基于网络攻防博弈模型的最优防御策略选取方法

刘景玮[1,2] 刘京菊[1] 陆余良[1] 杨 斌[1] 朱凯龙[1]
(国防科技大学电子对抗学院 合肥 230037)[1] (31007部队 北京 100039)[2]

摘 要 为了降低安全风险损失,并在有限的资源下做出最优网络防御决策,设计了一种网络攻防博弈最优策略选取方法。首先,建立网络攻防博弈模型,证明了该模型混合策略纳什均衡的存在性;然后,给出了基于该模型的网络攻防策略选取算法,包括基于网络攻防策略图的攻防策略搜索算法、攻防双方不同策略下基于通用漏洞评分系统的效用函数量化计算方法和混合策略纳什均衡求解方法等;最后,在一个典型的网络攻防实例场景下对模型的有效性进行了分析和验证。实验结果表明,该模型能够有效地生成最优防御决策方案。

关键词 网络安全,博弈论,攻防博弈,最优策略
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.06.020

Optimal Defense Strategy Selection Method Based on Network Attack-Defense Game Model

LIU Jing-wei[1,2] LIU Jing-ju[1] LU Yu-liang[1] YANG Bin[1] ZHU Kai-long[1]
(College of Electromagnetic Countermeasure, National University of Defense Technology, Hefei 230037, China)[1]
(Troops 31007, Beijing 100039, China)[2]

Abstract In order to reduce the loss of security risk and make the optimal network defense decision under the limited resources, the optimal defense strategy selection method based on attack-defense game model was proposed. First, network attack-defense game model was established and the existence of equilibrium model of the mixed strategy Nash was proved. Then, the network attack-defense strategy selection algorithm based on the model was given, including the attack-defense strategy searching algorithm based on network attack-defense strategy graph, the calculation method of utility function under varied attack-defense strategies based on the common vulnerability scoring system and the method for solving mixed strategy Nash equilibrium. Finally, the validity of the model was analyzed and verified in a typical attack-defense experiment. The experimental results show that the model can effectively generate the optimal defense strategy.

Keywords Network security, Game theory, Attack-defense game, Optimal strategy

随着计算机网络技术的快速发展和普及,网络安全日益成为影响网络应用的重要因素[1]。在网络攻防对抗中,为了最大化攻击效果,攻击者将尽可能地使用所有可用的攻击手段。相应地,防御系统也将针对所有的攻击行为和脆弱点采取防护措施。由于资源和成本的限制,攻防双方必须在信息安全的风险和投入之间取得平衡,利用有限的资源做出合理的决策,以最小的代价取得最大的收益[2]。因此,网络攻防对抗的本质可被抽象为攻防双方间的博弈[3],网络攻防的最优防御策略问题适合运用博弈论[4]来进行研究。

目前,博弈论在网络安全领域特别是在网络攻防策略选取的研究中取得了一定成果[5-8]。姜伟等[9-10]提出了一种基于网络系统安全测评的网络攻防博弈模型,该模型能够对风险进行评估,并依据最优防御成本制定主动防御策略;但其在攻防策略的效用函数量化计算中存在主观性过强的问题。林旺群等[11]提出了完全信息动态博弈主动防御模型,通过"虚拟节点"将网络攻防图转化为攻防博弈树,并分别给出了适应于完全信息和非完全信息两种场景的攻防博弈算法;但该算法未充分考虑攻击者的意图和行为的随机变化等。刘刚等[12]利用状态攻防图,结合安全脆弱点评估系统计算效用矩阵并对其进行建模,基于博弈模型计算混合策略纳什均衡,从而给出最优攻防决策;但该防御策略由于局限于与攻击策略逐一对应,因此并未考虑所有可能的防御策略。

针对上述研究的不足,本文建立了解决网络攻防策略选取问题的网络攻防博弈模型,证明了混合策略纳什均衡的存在性,明确了该模型的可行性;定义了网络攻防策略图的概念,将寻找攻防策略问题转化为寻找图中两点间所有简单路径的问题,弥补了攻防策略考虑不够全面的不足;结合通用漏洞评分系统[13](Common Vulnerability Scoring System, CVSS),对攻防双方在不同策略下的效用函数进行了量化计算[14],解决了主观性过强的问题;给出了求解该模型混合策略纳什均

到稿日期:2017-04-14 返修日期:2017-07-06 本文受国家自然科学基金(61602491)资助。
刘景玮(1990-),男,硕士生,主要研究方向为网络安全态势感知,E-mail:jjszjpsg@163.com;刘京菊(1974-),女,硕士,副教授,主要研究方向为网络安全态势感知、网络安全检测,E-mail:80822448@qq.com(通信作者);陆余良(1964-),男,博士,教授,主要研究方向为网络安全评估;杨 斌(1989-),男,博士生,主要研究方向为计算机网络安全;朱凯龙(1991-),男,硕士生,主要研究方向为网络异常检测。

衡的标准非线性二次规划表达式;最后在一个典型的网络攻防实例场景下对模型和算法的有效性进行了分析和验证。

1 网络攻防博弈模型

网络攻防博弈模型 NADGM(Network Attack-Defense Game Model)描述了网络攻防对抗中攻击者和防御系统的基本信息、网络环境、脆弱性信息、攻防双方所有可能的攻击和防御动作以及攻防双方在不同策略下采用的效用函数。

1.1 网络攻防博弈模型的定义

定义 1 网络攻防博弈模型 NADGM 是一个六元组,可表示为 $NADGM=(P,H,F,E,S,U)$。

1)$P=\{Attacker,DefendSystem\}$,表示参加博弈的局中人集合,即为攻击者和防御系统。若攻击者的数量大于 1,则表示有多个非一致行动攻击者进行攻击;若防御系统的数量大于 1,则表示系统有多个非协同防御系统进行防御。

