基于多阶段攻防信号博弈的最优主动防御

张恒巍,李 涛
(信息工程大学三院,河南郑州 450001)

摘 要: 从网络攻防对抗的实际场景出发,针对具有不完全信息约束的多阶段动态攻防过程,构建了多阶段攻防信号博弈模型.针对多阶段攻防过程中信号作用衰减的问题,提出信号衰减因子进行量化描述.在此基础上,设计了多阶段攻防博弈均衡的求解方法,并给出了最优主动防御策略选取算法.通过仿真实验验证了本文模型和方法的有效性,并且分析总结了多阶段攻防博弈的规律.

关键词: 网络攻防;多阶段信号博弈;信号衰减;博弈均衡;防御策略
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)02-0431-09
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.02.023

Optimal Active Defense Based on Multi-stage Attack-Defense Signaling Game

ZHANG Heng-wei, LI Tao
(*The Third Institute, Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: From the real network attack-defense, aimed at the multi-stage and dynamic attack-defense process with the restriction of incomplete information, the multi-stage attack-defense signaling game model is proposed in the paper. Considering attenuation of the signal effect in the multi-stage attack and defense, signal attenuation factor is proposed for the quantification of attenuation. Based on the above, we design the solution for game equilibrium in multi-stage attack and defense. Then the algorithm of optimal active defense strategies selection is proposed. Finally, a simulation experiment is conducted to verify the effectiveness of the model and method proposed in the paper, through which some rules in the multi-stage attack-defense game are concluded.

Key words: network attack and defense; multi-stage signaling game; signaling attenuation; game equilibrium; defense strategies

1 引言

当前各类信息安全事件严重威胁网络安全[1],而防火墙、入侵检测等安全技术,其实质是一种被动等待式的安全保护措施.在攻击造成大规模破坏之前,有效地分析和预测攻击行为及其危害,有针对性的采取主动防御措施已经成为急切的现实需求[2].积极探索并构建网络安全主动防御体系已成为近年来解决信息安全问题的新方向和研究热点[3].博弈论与网络攻防所具有的目标对立性、关系非合作性和策略依存性高度契合[4],目前基于博弈模型的攻防行为分析和防御策略选取研究已取得了丰富的成果.

网络攻防博弈分析必须解决两个关键问题:如何破解博弈信息不完全的约束以及如何描述博弈方的行动顺序.部分研究者基于攻防双方具有完全博弈信息并且同时行动的假设开展研究,例如文献[5]将网络攻防建模为两角色零和博弈过程,基于完全信息静态博弈理论分析攻防行为,研究最优主动防御策略的选取.文献[6]以在线社交网络为背景,在完全信息条件下构建静态博弈模型对攻击者行为进行分析.由于网络攻防双方的对立竞争关系,掌握对方的博弈信息非常困难,因此完全信息假设很难满足.针对网络攻防中不完全博弈信息的实际情况,文献[7]中构建了静态贝叶斯攻防博弈模型,通过求解静态贝叶斯均衡实现最优防御策略的选取.文献[8]引入不完全信息静态博弈理

收稿日期:2015-08-03;修回日期:2016-05-30;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61303074,No.61309013);河南省科技计划基金(No.13210231002)

论,对蠕虫病毒攻击和防御策略的效能进行了分析研究. 文献[9]针对网络战的攻防决策问题采用不完全信息重复博弈进行了建模和研究. 另一方面,由于网络攻防的动态性,攻防双方同时行动的限制条件很难满足,因此动态博弈理论更加符合实际,研究成果实用性和指导意义更大. 文献[10]和文献[11]均提出运用随机博弈理论来分析网络攻防过程,不足之处在于状态转移概率函数不易确定,使得模型通用性和实用性受到限制. 文献[12]中引入动态博弈理论研究网络安全主动防御,通过求解和分析博弈均衡实现最优防御策略的选取. 但是,上述成果全部以完全博弈信息为前提,虽然实现了攻防博弈的动态分析,但仍然存在较大的不足.

不完全信息动态博弈模型可以同时满足上述两个条件,尤其是信号博弈模型(Signaling Game Model),因为可以准确描述情报信息对攻防双方策略选择的关键作用而受到研究者的特别关注. 文献[13]针对 DDoS 攻击的防御决策问题,构建信号博弈模型研究攻防行为和信号作用机理,在均衡分析的基础上设计了最优防御策略选择算法. 文献[14]采用信号博弈模型建模攻防场景,分析攻防双方的博弈收益,设计了一种信息安全防御机制.

但是,上述文献受制于基本信号博弈模型的限制,都只能对单阶段网络攻防行为进行分析,即在模型中攻防双方的策略选择和对抗过程限制为仅一个回合,无法满足动态多阶段攻防博弈分析的需求. 由于实际的网络攻防过程往往持续多个阶段,且双方能够根据前一阶段对抗的过程和结果信息更加准确地掌握对手情况,进而修改自身的行为策略. 因此,具有不完全信息性、动态性、多阶段性特征的攻防行为分析模型更加符合实际. 然而和基本信号博弈不同,在动态多阶段信号博弈中,信号的作用随攻防进程的发展而动态变化,所以动态多阶段攻防信号博弈模型的构建和分析难度大,目前据我们所知尚未有公开文献予以讨论.

本文构建多阶段攻防信号博弈模型,对随着攻防进程的演进,不同阶段中双方逐渐更加全面地了解对手类型,进而调整自身行为策略的决策过程进行研究. 通过分析不同阶段中博弈信号作用的变化机理,提出信号衰减因子表征博弈信号作用在不同阶段的变化. 在上述基础上,通过对不同阶段博弈均衡的分析,说明博弈信号及其释放机制在主动防御中的作用,并设计最优防御策略选取方法. 与已有工作相比,本文方法能对信息受限条件下的动态多阶段攻防过程进行分析,适用性更强,防御策略选取的准确性和可信性更好.

