doi: 10.3969/j.issn.0490-6756.2018.04.016

基于量子谐振子的 RoQ 攻击识别方法

邓怀勇[1], 马　琴[1], 陈国彬[2], 张广泉[3,4]

(1. 重庆水利电力职业技术学院, 重庆 402160; 2. 重庆工商大学融智学院, 重庆 400033;
3. 苏州大学计算机科学与技术学院, 苏州 215006; 4. 中国科学院计算机科学国家重点实验室, 北京 100080)

摘　要: 针对当前降质服务攻击给 TCP 服务质量带来的问题,提出了一种基于量子谐振子算法的 RoQ 攻击识别方法.该方法以量子谐振子为载波,计算量子谐振子从高能态向基本态转变过程,以此监测统计异常网络流和数据包丢失变化,对降质攻击进行识别.实验结果表明,该方法能够有效刻画漏检率、丢失率等参数变化,准确识别降质攻击.

关键词: 降质服务; 降质攻击; 识别; 量子谐振子

中图分类号: TP393　　**文献标识码**: A　　**文章编号**: 0490-6756(2018)04-0752-05

The RoQ attack recognition method based on quantum harmonic oscillator

DENG Huai-Yong[1], *MA Qin*[1], *CHEN Guo-Bin*[2], *ZHANG Guang-Quan*[3,4]

(1. Chongqing Water Resources and Electric Engineering College, Chongqing 402160, China;
2. Rongzhi College, Chongqing Technology and Business University, Chongqing 400033, China;
3. Computer Science and Technology, Soochow University, Suzhou 215006, China;
4. Computer Science, Chinese Academy of Sciences, Beijing 100080, China)

Abstract: In order to improve the current degradation of service attacks to reduce TCP's service quality, a RoQ attack recognition method is presented by quantum oscillator algorithm. In this method, the quantum harmonic oscillator is set as the carrier, and is calculated the transition from high-energy state to the base state of quantum oscillator. So, the abnormal network traffic and the change of packet loss aremonitored and counted, and the degraded attack is identified. The experiment results show that, this method caneffect depict the factors, such as missed inspectionrate and loss rate, and accurately identify the degraded attack.

Keywords: Reduction of quality; Degraded attack; Recognition; Quantum harmonic oscillator

1　引　言

随着网络时代的发展,信息的传递不断加快,人们依赖于无线网络的使用也越来越多,对于网络的安全性能要求也越来越高.非法用户常常使用降质服务(Reduction of Quality,RoQ)来攻击网络,因此研究人员不断提出新的构思以及算法来优化网络安全性能,达到提高网络安全使用的目的[1-3].传统研究更多集中在 DDoS 攻击,而 RoQ 攻击作为当前流行的网络攻击手段,日益受到研究人员重视.

RoQ 攻击是一种非典型的拒绝服务的降质攻

收稿日期: 2017-07-07
基金项目: 中国科学院计算机科学国家重点实验室开放课题(CSYSKF0908); 江苏省自然科学基金(BK2011152); 重庆市教委科学技术研究项目(KJ1601903); 重庆水利电力职业技术学院科研项目(K201506).
作者简介: 邓怀勇(1979－), 男, 副教授, 硕士, 研究方向为物联网.
通讯作者: 陈国彬. E-mail: Darnell66@hainan.net