2)H 表示主机节点集合。对于每一个主机节点,$h=(HostID,Authority,Connectivity,v)$,$HostID$ 为该主机节点的编号,$Authority$ 表示主机节点提供使用的权限,$Connectivity$ 表示该主机节点与其他节点的联通关系,V 表示该主机的脆弱性集合。对于每一个脆弱性 v,$v=\{VulID,CVE,Precondition,Effect\}$,$VulID$ 表示脆弱性编号,CVE 表示该脆弱性的 CVE 编号,$Precondition$ 表示该脆弱性被成功利用时需要满足的前提条件集,$Effect$ 表示该脆弱性被成功利用后的后果集。

3)F 表示防御系统的防御动作集合,即防御系统可能做出的所有防御动作的集合。对于每一个防御动作,$f(v)$表示防御系统对脆弱性 v 进行修补。

4)E 表示攻击者的攻击动作集合,即攻击者可能使用的所有原子攻击集合。对于每一个原子攻击 e,$e=(AttackID,Source,Destination,VulID)$,$AttackID$ 表示原子攻击编号,$Source$ 表示原子攻击来源的主机节点,$Destination$ 表示原子攻击目标。

5)$S=\{S^A,S^D\}$,表示局中人的策略集合。$S^A=\{s_1^a,s_2^a,\cdots,s_i^a,\cdots,s_k^a\}$表示攻击者的攻击策略集,即攻击者为了达到攻击目标可能使用的所有攻击策略集合;$S^D=\{s_1^d,s_2^d,\cdots,s_j^d,\cdots,s_h^d\}$表示防御系统的防御策略集,即防御系统可能使用的所有防御策略集合。攻击策略 $s_i^a=(e_1,e_2,\cdots,e_n)(e\in E)$表示攻击者依次使用 $e_1,e_2,\cdots,e_n$ 等攻击动作进行攻击;防御策略 $s_j^d=\{f(v_1),f(v_2),\cdots,f(v_m\}(f(v)\in F)$表示防御系统对 $v_1,v_2,\cdots,v_m$ 等脆弱性进行修补。

6)$U=\{U^A,U^D\}$,表示局中人的效用函数集合。U^A 和 U^D 分别表示攻击者和防御系统的效用函数,可表示为:

$$U^A=\begin{bmatrix} u^a(s_1^a,s_1^d) & \cdots & u^a(s_1^a,s_h^d) \\ \vdots & \ddots & \vdots \\ u^a(s_k^a,s_1^d) & \cdots & u^a(s_k^a,s_h^d) \end{bmatrix}$$

$$U^D=\begin{bmatrix} u^d(s_1^a,s_1^d) & \cdots & u^a(s_1^a,s_h^d) \\ \vdots & \ddots & \vdots \\ u^d(s_k^a,s_1^d) & \cdots & u^a(s_k^a,s_h^d) \end{bmatrix}$$

其中,$u^a(s_i^a,s_j^d)$和 $u^a(s_i^a,s_j^d)(i\in[1,k],j\in[1,h])$分别表示在攻击者采取策略 s_i^a 和防御系统采取策略 s_j^d 时攻防双方各自得到的效用。

1.2 最优网络攻防策略的存在性证明

定义 2(纳什均衡,Nash Equilibrium)[15] 给定一个网络攻防博弈模型 $NADGM=(P,H,F,E,S,U)$,s_i^a 是攻击者策略,s_j^d 是防御系统策略。当且仅当该策略是攻防双方的最优策略时,策略(s^{a^*},s^{d^*})是一个纳什均衡,即满足:

$$\forall i,u^a(s^{a^*},s^{d^*})\geqslant u^a(s_i^a,s^{d^*})$$

$$\forall j,u^d(s^{a^*},s^{d^*})\geqslant u^d(s^{a^*},s_j^d)$$

因此,在网络攻防博弈中,纳什均衡就是攻防双方的最优攻防策略,攻防双方只有采取纳什均衡策略才能获得最大化收益。但由于网络攻防博弈中双方的行动具有不确定性,网络攻防博弈的纯策略纳什均衡可能并不存在,因此需要考虑混合策略下的纳什均衡。

$\theta(s_i^a)$表示攻击者选取策略 s_i^a 的概率,$\theta(s_j^d)$表示防御系统选取策略 s_j^d 的概率。$\forall i,\forall j,s_i^a\in S^A,s_j^d\in S^D,0\leqslant\theta(s_i^a)\leqslant 1,0\leqslant\theta(s_j^d)\leqslant 1,\sum_{\forall s_i^a}\theta(s_i^a)=1,\sum_{\forall s_j^d}\theta(s_j^d)=1$。混合攻击策略 $\theta(s^a)=(\theta(s_1^a),\theta(s_2^a),\cdots,\theta(s_k^a))$表示攻击者以概率的形式选取所有可能的攻击策略,混合防御策略 $\theta(s^d)=(\theta(s_1^d),\theta(s_2^d),\cdots,\theta(s_i^a),\cdots,\theta(s_h^d))$表示防御系统以概率的形式选取所有可能的防御策略。若 $\theta(s_i^a)=1,\forall w\neq i,s_w^a=0$,即 $\theta(s^a)=(0,\cdots,\theta(s_i^a),\cdots,0)$,则混合策略 $\theta(s^a)$退化为纯策略 s_i^a,因此纯策略是混合策略的一种特殊情况。

