Computer Science and Application 计算机科学与应用, 2018, 8(3), 266-274
Published Online March 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.83031

Hans汉斯

Malicious Code Detection Method Based on WIG-GA Feature Selection Algorithm

Guan Wang[1,2], Ranran Hao[1,2], Shangwei Gao[1]

[1]College of Computer Science, Beijing University of Technology, Beijing
[2]Key Laboratory of Trustworthy Computing in Beijing, Beijing
Email: noneundefine@163.com

Received: Mar. 5th, 2018; accepted: Mar. 19th, 2018; published: Mar. 27th, 2018

Abstract

In order to solve the problem of feature dimensionality in current malicious code detection, this paper proposes a method of feature selection of malicious code based on information gain algorithm which introduces frequency weight factor and genetic algorithm. This method can select the optimal feature subset that can effectively distinguish between normal code and malicious code, and achieve dimensionality reduction. This method uses the strong global search ability of genetic algorithm to search the feature subset. At the same time, the information gain algorithm based on the frequency weighting factor is used as the fitness evaluation of the feature subset. At last, we use a variety of popular classifiers to learn and verify. Experiments show that this method can effectively reduce the dimensions of features in malicious code detection and effectively improve the learning efficiency and accuracy of the classifier.

Keywords

Malicious Code, Dimensionality Reduction, Genetic Algorithm, Classification

基于WIG-GA特征选择算法的恶意代码检测方法

王　冠[1,2]，郝冉冉[1,2]，高尚伟[1]

[1]北京工业大学计算机学院，北京
[2]可信计算北京市重点实验室，北京
Email: noneundefine@163.com

收稿日期：2018年3月5日；录用日期：2018年3月19日；发布日期：2018年3月27日

文章引用：王冠，郝冉冉，高尚伟．基于WIG-GA特征选择算法的恶意代码检测方法[J]．计算机科学与应用, 2018, 8(3): 266-274. DOI: 10.12677/csa.2018.83031

摘　要

针对当前恶意代码检测中特征高维度问题，本文提出一种基于引入频率权重因子的信息增益算法和遗传算法相结合的恶意代码特征选择方法，该方法可以选择出能够有效区分正常代码与恶意代码的最优特征子集，实现特征的降维。该方法利用遗传算法较强的全局搜索能力进行特征子集的搜索，同时采用基于频率权重因子的信息增益算法作为特征子集的适应度评价，最后在当前流行的多种分类方法中进行学习和验证。通过实验表明：该方法可以有效的降低恶意代码检测中特征的维度，有效的提高了分类器的学习效率和精度。

关键词

恶意代码，特征降维，遗传算法，分类

1. 引言

随着互联网的发展，恶意代码也在迅速增多[1]，变种的未知恶意代码给社会以及人们的日常生活带来的威胁也随之加剧。恶意代码包括木马、蠕虫等多种类型，可以窃取人们信息，攻击网络，破坏基础设施。面对当前恶意代码的泛滥，仅靠人工的逆向检测分析是远远不够的，因此数据挖掘与机器学习技术被应用到恶意代码检测中，进行恶意代码的自动化检测。机器学习恶意代码检测模型首先是要进行代码的特征提取，然后将提取的特征供分类器学习，目前有效的特征提取方法是采用 N-gram 模型[2]提取字节序列特征，已经被广泛应用在了恶意代码检测中，但是提取后的特征维度很高，不利于分类器的学习。

本文提出一种基于引入频率权重因子的信息增益算法和遗传算法相结合的恶意代码特征选择方法，该方法可以选择出能够有效区分正常代码与恶意代码的最优特征子集，实现特征的降维。