2 多阶段攻防信号博弈模型

2.1 多阶段攻防博弈过程分析

从网络攻防的实际分析,一方面,安全防御需要服从网络系统提供公共服务的要求. 另一方面,攻击者一般事先对防御系统进行探测,通过分析探测到的系统指纹、漏洞等信息了解防御措施和强度,或利用公开信息收集系统的安全防御情况. 上述由攻击者探测或防御者释放的有关防御措施的信息是攻击决策的重要依据,本文将其定义为防御信号. 防御信号的存在具有普遍性,是攻击者分析和判定防御类型,进而决定是否攻击、采取何种攻击方式的关键要素之一,对防御信号实施管控能够对攻击行为施加重要影响,改变攻防双方的收益. 防御者通过有针对性地主动释放真实描述防御系统的信号(简称真实防御信号)以及虚假的诱导性信号(简称虚假防御信号),能够影响和制约攻击者的情报判断和行动决策,起到威慑攻击者、诱导攻击行为、增加防御收益等作用. 因此,具备防御信号主动选择和释放机制的防御策略选取方法可以起到主动防御的作用.

借鉴动态博弈和信号博弈基本理论[16],定义防御者为信号博弈的领先者(Leader)和信号发送者,攻击者为跟随者(Follower)和信号接收者. 通过分析攻防博弈过程和防御信号作用机理,不同博弈阶段中双方的行动顺序和信号作用强度均会发生变化. (1)在起始阶段,①防御者通过防御信号对攻击者进行威慑、欺骗和诱导;②攻击者通过前期的探测行为和情报收集形成对防御者类型初始的先验概率判断,在防御信号的作用下,依据贝叶斯法则形成对防御类型的后验概率,并据此选择攻击策略;③防御者选取当前最优防御策略实施安全防御. (2)在下一阶段,①攻击者将上一阶段得到的防御类型后验概率作为本阶段的先验概率判断;②在防御信号的作用下,攻击者依据贝叶斯法则形成本阶段的防御类型后验概率,并据此选择攻击策略;③防御者选取本阶段的防御策略. (3)后续阶段攻防过程的分析可以同理类推,详细分析参见 3.2 节.

从信号作用的视角分析,随着攻防过程的进行,借助已发生的博弈过程和结果等信息,攻击者对防御者的了解逐渐清晰、准确,相比起始阶段,后续阶段中虚假防御信号的威慑、欺骗和诱导作用将会出现衰减. 根据信号博弈基本理论[16],本文在 2.2 节定义信号衰减因子 δ 表征虚假防御信号在不同博弈阶段的衰减程度,对博弈过程中 δ 作用的详细分析参见 3.2 和 3.3 节.

2.2 多阶段攻防信号博弈模型定义

定义 1 动态多阶段攻防信号博弈模型 G 可以表示为九元组 $G=(N,\Theta,M,\delta,S,P_A,\tilde{P}_A,T,U)$,其中

①$N=(N_D,N_A)$是局中人集合,N_D 代表防御者,为领先者;N_A 代表攻击者,为跟随者.

②$\Theta=(\Theta_D,\Theta_A)$是防御者与攻击者的类型空间. 防御者的类型属于私人信息,根据防御能力的不同,可分为若干类型,即 $\Theta_D=(\theta_i\mid i=1,2,\cdots,n)$;攻击者类型为 $\Theta_A=(\eta)$.

③M 表示防御信号空间,则 $M\neq\varnothing$,$M=(m_j\mid j=1,2,\cdots)$. 防御者依据设定的信号释放机制选择和释放信号,为便于表述,设信号名称与防御者类型名称一致. 出于威慑、欺骗和诱导攻击者的目的,防御信号和防御者类型不具有必然的一致性.

④T 是多阶段博弈的阶段数. $T=\{1,2,\cdots n\}$,当前阶段博弈过程用 $G(T)$表示.

⑤δ_T 是信号衰减因子,代表随着博弈阶段数 T 的增加,防御信号作用的衰减程度,$0\leqslant\delta_T\leqslant1$.

对于虚假防御信号,当 $T=1$ 时,$\delta_1=1$,即在第一阶段攻防博弈中,信号未发生衰减,此时虚假防御信号的威慑、欺骗和诱导作用最大;当 $1<T<n$ 时,$0<\delta_T<1$,且若 $T<T'$,则 $0<\delta_{T'}<\delta_T<1$,即随博弈进程推进,信号发生衰减且衰减程度递增,威慑、欺骗和诱导作用下降;当 $T=n$ 时,$\delta_n=0$,此时虚假防御信号对攻防博弈的影响消失,$G(T)$退化为不完全信息静态博弈. 对于真实防御信号,信号作用不衰减,特记为 $\delta(\delta\equiv1)$. 信号衰减因子在求解博弈均衡时直接影响后验概率计算,详见 3.1 节.

⑥$S=(D,A)$是防御者与攻击者的策略空间,$D=\{d_g\mid g=1,2,\cdots\}$和 $A=\{a_h\mid h=1,2,\cdots\}$分别表示防御策略和攻击策略.

⑦P_A 是攻击者对防御类型的先验概率判断,其中 $P_A=(p_A(\theta_1),p_A(\theta_2),\cdots,p_A(\theta_n))=(\gamma_1,\cdots,\gamma_n)$.

⑧$\tilde{P}_A$ 是攻击者的后验概率集合,$\tilde{P}_A=\tilde{P}_A(\theta_i\mid m_j)=(\mu_1,\cdots,\mu_n)$为攻击者观测防御信号 m_j 后,使用贝叶斯法则计算得到的防御者类型后验概率.

⑨$U=(U_D,U_A)$是防御者和攻击者的收益函数.

2.3　攻防策略收益量化和计算

文献[4,5,14]对攻击防御策略分类、策略成本/回报量化、策略收益计算的方法进行了研究和总结,但是都未对防御信号的作用进行量化,本节基于上述文献进行改进.

定义 2　攻击成本 AC(Attack Cost)、防御成本 DC(Defense Cost)以及攻击致命度 AL(Attack Lethality)、系统损失代价 SDC(System Damage Cost)的定义及计算方法参见文献[4,5,14].

