基于随机 Petri 网模型的降质服务攻防效果评估

施江勇 鲜 明 王会梅 刘 建
(国防科学技术大学电子信息系统复杂电磁环境效应国家重点实验室 长沙 410073)

摘 要 针对DoS攻击的弱点,降质服务攻击(RoQ)利用常见的网络或终端系统自适应机制中存在的安全漏洞,通过间歇性地发送高强度攻击脉冲,降低受害者端的服务性能。RoQ攻击的隐蔽性更强,攻击效率更高,同时也给其检测和评估提出了挑战。分析了目前针对RoQ攻击的防范措施,主要有修改协议、攻击流特征检测以及自适应检测修复等。通过构建RoQ攻防的随机Petri网模型,使用SPNP软件仿真得出了服务质量随攻防博弈过程的变化情况,从而对不同防范措施的效果进行评估,为网络战攻防决策提供一些参考。

关键词 随机Petri网,降质服务攻击RoQ,攻防博弈,效果评估
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.07.011

RoQ Defense Effect Evaluations Based on SPN Model

SHI Jiang-yong XIAN Ming WANG Hui-mei LIU Jian
(State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System, National University of Defense Technology, Changsha 410073, China)

Abstract To avoid the weakness of DoS attack, Reduction of Quality Attacks(RoQ) utilizes the security vulnerabilities in self-adaptive mechanism of network and terminal system by sending high strength pulse intermittently, thus reducing the service quality of victims. RoQ attacks are more elusive and efficient, which brings challenges to its detection and evaluation. Right now the defense technologies to RoQ attacks mainly include mending protocol, detection of attack flows' features, self-adaptive detection and repairmen, and so on. This paper builded a Stochastic Petri Net(SPN) and used it in SPNP software to simulate the service quality changes in the process of attack and defense game. By evaluating the effects of different defense ways, this paper offered some consultancy for decision-makings in cyber defense activities.

Keywords SPN, RoQ, Attack and defense game, Effect evaluationa

1 引言

近年来,随着对DoS攻击研究的深入,针对DoS攻击泛洪式、高频率以及完全拒绝服务的特点提出了很多防御DoS攻击的方法[1],使其得到了有效抑制。与此同时,出现了一种新攻击手段——降质服务攻击(RoQ)。

降质服务的概念源于Rice大学的Aleksandar Kuzmanovic在2003年计算机网络方面的顶级会议SIGCOMM上提出的shrew攻击,shrew攻击是一种针对TCP协议的低速率拒绝服务攻击,具有高隐蔽性的特点。在2004年的SIGCOMM会议上,受shrew攻击思想的启发,波士顿大学的Mina Guirguis和Azer Bestavros首次提出了RoQ攻击的概念[2]。降质服务攻击是一类近似DoS攻击的新型攻击,不过又呈现了一些新的特点。

1. 攻击效率更高、隐蔽性更强、检测难度更大;

2. 攻击目标范围更大,利用网络和终端系统适应性控制机制缺陷;

3. 攻击形式更加多样。

本文试图将随机Petri网模型与降质服务攻防过程结合起来,用于分析和评估降质服务攻防的效果。通过随机Petri网搭建降质服务攻防的模型,设置模型的相关参数,使用SPNP软件仿真得出了服务质量随着攻防博弈过程的变化情况,从而对防范措施的有效性进行评估,为网络战攻防效果评估提供一些新的方法。

2 降质服务攻击的分类

在RoQ攻击的概念提出后的几年里,Mina Guirguis对RoQ攻击的攻击方式不断改进和扩充,提出了针对多种适应性控制机制的RoQ攻击方式,并通过实验对其攻击效果进行了验证。在2004年的CCN会议上,Guirguis提出了针对Internet资源的RoD攻击,其实质是根据路由器队列管理的适应性控制机制特点,通过发送脉冲式的攻击流降低目标路由器的性能。在2005年的INFOCOM会议上,Guirguis提出了针对网络终端系统的RoQ攻击。它根据终端系统的访问控制机制特点,通过短时间发送大量请求使系统不堪重负,进入低效的不稳定状态,从而降低系统性能。在2007年的INFO-

