丁士杰，张志伟，谢军．气象灾害系统的恶意代码攻击自动化免疫方法[J]．灾害学，2020，35(2)：18-21.[DING Shijie, ZHANG Zhiwei and XIE Jun. Automatic Immune Method of Malicious Code Attack in Meteorological Disaster System [J]. Journal of Catastrophology, 2020, 35(2): 18-21. doi: 10.3969/j.issn.1000-811X.2020.02.004.]

气象灾害系统的恶意代码攻击自动化免疫方法*

丁士杰[1]，张志伟[2]，谢 军[1]

（1. 宿州学院 商学院，安徽 宿州 234000；2. 宿州学院 信息工程学院，安徽 宿州 234000）

摘 要：对气象灾害系统的恶意代码防御是该领域中的重点内容，为了有效缓解和改善恶意代码给气象灾害系统带来的安全隐患，该文提出了气象灾害系统的恶意代码攻击自动化免疫方法，首先识别和提取恶意代码动态特征，针对动态特征实行编码操作，将编码结果当作未成熟识别器其中一个来源，未成熟的识别器历经阴性筛选得到成熟识别器，并对抗原亲和程度高且已经成熟的识别器实行克隆和变异等操作，获取具备高亲和度的识别器下一代，通过所得识别器检测出恶意代码。基于恶意代码检测结果，融合动态免疫规则，并引入联合式免疫算法，获得主客体集合与行为集合及安全政策相结合下的气象灾害系统的恶意代码自动化免疫模型，由此完成恶意代码攻击自动化免疫。

关键词：气象灾害系统；移动恶意代码；自动化免疫；动态免疫规则

中图分类号：X43；P642；X915.5　　**文献标志码**：A　　**文章编号**：1000-811X(2020)02-0018-04

doi：10.3969/j.issn.1000-811X.2020.02.004

气象灾害主要包括龙卷风、暴雨、高温干旱、冰冻、山洪、地震、沙尘暴等[1]。虽然人们能及时预报当前气象灾害，但这种预报还存在一定局限性，当前气象灾害系统的免疫能力存在薄弱环节，气象监测不能满足经济快速发展对突发灾害预报的需求[2]。且气象灾害系统中经常含有一些恶意代码，这对系统安全产生了严重威胁。通常情况下，使用者会利用一些防木马病毒的技术来保护气象灾害系统安全，虽然起到了一定作用，但整体看来效果并不是十分乐观[3]。为了有效缓解和改善恶意代码给气象灾害系统带来的安全隐患，必须将恶意代码自动化免疫研究提上日程。

罗小双等[4]考虑到恶意攻击问题，提出将Bloom Filter数据结构应用至系统信息安全保护中，实现恶意攻击免疫。所提出的方法可以保障数据传输两端的隐私安全性，并得到两端数据集合中存在的交集。两端中的一端可以得到交集中的元素，而另一端则无法获得交集，双方均无法得到或者预测出对方除了交集以外的元素，以此高效保障了信息安全性，达到免疫的目的。王盼等[5]将研究重点放在了终端恶意代码识别和免疫上，并提出针对终端恶意代码识别的模型—MPMD-DIM，该模型能够使终端与分布式的识别检测服务设备间协同运行，以此提高恶意代码检测效率。该模型通过优化后的反向选择法与动态克隆选择法完善恶意软件识别流程，同时及时给出免疫响应。利用分布式的识别服务设备间疫苗选择及接种，生成二次免疫响应，进而提高识别检测速度。

现今，恶意代码横行，对其免疫算法进行研究是气象灾害系统安全运行的重点内容[6]。本文提出将动态免疫规则引入至气象灾害系统的恶意代码自动化免疫中，以高效解决当前研究成果存在的问题和满足现实需求。

1 气象灾害系统的恶意代码自动化免疫

1.1 恶意代码检测

以更稳定可靠地实现恶意代码免疫为目的，利用动态分析的方式，基于生物免疫体系防御病毒等一系列抗原定义，将恶意代码动态特征识别并提取出来，依据实值向量编码的方式得到抗原。当未成熟识别器自身耐受成功之后得到成熟识别器，通过克隆选择法改进成熟识别器，获取具备高亲和度的识别器下一代，通过所得识别器检测并提取出恶意代码。气象灾害系统的恶意代码检测详细过程如下。

(1)恶意代码动态特征识别与提取

利用气象灾害模拟器当作恶意代码正常运行背景，并将待研究的对象安装至模拟器中，监控整个运行过程。同时对源代码进行修改，并在监

* 收稿日期：2019-11-02　　修回日期：2020-02-07
基金项目：安徽高校自然科学研究重点项目(KJ2018A0448)；安徽省教育厅人文社科研究重点项目(SK2017A0465)
第一作者简介：丁士杰(1979-)，男，安徽宿州人，硕士，讲师，主要研究方向为网络安全．E-mail：709417149@qq.com