击，包括了脉冲攻击、循环攻击、自耗攻击和泛攻击，RoQ 攻击的特点有以下 4 个：(1) 攻击目标不具体明确；(2) 攻击效果不明显；(3) 攻击成本不高；(4) 攻击特征较为独特，隐蔽性强. 实验数据显示，在同等条件下，遭受攻击时数据流增加到原来的 5 倍，受害流吞吐率下降到原来的 77.42%，而延迟抖动增加到原来的 110 倍. RoQ 攻击主要分为单链路和多链路两种，都属于非典型的拒绝服务攻击[4]. 它们是通过短时间间隔里发送大量数据包来降低 TCP 服务质量，由于环境的复杂性，这种攻击较于传统的拒绝服务攻击具有更好的隐蔽性和多变性. 现有的研究大多集中于单链路网络的攻击与检测[5]，针对于多链路的研究较少. 文献[6]中提出了基于广义熵和信息距离在分离度上提出了一种检测方法，用于检测计算链路受到 RoQ 攻击后的流量变化情况，达到分析攻击流的信息度变化目的；文献[7]提出一种采用负熵作为目标函数的攻击流特征检测算法，建立分离算法盲源分离数学模型，达到快速分离源信号的目的；文献[8]提出了分数阶傅立叶变化和离散傅立叶变化，分析攻击数据的时频特征，但是在传统路由器网络模型中难以开展；文献[9]采用自相关分析法提取 RoQ 攻击数据的周期性特征，进而研究了 RoQ 攻击的可阻止性；文献[10]针对拥塞的 RoQ 攻击原理的基础，对比和 DDoS 拒绝服务攻击的原理，建立系统化模型进行系统化分类讨论研究；文献[11,12]提出了基于快速 ICA(Independent Component Analysis)的攻击流特征提取算法，但是该算法只能在算时间内发送数据包；文献[13]采用牛顿迭代法有效降低问题的复杂度，但由于 RoQ 攻击的隐蔽性问题，导致该方法比较片面；文献[14]基于 DoS 攻击模型的基础，利用小波在速率较低的特征，刻画了 RoQ 攻击时的攻击流和其他的数据流变化，将两者分隔开研究从而得到一种的诊断模型. 以上方法都存在漏检率高，成本开销大，计算较为繁琐等问题.

在上述工作的基础上，本文根据双链路提出了基于量子谐振子算法的 RoQ 攻击识别方法. 它具有检漏率高、成本低以及易操作的特点，在识别降质攻击的原则上，能反应敏捷地识别攻击，提高网络安全度，使得针对于无线网络的使用性能有所提高.

2　一种 RoQ 攻击识别模型

假设 Y 表示一段统计的时间刻度，将 Y 分割为 k 个长度为 z 的子序列 a_k，定义 k 个子序列的数学期望和 $D(a_k)'$ 函数，可得

$$Y(a_k) = \frac{1}{z}\sum_{j=1}^{z} a_j (0 < z < \left|\frac{m}{k}\right|), kz = m \tag{1}$$

$$D'(a_k) = \frac{1}{x}\sum_{j=1}^{x}[y_j - E(a_k)]^2 (0 < z < \left|\frac{x}{k}\right|), kz = s \tag{2}$$

这里定义 TOD 流度量矩阵 $X_{(X_{ij})}$，其中 X_{ij} 表示第 j 个 TOD 流在第 i 个记录时间间隔内的流量值，对 TOD 流进行 m 次采样得到 $X = [X_1, X_2, \cdots, X_m]$，如下式所示.

$$T_{a,n,\delta} = F_{a,n-1,\delta}\frac{a(n-1)}{n-a}F_{an-1,\delta} \tag{3}$$

由此可得采样值，并利用式(4)来刻画异常子序列下的网络流变化，如下式.

$$T^2_{(m)} = t^{F_{an-1,\delta}\frac{a(n-1)}{n-a}F_{an-1,\delta}}_{(m)} \Lambda^{-1} t_{(m)} \frac{\sqrt{a}}{\pi^{\frac{1}{4}}} e^{-\frac{a^2x^2}{2}} \tag{4}$$

其中，n 表示全部特征个数；a 表示异常个数；δ 为显著水平；$F_{a,n-1,\delta}$ 为显著水平 δ 且自由度为 $a(n-1)$ 条件下的 F 分布临界值；Λ 是对应特征值所构成的对角阵；T^2 是统计标量，反应过程自变量的变化情况，当 $T^2 \approx 7.8$ 查表得当临界值超过 99%时，网络流出现异常.

若攻击速率为 V，攻击时长 L，攻击周期 t，采用傅立叶交换技术把时间域序列变换成数据包的流量域，在某一确定范围内检测 RoQ 攻击，采样时间为 i 秒内的采样数据包设为 $x(n)$，$x(n)$ 为时间序列，则根据式(5)～(7)刻画 TCP 流量域的变化.

$$x(n) = \sum_{i=1}^{n}(100(x_{i+1} - x_i^2)^2 + (x_i - 1)^2) \tag{5}$$

$$DET(x(n), M) = \frac{1}{N}\sum_{K=1}^{N-1} x(n) e^{\frac{-j2\pi Mk}{N}} \sum_{i=1}^{\beta} \frac{1}{\sqrt{2\pi}\alpha\beta} e^{-\frac{(x-x_i)^2}{2a^2}} \tag{6}$$

