一种接入认证机制的性能分析方法

刘 伟[1] 杨 林[2] 李泉林[3]

(92664部队 青岛 266031)[1] (中国电子系统设备工程公司 北京 100039)[2]

(清华大学工业工程系 北京 100084)[3]

摘 要 认证机制对于网络安全防护具有重要的意义。大多数研究者主要关注的是提出新的认证方法、分析认证协议安全性等方面,而忽视对认证方法本身性能量化分析的研究。将认证过程看作是一个类生灭过程,通过建立两维的排队模型,求得其稳定概率分布来计算一些重要的性能指标。实验证明,利用所提出的这种通用的分析方法可以有效评价认证方法的性能。

关键词 认证,网络安全,排队模型,性能分析

中图法分类号 TP393 **文献标识码** A

Performance Analysis Method for Access Authentication Mechanism

LIU Wei[1] YANG Lin[2] LI Quan-lin[3]

(NO. 92664 Troop, Qingdao 266031, China)[1] (Institute of China Electronic System Engineering, Beijing 100039, China)[2]

(Department of Industrial Engineering, Tsinghua University, Beijing 100084, China)[3]

Abstract Authentication mechanism has important meanings to network security defence. Most researchers mainly focus on putting forward new authentication methods and analyzing the security of authentication protocols, but ignoring the research of quantitative analysis on authentication method. By analyzing the system of authentication as a quasi-birth-and-death process, establishing a two-dimensional queuing model, the steady probabilities distribution can be obtained to compute some important indices. The experimental results prove that the general analytical method can effectively evaluate the performance of authentication method.

Keywords Authentication, Network security, Queuing mode, Performance analysis

认证是网络访问控制的基础,是网络安全防护的第一道屏障,某种程度上来说,也是最重要的一道防线。安全的通信总是始于身份认证的握手过程,因此认证机制对于网络安全防护具有重要的意义。

针对不同的应用环境,研究者已提出多种不同的认证方法,但是只有少量的文献针对这些认证方法建立严格的数学模型并进行性能分析。本文应用马尔可夫分析方法,将整个系统看作是一个类生灭过程,建立两维的排队模型,通过一些重要的性能指标来分析系统性能。

1 相关工作

用于分析系统性能的方法主要有5类:第一类是使用马尔可夫分析方法[1,2,6,10],第二类是使用Petri网方法[3],第三类是使用神经网络的方法[4],第四类是采用混合方法[7,9],第五类是开发专用的分析工具[8]。文献[1,6]用一个三维马尔可夫链模型对具有强制性优先权的话音/数据无线网络进行建模,给出了对系统进行数字分析的方法,用以估计初始呼叫的阻塞概率以及转移呼叫请求被强制终止的概率等指标。文献[2]对虚拟专用网中具有多类QoS的IPv6流量进行了建模和性能分析,将VPN中的IP路由器看作是一个串联的排队系统,该系统的每个出链路都由两个并行的具有不同优先级的输出队列组成,高优先级的队列用于传输对延迟敏感的流量,而低优先级的队列用于传输对延迟不敏感的流量。文中给出了针对不同的指标(例如流量吞吐量、数据包丢失率以及端到端延迟)系统性能的折中。文献[3]使用分级的时间有色Petri网建立一个通用框架对分布式计算环境进行建模,用于性能分析。该文把一个HTTP Web服务器建模为有色Petri网,通过对其进行性能分析,揭示出Web服务器对不同的请求到达速率所能够做出的不同响应。文献[4]将神经网络的方法用于分析计算机系统的性能,使用从计算机系统中提取出的性能数据,使用基于Kohonen的神经网络分析这些性能数据,以试图找出计算机系统的瓶颈。文献[5]通过对呼叫转移延迟建立概率模型,分析其对TDMA蜂窝系统的性能影响。文献[7]用排队Petri网(QPN)模型来分析分布式电子商务系统的性能,使用QPN,可以很容易地对同步、阻塞、资源竞争等现象进行建模。文献[8]开发了一个专用的研究

到稿日期:2010-02-05 返修日期:2010-04-26 本文受"十一五"装备预研项目(513150604),国家自然科学基金项目(10671107),国家"九七三"重点基础研究发展规划基金项目(2006CB805901)资助。

