网络系统可生存性评估与增强技术研究概述*)

张乐君 国 林 王 巍 杨 武 杨永田

(哈尔滨工程大学信息安全研究中心 哈尔滨 150001)

摘 要 网络系统可生存性是网络安全研究的新方向,它突破了传统的网络安全的概念,从新的角度对网络安全问题进行研究。本文首先对网络系统可生存性研究领域进行了总结,回顾了可生存性概念以及可生存系统的关键属性,论述了可生存性评估和增强技术之间的关系。然后,阐述了国内外可生存性评估模型以及可生存性增强技术的研究现状和技术方法,分析了不足之处,并提出可生存性评估技术与增强技术的结合,以及生存性进化等方面是未来发展方向。

关键词 可生存性,评估模型,增强技术

The Research Summarization of Technology of Network System Survivability Evaluation and Enhancement

ZHANG Le-Jun GUO Lin WANG Wei YANG Wu YANG Yong-Tian

(Information Security Research Center of Harbin Engineering University, Harbin 150001)

Abstract As a new direction in network security, survivability is different from traditional network security, it gives a new way to research the network security. First, the research of survivability for network system is summarized and discussed in this paper. Survivability definition and Survivability key attributes are reviewed. The relationship of evaluation and enhancement technology is expounded. Second, this paper introduces survivability evaluation models and survivability enhancement methods at home and abroad, and then analyzes their defects, puts forward the cooperation of evaluation model and enhancement technology and survivability evolution are the orientation of survivability research.

Keywords Survivability, Evaluation model, Enhancement technology

随着国家信息化带动工业化发展战略的确定,计算机网络与信息系统建设取得了长足的进步,网络系统广泛地应用于工业、商业、政府和国防部门。网络系统内、外部环境日趋复杂使得任何网络系统都不可能是绝对安全的;然而,人们对计算机网络的依赖程度越来越大,而且越来越多的系统采用了分布式体系结构,这给传统的网络安全技术带来巨大的压力。

人们在经历了网络安全技术的"防"、"检"两个阶段后,提出了"容"技术思想。网络系统的可生存性正是在这个阶段提出来的。由于网络系统生存性的研究与传统的网络安全理念不同,人们更多地关注持续服务的能力,因此能源、金融、政府等相关部门对其关注程度越来越高。从国家层面上来说,针对国家基础设施的关键服务网络系统可生存性的研究也在如火如荼地开展。大部分研究内容是围绕可生存性概念、可生存性评估模型与可生存性增强方法展开。

1 可生存性概念

可生存性是 Barnes 等人于 1993 年提出的,是指系统提供基本服务的能力,即系统在面临攻击、失效和偶然事件的情况下仍然可以按照需求及时完成任务的能力[1]。在完成基本服务的同时系统仍然保持其基本属性,如数据完整性、机密性等其他属性[2~4]。可生存性是衡量网络系统"容侵、容错、容灾"能力的重要依据。网络系统的可生存性建立在传统安全理论、可信计算等基础之上,正在成为一个新的研究方向。

网络系统生存性概念的提出得到广泛的重视,是因为其中具有丰富的内涵和不同的安全理念。首先,网络安全追求目标的转移。可生存性基本含义表明,系统安全目标不再是保证整个系统的绝对安全可靠,而是保证系统中提供的一些基本服务的正确性、连续性、无间隙性;其次,不存在绝对的生存性。生存性研究的一个关键假设是:系统的任何部件均可能发生故障或被入侵,然而,没有一个系统能够应对不受限制的恶意故障或攻击。因此,一个系统的生存性总是相对于给定的内外部环境(故障模型和攻击模型)而言的,绝对的生存性实际上是不存在的。最后,可生存性是网络系统的整体特性。系统整体的可生存性设计得好,有可能比某些组成部分的可生存性强,某些功能甚至可能不具备可生存性,但整个系统仍有良好的可生存性。

可生存性研究的重要性已得到广泛的关注。目前,可生存性的研究主要是在吸收其它学科尤其是可靠性设计的研究成果的基础上开展的。研究重点包括可生存性的基本概念、可生存性体系结构、可生存性系统模型、可生存性系统分析与设计、可生存性系统工程方法和工具、可生存性风险评估、可生存性系统评价与测试、可生存性系统增强技术等等。人们在不断寻求开放互联网络环境下的容错、容侵、容灾的硬、软件解决方案。

