文章编号:1671-4598(2022)10-0051-06 DOI:10.16526/j.cnki.11—4762/tp.2022.10.009 中图分类号:TP391 文献标识码:A

基于蚁群算法的无线通信网络安全漏洞检测方法

李 梅，朱明宇
（苏州高博软件技术职业学院 信息与软件学院，江苏 苏州 215163）

摘要：针对无线通信网络存在因漏洞数据大量累积，而造成通信网络运行速率下降的问题，提出基于蚁群算法的无线通信网络安全漏洞检测方法；根据最大、最小蚂蚁系统定义原则，采用蚁群算法，建立完整的数学模型表达式；结合网络爬虫技术，将待测数据载荷单元整理成既定组合形式，遵循绕过规则，提取待测安全漏洞数据；分析SQL注释语句与URL编码条件，设置动态化查询指令，选取其中表现为空的信息字节，建立信息剥离表达式，实现无线通信网络安全漏洞检测；实验结果表明，设计方法的漏洞信息检测量均值达到了4.37 Mb，该检测方法有效提高了检测量，解决了因漏洞数据大量累积而造成的通信网络运行速率下降的问题。

关键词：蚁群算法；无线通信网络；安全漏洞检测；爬虫技术；载荷单元；动态指令

Wireless Communication Network Security Vulnerability Detection Method Based on Ant Colony Algorithm

LI Mei，ZHU Mingyu
(Department of Information and Software Technology，Suzhou Gaobo Vocational College of Software Technology，Suzhou 215163，China)

Abstract：Aiming at the problem of the operation declining rate of wireless communication network due to the accumulation of vulnerability data，Wireless communication network security vulnerability detection method based on ant colony algorithm is proposed. According to the definition principle of maximum and minimum ant system，the complete mathematical model expression is established by ant colony algorithm. Combined with the web crawler technology，the load units of the data to be tested are sorted into the established combination form，and the security vulnerability data to be tested is extracted according to the bypass rules. The SQL annotation statement and URL coding conditions are analyzed，the dynamic query instructions are set，the empty information bytes are selected，the information stripping expression is established，and the wireless communication network security vulnerability detection is realized. The experimental results show that the average amount of vulnerability information detected by the designed method reaches up to 4.37Mb，which effectively improves the amount of detection and solves the problem of communication network operation declining rate caused by the massive accumulation of vulnerability data.

Keywords：ant colony algorithm；wireless communication network；security vulnerability detection；crawler technology；load cell；dynamic instruction

0 引言

蚁群算法是一类概率型执行算法的统称，可以用来寻找最优路径[1]，以便获得最准确的数值求取结果。从宏观角度来看，蚁群算法同时具有启发式搜索、数据信息正负反馈、分布式计算等多项应用特征，故而其本质上始终保留了启发式全局优化运算的能力。与其他优化算法相比，蚁群算法的执行遵循正反馈机制，可以在运算过程呈现不断收敛的约束状态，并最终使得所选取指标参量无限逼近最优解。在蚁群算法认知中，每一个独立个体节点均可以感知外界环境的变化情况，且随着外界环境的不断改变，个体与个体之间的通讯形式不断发生变化[2]。为避免冗余运算步骤的出现，蚁群算法对于数据信息参量主要采取分布式计算的处理方式，在进行局部搜索时，该方法依据启发式原则提取运算参量，不仅避免求取结果陷入局部最优情况，还在短时间内，得到准确的全局最优解计算结果。

无线通信是一种远距离传输通讯模式，在互联网环境中，节点与节点之间传输关系的构建依靠网络负载波段，不需借助导体、线缆等实体传输结构[3]。该传输通讯模式简单、快捷，但是安全漏洞是无线通信网络安全策略中存在的缺陷，在非限制情况下，攻击性信息参量可以经由安全漏洞进入无线通信网络内部。相关学者张杰研究了无线铜线网络安全漏洞检测方法，该方法应用了被动分簇算法，

收稿日期:2022-05-20； **修回日期**:2022-07-05。
基金项目:江苏省高等职业教育高水平专业群(苏教职函[2021]1号)；江苏省高等职业教育高水平骨干专业建设项目(苏教高[2017]17号)。
作者简介:李 梅(1981-)，女，江苏无锡人，硕士，讲师，主要从事计算机软件及计算机应用、通信传感网方向的研究。
引用格式:李 梅，朱明宇.基于蚁群算法的无线通信网络安全漏洞检测方法[J].计算机测量与控制，2022，30(10)：51-56，109.