定义 3　信号欺骗代价 SDE(Signal Deception Expense)表示网络攻防博弈中,防御者为隐瞒防御系统真实信息,释放虚假信号欺骗、诱导攻击者所耗费的代价. 若信号和真实防御类型一致,则 SDE 为零. 通过真实等级和虚假信号伪装的虚假等级之间的差距,对 SDE 进行相对量化,采用区间[0,100]内的整数值表达. 参考文献[16],对 SDE 进行分级和赋值.

参考文献[4,5,14]对攻防策略收益量化和计算方法加以改进,则攻击收益计算公式为:

$$U_A(m_j,d_g,a_h,\theta_i)=\sum_{g,h}\mathrm{SDC}(d_g,a_h)-\mathrm{AC}_h \tag{1}$$

防御收益为:

$$U_D(m_j,d_g,a_h,\theta_i)=\sum_{g,h}\mathrm{SDC}(d_g,a_h)-\mathrm{DC}_g-\mathrm{SDE} \tag{2}$$

属于同一等级的防御策略的效果基本一致,若共有 g 个防御策略,则可以假设防御者采用等概率 $\beta=\dfrac{1}{g}$ 选择第 g 个策略,得到平均防御收益 $U_D(\theta_j)$.

$$U_D(\theta_i)=\sum_{g=1}^{k}\beta\cdot U_D(m_j,d_g,A_h,\theta_i) \tag{3}$$

3　攻防博弈均衡求解及最优主动防御策略选取

根据 2.1 节的分析,不同博弈阶段中攻防双方的行动顺序及信号作用强度动态变化. 因此,本节首先提出攻防信号博弈的精炼贝叶斯均衡求解方法,然后分析多阶段攻防博弈的求解过程.

3.1　精炼贝叶斯均衡求解

定义 4　博弈模型 G 具有均衡 $EQ=(m^*(d^*,\theta),a^*(a_h,m),\tilde{P}_A(\theta\mid m))$[15],其中 $m^*(d^*,\theta)$为防御者的类型依存信号策略,表明防御者 θ 释放信号 m^* 且选择信号依存策略 $d^*(m^*)$,简记为 $m^*(\theta)$;$a^*(a_h,m)$为攻击者的信号依存策略,简记为 $a^*(m)$;$\tilde{P}_A(\theta\mid m)$为攻击者判断防御类型的后验概率,简记为 $\tilde{P}_A$. 上述均衡称为精炼贝叶斯均衡,简记为 $EQ=(m^*(\theta),a^*(m),\tilde{P}_A)$,满足下列条件:

(Ⅰ) $a^*(m)\in\arg\max\limits_{a\in A}\sum\tilde{P}(\theta\mid m)U_A(m^*(\theta),a,\theta)$;

(Ⅱ) $m^*(\theta)\in\arg\max\limits_{m\in M}U_D(m,a^*(m),d^*(m^*),\theta)$;

(Ⅲ) $\tilde{P}(\theta\mid m)$为攻击者基于先验概率 P、观测的信号 m 和攻击策略 $a^*(m)$,通过贝叶斯法则计算得到.

精炼贝叶斯均衡解的计算步骤如下:

(1)构造信号博弈树上不同信息集的后验推断$P(\theta\mid m)$.

(2)计算推断依存的最优攻击策略

当攻击者观察到信号 $m\in M$ 时,基于防御者类型 θ 的后验推断 $P(\theta\mid m)$,选择攻击最优策略 $a^*(m)$,使自己的博弈收益期望 U_A 取最大值,即通过计算

$$\max\sum P(\theta\mid m)U_A(m(\theta),a,\theta)$$

得到攻击者推断依存的最优策略 $a^*(m)$.

(3)计算推断依存的最优防御策略

防御者 θ 预见到攻击者会在观察自己释放的信号 m 的基础上,选择最优策略 $a^*(m)$,故选择最优防御策略 $m^*(\theta)$,使自己的博弈收益期望 U_D 取最大值,即通过计算

$$\max U_D(m,a^*(m),\theta)$$

得到防御者推断依存的最优策略 $m^*(\theta)$.

(4)计算精炼贝叶斯均衡解

通过 δ 表达信号作用的变化程度,直接作用于后验概率 $\tilde{P}_A(\theta)$ 的计算,即 $\tilde{P}_A(\theta)=\delta\tilde{P}_A(\theta|m)$. 其中,$\tilde{P}(\theta|m)$ 基于由(2)和(3)获得的最优推断依存策略 $a^*(m)$、$m^*(\theta)$ 以及先验概率 P_A,通过贝叶斯法则计算得到;如果 $\tilde{P}_A(\theta)$ 和 $P(\theta|m)$ 不冲突,则精炼贝叶斯均衡解为 $EQ=(m^*(\theta),a^*(m),\tilde{P}_A(\theta))$.

依据博弈理论,均衡解中的策略是双方的最优选择[17]. 因此,防御方应选取 $m^*(\theta)$ 作为最优防御策略. 精炼贝叶斯均衡解的具体计算过程可参考文献[18].

3.2 多阶段攻防博弈均衡求解过程

假设防御者类型 $\Theta_D=(\theta_H,\theta_M,\theta_L)=$(高防御等级,中防御等级,低防御等级). 防御信号空间为 $M=\{m_H,m_M,m_L\}$,信号名称与防御类型对应,防御策略空间为 $m^*(\theta)$. 攻击者类型 $\Theta_A=(\eta)$,攻击策略空间为 $A=(A_1,A_2,A_3)$,防御类型先验概率为 P_A,攻击和防御收益为 (U_A,U_D).

(1)当 $T=1$ 时,进入第一阶段攻防博弈 $G(1)$

自然(Nature)首先选择防御类型的概率依次为 $p_A(\theta_H)$、$p_A(\theta_M)$以及 $p_A(\theta_L)$. 攻击者观察到信号 m_H 后,修正其对防御类型的判断,认为防御类型为 $\{\theta_H,\theta_M,\theta_L\}$ 的后验概率是 $\{O_H^1,O_M^1,O_L^1\}$;同理,观察到 m_M 和 m_L 信号后,认为防御类型为 $\{\theta_H,\theta_M,\theta_L\}$ 的概率分别是 $\{G_H^1,G_M^1,G_L^1\}$、$\{K_H^1,K_M^1,K_L^1\}$. u_{ij} 表示具体收益值. 攻防信号博弈树 $G(1)$ 如图 1 所示.