定义 3(混合策略纳什均衡) 给定一个网络攻防博弈模型 $NADGM=(P,H,F,E,S,U)$,$\theta(s^a)_i$ 是攻击者混合策略,$\theta(s^d)_j$是防御系统混合策略。混合策略$(\theta(s^a)^*,\theta(s^d)^*)$是一个纳什均衡,当且仅当该混合策略是攻防双方的最优响应策略,即满足:

$$\forall\theta(s^a)_i,u^a(\theta(s^a)^*,\theta(s^d)^*)\geqslant u^a(\theta(s^a)_i,\theta(s^d)^*)$$

$$\forall\theta(s^d)_j,u^d(\theta(s^a)^*,\theta(s^d)^*)\geqslant u^d(\theta(s^a)^*,\theta(s^d)_j)$$

定理 1(纳什均衡存在性) 给定一个网络攻防博弈模型 $NADGM=(P,H,F,E,S,U)$,则至少存在一个纳什均衡,包括纯策略纳什均衡和混合策略纳什均衡[16]。

网络攻防博弈模型 $NADGM=(P,H,F,E,S,U)$是一个矩阵型博弈,其攻防动作集 E 和 V、攻防策略集 S、效用函数都是有限的,因此网络攻防博弈模型 NADGM 是一个有限博弈。纳什利用不动点定理证明了每一个有限博弈都存在纳什均衡[17],因此网络攻防博弈模型 NADGM 存在一个稳定的纳什均衡,即给定一个网络攻防博弈模型,一定可以求解出其最优攻防策略。

2 网络攻防博弈最优策略的选取

网络攻防策略的选取十分复杂,以防御系统为例:当攻击者只存在一种攻击策略时,防御系统仅需选择效用最高的防御策略;但当存在多个可能的攻击策略时,防御系统需要综合考虑不同攻击策略下各防御策略的成本和代价,并且由于多个攻击策略的发生概率是未知的,如何保证防御策略的综合期望效用最高就更为复杂。基于博弈模型的网络攻防博弈最优策略选取算法可以较好地解决此类问题,具体描述如算法 1 所示。

算法 1 网络攻防策略选取算法 SSelection(P,H)

输入:参与博弈的局中人 P,主机节点信息 H

输出：最优攻击策略 s^{a*}，最优防御策略 s^{d*}

1. 根据定义初始化网络攻防博弈模型 NADGM；
2. 建立网络攻防策略图 NADSG；
3. 调用攻击策略搜索算法寻找所有可能的攻击策略集：$S^A=\{s_1^a, s_2^a, \cdots, s_k^a\}$；
4. 调用防御策略搜索算法寻找所有可能的防御策略集：$S^D=\{s_1^d, s_2^d, \cdots, s_h^d\}$；
5. 循环：对于每一对策略$(s_i^a, s_j^d)\in S^A\times S^D$
6. 　根据攻防策略效用函数量化方法，计算在攻击者使用策略 s_i^a 和防御系统使用策略 s_j^d 时的效用值 $u^a(s_i^a, s_j^d)$和 $u^d(s_i^a, s_j^d)$；
7. 循环结束；
8. 求解网络攻防博弈模型的混合策略纳什均衡，从而得到最优攻击策略 s^{a*} 和最优防御策略 s^{d*}；
9. 返回 s^{a*} 和 s^{d*}.

下面对网络攻防策略选取算法中的攻防策略搜索算法、攻防策略效用函数量化方法和混合策略纳什均衡求解方法进行详细介绍。

2.1　攻防策略搜索算法

在网络攻防博弈中，攻击方和防御系统均存在多种攻防策略，为了不遗漏可能的最优策略，需要搜索所有可能的攻防策略。本文基于攻防动作、脆弱性和主机权限节点建立网络攻防策略图，并对其进行搜索，以得到所有可能的攻防策略。

定义 4（网络攻防策略图，Network Attack-Defense Strategy Graph，NADSG）　网络攻防策略图一个有向图，$NADSG=(H,V,E)$。其中，H 是图的节点集，每一个节点表示一台主机，入度为 0；V 是 H 的子节点，每一个子节点表示主机节点的一个脆弱性，出度为 0；E 是图的有向边集，表示所有可能的攻击动作。

图 1 给出了网络攻防策略的一个示例。其中存在 3 台主机 h_1，h_2，h_3；4 个主机权限节点 h_1^{root}，h_2^{user}，h_2^{root}，h_3^{root}，其中 h_1^{root} 为攻击者的起始攻击节点，h_3^{root} 为攻击者的目标节点，攻击者从 h_1 开始以 h_2 为跳板攻击 h_3；h_2 节点存在 3 个脆弱性 v_1，v_2，v_3，h_3 节点存在 1 个脆弱性 v_4；有向边 e_1，e_2，e_3，e_4 表示攻击者可能使用的 4 个原子攻击。

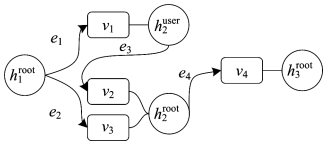


图 1　网络攻防策略示例

Fig. 1　Example of network attack-defense strategy

图 1 中存在两条可能的从攻击起点到目标节点的简单路径，分别为(e_1, e_3, e_4)和(e_2, e_4)。(e_1, e_3, e_4)表示攻击者首先使用原子攻击 e_1 通过脆弱性 v_1 获得 h_2^{user}，然后使用原子攻击 e_3 通过脆弱性 v_2 获得 h_2^{root}，最后使用原子攻击 e_4 通过脆弱性 v_4 获得 h_3^{root}。(e_2, e_4)表示攻击者首先使用原子攻击 e_2 通过脆弱性 v_3 获得 h_2^{root}，然后使用原子攻击 e_4 通过脆弱性 v_4 获得 h_3^{root}。

不难发现，从网络攻防策略图的攻击者节点到达目标节点的路径即为攻击者的攻击策略，因此可以将求解所有攻击策略的问题（即求解所有可能的原子攻击序列）转化为求解网络攻防策略图中指定两点间的所有路径的问题。攻击策略搜索算法如算法 2 所示。

