基于改进支持向量机的无线通信网络安全漏洞智能预警方法

田恬恬[1]，朱倩倩[2]
（1.郑州科技学院 大数据与人工智能学院，河南 郑州 450064；
2.郑州科技学院 信息工程学院，河南 郑州 450064）

摘要：交互信息在经过空口传输时容易受到各类攻击，为此，研究基于改进支持向量机的无线通信网络安全漏洞智能预警方法。以扫描调度作为漏洞的关键，按照四个部分设定漏洞信息搜索方式。针对任务形式部署并划分区域，对无线通信网络漏洞攻击目标进行捕获。采用二叉树中的最短距离算法，对支持向量机进行改进，实现无线通信网络的安全漏洞攻击智能预警。实验结果表明，文章方法可以在 3s 内实现不同漏洞类型的识别，可以在漏洞发起攻击前完成预警。

关键词：无线通信网络；支持向量机；二叉树；漏洞智能预警
中图分类号：TP6369.6　　**文献标识码：**A　　**文章编号：**2096-9759(2023)06-0076-03

0 引言

当今为信息网络时代，人们对信息的发布和获取很大程度上依赖于网络，尤其在交流和共享信息时需要通过移动通信技术，而随着人们对智能机的应用，越来越多的信息被盗取和查看，造成严重的信息损失，也产生严重的网络安全事件。探究网络运行安全的根源主要是黑客通过网络漏洞进行攻击，产生不同的网络攻击事件[1]。漏洞是计算机系统在通信协议或是硬件和软件中存在的不足和缺陷，非法用户可以通过漏洞获取额外权限，为此，需要设计一个漏洞检测和预警方法。漏洞本身是一个多分类的问题，与支持向量机的设计理念较为相似，从历史的大量计算机漏洞中发现其形成的作用机制，支持向量机可以通过已有的规律对信息进行分类，但目前对其在漏洞分类和检测中的研究不是很多。本文以此为基础选择该技术进行设计，为无线通信网络的安全漏洞预警提供理论支持。

1 扫描调度下搜索无线通信网络安全漏洞信息

扫描调度作为预警的关键环节[2]，在整个预警过程中非常重要，根据扫描调度的结果对无线通信网络中的漏洞信息进行搜索，具体流程如图 1 所示。

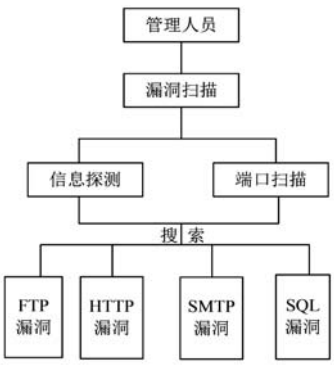

图 1 漏洞搜索示例

根据图中内容所示，在扫描调度下完成漏洞搜索共分为 4 个部分，分别为 FTP 漏洞搜索、HTTP 漏洞搜索、SQL 漏洞搜索、SMTP 漏洞搜索[3]。该过程主要通过网络管理人员总结无线通信网络中的漏洞，在开始工作时能够同时对上述部分完成搜索操作，也可以逐一完成搜索操作[4]。在扫描调度功能下对漏洞进行搜索，能够逐一发现无线通信网络中的漏洞问题，因此需要分别对每个部分的搜索方式和内容进行定义。

2 区域部署理论确定无线通信网络漏洞攻击目标

从获取到的漏洞信息中对服务网络中的通信协议进行分析，在终端处于运行状态时对不同区域进行任务部署，根据不同的漏洞攻击情况对应检测范围，以此确定无线通信网络中漏洞的主要攻击目标。在攻击位置获取方案中需要明确无线通信网络的终端手机号码所在的区域，为后续的目标标记作出铺垫[5]。

此次采用默认发送的方式监听无线通信网络中的传输信息，在不同的跟踪区域内部署伪装捕获信号，对漏洞的攻击目标终端是否在划定区域进行判断，不同的运营商对应的手机号段如表 1 所示。

表 1 不同运营商对应的手机号段

运营商	手机号段
中国联通	130、131、132、145、155、156、166、171、175、176、185、186
中国移动	134、135、136、137、138、139、147、150、151、152、157、158、159、172、178、182、183、184、187、188、198
中国电信	133、149、153、173、177、180、181、189、191、199
其它号段	14 号段为上网卡专属号码 如联通为 145、移动为 147