2. 相关工作

特征选择的过程是指从提取的特征集中搜索到能够代表特征空间的特征子集，根本选择过程是否依赖分类器可以将特征选择方法分为两大类过滤类和封装类。过滤类选择方法是指通过一定的评价标准，将评价指标较低的特征去除，达到降维的目的，常用的方法有信息增益[3]、增益比、文档频率等文本特征选择算法。过滤类的特征选择算法跟后续的分类算法分开，参数调整比较简单，因此通用性比较高，适合于大量数据的特征降维操作，但是通过评价标准进行特征选择不能确保特征空间的完整性，容易造成特征的缺失。封装类的选择方法依赖于后续的分类算法，需要通过不断调整分类算法的参数，才能达到一定的效率，此方法虽然分类精度较高，但是不断调整参数计算量大，性能较差。文献[4]综合考虑信息增益和特征规模进行特征选择，缩小了特征的维度，在一定程度上提高了分类器的效率和准确率，但是仅仅依据信息增益值的大小进行排序，会造成特征空间的不完整。文献[5]通过改进肯定选择分类算法进行恶意代码的检测，但是在特征选择上仍然是采用的通用的信息增益算法，该方法通用性差。文献[6]

将遗传算法应用到入侵检测系统的特征选择中去，提高了特征空间的搜索能力，当空间特征较少的时候可以通过穷举的方法选择合适的特征组合，但是当特征量很大的时候，通过穷举的方法便是很费时间的。上述方法都没有考虑恶意代码检测中，特征出现的次数，当特征的信息增益值一样，然后出现的次数不一样的时候，特征对于分类器的贡献也不一样，除此之外会造成空间解的丢失。本文提出将频率因子引入信息增益的计算中，同时采用遗传算法做为空间最优解的搜索策略，可以保证选出的代表空间的最优特征子集的完整性不被破坏。

3. 特征提取

N-gram 模型被广泛应用在自然语言处理领域，在恶意代码特征提取方面也有很好的效果。本文采用变长的 N-gram 模型提取字节层特征。在恶意代码检测中，N-gram 是使用一个长度为 N 的滑动窗口对二进制序列进行收集，得到长度为 N 的字节序列字符串。例如一段二进制字节序列 S = (14, 8B, 3C, 01, 15, 2C) 二进制字节序列，当 N 为 3 的时候，可以获得四段子序列分别为 S1 = (14, 8B, 3C,), S2 = (8B, 3C, 01), S3 = (3C, 01, 15), S4 = (01, 15, 2C)。但是定长的 N-gram 算法容易把有意义的字节序列断开，从而破坏能够区分正常代码和恶意代码的字节序列。变长的 N-gram 模型可以弥补这个缺点，并且取得了不错的效果[7]。所以本文采用引入专家投票算法的 N-gram 模型进行程序字节层特征提取，并通过 Trie 树的数据结构进行存储，将提取的字节序列特征以及特征出现的频率保存下来，然后再通过本文提出的特征选择方法进行特征属性的降维，最后将选择出的最优特征子集向量供后续的分类器使用。

4. 基于 WIG-GA 特征选择方法

N-gram 模型提取的字节特征较多维度较大[8]，大量的高维度特征会造成分类器的分类性能降低、分类精度下降等很多问题，因此对提取的字节特征进行降维，选出能够代表分类空间的最优特征子集是非常必要的。目前常用的特征选择方法有信息增益(IG)、特征权(TS)、文档频率(DF)等，这些方法虽然能通过对特征属性的删减达到降维的目的，但是可能会使特征空间丢失掉原来特征集所包含的全部信息。最优特征子集的选择问题实质上是一个特征组合的寻优问题，遗传算法(GA)，也被称为进化算法，是一种受进化论启发，通过模拟自然进化过程搜索最优解的算法。遗传算法在组合优化问题中得到了很好的应用，也引起了很多学者的关注，文献[9]针对遗传算法在组合优化问题中提出了几种不同的适应度函数的构造方法。本文提出一种基于引入频率权重因子的信息增益和遗传算法相结合的特征选择方法(introduced frequency weight factor information gain with genetic algorithm, WIG-GA)，将遗传算法作为搜索策略，结合引入频率权重因子的信息增益算法作为评价函数，经过选择、交叉、变异操作，实现特征维度缩减，选取出最有效的特征子集，供分类器学习与预测。

