

面向网络实时对抗的动态防御决策方法

冷强¹, 杨英杰¹, 常德显¹, 潘瑞萱¹, 蔡英², 胡浩¹

(1. 信息工程大学, 河南 郑州 450001;

2. 河南省理工学校, 河南 郑州 450001)

摘要: 如何基于网络外在威胁实施防御决策是构建网络信息防御体系的核心问题, 针对实时攻击带来的动态威胁进行科学有效的防御决策是构建网络动态应急防御体系的关键。针对动态防御决策问题, 首先基于属性攻击图理论设计了一种网络生存性博弈模型, 利用攻防矩阵表示攻防策略和路径, 并给出了攻防强度和网络生存性量化方法; 其次提出了单步与多步的攻、防策略支出计算方法, 并基于攻防策略支出给出防御决策; 最后通过实验进行防御决策技术的有效性验证。

关键词: 属性攻击图; 网络生存性; 网络攻防对抗; 攻防强度

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.201963

Dynamic defense decision method for network real-time confrontation

LENG Qiang¹, YANG Yingjie¹, CHANG Dexian¹, PAN Ruixuan¹, CAI Ying², HU Hao¹

1. Information Engineering University, Zhengzhou 450001, China

2. Henan Polytechnic University, Zhengzhou 450001, China

Abstract: How to implement defense decision based on network external threat is the core problem of building network information defense system. Especially for the dynamic threat brought by real-time attack, scientific and effective defense decision is the key to construct network dynamic emergency defense system. Aiming at the problem of dynamic defense decision-making, firstly a network survivability game model based on attribute attack graph theory is designed. The attack and defense matrix is used to represent the attack and defense strategy and path, and

收稿日期: 2019-01-25; 修回日期: 2019-04-08

通信作者: 胡浩, wjjhh_908@163.com

基金项目: 国家自然科学基金资助项目 (No.61902427); 国家高技术研究发展计划 (“863” 计划) 基金资助项目 (No.2015AA016006); 国家重点研发计划基金资助项目 (No.2016YFF0204003); “十三五” 装备预研领域基金资助项目 (No.61400020201)

Foundation Items: The National Natural Science Foundation of China (No.61902427), The National High Technology Research and Development Program of China (“863” Program) (No.2015AA016006), The National Key Research and Development Program of China (No.2016YFF0204003), The Equipment Pre-research Foundation during the National 13th Five-Year Plan (No.61400020201)

论文引用格式: 冷强, 杨英杰, 常德显, 等. 面向网络实时对抗的动态防御决策方法[J]. 网络与信息安全学报, 2019, 5(6): 58-66.

LENG Q, YAGN Y J, CHANG D X, et al. Dynamic defense decision method for network real-time confrontation[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 58-66.

the attack and defense strength and network survivability quantification method are given. Secondly, the single step and the multi-step attack and defense strategy payoff calculation method is proposed, and the defense decision is based on the attack and defensive strategy payoff. Finally, the effectiveness of the defense decision technology is verified through experiments.

Key words: attribute attack graph, network survivability, network attack-defense confrontation, attack-defense strength

1 引言

随着网络规模的扩大、复杂性的增加和攻击技术的不断发展,绝对防止网络遭受攻击和入侵的威胁是不可能实现的,大量的网络关键服务型节点需要满足网络遭受攻击时,在实施防御措施后能够提供足够的网络服务,满足网络的正常运转。因此,网络攻防双方在围绕网络的生存性实施攻防策略^[1-2],网络在攻防过程中生存与否是分析防御策略对系统安全有效和无效的关键。

网络状态攻击图^[3-5]是将网络每一时刻的安全状态作为一个节点进行网络攻防动作的分析。但在时间维度的推移下,网络状态是一个不断转变的过程,且存在往原有状态转变的情况,因此利用网络状态攻击图对攻击动作进行处理时,存在状态空间爆炸的问题。为了解决状态攻击图存在的问题,研究人员提出属性攻击图理论研究网络动态安全。属性攻击图是将网络中的条件或属性作为攻击图中的一个节点,因此在研究网络安全时,能够将攻击事件精确到网络中的某个节点,并对其进行分析研究。因此近年来属性攻击图成为网络安全的主要方法^[6-8]。

在面对攻击行为时,大部分网络安全人员为了维持网络的正常运转,需要采取一系列的防御措施,使网络得以生存。近年来博弈论逐渐成为研究网络安全防御决策的一个主流方法。文献[9]研究网络在攻防过程中的可生存性,量化分析了网络的安全状态;文献[2,10]构建动态网络攻防博弈模型开展网络防御决策研究;文献[11]将选择