到稿日期:2013-04-02 返修日期:2013-05-11
施江勇(1990—),男,硕士,主要研究领域为网络安全,E-mail:shijiangyong@nudt.edu.cn;鲜 明(1970—),男,研究员,主要研究领域为电子信息系统建模、仿真与评估;王会梅(1981—),女,讲师,主要研究领域为网络安全;刘 建(1986—),男,博士生,主要研究领域为网络安全。

COM 会议上，Guirguis 提出针对动态负载均衡机制的 RoQ 攻击。在 2009 年的 ICN 会议上，Guirguis 又提出针对内容自适应机制的 RoQ 攻击。另外，应用于 P2P 及覆盖网络等其他网络环境下的 RoQ 攻击也不断被提出。表 1 为常见的 RoQ 攻击的分类。

表 1 RoQ 攻击分类

按攻击的对象分类	针对动态负载均衡机制的 RoQ 攻击	针对内容自适应机制的 RoQ 攻击
按攻击的机制分类	针对 Internet 资源的 RoQ 攻击	针对网络终端系统的 RoQ 攻击
按攻击周期性分类	周期	非周期

各种不同的划分方法可以相互组合，从而形成多样化的攻击方式。本文主要按照攻击的对象和攻击机制的组合选取针对 Internet 资源内容自适应机制的 RoQ 攻击、针对 Internet 资源动态负载均衡机制的 RoQ 攻击、针对网络终端系统动态负载均衡机制的 RoQ 攻击，以及针对网络终端系内容自适应机制的 RoQ 攻击等 4 种具有典型代表性的攻击方法，研究其在攻防博弈中的效果。

3 降质服务攻击的防范

目前，对 RoQ 攻击防范主要有两类方法：一类是修改有漏洞的协议或参数，如针对 LDoS 攻击的随机化 minRTO 方法[5]，修改 RED 算法的参数[6]，但由于 Internet 协议已经被用户广泛使用，大规模修改协议不但会损害用户的利益而且也不现实；另一类是从攻击数据流特征角度，通过分析 RoQ 攻击特征来检测攻击的存在并进行数据的过滤，主要有时域、频域和时频双域 3 类方法。

3.1 协议修改

协议修改的检测防范方法利用了端系统最小超时等待时间 minRTO 一致性，即链路状态恢复时间过程具有固定的周期特性，通过随机化 minRTO 来破坏超时重传的周期规律，使得攻击者无法准确预测 TCP 端下一次发送时间，这样无法在准确的时间发送攻击数据，从而缓解 shrew 攻击的影响。

这种防御方法的缺点是无法确定攻击何时存在，而随机化所有包的超时重传时间会降低没有攻击时的 TCP 性能。

3.2 攻击流特征检测与过滤

攻击流特征检测与过滤主要是检测和过滤攻击数据的高速率特征。比如，Kuzmanovic 提出通过路由器 AQM 机制对高速率包丢弃过滤 shrew 攻击流，Sandeep 和 Andreas 提出通过控制路由器队列缓冲区的大小并使用合适的 AQM 技术，来避免 RoQ 攻击。基于高速率特征的检测与过滤的方法又可分为时域、频域和时频双域 3 类方法。

3.2.1 时域特征检测与过滤

时域特征检测与过滤的方法基于数据流周期性特征识别。对数据流取样、特征提取，在语音识别中常用动态时间环绕方法将数据与样本进行匹配，识别后采用差额循环算法进行带宽分配保护。这种方法的缺点是效率低，对已有 TCP 机制性能有影响。

比如 A. Shevtekar 等[3]人提出通过统计相邻数据包到达的时间间隔估计脉冲持续时间和周期，并和 RTT 和 RTO 做比较来进行匹配的方法，该方法只针对 TCP 超时重传引起的 RoQ 攻击。另外，Luo 和 Chang 等人[4]提出采用离散小波变换分离出流入和流出过程，并通过非参数化 CUSUM 算法进行变点检测，该方法可以检测出周期变化的 RoQ 攻击，但误检率较高。

