网络信息体系战时生存能力评估

牛志一,王锐华

军事科学院评估论证研究中心，北京 100091

摘要　基于网络信息体系在对抗性实战环境中面临的打击情况,研究了火力打击和网络攻击强度等级划分的标准、网络信息体系战时生存能力评估指标体系与方法,提出了节点和体系两个层次评估相结合、以提供服务的情况为结果的战时生存能力评估框架。

关键词　网络信息体系;生存能力;评估模型

信息化战争是体系与体系之间的对抗。网络信息体系作为作战力量的“聚合剂”、体系效能的“倍增器”,是打赢信息化战争的基础支撑。从“保存自己、消灭敌人”这一战争的根本目的和本质要求角度考虑,具备激烈对抗条件下的战时生存能力,是军队网络信息体系最基本的要求。只有在信息化战争中不被体系毁瘫,并根据任务变化、环境变化、威胁变化做出敏捷有效的调整应对,网络信息体系才能确保作战效能的最大程度发挥,夺取信息化战争的制胜权。

目前对网络信息系统生存能力的概念定义众多,尚未在学术界取得统一的标准,但是卡内基梅隆大学的CMU/SEI 研究小组在1997年给出了相对而言影响力更大、得到更广泛认同的定义[1]:网络信息系统的可生存性是指在遭受入侵、产生故障和发生意外事件时,系统依然能够及时完成关键任务的能力。

1　网络信息体系战时生存能力评估的总体框架

目前对生存能力评估的相关研究主要集中在两个方面:一是对武器装备战时生存能力评估的研究[2-4],在评估指标和评估方法上都取得了一定成果,但基本都局限在单一装备,没有上升到体系的层次,对网络信息体系的评估只能提供有限的参考;二是对网络系统生存能力评估的研究[5-6],形成了较为成熟的3R1A((抵抗性(resistance)、识别性(recognition)、恢复性(recovery)和自适应性(adaptation))模型,但一般只针对网络攻击,而对于战时生存能力来说,敌方的火力打击同样具有非常重要的影响。

现有的与生存能力评估相关研究大部分采用“评估指标+计算模型”的方法,生成无量纲的量化评估结果。此类评估能够在一定程度上衡量生存能力的高低,但是却无法解决军队网络信息体系在建设和应用中面对的最迫切问题:网络信息体系是否能够在对抗环境中支撑作战任务的顺利完成。

针对上述问题,本研究提出了一个以面对一定攻击强度(包括火力打击和网络攻击)为前提,将节点(通信装备与通信设施)和体系两个层次评估相结合,以网络信息体系提供服务的情况为结果,最终形成“面对XX级别的火力打击/网络攻击,网络信息体系能够正常

收稿日期:2018-11-10;修回日期:2018-11-19

作者简介:牛志一,助理研究员,研究方向为体系设计与仿真评估,电子信箱:niuniu99414@163.com

引用格式:牛志一, 王锐华. 网络信息体系战时生存能力评估[J]. 科技导报, 2018, 36(24): 33-36; doi: 10.3981/j.issn.1000-7857.2018.24.004

提供服务/降级提供服务/无法提供服务”评估结论的网络信息体系战时生存能力评估框架,如图1所示。

网络信息体系面对一定强度的攻击时,首先将攻击分解到各节点,利用节点生存性评估指标体系和计算模型,根据节点的属性评估其遭受攻击后的生存情况,形成体系中所有节点生存情况的集合;节点生存情况对体系的结构和性能造成影响,排除在攻击中已经失效的节点,构建新的网络信息体系结构;基于新的结构和性能评估网络信息体系能够提供的服务情况,形成评估结论。

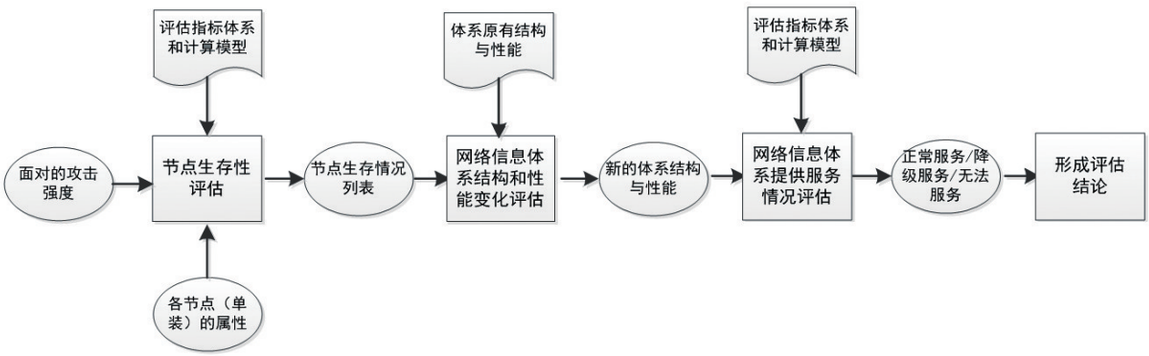

图1 网络信息体系战时生存能力评估框架

Fig. 1 The evaluation framework of networking information-centric system of system survivability in wartime