攻防策略的行为看作一个多阶段的博弈过程,动态分析选择的网络安全策略对网络系统安全的影响;文献[12]基于重复的攻防博弈理论研究无线网络抗DDoS攻击的方法;文献[13]构建了微分攻防博弈模型,给出了鞍点策略的计算方法和最优策略选取算法;文献[14]基于有限理性的不完全信息博弈模型,量化网络攻防双方的收益,研究动态、不断演化的网络攻防双方的最优策略集选取方法。但在上述研究中,都是将网络状态作为博弈结果,因此,每个策略是在该时刻的一个策略集,网络安全人员在采取网络防御措施时,不能很好地理解网络安全状态与防御措施之间的关系。

因此,本文提出了基于属性攻击图的网络生存性博弈策略分析研究的方法,量化攻防动作强度和网络安全状态,为网络安全管理员提供实施单点防御措施的建议。本文首先利用矩阵的方法表示网络节点的地址、攻击动作和攻击路径;其次量化攻防策略对网络系统生存性的影响;然后根据相应攻防策略的支出,计算最优防御策略,为网络安全管理人员提供更易于理解、合理的防御决策。

2 网络生存性博弈模型的构建

博弈模型包含博弈者、攻防策略、攻防收益等要素,在基于网络生存性度量网络安全状态的基础上,加入了网络生存性度量值,并且量化了攻防策略对网络安全的影响。下面给出网络生存性博弈模型的定义。

定义 1 网络生存性博弈模型 (NSGM, network survivability game model) 由七元组 $NSGM = (N, S, V, SI, g, U, f)$ 表示。

1) $N = (N_A, N_D)$, N 表示攻防博弈的参与人集合, N_A 表示攻击者, N_D 表示防御者。

2) $S = (S_A, S_D)$, S 表示攻防策略矩阵。其中

$$S_A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \quad S_D = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nk} \end{bmatrix}$$

n 表示该条攻击路径的节点数, 且攻击顺序为 $1 \rightarrow n$, m 表示攻击者在对 n 个节点进行攻击时, 对某个节点存在的最大攻击策略数, k 表示防御者对 n 个节点进行防御时, 对某个节点存在的最大防御策略数, a_{ij} 表示第 i 个节点的攻击策略 j ; d_{ij} 表示第 i 个节点的防御策略 j 。矩阵元素由 0,1 构成, 表示攻击者或防御者是否选择该策略。

为了方便对系统防御和攻击策略进行分析, 给出每个节点的攻击策略向量和防御策略向量表示: $S_D = (\vec{d}_1, \vec{d}_2, \cdots, \vec{d}_n)^T$, $S_A = (\vec{a}_1, \vec{a}_2, \cdots, \vec{a}_n)^T$ 。

3) V 表示网络生存性度量值 (NSM, network survivability metric), 表示在网络遭受故意攻击或意外事件时是否能确保关键任务的完成和确保足够的信息可用性和服务连续性的量化值^[1-2]。

为了量化分析攻防行为对网络系统的影响程度, 本文采用林肯实验室攻防行为数据库^[15]中的攻防动作强度分析网络攻防策略对系统的影响。

4) $SI = (SI_A, SI_D)$ 表示策略强度 (strategy intensity)。 SI_A 表示攻击策略强度, SI_D 表示防御策略强度, 且 $SI \in [0,1]$ 。

$$V = SI_D - SI_A \quad (1)$$

由于 $V \in [-1,1]$, 当 $V \in [0,1]$ 时, 表示网络系统当前安全, 有继续提供必需服务的能力; 当 $V \in [-1,0)$ 时, 表示网络系统存在较大的风险, 生

存性较低, 且 V 越小, 风险越大, 提供必需服务的能力越低。

5) g 表示攻防策略选取函数关系式。

攻击者对系统进行攻击时, 首先选择攻击节点, 则相对应的存在攻击向量 $\vec{a}_i$, 攻击者选择向量中的一个元素 a_{ij} 。对防御者来说, 为了维护网络系统的安全, 在面临某个攻击时, 需要对攻击动作做出反应, 因此, 得到一个防御策略集合, 在攻击者选择攻击策略 a_{ij} 时, 防御者选择防御策略集合中的任意一个元素, 使 $V \geq 0$, 则存在一个函数关系式为

$$SupS_{D_i} = g(S_A(a_{ij})) \quad (2)$$

引用集合中的上确界表达式对防御策略集进行表达。式 (2) 表示当攻击者选择攻击策略 a_{ij} 时, 防御者为了保持网络系统安全, 防御措施只能在 $SupS_{D_i}$ 中选择, 且 $SupS_{D_i} \in S_{D_i}(\vec{d}_i)$, $S_{D_i}(\vec{d}_i)$ 表示对节点 i 采取的防御措施的集合。

