高技术通讯 2012 年 第22卷 第4期:374~381

doi:10.3772/j.issn.1002-0470.2012.04.007

基于攻击图的网络安全策略制定方法研究①

马俊春②*** 王勇军* 孙继银**

(*国防科技大学计算机学院 长沙 410073)

(**第二炮兵工程学院 西安 710025)

摘 要 为了提高网络的整体安全性,提出了基于攻击图的网络安全策略制定方法。该方法首先从分布并行处理角度将不同区域的目标网络进行脆弱性分析任务划分,采用分布并行处理技术进行攻击图构建;其次,利用生成的全局攻击图识别目标网络中存在的脆弱性之间的关系,以及由此产生的潜在威胁;最后,将攻击图与遗传算法相结合,建立相应的数学模型,把安全策略的制定问题转化为带有惩罚的非约束优化问题,以最小的成本保证目标网络的安全。实验结果表明,该方法具有较高的攻击图生成效率,并且降低了攻击图生成时的系统资源消耗。该方法可以帮助网络安全管理人员有针对性地进行安全防护,能够适用于评估大规模复杂网络系统的整体安全性。

关键词 大规模网络,网络安全,攻击图,分布并行,安全策略

0 引 言

基于攻击图的网络漏洞分析是加强网络安全的重要方法。攻击图是一种基于模型的网络脆弱性评估方法,它从攻击者的角度出发,在综合分析多种网络配置和脆弱性信息的基础上,枚举出所有可能的攻击路径,从而帮助攻击者或防御者直观地理解目标网络内各个脆弱性之间的关系、脆弱性与网络安全配置之间的关系以及由此产生的潜在威胁。虽然攻击图可以使网络安全管理人员更好地理解网络受到攻击的步骤,但是随着网络规模的增大,软件的增多,网络中的漏洞也越来越多,生成的攻击图已经严重超出人们的理解能力,而且,安全管理人员真正需要的是可操作的安全策略,并根据这些策略提高网络的安全性。因此,研究大规模复杂网络系统的安全策略制定方法具有重要的现实意义。本文从提高网络的整体安全性的角度研究出了一种基于攻击图的网络安全策略制定方法。

1 相关工作

攻击图的构建方法经历了从手工分析到自动分析,从分析小型企业网络到大规模复杂网络的发展过程。Swiler 等首次提出了攻击图模型[1,2],根据已有的攻击模板,从目标状态开始,采用深度优先的搜索策略构建攻击图。由于该方法完全依靠手工完成,因此这种方法不能适用于大规模复杂网络的分析,但为后来的研究者对攻击图的自动产生、自动分析奠定了坚实的基础。目前美国、英国、俄罗斯、以色列等都在该方面投入了大量的科研力量,取得了显著的成果,尤其是美国麻省理工大学、卡内基梅隆大学和林肯实验室等研发出了 TVA[3]、MulVAL[4,5]、NetSPA[6]原型系统。

Phillips 和 Swiler 在文献[7]中首次提出了最小攻击代价分析方法。通过对攻击图的分析可以了解攻击者可能的攻击路径,从而通过改变网络配置达到网络防御的目的。由于分析方法过于简单,其准确性有待进一步考察。Sheyner 等人在文献[8,9]中提出了自动化生成攻击图的方法,并在此基础上提出了最小安全措施分析。Jha[10]等认为每一步原子攻击可以通过安全措施来阻止,他们基于状态攻击图寻找保障目标网络中关键信息资产安全的最小安全措施集。Noel[11-13]等提出的最小代价分析将代价与安全措施相关联,对基于利用的攻击图进行分

① 863 计划(2009AA01Z432)资助项目。

② 女,1983 年生,博士生;研究方向:信息安全;联系人,E-mail: chenshan1223@126.com

(收稿日期:2010-11-29)

析,他们认为阻止原子攻击的最好方式是从源头上把引起这些原子攻击发生的前提属性消除掉,并且每个安全弥补措施需要一定的成本,他们基于属性攻击图提出了最小成本的安全弥补措施集,但是该方法不适用于大型的具有含圈攻击路径的攻击图。Homer[14]等人认为采取安全弥补措施提高网络的安全性受到多种条件的约束,如重要服务的可用性需求、潜在威胁的代价以及安全弥补措施的成本,基于逻辑攻击图提出了一种自动化网络配置管理方法迭代寻找权衡了各种约束的网络配置方案,但是该方法无法应用于网络规模较大的真实目标网络。Lingyu[13]提出基于逻辑推理的方法,首先把该问题转化为布尔表达式,然后通过求该表达式的析取范式计算出所有的弥补措施集合,在此基础上求最小化弥补集,该方法在最坏情况下具有不可避免的指数时间复杂度,无法应用于网络规模较大的真实目标网络。

