

云计算环境下混合多样木马群检测技术仿真

金显华¹, 赵元庆²

(1 安阳师范学院 公共计算机教学部, 河南 安阳 455000; 2 安阳师范学院 计算机与信息工程学院, 河南 安阳 455000)

摘 要: 提出基于粒子辨别树联合算法的云计算环境下混合多样木马群检测方法. 对云计算环境下的木马进行有效的分类处理, 根据分类结果构建关联粒子入侵辨别树, 利用攻击特征更新理论和更新后密度分布理论完成云计算环境下混合多样木马群的检测. 实验结果表明, 利用该算法进行云计算环境下混合多样木马群检测, 能够有效提高检测效率, 降低漏检率.

关键词: 云计算; 木马群; 粒子辨别树

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2014)01-0132-05

Hybrid Variety Trojan Cloud Computing Environment of Simulation Test Technology

JIN Xian-hua¹, ZHAO Yuan-qing²

(1 Computer Teaching Department, Anyang Normal University, Anyang 455000, China;

2 School of Computer and Information Engineering, Anyang normal university, Anyang 455000, China)

Abstract: This paper proposes a cloud computing environment based on particle to identify tree algorithm hybrid variety Trojan detection method. According to the related theory, the particle swarm of Trojan cloud computing environment for effective classification processing, which provide data for various Trojan detection based. Establish particles to identify tree, complete hybrid variety Trojan group of cloud computing environment detection. The experimental results show that the algorithm presented in this paper for hybrid variety Trojan detection of cloud computing environment can effectively improve the efficiency of detection, lower miss rate, thus providing security for the network security.

Key words: cloud computing; Trojan group; particles to identify tree

1 引言

随着网络技术的不断发展和普及, 网络安全也日益受到人们的广泛关注^[1]. 在云计算环境下, 需要对木马进行准确的检测, 才能保证该网络环境的安全性^[2]. 因此, 云计算环境下的木马检测方法, 已经成为网络安全领域需要研究的热点问题^[3]. 现阶段, 主要的云计算环境下木马检测方法包括基于粒子群算法的木马检测方法、基于支持向量机算法的木马检测方法和基于敏感数据挖掘算法的木马检测方

法^[4-6]. 其中, 最常用的是基于敏感数据挖掘算法的木马检测方法^[7]. 由于云计算环境下的木马检测方法在网络安全方面占据十分重要的地位, 因此, 拥有广阔的发展空间^[8].

利用传统的敏感数据挖掘算法进行云计算环境下的木马检测, 由于云计算环境中存在大量的服务器混合的现象, 木马的特征也呈现极强的多样性, 导致难以用统一的约束条件进行木马检测, 造成木马检测的效率过低, 漏检率较高, 难以满足网络计算的实际需求^[9].

收稿日期: 2013-04-23; **修回日期:** 2013-06-17

基金项目: 国家自然科学基金青年基金项目(41001251); 河南省科技厅基础与前沿研究项目“分布式网络入侵检测关键技术研究”(112300410129)

为了避免上述缺陷,提出了一种基于粒子辨别树算法的云计算环境下混合多样木马群检测方法.根据粒子群相关理论,对云计算环境下的木马进行有效的分类处理,为多样木马群检测提供数据基础^[10].建立粒子辨别树,完成云计算环境下混合多样木马群的检测.实验结果表明,利用本文算法进行云计算环境下的木马检测,能够缩短检测时间,提高检测效率,同时提高木马检测的准确性,保证为云计算提供安全的网络环境.

2 传统云计算环境下木马检测原理及弊端

利用传统的敏感数据挖掘算法进行云计算环境下的木马检测,能够针对大量的混合服务器完成木马检测,为云计算提供安全的环境.其详细内容如下所述:

根据云计算环境下的网络数据关联性,能够得到上述网络计算过程中的约束条件,用上述约束条件能够描述云计算环境下网络数据的特征.根据下述公式可以计算云计算环境下网络数据特征之间的关联性:

$$Y_{G(z_k)} = \lim_{\Delta G(z_k) \rightarrow 0} \frac{\Delta G_{avg}}{\Delta G(z_k)} = \frac{\partial G_{avg}}{\partial G(z_k)} \quad (1)$$

