法,以分类错误率最小为优化准则,利用改进的差分进化算法实现 SVM 参数的组合优化,获得了一种更高分类精度的 SVM 算法。为了避免基本 DE 算法在求解 SVM 参数选择问题时陷入局部最优,提高 DE 算法的搜索效率,提出了一种改进差分进化算法,通过使用圆弧函数对变异缩放比例因子 F 以及交叉概率因子 R 进行自适应控制,同时结合随机新生个体替换操作,得到一种收敛速度更快、精度更高的 DE 算法。在此基础上,提出了一种基于 IDE-SVM 物联网物理层安全方法。实验结果表明基于改进后 SVM 算法的物理层安全方法认证准确率更高。

关 键 词:物理层安全;支持向量机;差分进化;参数优化

中图分类号:TN918.91

文献标志码:A

文章编号:1000-2758(2024)05-0882-09

在无线终端到无线基站的安全接入问题上,传统方法采用上层协议对其进行加解密。然而,这种方法会消耗大量系统资源,增加通信时延,也容易被计算能力更强的恶意攻击者破解。同时,这种方法默认物理层本身安全的条件有待论证,用于传输密钥的信道安全难以保障^[1]。

事实上,由于衰落信道的时变性、唯一性、信道互易性、位置互异性等特性,每个用户的物理层信息就类似用户的“指纹”,是独一无二的,因此可以利用物理层信息(包括大尺度衰落因子、信号到达时间等)对用户进行接入鉴权。这种方案直接利用了通信过程中的信道估计信息,不需要额外传输信息,其安全性不依赖算法的复杂度,因此消耗算力较低,理论上在一定通信的信息量下不可被破解^[2]。

目前的物理层认证方法大多基于信道信息的先验知识^[3]。随着 5G 应用的普及,物联网接入设备爆发式增长,物理层信息量激增。利用机器学习算法可以高效地对物联网终端物理层的海量数据进行规律分析和特征提取,建立基于机器学习算法模型

的物理层安全接入认证方式。无需事先知道关于信道的先验知识,模型以信道观测数据为基础,通过“自适应”的认证方式安全接入网络^[4]。

尽管机器学习中有很多复杂的算法,但物联网节点的算力有限,无法使用复杂的算法^[5]。SVM 算法简单高效、泛化能力强,对数据规模和数据分布的要求低,在小样本训练集上比其他算法性能更好。采用 SVM 算法在基站中建立物理层安全接入认证模型,直接通过信号与信道包含的信息在物理层进行安全接入鉴权。

在二分类问题中,SVM 目标是在特征空间内寻找 1 个超平面,该超平面能够最大化地分隔开 2 个不同的类别^[6]。然而数据中往往存在不能满足理想线性分隔约束条件的异点,为了调整分类超平面对于分类误差的关注程度,引入错误惩罚参数 C 。 C 取值大时对损失函数对误分类的样本惩罚增大,少数样本对决策面的影响增加,因此可能造成过拟合现象, C 取值小时损失函数对误分类的样本惩罚减小,则可能造成相反的“欠学习”现象^[7]。另一个问题是:利用信道特征分类这一问题是非线性的,因而需要通过核函数 ϕ 对特征进行非线性变换,将特征映射到一个新高维特征空间中去,从而将非线性问题变换为线性问题,最后用线性分类的方法在新空

收稿日期:2023-09-22

基金项目:国家自然科学基金(62071244)资助

作者简介:王强(1976—),高级工程师

通信作者:潘甦(1969—),教授 e-mail:supan@njupt.edu.cn

间中寻找一个超平面对特征进行分类。核函数的映射能力受到核函数参数 g 的影响。目前来看,优化支持向量机(support vector machine,SVM)算法的参数优化所面临的主要问题是对于核函数参数 g 和错误惩罚参数 C 的调优,这 2 个参数直接影响算法学习能力、分类精度和泛化能力^[8]。

现有该参数选择问题的研究弊端很明显,比如文献[9]提出了一种基于禁忌列表遗传算法的 SVM 改进方法,但该方法需求算例多,耗时长且需要一直更新禁忌表;文献[10]提出了使用粒子群优化和遗传算法的 SVM 参数选择方案,但是,方案都存在干扰操作实时性不高的问题;文献[11]提出了利用网格搜索算法进行参数组合寻优,但网格搜索步长对准确率和速度的影响很大,步长难以控制,制约算法运算速度和准确性。

文献[12]提出了基于差分进化算法的参数组合寻优方案,避免了上述方法的一些问题,但差分进化算法有自身的性能缺陷,会造成最终找不到最优参数组合。文献[13]基于此也对差分进化算法做出了相关改进,但算法改进方向过于单一化,导致收敛慢,性能提升较小,不能最大地避免陷入局部最优解,在 SVM 参数寻优的应用中并不理想。因此,本文在差分进化算法的基础上,又提出了一种新的基于改进差分进化算法(improved differential evolution,IDE)的 SVM 参数智能化选取方法(IDE-SVM)。

