基于最优攻击路径的网络安全增强策略研究

李庆朋[1] 王布宏[1] 王晓东[1] 张春明[2]
(空军工程大学信息与导航学院 西安 710077)[1] (空军西安飞行学院 西安 710077)[2]

摘 要 为实现目标网络的适度安全,提出了一种基于最优攻击路径的网络安全增强策略制定方法。该方法对攻击目标进行风险评估,在分析攻击图最优攻击路径的基础上制定安全增强策略。为了获取最优攻击路径,提出了一种基于蚁群优化算法的最优攻击路径生成方法,并改进了信息素更新方式。仿真实验表明,所提方法能够有效地产生安全策略集,改进后的蚁群算法具有较强的全局搜索能力和更好的收敛性。

关键词 攻击图,蚁群优化算法,最优攻击路径,网络安全
中图法分类号 TP393 **文献标识码** A

Approach on Network Security Enhancement Strategies Based on Optimal Attack Path

LI Qing-peng[1] WANG Bu-hong[1] WANG Xiao-dong[1] ZHANG Chun-ming[2]
(Information and Navigation Institute, Air Force Engineering University, Xi'an 710077, China)[1]
(Air Force Flight Academy of Xi'an, Xi'an 710077, China)[2]

Abstract To reach the proportional security of the goal network, an approach on network security enhancement strategies based on optimal attack path was proposed. The approach assesses the risk of attack target, and makes strategies for network security enhancement on the basis of optimal attack path. To obtain optimal attack path, an approach to generating optimal attack path based on ant colony optimization algorithm was proposed, and the pheromone updating way was improved. Simulation results show that the proposed approach can generate strategies effectively, and the improved ant colony optimization algorithm has strong global search ability and rapid convergence.

Keywords Attack graphs, Ant colony optimization, Optimal attack path, Network security

1 引言

深入分析网络安全脆弱性,不仅要分析目标网络中存在的每个脆弱点的影响,还要研究各脆弱点之间的内在联系。攻击图是一种基于模型的网络脆弱性评估方法,可自动分析目标网络内各脆弱点之间的联系,在此基础上,枚举所有可能的攻击路径[1]。为提高网络安全性,需要制定并实施一系列安全增强策略[2],以降低被攻击目标的安全风险,使其控制在可接受的范围内。关于安全增强策略,文献[3]利用贪心算法获得攻击者在成功入侵目标之前必须利用的最小关键脆弱点集合,根据集合制定并实施安全增强策略,使集合中的所有脆弱点失效,从而使攻击者无法成功入侵目标。文献[4]提出了最小化分析的方法,即通过尽可能少地修复攻击图的一些漏洞使整个攻击图失效。上述方法都是通过使整个攻击图失效,来完全消除攻击目标的安全风险。而根据信息安全风险控制理论,信息安全风险控制是依据风险评估的结果,评估成本与效益,采取适当的安全控制措施,使风险控制在可承受的风险程度之内。因此,本文提出了一种基于最优攻击路径的网络安全增强策略制定方法,该方法从攻击者的角度出发,通过逐步破坏最易被攻击者选择的最优攻击路径,来降低安全风险,达到适度安全。其中,攻击图的最优攻击路径生成是研究的重点和难点;蚁群优化算法(Ant Colony Optimization, ACO)是由 Dorigo 提出的一种群体智能算法[5],它通过随机策略解决复杂组合优化问题,如旅行商(TSP)问题[6]、车辆路径问题[7,8]等。在此基础上,本文提出了一种基于 ACO 算法的最优攻击路径生成方法。

2 安全策略制定框架

定义 1(攻击图) 攻击图是一个状态转换系统,本文用四元组 $G=(S,T,s_0,s_g)$ 表示。其中,S 是网络安全状态集合;$T\subseteq S\times S$ 是原子攻击集合,表示安全状态转换关系;$s_0\in S$ 是网络初始状态;$s_g\in S$ 表示攻击目标状态。