目前已涌现出了多种攻击图构建方法和安全策略制定方法,但通过分析发现,现有方法存在以下两方面的不足:第一,攻击图构建过程存在复杂度高、扩展性能低、状态爆炸问题,导致攻击图生成时的系统资源消耗较大,从而难以适用于大规模复杂网络系统。第二,安全策略制定方法可操作性差,难以应用于网络规模较大的真实目标网络。

为了解决上述问题,本文提出了一种基于分布并行处理的攻击图构建方法,该方法采用限制攻击步骤数和分布并行处理技术的优化策略,力图有效降低攻击图的规模,减少生成攻击图所需的系统资源。在此基础上,利用遗传算法将安全策略的制定问题转化为带有惩罚的非约束优化问题,以最小的成本保证目标网络的安全。

2 基于攻击图的网络安全策略制定方法

2.1 相关定义

为支持攻击图构建方法的可扩展性,能够适用于大规模复杂目标网络,本文采用分布并行的方法对脆弱性分析进行优化处理:首先将大规模复杂网络分为多个子网并进行编号;然后将防火墙安全策略进行预处理,提取出 accept 规则,并按子网编号进行分类;最后分布并行地构建不同子网的攻击图(即子攻击图),并将这些子攻击图融合成完整的攻击图(即父攻击图)。

定义 1:子攻击图(sub-attack graph, SAG)。SAG 定义为三元组 $< Attribute, Exploit, Edge >$,其中 *Attribute* 表示属性节点,包括原子攻击的前提属性集合和攻击被实施后所获得的新的后果属性集合。其初始值即初始属性节点集合,描述了目标网络在遭受攻击前主机上所运行的服务、开放的端口、存在的脆弱点以及预处理中提取出的防火墙 accept 安全策略等相关属性。*Exploit* 表示原子攻击节点,攻击者在对目标网络进行攻击时,通过有序的实施原子攻击不断改变目标网络的属性,从而一步一步地达到攻击者的目的。*Edge* 是有向边集合,包括原子攻击的前提边集合和原子攻击的后果边集合。SAG 满足下列约束:

(1)对 $\forall e \in Exploit$,令 Pre(e)为 e 的父节点集合,Post(e)为 e 的子节点集合,则($\wedge$Pre(e))$\rightarrow$($\wedge$Post(e)),表示只有当原子攻击的所有前提属性全部满足后,攻击者才能实施该原子攻击,且当原子攻击被成功利用后,其后果属性也全部满足。即该约束表示原子攻击的所有前提属性节点之间存在“与”关系。

(2)对 $\forall a \in Attribute$,令 Pre(a)为 a 的父节点集合,则($\vee$Pre(a))$\rightarrow a$,表示只要父节点集合中的任意一个原子攻击被成功实施后,属性 a 就能被满足。即该约束表示属性节点的父节点集合中的原子攻击之间存在“或”关系。

定义 2:父攻击图(total attack graph, TAG)。TAG 定义为三元组 $< SAG, Policy, Edge >$,其中 *SAG* 为采用正向、广度优先搜索的策略构建的子攻击图集合。*Policy* 为预处理中提取出的防火墙 accept 安全策略。*Edge* 是有向边集合,依据防火墙的 accept 安全策略,将不同的子攻击图连接起来。

定义 3:基于攻击图的网络安全策略制定方法定义为 8 元组:AGGA = (A, B, N, F, S, C, M, E)。其中:

(1) A 为本文提出的基于分布并行处理的攻击图构建方法(详细见 2.2 节)快速构建的攻击图。

(2) B 为对染色体进行编码,从而决定初始种群。编码的基本要求是要为染色体的基因型(代码串)和表现型(参数值)建立对应关系。本文采用二进制代码进行编码,对应关系就是二进制与十进制的转换关系。

(3) N 为初始种群。群体的个体数(群体的规模) N 应取得适中,如果 N 过小,则不易求得全局最小化解,若 N 过大,则运算量过大,收敛速度减慢,通常 N 取编码长度的 2 倍。