基于 WIG-GA 算法的特征选择算法流程如下图 1 所示：

4.1. 引入频率权重因子的信息增益算法(WIG)

信息增益(information gain, IG)是特征选择中的一个评价标准，表示在一定条件下信息不确定性减少的程度，也就是说如果一个特征能够为分类带来信息越多，那么这个特征的信息增益值就越大。其定义如下：

$$IG(M,Y)=H(M)-H(M|Y) \tag{1}$$

其中 M 为训练样本数据集，Y 为某一分类特征，$H(M)$ 为训练样本数据集的信息熵，$H(M|Y)$ 为在特征 Y 给定的条件下 M 样本数据集的条件熵，$IG(M,Y)$ 为训练样本数据集 M 的信息熵与在特征 Y 条件下的训练样本数 据集 M 的条件熵的差值。

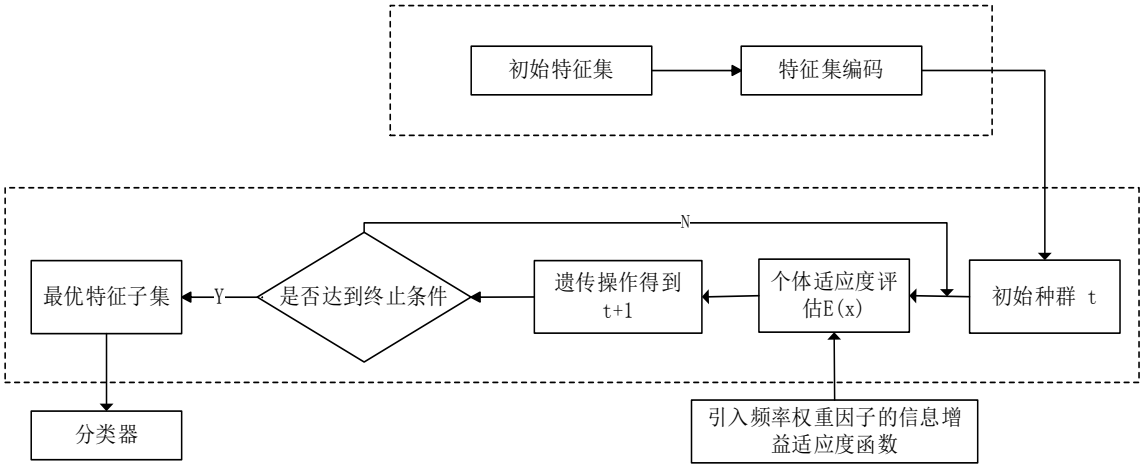

Figure 1. Feature selection process
图 1. 特征选择流程

在恶意代码检测中，设训练样本数据集的个数为 M，样本包含 c 个类别，每一类所包含的样本个数分别为$(x_1,x_2,x_3,\cdots,x_c)$，即 $\sum_{i=1}^{c}x_i=M$，则该样本数据集M的信息熵为：

$$H(M)=-\sum_{i=1}^{c}\frac{x_i}{M}\log_2\frac{x_i}{M} \tag{2}$$

设在训练样本数据集中，特征 Y 的值可以取 n 个，分别为$(b_1,b_2,b_3,\cdots,b_n)$，则特征 Y 把样本数据集分$(y_1,y_2,y_3,\cdots,y_n)$个子集，即 $\sum_{j=1}^{n}y_j=M$，则训练样本数据集 M 在特征 Y 下的条件熵为：

$$H(M\mid Y)=-\sum_{j=1}^{n}\frac{y_j}{M}\sum_{i=1}^{c}\frac{y_{ij}}{y_j}\log_2\frac{y_{ij}}{y_j} \tag{3}$$