定义 2(攻击代价) 原子攻击 $\tau_i(\tau_i\in T)$ 的攻击代价 $Cost(\tau_i)=1-Complexity(\tau_i)$,表示攻击者成功利用原子攻击 τ_i 需花费的代价。其中,$Complexity(\tau_i)$ 表示原子攻击 τ_i 的攻击复杂度,复杂度值越大,表示该原子攻击越容易被成功执行。文献[9]对几百种原子攻击进行了分析和对比,给出了攻击复杂度的量化标准,参考该标准可获得原子攻击的攻击复杂度,进而得到其攻击代价。

定义 3(攻击路径) 设 $path=s_0\rightarrow s_1\rightarrow\cdots\rightarrow s_n$ 是给定攻

到稿日期:2012-06-18 返修日期:2012-10-18 本文受陕西省自然科学基金(2010JM8004)资助。
李庆朋(1988-),男,硕士生,主要研究方向为计算机网络安全,E-mail:liqingpeng0219@foxmail.com;王布宏(1975-),男,博士,副教授,主要研究方向为计算机网络安全;王晓东(1976-),男,博士,讲师,主要研究方向为计算机网络安全;张春明(1986-),男,硕士,主要研究方向为计算机网络攻防。

击图 $G=(S,T,s_0,s_g)$ 的安全状态序列，其中，$s_i \in S(0 \leqslant i \leqslant n)$，若该序列满足 $(s_i,s_{i+1}) \in T(0 \leqslant i \leqslant n-1)$，则称该序列为一条攻击路径。

定义 4(最优攻击路径) 攻击路径的总代价是对该路径上的所有原子攻击的攻击代价求和，则最优攻击路径为总代价最小的攻击路径。

攻击图展示了攻击者从初始状态到达攻击目标状态的攻击路径，在实施攻击时，攻击者通常会选择最优攻击路径。因此，为了降低网络安全风险，网络管理员在制定安全策略时，应考虑如何破坏最优攻击路径。在上述研究的基础上，本文设计了基于最优攻击路径的网络安全增强策略制定框架，如图 1 所示。

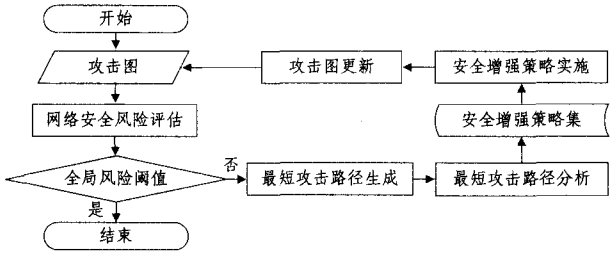

图 1 基于最优攻击路径的网络安全增强策略制定框架

图 1 所示的网络安全增强策略制定框架包含如下 3 个步骤，这 3 个步骤构成一个完整的网络安全增强策略制定周期：

步骤 1 基于攻击图进行攻击目标风险评估；

步骤 2 攻击目标风险阈值判断：若达到阈值，则执行结束；若未达到阈值，则基于最优攻击路径生成安全增强策略集，具体过程：首先利用 ACO 算法生成最优攻击路径，然后对其进行分析，选取该路径中信息素浓度或攻击代价最大的边(即原子攻击)作为目标，制定安全增强策略，并加入策略集；

步骤 3 实施安全增强策略，更新攻击图，执行步骤 1。

3 网络安全增强策略生成算法

利用 ACO 算法生成最优攻击路径，对最优攻击路径进行分析以生成安全增强策略，是本文研究重点，因此对风险评估和攻击图更新的方法不作详细阐述。

3.1 风险评估

网络安全风险是利用目标网络的一个或一组脆弱点使网络系统发生某种安全失效的潜在概率及危害的一种度量。因此，攻击目标 s_g 的安全风险可表示为：

$$Risk(s_g)=\sum_{\tau_i \in T} \chi_{\tau_i} M(\tau_i) \tag{1}$$

式中，$M(\tau_i)$ 表示原子攻击 τ_i 对网络的潜在影响，χ_{τ_i} 表示原子攻击 τ_i 对攻击目标 s_g 的影响系数，$\chi_{\tau_i} M(\tau_i)$ 指原子攻击 τ_i 对攻击目标 s_g 形成的风险。风险控制的目标是使 $Risk(s_g) \leqslant Risk_0$，$Risk_0$ 为风险阈值。