根据下述公式可以计算云计算环境下网络计算特征:

$$Y_{D(z_k)} = \lim_{\Delta D(z_k) \rightarrow 0} \frac{\Delta G_{avg}}{\Delta D(z_k)} = \frac{\partial G_{avg}}{\partial D(z_k)} \quad (2)$$

根据上述方法,可以对云计算环境下的木马相关数据进行有效的敏感性分析,并且将得到的敏感性分析结果传输到用户端.根据上述数据,能够利用下述公式计算云计算环境下的木马检测特征归属概率:

$$Y_{d(z_k)} = \frac{\sum_{z_k} [\Delta D_{10}(m) + \Delta D_{01}(m)]}{\Delta d(z_k)} \quad (3)$$

由于云计算环境下的木马数据特征之间的独立性较强,所以,可以将上述特征进行组合,得到下述结果:

$$G = G_{avg} + \sum_{k=1}^{K_{num}} \Delta \delta(z_k) Y_{\delta(z_k)} \quad (4)$$

利用敏感数据挖掘算法进行云计算环境下的木马检测的具体流程如下所述:

(1) 将云计算环境下的所有网络数据特征构成一个序列,通过运算获取该序列中元素之间的敏感性;

(2) 针对上述网络数据特征序列中的元素进行

有效的过滤,假设该特征小于设定的阈值,则删除该数据,得到一个新的网络特征序列 W_1 .

(3) 在云计算环境下木马检测时,删除网络特征中小于 $q-1$ 次的元素,将剩余的元素构成一个新的序列,能够用 W_{r-1} 表示.

(4) 针对新获取的云计算环境下网络特征序列进行元素敏感性计算.

(5) 建立敏感性较强的云计算环境下的网络特征集合,在该集合中进行最优目标搜索,得到木马特征.

根据上面阐述的方法,能够完成云计算环境下的木马检测,但是,在检测过程中,由于云计算环境中大量混合服务器参与,木马特征呈现集群多样性,无法约束,降低了云计算环境下木马检测的准确率.

3 云计算环境下木马检测优化方法

利用传统算法进行云计算环境下的木马检测,由于该环境中服务器大范围混合,造成木马特征呈现较强的集群多样性,降低了检测的准确性.为此,提出了一种基于粒子辨别树算法的云计算环境下混合多样木马群检测方法.

3.1 云计算环境下木马特征分类方法

根据粒子群相关原理,可以对所有的木马特征进行有效的分类处理,为云计算环境下的混合多样木马群检测提供依据.设置木马粒子群中全部粒子的数量可以用 q 表示,对应的空间维度可以用 F 表示.在木马粒子群特征空间中,进行最优粒子的搜索,可以得到特征空间中的最优点.

根据下述公式,可以对木马粒子群中的粒子进行位置更新:

$$X_k(m+1) = \phi X_k(m) + e_1 \text{rand}() (R_k - Z_k(m)) + e_2 \text{rand}() (R_i - Z_k(m)) \quad (5)$$

根据下述公式,可以对木马粒子群中的粒子进行速度更新:

$$X_k \in [-X_{\max}, X_{\max}]$$

$$Z_k(m+1) = Z_k(m) + X_k(m+1) \quad (6)$$

在上述公式中, Z_k 可以表示木马粒子群中第 k 个粒子的位置, X_k 可以用来表示木马粒子的运行速度.设置木马粒子群中第 k 个粒子的理想位置可以用 r_k 表示,该木马粒子群中全部粒子的当前最优位置可以用 R_k 表示,对应的权重能够用 ϕ 表示,木马粒子群中粒子的权重,可以决定粒子的运行速度. e_1 和 e_2 能够用来描述木马检测过程中的更新速度影响因子.更新速度影响因子在木马粒子更新的过程

中,需要不断进行优化处理,得到最优木马影响因子. $\text{rand}()$ 表示木马粒子在指定区域中的分布情况. 在木马粒子群中的粒子进行更新的过程中,粒子运行速度极大值可以用 $X_{\max}$ 表示.

