维普资讯 http://www.cqvip.com

基于角色访问的数据库自适应容侵结构*)

左永利　吴中福　吴开贵　邓　伟
(重庆大学计算机学院　重庆 400044)

摘　要　在数据库受到攻击的情况下，能够继续提供服务并根据攻击造成的不同损害进行自适应调整是非常重要的问题，所以本文首次提出基于角色访问的自适应容侵数据库结构。该结构根据用户的角色、入侵的历史纪录、系统状态等因素动态采取不同的容侵策略，因此在保证系统持续提供服务的同时，提高数据库的容侵能力。

关键词　容侵，访问控制，角色，神经网络

An Adaptive Architecture for Intrusion-tolerant Databases on Role-based Access Control

ZUO Yong-Li　WU Zhong-Fu　WU Kai-Gui　DENG Wei
(Computer College, Chongqing University, Chongqing 400044)

Abstract　For intrusion-tolerant database systems, it's crucial for them to dynamically change their behavior and continue delivering essential services under malicious attacks. Thus, combined with role-based access control, we propose an adaptive architecture to intrusion-tolerant databases for the first time in the literature. For systems intruded by malicious users, different adaptive intrusion-tolerant policies are taken in terms of users' different roles, historical logs of intrusion, different system states etc. Therefore, while keeping delivering essential services, we can enhance the system's intrusion-tolerant ability.

Keywords　Intrusion-tolerant, Access control, Role, Neural networks

1　前言

容侵的概念最早由 J. Fraga 和 D. Powell 在 1985 年提出[1]，Deswarte, Blain 和 Fabre 在 1991 年开发了一个具有容侵功能的分布式计算系统[2]，但相关研究工作的兴起则是在最近几年才开始。目前，美国国防高级研究项目署(DARPA)启动了一个新的研究和开发方向，名为"第三代安全"(The 3rd Generation Security, 3GS)[3]，主要研究容侵技术，包括系统在面临攻击的情况下保持系统高存活性和弹性(自动恢复)的能力，以及对这些能力进行评估的手段。欧洲启动了 MAFTIA 研究项目[4]，以期系统地研究容侵模型，建立大规模的可靠分布式应用。另外，我国的一些科研单位也在开展这方面的研究工作[5,6]。

容侵系统 ITS(Intrusion Tolerant System)是这样的一个信息系统，它能够在面向攻击的时候，仍然能持续地为预期的用户提供及时的服务。容侵系统能够检测一些用攻击避免和预防手段无法检测的信息攻击(这些攻击可能透过外层防御，即用攻击避免和预防手段设置的防御，如防火墙系统，认证和加密系统等)，并采取一些必要的措施保证关键应用的功能连续正确。容侵技术从本质上讲是系统保持高存活性(Survivability)的核心技术。根据安全需求，一个入侵容忍系统应达到以下目标：(1)能够阻止和预防攻击的发生；(2)能够检测攻击和评估攻击造成的破坏；(3)在遭受到攻击后，能够维护和恢复数据，继续提供持续服务或部分降级服务；(4)能够通过最近历史的攻击情况，动态改变系统策略，达到自适应的容侵能力。