控函数中设置日志记录模块，当恶意代码有控制指令调用该函数，对函数的参数信息进行记录[7]。将修改之后的源代码编译，以此获取新数据添加至模拟器中。通过快照技术，分析完一个样本就清理干净模拟器。采用 monkeyrunner 对用户在系统中的交互事件进行模拟，以此发出气象灾害恶意代码动态性操作。

经过上述操作，得到的气象灾害系统行为特征一共分为五种类型，分别为启动服务、视频服务、发送信息、跳转网络和文件操作。其中识别和提取到的气象灾害系统动态特征具体内容为：启动服务对应的数据内容为“名称”；视频服务对应的数据内容为“网址”；发送信息对应的数据内容为“网址”；跳转网络对应的数据内容为“IP 或者端口”；文件操作对应的数据内容为“路径”。

针对识别和提取得到的动态特征实行统一编码操作，并根据实值向量将特征编码成具有 6 个维度的向量，各维度根据 8b 数值描述。第 1 维描述的是特征种类，第 2 至第 6 维描述的是动态特征数据内容。经过编码，得到动态特征向量可表示为：

$$F=(f_1, f_2, f_3, f_4, f_5)。\tag{1}$$

式中：f_1, f_2, f_3, f_4, f_5 分别代表气象灾害系统动态特征基础向量值。针对动态特征向量 F 实行归一化操作。其中，设定 f_i^{max} 代表气象灾害系统 F 中第 i 维中最大值，f_i^{min} 代表系统 F 中第 i 维中最小值。f_i 代表气象灾害系统归一化之前特征向量值，f' 代表气象灾害系统归一化之后的特征向量，其表达式为：

$$f'_i=\begin{cases}(f_i-f_i^{min})/(f_i^{man}-f_i), & f_i^{man}>f_i^{min};\\ 0.5, & f_i^{man}=f_i^{min}。\end{cases}\tag{2}$$

（2）阴性筛选机制

实际上，阴性筛选机制是一种对生物免疫体系可以精准判断自我与非我状况的关键保障机制，以此提升恶意代码检测查准率，进而提升免疫精确性。在课题研究过程中，设置了两个没有成熟的识别器来源，其中包含：气象灾害系统恶意代码动态特征识别提取，此类识别器可以表征已经存在的恶意代码具备的特征；性能良好的成熟识别器克隆变异，获取优秀的识别器下一代。

在阴性筛选的整体流程中，没有成熟的识别检测器按顺序和自我集合中各元素进行配准操作，只有不配准自我元素则表示识别器已经成熟。气象灾害系统识别检测器可表示为：

$$d=(x_1, \cdots x_n)。\tag{3}$$

式中：n 代表气象灾害系统识别器维度。识别半径是 r_d，识别范围主要是将 d 当作中心，以 r_d 为半径的球体。识别器自我元素可表示为：

$$s=(y_1, \cdots y_n)。\tag{4}$$

对 d、s 间欧几里得距离进行计算：

$$ED(d, s)=\left(\sum_{i=1}^{n}(x_i-y_1)^2\right)^{\frac{1}{2}}。\tag{5}$$

经上述计算与分析，假设 $ED(d, s)<r_d$，那么自我元素 s 将会位于没有成熟的识别器中，即该识别器会被淘汰。

（3）克隆变异机制

在气象灾害系统恶意代码检测过程中，克隆变异机制主要是应用在免疫体系对抗原刺激生成的免疫响应基本特性的方式。其可以和抗原配准的免疫细胞遍历克隆增殖，历经克隆的细胞下一代根据变异可以增强对抗原产生的亲和力。

克隆的整体过程为：针对成熟了的识别器 d_i，基于其识别到的气象灾害系统恶意代码特征数量 N_i 判断其亲和度，其中，N_i 越大则抗原的亲和度就越高。设置阈值 T，如果 $N_i>T$，那么对其开展克隆与变异操作。识别器 di 克隆数量 $N(d_i)$ 可表示为：

$$N(d_i)=\alpha\cdot N_i。\tag{6}$$

式中：α 代表气象灾害系统克隆系数。气象灾害系统变异的整体过程如下：假设变异的识别器表达式为 $d=(x_1, \cdots, x_n)$，针对第 i 维元素 x_i，将其取值范围设置为 $[u, l]$，那么变异之后的值 α_i 可表示为：

$$a_i=\begin{cases}a_i+\triangle(u-a_i), & \zeta(0, 1)=0;\\ a_i-\triangle(a_i-l), & \zeta(0, 1)=1。\end{cases}\tag{7}$$