根据模板匹配原则分类处理获取的无线通信网络安全漏洞节点，根据相似性参量之间的实值匹配关系，将待处理数据信息分别存储在既定数据库主机之中[4]。但是该方法在单位时间内处理的漏洞信息总量少，难以解决因漏洞数据大量累积而造成的通信网络运行速率下降的问题。为避免发生上述情况，提出了基于蚁群算法的无线通信网络安全漏洞检测方法，该方法引入蚁群算法原则，并以此为基础，设计一种新型的无线通信网络安全漏洞检测方法。以期提高检测安全漏洞的能力。

1 蚁群算法

蚁群算法的理论概述研究包含最大最小蚂蚁系统构建、数学模型设计两个执行步骤，本章节将针对上述内容展开研究。

1.1 最大最小蚂蚁系统

最大最小蚂蚁系统是蚁群算法的理论基础，对于待处理信息参量具有“趋同性”约束作用。“趋同性”原则是指：最大蚂蚁系统会约束待处理信息参量的最大取值结果，使实值水平不断趋近于中心值指标；最小蚂蚁系统会约束待处理信息参量的最小取值结果，使其实值水平也不断向着中心值指标趋近[5]。

公式（1）反映了完整的“趋同性”定义原则：

$$\Delta e=\begin{cases}\dfrac{w}{q_{\max}}, w\to w_{\max}\\ \dfrac{w}{q_{\min}}, w\to w_{\min}\end{cases} \tag{1}$$

式中，$q_{\max}$ 表示趋向性指标的最大值，$q_{\min}$ 表示趋向性指标的最小值，w 表示无线通信数据的实际取值结果，$w_{\max}$、$w_{\min}$ 分别表示无线通信数据的最大与最小取值结果。

在“趋同性”原则的基础上，定义最大最小蚂蚁系统，准确求取约束性指标参量的平均数值 $\bar{\omega}$。规定 w_1、w_2 表示两个随机选取的无线通信数据指标，且 $w_1\neq w_2\neq w_{\max}\neq w_{\min}$ 的不等式条件恒成立。

最大最小蚂蚁系统表达式为：

$$\psi=\frac{\sqrt{|w_1{}^2|-|w_2{}^2|}}{\bar{\omega}\cdot\Delta e} \tag{2}$$

由于最大最小蚂蚁系统表达式具有明显的两极性，因此，在求取“趋同性”原则时，应避免极值指标之间的物理差值过大。在稳定无线通信数据取值结果的同时，确保约束性指标参量均值始终处于数值集合的中间位置。

1.2 数学模型

在蚁群算法的认知中，蚂蚁在行进路径上留下的信息素总量直接决定了选取蚂蚁对象从一个节点到另一个节点的转移状态。对于无线通信网络而言，蚁群算法的定义概念可以转化为——选取数据参量在传输路径上留下的关联信息总量决定了数据参量从一个节点到另一个节点的转移状态[6-7]。因此，在处于 t 时，数据参量从一个节点 r_1 到另一个节点 r_2 的转移概率 p 可表示为：

$$p=\frac{\xi\cdot y_t}{\psi\times\sum_{\sigma=1}^{+\infty}|y_{r_1}-y_{r_2}|^2} \tag{3}$$

式中，ξ 表示蚁群算法认证向量，σ 表示关联信息提取系数，y_t 表示 t 时刻的无线通信数据参量，y_{r_1} 表示 r_1 节点处的无线通信数据参量，y_{r_2} 表示 r_2 节点处的无线通信数据参量。

蚁群算法数学模型以转移概率 p 为基础，估算了无线通信数据在网络体系内由一个节点转移到另一个节点的能力，在制定安全漏洞检测策略时，需要以该项物理指标作为核心参考条件。设 i_{r_1} 表示无线通信向量在 r_1 节点处的转移系数，i_{r_2} 表示无线通信向量在 r_2 节点处的转移系数，ζ 表示无线通信数据的转向传输度量值，Δo 表示蚁群算法在单位时间内标记的无线通信数据总量。