为了保证提供基本服务的能力,网络系统必须具有表 1

*)基金项目:国家"242"信息安全计划基金资助项目"大规模网络安全预警分析技术"(2005A33)。**张乐君** 助教,博士研究生,CCF 会员,研究方向为网络安全,网络系统可生存性。**国 林** 副教授,硕士生导师,研究方向为计算机网络安全与信息安全。**王 巍** 副教授,硕士生导师,研究方向为网络安全与网络计算。**杨 武** 教授,硕士生导师,研究方向为网络安全。**杨永田** 教授,博士生导师,研究方向为计算机网络与应用,分布式计算机系统。

中所示四个属性。

表1 可生存性系统的四个关键属性

关键属性	描述	策略例子
抵抗攻击	抵抗攻击策略	认证 访问控制 加密 消息过滤 功能隔离
识别攻击及其影响范围	检测攻击(包括入侵)的策略,了解系统目前状态,评估危险程度	入侵检测 内部数据完整性检查
在攻击后修复基本的和所有的服务	保存损坏信息的策略,限制危险的程度,在运行期间,维护或保存系统的基本服务,在条件允许的情况下,保存用户的服务	冗余组件 数据恢复 系统备份和恢复
自适应以减少未来攻击的影响	根据从入侵中获得的知识改进系统生存性策略	识别新的入侵模式的能力

网络系统可生存性评估方面的研究是考察网络系统是否具有以上关键属性并量化系统拥有关键属性的程度,将网络系统可生存性的评估转化为对网络系统中关键属性的评估。可生存性增强方面的研究也是从关键属性入手,通过多种技术手段提高系统抵抗攻击、识别攻击、修复系统及自适应能力,达到增强系统可生存性的目的。在网络系统可生存性研究领域内,网络系统的可生存性评估技术与可生存性增强技术是相互促进、相互制约、不可分割的关系。"可生存性增强"是"可生存性评估"的最终目的;"可生存性评估"为"可生存性增强"的发展提供依据。

下文从介绍国内外对这两个方面的研究现状入手,总结了各自的优缺点,并提出了该研究领域未来的发展方向。

2 网络系统可生存性评估模型

所谓可生存性评估模型就是对复杂的信息系统进行简化以便进行可生存性分析而建立的模型,它是进行可生存性分析的基础。随着网络的大量应用,目前信息系统大多和网络结合在一起,基于网络结构的复杂性、网络规模的扩展性以及网络服务的多样性对网络信息系统进行生存性分析必然涉及到对系统的简化以及分析模型的建立。

2.1 基于系统结构的评估模型

网络信息系统的硬件物理设施通常可以表示为图的形式,而服务流可以抽象为调度问题,因而可以用图对系统网络拓扑或物理结构建模,进而分析系统的可生存性。卡内基梅隆大学 SEI 研究中心提出了 SNA(Survivable Network Analysis)生存性分析方法[5,6],用于评估现有系统的可生存性,从而提高系统在受到威胁时的生存能力。

SNA 分析可以在系统的生命周期、需求分析以及体系结构的层次进行,最终提出关于分析结果和建议的报告,分析结果通过生存性图的形式总结出来,列举了当前和推荐的体系结构的策略。Krings 提出一个 4 步模型[7],将生存性分析转化为一个参数化的图模型,结合模型抽象和表示,该模型是由图和调度算法组成的分析方法的基础,见图 1。

(1)系统定义:主要任务有:定义系统任务和主要功能需求;根据系统用户能力和所在区域、系统事务的类型和规模,定义系统使用环境;根据可能遇到不利条件的类型回顾系统风险;根据系统硬件组件和连接方式、软件配置和驻留信息确定体系结构等。

(2)基本性能定义:这一阶段的主要任务有:从系统提供的服务和数据中选择系统所要提供的基本服务和数据。基本服务和数据分别是系统在遭遇入侵、故障或意外情况下,也必须提供的服务和数据。