2　容侵数据库和角色访问控制

2.1　容侵数据库

目前，美国 DARPA 资助实施的 OASIS(Organically Assured and Survivable Information System，有机组成的高存活性信息系统)计划旨在研究入侵和攻击的方法。OASIS 计划支持的几个典型项目是 SITAR, ITTC, COCA, ITUA。2000 年 1 月，欧洲启动了 MAFTIA(Malicious and Accidental Fault Tolerance for Internet Applications，基于因特网应用的恶意和意外故障容忍)研究项目。数据库管理系统的容侵技术研究的主要内容是如何使数据库管理系统在遭受到成功的恶意攻击时，能够在对受到破坏的数据进行恢复的同时保留尽可能多的未受恶意攻击影响的其它授权用户在系统受攻击期间的工作结果，能够保持一定的及时提供可靠数据服务的能力。然而数据库容侵系统的自适应性却很少得到考虑，具有自适应容侵服务能力的数据库管理系统的理想情况是：数据库管理系统在遭受到恶意攻击破坏的情况下，能够发现系统被入侵，并及时对受到入侵影响的数据进行隔离和恢复，在系统恢复的同时能够保留尽可能多的未受恶意攻击影响的用户在系统受恶意攻击期间的工作结果；不间断地提供尽可能多的可靠、及时的数据服务；对系统自动进行参数配置，达到自适应的能力，消除攻击者在此次攻击中所利用的入侵途径，避免同样问题再次发生。国际上对数据库管理系统容侵技术的研究起源于美国，主要是 GMU 的 Sushil Jajodia, Paul Ammann 和 UMBC 的 Peng Liu 以及 North Dakota University 的 Branjendra Panda 等几个研究组。国内浙江大学计算机系蔡亮等[7]对信息战语义下数据库管理系统的恶意行为作了研究。

容侵系统大致可分为两种实现方式：一是攻击响应的容侵方法，通过检测到局部系统的失效或估计到系统被攻击，而加快反应时间，调整系统结构，重新分配资源，使信息保障上升到一种在攻击发生的情况下能够继续工作的系统。这种实现方法对"入侵检测系统"的要求比较高，但是由于不改变原系统大的结构，只是增加和修改一些模块，因此实现较为简单，花费也较小。二是攻击遮蔽的入侵容忍方法，就是待攻击

*)本文受国家自然科学基金(No. 30400446)资助。左永利　硕士研究生，主要研究方向：网络信息安全，入侵容忍。

维普资讯 http://www.cqvip.com

发生之后，整个系统通过冗余，多数表决，拜占廷协议等机制来屏蔽攻击造成的影响。这种方法需要重新设计整个系统，增加冗余硬件，并通过冗余、容错技术、门限密码学技术等来实现，所以系统的实现代价很大。

2.2 角色的访问控制

同时，基于角色的访问控制 RBAC(Role Based Access Control)技术[8]是近年来安全访问控制领域的研究热点，越来越受到人们的重视。RBAC 模型主要由三部分组成，即用户、角色和权限，其中用户是指信息系统的合法使用者，包括普通用户和系统管理员等；角色是指权限的集合，包括普通角色和管理角色等；权限是指用户对客体(信息系统)的操作功能，包括普通用户权限和管理权限等。RBAC 的基本思想是：如图 1，由用户在一个组织中担当的角色来确定用户在系统中的访问权限，也就是用角色来充当用户行使权限的中介，安全的管理就可以根据需要定义各种各样的角色，并设置合适的访问权限，而用户根据其责任和权利被指派为不同的角色。这样整个访问控制过程就被分成了两部分，即访问权限与角色相关联，角色再与用户相关联，从而实现了用户与访问权限的逻辑分离。RBAC 技术用角色实施对系统资源访问权限的统一管理，具有减少授权管理复杂性，降低系统开销的特点。

图 1 RBAC 示意图

彭文灵等[9]提出了一种基于 RBAC 的攻击屏蔽容侵机制，该文提出了攻击遮蔽下的角色访问容侵机制，并重点阐述了攻击发生时各个主从角色管理服务器之间的相互协调和转换策略。

目前攻击响应的容侵数据库是国内外的一个研究热点，可以分成以下两类：一类是对可疑入侵行为进行入侵隔离的事前预防；另一类是对受到攻击破坏后的系统自动进行破坏范围评估和恢复的事后补救。但是基于 RBAC 和攻击响应的容侵数据库结构在国内外均无相关文献报道。为此，本文提出了一种基于 RBAC 和攻击响应的的容侵数据库结构，且该结构能够根据用户的动态行为进行自适应的系统参数调节。具体地说，该结构根据用户的角色、用户的历史纪录等信息，用神经网络(当然也可使用其它的模式识别工具)来动态调整出各模块的控制参数(如系统的吞吐量，报警阈值等)，并针对不同用户角色采取不同的配置方案进行实时、自适应的状态迁移和系统参数调节。