(4) F 为染色体适应度函数。适应度函数是遗传算法进行选择、交叉和变异操作的依据,该函数的选取是一个技巧性很高、而理论上的研究又很不充分的复杂问题。

(5) S 为遗传算法基本的遗传算子之一:选择(selection)。即从初始种群中按一定的标准选定适应做亲本的染色体。按照达尔文的适者生存理论,愈能适应环境的生物品种,愈能繁衍(复制)其后代,而不适应环境的生物,其生存和繁衍能力较低,甚至可能被淘汰,所以选择的目的是为了将适应的染色体交配后复制出子代。

选择的方法较多,常用的有期望值法、适应度概率法(赌轮法)、最佳个体保存法等。DeJong 曾对以上三种方法的遗传算法性能进行对比,实验表明,采用期望值法的遗传算法,其离线性能与在线性能均高于采用另外两种方法的遗传算法性能,而采用赌轮法时,可能会产生随机误差,这种误差特别在群体数较大时更易发生。根据实际应用情况,本文采用期望值法。

(6) C 为遗传算法基本的遗传算子之一:交叉(crossover)。即为两个染色体的基因进行互换产生新的后代。与选择操作相比较,交叉操作能使基因排序变化更加灵活,实现真正意义上的人为重组,适于大范围操作。

在具体的实现过程中,交叉分两个步骤:第一步是选择两两匹配的对象,第二步是决定交换点及交换规则。常用的交叉方式有单点交叉、双点交叉、按序交叉和位置交叉等,根据实际应用情况,本文采用单点交叉。

(7) M 为遗传算法基本的遗传算子之一:变异(mutation)。即生物体中某一个或某几个基因位的变化,这种概率是很小的,在自然选择中,通常是千分之几或百分之几。由于本文采用二进制方式进行编码,所谓变异就是将基因值取反,即将 0 变 1,1 变 0。

(8) E 为遗传算法终止条件。经过选择、交叉、变异操作后得到新一代种群的基因型,对此种群再进行适应度计算,这一过程称为迭代。根据大量反复的实验数据结果,总结出判断遗传算法结束的条件是:

首先,根据初始属性的数目,即根据网络的规模,设定最小迭代次数。对于小规模,迭代次数可以小一些,比如 10,但对于大规模,迭代次数要大一些,比如 100。

其次,当迭代次数超过最小迭代次数时,则要判断新一代中是否存在某个染色体的选择概率超过 80%(用户可以自己设定)。如果存在,程序结束;若新一代中所有的染色体都相同,则程序结束。

定义 4:间隔元素、终端元素。所谓间隔元素,是指由于不同的搜索深度有可能具有相同的攻击路径,因此不同搜索深度的元素之间需用 (IP: IP) 隔开,(IP: IP) 则称为间隔元素。所谓终端元素,是指假设 IP_1 和 IP_2 之间存在攻击路径,即 (IP_1: IP_2) 满足,IP_2 为最终攻击目标,则称该元素为终端元素。

2.2 基于分布并行处理的攻击图构建方法

SAG 生成算法的思想及实现方法:首先根据子网的初始属性和攻击者的初始能力,采用正向、广度优先搜索策略,由攻击者所在的起始位置出发,依次分析其可达主机的可攻击性,并将可攻击的主机及其端口记录在队列 *BFSqueue-attackhost* 和 *BFSqueue-attack* 中。即根据子网的初始属性和攻击者的初始能力判断哪些攻击模式可以被攻击者利用,查询攻击模式和子网中的脆弱性信息,把攻击模式实例化;然后根据队列 *BFSqueue-attackhost* 和 *BFSqueue-attack* 中的信息,生成攻击路径。算法流程图如图 1 至图 3 所示。其中,图 1 为 SAG 生成算法流程图,图 2 为正向搜索算法流程图,图 3 为攻击路径生成算法流程图。对于攻击者所在的子网,在执行 SAG 生成算法时,该子网的初始属性和攻击者的初始能力由用户输入或者工具扫描获得。对于其余的子网,在执行 SAG 生成算法时,该子网中攻击者的初始能力从防火墙安全策略的 accept 规则获得,即假设 accept 规则中的源主机已经被攻击者攻下,是攻击者的起始位置。

SAG 生成算法说明如下:队列 *BFSqueue-start* 存放攻击者的起始位置集合。第一步,判断 *BFSqueue-start* 是否为空,如果为空,说明没有攻击者,则程序结束,否则提取 *BFSqueue-start* 的第一个元素进行分析,同时删除此元素,依次调用正向搜索子程序(图 2 所示)和攻击路径生成子程序(图 3 所示);第二步,循环执行第一步,直至 *BFSqueue-start* 为空,即分析了所有的攻击对。