6) $U = (U_A, U_D)$ 表示攻击者和防御者选择的策略的相应的支出矩阵。

$$U_A = \begin{bmatrix} u_{a_{11}} & u_{a_{12}} & \cdots & u_{a_{1m}} \\ u_{a_{21}} & u_{a_{22}} & \cdots & u_{a_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ u_{a_{n1}} & u_{a_{n2}} & \cdots & u_{a_{nm}} \end{bmatrix} \quad U_D = \begin{bmatrix} u_{d_{11}} & u_{d_{12}} & \cdots & u_{d_{1k}} \\ u_{d_{21}} & u_{d_{22}} & \cdots & u_{d_{2k}} \\ \vdots & \vdots & \ddots & \vdots \\ u_{d_{n1}} & u_{d_{n2}} & \cdots & u_{d_{nk}} \end{bmatrix}$$

U_A 表示攻击支出矩阵, U_D 表示防御支出矩阵, $u_{a_{ij}}$ 表示攻击者攻击节点 i 采取策略 j 的攻击支出, $u_{d_{ij}}$ 表示防御者对节点 i 采取防御措施 j 的支出。

分析攻击者对网络系统某个节点采取攻击时, 攻击者和防御者的支出情况。

7) f 表示攻防支出矩阵与攻防支出之间的函数关系式。

当攻击者对系统中节点 i 采取攻击措施 j 时, 防御者的防御措施为 $SupS_{D_i}$ 。则

$$f_A = u_{a_{ij}}, \quad f_D \in SupU_{D_i}$$

3 攻击策略支出分析

3.1 单步攻击策略支出

首先根据网络拓扑关系和网络节点存在的漏洞,得到攻击者的攻击策略矩阵 $\mathbf{S}_A$, 其中, $\mathbf{S}_A$ 表示由 0,1 组成的 $n \times m$ 矩阵。如

$$\mathbf{S}_{A_i} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & 1_{ij} & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

其中, $\mathbf{S}_{A_i}$ 中只有 1_{ij} 一个元素为 1, 其余元素为 0; $\mathbf{S}_{A_i}$ 表示攻击者对节点 i 实施攻击策略 j 的一步攻击动作。

为了对攻击策略支出矩阵进行数学计算, 引用文献[16]矩阵的元素形式范数计算公式进行攻击策略支出的计算。

设存在矩阵 $\mathbf{B}$, 则根据的元素形式范数计算公式得到 $\|\mathbf{B}\|_p^{[16]}$

$$\|\mathbf{B}\|_p = \left(\sum_{i=1}^n \sum_{j=1}^m |b_{ij}|^p \right)^{\frac{1}{p}} \quad (3)$$

根据攻防支出矩阵与攻击支出之间的函数关系式, 得到单步攻击动作的支出为

$$f_A^1 = f_{A_i} = \|\mathbf{S}_{A_i} \cdot \mathbf{U}_A^T \cdot \mathbf{S}_{A_i}^T\| \quad (4)$$

其中, f_A^1 表示攻击 1 步的支出, f_{A_i} 表示攻击者第 A_i 步攻击的支出。

下面结合一个简单的实例对单个攻击策略的攻击支出进行计算说明。

假设网络系统中的节点 n 具有 i 个漏洞, 且每个漏洞有一种攻击策略, 则攻击策略矩阵为 $\mathbf{S}_{A_n}$

$$\mathbf{S}_{A_n} = [a_{11} \quad a_{12} \quad \cdots \quad a_{1i}]$$

且攻击 i 个漏洞的攻击支出矩阵为

$$\mathbf{U}_{A_n} = [u_{11} \quad u_{12} \quad \cdots \quad u_{1i}]$$

则根据式 (4) 可知攻击者在攻击节点 n 时的攻击

支出为

$$f_{A_n} = \|\mathbf{S}_{A_n} \cdot \mathbf{U}_{A_n}^T \cdot \mathbf{S}_{A_n}^T\| = \left\| \left(\sum_{j=1}^i a_{1j} \cdot u_{1j} \right) \mathbf{S}_{A_n}^T \right\|$$

当攻击者攻击漏洞 l ($1 \leq l \leq i$) 时, 攻击支出为

$$f_{A_n} = \|\mathbf{S}_{A_n} \cdot \mathbf{U}_{A_n}^T \cdot \mathbf{S}_{A_n}^T\| = \|(1_{1l} \times u_{1l})[0, \cdots, 1_{1l}, \cdots, 0]^T\| = u_{1l}$$