式中：ζ 代表随机变量，其取值为 0 或者 1。

（4）识别提取

识别并提取出待测样本的动态特征是 $F=\{f_1, f_2, f_3, f_4, f_N\}$，$N$ 是特征的总数量[8-9]。识别检测器的集合是 $D=\{d_1, \cdots, d_M\}$，M 代表识别器总数。

将气象灾害系统动态特征数量进行初始化 $N_a=0$，针对 F 中各特征按照顺序和识别检测器集合 D 中元素进行配准，假设和某识别器的配准成功，那么 $N_a=N_a+1$。设 $P=N_a/N$，如果 P 比设置阈值 P_T 大，那么可判定该气象灾害系统中存在恶意代码程序。在上述方案中能够利用阈值 P_T 的大小增减，对查准率和查全率进行调节。

1.2　恶意代码自动化免疫

气象灾害系统是一个开放和动态式的系统，整个系统中各种类型的操作不断涌进。此种环境下，要保障阻止恶意代码扩散，促使恶意代码的传播与生成损坏的主客体以及行为构成相对完整的操作，就可以防止攻击的状况发生，以此达到免疫的效果[10-11]。基于该理念，在如何保障新进入的主客体和操作元素对气象灾害系统不产生危害方面，融合了动态免疫规则，防止恶意代码攻击[12-13]。

依据 1.1 计算分析可检测出气象灾害系统中存在的恶意代码，但一般情况下，恶意代码产生攻击是在添加攻击元素之后，由此，设定添加攻击元素才可以进行攻击的三项分别为 A'、B'、C'，当攻击元素引入之后通过某种规则控制住生成攻击的完整操作构成，能够有效防止攻击生成，实现免疫。

上述为一个动态免疫的过程，主要是针对气

象灾害系统中的移动恶意代码。为了提升恶意代码免疫查全率，引入联合式免疫算法[14]。事实上，气象灾害系统的安全性能属于一个动态性的定义，和信息体系的详细情况与安全政策等需求息息相关，信息体系详细情况不断变化和安全政策的日益调节，气象灾害系统安全指标也会随之变化[15-16]。在此，将气象灾害系统初始的安全状态定义成信息体系详细情况以及安全政策调节之后而达到的状态。

针对某气象灾害系统 $S(A^{'}, B^{'}, C^{'}, D^{'})$，假设 $\exists F^{''}\text{s.t}F^{''}P_T(s(A^{'}, B^{'}, C^{'}, D^{'})) = s_0(A_0^{'}, B_0^{'}, C_0^{'}, o)$，那么 $F^{''}$ 就是免疫计算模型。

其中，$F^{''}$ 通常情况下为一整套免疫规则亦或是一系列流程构成的集合，与信息体系详细状况及安全政策关联性很强[17-18]。

基于上述定义与推理能够获得主客体集合与行为集合及安全政策相结合下的气象灾害系统的恶意代码自动化防护模型，即免疫模型表达式为：

$$\begin{cases} F_S^{''}(A^{'}, B^{'}, C^{'}, D^{'}) = s_0(A_0^{'}, B_0^{'}, C_0^{'}, o); \\ b(A_0^{'}) = E^{'}, \ h(E^{'}) = A_0^{'}; \\ C_0^{'}(w(A_k^{'}), w(B_k^{'})) = C_0^{'}(A_0^{'}, B_0^{'}) \subseteq o; \\ G^{'}((C_0^{'} + c^{'})((A_0^{'} + a^{'}), (B_1^{'} + b^{'}))) = C_0^{'}(A_0^{'}, B_0^{'}) \subseteq o。 \end{cases} \tag{8}$$

式中：o 代表气象灾害系统中非攻击元素，b 代表气象灾害系统中一个备份函数。客体集合为 $B^{'}$，主体集合为 $A^{'}$，行为集合为 $C^{'}$，三个集合经函数 $F^{''}$ 获取安全政策范围中不会生成恶意攻击的子集合为 $A_0^{'}$、$B_0^{'}$、$C_0^{'}$，h 代表恢复函数，w 代表经验的校验函数，$G^{'}$ 代表控制构成恶意攻击的相对完整操作动态规则组成的集合，$a \in A^{'}$，$b \in B^{'}$，$c \in C^{'}$，$E^{'}$ 代表由主体和客体组建的集合[19-20]。