将样本数据集 M 的信息熵(2)和样本数据集 M 在特征 Y 下的条件熵(3)带入(1)式得：

$$IG(M,Y)=-\sum_{i=1}^{c}\frac{x_i}{M}\log_2\frac{x_i}{M}+\sum_{j=1}^{n}\frac{y_j}{M}\sum_{i=1}^{c}\frac{y_{ij}}{y_j}\log_2\frac{y_{ij}}{y_j} \tag{4}$$

根据上述公式计算，如果该特征的信息增益值越大，则该特征对区别样本数据集的能力越强。但是信息增益的计算是基于训练数据集的样本数量，也就是仅仅考虑了特征属性在样本数据集出现与否，而没有考虑该特征在样本数据集出现的次数。比如说特征属性 Y_1 和特征属性 Y_2 都在 X_c 类中出现而且在样本训练集其他类别中很少出现或者没有出现，在这种情况下，如果包含特征属性 Y_1 和特征属性 Y_2 的样本训练集个数一样或者差不多，那么根据公式(4)计算出来的特征属性 Y_1 和特征属性 Y_2 的信息增益值是一样的或者近似。但是在实际数据中，不同类别的恶意代码和正常代码中字节特征出现的次数差别是非常大的，因此本文把特征属性在类别出现的次数引入到信息增益的计算中。

设在训练样本中，有特征属性集$(Y_1,Y_2,Y_3,\cdots,Y_n)$，在X_c类中任一样本 $T_k\ (1\le k\le m)$，其中 m 为类 X_c 中样本的总个数，特征属性 Y_i 出现的次数为 $f_{ik}(Y_i)$，则特征属性 Y_i 在类别 X_c 中出现的次数标准化后的权重用 λ_{ci} 表示如下：

$$\lambda_{ci}=\sum_{k=1}^{m}\frac{f_{ik}(Y_i)-\min_{1\le t\le n}\left(f_{ik}(Y_t)\right)}{\max_{1\le t\le n}\left(f_{ik}(Y_t)\right)-\min_{1\le t\le n}\left(f_{ik}(Y_t)\right)} \tag{5}$$

然后针对不同的训练数据集中恶意代码类别和正常代码中样本个数的差异，本文才用归一量化的方法来消除这种差异带来的影响。

$$\lambda = \lambda_{ci} \Big/ \sqrt{\sum_{i=1}^{n} \lambda_{ci}^2} \tag{6}$$

然后在(4)式的基础上引入(6)式，得到改进的信息增益算法如下所示：

$$IG(M,Y) = -\sum_{i=1}^{c} \frac{x_i}{M} \log_2 \frac{x_i}{M} + \lambda \left(\sum_{j=1}^{n} \frac{y_j}{M} \sum_{i=1}^{c} \frac{y_{ij}}{y_j} \log_2 \frac{y_{ij}}{y_j} \right) \tag{7}$$

4.2. 基于 WIG-GA 算法的特征选择方案

遗传算法借鉴生物界的自然选择和进化论思想，通过遗传操作实现个体之间的信息交换，是一种被广泛应用于处理复杂以及非线性问题的自适应搜索算法。最优特征子集的选择实际上是组合优化问题，遗传算法在组合优化问题中得到广泛应用。本文提出的 WIG-GA 特征选择算法，以遗传算法作为特征组合的搜索策略，引入频率权重因子的信息增益作为特征子集的评估函数。

4.2.1. 个体编码与初始种群的产生

在遗传算法的使用中，不能对解空间的实际参数进行直接操作，因此需要对解空间的所有可行解进行编码。在本文中特征只存在选中与不选中两种情况，所以本文选择二进制编码的形式对特征属性集进行编码。

