网络抗毁性测度研究

明 亮[1], 王东霞[1], 张鲁峰[1], 王春雷[1,2]
(1. 北京系统工程研究所, 北京 100101; 2. 清华大学 计算机科学与技术系, 北京 100084)

摘 要: 针对网络抗毁性测度问题,依据抗毁性三原则——阻挡、识别和恢复,提出了多维网络抗毁性测度提取方法,该方法综合运用了多种抗毁性分析技术,结合实际验证筛选,为提炼抗毁性测度提供了有效途径;提出了三层树状结构的网络抗毁性测度集,为抗毁性测度提供了可行的分类参考;最后,提出了抗毁性测度度量方法并给出了其形式化描述,实现不同类型抗毁性测度值的获取。分析表明,提出的网络抗毁性测度提取方法、测度集合和度量方法具有良好的一致性和可行性。

关键词: 网络; 抗毁性; 测度
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1850-03
doi:10.3969/j.issn.1001-3695.2010.05.069

Research on metrics of network survivability

MING Liang[1], WANG Dong-xia[1], ZHANG Lu-feng[1], WANG Chun-lei[1,2]
(1. *Beijing Institute of System Engineering*, *Beijing* 100101, *China*; 2. *Dept. of Computer Science & Technology*, *Tsinghua University*, *Beijing* 100084, *China*)

Abstract: Metrics of network survivability is a challenge for network security research. This paper presented a new method to find out metrics of network survivability on multi-dimensionality, in accroding with three tenets of survivability: (1) resistance to intrusions, (2) recognition of intrusion effects, (3) recovery of services despite successful intrusions. Presented a metric set of network survivability organized with three-layers structure, which showed a feasible taxonomy for metrics. Presented a new approach to measure network surivivability, i.e. getting value of metrics of network surivivability, for different situations. Finaly, discussed the consistency and feasibility of the three research results above.

Key words: networks; survivability; metrics

网络抗毁性目前是国际网络信息安全界研究的热点[1,2]。网络抗毁性比较公认的定义是 Ellison 等人给出的:是指网络系统在遭受攻击、故障和意外事故时仍能够及时完成其关键任务的能力[3]。网络抗毁的目标是维护必要的网络系统服务,支持组织任务完成。

网络抗毁性测度是网络抗毁性的量化指标,选取合理的网络抗毁性测度,是进行网络抗毁能力评估的客观依据和前提条件。由于网络系统的复杂性以及缺乏对人为有意攻击的建模分析,缺乏对网络抗毁性数据进行系统分析、科学提炼的方法,因此,目前国际上网络抗毁性测度的研究成果非常有限[4]。本文从目前已得到公认的网络抗毁性原则入手,提出了测度提取方法、测度体系和测度度量方法等一整套解决方案,为网络抗毁性测度研究提供了一条系统可行的研究途径。

1 多维度网络抗毁性测度

依据文献[3]中提出的抗毁性三原则,即入侵阻挡、入侵识别和入侵恢复,本文从多个维度进行分析,包括自身属性、网络分层、正逆向分析、模型分析等,提出了多维测度提取方法。

1.1 多维抗毁性测度提取方法

多维测度提取方法的基本原理是:三结合一验证。三结合是在抗毁网络体系结构、威胁模型、攻击模型的基础上,准确分析抗毁需求,将网络抗毁属性分析与网络分层模型分析相结合,将抗毁能力正向分析与逆向分析相结合,并与网络拓扑模型、形式化分析等多种理论分析相结合,建立抗毁性测度初选集;一验证是利用网络抗毁采集数据对抗毁性初选测度进行检验,根据结果判断测度的有效性。方法原理如图 1 所示。

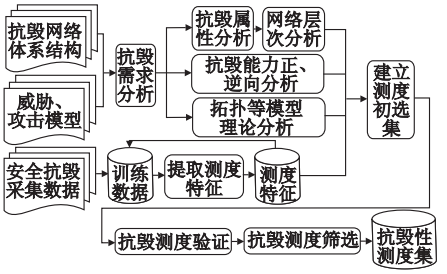

图1 多维抗毁性测度提取方法原理图

多维抗毁性测度提取方法的具体步骤如下:

a)提取网络抗毁性需求。通过对抗毁性网络系统的体系结构、网络威胁模型和攻击模型进行分析,得到准确的抗毁性需求,为后续抗毁性分析提供明确指导。网络抗毁性应包含的能力有阻挡攻击、识别威胁、恢复重构和自适应演化等。网络威胁模型和攻击模型应面向特定恶劣环境下的威胁和攻击,能