3 自恢复的容侵数据库结构

3.1 容侵数据库结构

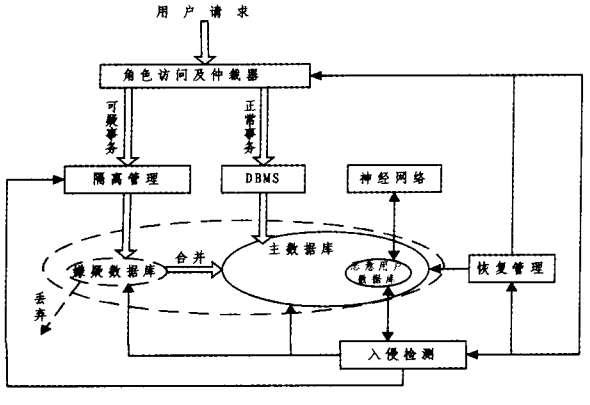

图 2 容侵数据库结构

3.2 工作机制

3.2.1 自适应机制

自适应的容侵数据库可以根据数据库系统的当前状态动态地调节各模块的工作机制。通常情况下，不同角色的恶意用户其行为模式是不同的，对数据库造成的损害程度也不同。即使是同一个恶意用户，其攻击行为也有一定的随机性，他可能在某段时间内对数据库的攻击频率很高，而在其他的某段时间里，攻击强度又有所减弱或恢复正常等。所以使容侵数据库系统具有自适应机制是非常必要的。为此，本文采用神经网络技术，根据恶意用户数据库中不同角色的历史攻击情况训练一个三层 BP 网络，每个神经元由 Sigmoid 型函数所控制。本结构对于不同的角色可训练生成不同的容侵策略，对于同一用户不同时期的攻击，也可根据其攻击强弱历史记录生成相应的策略，动态调整系统模块的参数，从而让数据库系统在当今复杂的网络环境中，具有很好的自适应容侵的能力。

3.2.2 主要模块介绍

(1)入侵检测模块

我们的入侵检测模块采用基于聚类分析的非监督式异常检测方法[14]确定两个常数来表示聚类的半径：阈值恶意阈值 THm 和可疑阈值 THs，为用户角色的事务产生三种检测结果：可靠事务，恶意事务，可疑事务，当对某个事务的检测值超过阈值 THm，则该事务为恶意事务；如果检测值小于 THm 但大于阈值 THs，则该事务为嫌疑事务；检测值小于 THs 则为可靠事务。虽然现在有很多入侵检测的算法，但本文的入侵检测模块与其它的入侵检测存在以下的不同处：(1)与系统中的其它模块结合紧密，并接受神经网络模块的控制(如对经常出现恶意行为的用户，调高其可疑阈值和恶意阈值)；(2)增加了应用环境的语意的结合(如一个商家平常一周只有 10 万营业额，突然本周一上午就超过 50 万，那么就应对这种情况报警)；(3)对于不同的层次(如应用层、会话层、事务层等)的不同入侵检测算法进行集成，成为一个统一的模块。

入侵检测模块实时分析数据库的事务操作，一旦发现恶意事务，立刻通知仲裁器，拒绝该用户角色当前会话的后续事务的处理，告知恢复管理模块对该用户角色恶意事务对数据库的操作进行撤消，使被修改的数据恢复到正确状态，并在恶意用户数据库中进行相应记录。

