第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·安全技术· 文章编号：1000—3428(2006)20—0138—02 文献标识码：A 中图分类号：TP311

# 一种基于CORBA分布式对象的容侵恢复策略

李庆华[1,2]，张 胤[1,2]，赵 峰[1,2]
（1. 华中科技大学计算机科学与技术学院，武汉 430074；2. 国家高性能计算中心，武汉 430074）

**摘 要：**基于分布式对象容忍入侵系统的研究是入侵容忍的研究热点之一。国内外对分布式对象容忍入侵系统架构方面已做了一定的研究，但均未侧重于系统中对象恢复策略。该文在研究SITAR模型的基础上提出了一种基于CORBA中间件分布式对象容忍入侵系统的模型，在该模型下提出了分布式对象的对象恢复策略，和传统恢复策略相比，该恢复后的对象对原来的入侵攻击在某种程度上有一定的免疫力。通过一个实例验证了恢复策略，结果表明它可使对象向前恢复到正确结果。

**关键词：**入侵容忍；分布式对象容忍入侵系统；恢复策略；CORBA

# Heterogeneous Recovery Strategy Based on CORBA for Intrusion Tolerant Distributed Object System

LI Qinghua[1,2], ZHANG Yin[1,2], ZHAO Feng[1,2]
(1. School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074;
2. National High Performance Computing Center, Wuhan 430074)

**【Abstract】** Distributed object based intrusion tolerant system (ITDOS) has become one of the attractive issues on intrusion tolerance. There have been many significant researches on the model of a heterogeneous intrusion tolerant distributed object system, but few of them focus on distributed object recovery strategy. This paper presents a model of ITDOS based on middleware, CORBA, which is based on the researches of the SITAR model, and presents a recovery strategy for ITDOS in this model. The objects, recovered by the recovery strategy, can resist the attack of the last to some extent. It is validated by experiment that the strategy correctly performs forward recovery.

**【Key words】** Intrusion tolerance; Intrusion tolerant distributed object system; Recovery strategy; CORBA

近年来一种新的安全概念——入侵容忍（Intrusion Tolerance，IT）越来越被计算机安全领域所重视。与传统的防火墙、入侵检测等安全技术不同，容忍入侵的目的是即使系统的某些组件遭受到攻击者的破坏，整个系统仍能提供全部或降级的服务[1]。基于分布式对象容忍入侵系统的恢复研究是入侵容忍的研究热点之一。任何恢复策略大多是针对某种特定模型的，本文的恢复策略也不例外。我们在研究SITAR[2]容侵系统模型的基础上考虑到分布式对象的恢复、分组通信的管理和异构对象之间的通信，提出了一种异构分布式对象容忍入侵系统的模型——基于CORBA[3]分布式对象容侵系统架构。容侵中的恢复不同于容错中恢复，它有其自身的特点，在容侵恢复中仅通过冗余是不能解决问题的：首先，这些同构冗余的系统都是具有同类型的脆弱性，所以它们不能抵抗同类型的入侵；其次是因为小概率事件的故障可能由于故意安排而必然发生。从这个意义上说，容侵恢复与容错恢复有本质的区别。和传统恢复策略相比，本文提出的恢复后的对象对原来的入侵攻击在某种程度上有一定的免疫力。

## 1 ITDOS模型

SITAR容侵系统模型是由美国DARPA支持的一项研究计划，它的目标是保护COTS(Commercial - Of - The - Shelf)服务器[2]。本文在研究上述模型的基础上提出了一种新的ITDOS（Intrusion Tolerant Distributed Object System）模型。

和SITAR相比，本文提出的ITDOS模型中，为客户端服务的不是SITAR中的COTS Servers，而是冗余域服务器（Replication Domain Server，RDS）。冗余域服务器包含着分布式CORBA对象。它是分布式CORBA对象载体，并对其进行管理。它还需要增加分组管理器（Group Manager，GM）。GM在ITDOS系统中主要是处理各个冗余域之间的关系和虚连接的管理。其中还需要连接管理模块的支持，CORBA的通用对象请求代理间通信协议(General Inter-ORB Protocol，GIOP)需要ORB整合Castro-Liskov传送器[4]。ITDOS是在Castro-Liskov传输层上建立的虚链路连接。为了能使下面的恢复策略能够进行，还需要对象恢复代理（Object Recovery Proxy，ORP），它主要是为各个异构对象提供恢复服务。为了支持ITDOS在中异构对象恢复的时候能够相互交换信息，需要增加一个公用对象平台（Common Object platform，COP）。它在ORP的底层，为ORP建立一个统一的公共对象的平台。它的作用是把具体的语言实现的对象转变成公共平台的对象。公用对象平台是建立在公用对象虚拟机上的。它为COP提供基础运行环境。本文的架构还需要一个能为什么会话密钥产生伪随机数的模块——分布式伪随机函数本质上是一个投硬币的随机访问模式[5]，去生成共享的密钥。