蚁群算法的数学模型表达式为：

$$i=\frac{1}{p}\cdot\frac{\sqrt{\zeta\cdot(i_{r_1}-i_{r_2})}}{|\Delta o|^2} \tag{4}$$

由于 i_{r_1} 系数、i_{r_2} 系数之间不具备明显的相关性，因此，在建立蚁群算法数学模型时，不考虑 r_1 节点、r_2 节点选取结果对无线通信向量取值造成的影响。

2 待测数据提取

2.1 爬虫相关技术

无线通信网络安全漏洞检测指令的制定需要爬虫技术的配合。网络爬虫技术可以按照既定规则抓取处于攻击状态的数据信息参量，并将抓取结果以程序脚步的形式，反馈给无线通信主机，并以此保障无线通信网络的绝对稳定性[8]。常见的无线通信网络安全漏洞检测爬虫包括 HTTP 状态码、Form 表单、深度去重 3 种组成形式，其具体应用能力如表 1 所示。

表 1 爬虫应用能力说明

编号	爬虫名称	应用能力
1	HTTP 状态码	将检测到的攻击性数据反馈回无线通信网络主机，根据爬虫机制的作用形式，完善数据信息查询指令
2	Form 表单	借用爬虫机制，建立无线通信网络节点与检测主机之间的连接关系，分别存储攻击性数据与常规通信数据
3	深度去重	整理无线通信网络中部分重复或完全重复的数据信息参量，利用爬虫机制去除处理该数据

为使爬虫机制能够更好地适应无线通信网络的连接形式，在设置检测节点时，需要严格遵循蚁群算法原则。

2.2 载荷单元生成与组合

载荷单元生成与组合是两个相互递进的执行环节，前者注重根据蚁群算法选取无线通信网络中安全漏洞数据的载荷单元参量，其可以区分攻击性数据与常规传输数据，从而缓解通信主机的检测压力[9]；后者注重重新排列选取安全漏洞数据载荷单元参量，一方面避免相邻载荷单元参

量之间出现明显的相互干扰，另一方面实现重新规划与处理爬虫节点。

设 s_1、s_2、…、s_n 表示 n 个不相等的无线通信网络安全漏洞数据载荷单元参量，f 表示基于蚁群算法原则的载荷单元筛选系数，τ 表示取值指标的初始值，ζ 表示无线通信网络主机对于安全漏洞数据的处理权限。

基于蚁群算法的无线通信网络安全漏洞数据载荷单元生成表达式为：

$$a=\frac{\sum_{\tau=1}^{+\infty} f\times(s_1+s_2+\cdots+s_n)}{i\times(\zeta^2-1)} \tag{5}$$

无线通信网络安全漏洞数据载荷单元的组合表达式为：

$$d=\vartheta\cdot\left[\frac{a}{\bar{\omega}^2}\right]\cdot\left(\frac{{g_1}^2}{{g_2}^2}\right) \tag{6}$$

式中，$\bar{\omega}$ 表示数据载荷度量值，ϑ 表示载荷排列系数，g_1、g_2 表示两个不相等的无线通信网络安全漏洞数据载荷单元特征值。载荷单元生成、载荷单元组合两个处理流程之间具有明显的顺承关系，因此，在检测无线通信网络安全漏洞时，两个实践步骤的执行需要同时遵循蚁群算法应用原则[10]。

2.3　绕过规则

通常攻击性无线通信数据编码安全漏洞载荷单元，从而指令文件绕过通信主机的检测，直接成功执行任务，因此在蚁群算法作用下，引入绕过规则，并按照该标准重新编码安全漏洞载荷单元，达到减少攻击性数据误报率的目的。根据安全漏洞载荷单元组成形式的不同，绕过规则的定义标准也会有所不同，也只有这样才能最大化保证无线通信网络主机的执行能力，使得安全漏洞节点能够得到准确检测[11-12]。在执行绕过规则时，应注重漏洞节点编码向量极值之间的数值配比关系。规定 $\boldsymbol{k}_{\max}$ 表示漏洞节点编码向量的极大值，$\boldsymbol{k}_{\min}$ 表示编码向量的极小值，在蚁群算法作用下，极限指标间的最小差值必须大于自然数“1”，但又不得大于平均编码向量 $\bar{\boldsymbol{k}}$（$\bar{\boldsymbol{k}}$ 表示向量 $\boldsymbol{k}_{\max}$ 与向量 $\boldsymbol{k}_{\min}$ 的平均值）。

