

# 一种新的网络攻击检测方法

赵攀, 江宁波, 邱玲

(四川理工学院计算机学院, 四川 自贡 643000)

**摘要:**为了有效判断网络数据包是否存在被攻击的可能性,在以往的研究基础上提出了一种新的检测算法 DMPSO。该算法根据数据包属性的离散度定义了状态检测指标,并利用粒子群优化方法给出了标准差分布的计算流程,以此判断数据包的异常状况。最后,进行仿真实验,对比了与其它算法之间的性能状况,结果表明 DMPSO 具有较好的适应性。

**关键词:**网络攻击;检测;变异算子;数据包;标准差;粒子群优化

**中图分类号:**TP393

**文献标志码:**A

## 引言

越来越多的网络攻击给用户带来了极大的安全隐患,如何有效地检测和防御攻击成为当前网络安全领域研究的热点和重点<sup>[1]</sup>。传统的网络攻击检测方法,主要集中在量化分析和数据统计方面,存在检测精度不高、检测方法单一等问题,正逐步显现其缺点和不足<sup>[2-4]</sup>。

粒子群优化(Particle Swarm Optimization, PSO)算法是一种基于群体智能的全局优化进化算法,广泛应用于函数寻优、神经网络训练、模式分类、模糊系统控制和工程应用领域<sup>[5]</sup>。传统的 PSO 算法在执行后期,所有粒子方向一致速度趋近于零,导致局部最优和出现过早收敛,进而使优化效果无法达到最佳。很多学者对此进行研究,取得了一些改进,但效果有限。文献[6]引入了基于遗传算法中基因突变的观点,保持粒子飞行的多样性,但这种突变是被动的,而且会以很高的概率再次被吸引回以前的最优解,效率低下。文献[7]提出了额外生成与迭代次数相同的粒子,利用适应度值保存粒子历史最优值。虽然也改善了粒子多样性,但这种方法以显著增加计算量和牺牲系统内存为代价。文献[8]基于随

机系统的矩方程法来分析连续型 PSO 算法的均方收敛性,充分考虑了随机因素,给出了保证算法均方收敛域。文献[9]将自适应加速度系数调整策略引入到 PSO 中,以有效地控制全局和局部搜索,同时根据种群适应度方差对陷入早熟收敛的粒子进行混沌扰动,提高算法收敛的精度,但误报率有待进一步提高。

在上述研究的基础上,本文基于粒子群优化算法提出了一种新的检测方法,即结合变异算子来改进粒子群优化算法的缺陷,以此提高检测网络攻击的成功率。首先结合数据包属性的离散度给出了检测指标,同时通过获得数据包属性的标准差分布来判断是否存在被攻击的可能性。最后,进行仿真实验,对比研究了该算法与其它算法之间的性能状况。

## 1 网络攻击状态检测指标

将 HTTP 协议中数据包看作遵循一定标准的字符串,具有  $k$  个通用属性的数据域组成,令数据包  $Y = [y_1, y_2, \dots, y_k]$ , 其中  $y_k$  表示 Data 头部,主要包括 Host 地址、源端 IP 地址、目的端 IP 地址等。对于  $n$  个数据包的样本集合  $Z = [Y_1, Y_2, \dots, Y_n]$ , 则可以表示为:

收稿日期:2014-05-04

基金项目:四川省教育厅重点项目(13ZA0118);人工智能四川省重点实验室开放基金项目(2012RYY02);四川理工学院培育项目(2012PY13);企业信息化与物联网检测技术四川省高校重点实验室项目(2013WYJ01)

作者简介:赵攀(1976-),男,四川自贡人,副教授,硕士,主要从事计算机网络通信与数据处理方面的研究,(E-mail)zhaopan827@gmail.com

$$Z = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1k} \\ y_{21} & y_{22} & \cdots & y_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & \cdots & y_{nk} \end{bmatrix} \quad (1)$$

那么,这  $n$  个数据包第  $k$  个属性可采用序列  $Z_k = [y_{1k}, y_{2k}, \dots, y_{nk}]$  表示。令第  $k$  个属性的离散度为  $\beta(Z_k)$ , 则整个样本集合的离散度  $\beta(Z)$  为:

$$\beta(Z) = \frac{1}{k} \sum_{i=1}^k \beta(Z_i) \quad (2)$$

同时,假设某属性  $k$  的平均离散度为  $\overline{\beta(Z_k)}$ , 这里采用标准差  $\lambda$  来刻画数据包属性与整体平均离散度之间的偏差:

$$\lambda = \sqrt{\frac{1}{n} \sum_{i=1}^n (\beta(Z_{ik}) - \overline{\beta(Z_k)})^2} \quad (3)$$

$\lambda$  越大意味着该数据包与标准样本偏离越远,越有可能被攻击篡改信息。

## 2 算法描述

具体算法 DMP SO (Detection Method based of Particle Swarm Optimization) 如下所述:

(1) 在开始时刻初始化网络参数,并确定粒子群规模  $n$ , 产生粒子群的初始位置  $s(i,0)$  和初始速度  $v(i,0)$ 。

(2) 将待检测某数据包  $Y = [y_1, y_2, \dots, y_k]$  视作粒子  $i$ , 判断当前粒子  $i$  的标准差  $\lambda$  是否小于阈值  $\lambda_{\max}$ , 如果不满足则根据式(4)和式(5)所示的变异算子替换  $s(i,0)$ , 否则保持不变。

$$s(i, t+1) = s(i, t) + (s(\max, t) - s(\min, t)) \cdot (1 - \text{rand}())^{\varphi} \quad (4)$$

其中,  $s(\max, t)$  和  $s(\min, t)$  分别为粒子位置  $s(i, t)$  的边界,  $\varphi$  为变异分布指数,  $\text{rand}()$  为(0,1)之间的随机数。

(3) 按照式(5)所示的适应度函数计算粒子  $i$  的适应值  $f(\lambda)$ , 并将粒子  $i$  的最佳位置  $s_{opt}$  确定为当前位置, 同时暂时令  $s_{opt}$  为种群的最佳位置  $s_o$ 。

$$f(\lambda) = \frac{1}{1 + e^{-\lambda}} \quad (5)$$

(4) 根据当前最佳位置  $s_{opt}$ , 结合式(6)和式(7)更新粒子的位置和速度,

$$v(i, t) = v(i-1, t) + \eta |s_{opt} - s(i, t)| \cdot (1 - \text{rand}()) \quad (6)$$

$$s(i, t) = s(i-1, t) + v(i-1, t) \Delta t \quad (7)$$

其中,  $\eta$  为状态更新参数,  $\eta > 0$ 。

(5) 如果粒子  $i$  的标准差  $\lambda$  小于阈值  $\lambda_{\max}$  则跳转到步骤(6), 否则以  $s(i, t)$  作为初始点, 采用变异算子计算的结果替换  $s(i, t)$ , 并重新计算其适应度。

(6) 判断粒子  $i$  的适应度是否优于  $s_{opt}$  的适应度, 如果是则令  $s_{opt}$  为粒子  $i$  的适应值。

(7) 判断粒子  $i$  的适应度是否优于  $s$  的适应度, 如果是则令  $s$  为粒子  $i$  的适应值。

(8) 输出当前粒子的标准差  $\lambda(i)$ , 并令  $i = i + 1$ , 跳转到步骤(2)重复计算, 直至获得所有粒子标准差分布  $\lambda = [\lambda(1), \lambda(2), \dots, \lambda(k)]$ , 同时判断每个  $\lambda(i)$  是否超出规定阈值, 如果超出存在被攻击的可能性。

(9) 算法结束。

## 3 仿真实验

针对上述改进的 DMP SO 算法, 本文利用 OPNET 和 MATLAB 进行仿真实验来验证其有效性。这里基于 OPNET 建立如图 1 所示的仿真拓扑结构, 其网络参数设置为: 每个数据包大小为 512 b, 链路带宽为 20 M, 每个网络节点缓冲区为 1024 Kb, 延时 10 ms。其中, 节点  $S$  作为数据源端 (IP 地址设为 192.168.0.1), 节点  $D$  作为数据接收端 (IP 地址设为 192.168.0.100), 节点  $f$  为攻击源 (IP 地址设为 192.168.0.2), 不定期向网络中发动攻击 (包括 DoS、Probe、R2L 和 U2R 等), 其余为中转节点 (从节点  $a$  到节点  $g$  的 IP 地址分别设为 192.168.0.3 到 192.168.0.9)。设置粒子群规模  $n = 100$ , 变异分布指数  $\varphi = 0.5$ , 状态更新参数  $\eta = 2$ 。令节点  $S$  处每秒发送 1000 个数据包到节点  $D$ , 每个数据包  $Y = [y_1, y_2, y_3]$ , 其中,  $y_1$  表示数据包长度,  $y_2$  表示数据包时间戳,  $y_3$  表示数据包源端地址。在节点  $D$  处设置监听, 收集从节点  $S$  发送的数据包并进行状态分析, 令节点  $f$  发动 DoS 攻击。

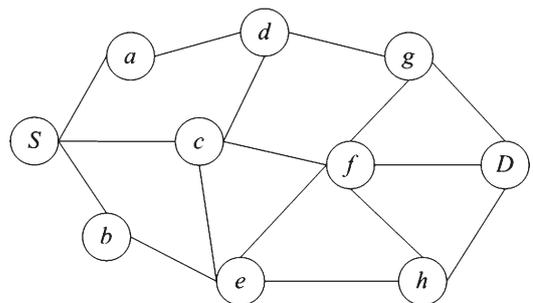


图1 网络拓扑结构图

将 DMP SO 算法、DMCM 算法、文献[10]提出的 IHMM 算法以及节点  $D$  处实际监听的结果进行对比, 图 2 显示了其数据包长度检测的情况。从图 2 可以看出,