刘 伟(1979—),女,博士,主要研究方向为网络安全,E-mail:xflw1001@163.com;杨 林(1970—),男,博士生导师,主要研究方向为信息安全;李泉林(1965—),男,博士,副教授,主要研究方向为随机模型、排队网络、可靠性、网络安全。

平台——eDragon 环境，来对新的基于 Web 的技术进行完整的性能分析。文献[9]提出了一种基于蚁群寻食机制的仿真算法用来求解工作流模型各活动节点的平均触发次数，并结合马尔可夫排队网络理论得到工作流模型的各项性能指标。文献[10]在一个 CDMA 蜂窝系统中，用一个呼叫转移队列建立软呼叫转移的马尔可夫链模型。

在针对认证机制进行性能分析的文献中，文献[11]使用基于 M/D/1 和 M/G/1 的单个排队模型来对比 Kerberos 以及 Diffie-Hellman 系统性能。文献[12]从 3 个方面分析第三代无线网络的认证协议，分别是等待概率、存储负载以及从 SGSN 到 HLR/AuC 的认证数据请求的期望数。文献[13]提出基于闭环排队网络来分析认证协议设计的性能，仅考虑了用户在这个闭环网络中的循环过程，即等待服务，消耗处理资源，进入下一个服务点。文献[14]针对无线网络的挑战/应答认证机制，分析了其认证代价、延迟以及呼叫丢失率。

2 接入认证过程

整个接入认证过程（如图 1 所示）简述如下：用户通过插入证明自身身份的 USB-Key（X.509 数字证书）登录计算机，基于网络接入认证协议 NAAP（Network Access Authentication Protocol），终端用户将其数字证书与入网请求一同发送给接入认证设备，以验证请求上网的终端用户身份。身份认证通过后，接入认证设备通过授权管理协议 AMP（Authorization Management Protocol）与授权管理服务器交互，将用户的身份信息递交到接入授权管理服务器请求接入权限判决。设计中，对用户的接入授权管理采用分层分域管理模式，每个用户的接入权限由本域的接入授权管理系统授权。一旦用户被授予接入权限后，可以在任何接入认证点（网络接入认证设备处）登录网络。如果用户在其归属地登录网络，接入授权管理系统根据用户的信息（通过用户的属性证书）判决用户的接入权限。如果用户漫游至外地登录网络时，接入点的授权管理服务器将判决请求转发到用户原注册域（原归属域）的接入授权管理系统，进行权限判决，最后将判决结果返回给接入点的网络接入认证设备，并确认是否允许该用户接入。

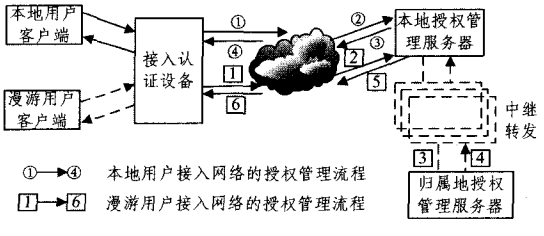

图 1 本地用户与漫游用户的接入认证过程

与本地用户相比，漫游用户的接入认证处理时间较长，而漫游用户的数量相对少于本地用户数。如何合理设置接入认证设备的参数，使其尽可能降低接入认证连接失败率，提高设备的使用率，是值得我们研究的问题。

3 模型描述

首先假设本地与漫游用户的到达分别服从参数为 λ_h，λ_w 的泊松分布，且各自的入网认证请求的处理速率分别服从参数为 μ_1 和 μ_2 的指数分布，同时假设 N 为接入认证设备的最大处理能力，即能够同时处理 N 个用户的接入认证请求。某时刻 t，设接入认证设备中的本地用户数为 $N_1(t)$，漫游用户数为 $N_2(t)$，很明显，$N_1(t)+N_2(t)\leqslant N$，因此$\{N_1(t),N_2(t):t\geqslant 0\}$是一个二维马尔可夫链，其状态空间 Ω 为$\{(n_1,n_2):n_1\geqslant 0,n_2\geqslant 0,n_1+n_2\leqslant N\}$。系统的状态转移图如图 2 所示。