基于蚁群算法的无线通信网络安全漏洞节点绕过编码规则表达式为：

$$h=d\cdot\left|\frac{\boldsymbol{k}_{\max}-\boldsymbol{k}_{\min}}{\bar{\boldsymbol{k}}^2}\right|^{\theta^2-1}_{\theta\neq 0} \tag{7}$$

式中，θ 表示攻击性传输数据的误报系数。在制定绕过规则时，为避免对无线通信网络安全漏洞节点的错误编码，同时考虑爬虫定义条件、载荷单元生成与组合标准。

3　无线通信网络的安全漏洞检测

3.1　SQL 注释语句

SQL 注释语句表明了无线通信网络安全漏洞节点对于传输数据的编码能力。在蚁群算法作用下，SQL 注释语句占据的存储空间越大，其执行指令的编码长度越长，即无线通信网络安全漏洞节点对于传输数据的编码能力强；反之，若 SQL 注释语句所占据的存储空间小，其执行指令的编码长度短，即无线通信网络安全漏洞节点对于传输数据的编码能力弱[13-14]。在无线通信网络中，SQL 注释条件最大化突出安全漏洞节点的编码特征，对于网络主机而言，在处理传输数据时，可以结合已知编码特征与数据信息参量，从而避免漏洞数据大量累积，实现大幅提升通信网络运行速率。设 j_1、j_2、…、j_n 表示 n 个不同的漏洞数据注释向量，在检测信息参量时，注释向量之间的编码处理始终保持相乘运算的关系。

$$l=\frac{\left[j_1\cdot j_2\cdot\cdots\cdot j_n\right]^2}{(n-1)\cdot h}{\left|\Delta j\right|}^2 \tag{8}$$

式中，Δj 表示漏洞数据注释指标在单位时间内的传输总量，且 $\Delta j\geqslant 1$ 的不等式条件恒成立。规定在执行 SQL 注释语句时，漏洞数据的传输顺序不发生改变，编码向量所处位置也只能由首位注释节点运动至末位注释节点。

3.2　URL 编码

URL 编码是一种多功能检测机制，无线通信网络主机根据安全漏洞节点的排列形式，选择合适的码源样本编码数据信息参量，但由于蚁群算法并不能适配所有数据样本编译格式，因此，符合无线通信网络安全漏洞检测需求的编码形式只有二进制、八进制两种类型，具体编码原理如图 1 所示[15]。

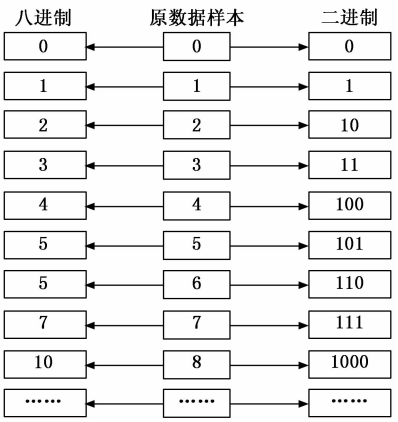

图 1　无线通信网络的 URL 编码原理

二进制、八进制是两种完全独立的 URL 编码形式——执行二进制 URL 编码指令时，漏洞信息的最小进位数值为“2”，最末位编码节点的定义数值为“2^0”，从最末位开始前向编码节点的定义数值依次为“2^1”、“2^2”、“2^3”，…，“2^n”，若当前节点处的实际数值为“1”，则该节点的实际编码结果为“1 乘以当前编码节点的定义数值”[16]。执行八进制 URL 编码指令时，漏洞信息的最小进位数值为“8”，最末位编码节点的定义数值为“8^0”，从最末位开始前向编码节点的定义数值依次为“8^1”、“8^2”、“8^3”，…，“8^n”，该节点的实际编码结果为“当前记录数值乘以当前编码节点的定义数值”。