设特征集 $F = (f_1, f_2, f_3, \cdots, f_n)$，总长度为 n，经过编码后的二进制基因位序列 $S = (s_1, s_2, s_3, \cdots, s_n)$，$s_i$ 的取值为{0,1}，如果特征被选中则 s_i 的取值为 1，如果没有被选中则 s_i 的取值为 0，每一个特征子集都是种群的一个个体。例如有 4 个特征(v_1, v_2, v_3, v_4)，$S = (0,1,1,0)$，则被选中的特征为(v_2, v_3)。初始种群通过随机的方式产生。

4.2.2. 适应度评估函数设计

遗传算法仅通过适应度函数对种群中的个体进行评估，依据评价函数的值来确定哪个个体可以被遗传到下一代，哪个个体会在遗传的过程中被淘汰。本文用引入频率因子的信息增益算法作为个体特征子集的评价标准，通过后续的选择、交叉、变异等遗传操作以及种群的不断迭代，当达到最大的迭代次数或者连续 3 代个体平均适应度不再发生变化的时候，选取最后一代中适应度最好的个体，解码后即为选择出的最优特征子集。

设种群中个体 S，结合公式(7)引入频率权重因子的 IG 算法，则个体 S 的改进平均信息增益值为：

$$IG_{\text{avg}} = \frac{\sum_{i=1}^{n} code(s_i) * IG(s_i)}{\sum_{i=1}^{n} code(s_i)} \tag{8}$$

其中 n 为子集所包含的特征个数，$code(s_i)$ 表示子集中特征 s_i 的二进制编码值，$IG(s_i)$ 表示子集中特征 s_i 的改进信息增益值。

除此之外，特征的选择个数也是一个重要的约束条件，能代表空间解能力的特征子集所包含的个数越少越好，所以本文引入惩罚函数 $\Phi(x) = r * u_{s_i}$，其中 r 为惩罚系数，u_{s_i} 为子集中的特征个数。结合(8)式作为最终的评价函数：

$$E(x) = IG_{\text{avg}} - \Phi(x) \tag{9}$$

4.2.3. 遗传操作

遗传算法根据每一代种群中个体的评价函数值，对其通过遗传操作逐步寻找最优子集。每一代种群都需要通过选择、交叉、变异之后才能得到下一代。

1) 选择算子的设计

选择算子的目的是为了让评价高的特征子集能够被保存下来，评价低的特征子集不被保存到下一代。本文通过计算每个特征子集的适应度函数值，然后把适应度值进行排序，通过蒙特卡罗(Monte Carlo)选择方法，选出下一代的种群。在这种方法中，每个特征子集选中的概率与其适应度值成正比。设某个特征子集的适应度值为 $E(S_i)$，特征子集的个数为 n，则选择概率为：

$$P=\frac{E(S_i)}{\sum_{i=1}^{n}E(S_i)} \tag{10}$$

2) 交叉算子和变异算子的设计

交叉算子通过替换重组两个父代的基因，生成结构更复杂的子代基因。不仅可以提高全局搜索能力，还可以保持个体的多样性。变异算子通过改变某些基因座上的值，当遗传算法到达最优子集的临近域的时候，可以通过变异算子提高布局搜索能力。本文采用单点交叉与单点变异的方法进行选择后的遗传操作。交叉概率 P_c 和变异概率 P_m 对算法的搜索性能有很大的影响。概率越大新的特征子集产生越快，但是如果概率过于大，适应度强的特征子集又容易被破坏掉。本文采用自适应的交叉概率和变异概率，P_c 和 P_m 为：

$$P_c=\begin{cases}P_{c_1}-\dfrac{(P_{c_1}-P_{c_2})(E'-E_{\text{avg}})}{E_{\max}-E_{\text{avg}}}, & E\geq E_{\text{avg}}\\ P_{c_1}, & E'<E_{\text{avg}}\end{cases} \tag{11}$$

$$P_m=\begin{cases}P_{m_1}-\dfrac{(P_{m_1}-P_{m_2})(E_{\max}-E)}{E_{\max}-E_{\text{avg}}}, & E\geq E_{avg}\\ P_{m_1}, & E<E_{avg}\end{cases} \tag{12}$$