(2)隔离模块

如果入侵检测模块识别出可疑事务则通知仲裁器进行隔离管理：开始时为每个数据项 x 关联一个唯一的主版本号 x[main]，只有可靠事务可以直接修改 x[main]的值，当可疑事务 S_i 要更新 x 时，为 x 关联一个嫌疑版的 x 值 $x[S_i]$，它的初始值等于 x[main]，以后 S_i 对 x 的更新都分配一个唯一的版本号 $x[S_i][t_j]$(其中 t_j 是个时间戳)，这样可实现多个可疑用户的隔离，即每个可疑用户都有一个虚拟嫌疑数据库版本，各版本间采用的是基于完全隔离策略的数据库版本隔离协议[10]。通过仲裁器把该可疑事务用户提交的后续事务定位到一个虚拟的嫌疑数据库中，在嫌疑数据库中为多个可疑用户透明地建立数据库的嫌疑版本，并对嫌疑数据库进行动态检测，如果证明是恶意的就直接将其丢弃，如果证明是可靠事务(即使有多个可疑用户的事务对 x 进行了更新)，则采用优先图(Precedence graph)[10]将其和主数据库合并，解决了所有的嫌疑数据库和主数据库对数据操作的不一致。

(3)恢复管理模块

恢复管理模块定位恶意事务的破坏，并对恶意事务造成

维普资讯 http://www.cqvip.com

的破坏进行即时恢复[11]：当检测到有恶意事务时，恢复管理模块定位到恶意事务的发生时间，向前扫描直到日志末，记录所有的恶意事务和可疑事务，再向后进行 undo 恢复操作。由于恶意事务对数据造成的污染将直接影响到后续读这些污染数据的事务，形成所谓的破坏扩散，因此在恢复恶意事务的同时还要进行被污染事务的恢复，不断把后续被污染的事务也包含到恢复事务集中来。文[11]证明，当恢复速度大于扩散速度时，在足够的时间条件下，恢复范围会越来越小，最后中止。如果恢复速度小于扩散速度，恢复将不会终止，那么一种自然的做法就是，如果在时间 t 内恢复还未完成，就采取某些策略（如降低系统的吞吐量，减缓接收事务的速度；暂时停止恶意用户的事务等措施）减缓扩散速度，使此次恢复处理尽快终止。我们采用的策略如果在规定的时间范围 t 内未完成恢复或恢复速度小于扩散速度，则由仲裁器进行事务接收延迟（DT：Delay Time），一定时限内减缓仲裁器接收事务的速度，减缓扩散速度，在事务恢复完成后恢复 DT 值（DT=0），使仲裁器接收事务速度正常。

恢复过程只有在满足以下三个条件的前提下，才能确信恢复终止：

1）每一个恶意事务都已经被修复；

2）每一个被污染事务都已经修复；

3）进一步的扫描没有检测到任何新的事务的破坏。

（4）神经网络模块

不同应用领域的不同用户在不同时期对数据库进行恶意操作的几率是随机的，但在一定的短时间段内其行为是一致的，为此，我们在本结构中采用了神经网络技术（也可采取其它的模式识别方法[12]，我们下一步将对不同的方法进行仿真比较），根据用户近期对数据库的操作的历史数据和日志信息，得出相应的控制参数。我们维持一个恶意用户的数据库，实时记录恶意用户在某个时间段里对数据库的操作情况。主要记录用户 ID、时间、提交的总事务数、恶意的事务数、可疑事务数、该用户对应的 THm 和 THs 等信息。把恶意用户数据库信息归一化预处理后作为神经网络的输入信息，用一个三层的 Sigmoid 型误差反向传播网络（Back propagation network，简称 BP 网络）来模拟自适应容侵系统，对于不同角色可定期的训练和调节参数，对恶意用户可实时调节参数。网络训练好后，神经网络模块就根据不同用户的近期活动状况及其角色生成不同的参数（并将其记录在恶意用户数据库中）：调高或降低 THm、THs，调节对用户角色的入侵检测强度，提供更好的自适应容侵机制。