3.3　动态查询指令

制定动态查询指令时，获取无线通信网络安全漏洞信息的实时存储量，并结合 SQL 注释语句与 URL 编码原则，

定义检测节点中数据信息参量的传输行为。从宏观角度来看，动态查询指令对于安全漏洞信息的处理注重同步性，要求节点参量与数据信息之间，需要保持同等级映射关系；从微观角度来看，动态查询指令不得脱离安全漏洞信息参量而独立存在，且前者对于后者能够起到明显的传输促进作用[17-18]。设 $\dot{b}$ 表示无线通信网络安全漏洞信息的动态特征，$\bar{V}$ 表示无线网络主机在单位时间内所能承担的漏洞数据传输量均值，ρ 表示漏洞数据参量的分布密度。联立上述物理量，可将基于蚁群算法的无线通信网络安全漏洞动态查询指令表达式定义为：

$$m = l \times \frac{\left(\rho \dfrac{\dot{b}}{|\bar{V}|}\right)}{\sum \mu \cdot (v_1^{\,2} - v_2^{\,2})} \tag{9}$$

式中，μ 表示已定义无线通信网络安全漏洞信息的实时查询系数，v_1、v_2 表示两个随机选取的查询指令编码向量，且 $v_1 \neq v_2$ 的不等式条件恒成立。规定动态查询指令的执行越密集，无线网络主机处理安全漏洞信息的能力越强，因此，在实施数据编码时，要求 $\dot{b}$ 指标、μ 指标的取值不能同时等于自然数“1”。

3.4 空字节

空字节是已存储无线通信网络安全漏洞信息中占编码向量为空的数据节点，在已知动态查询指令定义标准的情况下，空字节占存储空间越大，漏洞节点对于数据信息参量的承载能力越差，为获得准确检测结果，无线通信网络主机消耗的连接时间越长[19]。由于无线通信网络主机无法直接分离攻击性数据与常规传输数据，因此，在定义空字节时，需要漏洞节点时刻处于完全闭合的连接状态。设 ε 表示攻击性数据标记指征，α 表示常规传输数据标记指征，x_ε 表示基于系数 ε 的信息字节编码参量，x_α 表示基于系数 α 的信息字节编码参量。

无线通信网络安全漏洞待检信息的空字节定义表达式为：

$$z = \frac{\lambda \cdot X - m^2}{\sum [x_\varepsilon]^\varepsilon + [x_\alpha]^\alpha} \tag{10}$$

式中，λ 表示基于蚁群算法的待检信息定义系数，X 表示无线通信网络主机对于安全漏洞待检信息的实时承载条件。在定义空字节表达式时，将动态查询指令看作已知执行条件，若攻击性数据与常规传输数据之间不具备明显差异性，规定空字节定义点两端的信息样本需要分属于不同的数据库存储主机[20]。

3.5 信息剥离

信息剥离是指从混合数据文本中分离出攻击性数据，便于无线通信网络主机检测与处理数据。当空字节含量低于理想数值标准时，主机元件会按照蚁群算法剥离混合数据文本中的明显特征参量，并将这些数据信息暂时存储于数据库主机。对于剩余漏洞信息特征参量而言，由于已剥离文本满足的字符定义式不完全相同，所以在建立信息剥离表达式时，应考虑混合数据文本与攻击性数据信息参量之间的实值配比关系[21-22]。设 δ 表示漏洞信息样本混合系数的初始值，ΔU 表示攻击性数据信息的单位提取总量，$\vec{\boldsymbol{D}}$ 表示漏洞信息样本的检测译码向量，$\tilde{I}$ 表示攻击性数据的剥离特征。

无线通信网络安全漏洞检测方法的信息剥离表达式为：

$$c = \sum_{\delta=1}^{+\infty} z \cdot \Delta U \cdot \left| \frac{(\tilde{I})}{\vec{\boldsymbol{D}}} \right| \tag{11}$$

在蚁群算法作用下，控制空字节指标的实际取值，使其在执行信息剥离指令时，起到促进性的作用。

4 实例分析

4.1 实验方案

在无线通信网络环境中，主机元件在单位时间内检测的漏洞信息总量可以反映当前应用方法的实际检测能力。主机元件在单位时间内检测的漏洞信息总量越多，漏洞数据的实时累积量越小，此时通信网络的运行速率较快，当前应用方法的实际检测能力越强；反之，若主机元件在单位时间内检测的漏洞信息总量少，漏洞数据的实时累积量大，此时通信网络的运行速率慢，当前应用方法的实际检测能力弱。采用对比分析实验的方式验证设计方法的有效性和可行性，具体实验执行流程如下：