2 火力打击和网络攻击强度等级划分方法

对攻击强度进行等级划分,是上述网络信息体系战时生存能力评估框架能够应用于实际的前提。对于火力打击和网络攻击这两种攻击方式来说,无论主体、对象、手段方法和杀伤模型等方面都有很大差异。

1)火力打击强度等级的划分方法。

网络信息体系面对的火力打击强度通常由敌方武器的威力和数量决定,参考单一武器装备和建筑物对火力打击的防护经常用能抵抗的TNT当量来衡量,而对于网络信息体系,还需要考虑敌方能够实施的攻击数量和目标选择策略,才能全面评价受到的火力打击强度。

综上,可通过TNT当量、攻击次数和目标选择策略3个指标,设置对火力打击强度的分级标准。在这3个指标中,TNT当量和攻击次数是定量指标,可用其组合指标值作为标准的临界值,例如“5千TNT当量级攻击500次,1万TNT当量级攻击200次,5万TNT当量级攻击100次”,再搭配对目标选择策略的定性描述,如“可根据目标重要程度智能化规划攻击次数和当量投放”,即可界定某一级的火力打击强度标准。

2)网络攻击强度等级的划分方法。

参考林雪纲等[7]在安全事件分级方面的研究成果,从被攻击对象的角度综合考虑攻击事件的抵抗难度和危害程度,通过以下5个指标设置对攻击事件强度的分级标准。

必需资源:发起这种攻击需要的资源如内存和网络带宽如何,需要的资源越少,该指标值越大。

漏洞可利用性:可否利用现有的漏洞来发起该攻击事件,可用漏洞数目多少,是否已经公开,公开多长时间,是否发布了对应的补丁,可利用的漏洞数目越多,漏洞发布时间越久,该值越大。

附带后果:该事件是否会产生其他副作用,累加后会不会造成更大危害,如洪水攻击在可能导致节点崩溃的同时,也会造成网络阻塞,附带后果越大,则该值越大。

恢复代价:需要多少时间或其他资源来恢复因为该攻击事件造成的损害,需要的代价越大,该值越大。

前提条件:发动该事件是否需要其他前提条件,该条件是否容易满足,前提条件越少,该指标值越大。

综合应用层次分析法和专家打分法,每个指标设置一个重要性权值,表示该指标在攻击事件危害性中的比重,针对具体攻击事件由专家为每一指标打分,加权求和后得到该攻击事件区间为[0,1]的强度值。可对强度值记性划分来定义攻击事件强度标准,例如攻击

强度均匀划分为5个等级,那么强度值在 (0.8,1]区间内的事件即为5级攻击事件。如果网络信息体系受到的攻击由多个攻击事件构成,则强度最高的攻击事件等级即为攻击等级。

3　网络信息体系战时生存能力评估指标的体系研究

指标体系是网络信息体系战时生存能力评估的基础,根据评估框架中的需要,网络信息体系战时生存能力评估要考虑节点和体系两个层次,如图2所示。

对节点的评估指标包括火力打击和网络攻击两个方面。面对火力打击的指标可从3个角度考虑:一是“能否降低敌方攻击命中率”;二是“被命中后能否抵抗攻击的杀伤力”;三是“被杀伤失效后能否及时维修恢复或启用备份”,因此评估指标主要包括隐蔽能力、机动能力、干扰和拦截敌方攻击能力、防护能力、维修恢复及备份能力等。面对网络攻击的评估指标参考较为成熟3R1A[8]模型,主要包括抵抗性、识别性、恢复性和自适应性等。

在体系层次上,能够对网络信息体系提供服务造成影响的评估指标,除了体系自身的组成结构以外,还包括其鲁棒性、抗毁性、自组织性等。

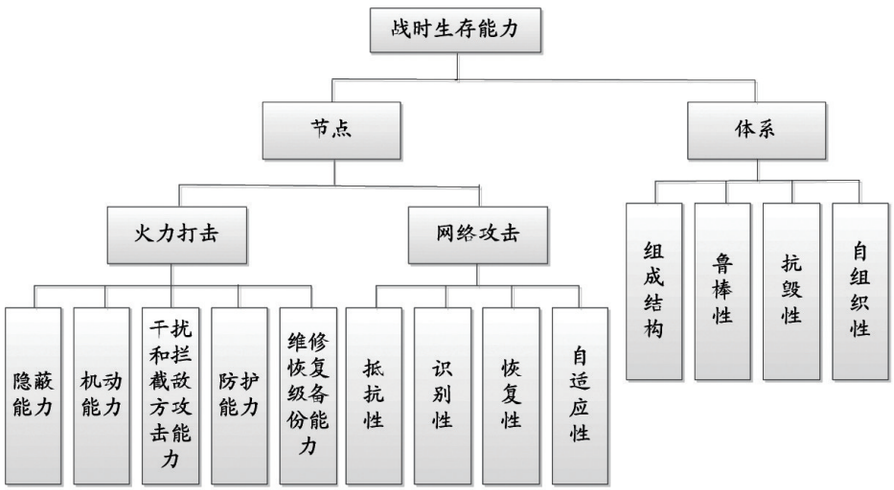

图2　网络信息体系战时生存能力评估指标体系

Fig. 2　The indicator system of networking information-centric system of system survivability in wartime