根据上述说明，ITDOS的架构如图1所示。

**基金项目：**国家自然科学基金资助项目（60273075）
**作者简介：**李庆华(1940－)，男，教授、博导，主研方向：并行计算，网络安全，智能软件；张 胤，硕士生；赵 峰，博士
**收稿日期：**2005-11-15 **E-mail：**zhangyin20012@sina.com

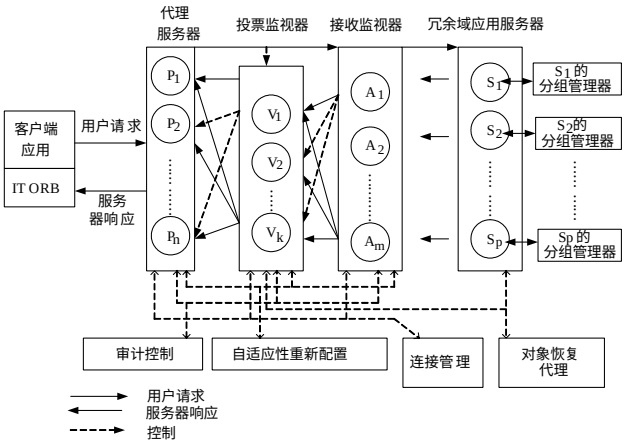


**图 1 系统总体架构**

其工作流程如下：

代理服务器(Proxy Server，PS)负责接收 Clients 想发给远程对象的 Request，并将 Request 发送给投票监控器（Voter)、接收监视器（Acceptance Monitors，AM)。AM 检查用户请求的合理性，如果合理，则向对应的远程 CORBA 对象组发送用户请求。组内的 CORBA 对象收到用户请求后，处理请求，然后向 AM 发送服务器传递服务器对象的响应，AM 对响应进行完整性检查并监视 CORBA 对象的异常行动，分析判断 CORBA 对象是否正常，然后将响应和判断结果交给 Voter。Voter 通过 Byzantine 协议选举出正确的服务器响应传给 PS。PS 将服务器响应回给客户端。

在本 ITDOS 模型中，当冗余的应用服务器域被入侵时，AM 会监视并发现它；当 AM 被部分入侵，给出错误的判断时，Voter 会投票选举出大多数 AM 的正确判断；当 Voter 被部分入侵时，Byzantine 协议会确保大多数好的 Voter 仍然会得出正确判断，送给 PS；当 PS 入侵时，客户端可以选择其它的 PS 提供服务，这在现有的网络技术中是很常见的。

## 2 异构系统容侵对象恢复策略

### 2.1 异构系统容侵恢复策略

为使本文概念上自包，先给出相关定义：

**定义 1** 系统当前需要收到攻击恢复的对象集合，记作：$Oset_B$。

**定义 2** 任意对象 A，其中为系统中任意一个对象，在系统中的异构冗余对象集合，记作：$Rset_A$。

**定义 3** ITDOS 模型中的对象恢复代理，记作：ORP。

**定义 4** ITDOS 模型中的投票监视器，记作：Voter。

**定义 5** ITDOS 模型中的冗余域服务器，记作：RDS。

恢复策略步骤如下：

(1)恢复策略开始时系统得到当前受攻击的对象集 $Oset_B$。设任意一个对象 A，其中 $A \in Oset_B$。然后对 A 进行下列步骤 b 到步骤 l 恢复。直到 $Oset_B = \phi$。恢复任务结束。