3.2.2 频谱特征检测与过滤

频谱特征检测与过滤的防范方法将路由器数据包到达速率作为时域采样序列，对其进行预处理，尽量放大攻击流与正常流在频谱上的区别，然后进行傅里叶变换得到频域序列，对频谱进行分析，将其与预先通过学习生成的攻击库匹配，判定 RoQ 攻击是否存在，从而进行数据包过滤。

对于频域检测方法，Yu Chen 等[5]通过傅里叶变换分析网络流量在频域内的能量分布，RoQ 攻击流的能量与正常流量相比主要集中在低频段，并提出针对低频特征的协同检测方法。该方法对周期固定的 RoQ 攻击检测率较高，对变周期攻击检测效果一般。Habin Sun 等人[6]使用自相关分析法提取攻击数据流的周期性特征并采用基于动态时间环绕的匹配方法进行检测。该方法计算和存储的开销较大，对变周期检测效果欠佳。

3.2.3 时频双域检测

Xiapu Luo 基于小波检测方法，将时频域结合起来，对攻击数据流进行准确描述，以检测变周期的 RoQ 攻击。

何炎祥、曹强等[7]提出了一种基于小波分析的低速率 DoS 攻击单点检测方法，该方法利用小波在时频域良好的局部特征将 RoQ 攻击流和背景数据流分隔开来，并在提取特征后用 BP 神经网络诊断攻击。何炎祥、钟海等[8]提出了基于支持向量机的 RoQ 综合检测方法，该方法利用 CUSUM 和 DFT 提取时频双域的攻击特征。上述两种方法对固定周期、变周期的 RoQ 攻击和传统 DoS 攻击有较高的检测率，但是由于是单点检测，定位攻击源较困难。

其他针对检测和防范方法的研究还包括文献[9]中基于 NS2 平台仿真结果提出的应对低速 DDOS 攻击的方法、文献[10]提出的非参数化检测方法和混合防御系统等。这类方法主要针对低速 DDOS 攻击，具有一定的局限性。

4 随机 Petri 网建模

Petri 网的概念是由 Carl Adam Petri 于 1962 年提出的。Petri 网在描述和分析具有分布、并发、异步等特征系统上有独特的优势，被广泛应用于离散事件系统建模和系统性能分析。Petri 网除了具有类似流程图、框图和网图的可视功能描述之外，还可通过标记(token)的流动模拟系统的动态活动。实际应用中，Petri 网得到了不断的改进，产生了如时间 Petri 网、随机 Petri 网、着色 Petri 网、谓词 Petri 网等不同形式。其中，随机 Petri 网给每个变迁赋予了一个随机的延迟时间，其状态空间同构于一个连续时间的马尔科夫链，结合马尔科夫过程的分析和计算方法，可以为模型的数学评价和性能分析提供很好的途径。降质服务攻防对抗活动中，攻防双方的博弈过程可以抽象为一系列的状态和变迁。考虑到实际过程中攻防双方的决策是根据当前的系统状态动态调整的，我们为每一个变迁引入了相应的选择概率，这正好与随机 Petri 网的思想一致，因此选择构建了随机 Petri 网模型来分析降质服务攻防博弈过程，并充分利用了随机 Petri 网的直观性和数学分析的优势。

4.1 参数设置

在 Petri 网建模过程中，用成本来衡量防御方法的复杂性，用防御方法达到效果所用的时间即速率来衡量实时性，用防御方法的最终效果来衡量灵敏性。根据实际统计值设定对应的参数，如表 2 所列。另外，效费比是攻击效果与成本的比

值，将效费比进行归一化处理的值作为攻击方选择该攻击方式的概率，这符合实际决策过程的思路。

表 2　攻击行为的参数设置

	针对 Internet 资源内容自适应机制的 RoQ 攻击	针对 Internet 资源动态负载均衡机制的 RoQ 攻击	针对网络终端系统动态负载均衡机制 RoQ 攻击	针对网络终端系内容自适应机制的 RoQ 攻击
成本	2	4	3	1
效果	1	4	3	2
速率	3	1	4	2
效费比	0.5	1	1	2
选择概率	0.11	0.22	0.22	0.45