其中，$M=0, 1, \cdots\cdots, N-1$. 通过对 $x(n)$ 简单的(0,1)替代简单离散傅立叶变化，结合式(1)和式(2)分析数据流量在整个过程中的异常子序列漏检率

$$P = \frac{1}{4000}\sum_{i-1}^{n} DET(x(n), M)^2 - \prod_{i-1}^{n}\cos\left(\frac{x(n)}{\sqrt{n}}\right) + 1 \tag{7}$$

假设 E_X 接收的数据情况为 X,刻画在某吞吐量范围内 TCP 数据包的丢失率 κ. $X=\{x_{11},x_{12},\ldots,x_{ij},\ldots,x_{n1},x_{n2}\}$,$1\leqslant i\leqslant n$,$j=1,2$,在 i 个流量包的第 j 个短分组成功到达 E_X,记为 $x_{ij}=1$,否则 $x_{ij}=0$. 同理 E_Y 的分组 $Y=\{y_1,\ldots,y_k,\ldots,y_n\}$,$1\leqslant k\leqslant n$,当第 k 个长分组成功到达 E_Y 时,记为 $y_k=1$,否则 $y_k=0$,根据两条链路的收包情况,计算根节点与父节点链路上的丢包率,如下式.

$$\kappa=\frac{\xi_1\sum_{i=1}^{n}\sum_{j=1}^{2}x_{ij}+\xi_2\sum_{k=1}^{n}y_k}{n(2\xi_1+\xi_2)} \tag{8}$$

其中,ξ_1,ξ_2 分别表示短分组和长分组的包长;n 表示源节点发送流量包的总长. 实验数据表明,当客户端受到攻击时会产生短时间内较大范围的拥堵,流量域增大. 通过刻画网络攻击脉冲异常子序列、异常网络流、TCP 数据包的丢失率对 RoQ 攻击进行识别.

3 基于量子谐振子算法的攻击识别方法

本文主要通过量子谐振子算法[15-18]对 RoQ 攻击识别进行分析,该算法具备好的寻优能力和收敛性,在基态最稳定且呈高斯曲线分布,寻优概率较高. 令

$$|\Gamma_n(x)|^2=\frac{1}{\sqrt{2^n n}}H_n(\alpha x)e^{-\frac{m\omega x^2}{2\hbar}}\left(\frac{m\omega}{\pi\hbar}\right)^{\frac{1}{4}} \tag{9}$$

其中,$\Gamma_n(x)$表示波函数;n 表示能级数;H 为哈密顿算符;m 表示粒子的广义质量;ω 表示粒子的振动频率;$\hbar$ 为普朗克常量,满足能量公式如下.

$$E=n\hbar\omega+\frac{1}{2}\hbar\omega \tag{10}$$

假设在一维空间内,将一定条件下的量子谐振子的运动轨迹和网络信号变化进行对比,利用式(1)和式(2)的统计捕捉异常子序列 $Y(a_k)$,根据薛定谔方程变形定义攻击脉冲持续时间 $T_n(x)$,如下式.

$$|T_n(x)|^2=\frac{1}{x}\sum_{j=1}^{x}[y_j-E(a_k)]^2\frac{1}{2^n n!}\left(\frac{m\omega}{\pi h}\right)^{\frac{1}{2}}e^{-\frac{a^2x^2}{2}}|H_{n(ax)}|^2 \tag{11}$$

根据式(3)和式(4)确定异常网络流 a_k,计算检测率 χ,如下式.

$$\chi=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\alpha_k e^{-\alpha m w}\mathrm{d}\omega\lim_{n\to\infty}\frac{n!}{(n-r)!} \tag{12}$$

这里将数据流变化看作一个微观振动过程,构造刻画流量域函数 $\Phi_{\Psi(x)}$,如下式.

$$\Psi(x)=A_n e^{-ax^2/2}H_n(ax)(\Psi_0=A_0e^{-a^2x^2/2}) \tag{13}$$

$$\Phi_{\Psi(x)}=\left[\frac{M\omega^2x^2}{2}+\left(-\frac{t^2}{2m}\frac{L^2}{Lx^2}\right)\right]\Psi(x) \tag{14}$$

其中,X 是周期性运动的一个状态点;$H_n(ax)$是一个基于量子谐振子的 Hermite 多项式. 根据上述方法,这里提出如下识别算法.