(3)系统受威胁性定义:这个阶段要求根据操作系统的操作环境选择具有代表性的入侵方法,定义入侵使用情境进行跟踪确定受威胁的部件。

(4)存活性分析:软点(softspot)组件是指受威胁的基本组件。基本组件是指支持系统基本服务和数据的组件,如果基本组件遭到破坏,系统就无法提供应有的基本服务,生存性就自然受到影响。所以 SNA 的最后一个步骤就是要对系统的软点组件进行分析。通过对系统软点组件的 3R(Resistant、Recognize、Recover)特性的分析,得到 SNA 的分析的结果,提出体系结构级的相应修改建议。

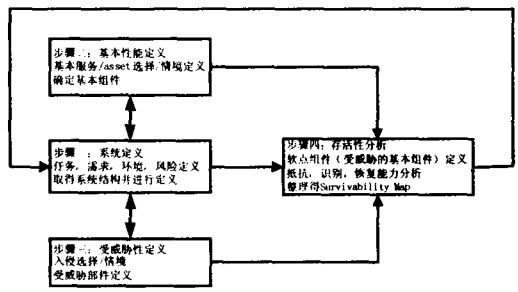

图1 SNA 分析方法

大量的研究工作都以 SNA 分析方法为基础展开,而传统的 SNA 分析方法只能对系统的 3R(Recongnize,Recover,Resistance)性能作出"定性"的分析。文[8]在 SNA 分析的基础上,分别对入侵的危险程度、识别率、服务恢复时间等性能确定了参数模型,对 3R 的各个性能提出一个"量化"方案。

总体来说,SNA 还处于探索阶段,还没有形成规范化的规则集用于分析;在 3R 量化分析中,各种参数的选择需要大量成功案例支持;由于网络系统攻击技术不断的发展,这些策略和案例需要频繁的检查和不断的改进。

2.2 基于系统服务组件的评估模型

该模型以信息系统提供的服务组件为中心,根据服务涉及到的系统组件将系统进行简化和建模,在数学上通常表现为一个类似树的结构,该模型把系统的可生存性评估分解为对各个组件可生存性的计算,把系统整体可生存性分解为各个组件可生存性问题来求解,通过综合评估所涉及到的各个组件的可生存性情况,得到该系统的可生存性状态。

郭博渊[9]等人将系统服务的故障归结到原子服务(某个硬件、软件或它们的组合)中去,简化了可生存性的计算,通过对分布式网络系统中系统与配置、服务之间支持依赖关系的定量描述来刻画系统服务的可生存性。DSO National Laboratories 将系统可生存性量化任务分解为四个层次,通过计算各服务组件可生存性,最终归结出系统的可生存性[10],如图 2。图中第一层是量化系统可生存性任务;第二层 S 是影响系统可生存性的关键属性,例如:抵抗攻击、识别攻击、服务恢复、自适应演化等等;第三层 C 是可生存关键属性的服务集合;最后一层 SV 是服务集合中服务组件。该方法的各层次之间通过多种依赖关系描述,分别为,I,影响系统可生存性关键属性的重要程度;P,各个服务优化组合;$\mathcal{L}$,服务组件的可

生存性。

因为该模型从系统组件出发，所以要详细了解系统各个组件的设计方法及其层次结构，以便对系统服务组件进行充分评测；其次，组件可生存性与系统可生存之间的依赖关系缺乏通用的规范化标准；受网络规模的限制，如何从真实系统体系结构自动生成评估模型还是一个难点。

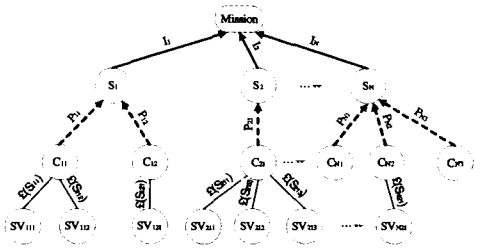

图 2　可生存性计算层次化结构示意图

2.3　基于数据流图的评估模型

文[11]提出了基于生存数据流图的评估方法。该方法的核心思想是：采用问题空间转换思路，基于数据流关系，建立系统的一种图模型，其生存性计算转换为图的连通性计算。首先，将配置操作指令的执行过程看成是由对消息内容的分解、传递、转换、细化等一系列对数据流操作处理构成的；将与生存性相关的所有元素的功能统一抽象为数据流的输入、处理和输出三个环节，构造一种反映元素之间数据流逻辑关系的图模型，将生存性计算转换为图的连通性计算。采用 Monte Carlo 方法为计算系统生存性构造一个合适的概率模型，依照模型进行大量的统计实验，然后通过模型或过程的抽样实验来计算所求参数，最后给出可生存性的近似值。