DMP SO 算法检测的数据包长度状态  $y_1$  与节点  $D$  处实际监听结合比较接近,其次是 DMCM 算法。对检测数据进行数据分析,DMPSO、DMCM、IHMM 与实际结果的误差分别为:3.62%、5.05%和 8.28%。

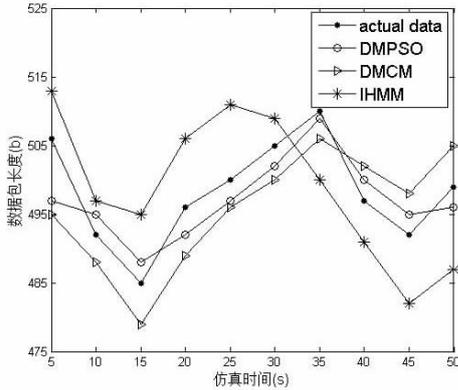


图 2 数据包长度检测结果比较

其次,图 3 给出了在上述仿真环境下,DMPSO、DMCM 和 IHMM 这三种算法的数据包长度标准差  $\lambda$  变化情况。从图 3 可以看出,在实验进入平稳过程后(仿真时间 15 s 后),DMPSO 所对应曲线的标准差小于其余两种算法。并且从标准差的抖动情况来看,DMPSO 也趋于稳定,而 IHMM 对应曲线的抖动较大。

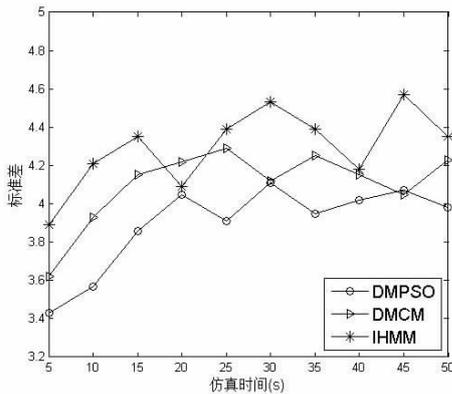


图 3 数据包长度标准差比较

表 1 给出了当节点  $f$  分别发动 DoS、Probe、R2L 和 U2R 攻击下,DMPSO、DMCM 和 IHMM 算法的检测成功率、漏报率以及误报率对比情况。从表 1 可以看出,本文改进的 DMPSO 算法性能较 DMCM 和 RETMMAD 算法有了明显的提高。

#### 4 结束语

为了有效判断网络是否存在被攻击现象,本文在以往研究的基础上利用粒子群优化算法提出了一种新的检

表 1 不同攻击种类下检测结果比较

算 法		DoS	Probe	R2L	U2R
DMPSO (%)	成功率	95.43	91.15	89.03	84.23
	漏报率	4.57	8.75	9.02	15.77
	误报率	0	0	2.95	0
DMCM (%)	成功率	95.17	89.21	86.75	82.69
	漏报率	4.83	10.79	9.54	17.31
	误报率	0	0	3.71	0
IHMM (%)	成功率	91.85	86.41	83.68	80.12
	漏报率	9.15	13.59	11.09	19.88
	误报率	0	0	5.23	0

测算法 DMPSO。首先该算法结合数据包属性的离散度和标准差定义了数据包样本判别指标,同时基于粒子群优化算法给出了其标准差分布的计算流程。最后,通过仿真实验对比研究了该算法与 DMCM 算法、IHMM 算法在不同攻击种类下的性能状况,结果发现 DMPSO 具有较好的适应性。在后续研究中,可以考虑结合多种网络环境来建立诸如 DoS、Probe、R2L 和 U2R 等各类攻击的检测方法,以此建立完善的评价体系结构。

#### 参 考 文 献:

- [1] Wang W, Daniels E. A graph based approach toward network forensics analysis[J]. ACM Transactions on Information and System Security, 2008, 12(1): 1-33.
- [2] Claudno E C, Abaelouahab z, Teixeira M M. Management and integration of information in intrusion detection system: data integration system for IDS based multi-agent systems[C]//Proceeding of 2006 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology Workshops, Hong Kong, December 18-22, 2006: 49-52.
- [3] 全亮亮, 吴卫东. 基于支持向量机和贝叶斯分类的异常检测模型[J]. 计算机应用, 2012, 32(6): 1632-1635.
- [4] 周东清, 张海峰, 张绍武, 等. 基于 HMM 的分布式拒绝服务攻击检测方法[J]. 计算机研究与发展, 2005, 42(9): 1594-1599.
- [5] Yamille D V, Ganesh K V. Particle swarm optimization: basic concepts, variants and applications in power systems[J]. IEEE Transactions on Evolutionary Computation, 2008, 12(2): 171-195.
- [6] Asanga R, Samma K H. Self-organizing hierarchical particle swarm optimizer with time-varying acceleration coefficients[J]. IEEE Transactions on Evolutionary Computation, 2004, 8(3): 240-255.

(下转第 28 页)