算法 2　攻击策略搜索算法 SAStrategy($NADSG, h_0, h_g$)

输入：网络攻防策略图 NADSG，起始节点 h_0，目标节点 h_g

输出：攻击策略集 AStrategy

1. 如果 h_0 与 h_g 为同一节点；
2. 　则将策略 temp 加入策略集 Astrategy；
3. 否则
4. 循环：对于每一个以 h_0 为起点的有向边 e
5. 　　将 e 加入到 temp；
6. 　　将 e 指向的节点 h 的所有子节点和指向 h 的所有有向边从 NADSGNADSG 中去除；
7. 　　调用算法 SAStrategy(NADSG, h, h_g)；
8. 　　从 temp 中去除 e；
9. 　　恢复去除的 h 的所有子节点和指向 h 的所有有向边；
10. 循环结束.

对于防御系统而言，其策略是修补不同的系统脆弱性，因此求解防御策略的问题可以转化成求解脆弱性集合的所有子集的问题。防御策略搜索算法如算法 3 所示。

算法 3　防御策略搜索算法 SDStrategy(v)

输入：脆弱性集合 v

输出：防御策略集 DStrategy

1. 如果 v 为空；
2. 　则将策略 temp 加入策略集 DStrategy；
3. 否则从 v 中任选一脆弱性 vq；
4. 将 vq 从 v 中删除；
5. 调用算法 SDStrategy(v)；
6. 将 vq 加入 temp；
7. 调用算法 SDStrategy(v).

2.2　攻防策略效用函数的量化

现有的网络攻防的成本和收益计算方法中均不同程度地存在主观性过强的问题，为避免该问题，模型采取基于 CVSS 评分的机制来量化成本和收益的方法。CVSS 是一个行业公开标准，主要用于评测漏洞的严重程度，并帮助用户确定所需反应的紧急度和重要度。

2.2.1　攻防成本的计算

对于一个攻击动作 e，$profit^e$ 和 $cost^e$ 分别表示攻击方发动原子攻击 e 后的收益和成本。对于一个防御动作 v，$profit^v$ 和 $cost^v$ 分别表示防御系统对脆弱性 v 修补后的收益和成本。

攻击方发动原子攻击的成本 $cost^e$ 和防御方防御该原子攻击的成本 $cost^v$ 受该原子攻击实施的难易程度、攻击类型等多个因素的影响。为了简化计算，本文仅考虑脆弱性被利用的难易程度 $Utilizability$。

脆弱性越容易被利用，则防御系统针对该脆弱性攻击所需投入的成本就越高。基于 CVSS 标准，可以定义 $cost^v$ 为：

$$cost^v=\mu\cdot Utilizability$$

相应地，脆弱性越容易被利用，攻击者在攻击时投入的成本就越小。基于 CVSS 标准，可以定义 $cost^e$ 为：

$$cost^e=\frac{\mu}{Utilizability}$$

其中，μ 为修正因子，根据 CVSSv2.0 的定义取值为 20；*Utiliza-bility* 表示脆弱性的可利用性，基于 CVSS 标准可以定义为：

$$Utilizability = AccessVector \cdot AccessComplexity \cdot Authentication$$

其中，*AccessVector* 表示该脆弱性可被利用的访问方式，*AccessComplexity* 表示该脆弱性的访问复杂度，*Authentication* 表示原子攻击所需要的权限。根据 CVSSv2.0 标准，各要素的度量及取值如表 1 所列。

表 1 *Utilizability* 要素取值

Table 1 *Utilizability* element value

要素	度量	取值
AccessVector	Local	0.395
AccessVector	AdjacentNetwork	0.646
AccessVector	Network	1.000
AccessComplexity	Low	0.710
AccessComplexity	Medium	0.610
AccessComplexity	High	0.350
Authentication	None	0.704
Authentication	Single	0.560
Authentication	Multiple	0.450

2.2.2 攻防收益的计算

定义攻击方发动攻击动作 e 的收益 $profit^e$ 等于原子攻击对网络系统造成的危害 *Impact*；防御系统修补脆弱性 v 后的收益 $profit^v$ 即为修补脆弱性 v 后系统免受的危害，在数值上也等于利用该脆弱性的原子攻击对系统造成的危害。因此，$profit^e = profit^v = Impact$。

根据 CVSS 中脆弱点损害的计算方法，定义原子攻击攻击成功的危害 *Impact* 为：

$$Impact = \lambda \cdot Importance \cdot (1-(1-Confidentiality) \cdot (1-Integrity) \cdot (1-Availability))$$

其中，λ 为修正因子，根据 CVSSv2.0 标准取值为 10.41；*Importance* 表示该脆弱性对系统的重要程度，取值范围为[0，1]；*Confidentiality* 表示该脆弱性对系统造成的机密性危害；*Integrity* 表示造成的完整性危害；*Availability* 表示造成的可用性危害。根据 CVSSv2.0 标准，要素 *Confidentiality*，*Integrity*，*Availability* 的度量及取值如表 2 所列。

表 2 *Impact* 要素取值

Table 2 *Impact* element value

要素	度量	取值
Confidentiality，*Integrity*，*Availability*	None	0
	Partial	0.275
	Complete	0.660

2.2.3 攻防策略效用的计算

当攻击者使用攻击策略 $s_i^a = (e_1, e_2, \cdots, e_n)$，防御系统使用防御策略 $s_j^d = \{f(v_1), f(v_2), \cdots, f(v_m)\}$ 时，攻击策略 s_i^a 的效用 $u^a(s_i^a, s_j^d)$ 为：

$$\begin{aligned} u^a(s_i^a, s_j^d) &= u^a((e_1, e_2, \cdots, e_n), \{f(v_1), f(v_2), \cdots, f(v_m)\}) \\ &= \sum_{\forall e_p \in s_i^a, e_p.v \notin \{v_1, v_2, \cdots, v_m\}} profit_p^e - \sum_{\forall e_p} cost_p^e \end{aligned} \quad (1)$$