3.2 多步攻击策略支出

首先对攻击者的攻击步数进行分析。攻击者在对网络系统进行攻击时, 有时由于技术原因或者对系统信息掌握不足, 某些攻击动作不成功, 则攻击者存在对相同目标进行相同攻击动作的情况。为了符合实际情况, 假设攻击者在对相同节点进行攻击时, 攻击次数越多, 攻击支出越少, 给定参数 $\lambda \in (0, 1)$, 当对某个相同目标执行第 n 次相同攻击动作时, 第 n 次的攻击支出为第一次的 λ^n 倍。根据上述情况, 下面对多步攻击动作进行分析, 则攻击者在实施攻击动作时, 可以分成单步攻击动作的情况进行分析, 因此将多步攻击行为分成多个单步攻击行为进行分析。下面给一个简单的例子。

当攻击者实施多步攻击时, 计算攻击者的多步攻击支出, 攻击者实施了 $\mathbf{S}_{A_1}, \mathbf{S}_{A_2}, \cdots, \mathbf{S}_{A_q}$ 的 q 步攻击策略, 则 q 步的攻击支出为

$$f_A^q = \sum_{i=1}^q f_{A_i} \quad (5)$$

由于存在重复攻击的情况, 因此在对攻击支出进行计算时, 考虑 f_A^q 中系数不为 1 的函数关系式

$$f_A^q = v_{11}u_{a_{11}} + v_{12}u_{a_{12}} + \cdots + v_{nm}u_{a_{nm}} = \sum_{j=1}^m \sum_{i=1}^n \sum_{k=1}^{v_{ij}} \lambda^{k-1} u_{a_{ij}} \quad (6)$$

其中, $v_{11}, v_{12}, \cdots, v_{nm} \in \{0, 1, 2, \cdots\}$ 为相应的攻击策略的攻击次数。

4 防御支出与策略选取分析

防御者在面对攻击者的攻击时, 由于具有防御措施上确界集合, 因此只需要在集合中选取防御决策分析防御支出。

4.1 单步防御决策支出分析

当攻击实施一步攻击动作, 且没有发现其余的攻击动作时, 由式(1)可知, 防御者存在防御策略选择, 且防御者的防御策略支出是以集合的形式表示的。

在面对已知系统漏洞和系统关联关系时, 防御者的防御策略根据攻击者的攻击策略进行改变。

当攻击者的攻击策略为 a_{ij} 时, 防御者的防御策略集为 $SupS_{D_i}$, 防御者采取的防御策略在保证网络系统生存情况下的支出最少, 则称该防御策略为最优防御策略。因此, 防御者在面对攻击者的攻击动作时, 当 $u_{il} = \min(SupU_{D_i})$ 得到防御策略为 d_{il} , 且 $d_{il} \in SupS_{D_i}$ 。则防御策略矩阵为

$$S_{D_i} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & 1_{il} & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

其中, S_{D_i} 中元素只有 d_{il} 为 1, 其余元素为 0。

下面结合一个简单的实例对防御策略支出进行计算说明。

假设攻击节点 m 的漏洞 i , 且漏洞 i 的防御策略有 j 种, 则防御策略矩阵为 S_{D_m}

$$S_{D_m} = [d_{m1} \quad d_{m2} \quad \cdots \quad d_{mj}]$$

根据最优防御决策原则可知, 在满足网络可生存性条件下支出最少的防御策略为最优防御决策, 则根据式(2)取防御矩阵 S_{D_m} 中的防御策略为

$$S_{D_m} = [0 \quad \cdots \quad d_{ml} \quad \cdots \quad 0]$$

其中满足:

$$SI_{d_{ml}} > SI_{a_{ml}} \\ u_{ml} = \min(SupU_{D_m})$$

与单个攻击策略支出计算方式相同, 得到单个防御策略支出为

$$f_{D_m} = \|S_{D_m} \cdot U_{D_m}^T \cdot S_{D_m}^T\|_1 = \|(1_{ml} \cdot u_{ml})[0, \cdots, 1_{ml}, 0]^T\|_1 = u_{ml}$$

4.2 多步防御支出与策略选取

防御者根据多个攻击动作选取多个最优防御策略, 使网络系统维持生存性度量值大于 0。防御动作与攻击动作支出的分析相同, 首先假设攻击者与防御者业务能力相同, 当防御者多次实施相同防御策略时, 防御支出相应减少, 且参数为 λ , 则根据式(5)和式(6)得到多步防御策略支出为

$$f_D^p = \sum_{i=1}^p f_{D_i} = \\ \eta_{11}u_{d_{11}} + \eta_{12}u_{d_{12}} + \cdots + \eta_{nk}u_{d_{nk}} = \\ \sum_{i=1}^n \sum_{j=1}^k \sum_{l=1}^{\eta_{ij}} \lambda^{l-1} u_{d_{ij}} \quad (7)$$