1 基于 IDE-SVM 算法的物理层信息的安全接入方法

1.1 SVM 算法及其参数组合优化

1.1.1 基于 DE 算法的 SVM 参数优化方法

1) DE 算法的基本原理

DE 是基于群体智能理论,通过群体内个体间的相互合作、竞争进而产生的智能优化搜索算法,是一种随机启发式搜索算法。变异、交叉和选择是 DE 算法的 3 个核心操作,其关键思想在于对当前种群中的每一个向量,都要通过种群中另外 2 个随机选择的不同向量来进行干扰。

使用 DE 算法处理函数的优化问题,对于最小化函数问题 $\min f(\mathbf{x})$,假设有 $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_d]$,其中 d 是该函数优化问题的维数,对于向量 $\mathbf{x}$,其第 k

维参数变量具有上下界限: $l_k \leq \mathbf{x}_k \leq u_k(k = 1, 2, 3, \cdots, d)$,差分进化算法所生成的种群中每一个个体都是该函数优化问题的一个解 $\mathbf{x}_i = [\mathbf{x}_{i1}, \mathbf{x}_{i2}, \cdots, \mathbf{x}_{id}]$, $\mathbf{x}_i$ 表示算法种群中的第 i 个个体,从给定的约束范围内中,随机选择初始化种群个体,建立优化搜索的初始选择点。假定所有初始化种群都是符合均匀概率分布的,那么初始化种群操作则如(1)式所示。

$$\mathbf{x}_{ik}(0) = \text{rand}[0, 1] \cdot (u_k - l_k), i = 1, 2, \cdots, N \tag{1}$$

式中: $\text{rand}[0, 1]$ 表示 0 ~ 1 之间的随机数; N 表示种群规模,即随机产生了 N 个个体组成了初始种群。

标准差分进化算法的变异成分是父代的差分矢量,当下种群中的每个个体 $\mathbf{x}_i(g)$ 都会经过变异产生新的个体 $\mathbf{v}_i(g)$,其中 g 表示该种群进化到的代数。不同的 DE 算法方案会有不一样的变异个体的生成方法,标准差分进化算法变异操作如(2)式所示。

$$\mathbf{v}_i(g) = \mathbf{x}_{r_1}(g) + F \tag{2}$$

式中,序号 i, r_1, r_2, r_3 都不相同, F 为变异算子,是一个取值范围为 $[1, 2]$ 的实常数,用以控制偏差变量的放大作用。由(2)式可知, F 越大,基向量 $\mathbf{x}_{r_1}(g)$ 变异越多,种群多样性越丰富。

变异操作结束后将开始交叉操作,交叉的目的是增加干扰参数向量的多样性,避免早熟。每一个变量都需要生成一个位于 0 ~ 1 之间均匀分布的随机数。根据判定条件,交叉操作选择接受目标个体的对应分量还是保留当前个体的对应分量。交叉操作如(3) ~ (4)式所示。

$$u_i(g) = [\mathbf{u}_{i1}(g), \mathbf{u}_{i2}(g), \mathbf{u}_{id}(g)] \tag{3}$$

$$u_{ij}(g) = \begin{cases} v_{ij}(g), & \text{若 } \text{rand } b(j) < R \text{ 或 } j = \text{rnbr}(i) \\ \mathbf{x}_{ij}(g), & \text{若 } \text{rand } b(j) > R \text{ 或 } j \neq \text{rnbr}(i) \end{cases} \tag{4}$$

式中: $\text{rand } b(j)$ 表示生成 $[0, 1]$ 之间第 j 个随机数; $\text{rnbr}(i) \in (1, 2, 3, \cdots, d)$ 表示一个随机选择序列,保证 $u_{ij}(g)$ 从 $v_{ij}(g)$ 处获得至少一个参数。交叉算子 $R \in [0, 1]$,分析交叉操作公式可知: R 取值影响着种群的多样性和收敛速度, R 越大, $\text{rand } b(j) \leq R$ 的概率越大, $u_{ij}(g)$ 中参数由 $v_{ij}(g)$ 提供的就越多,有利于局部搜索和加速收敛速率。 R 越小则相反,会增加种群多样性,有利于全局搜索。

选择操作相对简单,决定 $u_{ij}(g)$ 能否替代 $x_{ij}(g)$ 成为下一代种群个体,假设 $u_{ij}(g)$ 的适应度函数值为 p , $x_{ij}(g)$ 的适应度函数值为 q ,适应度函数值越大越好。DE 算法依照贪婪准则,将 $u_{ij}(g)$ 的适应度函数值与 $x_{ij}(g)$ 的适应度函数值相比较,优胜者则成为下一代种群个体。如(5)式所示

$$x_{ij}(g+1) = \begin{cases} x_{ij}(g), & q > p \\ u_{ij}(g), & q \leq p \end{cases} \quad (5)$$

通过贪婪准则,在这种选择机制下,能够保证第 $g+1$ 代种群都比第 g 代相对应的个体好或者一样,如此逐步搜索找到最优解。

2) IDE 算法的原理与优势

参数自适应改进:DE 算法随着迭代次数的增加,种群多样性下降,有早熟收敛的缺陷。根据上述分析可知,DE 算法参数的设置对搜索性能有一定影响。DE 算法中的参数有: N , F 以及 R 。 N 的选取直接影响算法的搜索结果, N 值越大,全局搜索的最优解越好,但种群规模增加会导致算法消耗更多的系统资源,降低搜索效率。 F 和 R 参数的调节对算法搜索效率的影响较小。