其中，$\forall e_p \in s_i^a, e_p.v \notin \{v_1, v_2, \cdots, v_m\}$ 表示利用防御策略没有修补的脆弱性所进行的所有攻击动作。防御策略 s_j^d 的效用 $u^d(s_i^a, s_j^d)$ 为：

$$\begin{aligned} u^d(s_i^a, s_j^d) &= u((e_1, e_2, \cdots, e_n), \{f(v_1), f(v_2), \cdots, f(v_m)\}) \\ &= \sum_{\forall v_q, v_q \in \{e_1.v, e_2.v, \cdots, e_n.v\}} profit_q^d - \sum_{\forall v_q} cost_q^d \end{aligned} \quad (2)$$

其中，$\forall v_q, v_q \in \{e_1.v, e_2.v, \cdots, e_n.v\}$，表示所有修补的攻击策略所利用的脆弱性。由式(1)、式(2)即可计算出攻防双方不同策略组合下的效用。

2.3 混合策略纳什均衡求解方法

对于矩阵型博弈求解混合策略纳什均衡的问题，常用的方法之一是将其转化为标准非线性规划问题进行求解[18]。将网络攻防博弈模型混合策略纳什均衡转化为标准非线性二次规划，具体表达式如下：

$$\begin{aligned} &\min\ z = \beta^a - \theta(s_i^a) U^A \theta(s_j^d)^{\mathrm{T}} + \beta^d - \theta(s^d af_i) U^D \theta(s_j^d)^{\mathrm{T}} \\ &\text{s.t. } \forall i = 1, 2, \cdots, n \\ &\quad \forall j = 1, 2, \cdots, m \\ &\quad \theta(s_i^a) \geqslant 0, \theta(s_j^d) \geqslant 0 \\ &\quad \sum_{i=1}^{n} \theta(s_i^a) = \sum_{j=1}^{m} \theta(s_j^d) = 1 \\ &\quad \theta(s_i^a) U^A \theta(s_j^d)^{\mathrm{T}} \leqslant \beta^a \\ &\quad \theta(s_i^a) U^D \theta(s_j^d)^{\mathrm{T}} \leqslant \beta^d \end{aligned}$$

其中，β^a 和 β^d 分别表示在纳什均衡点攻击者和防御系统的期望效用；$\theta(s_i^a) U^A \theta(s_j^d)^{\mathrm{T}} \leqslant \beta^a$ 表示在纳什均衡中，攻击方采用任意一个策略得到的期望效用均不大于在纳什均衡点攻击者的期望效用。同样地，$\theta(s_i^a) U^D \theta(s_j^d)^{\mathrm{T}} \leqslant \beta^d$ 表示在均衡情况下，防御方采用任一策略得到的期望效用均不大于在纳什均衡点防御系统的期望效用。对于这样的标准非线性优化问题，使用通用的拟牛顿法即可求解[19]。

3 实例与分析

为了验证本文方法的有效性，设计了典型的网络攻防场景进行实验，如图 2 所示。攻击机位于外部网络；内网中包含 4 台服务器，分别为 Web 服务器、FTP 服务器、Mail 服务器和 DB 服务器；防火墙将内部网络与外部网络隔离开，防火墙的详细规则如表 3 所列。

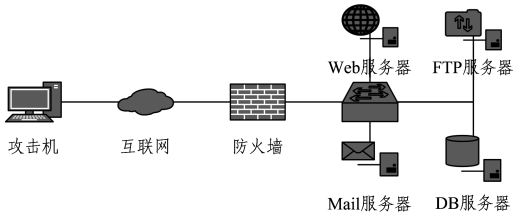


图 2 实验环境拓扑图

Fig. 2 Topological diagram of experimental environment

表 3 防火墙规则

Table 3 Firewall rules

访问来源	访问目标	开放服务(端口)	规则
所有	Web 服务器	HTTP(80)	Allow
所有	MAIL 服务器	SMTP(25)，IMAP(143)	Allow
Web 服务器	DB 服务器	Oracle DB(1521)	Allow
Mail 服务器	DB 服务器	Oracle DB(1521)	Allow
FTP 服务器	DB 服务器	Oracle DB(1251)	Allow
Web 服务器	FTP 服务器	FTP(20，21)	Allow
Mail 服务器	FTP 服务器	FTP(20，21)	Allow
DB 服务器	FTP 服务器	FTP(20，21)	Allow
其他			Forbidden

FTP 服务器、DB 服务器不能直接从外网访问，Web 服务

器和 Mail 服务器分别对外网提供 HTTP 服务、SMTP 服务和 IMAP 服务；攻击者在攻击主机上具有 root 权限，并发起以获取 DB 服务器的 root 权限为目标的攻击行为。

为了突出实验效果，设置本次实验中的脆弱性均为远程网络访问权限获取的漏洞。目标系统的脆弱性和所在节点的重要程度如表 4 所列。

表 4　系统的脆弱性和所在节点的重要程度

Table 4　System vulnerability and importance of node

脆弱性	所在节点	CVE 编号	后果	重要程度
v_1	Web 服务器	CVE-2013-0003	获取 root 权限	0.7
v_2	Mail 服务器	CVE-2014-3333	获取 root 权限	0.5
v_3	Mail 服务器	CVE-2015-1312	获取 root 权限	0.5
v_4	DB 服务器	CVE-2010-3585	获取 root 权限	1
v_5	FTP 服务器	CVE-2012-2015	获取 root 权限	0.3
v_6	FTP 服务器	CVE-2010-3972	获取 root 权限	0.3