Step 1 初始化参数,设定迭代特征次数 n 等参数;

Step 2 从某一时间点开始建立采样序列 $X=[X_1,X_2,\cdots,X_p]$,在核心路由、网关、终端接收 TCP 数据包;

Step 3 在某一段时间内的持续脉冲,捕捉异常序列 $D'(a_k)$,利用式(1)和式(2)将序列进行统计分析,将统计结果交给下一层;

Step 4 结合式(3)和式(4)识别攻击信号和合法信号 $\zeta_x=\sum_{m=1}^{x}T_{a,n,\delta}$,若 ζ_x 是合法信号,则跳转到 Step 8,否则跳转到 Step 5;

Step 5 如果 $\zeta_x^2(x)>T_{(m)}^2$,出现异常网络流,输出并启动监听,实时记录每一步骤;结合傅立叶变换和式(5)分析异常网络流,判断拥堵情况;否则标记为正常信号,监听结束;

Step 6 如果流量域 $DET(x(n),M)$ 的变化明显产生拥堵,那么服务质量下降;否则进行攻击识别,调用特征进行比较,监听结束;

Step 7 结合式(6)和式(7),基于算法的寻优率,并利用式(8)、式(11)~(13)刻画攻击网络流、丢包率情况,生成攻击特征数据反馈给管理员,结束监听;

Step 8 统计目标序列的特征情况,输出结果;

Step 9 算法结束.

4 仿真实验

为了验证基于量子谐振子算法识别方法的有效性,本文利用 Matlab 进行数据仿真实验,首先建立 RoQ 攻击和无攻击的仿真环境,注入标记攻击流,并提前分析测量数据的主成分[18],规划 p 个 TOD 流,基于量子谐振子算法提取攻击特征. 假设在该仿真场景中,建立一个有 100~150 个节点的 Base T 网,设置一个攻击者工作站,初始化时伪装

成普通站点，第 50 s 开始攻击，三个受害服务端，部署两台 Cisco4000 路由器，背景流量设置访问 web，ftp，email 服务，带宽为 10 Mbps，相互之间的链路为网络瓶颈，设置攻击时间为第 50 s，攻击周期为 1.25 s，脉冲持续时间在 0.1～0.27 s 之间. 实验通过调整正常用户的数量，设定随机对象，判断模拟攻击是否有效，根据式(4)计算 T^2 统计量，

在判定过程中出现 T^2 超出相应的控制限，如图 1 所示，可以判定该过程攻击网络流导致出现攻击现象，可以刻画攻击特征. 在攻击状态下，比较降质服务数据流特征变化，设置 0～1000，如图 2 所示，工作站在第 50 s 发出攻击流，捕捉被攻击服务器的流量，可以看出 RoQ 攻击发起后，网络数据流经过服务器波动较正常值有所波动，但平均波动值不大.