正向搜索算法描述:在正向搜索算法具体的实现过程中,本文定义了 3 个队列:*BFSqueue-attackhost*、*BFSqueue-attack* 和 *BFSqueue*。其中 *BFSqueue-attackhost* 以(攻击点主机:目标攻击点)的格式存放攻击成功的主机对集合,该队列反映从

起始攻击点到目标攻击点的搜索路径,由于主机可以开放多个端口,可以同时存在多个攻击,因此队列中有重复的元素;*BFSqueue-attack* 以(攻击点主机:攻击目标主机:目标主机端口)的格式存放攻击成

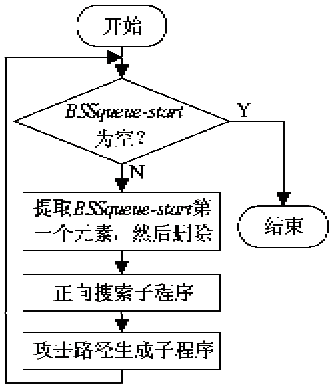

图1 SAG生成流程图

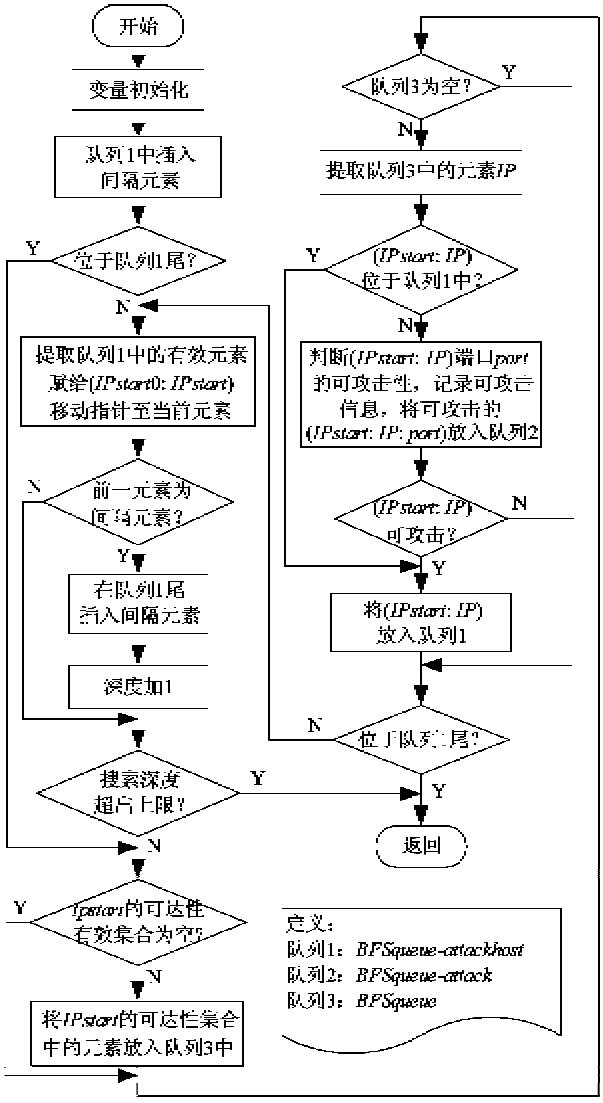

图2 正向搜索算法实现流程图

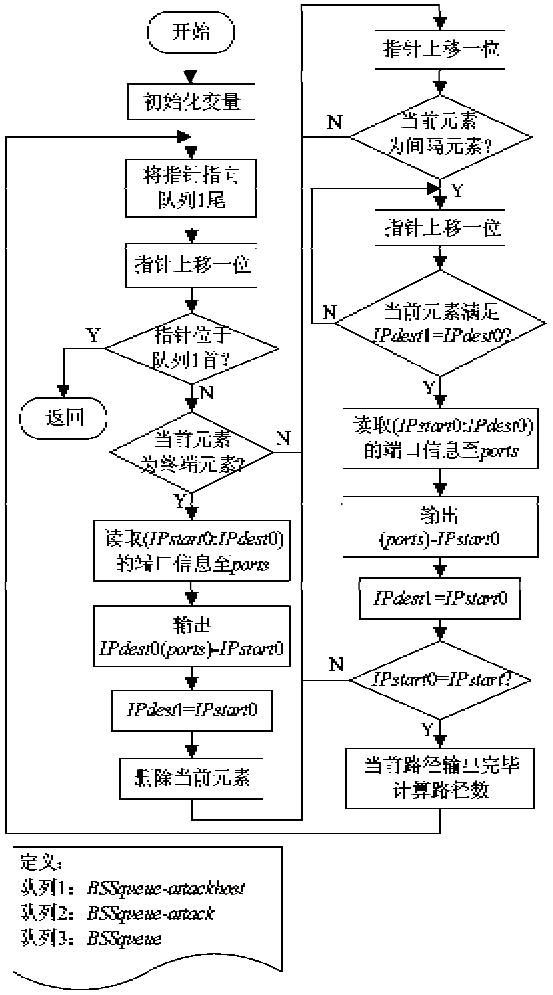

图3 攻击路径生成实现流程图

功的主机对集合,由于该队列反映攻击点主机通过哪些端口可以攻下攻击目标主机,因此该队列中没有重复的元素;*BFSqueue* 是一个动态队列,存放起始攻击点的所有可达主机。

算法通过间隔元素将不同搜索深度的有效元素间隔开,以便在攻击路径生成子程序中能够有效识别。在具体算法实现中,首先提取队列 *BFSqueue-attackhost* 中的有效元素,以该元素中的目标攻击点为新的攻击点主机,判断其可达性集合中是否有可攻击的主机,如果有,则分别将该攻击对和可攻击信息放入队列 *BFSqueue- attackhost* 和 *BFSqueue-attack* 中。通过依次对队列 *BFSqueue-attackhost* 中的有效元素进行判断,便可实现从起始攻击点到最终攻击目标的正向搜索。

由于攻击者不会采用很复杂的攻击手段,就是说攻击者不会以太多的主机为跳板进行攻击,而且有的攻击路径根本不会出现攻击目标,对此攻击路径进行更深层次的搜索没有意义,因此在正向搜索