根据节点、脆弱性和连通关系信息建立网络攻防策略图，如图 3 所示，在此场景中攻击者共有 16 个可能的原子攻击和 6 个可能的防御动作。

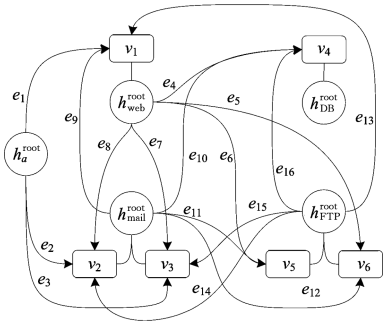


图 3　网络攻防策略图

Fig. 3　Network attack-defense strategy graph

使用上文中的攻防策略效用函数量化计算方法对攻防策略的效用进行量化计算。根据成本和收益的定义及相应脆弱性的 CVSS 评分，得到攻击和防御动作的成本和收益，如表 5 所列。将攻防双方不同的策略代入式(1)和式(2)，得到攻击者和防御系统的效用函数 U^A 和 U^D。

表 5　网络攻击动作和防御动作的成本和收益量化表

Table 5　Cost and profit quantification of network attack and defense action

脆弱性	*AccessVector*	*AccessComplexity*	*Authentication*	*Utilizability*	$cost^v$	$cost^e$	*Confidentiality*	*Integrity*	*Availability*	*Impact*
v_1	NETWORK	MEDIUM	SINGLE	0.3416	6.832	2.9274	COMPLETE	COMPLETE	COMPLETE	7.000
v_2	NETWORK	LOW	SINGLE	0.3976	7.952	2.5151	COMPLETE	COMPLETE	COMPLETE	5.000
v_3	NETWORK	LOW	NONE	0.4998	9.997	2.0006	COMPLETE	COMPLETE	COMPLETE	5.000
v_4	NETWORK	LOW	SINGLE	0.3976	7.952	2.5151	COMPLETE	COMPLETE	COMPLETE	10.000
v_5	NETWORK	LOW	NONE	0.4998	9.997	2.0006	PARTIAL	PARTIAL	PARTIAL	1.932
v_6	NETWORK	LOW	SINGLE	0.3976	7.952	2.5151	COMPLETE	COMPLETE	COMPLETE	3.000

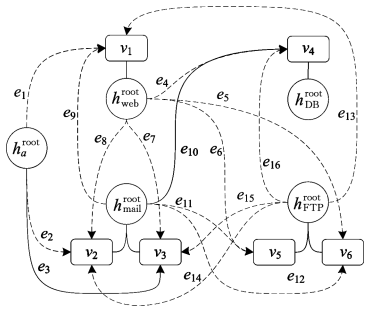
使用攻击策略搜索算法找到 29 个可能的攻击策略，如表 6 所列；使用防御策略搜索算法找到 64 个的可能的防御策略。

表 6　攻击策略集

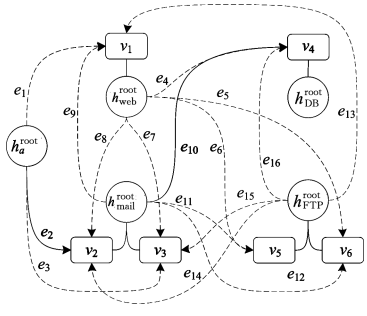
Table 6　Attack strategy set

策略	攻击序列				策略	攻击序列			
s^a_1	e_1	e_4			s^a_{16}	e_2	e_9	e_4	
s^a_2	e_1	e_5	e_{16}		s^a_{17}	e_3	e_9	e_4	
s^a_3	e_1	e_6	e_{16}		s^a_{18}	e_2	e_{11}	e_{16}	
s^a_4	e_1	e_7	e_{10}		s^a_{19}	e_2	$e_1 2$	e_{16}	
s^a_5	e_1	e_8	e_{10}		s^a_{20}	e_3	e_{11}	e_{16}	
s^a_6	e_1	e_5	e_{15}	e_{10}	s^a_{21}	e_3	e_{12}	e_{16}	
s^a_7	e_1	e_5	e_{14}	e_{10}	s^a_{22}	e_2	e_9	e_5	e_{16}
s^a_8	e_1	e_6	e_{15}	e_{10}	s^a_{23}	e_2	e_9	e_6	e_{16}
s^a_9	e_1	e_6	e_{14}	e_{10}	s^a_{24}	e_3	e_9	e_5	e_{16}
s^a_{10}	e_1	e_7	e_{11}	e_{16}	s^a_{25}	e_3	e_9	e_6	e_{16}
s^a_{11}	e_1	e_7	e_{12}	e_{16}	s^a_{26}	e_2	e_{11}	e_{13}	e_4
s^a_{12}	e_1	e_8	e_{11}	e_{16}	s^a_{27}	e_2	e_{12}	e_{13}	e_4
s^a_{13}	e_1	e_8	e_{12}	e_{16}	s^a_{28}	e_3	e_{11}	e_{13}	e_4
$s^a_1 4$	e_2	e_{10}			s^a_{29}	e_3	e_{12}	e_{13}	e_4
$s^a_1 5$	e_3	e_{10}							