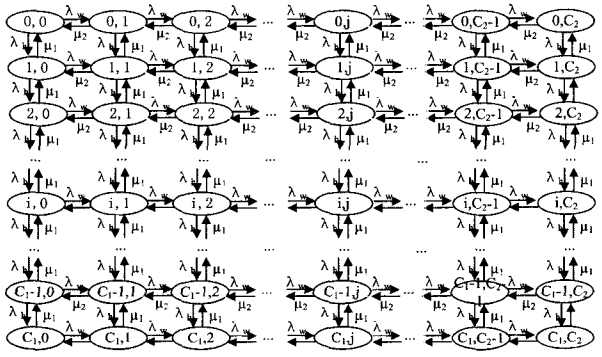

图 2 系统状态转移图

为简化起见，我们将整个状态空间划分为 $N+1$ 级，对于每一级 $i=\{(i,j),0\leqslant j\leqslant N-i\}$，且 $0\leqslant i\leqslant N$，其中 i 表示本地用户，j 表示漫游用户，从图 2 的状态转移图中，很容易获得如下的状态转移矩阵：

$$A=\begin{pmatrix} A_{0,0} & A_{0,1} & A_{0,2} & \cdots & A_{0,N} \\ A_{1,0} & A_{1,1} & A_{1,2} & \cdots & A_{1,N} \\ A_{2,0} & A_{2,1} & A_{2,2} & \cdots & A_{2,N} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ A_{N,0} & A_{N,1} & A_{N,2} & \cdots & A_{N,N} \end{pmatrix} \tag{1}$$

式中，A 中的每一项 $A_{m,n}$ 都是一个 $(N+1-i)(N+1-i)$ 子矩阵，其中 $A_{m,n}$ 表示在 i 级中，两种状态之间的转移概率矩阵，而 $A_{m,n}(m\neq n)$ 表示不同级之间状态的转移概率矩阵。根据马尔可夫链的特性，对于 A 中的任意项 $A_{m,n}$，如果 $n-m>1$，那么 $A_{m,n}=0$，因此上述矩阵（式(1)）可以简化为：

$$A'=\begin{pmatrix} A_{0,0} & A_{0,1} & 0 & \cdots & 0 \\ A_{1,0} & A_{1,1} & A_{1,2} & \cdots & 0 \\ 0 & A_{2,1} & A_{2,2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & A_{N,(N-1)} & A_{N,N} \end{pmatrix} \tag{2}$$

式中，矩阵 A' 的每一项元素的值可以由以下 3 种类型的子矩阵来唯一确定。

①对于对角子矩阵 $A_{m,m}$：

$$A_{m,m}(a,b)=\begin{cases} D_{m,m}(a,b)-\lambda_w I_{N+1-i}-A_{m,m-1}-A_{m,m+1}, & \text{如果 } a=1 \\ D_{m,m}(a,b)-\lambda_w I_{N+1-i}-\mu_2 I_{N+1-i}- & \\ \quad A_{m,m-1}-A_{m,m+1}, & \text{其他情况} \end{cases}$$

其中，

$$D_{m,m}(a,b)=\begin{cases} \lambda_w, & 1\leqslant a\leqslant N+1-i,\text{且 } 2\leqslant b\leqslant N+2-i \\ \mu_2, & 2\leqslant a\leqslant N+2-i,\text{且 } 1\leqslant b\leqslant N+1-i \\ 0, & \text{其他情况} \end{cases}$$

式中，I_n 是 $n\times n$ 的单位阵。

②对于下三角子矩阵 $A_{m,m-1}$：

$A_{m,m-1}=\mu_1 I_{N+1-i}$，$1\leqslant m\leqslant N$

③对于上三角子矩阵 $A_{m,m+1}$：

$A_{m,m+1}=\lambda_h I_{N+1-i}$，$0\leqslant m\leqslant N-1$

对于每一个状态 (n_1,n_2)，用 $\pi(n_1,n_2)$ 来表示其稳定状态概率，由于将整个状态空间划分为 $N+1$ 级，因此系统的稳定

状态概率向量可表示为 $\pi=(\pi_0,\pi_1,\cdots,\pi_i,\cdots,\pi_N)$，进一步可以得到 $\pi_i=(\pi(i,0),\pi(i,1),\cdots,\pi(i,N-i))$。而向量 π 的值可以通过求解方程 $\pi A'=0$ 以及方程 $\pi e=1$ 得到，其中 0 和 e 分别为零向量和单位向量。