然而,DE 算法针对 F 与 R ,都是依据经验设定一个常量,对于实际中不同的优化问题,使用常量显然不能使算法的精度达到最佳。根据算法原理分析,不难发现要使算法性能增强,避免早熟,参数 F 需要在算法搜索早期具有较大值,通过增加个体间差异来降低算法陷入局部最优的概率;而在搜索后期, F 要取较小值,使算法向最优解方向搜索,加快收敛。参数 R 则相反,在前期要保持较小值,后期保持较大值。这样在前期加强全局搜索,定位出全局最优解的搜索区间,减少不必要的计算,到后期加快向最优解聚焦。因此,本文提出了一种针对 DE 算法控制参数的自适应改进方案,在 F 与 R 各自的取值范围内,利用圆弧函数,将 2 个参数的取值与当前迭代次数联系起来,具体改进方法如(6)式所示

$$F = 2 \cdot \sqrt{1 - \left(\frac{g}{G}\right)^2} = 2 \cdot (1 - R) \quad (6)$$

式中: g 为当前迭代次数; G 为设定的终止迭代次数, $F \in [0, 2]$, $R \in [0, 1]$ 。

变异操作改进:将 DE 算法常用变异机制相结合,使变异机制在搜索前期更侧重于随机个体 $x_{r_1}(g)$,保持种群多样性,而在搜索后期侧重当前最优个体 $x_{\text{best}}(g)$,加快算法收敛,如(7)式所示。

$$v_i(g) = \gamma \cdot x_{r_1}(g) + 1(1 - \gamma) \cdot x_{\text{best}}(g) + F \cdot [x_{r_2}(g) - x_{r_3}(g)] + F \cdot [x_{r_4}(g) - x_{r_5}(g)] \quad (7)$$

式中: $\gamma = \frac{F}{2}$, $x_{r_1}(g)$ 为当前种群随机个体; $x_{\text{best}}(g)$ 为当前种群最优个体; $\text{best}, r_1, r_2, r_3, r_4, r_5$ 互不相同。

选择操作改进:为了确保进化向正确的方向进行,DE 算法选择操作依照贪婪准则,将生成的 $u_{ij}(g)$ 的适应度函数值与 $x_{ij}(g)$ 的适应度函数值一一对应比较,这样可以保证下一代种群比上一代优秀,即当 $u_{i1}(g)$ 的适应度函数值优于 $x_{i1}(g)$ 时, $x_{i1}(g)$ 被淘汰,但是如果 $x_{i1}(g)$ 的适应度函数值是剩余所有个体中最好的或是较优的,那么当出现这种 2 个优秀个体相比较情况时,必然会损失一个临时较优解,不利于搜索向较优方向进行,也降低了算法搜索效率。因此,本文提出一种新的选择方案,即优秀个体保留,低劣个体去除的方法。将 $u_i(g)$ 与 $x_i(g)$ 的所有个体合并起来,共 $2N$ 个,按照适应度函数值排序,将排序后的前 10% 优秀个体保留下来,末 10% 的较差个体全部去除,在剩余 80% 的个体中先按照标准选择机制一一对应比较选择,使 N 保持不变。若存在多余个体,则按适应度函数值排序末位淘汰,最终组成新一代种群。该方法不仅能够保存优秀个体,避免退化现象的发生,还能剔除最差个体加快差分进化速度。

随机新生个体替换操作:DE 算法之所以会陷入局部最优,其本质是随着迭代次数的增加,种群个体间的差异性逐渐缩小,出现了聚焦现象。在此引入种群个体适应度函数值方差的概念,假设种群个体数为 N ,第 i 个个体的适应度函数值为 $f_i(g)$,当前种群的平均适应度函数值为 $f_{\text{average}}(g)$,那么定义该方差为 δ^2 ,如(8)式所示

$$\delta^2 = \frac{1}{N} \sum_{i=1}^N |f_i(g) - f_{\text{average}}(g)|^2 \quad (8)$$

适应度方差 δ^2 是用来描述当前种群的聚集状态, δ^2 越大说明种群个体间差异性越大, δ^2 越小则说明种群聚焦程度严重,若 $\delta^2 = 0$,那么此时算法就很可能陷入了局部最优。为了使算法能够跳出局部最优解,继续进行有效搜索,为方差设定一个阈值 τ ,假设设定的终止迭代次数为 L 次, $\delta^2 \leq \tau$ 的次数记为 c ,每有一次 $\delta^2 \leq \tau$, $c = c + 1$;每有一次 $\delta^2 > \tau$,

$c = 0$ 。在迭代到 $\lfloor L/2 \rfloor$ 次之前,若连续 M 次迭代都有 $\delta^2 \leq \tau$,即 $c = M$,就判定算法陷入局部最优,则随机生成 k 个新个体,替换当前种群中第 $1 \sim k$ 个个体。其中 $\lfloor x \rfloor$ 为向下取整, $\tau \in [0, 1], M \in [5, 10], k \leq \lfloor N/10 \rfloor$ 。