该模型是一种对系统可生存性评估的模拟试验方法，基于服务组件的评估模型注重服务节点，基于数据流图模型关注服务逻辑连接图的连通性，是从另一个角度刻画生存性。此外，该模型亦可应用到实际网络中，根据数据流的响应时间，丢包率等情况将数据链路连通情况划分为多个等级，以此为根据量化系统在实际环境中的可生存性。Monte Carlo 方法可用于分析十分复杂的对象和复合故障、攻击的影响，并可从多角度进行分析。其主要缺点是该算法需要消耗大量计算资源。

2.4　基于潜在攻击的评估模型

该模型的核心思想是通过考察系统服务在不同级别攻击下的服务质量来量化网络系统的可生存性，响应时间是衡量服务质量的重要指标。

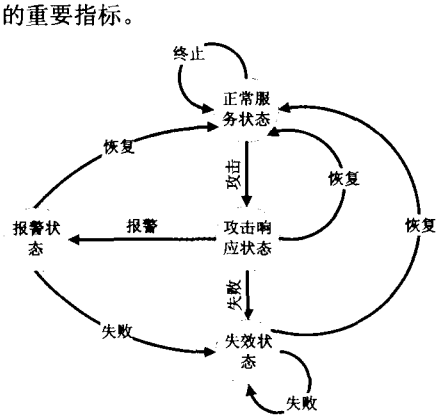

图 3　DoS 攻击下网络系统状态迁移图

McDermott[12]首先定义系统服务状态（正常状态、攻击响应状态、报警状态、失效状态），然后，根据网络攻击的随机性，采用随机进程代数（Stochastic Process Algebra，SPA）模拟攻击者和系统的行为，并建立攻击过程模型；其次，用转换概率矩阵建立系统面临攻击的反应模型；最后，采用数学公式分析网络系统遭受攻击后系统的终结状态来量化网络系统生存性。这种研究方法是基于预测（即潜在攻击下）的生存性，因此攻击者的能力和持续攻击的可能性也应考虑在内，极大地增加了计算复杂性。图 3 描述了 DoS 攻击下，网络系统服务的状态迁移情况。

此外，也可利用真实攻击对网络系统可生存性进行测试分析。通过考察真实攻击对网络系统的影响量化系统的可生存性。但由于真实攻击会对网络系统产生不可恢复影响，攻击的复杂性和多样性不断增加、发展，以及网络系统外部环境不断变化等多方面因素影响，导致这种方法研究存在一定的局限性。

3　网络系统可生存性增强

3.1　基于 3R 的可生存性增强技术

SEI 研究中心提出了基于 3R 的可生存性增强技术[13]，即首先将系统划分成不能攻破的安全核和可恢复部分，其中基本服务不可攻破，入侵模式是有限集合。然后针对一定的攻击模式，制定相应的抵抗（Resistance）、识别（Recognition）和恢复（Recovery）的消减策略，并建立系统可生存性影射表。该模型强调系统防护技术的不断进步是生存性方法学研究的前提。

该研究从可生存关键属性出发，为可生存性增强技术的研究提供了理论依据，但还处于理论模型阶段，未形成完整的理论体系结构和实用技术。

3.2　基于异构网络的可生存性增强技术

网络的拥塞是导致网络服务不可用的重要原因之一。基于异构网络的可生存性增强技术是通过是增加网络的异构性，减少攻击对网络的影响，从而保证网络系统能够为用户持续提供服务。攻击具有针对性特点，即任何一种攻击都是针对网络中某一漏洞而设计，例如：操作系统、网络协议、服务类型等。如果一个网络完全是采用同一种结构，那么在遭受大规模攻击时，所有同构的网络都将受到影响，导致毁灭性结果。