其中, 当 $p=1$ 时, 为特殊的单步防御策略支出计算公式, 即式(4)。

$\eta_{11}, \eta_{12}, \cdots, \eta_{nk} \in \{0, 1, 2, \cdots\}$ 为相应的防御策略实施的次数。

当 $\eta_{11}, \eta_{12}, \cdots, \eta_{nk}$ 中 $\exists \eta_{ij} \neq 0$, 则表示根据攻击者攻击策略选取的防御策略, 使网络的可生存性 $V \geq 0$ 且支出最少的防御策略, 即为 d_{ij} 。

5 实验

5.1 实验分析

为了验证防御策略选取对网络系统安全的影响, 构建的网络环境如图 1 所示, 具体包含 3 个主机和 2 个服务器, 2 个防火墙和 2 个入侵检测系统 (IDS, instruction detection system)。

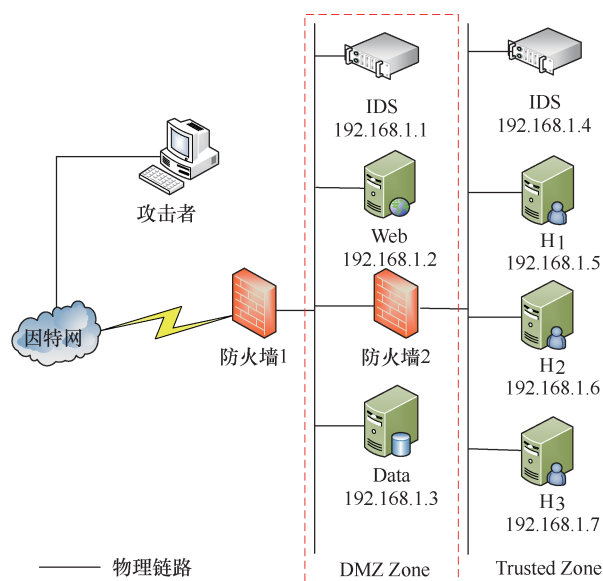


图1 构建的网络环境

在图1的实验环境中，攻击者通过网络对系统中的主机和服务器进行攻击。首先给出攻防动作强度表^[15]；攻防支出是基于攻击者和防御者的能力在同一水平下确定的，不同的攻防强度需要不同的攻防支出，为了提高实时分析效率，本文将攻防支出分为3个等级，分别对应攻防强度如表1和表2所示；表3为实验环境的网络系统节点的信息表；表4是查询CVE^[17]、NVD^[18]得到具体的漏洞攻防动作表（注：表4中的字母和数字是表1和表2中的序号）。

表1 攻击动作强度

序号	攻击动作名称	攻击强度	攻击支出
a ₁	Remote buffer overflow	0.95	3
a ₂	Install Trojan	0.80	
a ₃	Steal account and crack it	0.70	
a ₄	Send abnormal data to GIOP	0.50	2
a ₅	Shut down Database server	0.45	
a ₆	LPC to LSASS	0.40	
a ₇	Oracle TNS Listener	0.35	1
a ₈	Ftp RHOST attack	0.30	
a ₉	Sr-Hard blood	0.25	

表2 防御动作强度

序号	防御动作名称	防御强度	防御支出
d ₁	Limit packets form ports	0.8	3
d ₂	Install Oracle patch	0.8	
d ₃	Reinstall Listener program	0.8	
d ₄	Uninstall delete Trojan	0.7	
d ₅	Limit access to MDSYS.SDO_CS	0.7	
d ₆	Renew root data	0.6	2
d ₇	Restart Database server	0.6	
d ₈	Limit SYN/ICMP packets	0.5	
d ₉	ADD physical resource	0.5	
d ₁₀	Repair database	0.4	
d ₁₁	Correct homepage	0.4	1
d ₁₂	Delete suspicious account	0.3	
d ₁₃	Redeploy firewall rule and filtrate malicious packets	0.3	
d ₁₄	Patch SSH on Ftp	0.2	

表3 节点信息

Host/Server	Protocol/Vulnerability	Port
Web	IIS	445&80
Data	Apache	80
H ₁	HIDP	445
H ₂	GUN Wget	80
H ₃	NDproxy	445

表4 漏洞的可利用攻防动作

Protocol/Vulnerability	Attack Active	Defense Active
IIS	a ₂ , a ₇	d ₃ , d ₄
Apache	a ₁	d ₁ , d ₈ , d ₁₃
HIDP	a ₄ , a ₅ , a ₈	d ₁ , d ₆ , d ₇ , d ₁₀
GUN Wget	a ₂ , a ₇ , a ₈	d ₃ , d ₄ , d ₁₂
NDproxy	a ₃ , a ₇	d ₃ , d ₆