此时,$\delta_1=1$. 基于 3.1 节的方法求解本阶段信号博弈的精炼贝叶斯均衡,记作 $EQ_1=(m^*(\theta),a^*(m),\tilde{P}_A(\theta))$,其中 $a^*(m)$ 和 $m^*(\theta)$ 为攻击者和防御的最优策略,$\tilde{P}_A(\theta)$ 是攻击者对防御类型的后验概率判断. 防御方在第一阶段应选取 $m^*(\theta)$ 作为最优防御策略.

当博弈 $G(1)$ 结束后,攻击者通过后验概率 $\tilde{P}_A(\theta)$ 修正了自身对防御类型的判断. 因此,当进入第二阶段攻防博弈后,攻击者会选择 EQ_1 中的 $\tilde{P}_A(\theta)$ 作为此时对防御类型的先验判断,自然(Nature)的作用被替代,博弈结构发生变化. 另一方面,通过分析、比较 $G(1)$ 的博弈过程和结果信息,攻击者会增强对虚假防御信号的分析和甄别能力,因此从第二阶段开始,$0<\delta_2<1$,信号衰减作用开始出现.

(2)当 $T=2$ 时,进入第二阶段攻防博弈 $G(2)$

攻击者利用 EQ_1 中 $\tilde{P}_A(\theta)$ 定义防御类型的先验判断,第二阶段攻防信号博弈树 $G(2)$ 如图 2 所示.

由于在该阶段信号衰减作用开始出现,设 $0<\delta_2<1$,则对于释放虚假防御信号的博弈路径上的后验概率 O_L^2,有 $O_L^2=\delta_2\tilde{P}(\theta_L|m_H)$,其余的 O_M^2、G_H^2、G_L^2、K_H^2、K_M^2 同理计算. 而对于释放真实防御信号的博弈路径上的后验概率 O_H^2,则有 $\hat{\delta}\equiv1$,故 $O_H^2=\hat{\delta}\tilde{P}(\theta_H|m_H)=\tilde{P}(\theta_H|m_H)$,$G_M^2$、$K_L^2$同理计算. 基于 3.1 节的方法可以得到第二阶段的精炼贝叶斯均衡,记作 EQ_2. 防御方在第二阶段应选取 EQ_2 中的 $m^*(\theta)$ 作为最优防御策略.

当博弈 $G(2)$ 结束后,攻击者同样利用后验概率 $EQ_2[\tilde{P}_A(\theta)]$ 再次修正对防御类型的判断,并将 $EQ_2[\tilde{P}_A(\theta)]$ 作为第三阶段的先验判断. 第三阶段时,$0<\delta_3<\delta_2$,虚假防御信号作用进一步衰减. 后续分析依此类推.

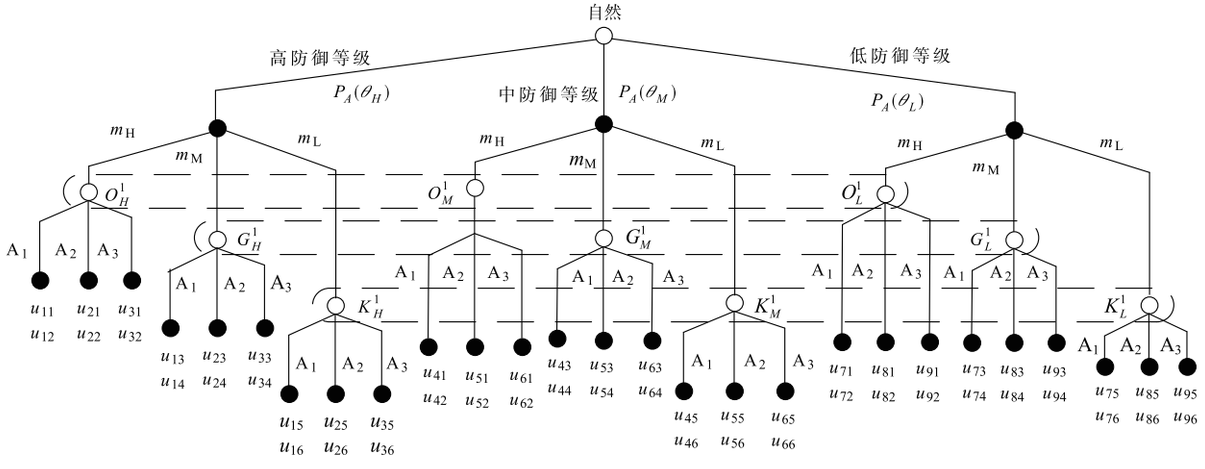

图1 攻防博弈树$G(1)$

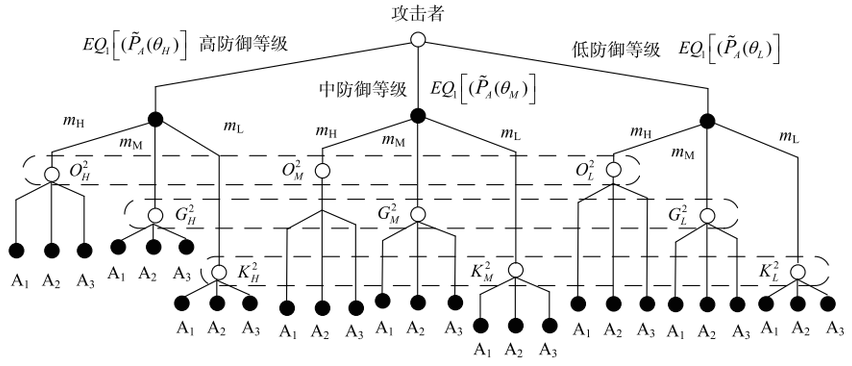

图2　攻防博弈树$G(2)$

(3)当 $T=n$ 时,进入第 n 阶段攻防博弈 $G(n)$

设第 n 阶段时,信号衰减因子 $\delta_n=0$,虚假防御信号的作用会消失,攻击者可以完全甄别虚假信号,而真实防御信号和真实防御类型构成对应关系,根据信号博弈基本理论,此时 $G(n)$ 退化为不完全信息静态博弈,得到如图 3 所示的博弈树.