根据表中内容所示对漏洞攻击的具体目标进行确定，主要通过对手机号的运营商基站频率监听，在通常情况下终端会在无操作时段内处于空闲状态[6]。根据不同的明文传输形式，对漏洞的捕获提供基础。在无线通信网络进入空闲状态时，以非连续性寻呼通道进行监听确定攻击位置，计算方式如下：

$$[SFD]MOD[Q]=([Q]DIV[W])\times([ER-RT]MOD[W]) \quad (1)$$

$$Y-U=FLOOR\left(\frac{[ER-RT]}{[W]\times[W_P]}\right)MOD[W_P] \quad (2)$$

收稿日期：2023-01-29
基金项目：基金课题：1.郑州科技学院科技攻关项目“基于 KIII 的嗅觉神经系统仿生模型构建及仿生程度评估”（2022XJKY06）；2.郑州市社科联调研课题“推动郑州市有色金属工业数字化与智能化转型研究”（ZSLX20220989）。
作者简介：田恬恬（1995-），女，河南洛阳人，硕士，助教，研究方向：人工智能。

公式中："*MOD*"表示取模。"*DIV*"表示除法。"*FLOOR*"表示逐一向下取整过程。[*Q*]表示终端的运行周期。[*W*]表示在总寻呼中的帧数，表示为[*Q*]=min([*Q*],[*AS*]，其中 [*AS*]表示寻呼密度，由无线通信网络中的传输消息确定，一般取值为 $[AS]\in\left\{4Q,2Q,\ Q,\frac{Q}{2},\frac{Q}{4},\frac{Q}{8},\frac{Q}{16},\frac{Q}{32}\right\}$。而[*WP*]与 [*W*]为相对位置，表示为 $[W_P]=\max\left(1,\frac{[W_P]}{[Q]}\right)$。[*ER-RT*] 表示身份标识。在不同的模式下确定漏洞攻击位置与参数 *Y-U* 相关，以 FDD 和 TDD 两种模式进行取值，具体如表 2 所示。

表 2 不同模式下参数取值

$[W_P]$	1	2	4
Y-U = 0	0	0	0
Y-U = 1	9	9	9
Y-U = 2	5	9	9
Y-U = 3	1	5	9
Y-U = 4	9	4	0
Y-U =5	9	9	9
Y-U = 6	0	4	5

根据表中内容所示在不同的参数取值范围中，针对终端周期和基站中的传输相对位置获取运行周期，在一个周期内通过监听寻呼帧数和密度，查看是否在无线通信网络中存在干扰，从而判断终端中是否存在漏洞攻击。在获得寻呼数据后，若该寻呼记录能够匹配到属于自己的终端则能够建立新的连接，若未找到匹配记录则认定为漏洞代码，可以进行捕获。

3 基于改进支持向量机智能预警安全漏洞攻击

本文将二叉树算法与支持向量机进行融合，对支持向量机计算方式进行改进，以此实现无线通信网络中安全漏洞的预警。上文中对网络终端的漏洞进行捕获和标记，将获取到的漏洞按照二维线性方式进行划分，设置 *D* 表示为漏洞与正常传输数据的分类线，其中 D_1 和 D_2 分别表示两组样本中离分类线最近的点形成的直线，此时漏洞和正常传输数据可以形成一个最优的分类面，具体情况如图 2 所示。

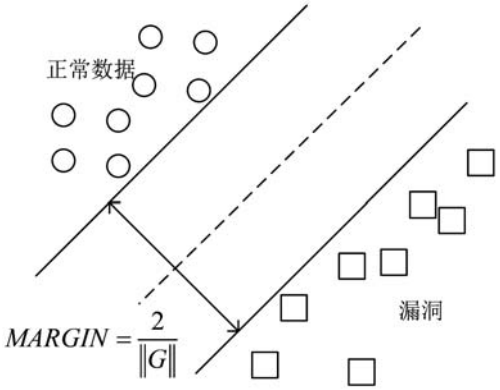

图 2 支持向量机下最优分类示意图

根据图中内容所示，*MARGIN* 表示分类间隔，在归一化处理后为 $MARGIN=\frac{2}{\|G\|}$，其中 *G* 表示置信参数。按照最优分类线将两个类型数据无错误地分开，保证分类过程中空隙最大化，设置漏洞的线性可分样本为（H_K，J_K），其中 *K*=1，2，…，*L* 表示漏洞量，则分类后的漏洞所在面方程如下：

$$G\times H_K+Z=J_K \tag{3}$$

公式中：*Z* 表示样本的判断函数。此时 J_K 表示类标号，取值范围为{+1，-1}。在支持向量机中要想做大化间隔空隙需要使||G|| 最小，才能实现漏洞样本的正确分类，因此满足条件后且使||G|| 最小即为支持向量机的最优分类面。