最后，调用攻防博弈最优策略选取算法将求解混合策略纳什均衡转化为求解标准非线性二次规划问题，结果保留至小数点后 4 位，可得最优混合攻击策略为(0,0,0,0,0,0,0,0,0,0,0,0,0,0.1970,0.8030,0,0,0,0,0,0,0,0,0,0,0,0,0,0)，即有 80.30%的概率采用策略 s^a_{15}，有 19.70%的概率采用策略 s^a_{14}，如图 4 所示。以图 4(a)为例，最优攻击策略中有 80.30%的概率攻击者将率先利用邮件服务器上的 CVE-2015-1312 脆弱点发起攻击，获取邮件服务器的 root 权限；然后利用数据库服务器上的 CVE-2010-3585 脆弱点发起攻击，获取数据库服务器的 root 权限。



(a) s^a_{15}

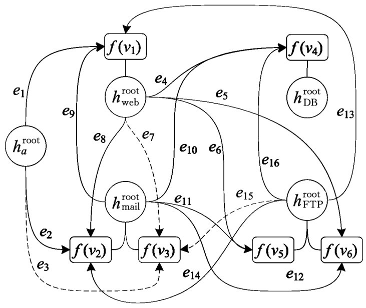


(b) s^a_{14}

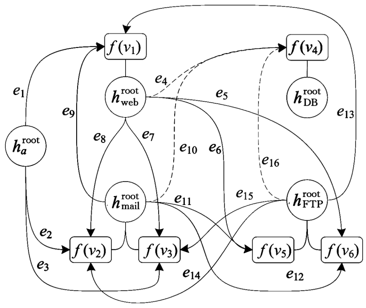
图 4　最优混合攻击策略

Fig. 4　Optimal mixed attack strategy

求得的最优混合防御策略为 s^{d^*} =(0,0,0,0,0.3140,0,0,0,0.6859,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),即有 68.59%的概率采用策略 s_9^d、有 31.40%的概率采用策略 s_5^d、有 0.01%的概率采用其他策略,如图 5 所示。以图 5(a)为例,最优攻击策略中有 68.59%的概率防御系统将采用更新 SAP ERP 软件修补 CVE-2015-1312 脆弱点来实现对系统的防御。显然,依据求得的最优防御策略,防御系统将优先加固系统的“关键节点”v_4,这一决策行为符合网络攻防中的实际情况。



(a)s_9^d



(b)s_5^d

图 5　最优混合防御策略

Fig. 5　Optimal mixed defense strategy

结束语　针对相关研究中存在的效用函数量化主观性过强、攻防策略考虑不够全面的问题,本文建立了网络攻防博弈模型,给出了基于该模型的网络攻防策略选取算法,包括网络攻防策略图的攻防策略搜索算法、攻防双方不同策略下基于通用漏洞评分系统的效用矩阵量化计算方法和混合策略纳什均衡求解方法。基于典型网络攻防场景的实验结果表明,网络攻防博弈模型和网络攻防策略选取算法能够较好地描述攻击者与防御系统间攻防过程的定量关系,其提供的网络攻防最优策略能够很好地找到针对某个威胁危害程度最大的节点和路径,有效地降低了安全风险损失,并能够在有限的资源下做出最优网络防御决策。

参 考 文 献

[1] HAMILTON S N,MILLER W L,OTT A,et al. The Role of Game Theory in Information Warfare[C]// 14th Information Surlivability Workshop(ISW-2001/2002). Vancouver,Canada,2002:46-56.

[2] WU Y,FENG G,WANG N,et al. Game of information security investment:Impact of attack types and network vulnerability[J]. Expert Systems with Applications,2015,42(15/16):6132-6146.

[3] ROY S,ELLIS C,SHIVA S,et al. A Survey of Game Theory as Applied to Network Security[C]// Hawaii International Conference on System Sciences. IEEE,2010:1-10.

[4] KUHN H W,MORGENSTERN O,RUBINSTEIN A. Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition)[M]// Theory of Games and Economic Behavior. Princeton:Princeton University Press,1944:2-14.

[5] LYE K W,WING J M. Game strategies in network security[J]. International Journal of Information Security,2005,4(1):71-86.

[6] MEDIA. Game Theory for Network Security[J]. Game Theory Applications in Network Design,2013,15(1):472-486.

[7] XI R R,YUN X C,ZHANG Y Z,et al. An Improved Quantitative Evaluation Method for Network Security [J]. Chinese Journal of Computer,2015,38(4):749-758. (in Chinese)
席荣荣,云晓春,张永铮,等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报,2015,38(4):749-758.

[8] GAO N,GAO L,HE Y Y,et al. Dynamic security risk assessment model based on Bayesian attack graph[J]. Journal of Sichuan University(Engineering Science Edition),2016,48(1):111-118. (in Chinese)
高妮,高岭,贺毅岳,等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报(工程科学版),2016,48(1):111-118.

[9] JIANG W,FANG B X,TIAN Z H,et al. Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model [J]. Chinese Journal of Computer,2009,32(4):817-827. (in Chinese)
姜伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2009,32(4):817-827.

[10] JIANG W,TIAN Z H,ZHANG H L,et al. A Stochastic Game Theoretic Approach to Attack Prediction and Optimal Active Defense Strategy Decision[C]// IEEE International Conference on Networking,Sensing and Control. IEEE,2008:648-653.

[11] LIN W Q,WANG H,LIU J H,et al. Research on Active Defense Technology in Network Security Based on Non-Cooperative Dynamic Game Theory [J]. Journal of Computer Research and Development,2011,48(2):306-316. (in Chinese)
林旺群,王慧,刘家红,等. 基于非合作动态博弈的网络安全主动防御技术研究[J]. 计算机研究与发展,2011,48(2):306-316.

[12] LIU G,ZHANG H,LI Q M. Network security optimal attack and defense decision-making method based on game model [J]. Journal of Nanjing University of Science and Technology,2014,38(1):12-21. (in Chinese)
刘刚,张宏,李千目. 基于博弈模型的网络安全最优攻防决策方法[J]. 南京理工大学学报(自然科学版),2014,38(1):12-21.