由图1中的网络环境可知，攻击者需要通过互联网攻击DMZ区域的服务器，然后才能攻击Trusted区域的主机，攻击者获得的权限从Web、Data、H₁、H₂、H₃依次递增，即表示攻击者在获得后者的权限之后，不会再对前面的节点进行攻

击。结合表 3 网络开放的端口信息, 可知该网络环境的属性攻击图, 如图 2 所示。

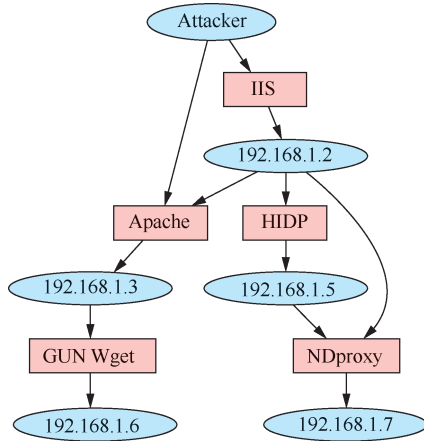


图 2 实验环境属性攻击图

由图 2 可知, 该网络系统有 4 条攻击路径。

- 1) Attacker $\rightarrow$ 192.168.1.3 $\rightarrow$ 192.168.1.6
- 2) Attacker $\rightarrow$ 192.168.1.2 $\rightarrow$ 192.168.1.3 $\rightarrow$ 192.168.1.6
- 3) Attacker $\rightarrow$ 192.168.1.2 $\rightarrow$ 192.168.1.5 $\rightarrow$ 192.168.1.7
- 4) Attacker $\rightarrow$ 192.168.1.2 $\rightarrow$ 192.168.1.7

根据表 1、表 2 和节点的漏洞信息, 可知攻击矩阵和防御矩阵为

$$S_i = \begin{bmatrix} a_{192.168.1.3, a_1} & 0 & 0 \\ a_{192.168.1.6, a_2} & a_{192.168.1.6, a_7} & a_{192.168.1.6, a_8} \end{bmatrix}$$

$$S_{ii} = \begin{bmatrix} a_{192.168.1.2, a_2} & a_{192.168.1.2, a_7} & 0 \\ a_{192.168.1.3, a_1} & 0 & 0 \\ a_{192.168.1.6, a_2} & a_{192.168.1.6, a_7} & a_{192.168.1.6, a_8} \end{bmatrix}$$

$$S_{iii} = \begin{bmatrix} a_{192.168.1.2, a_2} & a_{192.168.1.2, a_7} & 0 \\ a_{192.168.1.5, a_4} & a_{192.168.1.5, a_5} & a_{192.168.1.5, a_8} \\ a_{192.168.1.7, a_3} & a_{192.168.1.7, a_7} & 0 \end{bmatrix}$$

$$S_{iv} = \begin{bmatrix} a_{192.168.1.2, a_2} & a_{192.168.1.2, a_7} \\ a_{192.168.1.7, a_3} & a_{192.168.1.7, a_7} \end{bmatrix}$$

$$D_i = \begin{bmatrix} d_{192.168.1.3, d_1} & d_{192.168.1.3, d_8} & d_{192.168.1.3, d_{13}} \\ d_{192.168.1.6, d_3} & d_{192.168.1.6, d_4} & d_{192.168.1.6, d_{12}} \end{bmatrix}$$

$$D_{ii} = \begin{bmatrix} d_{192.168.1.2, d_3} & d_{192.168.1.2, d_4} & 0 \\ d_{192.168.1.3, d_1} & d_{192.168.1.3, d_8} & d_{192.168.1.3, d_{13}} \\ d_{192.168.1.6, d_3} & d_{192.168.1.6, d_4} & d_{192.168.1.6, d_{12}} \end{bmatrix}$$

$$D_{iii} = \begin{bmatrix} d_{192.168.1.2, d_3} & d_{192.168.1.2, d_4} & 0 & 0 \\ d_{192.168.1.5, d_1} & d_{192.168.1.5, d_6} & d_{192.168.1.5, d_7} & d_{192.168.1.5, d_{10}} \\ d_{192.168.1.7, d_3} & d_{192.168.1.7, d_6} & 0 & 0 \end{bmatrix}$$

$$D_{iv} = \begin{bmatrix} d_{192.168.1.2, d_3} & d_{192.168.1.2, d_4} \\ d_{192.168.1.7, d_3} & d_{192.168.1.7, d_6} \end{bmatrix}$$