在前 n-1 阶段,信号衰减因子 $\delta_n>0$,即各个阶段都是攻防信号博弈,博弈均衡解可通过 3.1 节中的方法求取. 博弈进行至第 n 阶段时,博弈结构退化为不完全信息静态博弈,基于线性规划的 Lebg-plex 求解算法[19]非常成熟,本文不再介绍.

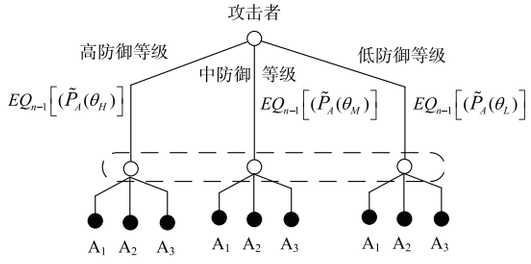

图3　攻防博弈树$G(n)$

3.3　多阶段最优主动防御策略选取算法及对比分析

在前文基础上,给出多阶段攻防博弈的最优主动防御策略选取算法.

算法 1　多阶段攻防博弈的最优主动防御策略选取算法

Input:多阶段攻防博弈模型 G
Output:各阶段最优防御策略
BEGIN
Initialize $(\boldsymbol{\Theta}_D=(\theta_1,\theta_2,\cdots,\theta_n))$;
//初始化防御类型空间
Initialize $(M=(m_1,\cdots,m_n),P_A=(p(\theta_1),\cdots,p(\theta_n)))$;
//初始化防御信号空间和类型先验概率
Initialize$(S=(D,A),D=\{d_1,\cdots,d_g\},A=\{a_1,\cdots,a_h\})$;
//初始化策略集
while $(a_h\in A\&\&m_j\in M\&\&d_g\in D)$//计算收益
{ $U_A(m_j,d_g,a_h,\theta_i)=\sum_{g,h}\mathrm{SDC}(d_g,a_h)-\mathrm{AC}_h$;
$U_D(m_j,d_g,a_h,\theta_i)=\sum_{g,h}\mathrm{SDC}(d_g,a_h)-\mathrm{DC}_g-\mathrm{SDE}$;}
for $(i=1;\ i\leqslant s;\ i++)$//$s$ 为博弈过程的阶段数
{
if $(\delta_T>0)$//信号博弈,求解精炼贝叶斯均衡
{$a^*(m)\in\arg\max_{a\in A}\sum\tilde{P}(\theta|m)U_A(m^*(\theta),a,\theta)$;
$m^*(\theta)\in\arg\max_{m\in M}U_D(m,a^*(m),d^*(m^*),\theta)$;
//计算最优攻击和防御策略
Bayesian$(\tilde{P}_A(\theta),\delta_T)$;//利用信号衰减因子和贝叶斯法则计算防御类型后验概率
Create $(m^*(\theta),a^*(m),\tilde{P}_A(\theta))$
//构建精炼贝叶斯均衡解 EQ
Output$(m_p^*(\theta))$;//输出本阶段最优防御策略
$P_A=\tilde{P}_A(\theta)$;//用防御类型后验概率更新先验概率
}
If$(\delta_T=0)$//退化为不完全信息静态博弈
{Lebg-plex(a^*,d^*) //用 Lebg-plex 算法计算博弈均衡解
Output(d^*); //输出本阶段最优防御策略
}
}
END

若博弈过程的阶段数为 s,防御类型数量为 n,max(攻击策略,防御策略)$=m$,则根据动态博弈基本理论[15],求解精炼贝叶斯均衡的平均时间复杂度为 $O(2n+2m^3)$,采用 Lebg-plex 算法计算不完全信息静态博弈均衡解的平均时间复杂度为 $O(m^3)$,因此本文算法的时间复杂度低于 $O(2s(n+m^3))$,存储空间主要用于收益和均衡计算的中间结果,为 $O(nm)$.

将本文提出的方法和其它文献进行对比,详见表 1. 博弈过程是指动态博弈模型是否具备分析多阶段攻防过程的能力,具备这一能力的模型更加符合实际要求,对防御决策的指导作用更强. 均衡求解是指文献中是否给出了均衡解的计算方法,由于动态博弈的求解相比静态博弈更加困难,尤其是动态多阶段博弈的求

解过程更为复杂,如果没有详细的求解方法会削弱实用性.

表 1 对比分析

研究文献	博弈类型	博弈者类型	模型扩展性	博弈过程	均衡求解
文献[7]	不完全信息静态	n	好	-	详细
文献[12]	不完全信息动态	3	一般	单阶段	无
文献[14]	不完全信息动态	3	一般	单阶段	简单
文献[17]	不完全信息动态	n	好	单阶段	一般
本文	不完全信息动态	n	好	多阶段	详细

4 仿真实验与分析

4.1 仿真实验环境

构建如图 4 所示的典型信息系统进行实验验证. 安全防御规则限制系统外主机(包括攻击者)的访问请求,规定只能访问网络服务器;应用服务器和网络服务器允许访问数据库服务器. 但是,借助于多步攻击过程,攻击者能够取得访问应用服务器和数据库服务器的权限[20,21].

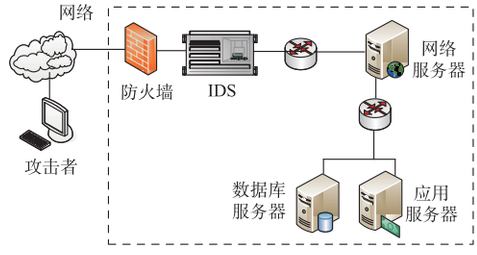

图4 实验系统结构

4.2 博弈收益计算

参考文献[16,22]给出原子攻击信息,如表 2 所示. 利用文献[4,5]的方法在分析路由文件、漏洞数据库、防御策略的基础上,获得可能的攻击策略为 $A_1\{a_1, a_4\}$,$A_2\{a_2, a_6\}$,根据历史数据分析,其操作代价 AC 分别为-580 和-310.