设置云计算环境下木马群检测的过程中,全部木马构成的粒子群中,粒子的数目是 Q ,每个粒子的运行范围可以用 N 表示,利用下述公式能够计算木马粒子群中粒子的分布密度:

$$F_Q = \frac{1}{1 + G(Q)}$$

$$G(Q) = \frac{1}{N} \sum_{l=1}^N G_l(Q)$$

$$G_l(Q) = \sum_{k=1}^Q -r_{kl} \log r_{kl} \quad (7)$$

在上述公式中, r_{kl} 表示第 Q 个粒子在第 l 个区间中的概率, $G(Q)$ 表示木马粒子群中所有粒子的信息熵, $G_l(Q)$ 表示第 l 个木马粒子的信息熵, F_Q 表示所有粒子的分布密度,该分布密度的取值区间是 $F_Q \in (0, 1)$. 在木马群构成的粒子群中,如果 $F_Q = 1$,则代表该粒子群中的全部粒子都是相同的.

根据上面阐述的方法,能够得到木马粒子群中全部粒子的分布情况如图 1 所示.



图 1 木马粒子群中粒子分布图

设置木马粒子群中全部粒子的数目是 Q , $C_k \in C$, 则可以得到木马粒子 C_k 的邻域集合如下所述:

$$T(C_k) = \{T_l | 0 < \|C_k - T_l\| < t, T_l \in T\} \quad (8)$$

对木马粒子群中的所有粒子进行自适应调整,其流程如下所述:

(1) 设置木马粒子群中所有粒子的分布密度是 F_Q , 对应的分布阈值是 ∂ , 如果 $F_Q > \partial$, 则可以对木马粒子群中的粒子进行有效的更新, 提高了木马粒子群在分类过程中粒子的更新速度, 提高分类效率.

(2) 在迭代处理的过程中, 木马粒子可以用 C_k 表示, 邻域中的木马粒子可以用 P 表示. 针对上述粒子进行差值计算, 可以得到一个新的粒子集合 F , 有效提高木马粒子群中粒子的寻优能力, 实现木马特征粒子群中木马特征的分类处理.

根据上面阐述的方法, 能够对木马特征粒子群

中的粒子进行有效的分类处理, 为木马群检测提供依据.

3.2 构建粒子辨别树

根据云计算环境下的混合多样木马特征, 可以实现粒子辨别树的构建, 利用攻击特征更新理论和更新后密度分布理论完成云计算环境下混合多样木马群的检测. 粒子辨别树是一种树结构, 该树结构中包含多个不同的层次, 其中, 每一个层次都可以用来描述一种木马特征. 粒子辨别树构建的详细内容如下所述:

设置云计算环境下混合多样木马群中木马特征数量能够用 p 进行描述, 上述木马特征构成的集合是 $\{t_1, t_2, \dots, t_p\}$, 木马特征之间具有较强的关联性, 这些数据之间的关联性构成的集合可以用 $P(t_1)$,

$P(t_2), \dots, P(t_p)$ 表示, 设置 $\sum_{k=1}^p P(t_k) = 1$, 则可以得到云计算环境下混合多样木马的信息熵如下所述:

$$I(T) = q_1 Y(t_1) + q_2 Y(t_2) + \dots + q_p Y(t_p)$$

$$= - \sum_{k=1}^p p(t_k) \log_2 p(t_k) \quad (9)$$

设置云计算环境下混合多样木马群中木马的数量是 m , 粒子辨别树中所有粒子的属性数目能够用 $w = \{w_1, w_2, \dots, w_w\}$ 表示, 根据粒子属性能够将木马对应的特征空间分割为 e 个子单元. 根据下述公式可以计算木马粒子群中粒子的信息熵:

$$L(b_i) = - \sum_{k=1}^m p_k \log_2 (q_k) \quad (10)$$

根据下述公式可以计算混合多样木马群中的木马密度分布特征值:

$$Y(D) = \sum_{l=1}^e \frac{|b_l|}{|F|} \times L(b_l) \quad (11)$$

设置混合多样木马群中木马特征的数目是 r , 利用下述公式可以计算云计算环境下混合多木马群中子单元的信息量:

$$L(r, n) = - \frac{r}{r+n} \log_2 \frac{r}{r+n} - \frac{n}{r+n} \log_2 \frac{n}{r+n}$$

$$B(D) = \sum_{k=1}^e \frac{r_k + n_k}{r + n} L(r_k, n_k) \quad (12)$$

根据下述公式可以计算云计算环境下混合多样木马群检测的信息增益:

$$\text{win}(D) = L(r, n) - B(D) \quad (13)$$

通过上面阐述的方法, 能够根据粒子群相关理论, 对云计算环境下的木马进行有效的分类处理, 为多样木马群检测提供数据基础. 建立粒子辨别树, 完成云计算环境下混合多样木马群的检测.