弗吉尼亚大学正在研究一个由 DARPA/ITO 资助的“自适应可生存多网络的信息系统生存性”课题，开展多个异构网络的关键服务集、受攻击时的 QoS 保障、受损后的网络系统管理策略等相关问题的研究。研究在网络遭到攻击的情况下如何最大限度地减少网络拥塞，以保证关键的网络服务能够优先使用网络资源和尽快地恢复网络[14]。

该技术的技术路线是通过结合异构理论改造通讯网络，以实现增强网络中通讯系统的可生存性。从本质上来说，该方法并不是以网络系统本身为出发点进行设计，但却为网络系统的异构性研究提供了理论基础。

3.3　基于动态漂移的生存性增强技术

基于动态漂移的生存性增强技术的核心思想是：提供服务的组件发生故障（攻击、错误、自然灾难）时，通过漂移技术将用户服务请求转接到其他提供类似服务的组件上，保证系统能够持续提供服务。

传统的漂移技术包括：DNS 轮转、URL 重定位、IP 重定向、IP 欺骗等。此外，Rutgers University 的 Disco Lab 为了使客户端和服务器端都能够支持动态漂移，提出了连接迁移技

术。该技术通过改造传统协议的方法实现。各种漂移技术对比请见表2。

表2 漂移技术综合比较

名称	是否需要前端调度	能否支持跨广域网备份	漂移转换时间	转换力度	对客户是否透明
DNS轮转	是	支持	长	最大	透明
URL重定位	是	支持	中	中	透明
IP重定向	是	不支持	短	中	透明
IP欺骗	否	不支持	最长	大	透明
连接迁移	否	支持	最短	小	透明

国防科技大学针对信息系统的应急响应与恢复问题，融合了异构网络技术和漂移技术，提出了“多样化动态漂移技术[15]”，旨在通过分布式动态备份、多样化主动漂移以及快速恢复等机制，使原来网络中静止的和被动的目标变成运动的、主动的目标，通过不断漂移以提高信息系统在信息战环境下的生存能力。

传统漂移技术具有漂移转化时间长、转换力度大、不易管理的缺点；连接迁移技术目前还不成熟，并且需要同时改造网络系统和客户端程序。“多样化动态漂移技术”需要设计并实现多种异构系统，这必然增加系统的开发成本；此外，攻击的多样性和智能性使构成异构系统的组件群复杂度大大增加，无法应用于大型网络系统。

3.4 基于P2P的生存性增强技术

目前，P2P技术广泛地应用在计算和存储共享、搜索、即时通信、网络电视等很多领域。P2P覆盖网具有较强的抗易碎性、可扩展性、健壮性和负载均衡等的特点。

文[16]中，将P2P技术应用到开放层次式网络系统的生存性增强中，如：DNS系统、网络时间同步系统等，该方法将生存性增强的关键归结为P2P覆盖网拓扑的抗易碎性。通过破碎状态检测算法和自愈方法，使得网络系统能够持续提供用户所需要的服务。当发生攻击事件时，通过预先建立的P2P关键服务覆盖网，首先调度资源搜索算法搜索提供类似服务的P2P网中节点，然后将受攻击服务器中的连接关系切换到该节点中，使该节点代替受攻击服务器继续提供对外服务，当节点修复完成以后，重新连接到层次式结构网络中，如图4描述了节点（a,b,b）和（a,b,b,b）遭受攻击后系统连接的变化情况，采用该技术后工作节点数由5个扩展到了8个。

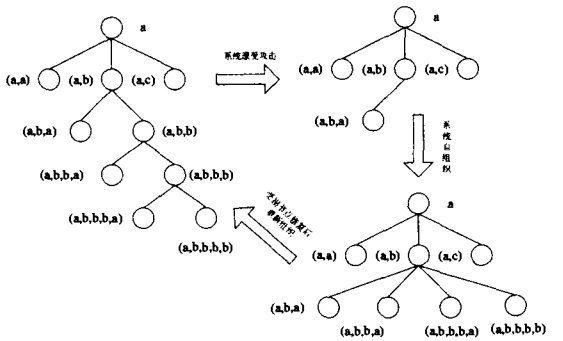

图4 攻击情况下基于P2P技术生存性增强系统连接变化情况示意图

该方法是在动态漂移基础之上的一种扩展。它的动态性和抗易破碎性更加健壮，并有简单的自愈能力。但由于所有P2P网中节点都采用相同的结构，当大规模扩散型攻击会在网络中产生大量的迁移连接，导致网络阻塞，系统瘫痪。