(2)A 对象会向对象恢复代理（ORP）发出恢复请求，ORP 根据 A 对象的类型，得到 $Rset_A$。

(3)ORP 向所有 $Rset_A$ 中的对象所在的 RDS 发出请求。请求 $Rset_A$ 中所有的对象状态同步。

(4)RDS 在收到 ORP 的请求后通过 GM 对所有包含 $Rset_A$ 对象的 RDS 进行对象状态同步。

(5)同步完成后，RDS 将同步后的对象状态传给 Voter。

(6)Voter 通过 Byzantine 协议选举出正确的对象返回给 ORP。

(7)ORP 得到 Voter 的响应对象，并利用公用对象平台作为中间桥梁。重构对象 $A'$。

(8)ORP 通过网络传输 $A'$到 A 的服务器上，并用 $A'$代替 A 对象。

(9)调用原来 A 对象的服务器上 A 的析构函数。

(10)用 $A'$对象代替 A。

(11)重新生成和 A 对象服务器相关的所有 RDS 中的分组管理器中的共享密钥（避免服务器相同的手段攻击)。

(12)把 A 从 $Oset_B$ 中删除。

其调用关系见图 2。

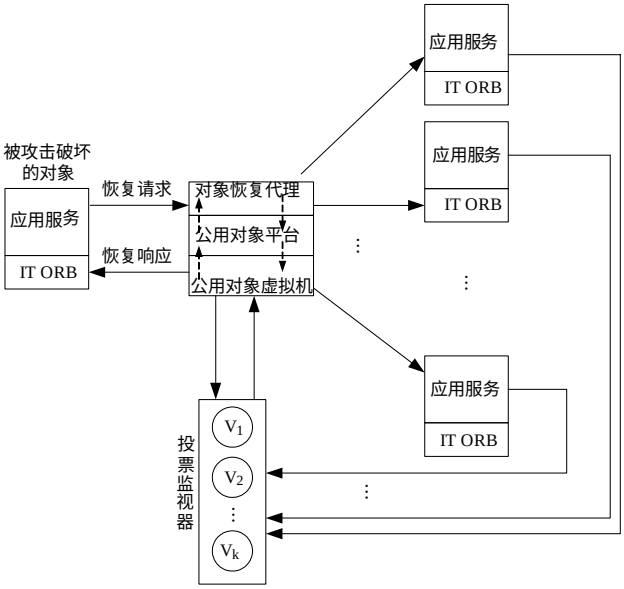


**图 2 ITDOS 对象恢复原理**

在上述恢复策略中，首先恢复代理中建立的公用对象平台为异构对象进行转换数据提供了服务。其次如果攻击者破解了对象之间的会话密钥，向对象发出虚假请求。为了避免被恢复的对象受到相同的攻击，我们就在恢复期间要重新生成跟他能建立会话的会话密钥。这样就对原来的攻击者有免疫能力。优点是：本文的恢复策略是针对对象，恢复粒度比服务器的恢复要小，比服务器级的恢复要灵活得多；对象恢复用到了对象恢复代理，对 $Rset_A$ 中对象经过 Voter 利用 Byzantine 协议选举出正确的对象返回给对象恢复代理，提高了系统的可靠性。本文的恢复策略适合上述的任何一种方案。

### 2.2 实例

在保险业信息系统中，系统生产一张保单的时候，要根据用户录入的信息去计算当前保单的保费。所以保费计算是一个系统中非常重要的模块。计算保费的时候会调用所有 Pc 对象中的 cl(contract)方法。

假设用户的保费计算的请求发给应用服务器，这时所有 Pc 对象都会计算保费。计算出来的结果都会传到系统的 Voter，Voter 通过 Byzantine 协议选举出正确的 Response 传给用户。同时也会发现那些冗余域服务器（RDS）中的 Pc(i)对象有错误。这时就需要用恢复策略对这些对象进行恢复，同时把已经受攻击的 Pc(i)对象设为不可用。

具体恢复如下：需要对其中的 Pc(i)对象进行恢复。ORP 在一段时间收到的恢复请求的对象集合为 $Oset_B$。Pc(i) $\in Oset_B$。当系统到了恢复时间时，恢复代理逐个取出 $Oset_B$ 中要恢复的对象。当取到刚刚需要恢复的 Pc(i)对象时，ORP 会先去查找配置，得到所有包含 Pc 的冗余域的集合 Rest。ORP 会向所有 Rest 中的冗余域发出同步的请求，Rest 中的冗余域收到同步请求后通过 GM 进行同步。然后对所有

(下转第 165 页)