步骤一：选择客户端 PC 主机作为实验对象，将其接入无线局域网通信环境之中；

步骤二：选择基于蚁群算法的无线通信网络安全漏洞检测方法作为实验组应用方法；

步骤三：选择传统被动分簇算法作为对照组应用方法；

步骤四：设计实验场景，实验均在该场景下完成验证。

步骤五：说明实验设备和实验参数。

步骤六：按照图 2 所示的流程，记录实验组、对照组的实验数值；

步骤七：对比实验组、对照组记录数值，总结实验规律。

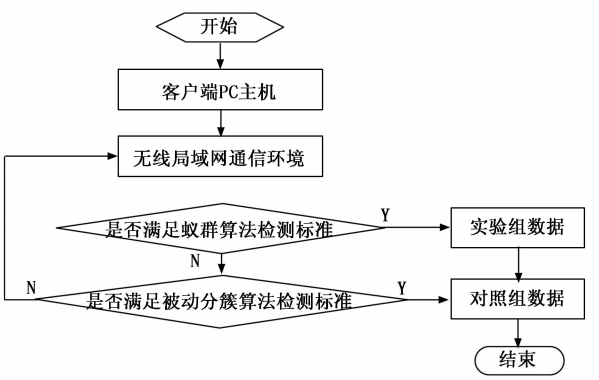

图 2 实验数据处理流程

4.2 实验场景与参数

实验在检测漏洞信息量的基础上，还涉及检测安全漏洞的成功率，基于此，构建无线通信网络安全漏洞实验场景，如图 3 所示。

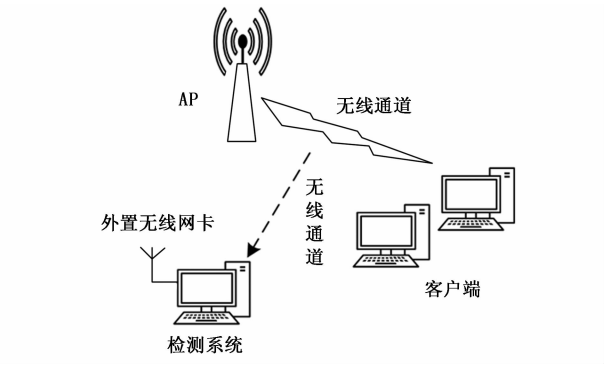

图 3　无线通信网络安全漏洞场景

根据图 3 构建无线通信网络安全漏洞场景，该场景涉及了路由器、电脑等，具体实验设备如表 2 所示。

表 2　实验设备

序号	名称	数量
1	无线路由器	1 台
3	检测 PC	1 台
4	客户端 PC	2 台
5	USB 无线网卡	2 个

表 2 中的 2 个 USB 无线网卡，一个用于检测 PC，另一个用于第三方检测 PC。PC 机均为 IPASON 的 B3060，CPU 为英特尔酷睿 i5，显存容量为 5GB。同时，客户端 PC 采用安全漏洞数据集，该数据集是对 NVD、Secunia、SecurityFocus、CNVD、CNND、NSFocus 漏洞平台的数据进行采集和整理而成。数据集共包括 6 个数据文件，分别为：NVD1.zip， Secunia2.zip、 SecurityFocus3.zip、 CNVD4.zip、CNND5.zip、NSFocus6.zip，即 6 大类安全漏洞。完成上述设计后，设计实验初始参数，具体参数如表 3 所示。

表 3　实验参数

序号	名称	参数
1	漏洞数据载荷单元参量	256
2	漏洞信息样本混合系数的初始值	$1\sim+\infty$
3	漏洞信息的最小进位数值	2
4	编码节点的定义数值	“2^1”、“2^2”、“2^3”,…,“2^n”
5	安全漏洞类型数	6

在实验过程中，漏洞数据注释指标在单位时间内的传输总量大于等于 1，并且在执行 SQL 注释语句时，漏洞数据的传输顺序不发生改变，编码向量所处位置也只能由首位注释节点运动至末位注释节点。

4.3　性能分析

按照上述流程验证设计方法的有效性和可行性，首先以无线通信网络的漏洞信息检测量为性能指标，该指标可以反映检测方法的检测工作量，该值越高，表明检测方法的性能越好。表 4～6 记录了实验组、对照组漏洞信息检测量的实验数值（相邻记录节点之间的间隔时长为 10 min）。