收稿日期: 2009-09-22; **修回日期**: 2009-11-02

作者简介:明亮(1979-),男 湖北武汉人,助理研究员,博士,主要研究方向为网络安全、网络技术 (mingliang78@yahoo.com.cn);王东霞,女,研究员,硕导,博士,主要研究方向为网络安全、网络技术;张鲁峰,男,副研究员,博士,主要研究方向为网络安全、网络技术;王春雷,男,助理研究员,博士研究生,主要研究方向为网络安全、网络技术.

对人为攻击、自身故障、意外事故等多种毁伤效应进行单项和组合建模。

b)综合考虑网络抗毁性的多个维度,进行抗毁性测度的三结合分析。结合一是将网络抗毁属性分析与网络分层模型分析相结合,网络抗毁属性包括适应性、鲁棒性、可用性、可控性等;网络分层需考虑网络在链路层、传输层、网络层、应用层等应具备的连通、传输、路由、服务能力等,可使用的工具有体系结构折中分析工具(architecture tradeoff analysis method, ATAM)[5]。结合二是对抗毁能力进行正向与逆向相结合分析,正向分析指的是系统具有的可以通过某些过程达到或获得的性质,通过这些过程获得的网络的性质,不仅可以用来度量一个网络的安全抗毁性,而且还可以用来改进网络的安全抗毁性,如连通性等。而逆向分析则从分析这些性质的对立面入手,将其看成网络的目前没有达到的性质,从反向对系统的抗毁性进行测量。例如,采用多径路由机制的网络,可以采用平均多路径数作为正向测度,而采用路由中断时间作为逆向测度。可使用的工具有抗毁网络分析工具(survivable networks analysis,SNA)[6]。结合三是将网络拓扑模型、形式化分析等多种理论分析相结合,对于部分抗毁性相关属性可以通过严谨的数学建模和逻辑推理,建立指标并进行度量。例如,基于网络拓扑图,可以利用图论中的理论知识,从网络中提取出网络粘聚度、网络连通度、最大连通片尺寸比等重要的抗毁性测度,可使用的工具有新兴算法模拟环境和语言工具(emergent algorithm simulation environment and language,Easel)[7]、NS2、Openet 等。

c)从抗毁性数据中挖掘测度特征。抗毁性数据是指已知某种毁伤及其恢复过程所对应的路由数据、流量数据、配置数据等。利用数据挖掘理论知识,对大量抗毁性原始数据进行相关性分析和相似度分析,形成测度规则库,最终提取出反映网络安全抗毁特征的测度。

d)建立抗毁性测度初选集。综合运用 b)中三种测度分析方法和 c)中基于数据挖掘的测度提取方法,将这些方法提取到的测度和测度特征汇总,建立测度初选集。

e)一验证是把测度初选集放在真实网络或仿真环境中进行验证,加入毁伤激励,通过测量,观察测度值是否发生相应变化,变化是否准确,从而剔出不能有效体现抗毁特性的测度,筛选出合理的测度,再进行测度的去冗余合并,最终得到抗毁性测度集合。