3.2 最优攻击路径生成

TSP 问题是指在 n 个城市中，一个人从其中的一个城市出发，按照一定的路径访问除出发城市外的其他城市恰好一次，最后回到出发城市，并要求经过路径的总长度最短。本文的攻击图问题则有所区别：在 n 个节点中，攻击者从起始节点出发，按照一定的路径到达目标节点，中途访问除起始节点和目的节点外的其他节点最多一次，并要求所经过路径的总权重最小。因此，本文在求解 TSP 问题的 ACO 算法基础上进行了改进，以应用于求解攻击图最优攻击路径的问题，同时，改进了信息素更新规则，加快了算法收敛速度。

3.2.1 最优攻击路径模型

根据上述定义可知，最优攻击路径就是在攻击图的源节点和目标节点之间寻找一条满足攻击代价之和最小的路径。因此，最优攻击路径的数学模型可描述为：

$$\min G=\min\left(\sum_{\tau_i \in T} X_{\tau_i} Cost(\tau_i)\right) \tag{2}$$

式中，$G=\sum_{\tau_i \in T} X_{\tau_i} Cost(\tau_0)$ 表示每条攻击路径的攻击代价，对于每条攻击路径，若原子攻击 τ_i 在该条攻击路径上，则 X_{τ_i} 为 1，否则为 0。

3.2.2 蚂蚁转移规则

蚂蚁从源节点开始，逐步向目标节点移动，根据路径上遗留下的信息素进行路径的选择。用 $\mu_{ij}(t)$ 表示 t 时刻边 (i,j) 上的信息素，算法开始时，初始化各条边上的信息素，令 $\mu_{ij}(0)=C$。首先将 m 只蚂蚁放置在起始节点上，并将该节点存入蚂蚁的禁忌表；然后，蚂蚁 $k(k=1,2,\cdots,m)$ 在节点 i 时，采用随机性选择的概率决策规则确定节点 j 的转移概率，并将节点 j 加入蚂蚁 k 的禁忌表。转移概率公式如下：

$$P_{ij}^k(t)=\begin{cases}\dfrac{[\mu_{ij}(t)]^\alpha[\eta_{ij}(t)]^\beta}{\sum\limits_{s \in Allowed_k}[\mu_{is}(t)]^\alpha[\eta_{is}(t)]^\beta}, & j \in Allowed_k \\ 0, & \text{否则}\end{cases} \tag{3}$$

式中，$P_{ij}^k(t)$ 表示在 t 时刻蚂蚁 k 由节点 i 转移到节点 j 的概率；η_{ij} 表示启发式因子，$\eta_{ij}=\dfrac{1}{\lambda_{ij}}(\lambda_{ij} \neq 0)$，$\lambda_{ij}$ 表示边 (i,j) 对应原子攻击的攻击代价；α 和 β 分别表示信息素和攻击代价对转移概率的影响程度；$Allowed_k$ 表示蚂蚁 k 下一步允许选择的节点集合。

3.2.3 信息素更新规则

蚂蚁在经过的路径上留下信息素，而信息素随着时间的推移逐渐挥发。在每次迭代过程中，当 m 只蚂蚁都找到一条路径后，各条路径上的信息素将按下式进行更新：

$$\mu_{ij}(t+n)=(1-\delta)\mu_{ij}(t)+\sum_{k=1}^{m}\Delta\mu_{ij}^k \tag{4}$$

式中，δ 表示信息素挥发系数，$\delta \in (0,1)$，则 $1-\delta$ 表示信息素残留因子；$\Delta\mu_{ij}^k$ 表示第 k 只蚂蚁在本次迭代中留在边 (i,j) 上的信息素，可按下式进行计算：

$$\Delta\mu_{ij}^k=\begin{cases}\dfrac{Q}{L_k}\left(1-\dfrac{\lambda_{ij}}{L_k}\right), & \text{若第 } k \text{ 只蚂蚁在本次迭代中经过}(i,j) \\ 0, & \text{否则}\end{cases} \tag{5}$$