1.1.2 基于改进差分进化算法的 SVM 参数组合优化

1) 参数选择对 SVM 性能影响分析

非线性 SVM 算法的性能优劣很大程度上取决于惩罚参数 C 和核函数参数 g 的取值。核函数的参数直接影响样本数据在高维特征空间中分布情况。特征子空间的维数越高,得到的最优分类超平面就会越复杂。因此,只有通过使用合适的核参数才能得到合适的特征子空间,从而使 SVM 分类器具有高效精确的分类能力。因此,核函数参数 g 及错误惩罚参数 C 的好坏对 SVM 性能有巨大影响。

2) IDE-SVM 算法

采用高斯核函数,定义误判率为种群个体适应度函数,误判率最小为优化目标,如(9)式所示

$$\min f = a \cdot \left(\frac{A_1}{B_1} + \frac{A_2}{B_2} \right) \tag{9}$$

式中: B_1, B_2 分别为2类样本的总数; A_1, A_2 分别为2类样本的误判数目; a 为缩放因子,用来调节适应度函数值变化的明显程度。IDE-SVM 算法具体步骤如下:

第1步 初始化种群,对参数 (L, N, F, R, τ, M, k) 进行设置,设置 C 和 g 的取值范围,并依据取值范围随机生成 N 组 (C, g) ,作为初始种群 $\mathbf{x}_i(g)$ 。

第2步 以第一步中获得的 (C, g) 作为 SVM 算法的参数,对样本数据进行训练和检验,并得到样本的分类结果,依据(9)式计算适应度函数值。

第3步 依据(7)式开始变异操作,生成临时解 $\mathbf{v}_i(g)$ 。

第4步 依据(4)式,进行交叉操作,生成新解 $\mathbf{u}_i(g)$ 。

第5步 依据(9)式计算新解 $\mathbf{u}_i(g)$ 种群的个体适应度函数值,并将其与当前种群 $\mathbf{x}_i(g)$ 合并排序,按照改进的选择操作进行选择,生成临时下一代种群 $\mathbf{t}_i(g+1)$ 。

第6步 依据(8)式计算种群 $\mathbf{t}_i(g+1)$ 的个体适应度方差 δ^2 ,对当前迭代次数和方差进行判定,决定是否进行随机新生个体替换操作,设替换操作后的种群为 $\mathbf{s}_i(g+1)$ 。若不需替换,则 $\mathbf{x}_i(g+1) =$

$\mathbf{t}_i(g+1)$,否则 $\mathbf{x}_i(g+1) = \mathbf{s}_i(g+1)$ 。

第7步 如果达到了终止条件,输出 SVM 最优参数组合 (C, g) ,否则转至第2步。

1.2 问题场景模型

考虑一个基站、一个合法的物联网无线终端及一个非法终端。令 $\boldsymbol{\tau}_A$ 为合法终端的信道特征向量

$$\boldsymbol{\tau}_A = [\tau_{A,0}, \tau_{A,1}, \dots, \tau_{A,N}] \tag{10}$$

式中,下标 N 代表每帧信号均匀采样的样本个数。合法无线终端正在向基站发送信息,此时非法信号尝试接入,基站需要从接收到的信号中找出合法信号。假设需检测信号的信道特征向量为

$$\boldsymbol{\tau}_f(m) = [\tau_{f,0}(m), \tau_{f,1}(m), \dots, \tau_{f,N}(m)] \tag{11}$$

式中:下标 f 表示需要鉴别发送者的身份; m 表示需要检测帧的编号。

研究中有如下假设:①非法信号源与合法无线终端相距一个波长以外,此时非法终端与合法终端信道不同。对于5G通信系统,波长为厘米级或者毫米级,所以非法信号源必然处于距与合法无线终端一个波长以外的距离。②无线终端的信道是慢衰落的。这个假设在终端设备不是高速移动的情况下是成立的。

根据上述假设,终端安全接入认证问题可以用假设检验问题表示。在无线基站侧建立已检测的合法无线终端的信道特征作为先验信息,对连续的信道特征进行相似性检测,判断其是否来自于合法无线终端。首先需要进行假设检验的就是首个信道特征信号帧的特征参量 $\tau_f(1)$,即

$$\begin{cases} H_0: \tau_f(1) = \tau_A(0) \\ H_1: \tau_f(1) \neq \tau_A(0) \end{cases} \tag{12}$$

$$\begin{cases} H_0: \tau_f(1) \text{ 来自合法无线终端 } A \\ H_1: \tau_f(1) \text{ 来自非法干扰信号源} \end{cases} \tag{13}$$

同时,利用接收到的信道特征参量对 SVM 进行训练,并对随后接收到的信道向量进行检验。因此,基于信道的认证问题可以表示为:利用合法终端已判决的信道向量 $\boldsymbol{\tau}_A(i-1)$,判断下一个连续的信道向量 $\boldsymbol{\tau}_A(i)$ 是否来自于合法终端^[14]。

1.3 物理层特征提取

在5G大规模天线通信系统中,使用多天线阵列,使得不同信号到达接收端的时间、大尺度衰落因子和到达接收天线的到达角也不同,因此这3个物理层参数适合用于信号安全接入认证。