4　评估方法

定义节点的生存性K为受到攻击依然生存的概率,以生存性对节点生存能力进行评估,根据条件概率的相关公式,对于火力打击:

$$\begin{aligned} K_h &= 1-P_h = 1-P_m P_{f/m} P_{b/f,m} \\ P_m &= (1-K_y)(1-K_j)(1-K_g) \end{aligned} \tag{1}$$

其中,P_h为结点被打击后失效的概率;P_m为打击命中的概率;$P_{f/m}$为打击命中命中后节点未能成功抵抗的概率;$P_{b/f,m}$为节点受损后不能在要求时间内完成维修或启用备份的概率;K_y为因节点隐蔽性使打击未能命中的概率;K_j为因节点机动性使打击未能命中的概率;K_g为成功干扰或拦截打击的概率。

对于网络攻击:

$$K_w = 1-P_w = 1-P_d P_{s/d} P_{h/d,s} P_{z/d,s,h} \tag{2}$$

其中,P_d为网络攻击抵抗失败的概率;K_s为网络攻击抵抗失败后识别也失败的概率;K_h为节点受损后不能在要求时间内及时恢复的概率;K_z为因节点自适应性不能免疫此次攻击的概率。

当节点同时受到独立的多重火力打击或者网络攻击时,最终的生存性为

$$K_o = \prod_{n=1}^{N} K_n \tag{3}$$

式中,N为受到攻击的总数量;K_n为第n次攻击后的生存性。

对网络信息体系中的所有节点进行评估后,可到

全局的生存性清单,在此基础上可以建立网络信息体系的仿真模型,根据所有节点的生存性模拟出体系结构的变化,以及对服务影响的情况。通过多次仿真结果的综合分析,形成对网络信息体系面对一定攻击强度的生存能力评估结果。

5 结论

随着体系作战概念的不断深化发展,网络信息体系在军队战斗力的形成过程中发挥着越来越重要的作用。网络信息体系能否在对抗性实战环境中支撑作战任务的顺利完成,是体系发展过程中不可避免的问题。通过对攻击强度标准、评估指标和评估方法等方面的研究,提出了任务导向的网络信息体系战时生存能力评估框架,得到具有实际意义的评估结果,对于网络信息体系的建设与应用具有重要的指导意义。下一步工作重点在于进一步完善丰富评估指标体系内容,以及深化研究体系结构变化与服务质量的关联模型。

参考文献(References)

[1] Ellison R J, Fisher D A, Linger R C. Survivable network system: An emerging discipline[R]. Technical Report, CMU/SEI-97-TR-013, Carnegie Mellon University, 1997.

[2] 李立甫, 王雨, 朱岩家. 通信装备战场生存能力综合评价方法研究[J]. 重庆通信学院学报, 2008(9): 22-25.

[3] 刘天坤, 熊新平, 赵育善. 网络化防空导弹体系生存能力的评估与权衡[J]. 系统工程与电子技术, 2007, 29(2): 226-229.

[4] 王旭, 宋笔峰. 一对一遭遇时飞机生存力-探测时间解析模型[J]. 航空学报, 2008, 29(4): 914-918.

[5] 王鹏飞, 赵文涛, 张帆, 等. 网络系统可生存能力量化评估的指标体系研究[J]. 计算机工程与科学, 2014, 36(6): 914-918.

[6] 林雪纲, 许榕生. 信息系统生存性的量化分析框架[J]. 电子与信息学报, 2006, 28(9): 1721-1725.

[7] 林雪纲, 郑捷文, 熊华, 等. 计算机与网络事件的分类分级研究[J]. 计算机工程, 2006, 32(9): 4-6.

[8] 王鹏, 王莉, 高斌. 综合电子信息系统生存能力评估方法[J]. 指挥控制与仿真, 2014(10): 67-71.

Study on evaluation of networking information-centric system of system survivability in wartime

NIU Zhiyi, WANG Ruihua

Center for Assessment and Demonstration Research, Academy of Military Sciences PLA, Beijing 100091, China

Abstract On the basis of the situation faced by the networking information-centric system in actual combat environment, this paper studies the criteria for classifying fire strike, network attack intensity, and the indicator system and method for evaluating the system survivability of networking information-centric system in wartime. The evaluation framework of survivability in wartime has two levels, namely node and system, and provides service situation as the result of the evaluation. This work may guidethe system survivability evaluation research of networking information-centric system towards more meaningful results.

Keywords networking information-centric system of system; survivability; evaluation model

(责任编辑 田恬)