其中 E' 是要交叉的父代特征子集中比较大的评价函数值，E 是要发生变异的特征子集的评价函数值，$E_{\max}$ 和 E_{avg} 是当代全体中评价函数的最大值和平均值。

4.2.4. 算法描述

本文特征选择算法如下所示，其中输入特征集 F，初始特征集的大小 M，评价函数 E，适应度变化阈值 δ，惩罚系数 r，交叉参数 P_{c_1},P_{c_2}，变异参数 P_{m_1},P_{m_2}，T 为最大的迭代次数。输出能够代表特征空间的最优特征子集。

```
Algorithm: Feature Selection Algorithm
Input: Feature set(FS)
Output: Relative optimal feature subset（ROFS）
1 begin
2     initialize（F,M,E,δ,r,P_c1,P_c2,P_m1,P_m2,T）
3     initialize P(0), t=0
4      while (t≤T) do
5           for i=1 to M do
6                calculate E(i)
7           end for
8                calculate average E(i)
9                changeState = checkFitnessInThreeGenerationChange(E(t),t)
```

```
10              if(changeState)
11                  break;
12          for i=1 to M do
13              select of P(t)
14          end for
15          for i=1 to M/2 do
16              crossover of P(t)
17          end for
18          for i=1 to M do
19              mutation of P(t)
20          for i=1 to M do
21              P(t+1) = P(t)
22          end for
23          t=t+1
24      end while
25  end
```

5. 实验与分析

本文实验的数据分为两个部分，正常程序和恶意程序，恶意程序来源于网站 http://vx.netlux.org，正常程序从 Windows 程序中获取，正常程序选取 120 个，恶意程序选取 118 个，通过变长 N-gram 算法提取 500 个字节特征，分类算法由 MATLAB 实现。本文实验采用 K 折交叉验证的方式，其中 K 取 10，将数据集样本分为 10 份，每份轮流作为测试集，剩下的九份作为训练集，通过十次的分类结果对该特征选择方法的有效性进行验证。

本文选择 MATLAB 中实现的 C4.5、SVM、RBF network、Native Bayes、Random tree 五种分类算法进行实验测试，并采用检测率、准确率、误测率这几个指标作为检测的评价标准。检测率(TPR True Positive Rate)即为能有效检测出恶意代码的概率，准确率(Accuracy)即样本数据被正确分类检测的概率，误测率(FPR False Negative Rate)即正常样本被检测错误的概率。

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{13}$$

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{14}$$

$$\mathrm{Accuracy}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{FN}+\mathrm{FP}+\mathrm{FN}} \tag{15}$$

其中 TP(True Positive)表示将样本的恶意程序正确分类为恶意程序的个数，FP (False Positive)将正常程序错误分类为恶意程序的个数，TN (True Negative)表示将正常程序正确分类为正常程序的个数，FN (False Negative)将恶意程序错误分类为正常程序的个数。

通过表 1 的实验数据可以发现，本文的特征选择方法的平均建模时间和平均样本处理时间要明显比 IG 方法和原始特征集全部使用的情况少，时间性能有较大的提高，其中 Random tree 和 Native Bayes 的建模时间相对于其他分类器相对较好并且样本的平均处理时间也比其他分类器相对较少。通过表 2 的实验数据可以发现在不同分类器检测的情况下，使用本文提出的特征选择方法的检测准确率和检测率相对于 IG 方法和特征全部使用的情况下有一定的提高，并且误测率有了一定的降低，其中 Native Bayes 和