4 实验结果分析

为了评价不同的云计算环境下木马检测方法的有效性,需要进行一次实验.在实验的过程中,木马相关数据能够用表 1 进行描述.

表 1 木马类型数据表

木马类型	木马数目/个
normal	652
probe	127
dos	345
u2r	315

分别利用传统算法和本文算法进行云计算环境下混合多样木马群的检测,检测的效率能够用图 2 进行描述.

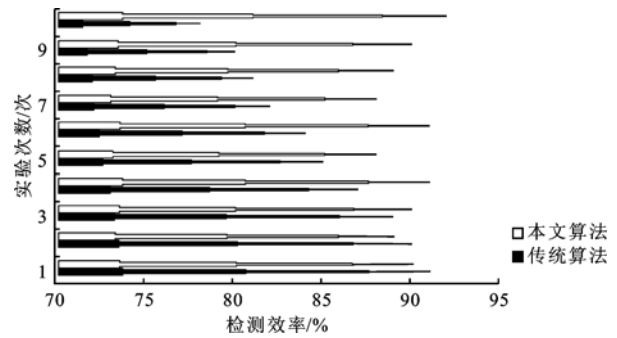


图 2 不同算法检测效率对比

根据图 2 可以得知,利用本文算法进行云计算环境下混合多样木马群检测,检测的效率高于传统算法,保证了检测的实时性.

在上述利用不同算法进行混合多样木马群检测的过程中,检测的漏检率能够用图 3 进行描述.

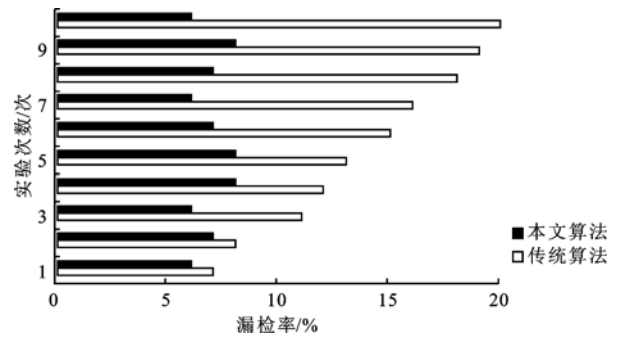


图 3 不同算法漏检率对比

根据图 3 能够得知,利用本文算法进行云计算环境下的混合多样木马群检测,检测的漏检率远远低于传统算法,充分展示了本文算法的优越性.

对上述实验过程中的相关数据进行整理分析,能够得到表 2 和表 3,如下所述.

表 2 传统算法实验数据表

实验次数	木马数量/个	检测效率/%	漏检率/%
1	12	91	7
2	18	90	8
3	23	89	11
4	34	87	12
5	42	85	13
6	48	84	15
7	53	82	16
8	58	81	18
9	61	80	19
10	63	78	20

表 3 本文算法实验数据表

实验次数	木马数量/个	检测效率/%	漏检率/%
1	18	90	6
2	19	89	7
3	23	90	6
4	25	91	8
5	34	88	8
6	41	91	7
7	48	88	6
8	52	89	7
9	66	90	8
10	78	92	6

利用本文算法进行云计算环境下的混合多样木马群检测,检测耗费的时间比传统算法短,检测效率高于传统算法,检测的漏检率低于传统算法,在时间和准确性上都展示了本文算法的优越性,能够最大限度的满足实际网络计算的需求.

5 结束语

本文提出了一种基于粒子辨别树算法的云计算环境下混合多样木马群检测方法.根据粒子群相关理论,对云计算环境下的木马进行有效的分类处理,为多样木马群检测提供数据基础.建立粒子辨别树,完成云计算环境下混合多样木马群的检测.实验结果表明,利用本文算法进行云计算环境下混合多样木马群检测,能够有效缩短检测时间,提高检测准确性.