下面以 b)中结合一为例,着重分析从网络分层角度提取抗毁性测度的过程,如图 2 所示。

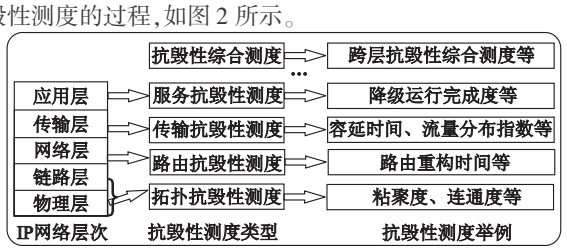

图2　网络抗毁性测度技术途径

根据网络的分层模型,对抗毁性进行进一步细化,得出基于网络连通、路由、传输、业务等能力的抗毁性测度,即拓扑抗毁性测度、路由抗毁性测度、传输抗毁性测度、服务抗毁性测度。拓扑抗毁性测度主要针对网络的链路层,考虑的测度包括网络粘聚度、网络连通度、最大连通片尺寸比等;路由抗毁性测度主要针对网络的网络层,考虑的测度包括路由恢复时间、路由重构时间等;传输抗毁性测度主要针对网络的传输层,考虑的测度是最大容延时间、端端可靠性、端端可用性、节点容量、流量强度指数、流量分布指数等;服务抗毁性测度主要针对网络的应用层,考虑的测度包括全功能运行完成度、降级运行完成度、最低运行完成度等。通过对测度进行科学定义,分析不同层次、类型测度之间的内在联系,继而对多层次、多类型测度进行功能互补、有机融合,最终形成一套行之有效、可操作性强的网络分层抗毁性测度集合。

1.2　网络抗毁性测度集

在网络抗毁性三原则指导下,抗毁网络具有的四个关键特征,即阻挡(resistance)、识别(recognition)、恢复(recovery)和自适应(adaptation)[6]。基于这四个特征,本文结合抗毁属性建立抗毁性测度集,其结构如图 3 所示。

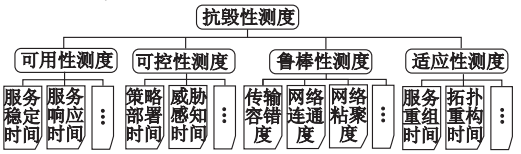

图3　网络抗毁性测度集示意图

图 3 中,以抗毁性测度为根建立了三层树型结构,第二层分为可用性、可控性、鲁棒性和适应性四个中间测度。其中,鲁棒性测度对应抗毁网络的入侵阻抗和入侵识别特征,用于描述网络在遭受网络攻击、物理打击和电磁干扰时,通过外部加固、优化网络结构、设置安全防护措施等手段有效抵抗攻击,避免或减少网络毁伤,同时对毁伤类型、特征进行识别;适应性测度对应抗毁网络的恢复和自适应特征,用于描述网络部分设施被毁伤后,通过预先制定的抗毁策略,调整或重建网络资源,减轻毁伤带来的恶劣后果,保持网络系统功能的连续性,在此过程中使网络得到演变进化,具备未来抵御类似攻击的能力;可用性测度是抗毁网络的最终目标,用于描述网络系统功能在一段时间内的有效程度;可控性测度是抗毁网络的必备属性,用于描述网络系统状态的可感知、可改变程度。第三层为基础测度,是对中间测度的进一步细化和明确,主要包括各种可直接测量或计算的测度,基础测度值的获取方法将在下一章详细描述。

2　网络抗毁性测度度量方法

为了获取网络抗毁性测度集的基础测度值,本文建立基于三种途径的安全抗毁测度度量方法,即基于模型解析的抗毁测度值获取途径、基于仿真实验的抗毁测度值获取途径和基于实网测量的抗毁测度值获取途径,如图 4 所示。

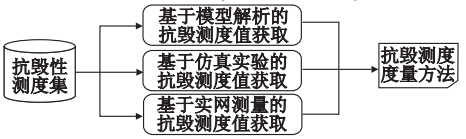

图4　网络抗毁性测度度量方法

基于模型解析的抗毁测度值获取途径主要针对通过理论分析方法提炼出来的测度,其优点是便于实施,缺点是逼真度稍差,测量精度依赖于建模准确性,测量结果有待于真实网络检验;基于仿真实验的抗毁测度值获取途径主要针对在实网中不易或不能得到、但能通过仿真实验获取的测度,如大规模网络的攻破时间,在实网中测量时存在破坏性大、不易重复、代价高的缺点,但是在仿真环境测量就没有这样的顾虑,其缺点是测量结果仍有待于真实网络检验;基于实网测量的抗毁测度值

获取途径主要针对需要在真实环境中得到的测度,如抗毁策略部署时间、威胁感知时间等,其优点是测度值真实可信。在实际度量时,根据可行性进行选择。

在实施度量方法时,针对网络遭受攻击前后的正常、对抗、毁伤、恢复和演化等五个状态阶段,需要为测度构造不同阶段的测试场景,设计不同场景下的测试方法和测试工具,然后将这些场景、方法和工具结合起来,形成针对该测度的测试用例。