信号到达时间 t :信号从发送端到接收端所经历的时间,为了设置门限值更容易,对 t 做如下变换

$$t = \frac{\min(t_{\tau_A}, t_{\tau_f})}{\max(t_{\tau_A}, t_{\tau_f})}$$

(14)

信号的大尺度衰落因子:假定符号 $\varphi(\tau)$ 表示信道 τ 的大尺度衰落因子。同样对 $\varphi(\tau)$ 做如下变换

$$\varphi = \frac{\min(\varphi_{\tau_A}, \varphi_{\tau_f})}{\max(\varphi_{\tau_A}, \varphi_{\tau_f})}$$

(15)

信号到达角和信号到达高度角:假设第 m 个用户第 i 个到达角为 $\theta_{m,i}$,导向矩阵记为 $\mathbf{R}_m$,采用矩阵的二范数来反映其特征

$$p(\tau_A) = \|\mathbf{R}_m\|_2$$

(16)

同样做如下变换

$$\theta = \frac{\min(p(\tau_A), p(\tau_f))}{\max(p(\tau_A), p(\tau_f))}$$

(17)

这样,第 i 帧的特征向量就可表示为

$$\mathbf{x}_i = (t_i, \alpha_i, \theta_i)$$

(18)

如此,比较 2 个信道向量的相似性就通过 $\mathbf{x}_i$ 来完成。

1.4 安全接入方法流程

图 1 为物理层安全接入方法流程图。

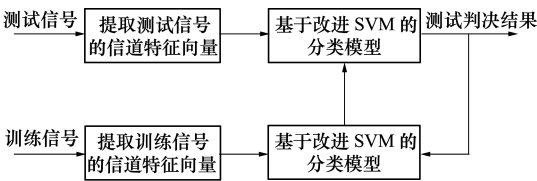


图 1 无线终端安全接入方法流程图

具体步骤如下:

- 1) 提取信号的特征值 $(x_1, x_2, \cdots, x_n)$, 同时与信号明确合法与否的标签 $\mathbf{y}_k$ 构成特征向量 $\{\mathbf{x}_i | \mathbf{x}_i \in \mathbf{R}^2, \mathbf{y}_i \in \{-1, 1\}\}$, 并将其视作训练样本集合。
- 2) 在离线训练阶段,用上述样本集作为模型输入来求解二次规划方程并寻找最优超平面。
- 3) 在测试阶段,提取接信号的物理层特征并组成特征向量,使用训练过的 SVM 对信号来源是否合法做出判定。
- 4) 再学习阶段,将已分类的合法和非法无线终端的特征向量加入原先样本集再次训练 SVM,这样做是为了适应用户信道的缓慢变化。

2 实验分析

2.1 IDE 算法性能

本文采用典型的优化算法测试函数测试 IDE 算法性能,这里标准 DE 的 R 值设为 0.2, F 值设为 0.5。而 IDE 算法中的 F 和 R 分别按照(6)~(7)式进行自适应变化,且变异策略也按照(8)式进行,选择和替换操作按照改进方案进行。为避免实验偶然性,保证测试质量,算法独立运行 20 次,算法迭代次数为 500,种群大小为 100,维数为 10。结果如表 1 所示。

平均最优适应值用于衡量被测算法求解精度的优劣。平均最优适应值值越小,求解精度越高。标

表 1 算法寻优测试结果

函数	算法	最优解	平均最优适应值	标准差
Griewank	DE	4.521×10^{-9}	5.942×10^{-9}	9.201×10^{-10}
	IDE	0	0	0
Ackley	DE	2.051×10^{-4}	2.433×10^{-4}	1.705×10^{-5}
	IDE	4.236×10^{-15}	4.441×10^{-15}	2.492×10^{-30}
Rastrigrin	DE	23.46	38.96	4.079
	IDE	0	0	0
Schaffer	DE	4.722	5.254	4.068×10^{-1}
	IDE	1.211×10^{-4}	1.024×10^{-1}	1.199×10^{-1}
Sphere	DE	8.85×10^{-8}	1.40×10^{-7}	3.33×10^{-8}
	IDE	1.14×10^{-117}	2.45×10^{-111}	4.97×10^{-111}

准差用于衡量算法稳定性,标准差值越小被测算法的稳定性越高。迭代相同次数的最优解越小,代表算法的收敛速度更快。表 1 通过对比这 3 个值可以看出 IDE 算法相较于标准 DE 算法求解精度高,稳定性更好,观察最优解对比发现 IDE 算法求得的解也更接近理论最优解,收敛速度更快,跳出局部最优解的能力更强。

2.2 基于 IDE 的 SVM 算法性能

实验数据选自 UCI 机器学习标准库中数据集。该数据集对应的任务是典型的二分类任务。由于 SVM 算法计算代价较大,为了能够快速测试,选取数据集中 500 组样例。实验数据选取不平衡会而影响分类结果,因此实验选取的 2 类样本数接近。实验样本中,70% 作为训练样本,30% 作为测试样本,核函数采用高斯核函数。