由于支持向量机只能提供维数内的漏洞分类，因此以二叉树算法改进支持向量机，以二叉树中最短距离法设定支持向量机的漏洞预警流程：

$$V_{N,M}=\min\left\{\left\|H_K-H_L\right\|\middle|H_K\in V_N,H_L\in V_M\right\} \tag{4}$$

式中：V_N、V_M 分别表示划分的两个子类。两组类别中最近的样本向量的欧式距离为 $V_{N,M}$。一般情况下对于预警过程首先计算类之间的距离，其次对于每个类会存在与其它类的距离值，分别将各自的距离进行排序并编号，最后根据从大到小的顺序生成二叉树，距离顶端最近的类即为漏洞所在位置，对其进行标记并完成预警。

4 实验测试分析

为验证设计方法能够在无线通信网络安全中实现漏洞预警，采用对比测试的方法进行论证。分别采用基于神经网络的预警方法和基于层次分析的预警方法作为测试对照组，分别与本文方法进行比较，验证不同方法的预警效果。整个实验测试通过 MATLAB 测试平台完成，在设计无线通信网络结构的基础上，分别选择不同的网络安全漏洞形式，连接选择的三组预警方法，实现不同预警方法应用的有效性测定。

为保证实验测试的准确性和真实性，此次测试按照实际无线通信网络中存在的安全漏洞作为测试对象，分别对不同类型的网络安全漏洞进行识别。只有在较短的时间内发现网络安全漏洞，并对其攻击类型和数量进行准确统计，才能够在其发起攻击前作出预警。本文共选择 16 种安全漏洞作为测试对象，对其名称和数量进行统计，具体情况如表 3 所示。

表 3 无线通信网络安全漏洞名称以及数量（个）

名称	数量	名称	数量
SES	4	XSS	2
COOLIE	6	DDOS	10
TOKEN	10	PROXY	12
XMLHIY	2	TZF.52	6
T.2ZFDF	4	SCTIOP	8

根据表中内容所示，在选择的不同漏洞中每一组包含的数量最多不超过 5 组，说明在每一种类型下均可以在少量的数量下实现网络攻击，对无线通信网络造成影响。而安全漏洞越少其攻击时间越短，其自带的攻击性就越大，因此需要快速且准确地对其进行识别，分别将上述情况上传到测试平台中，分别连接三组测试方法完成漏洞识别，具体结果如图 3 所示。由图 3 可知，在基于神经网络的预警方法的应用下基本上可以完成各组漏洞的组数识别，仅在"TOKEN"漏洞和"PROXY"漏洞中缺少 1 组。在基于层次分析的预警方法中虽然可以完成识别，但基本都存在数量丢失的情况，在实际应用中也会影响无线通信网络的运行。而本文方法可以实现全部漏洞的识别，且对每一组漏洞的识别结果也与表 1 中数据相

基于遗传算法的通信电缆敷设优化方法研究

杨宝金[1]，赵子彦[2]
（1.江苏红峰电缆集团有限公司，江苏 宜兴 214251；2.战略支援部队，江苏 南京 210000）

摘要：常规通信电缆敷设优化方法主要依托于改进蚁群算法，该方法易受到相关约束规则下单值性条件的影响，导致电缆敷设方案对应的载流量较小。为此，文章提出基于遗传算法的通信电缆敷设优化方法研究。利用有限元法和傅里叶变换原理计算电缆温度场，通过分析导体热平衡原理求取相关约束规则下的单值性条件，并结合温度场值建立电缆敷设模型，引入遗传算法，求解模型，获得最优敷设方案。对比实验结果表明，所提电缆敷设优化方法的载流量更大，其最低值达到了 2605A，具备了更高的应用价值。

关键词：遗传算法；通信电缆；电缆敷设；优化方法
中图分类号：TM621.7　　**文献标识码：**A　　**文章编号：**2096-9759(2023)06-0078-03