表 2 原子攻击动作描述

序号	原子攻击动作名称	类别	AL
a_1	Remote buffer overflow	User	6
a_2	Wu-Ftpd Sockprintf	User	7
a_3	LPC to LSASS process	User	7
a_4	Apache chunk overflow	Root	5
a_5	Steal account and crack it	Root	8
a_6	Oracle TNS Listener	Root	10

假设防御者类型 Θ_D = (高防御等级 θ_H,低防御等级 θ_L),对应信号空间 M = (高防御信号 m_H,低防御信号 m_L). 参考美国麻省理工大学的攻防行为数据库[23],综合各方面指标,防御策略如表 3 所示.

表 3 原子策略描述

原子防御动作	θ_H		θ_L	
	d_1	d_2	d_3	d_4
Limit packets from ports	√	√	√	
Install Oracle patches	√	√		
Reinstall Listener program	√			
Uninstall delete Trojan		√		
Limit access to MDSYS		√		√
Renew root data	√		√	
Restart Database server	√	√	√	√
Limit SYN/ICMP packets		√		
Add physical resource	√			√
Repair database	√	√	√	√
Correct homepage				
Delete suspicious account	√	√		

信号欺骗代价 SDE 分别为(SDE1,SDE2,SDE3) = (10,50,100). 不同防御等级选择各自策略的概率均为(0.5,0.5). 攻击者对防御类型的先验概率判断为 P_A = (0.6,0.4),基于文献[5,14]中的公式及本文公式(1)和(2)计算攻防策略的收益.

当防御类型为 θ_H,采用防御策略 d_1,发出防御信号 m_H;攻击策略为 A_1 时,

$$U_A = \sum_{g,h} \mathrm{SDC}(d_g, a_h) - \mathrm{AC}_h$$
$$= 10 \times 4 \times 20 + 10 \times 5 \times 30 - 580 = 1720$$

$$U_D(\theta_H, d_1) = \sum Dcost_{ij}(a_e) + Decost_{ij} + CC$$
$$= 10 \times 4 \times 20 + 10 \times 5 \times 30 - 260 = 2040$$

同理,当采用防御策略 d_2 时,则 U_A = 1720,$U_D(\theta_H, d_2)$ = 1990. 综上,该情况下 U_A = 1720,U_D = 0.5 × 2040 + 0.5 × 1990 = 2015. 基于同样方法,可求得其余博弈收益,形成博弈树如图 5 所示.

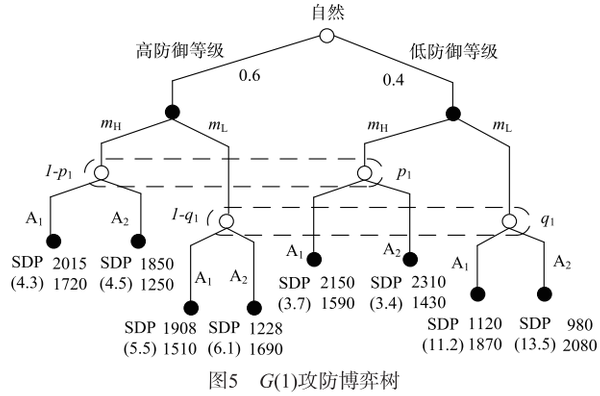

图5 $G(1)$攻防博弈树

借鉴文献[24]中分析 QoS 性能的方法,结合实验系统的实际情况,选择网页浏览、在线流视频和 FTP 文件下载等应用服务项目,采用平均服务延迟率 SDP(Service Delay Percent)量化不同防御策略造成的系统 QoS 下降. 实验中各项服务分别完成 20 次,取完成时间的平均值,与未发生攻防对抗时的平均完成时间对比,获得 SDP 值,如图 5 所示.

4.3　多阶段博弈均衡求解及防御策略选取

假设攻防对抗分为 3 个阶段,第 1 阶段信号衰减因子 $\delta_1=1$,第 2 阶段 $\delta_2=0.5$,第 3 阶段 $\delta_3=0$.

(1)第 1 阶段攻防博弈 G(1)

本阶段的信号攻防博弈树如图 5 所示.

计算可得在不同信息集上构造的后验推断为 $p_1^*=0.42, q_1^*=0.52$. 根据 3.1 节方法得到 G(1)可能的均衡解如下:

$p_1>p_1^*, q_1>q_1^*$ 时,精炼贝叶斯均衡 $EQ=[(m_H, m_H)\rightarrow(A_1, A_1), p_1=0.6, q_1=0.5]$,为混同均衡,记为 PE1.

$p_1>p_1^*, q_1<q_1^*$ 时,$EQ=[(m_H, m_H)\rightarrow(A_1, A_2), p_1=0.6, q_1=0.5]$,混同均衡,记为 PE2.

$p_1<p_1^*, q_1>q_1^*$ 时,$EQ=[(m_H, m_L)\rightarrow(A_2, A_1), p_1=1, q_1=0]$,分离均衡,记为 SE1.

$p_1<p_1^*, q_1<q_1^*$ 时,$EQ=[(m_L, m_L)\rightarrow(A_2, A_2), p_1=0.6, q_1=0.5]$,混同均衡,记为 PE3.

因此,当保证(p_1^*, q_1^*)和(p_1, q_1)不冲突时,得到 $G(1)$的精炼贝叶斯均衡为混同均衡 PE2. 表明防御者选择低防御等级,同时释放高防御信号,是最优防御策略. 说明防御者利用信号的作用展示了超出实际的防御能力,并以此对攻击者进行欺骗和诱导,降低了可能遭受的损失,发挥了主动防御的优势. 攻击者观测到信号 m_H 后,认为防御类型为(θ_H, θ_L)的后验概率是$(1-p_1, p_1)=(0.4, 0.6)$,说明攻击者对防御者的伪装和欺骗有察觉,推断其为低防御类型的概率提高.

(2)第 2 阶段攻防博弈 G(2)

攻击者在第 1 阶段得到防御类型后验概率判断(0.4,0.6),在 G(2)博弈中可用其定义防御类型的先验判断. 同时,攻击者借助第 1 阶段博弈过程和结果信息的反馈,增强了对虚假防御信号的甄别能力,故在本阶段信号衰减作用出现,取 $\delta_2=0.5$. 第 2 阶段的信号攻防博弈树如图 6 所示.