同样地，我们对攻击方法的 Petri 网模型参数进行设置（见表 2），并通过计算得到对应的效费比和防御行为的选择概率。其中，速率、成本、效果参数根据实际试验和攻防实践中的统计值设定，并在后续的评估效果验证过程中不断调整和优化。

表 3　防御行为的参数设置

	协议修改	时域特征检测过滤	频域特征检测过滤	时频域特征检测与过滤
速率	4	1	2	3
成本	1	2	2	3
效果	2	3	2	4
效费比	2	1.5	1	1.33
选择概率	0.343	0.257	0.172	0.228

4.2　状态建模

状态建模使用 SPNP 软件，该软件是模拟随机 Petri 网模型的优秀软件，是由美国 Duke 大学的 Trivedi 教授领导的小组研究和开发的。经过多年的发展，SPNP 软件已经成为一个相当成熟的随机 Petri 网建模软件，可以通过设定各个变迁（图中矩形）和状态（图中圆圈）的初始值来模拟各种不同条件下的系统情况。通过设置变迁的参数，如实施速率、概率等来模拟真实的事件发生情况。针对 RoQ 攻防博弈过程建立的随机 Petri 网模型如图 1 所示。

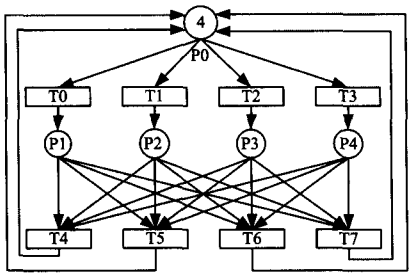

图 1　RoQ 攻防的 Petri 网模型

其中，P0 为初始状态（系统正常），最开始包含 4 个标记，通过标记的流动反映攻防行为的走向和系统的当前状态，并作为最终计算防御行为效果的指标。其他状态的含义如表 4 所列。

表 4　Petri 网模型中状态的含义

状态	含义
P0	系统正常
P1	遭到针对 Internet 资源内容自适应机制的 RoQ 攻击
P2	遭到针对 Internet 资源动态负载均衡机制的 RoQ 攻击
P3	遭到针对网络终端系统动态负载均衡机制的 RoQ 攻击
P4	遭到针对网络终端系内容自适应机制的 RoQ 攻击

每个变迁对应着一种攻击行为或者防御行为，也反映了系统状态的转换过程。每个变迁都包含两个参数，一个是该变迁对应的行为的选择概率，另一个是该变迁的实施速率，根据上文的结果，其设置如表 5 所列。

表 5　Petri 网模型中变迁的含义和参数设置

变迁	含义	参数设置（选择概率，实施速率）
T0	针对 Internet 资源内容自适应机制的 RoQ 攻击	(0.11,3)
T1	针对 Internet 资源动态负载均衡机制的 RoQ 攻击	(0.22,1)
T2	针对网络终端系统动态负载均衡机制的 RoQ 攻击	(0.22,4)
T3	针对网络终端系内容自适应机制的 RoQ 攻击	(0.45,2)
T4	时频域特征检测与过滤	(0.228,3)
T5	时域特征检测与过滤	(0.257,1)
T6	频域特征检测与过滤	(0.172,2)
T7	协议修改	(0.343,4)

4.3　结果分析

图 2 为相应的状态中标记数目不为零的概率随着系统时间变化而变化的情况，其中横坐标为时间，纵坐标为状态标记非空的概率，从上至下依次为 P0－P4 状态对应的曲线。标记不为零的概率即表示系统处于当前状态的概率，概率越大表示越有可能达到这一状态。从图 2 中表示 P0 的曲线的情况可以看出，刚开始遭受攻击时系统正常的概率几乎为 0，在采取各种防御措施后系统正常的概率明显攀升，到后期稳定在 1 附近，即系统基本正常。