式(8)属于一个闭环控制程序，能够使气象灾害系统在开放式的背景下防止攻击生成，完成恶意代码自动化免疫，并在一定程度上增强免疫可靠性。

2 模型实验结果与分析

为了验证所提算法有效性，得到对真实样本的免疫效果，在气象灾害系统中采集了恶意代码与正常的数据样本各 200 个进行实验，实验平台搭建在 MATLAB 上。测试过程中将样本划分成 2 个集合，分别为训练样本集合、测试样本集合。

实验过程中，把训练样本集合中恶意代码与正常程序在气象灾害模拟器中运作，并监控与记录整体行为特性，进行实值编码之后获取特征向量。将其中的恶意代码特征当作没有成熟的识别器来源，而正常的样本程序特征向量当作自我元素中的集合，通过阴性筛选机制获取成熟的识别器。

利用本文算法流程对恶意代码进行检测和免疫，对恶意代码进行检测的过程中，采用阴性筛选机制对检测精确性进行了调整，其是一种对生物免疫体系可以精准判断自我与非我状况的关键保障机制，进而可以有效检测出恶意代码。另外，利用主客体集合与行为集合及安全政策相结合构建的气象灾害系统的恶意代码自动化免疫模型，(图 1)。由图 1 可知，该气象灾害系统的恶意代码自动化免疫模型实际上是一个闭环控制程序，能够使气象灾害系统在开放式的背景下防止攻击生成。

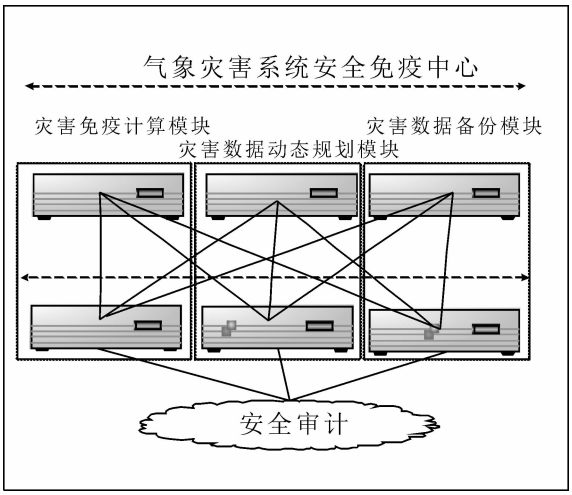

图 1 气象灾害系统的恶意代码自动化免疫模型

本文算法没有受到恶意样本数量和实验次数增加的干扰，为了提升气象灾害免疫，引入了联合式的免疫算法，并通过设置阈值对恶意代码检测进行了调节，更加高效地提升了所提算法的免疫性能。利用克隆代数对气象灾害系统的恶意代码检测(图 2)，随着克隆代数逐渐增大，气象灾害系统的恶意代码免疫可靠性逐渐上升，在识别器数量达到 600 个时，200 代的恶意代码免疫可靠性达到 95%，且识别器的数量越多，检测结果免疫可靠性也会逐渐上升，本文所提出方法可有效缓解和改善恶意代码给气象灾害系统带来的安全隐患。

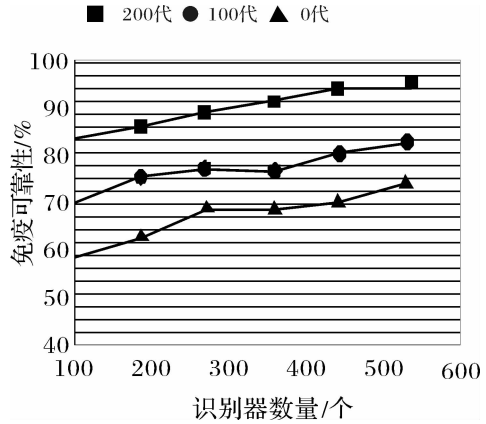

图 2 克隆代数对恶意代码检测结果

3　结论

气象灾害系统安全一直是该领域的研究重点，为了有效解决当前恶意代码检测与免疫相关成果存在的问题，提出利用动态免疫规则实现气象灾害系统的恶意代码自动化免疫。过程中，先对气象灾害系统中的恶意代码进行了识别与提取，然后分别结合动态免疫规则和信息体系详细情况以及安全政策实现恶意代码自动化免疫。经测试对所提算法进行验证，试验结果表明，该算法性能较为完善，具有较高的可靠性，可应用于实际的恶意代码攻击自动化免疫中。

参考文献：

[1] 王军，黄杰飞，程勇．基于大数据处理的农业气象灾害分类模型[J]．计算机仿真，2017，34(5)：353-356，370.