首先对 DE 算法中的参数进行初始化设置:最大进化代数 $G = 500$,种群规模 $N = 80$,缩放因子 k 和交叉概率 R 按改进的自适应方案设置,方差阈值 $\tau = 1, M = 5, k = 8$ 。SVM 惩罚参数 C 以及高斯核函数参数 g 的取值范围均设置为 $[0.000\ 1, 1\ 000]$ 。误判率函数即适应度函数中 $a = 3$ 。实验结果如表 2 所示。

表 2 算法实验结果对比			
算法模型	错误惩罚因子 C	RBF 核参数 g	准确率/%
SVM	31	2.653	92.32
IDE-SVM	43	0.362	98.96

从表 2 可以看出,与标准 SVM 算法模型相比,IDE-SVM 算法模型,分类精度更高,分类结果更准确。

2.3 物理层安全仿真分析

仿真实验假设合法无线终端与基站相距 300 m 且处于低速移动状态,非法信号源以同样的频段模拟合法无线终端与基站进行通信。基站侧对接收信号的每个子帧进行 15 次均匀采样并提取对应的物理层特征得到信道特征向量。合法无线终端样本标签为 1,非法信号样本标签为-1。信道使用互耦信道模型,基站采用线性天线阵列,信道的信噪比为 15 dB,依据在非视距场景下到达时间差(TDOA)和到达角(AOA)的误差模型^[15],分别取合法无线终端

TDOA 分布区间 $U(1\ \mu\text{s}, 1.3\ \mu\text{s})$, AOA 分布区间 $U(0.1\pi, 0.15\pi)$,取非法干扰信号源 TDOA 分布区间 $U(1.5\ \mu\text{s}, 1.6\ \mu\text{s})$, AOA 分布区间 $U(0.3\pi, 0.35\pi)$,与基站相距 200 m,通信系统其他基本参数如表 3 所示。

表 3 系统基本参数表	
参数名称	值或范围
载波频率/GHz	28
基站天线数目	128
路径损耗指数	3
相邻天线间距	半波长
互耦信道模型天线阻抗	0.95
互耦信道模型负载阻抗及互阻抗	0.05

为防止因实验数据选取不平衡而导致分类结果影响,样本集共有 200 个,2 类数据样本数接近,仿真实验结果如图 2~3 所示。

图 2a) 是 SVM 参数选择优化前训练集的鉴权情况,从图中可以看出基于标准 SVM 的安全接入认证模型有 4 个样本出现了错误判定。

图 2b) 是 SVM 参数选择优化前基于训练集的参数选择结果与认证准确率,其中 g 和 C 是 SVM 2 个参数的选择结果,每组参数组合都对应着曲面上的一个接入认证准确率,从图中可以看出参数选择优化前安全接入认证模型基于训练集的漏警率(即假设 H_1 成立的条件下仍判别为来自合法无线终端)约 2.9%。

图 2c) 是 SVM 参数选择优化前测试集的鉴权情况,从图中可以看出基于标准 SVM 的安全接入认证模型有 2 个样本出现了错误判定,漏警率达到 3.4%,认证性能不佳。

图 3a) 是 SVM 参数选择优化后训练集的鉴权情况,图 3b) 是 SVM 参数选择优化后基于训练集的参数选择结果与认证准确率,从图中可以看出参数选择优化后安全接入认证模型基于训练集没有样本出现错误判定,漏警率 0.0%。

图 3c) 是 SVM 参数选择优化后测试集的鉴权情况,从图中可以看出 IDE 算法的安全接入认证模型预测结果与现实数据全都一致,收获的认可精准率可达 100%。