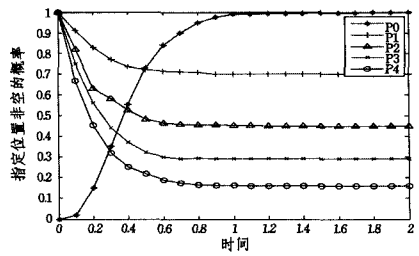

图 2　状态非空的概率随时间变化图

而图中其他曲线分别表示 P1－P4 中标记数不为零的概率，在系统稳定后都下降并稳定在一个相应数值，说明系统遭受攻击的状态在采取相应的防御措施后得到缓解。曲线值越小表示防御效果越好，从中可以看出，对 P4 的防御最成功，对 P1 的防御效果最差，由此可以推断对应的防御方法的效果，采用时频域特征检测与过滤的防御效果最好，采用协议修改的效果最差，相应地从攻击方来看，针对 Internet 资源内容自适应机制的 RoQ 攻击效果最好，而针对网络终端系内容自适应机制的 RoQ 攻击效果最差，这为实际行为中的攻防决策提供了一定的参考。

结束语　本文总结了各种降质服务攻击和防御的类型，并通过 Petri 网建立了降质服务攻防的博弈过程的模型，通过仿真参数的设置模拟了系统在受到 RoQ 攻击时状态的变换过程，以及采取相应的防御措施后系统状态恢复的过程。根据最后的仿真结果，我们得出采用时频域特征检测与过滤的防御效果最好，采用协议修改的防御效果最差，这为实际攻防决策过程提供了一定的参考。

Petri 网在离散事件的建模仿真方面具有独特的优势，如并行、不确定性、异步和分布描述能力等。随机 Petri 网在此

基础上又引入了实际事件发生时可能伴随的随机性，并以概率的形式来表示这种随机性，使得仿真的结果更加准确。下一步，将结合随机 Petri 网的仿真结果，对 RoQ 攻击和防御的效果进行实际验证，并通过实际验证的结果对 Petri 网模型的仿真参数进行优化，使其结果更具有准确性和通用性。

参 考 文 献

[1] 鲜明，包卫东，等. 网络攻击效果评估导论[M]. 长沙：国防科技大学出版社，2007

[2] 何炎翔，刘陶. 降质服务攻击及其防范方法[M]. 北京：机械工业出版社，2011

[3] Shevtekar A, Ansari N. Do Low Rate DoS Attacks Affect QoS Sensitive VoIP Traffic [C]// Proceedings of IEEE International Conference on Communications. 2006:2153-2158

[4] Luo Xia-pu, Chang R. On a New Class of Pulsing Denial-of-Service Attacks and the Defense [C]// Network and Distributed System Security Symposium. 2005:926-937

[5] Yu Chen, Kai Hwang. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis [J]. Journal of Parallel and Distributed Computing-Special issue: Security in grid and distributed systems, 2006, 66(9):1137-1151

[6] Sun H, Lui J C S, Yau D K Y. Defense against low-rate TCP attacks: dynamic detection and protection[C]// Proceedings of the 12th IEEE International Conference on Network Protocols. 2004:196-205

[7] He Yan-xiang, Cao Qiang, Liu Tao, et al. A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform [J]. Journal of Software, 2009, 20(4):930-941

[8] He Yan-xiang, Zhong Hai, Liu Tao, et al. Support Vector Machine Based Integrated Detection Method for RoQ Attacks [C]// The 3rd VARA. Huangshan, 2010:167-178

[9] Zhang Jing, Liu Bo, Hu Hua-ping, et al. Simulation and Analysis of Quiet DDOS Attacks [J]. Instrumentation, Measurement, Circuits and Systems Advances in Intelligent and Soft Computing, 2012, 127:71-81

[10] Tang Ya-juan. Countermeasures on Application Level Low-Rate Denial-of-Service Attack [J]. Information and Communications Security Lecture Notes in Computer Science, 2012, 7618:70-80

(上接第 24 页)

[3] Kahneman D. Thinking, Fast and Slow (Simplified Chinese translation edition)[M]. China CITIC Press, 2012

[4] 杜向阳. 心灵控制术[M]. 北京：电子工业出版社，2013

[5] Pessoal. On the relationship between cognition and emotion[J]. Nature Reviews. Neuroscience, 2008, 9(2):148-158

[6] LeDoux J. The Emotional Brain: the Mysterious Underpinnings of Emotinal Life[M]. New York, USA: Simon & Schuter, 1996