[2] 孙治贵，王元胜，张禄，等．北方设施农业气象灾害监测预警智能服务系统设计与实现[J]．农业工程学报，2018，34(23)：157-164.

[3] 韩兰英，张强，杨阳，等．气候变化背景下甘肃省主要气象灾害综合损失特征[J]．干旱区资源与环境，2019，33(7)：109-116.

[4] 罗小双，杨晓元，王绪安．一类可抵抗恶意攻击的隐私集合交集协议[J]．计算机应用，2017，37(6)：1593-1598.

[5] 王盼，梁意文．手机恶意软件检测的分布式免疫模型[J]．计算机工程与应用，2016，52(16)：30-35.

[6] 曹玉林，王小明，何早波．移动无线传感网中恶意软件传播的最优安全策略[J]．电子学报，2016，44(8)：1851-1857.

[7] 刘建勇，吴伟光，陈秉权，等．坝上温室育苗气象灾害系统预报制作与输出的自动化设计浅谈[J]．软件，39(9)：131-134.

[8] 邓兆琨，陆余良，黄钊．动静结合的网络恶意代码检测技术研究[J]．计算机应用研究，2019(7)：2159-2163.

[9] 王子腾．一种多机器学习算法集成的恶意代码检测系统[J]．网络安全技术与应用，2018(4)：33-34.

[10] 苗爱梅，郝寿昌，武永利，等．基于 GIS 的极端气象灾害预警与评估集成系统[J]．中国科技成果，2019，20(7)：20-21.

[11] 黄晓云，王静爱，尹卫霞，等．灾害系统视角下的石漠化风险评价研究——以贵州省大方县为例[J]．灾害学，2017，32(3)：87-90.

[12] 焦圣明，郑媛媛，王宏斌，等．灾害性天气个例库智能分析系统的设计与实现[J]．气象，2017，43(3)：354-364.

[13] 许皓皓，何彩芬．气象灾害数据库管理与分析系统开发与实现[J]．电子技术与软件工程，2017，14(17)：156-158.

[14] 宋文纳，彭国军，傅建明，等．恶意代码演化与溯源技术研究[J]．软件学报，2019，8(8)：2229-2267.

[15] 王杰，史颖慧，方家麟．基于 GIS 的电网气象灾害监测预警系统的探究[J]．自动化应用，2017(5)：92-93.

[16] 叶晓星．分析智能建筑灾害自动报警系统的设计思路[J]．智能城市，2017，3(12)：28-30.

[17] 车秀芬，张京红，黄海静，等．海南芒果气象灾害监测及气候品质认证系统研发[J]．气象研究与应用，2017，38(2)：45-48.

[18] 郭燕君，李芳．基于犹豫度的灾害链应急系统优先权排序研究[J]．灾害学，2017，32(1)：216-220.

[19] HE T，XUE J，FU J，et al. Research on Malicious Code Analysis Method Based on Semi-supervised Learning[C]// Chinese Conference on Trusted Computing and Information Security. Springer，Singapore，2017：227-241.

[20] 齐玉东，孙明玮，丁海强，等．基于特征匹配的恶意代码变种检测[J]．计算机与数字工程，2019，47(5)：1179-1183.

Automatic Immune Method of Malicious Code Attack in Meteorological Disaster System

DING Shijie[1]，ZHANG Zhiwei[2] and XIE Jun[1]

(1. *School of Business*，*Suzhou University*，*Suzhou* 234000，*China*；

2. *School of Informatics and Engineering*，*Suzhou University*，*Suzhou* 234000，*China*)

Abstract：The prevention of malicious code in meteorological disaster system is the key content in this field. In order to effectively alleviate and improve the security risks brought by malicious code to meteorological disaster system，the automatic immune method of malicious code attack in meteorological disaster system is proposed. Firstly，we identify and extract the dynamic characteristics of malicious code，code the dynamic characteristics，regard the coding result as one of the sources of the immature recognizer，the immature recognizer gets the mature recognizer after negative screening，and clone and mutate against the original recognizer with high affinity，so as to obtain the next generation of recognizer with high affinity The obtained recognizer detected malicious code. Based on the results of malicious code detection，dynamic immune rules are integrated，and the combined immune algorithm is introduced to obtain the automatic immune model of malicious code in meteorological disaster system under the combination of host object set，behavior set and security policy，thus completing the automatic immune of malicious code. Experimental results show that the algorithm can effectively alleviate and improve the security risks brought by malicious code to meteorological disaster system，and has strong immune reliability.

Key words：meteorological disaster system；mobile malicious code；automatic immunity；dynamic immunity rules