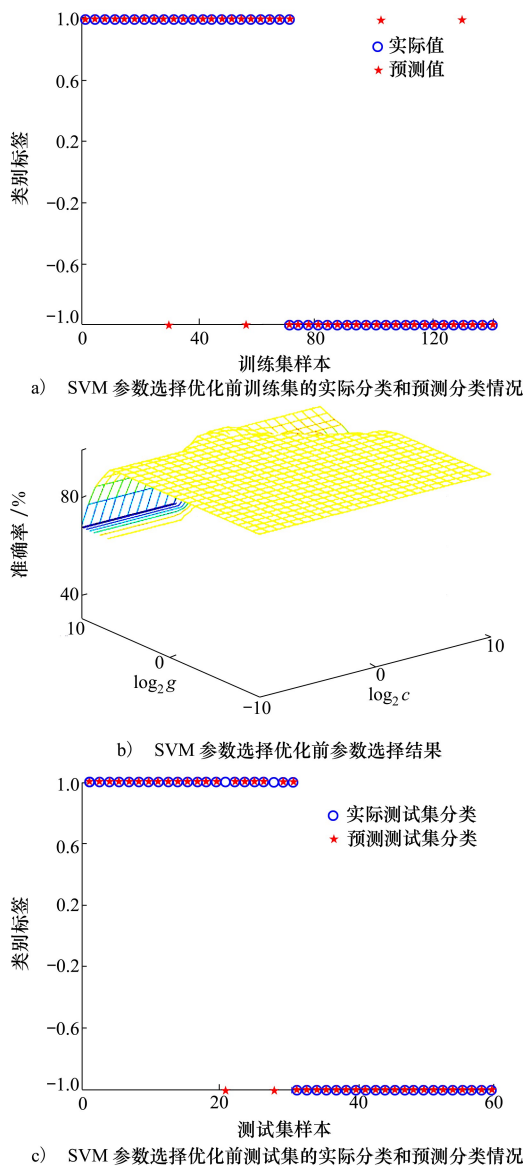


图 2 参数选择优化前实验结果图

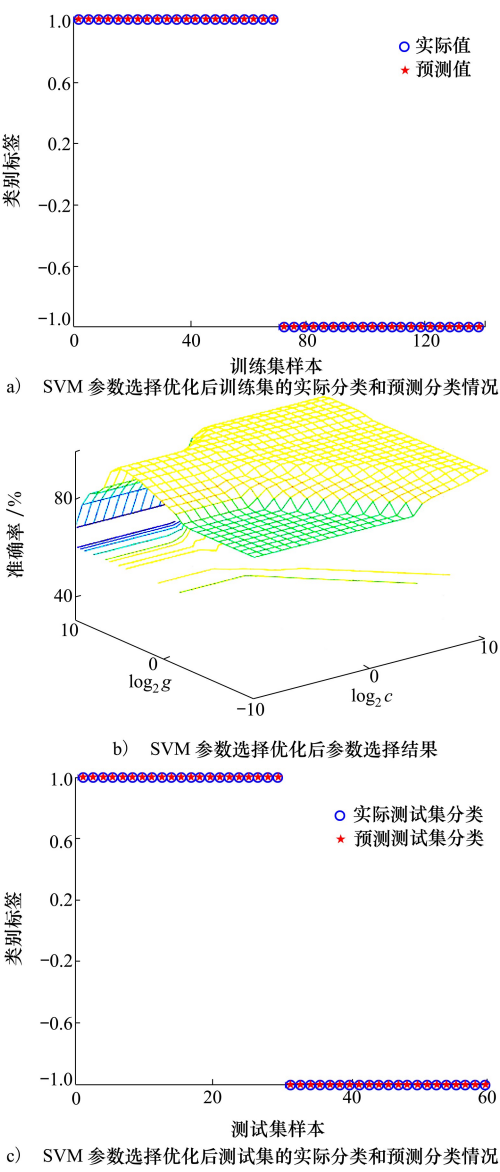


图 3 参数优化后实验结果图

3 结 论

本文主要研究了一种基于物联网物理层信息安全中的应用认证的 IDE-SVM 方案,这种方案直接利用了通信过程中的信道物理层信息进行安全接入鉴权,避免了使用复杂的通信上层协议进行加密解密

参考文献:

[1] ISHAQ M, AFZAL M H, TAHIR S, et al. A compact study of recent trends of challenges and opportunities in integrating inter-

和身份认证,降低系统资源的开销和针对上层协议的接入认证攻击,为无线通信终端安全接入问题提供了一种新的解决方案。IDE-SVM 算法为参数寻优问题提供了一种新的参数寻优方案,通过实验分析证明了此方案提高了算法分类精度和参数搜索的速度,进一步提高了无线终端鉴权的准确性。

- net of things(IOT) and cloud computing[C]//2021 International Conference on Computing, Electronic and Electrical Engineering, 2021: 1-4
- [2] CHEN Z, LI J, LI J, et al. GNSS multiparameter spoofing detection method based on support vector machine[J]. IEEE Sensors Journal, 2022, 22(18): 17864-17874
- [3] LIU Y, ZHANG P, LI X. Physical layer authentication using mmwave channel state information[C]//2021 International Conference on Networking and Network Applications, 2021: 30-33
- [4] AFEF L, FURQAN H M, ARSLAN H. Physical layer authentication scheme in beamspace MIMO systems[J]. IEEE Communications Letters, 2022, 26(7): 1484-1488
- [5] FODOR G, PARKVALL S, SORRENTINO S, et al. Device-to-device communications for national security and public safety[J]. IEEE Access, 2014, 2: 1510-1520
- [6] VAPNIK V N. An overview of statistical learning theory[J]. IEEE Trans on Neural Networks, 1999, 10(5): 988-999
- [7] KAZEMI A, BOOSTANI R, ODEH M, et al. Two-layer SVM, towards deep statistical learning[C]//2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence, 2022: 1-6
- [8] YIN T, LI Y, FAN J, et al. A novel gated recurrent unit network based on svm and moth-flame optimization algorithm for behavior decision-making of autonomous vehicles[J]. IEEE Access, 2021, 9: 20410-20422
- [9] GASCÓN-MORENO J, SALCEDO-SANZ S, ORTIZ-GARCÍA E G, et al. A binary-encoded tabu-list genetic algorithm for fast support vector regression hyper-parameters tuning[C]//Proceedings of the 2011 11th International Conference on Intelligent Systems Design and Applications, 2011: 1253-1257
- [10] CHEN C, XU X, WANG G, et al. Network intrusion detection model based on neural network feature extraction and PSO-SVM[C]//2022 7th International Conference on Intelligent Computing and Signal Processing, 2022: 1462-1465
- [11] WANG Z, JIANG Y, HU X, et al. A leaf type recognition algorithm based on SVM optimized by improved grid search method[C]//2020 5th International Conference on Electromechanical Control Technology and Transportation, 2020: 312-316
- [12] LI J, DING L, XING Y. Differential evolution based parameters selection for support vector machine[C]//2013 Ninth International Conference on Computational Intelligence and Security, 2013: 284-288
- [13] CHENG Y, LIU Z. Passive oppositional differential evolution for global optimization[C]//2019 11th International Conference on Intelligent Human-Machine Systems and Cybernetics, 2019: 323-327
- [14] WANG P, YAN Z, ZENG K. Bcauth: physical layer enhanced authentication and attack tracing for backscatter communications[J]. IEEE Trans on Information Forensics and Security, 2022, 17: 2818-2834
- [15] DAI C, YANG J, QIN Y, et al. Physical layer authentication algorithm based on SVM[C]//2016 2nd IEEE International Conference on Computer and Communications, 2016: 1597-1601