3.2.3 简要流程

下面，我们就以处理一个用户事务为例，简要介绍一下系统的处理流程。

用户请求经过系统防御机制后（如防火墙），首先由角色访问及仲裁器模块为用户分配一个角色和相应的权限，然后通知入侵检测模块从恶意用户数据库中读取此角色对应入侵检测模块的参数值，假设用户事务以正常事务进入数据库运行，在入侵检测的时间窗内，入侵检测系统发现该事务为恶意攻击，立刻通知角色访问及仲裁器，终止接受该用户本次会话的后续事务，并在恶意用户数据库中进行相应的记录，然后将后继工作交给恢复管理模块，由其根据日志和事务相关性确定破坏扩散的范围进行在线恢复，必要时可以使仲裁器的接收事务速度有一定的延迟（DT）。如果入侵监测系统发现用户事务是可疑事务时，则通知仲裁器对用户事务（包括此会话的后续事务）进行隔离管理，如果后续事务经入侵检测后均属正常，就将这些事务合并入主数据库，否则丢弃，并在恶意用户数据库中进行记录。因为往往恶意用户会连续发出恶意事务进行攻击，在下一次会话处理该用户事务前，由神经网络模块根据恶意用户数据库中此用户的攻击历史生成该用户下次进入时的相关系统参数（主要是 THm、THs 值），提高系统的自适应容侵能力。

在一段时间后，恶意用户数据库中可能有多个角色发生恶意用户攻击的纪录，我们再为这些角色，由神经网络根据攻击历史信息生成新的基于角色的 THm、THs 值，调节入侵检测模块的阈值，适应用户多变的攻击行为。

结论 本文基于角色访问提出了一个数据库自适应的容侵结构。该结构在面临入侵时能在线自动恢复；可根据用户的角色、历史纪录、不同的应用领域和系统容侵要求，运用神经网络技术对系统参数自动进行调节，提高系统的自适应能力。

下一步工作为：根据文[13]的信用卡事务数据和重庆大学远程教育资源库的事务数据，对该结构进行仿真；将操作系统级的容侵机制与数据库应用级的容侵机制进行无缝连接，从而形成多层容侵数据库系统；将文中思想应用于现行的商业数据库系统，如 Oracle、DB2 等。

参 考 文 献

1 Fraga J, Powell D. A fault and intruslon tolerant file system [J]. In: Proc. of the 3' Intl. Conf. on Computer Security. 1985. 203～218

2 Deswarte Y, Blain L, Fabre J-C. Intrusion tolerance in distributed computing systems [J]. In: Proc. of the 1991 IEEE Symposium on Research in Security and Privacy. 1991. 110～121

3 OASIS 网站. http://www. Darpa. mil/ipto/programs/oasis/techprogra m. htm, 2003

4 Powell D, Stroud R. Conceptual Model and Architecture of MAFTIA. MAFTIA Deliverable D21: [Research Report, RZ 3377]. IBM Zurich Research Laboratory. Jan. 2003. http://www/newcastle. research. ec. org/maftia/deliverables/D21. pdf

5 荆继武，周天阳. Internet 上的入侵容忍服务技术[J]. 中国科学院研究生院学报，2001，19(2)：119～123

6 荆继武，冯登国. 一种入侵容忍的 CA 方案[J]. 软件学报，2002，13(8)：1417～1422

7 蔡亮，杨小虎，董金祥. 信息战下的数据库安全-我国的持殊需求分析和对策[J]. 计算机研究与发展，2002，39(5)：568～573

8 Sandhu R, Samarati P. Access control: principles and practise [J]. IEEE Communications, 1994, 32(9):40～48

9 彭文灵，王丽娜，等. 基于角色访问控制的入侵容忍机制研究[J]. 电子学报，2005，33(1)：91～95

10 Jajodia S, Liu P, McCollum C D. Application-Level Isolation to Cope With Malicious Database Users [J]. In: Proc. 14th Annual Computer Security Applications Conference, Phoenix, AZ, 1998. 73～82

11 Ammann P, Jajodia S, Liu P. Recovery from Malicious Transactions [J]. IEEE Transactions on Knowledge and Data Engineering, 2002, 15(5):1167～1185

12 Richard O, Peter E, David G. Pattern Recognition, (Second Edition). Elsevier Science, 2003

13 Cyber Security Lab 网站：http://ist. psu. edu/s2/. 2003

14 Poanoy L, Eskin E, Stolfo S J. Intrusion detection with Unlabeled Data Using Clustering. In:Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001), Philadelphia, PA: November 2001. 5～8