当系统入侵检测系统监测到节点被攻击时, 利用攻策略矩阵的策略选择计算方法, 可以实时为系统安全管理人员提供精确的防御决策和建议。

下面假设在上述实验中由入侵检测系统监测到攻击策略为 $a_{192.168.1.5, a_5}$, 且攻击次数为 1。

根据式(6)可知攻击支出为

$$f_{a_{192.168.1.5, a_5}}^1 = 2$$

首先根据发生的攻击行为的 IP 地址确定攻击策略所处的策略矩阵为 S_{iii} , 且 $SI_A = 0.45$, 然后根据式(2)可知

$$SupS_{D_{iii}} = \{d_{192.168.1.5, d_1}, d_{192.168.1.5, d_6}, d_{192.168.1.5, d_7}\}$$

根据式(7)可知防御支出为

$$f_{d_{192.168.1.5, d_1}}^1 = 3$$

$$f_{d_{192.168.1.5, d_6}}^1 = 2$$

$$f_{d_{192.168.1.5, d_7}}^1 = 2$$

则为系统安全管理人员提供的防御策略为 $d_{192.168.1.5, d_6}$ 和 $d_{192.168.1.5, d_7}$ 。

根据攻击策略所在的策略矩阵可知, 攻击者下一步很可能对节点 192.168.1.7 实施攻击, 因此, 需要提前对节点 192.168.1.7 可能发生网络攻击行为的情况进行分析。

下面对多步攻击行为的防御策略选择的情况进行分析。

假设攻击者实施攻击的策略为 $a_{192.168.1.5, a_5}$, $a_{192.168.1.5, a_3}$, 且攻击次数分别为 3 次和 1 次。根据攻击行为 a_5 , 对 λ 进行赋值为 0.7。

根据式(6)可知攻击支出为

$$f_A^4 = f_{a_{192.168.1.5, a_5}}^3 + f_{a_{192.168.1.7, a_3}}^1 = 7.38$$

根据 IP 地址确定攻击策略矩阵为 S_{iii} , 且 $SI_{a_5} = 0.45$, $SI_{a_3} = 0.7$ 。根据式(2)可知

$$SupS_{D_{iii}} = \{d_{192.168.1.5, d_1}, d_{192.168.1.5, d_6}, d_{192.168.1.5, d_7}\}$$

$$SupS_{D_{iii}} = \{d_{192.168.1.7, d_3}\}$$

根据式(7)可知防御支出的 3 种情况为

$$f_D^4 = f_{d_{192.168.1.5, d_1}}^3 + f_{d_{192.168.1.7, d_3}}^1 = 9.78$$

$$f_D^4 = f_{d_{192.168.1.5, d_6}}^3 + f_{d_{192.168.1.7, d_3}}^1 = 7.38$$

$$f_D^4 = f_{d_{192.168.1.5, d_7}}^3 + f_{d_{192.168.1.7, d_3}}^1 = 7.38$$

则为系统安全管理人员提供实时的防御策略是 $d_{192.168.1.5, d_6}$ 和 $d_{192.168.1.7, d_3}$ 或 $d_{192.168.1.5, d_7}$ 和 $d_{192.168.1.7, d_3}$ 。

5.2 关联分析

文献[9-14]是基于状态攻击图考虑攻击策略和防御策略对系统安全状态的影响；大部分文献没有给出网络系统安全状态的具体量化方法；在对网络系统的攻击策略分析中，是在无限攻防对抗过程的情况下对攻防策略进行分析，提供的防御决策其实是策略集，但在具体的网络系统攻防过程中，管理人员不能实现无限试错的机会，且

对策略集的实施存在理解困难的问题。因此本文基于属性攻击图研究网络攻防策略集对网络系统生存性的影响。表 5 是对应的关联分析。

6 结束语

本文基于属性攻击图研究网络攻防对抗的策略选择，首先利用攻防矩阵表示攻防策略和路径；其次利用林肯实验室给出的攻防动作数据量化攻防强度和网络安全生存性；然后结合攻防策略支出研究在面临实际威胁时，为网络系统安全人员提供可读性强的安全策略；最后根据攻击策略矩阵预测攻击者下一步的攻击行为。未来的研究是在本文的基础上，结合机器学习等人工智能方法，实现攻防策略自动化分析，为网络安全人员提供更加快捷、方便和易理解的防御策略。

