摘要:

2017年7月，我参与某互联公司自主研发全国运营的网约车出行平台。该平台主要是为了解决客户在线预约网约车。包含用户叫车、自动派单、司机接单、行程结算、车辆管理等功能模块。我在该项目中担任系统架构师设计师一职，主要负责整个系统的架构设计。本文以该项目为例，主要论述高可靠性系统中软件容错技术运用过程。通过N版本技术来实现同一业务多版本实现方式达到软件冗余保障系统的高可靠性的目的；通过在请求数据中增加校验码的方式来实现数据冗余来达到检错和纠错的目的；通过集群技术来实现硬件上的冗余达到提升系统的可用性和可靠性目的；事实证明，使用这些技术手段使得项目整体能够克服项目中遇到的各种问题。最终项目得以顺利完成，取得预期目标，获得用户好评。

正文:

2017年7月，我参与某互联公司自主研发全国运营的网约车出行平台。我公司致力于网络出行市场服务是首批获得当地“网约车出行牌照”, 并且先后获得四川、河南、海南、山东等各地的合法运营牌照背景下。以构建一个合法、合规安全的网约车出行环境为使命。以解决用户打车难、提升用户的出行幸福感，拉动了产业链的发展，构建了一个完整的出行生态链的为目标，构建一个全国性的网约车出行平台。 网约车出行平台包括乘客端、司机端、后台管理系统三部分组成。乘客端供乘客查询车辆、发布订单、支付车费、评论司机；司机端供司机车辆信息认证、出车接单、乘客接送、车费提现等；管理系统主要是提供系统报表查询、规则配置、乘客管理、司机管理、分公司管理、账务管理等。本平台提供了专车、快车、出租车业务，乘客可以通过自身的需求来选择不同类型业务出行，司机需要上传自身拥有的运营车辆等证照信息到平台审核，只有当平台审核通过后才能正常的再平台上合法运营。我在该项目中担任系统架构师设计师一职，主要负责整个系统的架构设计。

出行平台定位是一个全国性的互联网平台。为了更好的为客户服务在平台建设过程中运营方提出了高可靠、高可用、高安全的要求。以保证系统连续运行工作，当硬件或者软件发生故障后，系统能够快速定位与处理，保证系统能够正常工作。为了达到系统的高可靠性，充分考虑容错能力，通常在软件设计上采用N版本技术和增加信息校验码的方法来系统系统的容错能力和安全性。通过N版本技术能够实现算法容错和软件容错。能够使我们快速完成对错误的定位和处理。通过校验码的方式能够有效的过滤非法的客户端请求，保障系统的安全性和增强系统的纠错能力。通常在硬件配置上采用硬件冗余的方法，以便在资源上保证系统的可靠性。结合平台实际我们采用集群技术来做硬件冗余，这样既保证系统资源的可靠性又提高了系统的可伸缩性。下面就项目中用到的提高系统可靠性采取的容错方法做具体的论述。

1、N版本技术实现软件冗余

在系统中我们在程序开发过程中通过N版本技术来实现软件冗余，来增加系统的容错性，下面使我们的具体做法。首先在系统中我们分析了对计算要求较高且不能出错的的功能模块有：财务对账、取消退款、公司结算等。这部分功能模块我们决定采用N版本的程序设计技术。通过不同的开发团队、不同的实现方式来完成相同的功能计算，保证多个版本的计算结果的正确性并且功能也是一样的。客户在调用这个业务的时候我们在程序内部内部会同时去调用多个版本的计算结果然后通过表决器来表决最终的结果。可以通过全等表决、非精确表决等方式对多个表决结果进行表决，来比较结果的一致性或者数据的相异性。这样做的目的可以很大程度上防止重要的业务在极端的情况出现计算问题或者触发错误导致计算错误或者系统一场等。这样做的缺点就是开发的成本比较高需要占更多的开发资源，所以我们对于这部分业务做了权衡过后才验证这些模块或功能这样做是可行的才决定实施这个方案。这个方案实施后能够在很大程度的系统的容错程度。

2、通过校验码来实现信息冗余

在系统设计过程中我们通过校验码来实现信息冗余预防黑客的恶意攻击。受到恶意的攻击是每个系统最头疼的事情，我们在项目设计的初期为了保障系统的安全性，可用性和高可靠性。我们决定增加校验码的方式来实现请求过滤和数据纠错。校验码的原理是通过增加一些冗余码，来检错和纠错。通过分析我们最终决定采用CRC循环冗余校验码来作为我们系统的纠错编码，下面是纠错码的具体实现。首先我们纠错码是放在网络的HTTP请求头上面，他数据源计算规则是：1、首先将所有需要请求的参数按照字典正序排列为数组；2、再按照数组顺序进行字符拼接为一个数据字符串；3、然后将字符串转换为二进制信息码然后截取最后8位。4、最后将这8位信息码转换为CRC校验码完成校验码的生成。通过上面的4个步骤完整校验码的生成，由于每次数据的请求头中包含了校验码，系统可以在业务网关这一层过滤掉一些校验码错误的请求，来阻挡一些恶意的攻击手段。达到提升系统的可靠性的目的。

3、通过集群技术来硬件冗余

在系统中设计我们通过集群技术来实现硬件冗余，在设计的过程中我们遇到的最大的一个问题就是业务可靠性问题，在软件可靠性上我们可以通过加强质量验收标准来提升可靠性，但是对于硬件是我们无法掌控的，我们所有的硬件服务器都是托管到机房的，而且我们是一个面向客户的互联网平台需要暴露到公网中。需要提供7 \* 24小时的服务能力。我们为了防止单机故障，通过集群的方式来提升可靠性防止单节点故障导致整个系统不可用，对比高性能主机集群技术可以提高更高的可用性而且便于管理，在价格上也有很大的性价优势。这样还不够，我们在系统的运行过程中经常由于机房的网络切割，停电等不可抗拒的因素。通过分析我们决定在本地机房集群的基础上增加异地机房集群来防止托管机房的故障或者区域的网络问题导致系统整体故障，通过这样的硬件集群加上异地多集群的方式来解决了硬件或者网络问题导致的业务中断，提升了系统的可靠性，提高了系统的无故障时间和满足了我们系统的可用性要求。

经过全体成员的不懈努力。在2018年2月，先后在四川、重庆、河南、贵州、海南等城市全国开展内测。2018年6月，全国正式发布运营。上线1年多程序一直稳定可靠运行。无较大线上生产事故、系统平稳运行。通过系统的可靠性容错技术的运用。完成系统如下目标：系统能够达到客户的一个任意请求能够在2秒内达到正确的响应；系统出现故障能够保证在30分钟内切换到备用服务或者回到上一个版本；保证平均无故障时间大于30天，保障系统具有较高的可靠性。上线以来得到了多个地区交通部门的点名表扬和和上万用户的好评。也为我们后续的开发、迭代、运维奠定了一个良好的基础。

项目上线至今运行1年多进入产品优化迭代阶段一直运行稳定运行，无较大生产事故。实践证明，系统能够顺利上线，并且稳定运行，性能良好。与系统可靠性容错技术的运用是密切相关的，让我们能够在系统出现故障后快速的定位出现问题的原因确保系统的正常工作，增强了系统的容错能力，同时也充分的利用了硬件资源的使用效率。