基于上述分析,下面对度量方法进行形式化描述。

度量方法描述包括测量途径、测度内容、网络状态三个要素。其中测量途径是度量方法的核心,其他要素是测量途径的约束条件。度量方法的相关概念定义如下:

a)测量途径 W。设 $W=\{w_1,w_2,w_3\}$。其中 w_1,w_2,w_3 分别代表基于模型解析的抗毁测度值获取途径、基于仿真实验的抗毁测度值获取途径和基于实网测量的抗毁测度值获取途径。

b)测度内容 M。设 $M=\{M_1,M_2,\cdots,M_i,\cdots,M_n\}$。其中 M_i 代表 1.2 节抗毁性测度集中的各个测度。

c)网络状态 S。设 $S=\{S_1,S_2,S_3,S_4,S_5\}$。其中 S_1,S_2,S_3,S_4,S_5 分别表示网络的正常、对抗、毁伤、恢复和演化等五个状态阶段。

d)度量方法全集 E。它是网络系统中按三个要素描述的全部度量方法的集合,表示为 $E=W\times M\times S$。

e)度量方法。根据某个具体问题中的实际需求分析构造的一个或多个度量方法,分别表示为 $E_1,E_2,\cdots,E_i,\cdots$,且 $E_i\in E$。设度量方法 $E_k=\{e_l,e_2,\cdots,e_i,\cdots,e_n\}$。其中:$e_i=(x,y,z)$,$x\in W,y\in M,z\in S$,且可以用 $x=w(e_i)$,$y=m(e_i)$,$z=s(e_i)$ 分别表示 X,Y,Z 的值。

各个度量方法描述如下:

a)基于 W 的度量方法。基于测量途径对度量方法进行分类定义。使用函数 fw 定义基于 W 的度量方法,$fw:W->E$。对于 W 中的任意 w,有与之对应的 E 的子集 E_w,即 $\forall w\in W$,有 $E_w\in E$,满足 $f_w(W)=E_w$。E_w 是基于 W 的度量方法。

b)基于 M 的度量方法。基于测度内容对度量方法进行分类定义。使用函数 fm 定义基于 M 的度量方法,$fm:M->E$。对于 M 中的任意 m,有与之对应的 E 的子集 E_m,即 $\forall m=M$,有 $E_m\in E$,满足 $f_m(M)=E_m$。E_m 是基于 M 的度量方法。

c)基于 S 的度量方法。基于网络状态对度量方法进行分类定义。使用函数 fs 定义基于 S 的度量方法,$fs:S->E$。对于 S 中的任意 s,有与之对应的 E 的子集 E_s,即 $\forall s\in S$,有 $E_s\in E$,满足 $f_s(S)=E_s$。E_s 是基于 S 的度量方法。

d)测量途径确定函数。为了确定度量方法中的测量途径,可以将测量途径确定函数定义为 $f:M\times S->\Psi(W)$。函数 f,描述了在某个网络状态中,度量某个测度时,可以确定的相应测量途径。

下面给出使用该度量方法的实例。

假设一个待测网络系统,根据需求确定的 W、M、S 如下:

$W=\{w_1,w_2,w_3\}$ 分别表示三种测量途径;

$M=\{$service responese time (SRT)、threat sensing time (TST)、network link degree (NLD)、topology reconstruction time (TRT)$\}$ 分别表示服务响应时间、威胁感知时间、网络连通度、拓扑重构时间;

$S=\{S_2,S_3,S_4\}$ 分别表示网络的正常、对抗、毁伤、恢复四个状态阶段。

则测量途径确定函数为

$$f(\mathrm{SRT},S_2)=\{w_2,w_3\}$$
$$f(\mathrm{SRT},S_3)=\{w_2,w_3\}$$
$$f(\mathrm{SRT},S_4)=\{w_2,w_3\}$$
$$f(\mathrm{TST},S_2)=\{w_2,w_3\}$$
$$f(\mathrm{TST},S_3)=\phi$$
$$f(\mathrm{TST},S_4)=\phi$$
$$f(\mathrm{NLD},S_2)=\{w_1,w_2,w_3\}$$
$$f(\mathrm{NLD},S_3)=\{w_1,w_2\}$$
$$f(\mathrm{NLD},S_4)=\{w_1,w_2,w_3\}$$
$$f(\mathrm{TRT},S_2)=\phi$$
$$f(\mathrm{TRT},S_3)=\{w_2,w_3\}$$
$$f(\mathrm{TRT},S_4)=\{w_2,w_3\}$$