参考文献：

- [1] FISHER J, LINGER R. Survivability: protecting your critical systems[J]. IEEE Journal of Internet Computing, 1999, 3(6): 55-63.
- [2] WANG CL, MIAO Q, DAI YQ. Network survivability analysis based on stochastic game model[J]. Multimedia Information Networking and Security, 2012, 55(10): 99-104.
- [3] 黄永洪, 吴一凡, 杨豪璞, 等. 基于攻击图的 APT 脆弱节点评估方法[J]. 重庆邮电大学学报(自然科学版), 2017, 29(4): 535-541. HUANG Y H, WU Y F, YANG H P, et al. Graph-based vulnerability assessment for APT attack[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2017,

表 5

关联分析

方案	攻击策略	防御策略	攻击支出	防御支出	攻防策略可读性	安全量化	策略强度量化	攻击预测
文献[9]	√	√	×	×	弱	√	×	×
文献[10]	√	√	√	√	弱	×	×	×
文献[11]	√	√	√	√	弱	×	×	×
文献[12]	√	√	×	×	强	×	×	×
文献[13]	√	√	×	×	弱	×	√	×
文献[14]	√	√	√	√	弱	×	×	×
本文	√	√	√	√	强	√	√	√

29(4): 535-541.

- [4] HU H, ZHANG H Q, LIU Y L, et al. Security metric methods for network multistep attacks using AMC and big data correlation analysis[J]. Security and Communication Networks, 2018
- [5] 胡浩, 叶润国, 张红旗, 等. 面向漏洞生命周期的安全风险度量方法[J]. 软件学报, 2018, 29(5).
HU H, YE R G, ZHANG H Q, et al. Vulnerability life cycle oriented security risk metric method[J]. Journal of Software, 2018, 29(5).
- [6] 吴迪, 连一峰, 陈恺. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9): 1938-1950.
WU D, LIAN Y F, CHEN K, et al. A security threats identification and analysis method based on attack graph[J]. Chinese Journal of Computers, 2012, 35(9): 1938-1950.
- [7] HOMER J, ZHANG S, OU X, et al. Aggregating vulnerability metrics in enterprise networks using attack graphs[J]. Journal of Computer Security, 2013, 21(4): 561-597.
- [8] 王会梅, 鲜明, 王国玉. 基于扩展网络攻击图的网络攻击策略生成算法[J]. 电子与信息学报, 2011, 33 (12): 3015-3021.
WANG H M, XIAN M, WANG G Y. A network attack decision-making algorithm based on the extended attack graph[J]. Journal of Electronics & Information Technology, 2011, 33(12): 3015-3021.
- [9] WANG H, CHEN Z F, ZHAO J P, et al. A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow[J]. Special Section on Convergence of Sensor Networks, Cloud Computing, and Big Data in Industrial Internet of Thing, 2018, (6): 8599-8609.
- [10] WANG Y Z, LIN C, CHENG X Q, et al. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computer, 2015, 38(2): 282-300.
- [11] SHEN S G, LI Y J, XU H Y, et al. Signaling game based strategy of intrusion detection in wireless sensor networks[J]. Computer&Mathematics with Applications, 2011, 62(6): 2404-2416.
- [12] DORASZEL A. Preventing DDoS attacks in wireless sensor networks: a repeated game theory approach[J]. ACM Transactions on Information and System Security, 2015, 13(2): 145-153
- [13] 张恒巍, 李涛, 黄世锐. 基于攻防微分博弈的网络安全防御决策方法[J]. 电子学报, 2018, 46(6): 1428-1435.
ZHANG H W, LI T, HUANG S R. Network defense decision-making method based on attack-defense differential game[J]. Acta Electronica Sinica, 2018, 46(6): 1428-1435.
- [14] HU H, LIU Y L, ZHANG H Q, et al. Optimal network defense strategy selection based on incomplete information evolutionary game[J]. IEEE Access, 2018, 6: 29806-29821.
- [15] GORDON L, LOEB M, LUCYSHYN W, et al. 2015 CSI/FBI computer crime and security survey[C]//2015 Computer Security Institute. 2015: 48-64.
- [16] ZHAN X Z. Matrix theory[D]. American Mathematical Society, 2010.

[作者简介]



冷强 (1993-), 男, 四川内江人, 信息工程大学硕士生, 主要研究方向为信息安全风险评估。



杨英杰 (1971-), 男, 河南郑州人, 博士, 信息工程大学教授, 主要研究方向为信息安全。



常德显 (1977-), 男, 河南邓州人, 博士, 信息工程大学副教授, 主要研究方向为信息安全。



潘瑞萱 (1995-), 女, 陕西华县人, 信息工程大学硕士生, 主要研究方向为 SDN 网络协议安全。



蔡英 (1983-), 女, 河南郑州人, 主要研究方向为金融信息安全与风险管理。



胡浩 (1989-), 男, 安徽池州人, 博士, 信息工程大学讲师, 主要研究方向为网络安全态势感知和图像秘密共享。