式中，Q 是经验性常数，表示完成一次迭代蚂蚁释放的总信息素；L_k 为本次迭代中第 k 只蚂蚁所经过的路径总长度；λ_{ij} 表示边 (i,j) 的权重。从式中可以看出，权重越小，原子攻击上分配的信息素就越多。Dorigo 给出了基本 ACO 算法中常用的信息素分配方式[5]。

$$\Delta\mu_{ij}^k=\begin{cases}\dfrac{Q}{L_k}, & \text{若第 } k \text{ 只蚂蚁在本次迭代中经过}(i,j) \\ 0, & \text{否则}\end{cases} \tag{6}$$

该式使一条路径上分配的信息素浓度相等，没有考虑不同权重的影响，改进后的信息素分配方式与基本 ACO 算法相比，增强了正反馈过程，加快了算法收敛速度。

3.2.4 算法描述

初始化参数:m,α,β,δ,NC_max,Q,Tau,Tabu;

//Tau 为信息素矩阵,Tabu 是用于记录 m 只蚂蚁所生成的路径的矩阵

while 迭代次数 NC<NC_max do

  for k=1 to m do(对 m 只蚂蚁循环)

    将蚂蚁 k 置于初始节点 s_0;

    将 s_0 存入禁忌表 Tabu(k);

    当前节点指针 $s \leftarrow s_0$;

    计算节点 s 的待访问节点集 $Allowed_k$;

    while $Allowed_k$ 非空 Then

      根据式(3)计算转移概率 Pk;

      按概率 Pk 选择下一个节点 s_1;

      将 s_1 存入进入禁忌表 Tabu(k),$s \leftarrow s_1$;

      计算节点 s 的待访问节点集 $Allowed_k$;

    end while

  end for

  根据式(4)和式(5)更新路径上的信息素;

  清空所有蚂蚁禁忌表中的数据;

  NC=NC+1;

end while

输出最优攻击路径;

end

3.3 安全增强策略及攻击图更新

获取最优攻击路径之后,就要制定并实施安全策略破坏最优攻击路径。若每条边上的信息素浓度不同,浓度越大,表明该条边在路径生成过程中被较多的蚂蚁选择过,说明该边对其他攻击路径的价值越大,根据效用理论[10],选取破坏最优攻击路径上的信息素浓度最大的边,将针对该边的安全策略加入安全增强策略集;若经过多次迭代后,最优攻击路径上信息素浓度相同,就选择权重最小的边加入安全增强策略集。

实施安全增强策略,对应该安全策略的原子攻击将失效,体现在攻击图则是将该原子攻击边删除,同时,依赖于该原子攻击的节点和边也将被删除。

4 实验分析

为了验证本文算法的有效性,论文对本文算法和基本 ACO 算法进行了仿真实验,实验平台为:CPU:1.66GHz;RAM:1GB;操作系统:Windows XP;开发工具:Matlab。为了便于比较,两种算法都采用了相同的参数设置。利用两种算法对图 2 所示的攻击图示例进行仿真分析,攻击图中的节点表示状态节点,用 s_0-s_n 表示,节点在坐标轴上的位置不具有实际意义,边的属性用二元组$(\tau_i, Cost(\tau_i))$表示。选取的参数分别为:$\alpha=1$,$\beta=0.5$,$\delta=0.1$,$Q=10$,各边的信息素初始化为 1,放置在起始节点的蚂蚁数量 $m=10$,迭代次数设为 100。仿真结果如图 2 所示。

从图 2 可知,两种算法得到的最优攻击路径都是红色线条连接的 $s_0 \rightarrow s_1 \rightarrow s_3 \rightarrow s_4 \rightarrow s_6$,验证了本文算法的有效性。