[7] Ralph A. Recognizing Emotion from Facial Expressions: Psychological and Neurological Mechanisms[J]. Behavioral and Congitive Neuro-science Reviews, 2002, 1(1):21-62

[8] Purves D, Augustine G J, Fitzpartrick D. Emotions(2nd Edition) [M]. Sunderland, USA: Sinauer Associates, 2001:2030-2076

[9] Emotion N S. Congition and Decision Making[J]. Congition and Emotion, 2000, 14(4):433-440

[10] Liu Y, Fu Q F, Fu X L. The interaction between cognition emotion[J]. Chinese Science Bulletin, 2009, (22)

[11] 浦江. 人工情感与全信息情感学[C]// 全国计算机新科技与计算机教育论文集. 成都：西南交通大学出版社，2007(8):338-341

[12] Pu Jiang. Research and Application of the Emotion-Intelligence Model Based on Comprehensive Information Theory[C]// The 2010 International Conference on Information Electronic and Computer Science. SRP press, 2010(11):1779-1783

[13] Pu Jiang. The Construction and Application Research of Emotional Theory based on the Comprehensive Information[C]// Shanghai 2010 ICCCI. V4, 2010(12):303-307

[14] Pu Jiang. The Research of Emotional Space and its Migration Mechanisms on the Comprehensive Information Emotional Theory[C]// Wuhan 2010 ISISE. 2010(12):287-290

[15] 浦江. 基于全信息理论的认知模型研究[J]. 徐州工程学院学报：自然科学报，2012, 27(4):49-54

[16] Pu Jiang. Comprehensive Information Emotional Theory—an assumption of cognitive-emotional interaction mechanism[C]// 2012 2nd IEEE International Conference on Cloud Computing and Intelligence Systems. Hangzhou China, October 2012(11): 1852-1858

[17] Pu Jiang. Research of Knowledge-emotion interaction mechanism based on Comprehensive Cognition Emotional Theory[J]. Applied Mechanics and Materials, 2012, 303-306(12):1435-1443

[18] 浦江. 全信息情感理论——一种认知情感交互机理的假说[J]. 智能系统学报，2013, 8(2):105-112

[19] Mellers B A, Schwart A, Ritov I. Emotion-based choice [J]. Journal of Experimental Psychology, 1999, 128(3):332-345

[20] Zajonc R B. Feeling and thinking: Preferences need no inference [J]. American Psychologist, 1980, 35(2):151-175

[21] 刘开第，吴和琴，庞彦军，等. 不确定性信息数学处理及应用[M]. 北京：科学出版社，1999

[22] 钟义信. 知识论：核心问题——信息 知识 智能的统一理论[J]. 电子学报，2001(4):526-530

[23] 钟义信. 机制主义：人工智能的统一理论[J]. 电子学报，2006(2):317-321

[24] 钟义信. 高等智能·机制主义·信息转换[J]. 北京邮电大学学报，2010(1):1-6

[25] 钟义信. "信息-知识论-智能"生态意义下的知识内涵与度量[J]. 计算机科学与探索，2007, 1(2):129-137

[26] 亚伯拉罕·马斯洛(美). 动机与人格(第三版)[M]. 许金声，等译. 北京：中国人民大学出版社，2007

[27] 刘烨，陶霖密，傅小兰. 基于情绪图片的 PAD 情感状态模型分析[J]. 中国图象图形学报，2009(5):753-758

[28] 王志良. 人工心理与人工情感[J]. 智能系统学报，2006(3):38-43

[29] 王志良，等. 人工情感[M]. 北京：机械工业出版社，2009

[30] 王志良，等. 人工心理[M]. 北京：机械工业出版社，2007

[31] 周松. 五维人格论——心理实验及发现的哲学思辨[M]. 九州出版社，2010

[32] 钟义信. "理解"论：信息内容认知机理的假说[J]. 北京邮电大学学报，2008, 31(3):1-8

[33] 温万慧，邱玉辉，刘光远，等. 情感生理反应样本库的建立与数据相关性分析[J]. 中国科学：信息科学，2011, 41(1):77-89

[34] 王志良，郑思仪，等. 心理认知计算的研究现状及其发展趋势[J]. 模式识别与人工智能，2011, 24(2):215-225