算法的实现过程中,采用限制搜索深度的策略,此搜索深度可以由用户设定。

攻击路径生成算法描述:本算法结合间隔元素和终端元素,先不考虑端口情况,从 *BFSqueue-attackhost* 的队列尾开始,分析 *BFSqueue-attackhost* 中主机的攻击路径,然后结合 *BFSqueue-attack* 中主机的端口信息,逐一写出攻击路径。

TAG 生成算法的思想及实现方法:(1)将防火墙安全策略的 accept 规则进行分类。如果策略中未出现对称的规则,则不需分类,如果出现对称的规则,则将此策略分为 A、B 两类,即对称的规则不能同时出现。比如策略中的 accept 规则为子网 1→子网 2,子网 1→子网 3,子网 2→子网 1,因为子网 1→子网 2 与子网 2→子网 1 对称,所以该策略应被分为两类,A 类为子网 1→子网 2,子网 1→子网 3,B 类为子网 2→子网 1。(2)依次判断 accept 规则中的源主机是否被攻击者攻下,如果被攻下,该 SAG 不需改变,如果没被攻下,则应去掉 SAG 中与之有关的攻击路径。(3) 依据防火墙安全策略的 accept 规则,将所有的 SAG 连接起来。其算法流程图如图 4所示。

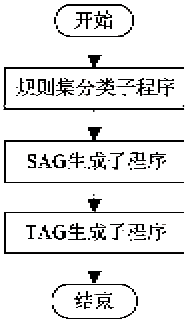

图 4 父攻击图生成算法程序流程图

在算法实现过程中,定义了 2 个队列:(1) *ACCqueue*,以"Type-规则"的格式存放分类好的规则集;(2) *SAG-queue*,存放根据规则集修正后的各类子攻击图集合。算法主要由 3 个子程序构成:规则集分类子程序(对 accept 规则进行分类,其算法流程图如图 5 所示);SAG 生成子程序(分布并行地构建不同子网的攻击图);TAG 生成子程序(将不同的子攻击图 SAG 融合成完整的攻击图,其算法流程图如图 6 所示。)