表 4　第一实验阶段实验数值

记录节点	漏洞信息检测量/Mb	
	实验组	对照组
1	3.2	3.1
	3.4	3.2
	3.5	3.4
	3.6	3.5
2	3.8	3.7
	3.8	3.8
	3.9	3.8
	4.1	4.0

表 5　第二实验阶段实验数值

记录节点	漏洞信息检测量/Mb	
	实验组	对照组
3	4.3	4.1
	4.3	4.1
	4.4	4.1
	4.3	4.1
4	4.5	4.3
	4.4	4.1
	4.5	4.2
	4.3	4.3

表 6　第三实验阶段实验数值

记录节点	漏洞信息检测量/Mb	
	实验组	对照组
5	4.5	4.1
	4.5	4.0
	4.5	3.8
	4.4	3.7
6	4.3	3.6
	4.2	3.6
	4.1	3.4
	4.0	3.2

根据表 4～6 的数据可知，实验组：在第一实验阶段中，实验组漏洞信息检测量呈现出不断增大的数值变化状态，其初始值 3.2 Mb 与最终实验数值 4.1 Mb 相比，上升了 0.9 Mb；在第二实验阶段中，实验组漏洞信息检测量的数值变化趋势则相对较为稳定，其初始值 4.3 Mb 与最终实验数值 4.3 Mb 完全相等；在第三实验阶段中，实验组漏洞信息检测量保持先稳定、再持续下降的数值变化状态，其初始值 4.5 Mb 与最终实验数值 4.0 Mb 相比，下降了 0.5 Mb。

对照组：在第一实验阶段中，对照组漏洞信息检测量保持连续上升的数值变化状态，其初始值 3.1 Mb 与最终实验数值 4.0 Mb 相比，上升了 0.9 Mb，与实验组上升幅度相同；在第二实验阶段中，对照组漏洞信息检测量也呈现出相对稳定的数值变化状态，其初始值 4.1 Mb 与最终实验数值 4.3 Mb 相比，上升了 0.2 Mb；在第三实验阶段中，对照组漏洞信息检测量也呈现出不断下降的数值变化状态，

其初始值 4.1 Mb 与最终实验数值 3.2 Mb 相比，下降了 0.9 Mb，下降幅度明显大于实验组。

分别选取第一实验阶段、第二实验阶段、第三实验阶段的极限数值，对实验组、对照组实验均值进行计算。分析数值计算结果可知，实验组漏洞信息检测量均值等于 4.37 Mb，对照组漏洞信息检测量均值等于 4.13 Mb，明显低于实验组均值水平。

综上可知，在蚁群算法作用下，主机元件在单位时间内检测的漏洞信息总量出现了明显增大的变化状态，该情况表示在这种检测方法的影响下，漏洞数据的实时累积量得到了控制，通信网络的运行速率快，即该方法的实际检测能力强，更符合实际应用需求。

由于无线通信网络安全漏洞的存在，攻击行为可以通过安全漏洞攻击客户端，从而发生丢失数据、隐私信息泄露等情况，发证该情的一个主要原因是安全漏洞的类型较多，导致检测难度高，因此，以不同类型的安全漏洞检测成功率反映安全漏洞检测性能，该指标值越高，表明设计方法的检测性能越好。实验采用安全漏洞数据集中的 6 大类数据，随机选择每类安全漏洞数量 200 条。应用实验组和对照组方法检测安全漏洞，实验具体结果如表 7 所示。

表 7 不同类型安全漏洞检测成功率

类型	检测成功率/%	
	实验组	对照组
NVD1	99.7	91.3
Secunia2	99.8	92.9
SecurityFocus3	99.7	90.8
CNVD4	99.5	91.7
CNND5	99.9	92.6
NSFocus6	99.8	91.1
均值	99.7	91.7

根据表 7 数据可知，实验组不同类型的安全漏洞检测成功率均在 99.5%以上，其中 CNND5 类型的检测成功率达到了 99.9，平均检测成功率达到了 99.7%，对照组的检测成功率均值达到了 91.7%，其中 Secunia2 类型的安全漏洞检测成功率最高，其值为 92.9%，SecurityFocus3 类型检测成功率最低，该值为 90.8%。两种方法相比可知，实验组的不同类型检测成功率提高了 8.0%，因此，蚁群算法的无线通信网络安全漏洞检测方法有效检测出不同类型的安全漏洞，提高了检测成功率。