4 性能分析及数值算例

本节用一些重要的指标，例如连接丢失率、缓存使用率以及等待概率来刻画系统的性能，用以指导实际参数的设置。

4.1 连接丢失率

连接丢失率对于系统来说是一个重要的度量方面。当系统中已经有 N 个用户之后，新到达用户的入网认证请求必然会被拒绝。使用计算得到的稳定状态概率向量，本地用户的连接丢失率可以表示为

$$p_h=\sum_{n_2=0}^{C_2}\pi(C_1,n_2)$$

同理可得漫游用户的连接丢失率为

$$p_w=\sum_{n_1=0}^{C_1}\pi(n_1,C_2)$$

式中，C_1，C_2 分别表示本地用户以及漫游用户的认证请求缓存区大小，且 $C_1+C_2=N$。

而总的丢失率可表示为

$$P_{\text{loss}}=\sum_{i=0}^{N}\pi(i,N-i)$$

以本地用户连接丢失率为例，图 3 显示了本地用户连接丢失率与到达速率之间的关系。从中可以看出，连接丢失率随着用户到达速率的增大而逐渐递增。我们发现，通过增加缓存空间，例如从 $C_1=6$ 递增至 $C_1=40$，只能够轻微降低连接丢失率。而在缓存空间大小相同的情况下，如果提高认证请求的处理速率，例如从 $\mu_1=20/\text{s}$ 递增至 $\mu_1=60/\text{s}$，则连接丢失率有了显著的降低。这说明，如需保持较小的连接丢失率，必须尽可能提高处理速率，保持其大于用户的到达速率。

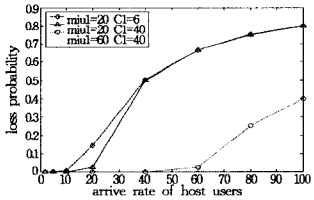

图 3 本地用户连接丢失率与到达速率之间的关系

4.2 缓存使用率

本地用户的缓存使用率定义为

$$\eta_1=\frac{1}{C_1}\sum_{n_1=0}^{C_1}\sum_{n_2=0}^{C_2}n_1\pi(n_1,n_2)$$

同理，漫游用户的缓存使用率可以定义为

$$\eta_2=\frac{1}{C_2}\sum_{n_1=0}^{C_1}\sum_{n_2=0}^{C_2}n_2\pi(n_1,n_2)$$

而接入认证设备总的使用率定义为

$$\eta=\frac{1}{N}\sum_{n_1=0}^{C_1}\sum_{n_2=0}^{C_2}(n_1+n_2)\pi(n_1,n_2)$$

同样，以本地用户的缓存使用率为例，图 4 显示了本地用户缓存使用率与到达速率之间的关系。从中可以看出，缓存利用率随着用户到达速率的增大而逐渐接近于 1。同时，在接入认证请求处理速率相同并且到达速率小于处理速率时，大缓存区使用率较低。例如，当 $\mu_1=60/\text{s}$，且到达速率 $\lambda<60/\text{s}$ 时，$C_1=20$ 的缓存使用率低于 $C_1=6$ 的使用率。而当到达速率大于处理速率之后，大缓存区的使用率逐渐增大，并大于小缓存区的使用率。例如当 $\mu_1=60/\text{s}$，到达速率达到 80/s 后，$C_1=20$ 的缓存使用率大于 $C_1=6$ 的使用率。这是因为当到达速率超过处理速率之后，对于缓存区小的设备，其连接丢失率大于缓存区大的设备，导致其使用率增加速率小于缓存区大的接入认证设备。而对于缓存区大小相同的设备而言，处理速率小的设备，在其缓存中排队等候处理的认证请求数据包更多，因此会更快速地占满整个缓存区。例如，当 $C_1=20$ 时，$\mu_1=40/\text{s}$ 的接入认证设备的缓存区使用率一直大于 $\mu_1=60/\text{s}$的使用率。因此，可以说缓存区的利用率与设备的处理速率以及缓存区大小都有关系，不能因为一味地追求提高速率，而忽视缓存区大小这个因素，通过合理地设置参数，可以达到一个理想的缓存区使用率。