2.3 基于遗传算法的安全策略制定方法

攻击图直观地展示了攻击者对目标网络进行攻击的全部路径,便于网络安全管理人员采取相应的

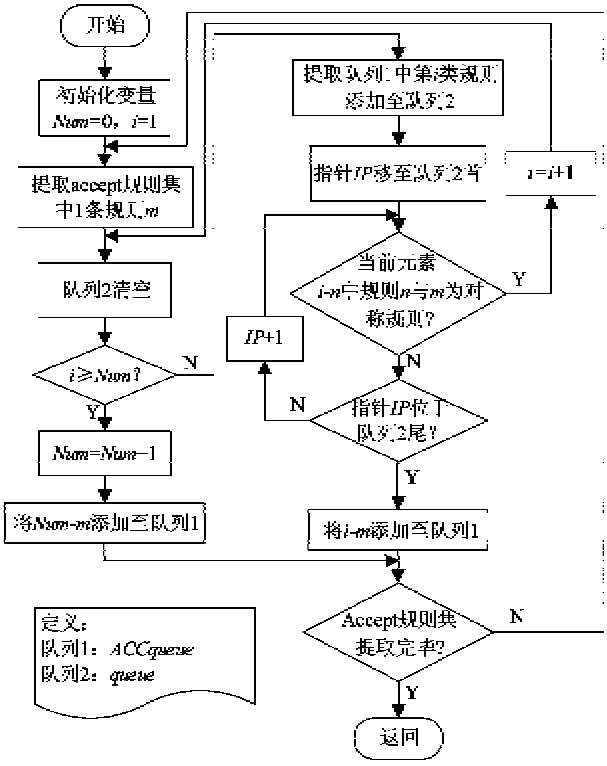

图 5 规则集分类子程序流程图

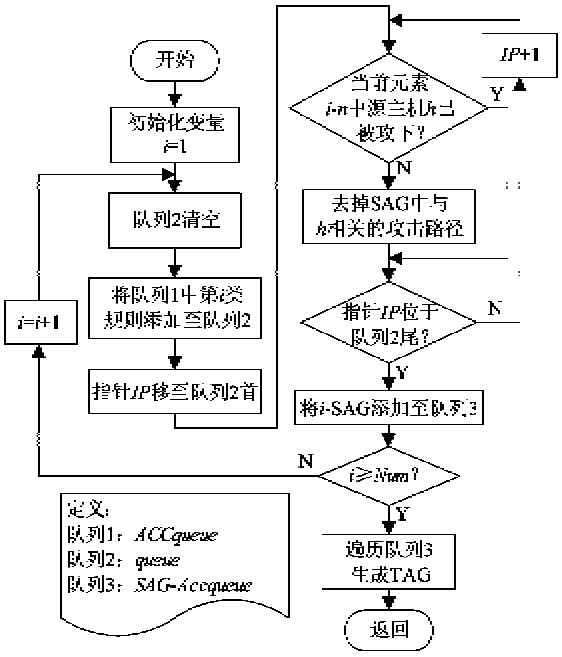

图 6 TAG 生成子程序流程图

安全策略进行防护。但随着网络规模的增大,生成的攻击图已经严重超出人们的理解能力,同时,由于采取不同的安全策略,需要不同的安全成本,因此在对网络安全策略制定方法的研究中,不可避免地面临一个在有限资源前提下的最优化决策问题,即以最小的安全成本获取保证目标网络的"适度安全",

该问题称为最优安全策略问题。

一方面由于最优安全策略问题是 NP 完全性问题[15],对于 NP 完全性问题,精确式搜索是不可能实现的,只能采用启发式搜索方法;另一方面与其它寻优算法相比,遗传算法具有以下优势[16]:(1)覆盖面大,利于全局择优;(2)对问题的依赖性较小,求解的鲁棒性较好;(3)具有并行计算的特点,可以用大规模并行计算来提高计算速度;(4)特别适用于复杂大系统问题的优化求解。因此,本文提出了一种基于遗传算法的安全策略制定方法。

在上节生成的攻击图的基础上,本文基于逻辑推理的方法,首先将攻击目标根据生成的攻击图转化为初始属性的布尔表达式 $g(x)$,然后再确定应采取的安全策略。在实际的应用中,首先要满足 $g(x)=0$,然后在使 $g(x)=0$ 的集合 $\{x_1, x_2, x_3, \cdots, x_n\}$ 中选出代价最小的 x。为了解决此问题,本文采用一种惩罚方法(penalty method),该方法的基本思想是设法对个体违背约束条件的情况给予惩罚,在适应度函数中用惩罚函数来具体体现这种惩罚,把约束优化问题转化成一个带有惩罚的非约束优化问题。

为了更好地说明安全策略制定方法的产生过程,将其应用于图 7 简单的攻击图实例,假设攻击目标为 $\{c_7\}$,且 $\mathrm{Cost}(c_1)=10$,$\mathrm{Cost}(c_2)=1$,$\mathrm{Cost}(c_3)=15$,$\mathrm{Cost}(c_4)=1$,通过手工分析,在此情况下最优安全策略为 c_2。下面验证本文所提方法的正确性。求解步骤如下:

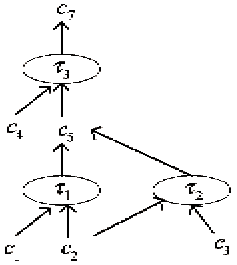

图 7　攻击图实例

(1)对染色体进行二进制编码。针对图 7 的攻击图,有 4 个初始属性 $c_1c_2c_3c_4$,采用二进制进行编码,0 表示不对该属性进行操作,1 表示对该属性进行弥补,比如 0001 则表示只对 c_4 进行弥补操作。由于所有的染色体基因型在 0001 与 1111 之间,则对应的十进制数值在 1 ~ 15 之间变化。

(2) 确定初始种群。由于染色体由 4 个基因组成,编码长度为 4,所以 N 取 8。

(3) 决定适应度函数 t_i。首先根据图 7 将攻击目标 c_7 转化为初始属性的布尔表达式 $g(x)$;其次将求最优安全策略问题转化成一个带有惩罚的非约束优化问题。通过大量的实验数据,针对 c_7 的适应度函数,当 r 取 30 时,可使惩罚适当。

$$f_i = -[\mathrm{cost}(c_1)\cdot c_1 + \mathrm{cost}(c_2)\cdot c_2 + \mathrm{cost}(c_3)\cdot c_3 + \mathrm{cost}(c_4)\cdot c_4] + r[1-g(x)]$$

$$t_i = (f_i - f_{\min} + 1)\cdot 100$$

$$g(x) = c_4 \wedge ((c_1 \wedge c_2) \vee (c_2 \wedge c_3))$$

(4) 计算选择概率 $P_i = t_i / \sum t_i$。

(5) 判断是否满足终止条件。若存在某个个体的选择概率 $P_i > 80\%$,或种群中相同个体的比重 $>80\%$,或迭代次数 >300 次,则迭代终止,找出最优解,执行第 10 步,否则执行第 6 步。

(6) 选择运算。根据期望值法每次随机选择一个个体作为父本,选择概率 P_i 越大的个体被选择成为父本的几率越大。

(7) 交叉运算。首先对父本进行随机配对,然后对每一对父本随机确定交叉染色体起始位置 a,对 a 位置以后的染色体进行交换。

(8) 变异运算。以 1% 的概率对交叉后产生的新的个体进行某个染色体的变异运算,即当某个个体的某个染色体变异时,对该染色体进行求反运算。

(9) 迭代执行第 4 步。

(10) 程序输出最优解 c_2,即 c_2 为该实例网络的最优安全策略,与手工分析结果一致。

该方法的核心算法如图 8。

3　实验结果及分析

通过模拟实验验证安全策略制定方法的有效性、可扩展性,模拟实验的硬件平台为 4 核 P4 3.2GHz处理器、4G 内存。

图 9 所示为在相同的实验环境下,分别将本文中算法与文献[13]和[15]中方法应用在初始属性个数为 50、100、200、500、1000 和 2000 的条件下,计算模拟网络的最优安全策略,分析它们在计算最优安全策略时 CPU 运行时间的变化趋势,如图 9 所示。从图中可以看出,文献[13]中算法具有较差的可扩展性,CPU 性能关于初始属性个数成指数增长,而本文中算法与文献[15]中算法的 CPU 性能关于初始属性个数成多项式增长,具有良好的可扩展性,同时,本文所提方法的性能优于文献[15]。

```
while(1)
{
    if (!flag)
    {
        creatInitdual(x00);
        floop=0;
        flag=true;
    }
    //计算适应度函数
    computFit(x00,fy);
    //计算选择概率
    computPi(fy,piy);
    //迭代终止条件：最大概率>80%，迭代次数大于
LOOPMIN
    py=xpi[0];
    if          ((int)(py*100-0.5)>80
(int)(py*10000)==(int)(1.0/XNUM*10000) |xpinum>0.8*XNUM)
    {
        if (floop<LOOPMIN)
            flag=false;
        else
            break;
    }
    if (floop>=LOOPMAX)
        break;
    floop++;

    if (flag)
    {
        //选择父代个体
        selectFather(x00,piy);
        //交叉operator
        breedSon(x00);
        //变异
        variation(x00);
    }
}
//找到最优解
findbest(x00,piy);
```