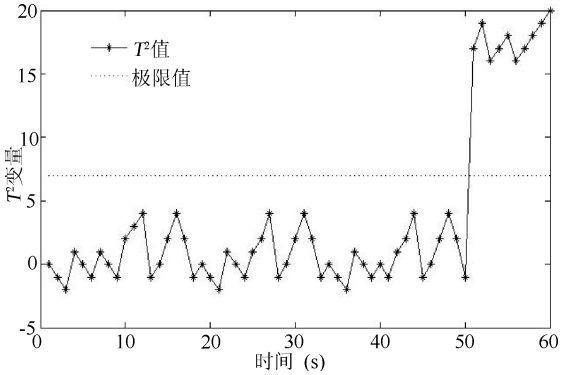

图 1　T^2 统计量

Fig. 1　The statistics of T^2

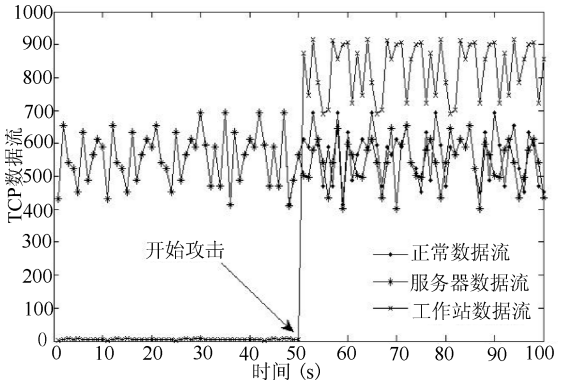

图 2 TCP 数据流变化情况

Fig. 2　The changes of TCP data flow

因为数据流的攻击特征容易被正常用户淹没，本文利用量子谐振子算法的寻优特性，将捕捉到的数据进行分析攻击特征提取识别. 实验使用 50 组含有 RoQ 攻击特征和 50 组正常数据流量的特征组成样本集，初始化时样本差别不大，随着 RoQ 的持续，可以看出本文算法的寻优和稳定特点. 下文将与蚁群算法相比(如图 3 所示)，相同时间段得到的数据分析比较，基于量子谐振子算法模型的丢包率较低，稳定性更强，从 15MB 开始，可以明显看到基于蚁群算法的识别模型丢包率开始明显上升，而基于量子谐振子算法的识别模型始终平缓变化，且平均值没有超过正常丢包率.

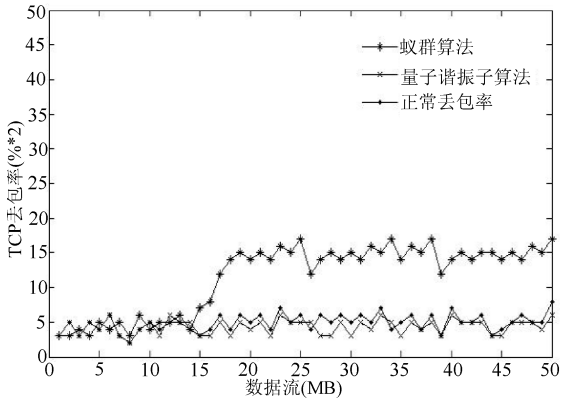

图 3　数据包丢失比较

Fig. 3　The comparison of packet loss

对节点数据进行捕捉分析，如图 4 所示，在 0～16 MB 阶段，检测数据变化平缓，但是随着数据流的增大，网络流量的加剧，异常网络流的捕捉在 22 MB 左右开始出现优势，检测率开始规律性变化，并且高于蚁群算法的平均检测率.

对采集的 P 组序列 $X=[X_1,X_2,\ldots,X_P]$ 进行分析，得到异常子序列，如图 5 所示，和正常得到的子序列的漏检率相比较，基于量子谐振子算法的识别模型平缓变化，低于基于蚁群算法的识别模型，不会受到数据流加剧的影响.

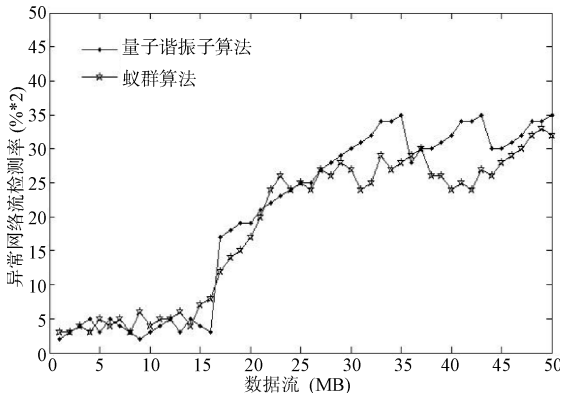

图 4　异常网络流比较

Fig. 4　The comparison of abnormal network flow

5　结　论

RoQ 攻击具有隐蔽性强等特点，因此在实际环境中难以有效识别. 对此，本文基于量子谐振子

算法,通过设置虚拟站点的形式捕捉特征,并监测统计异常子序列,得到异常网络流和数据包丢失变化等,在仿真实验中刻画数函数变量的漏检率、丢失率、检测率,同时利用 Maltab 平台进行仿真,模拟实际研究正常情况下的 T^2 和异常攻击时的变化,提取出降质服务攻击产生的数据特征,不断更新生成历史记录,实现识别攻击的优化和高效.通过仿真实验证明,本文的攻击识别特征明显,能有效识别降质服务攻击.