由于 ACO 算法采用随机选择策略,因此运行时算法的收敛周期可能会有些差别。本文对两种算法进行了 20 次重复实验,以比较两种算法的收敛性能。统计结果如图 3 所示。

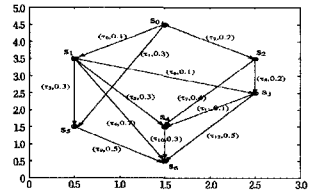

图 2 仿真所用攻击图及仿真结果

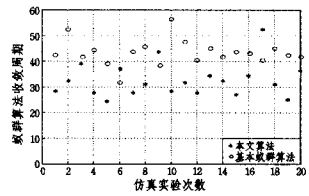

图 3 算法收敛周期统计

从图 3 的统计结果得出,本文算法重复进行 20 次仿真实验的平均收敛周期为 32.8,基本 ACO 算法的平均收敛周期为 43.6。由此可知,本文算法的平均收敛速度要优于基本 ACO 算法,同时,由于实验采用的攻击图规模较小,因此两种算法的收敛周期都比较小。随着攻击图规模的增大,收敛周期将变大。从统计结果分布的情况可以看出,两种算法每次的收敛周期可能不同,随机分布在一个区间内,这体现了 ACO 算法的随机选择策略会导致收敛周期出现差别。

分析得到的最优攻击路径后,发现(s_0, s_1)上的信息素浓度最大,将针对原子攻击 τ_0 的安全策略加入策略集,实施安全增强策略,进行攻击图更新,按照更新规则,需要删除状态节点 s_1 以及边(s_0, s_1)、(s_1, s_3)、(s_1, s_4)、(s_1, s_5)、(s_1, s_6)。然后根据更新后的攻击图对攻击目标进行风险评估,判断是否达到风险阈值。

结束语 网络安全增强策略的研究是确保网络安全的重要方面,通常难以定量分析。针对该问题,本文提出了一种基于最优攻击路径的网络安全增强策略制定方法,针对最优攻击路径,从攻击者的角度出发,提出了一种基于 ACO 算法的最优攻击路径生成算法。仿真结果表明,本文提出的网络安全增强策略制定方法可有效产生安全增强策略集,对实现目标网络适度安全具有重要意义;与基本 ACO 算法相比,本文提出的改进 ACO 算法不仅可准确地寻找出最优攻击路径,而且具有更好的收敛性。

参 考 文 献

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

[2] 司加全,张冰,尚大鹏,等. 基于攻击图的网络安全性增强策略制定方法[J]. 通信学报,2009,30(2):123-128

[3] Sheyner O, Haines J, Jha S. Automated generation and analysis of attack graphs[C]// Proc 2002 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2002:254-265

[4] Jha S, Sheyner O, Wing J. Two Formal Analyses of Attack Graphs[C]// Proceedings of the 15th IEEE Computer Security

[5] Colorni A, Dorigo M, Maniezzo V. Distributed optimization by ant colonies[C]// Varela F, Bourgine P. Proc of the ECAL'91 European Conf of Artificial Life. Paris: Elsevier, 1991:134-144

[6] 杜占玮,杨永健,孙永雄,等. 基于互信息的混合蚁群算法及其在旅行商问题上的应用[J]. 东南大学学报:自然科学版,2011,41(3):478-481

[7] 李琳,刘士新,康加福. 改进的蚁群算法求解带时间窗的车辆路径问题[J]. 控制与决策,2010,25(9):1379-1383

[8] 胡耀民,刘伟铭. 基于改进型蚁群算法的最优路径问题求解[J]. 华南理工大学学报:自然科学版,2010,38(10):105-110

[9] 汪立东. 操作系统安全评估和审计增强[D]. 哈尔滨:哈尔滨工业大学计算机科学与技术学院,2002

[10] 彭俊好,徐国爱,杨义先,等. 基于效用的安全风险度量模型[J]. 北京邮电大学学报,2006,29(2):6-9