[13] FIRST. Common Vulnerability Scoring System[EB/OL]. [2017-01-28]. https://www.first.org/CVSS.

[14] CHENG P,WANG L,JAJODIA S,et al. Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics[C]//

IEEE Symposium on Reliable Distributed Systems. IEEE Computer Society，2012：31-40.

[15] NASH J F. Equilibrium points in n-person games[J]. Proceedings of the National Academy of Sciences of the United States of America，1950，36(1)：48-49.

[16] FUDENBERG D，TIROLE J. Game Theory[J]. Mit Press Books，2009，1(7)：29-30.

[17] NASH J. Non-Cooperative Games[J]. Annals of Mathematics，1951，54(2)：286-295.

[18] CHATTERJEE B. An optimization formulation to compute Nash equilibrium in finite games[C]// International Conference on Methods and MODELS in Computer Science. IEEE，2009：1-5.

[19] 黄象鼎，曾钟钢，马亚南. 非线性数值分析的理论与方法[M]. 武汉：武汉大学出版社，2004.

（上接第 99 页）

其中最下方的直线是没有加入重传机制的节点的能量消耗。可以看出，该机制下功耗不随环境扰动而增加且其电能开销最低。图 10 中中间的曲线为加入动态重传机制后的能量消耗，可以看出，由于扰动而使重传机制介入，数据发送次数有所增加，从而能耗曲线较第一条有所增加。图 10 中最上方的曲线为立即重传机制下节点的能耗统计，其能耗也是随着扰动的产生而相应地增加，而由于其重传时机没有规避性，只是机械式地重复尝试发送，因此其能耗开销最大。

在抗干扰对抗实验中，在人流活动量最大、对网络干扰最严重的时段内分析节点的重传规律。节点通过 5 个重传区域将数据成功重传至基站端，图 11 给出了网络中节点在各重传区域所占的比例。数据重传基本在前 3 个重传区域成功发送并到达基站。实验结果表明，动态重传在重传时机上优于立即重传。一旦发生某时段内链路通信失败的情况，其能使节点重新加入到新的发送队列中，选择不同的时机进行发送，能较好地规避随机出现的干扰，从而有效地提高其发送成功率。动态重传机制使系统拥有更强的抗扰动能力，从而在总体上保障了数据发送的可靠性，同时该机制也兼顾了较低的能耗开销，通过提高发送的有效性来降低能耗的额外开销。

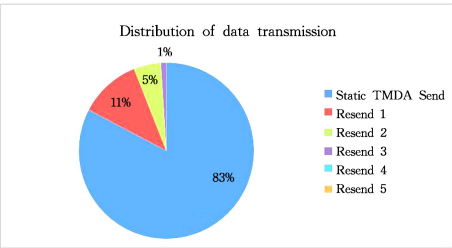


图 11　引入大量干扰源后的数据重传分布

Fig. 11　Data transmission after introducing a large number of interference sources

结束语　本文主要研究对数据发送实时性要求不高的无线传感器网络数据发送策略。针对低功耗节点与基站的通信特性，提出一种提高发送可靠性的算法，以抵抗通信链路的时变性以及外界环境随机变化而引起的通信质量不佳导致的数据丢失。加入动态重传机制后的系统在一定程度上提高了节点发送成功率。在未来的工作中，将研究加入动态重传机制后，如何优化网络最大负载。

参 考 文 献

[1] LI R，SUN G，LIAO H，et al. Lifetime analysis of wireless sensor networks under retransmission[C]// Reliability and Maintainability Symposium. IEEE，2014.

[2] COSTA D G，GUEDES L A，VASQUES F，et al. Partial energy-efficient hop-by-hop retransmission in wireless sensor networks[C]// IEEE International Conference on Industrial Informatics. IEEE，2013：146-151.

[3] LIN X，LIU X，LEI D，et al. RRM-B：Reliable retransmission mechanism for wireless sensor networks[C]// IEEE International Conference of Online Analysis and Computing Science. IEEE，2016：206-213.

[4] YING B. An adaptive compression algorithm for energy-efficient wireless sensor networks[C]// International Conference on Advanced Communication Technology. IEEE，2017：861-868.

[5] XU X Z，WANG C L. Node Density and TDMA Based Clustering Hierarchy Protocol of Wireless Sensor Network[J]. Chinese Journal of Sensors and Actuators，2015，28(11)：1689-1694.（in Chinese）
徐祥振，汪成亮. 基于节点密度与 TDMA 的无线传感器网络集簇协议[J]. 传感技术学报，2015，28(11)：1689-1694.

[6] DU M，HUANG J，SHI W R，et al. Low timedelay WSNs MAC protocol based on competition and TDMA[J]. Transducer and Microsystem Technologies，2014，33(10)：111-114.（in Chinese）
杜敏，黄剑，石为人，等. 基于竞争与 TDMA 的低时延无线传感器网络 MAC 协议[J]. 传感器与微系统，2014，33(10)：111-114.

[7] CHEN K F，LV N，ZHANG W L，et al. Cooperative dynamic TDMA MAC protocol based on awareness of transmission business[J]. Computer Engineering And Design，2015，36(10)：2607-2612.（in Chinese）
陈柯帆，吕娜，张伟龙，等. 基于业务量感知的动态 TDMA 协作 MAC 协议[J]. 计算机工程与设计，2015，36(10)：2607-2612.

[8] ZHANG Z S，YUAN H Q，YU F Q. A Dynamic Retransmission Algorithm for Wireless Sensor Networks[J]. 2013，26(7)：1019-1024.（in Chinese）
张足生，袁华强，于峰崎. 无线传感器网络动态重传算法[J]. 传感技术学报，2013，26(7)：1019-1024.