图 8 安全策略制定方法的核心算法

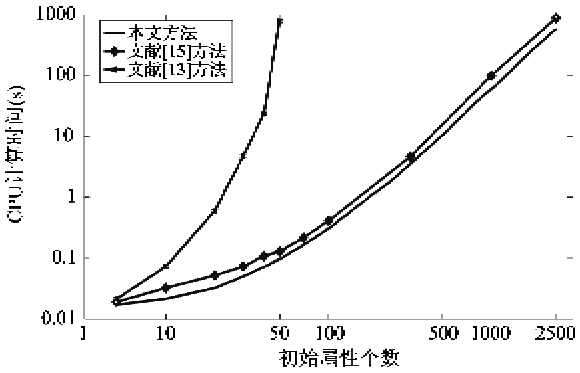

图 9 安全策略制定方法实验曲线图

4 结 论

为了提高网络系统的整体安全性，本文利用 Mysql、Visual Studio 2008、Graphviz、Visio 2007 等工具实现了攻击图的快速构建，该方法采用限制攻击步骤数和分布并行处理技术的优化策略，有效支持了攻击图构建方法的可扩展性，并将遗传算法应用于安全策略制定方法中。与其它寻优算法相比，遗传算法具有并行计算的特点，可以用大规模并行计算来提高计算速度，特别适用于复杂大系统问题的优化求解等问题。

参考文献：

[1] Swiler L P, Phillips C, Ellis D, et al. Computer attack graph generation tool. In: Proceedings of DARPA Information Survivability Conference and Exposition, Anaheim, USA, 2001. 1307-1321

[2] Swiler L P, Phillips C. A Graph-Based Network-Vulnerability Analysis System. Technical Report, SANDIA Report No. SAND97-3010/1, 1998

[3] Noel S, Jajodia S. Understanding complex network attack graphs through clustered adjacency matrices. In: Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, USA, 2005. 1063-9527

[4] Ou X M, Boyer W F, McQueen M A. A scalable approach to attack graph generation. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, USA, 2006. 336-345

[5] Ou X M. A logic-programming approach to network security analysis: [Ph. D dessertation]. Princeton: Princeton University, 2005. 56-67

[6] Lippmann R P, Ingols K W. Evaluating and Strengthening Enterprise Network Security Using Attack Graphs. Project Report, ESC-TR-2005-064

[7] Phillips C, Swiler L. A graph-based system for network vulnerability analysis. In: Proceedings of the New Security Paradigms Workshop, Charlottesville, USA, 1998. 71-79

[8] Sheyner O, Haines J, Jha S, et al. Automated generation and analysis of attack graphs. In: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, USA, 2002. 254-265

[9] Sheyner O, Wing J M. Tools for generating and analyzing attack graphs. In: Proceedings of the Workshop on Formal Methods for Components and Objects, Tehran, Iran, 2004. 344-371

[10] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs. In: Proceedings of the 15th IEEE Computer Security Foundations Workshop, Cape Breton, Canada, 2002. 49-63

[11] Noel S, Jajodia S, O'Berry B, et al. Efficient minimum-

cost network hardening via exploit dependency grpahs. In: Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, USA, 2003. 86-95

[12] Noel S, Jacobs M, Kalapa P, et al. Multiple coordinated views for network attack graphs. In: Proceedings of the Workshop on Visualization for Computer Security, Minneapolis, USA, 2005. 99-106

[13] Wang L, Noel S, Jajodia S. Minimum-cost network hardening using attack graphs. *Computer Communications*, 2006, 29(18):3812-3824

[14] Homer, J. A comprehensive approach to enterprise network security management:[Ph. D dessertation]. Manhattan: Kansas State University, 2008. 24-31

[15] 陈峰, 张怡, 苏金树等. 攻击图的两种形式化分析. 软件学报, 2010,21(4):838-848

[16] 朱剑英. 智能系统非经典数学方法. 湖北:华中科技大学出版社,1999. 20-38

A novel method of constituting network security policy based on attack graphs

Ma Junchun[*,**], Wang Yongjun[*], Sun Jiyin[**]

([*]School of Computer Science, National University of Defense Technology, Changsha 410073)

([**]The Second Artillery Engineering Institute, Xi'an 710025)

Abstract

In order to improve a network's total security, a novel method of constituting security policy based on attack graphs is presented. Firstly, it divides the total network into different areas, and uses the parallel and processing technology to constitute attack graphs; Secondly, it uses the overall attack graph to identify the network vulnerabilities' dependencies and the resulting potential threat; Finally, it combines the attack graph with the genetic algorithm to establish the corresponding mathematical model, so as to transform the constitution of a security policy into a non-restraint optimization problem with penalty to guarantee the network security with the least cost. The experimental results show that this method can improve the efficiency of attack graphs' generation and reduce the system's resource consumption greatly. The proposed method can help network security managers guard networks and can be used to assess large-scale networks' overall security.

Key words: large-scale network, network security, attack graph, distributed paralleled processing, security policy