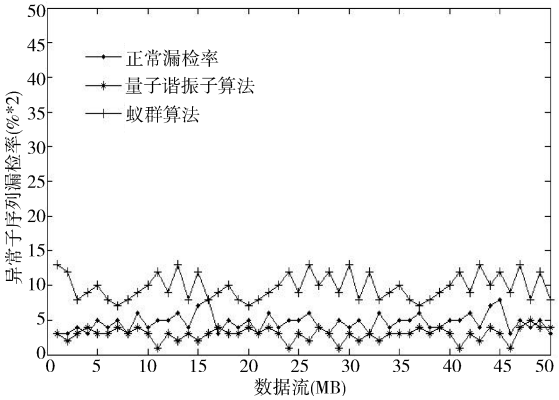

图 5 异常子序列比较

Fig. 5 The comparison of abnormalsubsequence

参考文献:

[1] 胡云山,申意,曾光,等. 针对减宽 SHA-1 算法的模差分攻击分析[J]. 四川大学学报:自然科学版,2016,53:1041.

[2] Yang H, Luo H, Ye F. Security in mobile ad hoc network: Challenge and solution[J]. IEEE Wirel Commun, 2004, 11: 38.

[3] 施江勇,鲜明,王会梅,等. 基于随机 Petri 网模型的降质服攻防效果评估[J]. 计算机科学,2014,41:58.

[4] 文坤,杨家海,张宾. 低速率拒绝服务攻击研究与进展综述[J]. 软件学报,2014,25:591.

[5] 文坤,杨家海,程凤娟,等. 骨干网络中 RoQ 攻击的检测、定位和识别[J]. 计算机研究与发展,2015,52:813.

[6] Yang X, Ke L, Wan L. Low-rate DDoS attacks detection and traceback by using new information metrics [J]. IEEE Trans Inf Foren Sec, 2011,6: 424.

[7] 彭天炜. 采用负熵目标函数和自相关成分的攻击流检测[J]. 科技通报,2014,30:83.

[8] 邓兵,陶然,平殿发. 基于分数阶傅里叶变换补偿多普勒徙动的动目标检测算法[J]. 兵工学报,2009,30:1034.

[9] Chang Y L, Lin T L. Network-based AVC whole frame loss visibility model and frame dropping methods [J]. IEEE Trans Image Process, 2012, 21: 3353.

[10] 任炜,刘腾红,金海. 移动 Ad Hoc 网络中针对拥塞的 RoQDDoS 攻击及其防御[J]. 计算机研究与发展,2006,43:1927.

[11] 欧世峰,高颖,赵晓晖. 自适应组合型盲源分离算法及其优化方案[J]. 电子与信息学报,2011,33:1243.

[12] 荣宏,王会梅,鲜明,等. 基于快速独立成分分析的 RoQ 攻击检测方法[J]. 电子与信息学报,2013,35:2307.

[13] 付小红,杨小牛,刘乃安. 基于四阶累积量的稳健的通信信号盲分离算法[J]. 电子与信息学报,2008,30:1853.

[14] Ralph A. Recognizing emotion from facial expressions: psychological and neurological mechanisms [J]. Behav Congitive Neurosci Rev, 2002, 1: 21.

[15] 王鹏,黄焱,任超,等. 多尺度量子谐振子高维函数全局优化算法[J]. 电子学报,2013,41:2465.

[16] 黄焱,王鹏,程琨,等. 多尺度量子谐振子优化算法的并行性研究[J]. 通信学报,2016,37:67.

[17] 王鹏,黄焱,袁亚男,等. 多尺度量子谐振子算法的收敛特性[J]. 电子学报,2016,44:1987.

[18] 燕京京,王鹏,范家兵,等. 基于量子谐振子模型的聚类中心选取算法[J]. 电子学报,2016,44:405.

引用本文格式:

中 文:邓怀勇,马琴,陈国彬,等.基于量子谐振子的 RoQ 攻击识别方法[J]. 四川大学学报:自然科学版,2018,55:752.

英 文:Deng H Y, Ma Q, Chen G B, *et al*. The RoQ attack recognition method based on quantum harmonic oscillator [J]. J Sichuan Univ: Nat Sci Ed, 2018, 55: 752.