计算可得在不同信息集上构造的后验推断为 $p_2^*=0.58, q_2^*=0.46$. 得到 $G(2)$可能的均衡解如下:

$p_2>p_2^*, q_2>q_2^*$ 时,$EQ=[(m_H, m_H)\rightarrow(A_1, A_1), p_2=0.8, q_2=0.5]$,混同均衡,记为 PE4.

$p_2>p_2^*, q_2<q_2^*$ 时,$EQ=[(m_H, m_H)\rightarrow(A_1, A_2), p_2=0.8, q_2=0.5]$,混同均衡,记为 PE5.

$p_2<p_2^*, q_2>q_2^*$ 时,$EQ=[(m_H, m_L)\rightarrow(A_2, A_1), p_2=1, q_2=0]$,分离均衡,记为 SE2.

$p_2<p_2^*, q_2<q_2^*$ 时,$EQ=[(m_L, m_L)\rightarrow(A_2, A_2), p_2=0.8, q_2=0.5]$,混同均衡,记为 PE7.

当保证(p_2^*, q_2^*)和(p_2, q_2)不冲突时,得到 G(2)的精炼贝叶斯均衡为 $PE4$. 攻击者观测到信号 m_H 后,认为防御类型为(θ_H, θ_L)的后验概率是$(1-p_2, p_2)=(0.2, 0.8)$. 表明防御信号的欺骗和诱导作用下降,攻击者推断为低防御类型的概率进一步提高.

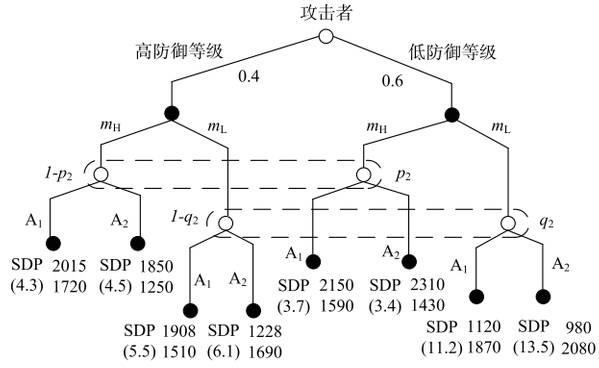

图6　$G(2)$攻防博弈树

(3)第 3 阶段攻防博弈 G(3)

信号衰减因子 $\delta_3=0$,虚假防御信号作用消失,G(3)退化为不完全信息静态博弈,博弈树如图 7.

利用 Lebg-plex 算法计算静态博弈的均衡,得到均衡策略为(D_1, A_2),此时最优防御策略为 D_1.

在上述三阶段攻防博弈中,第 1 阶段和第 2 阶段均为攻防信号博弈,虚假信号的作用不断下降,攻击者推断防御者是低防御等级的概率不断提升. 到第 3 阶段,攻击者能够完全甄别虚假信号,防御信号的作用消失,攻防博弈退化为不完全信息静态博弈.

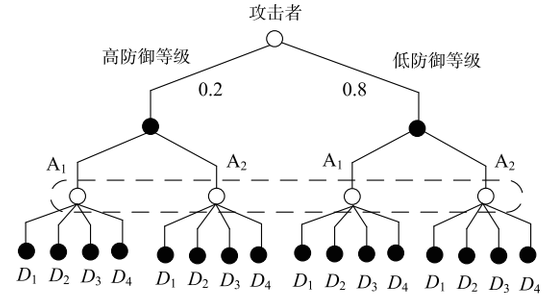

图7　$G(3)$攻防博弈树

4.4　实验分析

分析上述仿真实验,可以得出以下结论.

(1) 有效的防御信号选择和释放机制能提高主动防御能力,帮助防御者获得超出防御能力的防御效果.

在实验的前两个博弈阶段中,最优防御策略均为选择低防御等级并释放高防御信号. 采取该策略时,防御收益分别为(2310,2510),平均服务延迟率 SDP 分别为(3.4,3.7),在各项策略中均为最优. 表明利用防御信号可以达到欺骗攻击者的作用,诱导攻击者对防御类型的判断以及攻击策略的选择,提升防御收益. 可以在防御能力较低时,通过较小的投入获取超越能力的防御效果.

(2) 防御信号的作用在多阶段攻防过程中会迅速衰减,必须将防御信号选择和释放机制同其它防御手段配合使用. 在多阶段的攻防博弈过程中,随着博弈阶段数的增加,攻击者通过分析前序阶段的博弈过程和结果信息,能够增强对虚假防御信号的甄别能力. 在实验的前两个阶段,最优策略都是选择低防御等级并释放高防御信号,但是第 1 阶段的防御收益为 2310,而第 2 阶段为 2150,说明虚假防御信号的欺骗和诱导作用衰减,对防御收益的提升降低;同时,第 1 阶段攻击者对防御类型的后验推断为(0.4,0.6),第 2 阶段为(0.2,0.8),而第 3 阶段时,防御信号作用消失,攻防博弈退化为不完全信息静态博弈,攻击者确认防御类型的概率分布为(0.2,0.8). 因此,在攻防博弈中应认识到防御信号欺骗和诱导作用的有限性,将其作为应急防御手段,为调整防御系统和提升防御能力争取时间,通过和其它防御手段的配合使用共同增强防御效能.

(3) 加强投入,增强网络防御能力是规避重大安全损失的最优决策. 一方面,根据结论 2,防御信号欺骗和诱导的有效作用时间有限;另一方面,从综合分析各阶段的博弈收益和平均服务延迟率 SDP,则高防御类型的平均收益为 1750,平均 SDP 为 5.1;而低防御类型的平均收益为 1640,平均 SDP 为 8.8. 说明加大对安全防御的投入,提高防御能力,是面对网络攻击时降低预期损失的基础和关键.