该被测网络系统的抗毁性基于测度 M 的度量方法为

$$E_{ml}=f_m(\mathrm{SRT})=\{(w_2,\mathrm{SRT},S_2),(w_3,\mathrm{SRT},S_2),(w_2,\mathrm{SRT},S_3),(w_3,\mathrm{SRT},S_3),(w_2,\mathrm{SRT},S_4),(w_3,\mathrm{SRT},S_4)\}$$
$$E_{m2}=f_m(\mathrm{TST})=\{(w_2,\mathrm{TST},S_2),(w_3,\mathrm{TST},S_2)\}$$
$$E_{m3}=f_m(\mathrm{NLD})=\{(w_1,\mathrm{NLD},S_2),(w_2,\mathrm{NLD},S_2),(w_3,\mathrm{NLD},S_2),(w_1,\mathrm{NLD},S_3),(w_2,\mathrm{NLD},S_3),(w_1,\mathrm{NLD},S_4),(w_2,\mathrm{NLD},S_4),(w_3,\mathrm{NLD},S_4)\}$$
$$E_{m4}=f_m(\mathrm{TRT})=\{(w_2,\mathrm{TRT},S_3),(w_3,\mathrm{TRT},S_3),(w_2,\mathrm{TRT},S_4),(w_3,\mathrm{TRT},S_4)\}$$

上述度量方法描述的含义是在某种网络状态下,可以采用某种测量途径对某个测度进行度量。以拓扑重构时间(TRT)测度为例,fm(TRT)表示可以在毁伤、重构两种状态下,采用仿真实验或实网测量的方法对拓扑重构时间进行度量。

基于测量途径 W 的度量方法和基于网络状态 S 的度量方法可同理得到,这里不再赘述。实际中可以把测量途径 W 进一步描述为具体测试工具,则可以得到包含具体测试工具的度量方法。

3　结束语

本文从分析抗毁性内涵入手,基于公认的抗毁性三原则:阻挡、识别和恢复,提出了抗毁性测度提炼方法和抗毁性测度集,提出了针对基础测度的抗毁性测度度量方法并给出了其形式化描述,为研究抗毁性测度提供了系统的解决方案,具有一般性和可行性。下一步将进一步丰富完善抗毁性测度集中的基础测度,同时研究与之相应的度量工具实现技术。

参考文献:

[1] HOWARD F L. Survivability:a new security paradigm for protecting highly distributed mission critical systems[C]// Proc of the 38th Meeting of IFIP Working Group on Dependable Computing and Fault Tolerance. 2000.

[2] MICHA P, TOMASZ S, MICHA Z, *et al*. Path generation issues for survivable network design[C]// Proc of Computational Science and Its Applications ICCSA2008 International Conference. Perugia: Springer-Verlag, 2008: 820-835.

[3] ELLISON B, FISHER D A, LINGER R C, *et al*. Survivable network systems: an emerging discipline, CMU/SEI-97-TR-013[R]. Pittsburgh:Carnegie Mellon University, 1997.

[4] REIJO S. Towards a security metrics taxonomy for the information and communication technology industry[C]// Proc of International Conference on Software Engineering Advances. Finland: IEEE Computer Society, 2007:25-31.

[5] KAZMAN R, KLEIN M, BARBACCI M, *et al*. Architecture tradeoff analysis method, CMU/SEI-98-TR-008[R]. Pittsburgh:Carnegie Mellon University, 1998.

[6] NANCY R M, ROBERT J E, REHARD C L. Survivable network analysismethod, CMU/SEI-2000-TR-013[R]. Pittsburgh:Carnegie Mellon University, 2000.

[7] CHRISTIE A M. Network survivability analysis using easel, Technical Report CMU/SEI-2002-TR-039[R]. Pittsburgh:Carnegie Mellon University, 2002.

[8] VICKIE R W. A definition for information system survivability[C]// Proc of the 37th Hawaii International Conference on System Sciences. Hawaii: IEEE Computer Society, 2004:2086-2096.