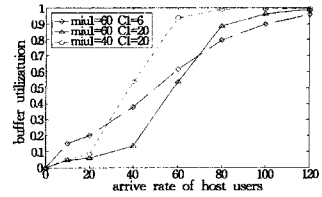

图 4 本地用户缓存使用率与到达速率之间的关系

4.3 等待概率

定义本地用户的等待概率为

$$\omega_h=\sum_{n_2=0}^{C_2}\pi(1,n_2)$$

同理可得漫游用户的等待概率为

$$\omega_w=\sum_{n_1=0}^{C_1}\pi(n_1,1)$$

图 5 显示了本地用户等待概率与服务速率之间的关系。从图中可以看出，在到达速率相同的情况下，等待概率随着服务速率的增大而降低。并且在缓存区大小相同的情况下，用户到达速率高时，其等待的概率也较大。例如，在 $C_1=20$、到达速率 $\lambda=50/\text{s}$ 时，用户的等待概率明显大于 $\lambda=30/\text{s}$ 的情况。而在用户到达速率相同的情况下，对于缓存区大的设备，用户的等待概率较大。例如，当到达速率都为 $\lambda=50/\text{s}$ 时，对于 $C_1=20$ 的设备，用户的等待概率大于 $C_1=6$ 的设备。这是因为到达速率相同时，对于缓存区小的设备，其连接丢失率增大，此时在缓存区大的设备中，等待处理的认证请求数据包逐渐增多，其等待概率必然增大。因此，等待概率必须在接入认证设备服务速率与缓存区大小之间找到一个最佳的平衡点。

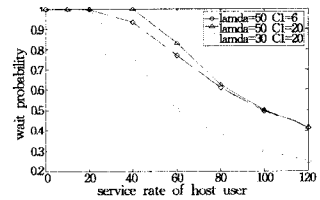

图 5 本地用户等待概率与服务时间之间的关系

结束语 本文对接入认证方法建立二维马尔可夫链模型，并对其进行了理论分析。通过建立性能指标，刻画了系统性能，分析了不同参数对性能指标的影响，用于指导实际参数的设置。下一步工作包括分析并建立更加完善的指标体系，全面地对认证方法进行分析论证。另外，如何简化模型的算法，提高其运算速度，也是今后研究的一个重要方向。

（下转第 77 页）

curity Symposium. Washington, DC, August 2003

[5] Baratloo A, Singh N, Tsai T. Transparent RunTime Defense AgainstStack-Smashing Attacks [C] // 9th USENIX Security Symposium. August 2000

[6] Zhang Q. The Synmthetix MemGuard Kernel Programmerps Interface [OL]. http://www. cse. ogi. edu/DISC/projects/synthetix/toolkit/MemGuard/memg-urad. html

[7] Ramalingam G. The undecidability of aliasing [J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1994, 16(5): 1467-1471

[8] Steensgaard B. Points-to analysis by type inference of programs with structures and unions[C] // Conference on Compiler Construction, LN-CS 1060. April 1996: 136-150

[9] Steensgaard B. Points-to analysis in almost linear time [C] // ACM Sym-posium on Principles of Programming Languages (POPL). January 1996: 32-41

[10] McPeak S, Necula G C, Rahul S P, et al. CIL: Intermediate language andtools for C program analysis and transformation[C] // Conference on Compiler Construction. 2002

[11] SPEC. Spec Benchmarks[OL]. http://www. spec. org

[12] Barrantes E G, Ackley D H, Forrest S, et al. Randomized instruction setemulation to disrupt binary code injection attacks [C] // ACM Conferen-ce on Computer and Communications Security (CCS). Washington, DC, October 2003

[13] Cowan C, Beattie S, Day R, et al. Protecting Systems from Stack Sm-ashing Attacks with StackGuad [Z]. Linux-Expo, Raleigh, NC, May 1999

[14] Cowan C, Pu C, Maier D, et al. StackGuard: Automatic Adaptive Det-ection and Prevention of Buffer-Overflow Attacks[C] // 7th USENIX S-ecurity Conference. San Antonio, TX, January 1998: 63-77