5 结束语

为了提高无线通信网络安全漏洞检测能力，研究了基于蚁群算法的无线通信网络安全漏洞检测方法。该方法应用了蚁群算法，并且结合了其他方法，优化检测方法，提高检测能力。与传统被动分簇算法相比，新型无线通信网络安全漏洞检测方法在蚁群算法的基础上，建立了完整的数学描述模型，又根据绕过规则定义标准，确定爬虫技术的应用形式，由于载荷单元的生成与组合状态并不唯一，因此，该方法在定义 SQL 注释语句与 URL 编码条件时，遵循的信息剥离标准不同。在实际应用过程中，这种新型检测方法可以扩大主机元件在单位时间内检测的漏洞信息总量，在增强通信主机对于漏洞信息精准检测能力的同时，解决因漏洞数据大量累积而造成的通信网络运行速率不断下降的问题，这与保障无线通信网络运行稳定性的设计初衷相符合。

参考文献：

[1] 张文柱，孔维鹏，高 鹏，等. 基于改进蚁群算法的无线传感网络路由算法研究 [J]. 计算机测量与控制，2020，28 (7)：274 - 279.

[2] 杨立炜，付丽霞，王 倩，等. 多层优化蚁群算法的移动机器人路径规划研究 [J]. 电子测量与仪器学报，2021，35 (9)：10 - 18.

[3] 王小虎，王 超，李 群，等. 基于黑盒遗传算法的电力系统网络安全漏洞挖掘方法 [J]. 沈阳工业大学学报，2021，43 (5)：500 - 504.

[4] 张 杰，景 雯，陈 富. 基于被动分簇算法的即时通信网络协议漏洞检测 [J]. 吉林大学学报（工学版），2021，51 (6)：2253 - 2258.

[5] 韩 露，史贤俊，林 云，等. 测试不可靠条件下基于精华蚂蚁系统的诊断策略优化方法 [J]. 电子测量与仪器学报，2021，35 (3)：130 - 136.

[6] 张家波，袁 凯，吴昌玉. 一种基于链路质量的蚁群优化 VANET 路由算法 [J]. 重庆邮电大学学报（自然科学版），2020，32 (2)：185 - 191.

[7] 王梓耀，陈俊斌，林 丹，等. 基于精英蚁群 Q 算法的中压配电网双 Q 规划模型 [J]. 电力自动化设备，2020，40 (11)：32 - 42.

[8] 毕玉冰，王文庆，刘超飞，等. 基于泛型思想的电力工业互联网爬虫框架研究 [J]. 热力发电，2020，49 (11)：20 - 27.

[9] 付光明，彭玉丹，孙宝江，等. 外压与弯矩组合载荷作用下筛管压溃载荷计算 [J]. 中国石油大学学报（自然科学版），2021，45 (2)：78 - 86.

[10] 周生通，朱经纬，周新建，等. 组合载荷作用下动车牵引电机转子系统弯扭耦合振动特性 [J]. 交通运输工程学报，2020，20 (1)：159 - 170.

[11] 王孝慈，董树锋，刘育权，等. 基于改进式 k-prototypes 聚类的坏数据辨识与修正 [J]. 电测与仪表，2022，59 (2)：9 - 15.

[12] 李文涛，颜 雄，夏 磊，等. BDS 卫星钟差半参数平差模型异常数据探测与处理 [J]. 测绘学报，2020，49 (1)：55 - 64.

[13] 王永贵，郭昕彤. SparkSql 上自适应数据集的高效频繁集挖掘算法 [J]. 计算机工程与应用，2020，56 (21)：72 - 78.

[14] 曹金超，黄 滔，陈 刚，等. 自然语言生成多表 SQL 查询语句技术研究 [J]. 计算机科学与探索，2020，14 (7)：1133 - 1141.

[15] 张 婷，钱丽萍，汪立东，等. 基于多层卷积模型的恶意 URL 特征自动提取 [J]. 计算机工程与设计，2020，41 (7)：1821 - 1828.

（下转第 109 页）