总结 网络系统可生存性评估模型分别从网络系统的系统结构、服务组件、数据流图以及潜在威胁攻击等方面开展，当前评估系统的策略是从不同角度分析系统可生存性，无法发掘影响系统可生存性的关节点，故应该融合网络系统内部因素及外部环境，从主机、系统服务、网络三个层次综合分析系统可生存性，方能形成一个全局的、有效的、量化的评估结果，我们小组正在从事这方面的模型研究。针对网络系统可生存性增强问题的研究，有些还处于理论探索阶段；有些虽然能化解某些已知攻击对系统可生存性的威胁，但攻击的多样性和智能性使异构组件群复杂度迅速增加，极大地增加了开发成本；有些对可生存性自愈方面做出一定贡献，但是在面向大规模扩散型攻击时不仅无法提供有效的增强手段，而且会对整个网络系统造成巨大负面影响。其根本原因是每一种增强技术都非通用的增强方法，无法应对所有的可生存性威胁事件，故只有根据可生存性评估结果，找到影响可生存性的关节点，有针对性地采取增强措施，才能更好地保证系统持续提供服务能力。

网络系统的可生存性是继安全性之后必然考虑的方向，针对网络系统的生存性评估和增强技术的研究虽然取得了一些进展，但整体上并没有形成一个统一的规范，研究成果也较少被实际应用。网络系统生存性评估和增强是一个复杂的工程，涉及的范围比较广泛，本文对近年来研究较多的生存性分析模型和增强技术进行了总结和探讨，并指出了其中的不足。就目前和将来的研究情况来说，可生存性量化方法、可生存网络系统体系结构、可生存性测试平台与工具、可生存性的监测、可生存性评估与增强协作、可生存性进化等技术将是研究重点和热点。本研究小组正在可生存性监测管理平台和可生存性进化技术方向上进行研究，并取得了一些成果。

参考文献

1 Hollway B A, Neumann P G. Survivable computer-communication systems: The problem and working group recommendations [R]. Washington: US Army Research Laboratory, 1993
2 Mead N R, Ellison R J, Linger R C, et al. Survivable Network Analysis Method
3 Ellison R J, Fisher D A, Linger R C, et al. An Approach to Survivable Systems [C]. In: the NATO IST Symposium on Protecting Information Systems in the 21st Century, Washington, DC, 1999, 10
4 Linger R C, Lipson H F, McHugh J, et al. Life-Cycle Models for Survivable Systems [R]. Sledge TECHNICAL REPORT CMU/SEI-2002-TR-026 ESC-TR-2002-026. 2002-10
5 Jha S, Wing J, Linger R. Survivability Analysis of Network Specifications. IEEE, 2000
6 Somesh J, ha Jeannette M. Wing Survivability Analysis of Networked Systems. IEEE, 2001
7 Taylor, Krings, Alves-Foss. Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening. In: ACM Workshop of Scientific Aspects of Cyber Terrorism, November 2002
8 高献伟，林雪纲，许榕生. 生存性分析方法中的3R量化分析. 计算机仿真，2004
9 郭渊博，马建峰. 分布式系统中服务可生存性的定量分析. 同济大学学报，2002
10 Gao Zhixing, et al. Survivability Assessment Modeling Dependencies in Information Systems ISW2001-2002
11 包秀国，胡铭曾. 两种网络安全管理系统的生存性定量分析方法. 通信学报，2004
12 McDermott J. Attack-Potential-Based Survivability Modeling for High-Consequence Systems. IEEE, 2005
13 Linger R C, et al. Requirements Definition for Survivable Network Systems [R]. http://www.sei.cmu.edu/97icre.pdf, 1999
14 Srikitja A, et al. On Providing Survivable QoS Services in the Next Generation Internet [R]. Supported in Part by NSF Grant NCR9506652 and DARPA under Agreement No. F30602-97-1-0257
15 黄遵国，卢锡城，王怀民. 可生存技术及其实现框架研究. 国防科技大学学报，2002.5
16 包秀国. 开放层次式系统的生存性增强技术研究：[哈尔滨工业大学博士论文]. 2005.1