[15] Kc G S, Keromytis A D, Prevelakis V. Countering code-injection at-tacks with instruction-set randomization [C] // ACM Conference on Com-puter and Communications Security (CCS). Washington, DC, October 2003: 272-280

[16] Bhatkar S, DuVarney D C, Sekar R. Address obfuscation: an effcie-nt approach to combat a board range of memory error exploits[C] // S-SYM'03: Proceedings of the 12thconference on USENIX Security Symposium. Berkeley, CA, USA, USENIX Association, 2003: 8-8

[17] Xu J, Kalbarczyk Z, Iyer R K. Transparent runtime randomization for security[C] // Proc. of 22nd Symposium on Reliable Distributed Systems (22nd SRDS'03). Florence, Italy, IE-EE Computer Society, October 2003: 260

[18] PaxTeam. Pax address space layout randomization (aslr) [OL]. http://pax. grse-curity. net/docs/aslr. txt, 2001

(上接第 50 页)

参 考 文 献

[1] Zeng Qing-an, Agrawal D P. An Analytical Modeling of Handoff for Integrated Voice/Data Wireless Networks with Priority Reservation and Preemptive Priority Procedures [C] // Proceeding of the Workshop on Wireless Networks and Mobile Computing in Conjunction with the International Conference on Parallel Processing (ICPP). 2000: 523-529

[2] Zheng Li, Zhang Liren. Modeling and Performance Analysis for IP Traffic with Multi-class QoS in VPN [C] // Proceedings 21st Century Military Communications Conference Volume 1. 2000: 330-334

[3] Wells L, Christensen S, Kristensen L M, et al. Simulation Based Performance Analysis of Web Servers [C] // Proceedings of 9th International Workshop on Petri Nets and Performance Models. 2000: 59-68

[4] Gruen R, Kubota T. A Neural Network Approach to System Performance Analysis [C] // Proceedings of IEEE. 2002: 349-354

[5] Turkboylari M, Madisetti V K. Effec of Handoff Delay on the System Performance of TDMA Cellular System [C] // Proceedings of 4th International Workshop on Mobile and Wireless Communications Network. 2002: 411-415

[6] Zeng Qing-an, Agrawal D P. Modeling and Efficient Handling of Handoffs in Integrated Wireless Mobile Networks [J]. IEEE Transactions on Vehicular Technology, 2002, 51(6): 1469-1478

[7] Kounev S, Buchmann A. Performance Modelling of Distributed E-BusinessApplications Using Queuing Petri Nets [C] // Proceedings of the 2003 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS-2003). Austin, Texas, March 2003: 143-155

[8] Camera D, Guitart J, Torres J, et al. Complete Instrumentation Requirements for Performance Analysis of Web Based Technologies [C] // 2003 IEEE International Symposium on Performance Analysis of Systems and Software. 2003: 166-175

[9] Xiao Zhengjin, He Qinming, Chen Qi. A Method of Workflow Model Performance Analysis Based on the Mechanism of Ant Colony Found Food [C] // Proceedings of the 6th World Congress on Intelligent Control and Automation. Dalian, China June 2006: 6983-6987

[10] Ma Xiaomin, Cao Yonghuan, Liu Yun, et al. Modeling and Performance Analysis for Soft Handoff Schemes in CDMA Cellular Systems [J]. IEEE Transactions on Vehicular Technqlogy, 2006, 55(2): 670-680

[11] El-hadidi M T, Hegazi N H, Aalan H K. Performance evaluation of a new hybrid encryption protocol for authentication and key distribution [C] // Proceedings of the 4th IEEE International Symposium on Computers and Communications. Los Alamitos, Calif: IEEE Computer Society Press, 1999: 16-22

[12] Zhang Yan, Fujise M. An Improvement for Authentication Protocol in Third-generation Wireless Network [J]. IEEE Transaction on Wireless Communications, 2006, 5(9): 2348-2352

[13] Harbitter A, Menasce D A. A Methodology for Analyzing the Performance of Authentication Protocols [J]. ACM Transactions on Information and System Security, 2002, 5(4): 458-491

[14] Liang Wei, Wang Wenye. An Analytical Study on the Impact of Authentication in Wireless Local Area Network [C] // Proceedings of 13th International Conference on Computer Communications and Networks. 2004: 361-366