IDE-SVM algorithm and it's usage in physical layer security method for IoT

WANG Qiang¹, ZHU Chenming¹, PAN Su², QIN Yuxi²

(1.China Information Consulting and Designing Institute Co.,Ltd., Nanjing 210019, China;
2.Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: To address the problem that there is no standard for the parameter selection of support vector machine (SVM) algorithm, a parameter optimization selection method based on the integrated improved differential evolution (IDE) algorithm is proposed, which uses the minimization of the classification error rate as the optimization criterion and the improved differential evolution algorithm to optimize the combination of SVM parameters to obtain an SVM algorithm with higher classification accuracy. At the same time, to avoid the basic DE algorithm from falling into local optimum when solving the SVM parameter selection problem and to improve the search efficiency of the DE algorithm. In this paper, an improved differential evolutionary algorithm is proposed to obtain a DE algorithm

with faster convergence and higher accuracy by using the circular arc function for adaptive control of the variance scaling factor F and the crossover probability factor R , combining with the random newborn individual replacement operation. Based on this, an IDE-SVM IoT physical layer security method based on IDE-SVM is proposed. The experimental results show that the authentication accuracy of the physical layer security method based on the improved SVM algorithm is higher than others.

Keywords: physical layer security; support vector machine; differential evolution; parameter optimization

引用格式:王强, 朱晨鸣, 潘甦, 等. IDE-SVM 算法及其在物联网物理层安全中的应用[J]. 西北工业大学学报, 2024, 42(5): 882-890
WANG Qiang, ZHU Chenming, PAN Su, et al. IDE-SVM algorithm and it's usage in Physical layer security method for IoT[J]. Journal of Northwestern Polytechnical University, 2024, 42(5): 882-890 (in Chinese)

© 2024 Journal of Northwestern Polytechnical University.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

简讯

学校第十四次党代会精神宣讲工作正式启动

(转自西工大新闻网 发布时间:2024 年 10 月 25 日 文字:郭青)

10 月 23 日下午,学校召开第十四次党代会精神宣讲工作启动会暨党的创新理论宣传宣讲工作研讨会。各基层党委(党总支)相关工作负责同志,教职工宣讲团、马克思主义学院教师宣讲团、工大青年宣讲团、“五老”宣讲团主要成员代表等 60 余人参加会议。会议由党委宣传部副部长王丽主持。

党委宣传部常务副部长张富利就学校第十四次党代会精神宣讲作首场报告。张富利强调,认真做好学校第十四次党代会精神的宣贯工作,是进一步学深悟透党的二十届三中全会和全国教育大会精神,推动党中央重大决策部署落实落地的重要举措。围绕党的二十届三中全会、全国教育大会对高校提出的新要求新任务,聚焦学校第十四次党代会确定的“天下工大、世界三航”远景目标、新“三步走”战略构想,张富利进行了系统解构和重点解读。

结合以往对党的创新理论宣讲工作开展实际,校团委刘辰一、马克思主义学院姚崇、离退休老同志黄迪民、光电与智能研究院訾方、外国语学院张桑桑、教育实验学院范翔、机关党委王强分别围绕进一步做好党代会精神宣贯和理论宣讲工作作交流发言,提出建议。大家一致认为,要先学一步、学深一层,以学促讲,以党的创新理论夯实宣讲基础;要丰富宣讲手段,探索线上线下相结合、多单位联学联讲的多样化方式,为师生打造沉浸式、互动式、体验式学习宣讲阵地;要提高宣讲的专业化、时代化水平,准确把握学校建设目标和发展战略,加强政策解读,及时回应师生关切,以身边人、身边事等鲜活案例,教育引导师生,激发师生斗志,推动学校第十四次党代会精神开花结果。

张富利就做好学校第十四次党代会精神宣讲工作提出三点建议。一是要坚持“只有做好了才算做了”的工作作风,以高度的责任感和使命感做好理论宣讲工作,提高宣讲标准,强化宣讲质量。二是要把宣讲和党中央要求、单位具体结合起来,讲清楚“天下工大、世界三航”的核心内涵、学校发展面临的挑战机遇和新“三步走”战略构想等重要内容,增强宣讲的针对性和有效性。三是要坚持目标导向,按照全校师生全覆盖的要求,加强组织领导,强化工作统筹,建强宣讲队伍,推动以学促干,让全校师生真正听得懂、记得住、用得上,以饱满高涨的精气神推进中国特色世界一流大学建设。