0 引言

在通信电缆[1]敷设工程中，电缆的敷设方式对通信效率起到至关重要的作用，电缆敷设经济合理性原则要求电缆的敷设路径要求最短、电缆载流量最大，但是现阶段的电缆敷设效果较差，导致电缆载流量较小。针对该问，许多学者进行了研究。文献[2]通过利用基于三维数字化技术对电缆敷设起点到终点进行单源路径扩展，以最短路径为优化目标，采用临时标号的方式，求得电缆敷设最优方案；文献[3]利用GIM模块化方法进行电缆敷设优化方法的研究，采用三维协同技术设计电缆模型，在搜索敷设规划路径中形成连通格栅化的固定布线路径，实现电缆管道敷设。但以上两种方法在敷设路径最小时电缆载流量较小。为了解决上述方法存在的问题，本文主要针对通信电缆敷设优化方法进行设计，并使用遗传算法解决电缆敷设问题，求解在相关规则约束下的最优敷设方案。

1 通信电缆敷设优化方法设计

1.1 通信电缆温度场的计算

研究电缆敷设方案进行优化方法时[4]，首先需要确定地下通信电缆[5]温度场值。在计算过程中，采用有限元法计算通信电缆温度场。利用有限元法对电缆温度场进行求取时，需要设立电缆导热微分方程和单值条件。依据傅里叶变换原理，可得到电缆敷设区域中含有同性质热源的导热微分方程式为：

$$r\frac{\partial t}{\partial \tau}=\nabla g\left(\lambda d_2\right)+d_3 \tag{1}$$

上式中，r 表示电缆直径；∇g表示导温系数；$\frac{\partial t}{\partial \tau}$表示微分偏

收稿日期：2023-01-13

作者简介：杨宝金（1969-）男，EMBA，高级电气工程师，副总兼技术总监，研究方向：电线电缆制造与研发领域；赵子彦（1991-），男，江西南昌人，本科学历，助理工程师，研究方向：有线通信（光端、线路及应用管理）。

一致，综合上述情况说明本文方法更加有效。

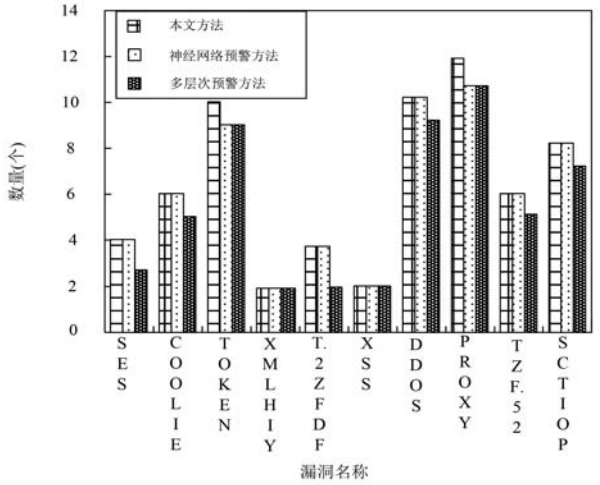

图 3 不同方法下安全漏洞识别结果

5 结语

本次设计方法根据无线通信网络的架构形式，以漏洞形成的机制提出一种智能预警方法，在改进支持向量机的作用下对漏洞进行简单防御，并在实验论证的基础上证明其实用性，取得的成果对无线通信网络的安全运行具有重要参考价值。但由于此次研究时间有限，在整个分析过程中仍存在少许不足之处，如对不同的漏洞预警没有进行数据的完整性保护，在产生攻击时可能会存在原始数据与攻击代码相融合的可能性，后续研究中针对中间攻击代码进行进一步的研究，为相关漏洞检查和预警提供相关依据。

参考文献：

[1] 袁磊,蒋刚,郝兴安,等.基于NARMAX模型的阀控非对称缸神经网络预测控制[J].液压与气动,2023,47(01):86-93.
[2] 张成虎,李鹏旭,王琪.网络金融犯罪预警系统研究——基于区块链和边缘计算[J].情报杂志,2023,42(01):59-65.
[3] 周杰,周润云,郭栋.基于CNN-PSO的电力供应链安全风险预警系统[J].自动化与仪器仪表,2022(12):190-195.
[4] 于烨,吴佳静,马国武,等.基于鲸鱼算法改进支持向量机的信息网络安全态势预测研究[J].微型电脑应用,2022,38(12):107-110.
[5] 陈庆超,韩松,毛钧毅.采用多层次特征融合SPP-net的暂态稳定多任务预测[J].控制与决策,2022,37(05):1279-1288.
[6] 赵巍,张智森,肖佳康,等.基于人工智能的5G通信网络运维规划方法[J].长江信息通信,2022,35(03):219-222.