5 结束语

博弈理论是研究网络安全主动防御的有效手段,但现有攻防博弈模型无法很好地刻画多阶段网络攻防场景. 为此,本文构建多阶段攻防信号博弈模型,通过分析防御信号作用的变化机理,提出信号衰减因子表征防御信号作用在不同博弈阶段的变化,并提出分析和求解多阶段博弈均衡解的方法,在此基础上,设计了多阶段最优防御策略选取方法,并利用仿真实例验证了所提出的模型和方法. 与现有研究成果相比,本文方法能够分析信息受限条件下的动态多阶段攻防过程,对网络安全主动防御决策的指导作用更加显著.

本文主要针对运用信号选择和释放方式的主动防御机制进行了研究,并未涉及其它防御机制,具有一定的局限性. 但是,提出的网络攻防模型对后续研究具有借鉴价值. 下一步将在此基础上,开展一般性攻防对抗的建模和分析,研究蜜罐网络、可信计算、拟态防御等安全机制的规律,探索包含多样化防御方式的安全防御决策方法.

参考文献

[1] Zhu Qiang, Li Fang-hua. Game theory of information security[J]. Chinese Journal of Electronics, 2015, 21(3): 1472 – 1486.

[2] Ocevcic H, Nenadic K, Solic K. Game theory: Active defense model and method[J]. IEEE Information and Network Security, 2015, 51(8): 395 – 406.

[3] Gordon L, Loeb M. Budgeting process for information security expenditures[J]. Communications of the ACM, 2015, 49(11): 121 – 125.

[4] WANG Yu-zhuo, YU Jian-ye, QIU Wen. Evolutionary game model and analysis methods for network group behavior[J]. Chinese Journal of Computers, 2015, 38(2): 282 – 300.

[5] JIANG Wei, FANG Bing-xing. Defense strategies selection based on attack-defense game model[J]. Journal of Computer Research and Development, 2014, 47(12): 714 – 723.

[6] White J, Park J S, Kamhoua C A, Kwiat K A. Game theoretic attack analysis in Online Social Network (OSN) services[A]. Proceedings of the 2014 International Conference on Social Networks Technology[C]. Los Angeles: IEEE, 2014. 1012 – 1019.

[7] WANG Jin-dong, YU Ding-kun, ZHANG Heng-wei. Active defense strategy selection based on static bayesian game[J]. Journal of Xidian University, 2016, 43(1): 144 – 151.

[8] LIU Yu-ling, FENG Deng-guo. Worm attack-defense strategy based on static bayesian game[J]. Journal of Software, 2014, 23(12): 712 – 723.

[9] Burke D. Towards a game theory model of information warfare[D]. Montgomery, AL: Air force Institute of Technology, Air University, 2015.

[10] Wang Chun-lei, Miao Qing, Dai Yi-qi. Network survivability analysis based on stochastic game model[J]. Multimedia Information Networking and Security, 2014, 55(10): 199 – 204.

[11] Yu Min, Liu Chao, Qiu Xin-liang, Zhao Shuang. Modelling and analysis of phishing attack using Stochastic Game[J]. Cyberspace Technology, 2015, 46(3): 300 – 305.

[12] LIN Wang-qun, WANG Hui, LIU Jia-hong. Research on active defense technology in network security based on non-cooperative dynamic game theory[J]. Journal of Computer Research and Development, 2014, 48(11): 306

-316.

[13] Filler T, Judas J, Fridrich J. Signaling game model: DDOS defense analysis [J]. Journal of Security Engineering, 2015, 39(3): 414-417.

[14] ZHANG Hengwei, Han Ji-hong, Yu Ding-kun. Defense policies selection method based on attack-defense signaling game model[J]. Journal on Communications, 2016, 37(5): 39-49.

[15] Steven Tadelis. Game Theory: An Introduction[M]. Princeton: Princeton University Press, 2014.

[16] Richard Lippmann, Joshua W. Haines. Analysis and results of the DARPA off-line intrusion detection evaluation [A]. Proceedings of the 17'th International Workshop on Recent Advances in Intrusion Detection[C]. New York: ACM, 2014. 162-182.

[17] Zhu Jian-min, Song Biao, Huag Qi-fa. Evolution game model of of fense-defense for network security based on system dynamics[J]. Journal on Communications, 2015, 35(1): 54-61.

[18] ZHANG Hengwei, LI Tao, WANG Jindong. Optimal active defense using dynamic multi-stage signaling game [J]. China Communications, 2015, 12(2): 114-122.

[19] Thomas H. Cormen, Charles E. Leisers on, Ronald L. Rivest. Introduction to Algorithms [M]. Boston: MIT Press, 2009.

[20] 高志伟,姚尧,饶飞. 基于漏洞严重程度分类的漏洞预测模型[J]. 电子学报,2014,42(9):1285-1287.
GAO Zhi-wei, YAO Yao, RAO Fei. Predicting model of vulnerabilities based on the type of vulnerability severity [J]. Acta Electronica Sinica, 2014, 42(9): 1785-1787. (in Chinese)

[21] 刘奇旭,张翀斌,张玉清. 安全漏洞等级划分关键技术研究[J]. 电子学报,2015,43(1):1779-1785.
LIU Qi-xu, ZHANG Chong-bin, ZHANG Yu-qing. Research on key technology of vulnerability threat classification[J]. Acta Electronica Sinica, 2015, 43(1): 1779-1785. (in Chinese)

[22] CVSS. Common Vulnerability Scoring System[DB/OL]. http://www.cve.mitre.org/, 2014-09-17.

[23] Gordon L, Loeb M, Lucyshyn W, Richardson R. 2015 CSI/FBI computer crime and security survey[A]. Proceedings of the 2014 Computer Security Institute[C]. San Francisco: IEEE, 2015. 48-64.

[24] SI Pengbo, ZHANG Qian, F. Richard. QoS aware dynamic resource management in heterogeneous cloud computing networks[J]. China Communications, 2014, 41(5): 144-159.

作者简介

张恒巍　男,1978 年出生,河南洛阳人,博士,信息工程大学讲师,研究方向为网络安全行为分析、信息安全风险评估.
E-mail: zhw11qd@126.com

李　涛　男,1992 年出生,甘肃甘谷人,信息工程大学硕士研究生,研究方向为网络安全主动防御.