Table 1. Time performance comparison
表 1. 时间性能比较

分类器	平均建模时间/min			平均样本处理时间/ms		
	全部	信息增益	本文算法	全部	信息增益	本文算法
C4.5	2.1	0.8	0.2	0.23	0.05	0.01
SVM	329.8	198.3	120.3	9.68	6.8	4.7
RBF network	2.4	0.91	0.75	0.27	0.09	0.04
Native Bayes	0.3	0.03	0.01	0.037	0.006	0.004
Random tree	0.1	0.08	0.07	0.029	0.007	0.005

Table 2. Classifier detection performance comparison
表 2. 分类器检测性能比较

分类器	Accuracy/%			TPR/%			FPR/%		
	全部	信息增益	本文算法	全部	信息增益	本文算法	全部	信息增益	本文算法
C4.5	89.2	89.7	89.9	99.4	99.1	98.9	0.19	0.1	0.05
SVM	90.1	90.3	90.7	99.7	99.5	99.9	0.23	0.13	0.07
RBF network	88.7	88.6	90.1	91.3	91.1	92.4	0.56	0.43	0.28
Native Bayes	93.2	93.4	94.5	99.3	99.2	99.8	0.47	0.38	0.29
Random tree	94.7	94.5	95.6	98.9	99.1	99.8	0.15	0.1	0.06

Random tree 的准确率和检测率相对于其他分类器相对较高。综合分析，本文提出的特征选择方法可以有效的实现特征维度的减少，相对 IG 方法有不论是在准确率还是检测率方面都有一定的提高，并且在 Native Bayes 和 Random tree 分类算法取得了很好的检测效果。

6. 结束语

本文提出一种引入频率权重因子的信息和遗传算法的特征选择方法，利用遗传算法较强的全局搜索能力作为特征空间的搜索策略，同时使用引入频率权重因子的信息增益算法作为特征子集的评价函数，然后通过变长 N-gram 模型提取字节层特征，最后通过不同的分类算法进行验证，实验结果表明该方法可以有效的缩短建模时间，提高检测效率。在后续的研究工作中，将通过提取指令层、函数结构图层等不同的特征进行验证，并研究更为有效的特征降维方法，加大样本数据集，进行进一步的验证，提高检测性能与准确率。

参考文献 (References)

[1] Lee, T., Kim, D., Jeong, H., *et al.* (2014) Risk Prediction of Malicious Code-Infected Websites by Mining Vulnerability Features. *International Journal of Security & Its Applications*, **8**, 291-294. https://doi.org/10.14257/ijsia.2014.8.1.27

[2] Abouassaleh, T., Cercone, N., Kešelj, V., *et al.* (2004) N-Gram-Based Detection of New Malicious Code. *Proceedings of the 28th Annual International Computer Software and Applications Conference*, **2**, 41-42.

[3] Berrar, D. and Dubitzky, W. (2013) Information Gain. Springer, New York, 1022-1023. https://doi.org/10.1007/978-1-4419-9863-7_719

[4] 郭宁, 孙晓妍, 林和, 等. 基于属性序约简的恶意代码检测[J]. 计算机应用, 2011, 31(4): 1006-1009.

[5] 张福勇, 赵铁柱. 基于肯定选择分类算法的恶意代码检测方法[J]. 沈阳工业大学学报, 2016, 38(2): 206-210.

[6] 朱红萍, 巩青歌, 雷战波. 基于遗传算法的入侵检测特征选择[J]. 计算机应用研究, 2012, 29(4): 1417-1419.

[7] Reddy, D.K.S., Dash, S.K. and Pujari, A.K. (2006) New Malicious Code Detection Using Variable Length n-Grams. *Information Systems Security*, **4332**, 307-323.

[8] 李盟, 贾晓启, 王蕊, 等. 一种恶意代码特征选取和建模方法[J]. 计算机应用与软件, 2015(8): 266-271.

[9] 陈果, 邓堰. 遗传算法特征选取中的几种适应度函数构造新方法及其应用[J]. 机械科学与技术, 2011, 30(1): 124-128.