参考文献:

- [1] Anjum F, Subhadrabandhu D, Sarkar S, et al. On optimal placement of intrusion detection modules in sensor networks [C]// 1st International Conference on Broadband Networks. Washington: IEEE Press, 2004: 433-439.
- [2] Subhadrabandhu D, Anjum F, Sarkar S. On optimal placement of intrusion detection modules in sensor networks [C]// Proceedings of the First International Conference on Broadband Networks. IEEE, USA: 2004: 690-699.
- [3] Mohammad Saniee Abadeh, Jafar Habibi, Zeynab Barzegar, et al. A parallel genetic local search algorithm for intrusion detection in computer networks [J]. Engineering Applications of Artificial Intelligence, 2007, 20(8):1058-1069.
- [4] 苏高利, 邓芳萍. 关于支持向量回归机的模型选择 [J]. 科技通报, 2006, 22(2):154-158.
- [5] 肖海军, 洪帆, 张昭理, 等. 基于融合分类和支持向量机的入侵检测研究 [J]. 计算机仿真, 2008, 25(4):

130-132.

- [6] 张新有, 曾华荣, 贾磊. 入侵检测数据集 KDD CUP 99 研究 [J]. 计算机工程与设计, 2010, 31(22): 4809-4816.
- [7] 卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述 [J]. 通信学报, 2004, 25(7):19-21.
- [8] 梁英, 曾鹏, 于海斌. 无线传感器网络中一种能量自适应的簇首选择机制 [J]. 信息与控制, 2006, 35(2): 141-146.
- [9] 刘韬, 皮国强. 人工免疫算法在网络入侵检测中的应用 [J]. 计算机仿真, 2011(11):91-94.
- [10] 马燕, 范植华. 基于神经网络的基因分类器 [J]. 计算机工程与设计, 2005, 26(2):308-311.

作者简介:

金显华 女, (1979—), 硕士, 讲师. 研究方向为图形图像处理.

赵元庆 男, (1976—), 硕士, 讲师. 研究方向为计算机软件与理论.

(上接第 131 页)

辑链中的传播特性. 在以后工作中, 将利用本文中的一些结论去研究如何用 FPGA 布局布线的传输特性模拟相同工艺条件下的 ASIC 布局布线特性, 从而达到提高对被测电路软错误率的预测精度.

参考文献:

- [1] Velazco R, Rezgui S, Ecoffet R. Predicting error rate for microprocessor-based digital architectures through CEU (Code Emulating Upsets) injection [J]. IEEE Transactions on Nuclear Science, 2000, 47(6): 2405-2411.
- [2] Gadlage M J, Ahlbin J R, Narasimham B, et al. Scaling trends in SET pulse widths in sub-100 nm bulk CMOS processes [J]. IEEE Transactions on Nuclear Science, 2010, 57(6):3336-3340.
- [3] Ferlet-Cavrois V, Paillet P, McMorow D, et al. New insights into single event transient propagation in chains of inverters-Evidence of propagation-induced pulse broadening [J]. IEEE Transactions on Nuclear Science, 2007, 55(6):2338 - 2346.
- [4] Celia López-Ongil, Mario García-Valderas, Marta Portela-García, et al. Autonomous fault emulation: a new

FPGA-based acceleration system for hardness evaluation [J]. IEEE Transactions on Nuclear Science, 2007, 54(1):252-261.

- [5] Narasimham B, Gadlage M J, Bhuvu B L, et al. Test circuit for measuring pulse widths of single-event transients causing soft errors [C]//IEEE International Conference on Microelectronic Test Structures. Edinburgh: IEEE, 2008:142-146.
- [6] Gadlage M J, Schrimpf R D, Benedetto J M, et al. Single event transient pulse widths in digital microcircuits [J]. IEEE Transactions on Nuclear Science, 2004, 51(6):3285-3290.
- [7] Cavrois V F, Pouget V, McMorow D, et al. Investigation of the propagation induced pulse broadening (PIPB) effect on single event transient in SOI and Bulk Inverter Chains [J]. IEEE Transactions on Nuclear Science, 2008, 55(6):2842-2853.

作者简介:

叶世旺 男, (1989—), 硕士研究生. 研究方向为 IC 抗辐射加固技术.

周婉婷 女, (1982—), 博士. 研究方向为 IC 抗辐射加固技术.