doi :10 .3969/j .issn .1001-2400 .2016 .01 .026

静态贝叶斯博弈主动防御策略选取方法

王晋东,余定坤,张恒巍,王 娜
(解放军信息工程大学密码工程学院,河南 郑州 450000)

摘要:由于不完全信息博弈最优防御策略选取方法仅考虑攻击者的类型,未考虑防御者类型,策略选取可操作性差,故提出了一种基于静态贝叶斯博弈的最优防御策略选取方法,构建了静态贝叶斯博弈模型,将攻击者和防御者分为多种类型.认为攻击者混合策略是防御者对攻击者可能采取行动的可信预测,对防御策略效能进行计算,并给出了最优主动防御策略选取算法,使策略选取可操作性更强.

关键词:静态贝叶斯;主动防御;混合策略均衡;网络安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1001-2400(2016)01-0144-07

Active defense strategy selection based on the static Bayesian game

WANG Jindong, YU Dingkun, ZHANG Hengwei, WANG Na
(Information Engineering University, Zhengzhou 450000, China)

Abstract: Nowadays, the optimal defense strategies selection based on the incomplete information game model has many disadvantages, such as ignoring the type of the defender, using the simple cost quantitative method, and choosing defense strategies improperly. To solve the problem, this paper proposes an active defense strategy selection based on the static Bayesian game theory, and constructs the static Bayesian game model. The model considers the types of the attacker and the defender, and improves the classical strategies taxonomy and cost quantitative method by considering the strike back act of the defender and the success attack rate. Then, this paper calculates and comprehensively analyzes the Bayesian equilibrium of the game. Taking mixed strategies Bayesian equilibrium of the attacker as the defender's prediction of the attacker's action, this paper calculates the defense effectiveness of defense strategies and performs a defense strategies selection algorithm. Finally, an example is provided to analyze and demonstrate the effectiveness of the model and algorithm.

Key Words: static Bayesian; active defense; mixed strategies equilibrium; network security

在网络安全防御中,采取合适的防御策略十分重要.而防御策略是否有效,不仅仅取决于防御者,攻击者和防御者策略具有互相依存性.在理想状态下,防御者应对系统面临的所有攻击都进行防护,这显然是不可能的,防御者应选取合理的防御策略来科学地把握防御成本与防御收益之间的平衡性.博弈论[1]与网络对抗行为有着天然的密切联系,能够充分地考虑攻击者和防御者策略的依存性及成本与收益之间的平衡性.正因如此,Liang 等[2]指出,博弈理论方法已在网络对抗领域发挥重要作用,是未来网络安全很有前途的研究方向.

姜伟等[3]将网络攻击者和防御者相互博弈的过程看成一种两角色博弈,建立了一个攻防博弈模型,并给出了零和及非合作零和博弈算法,不足之处在于使用完全信息静态博弈模型,与网络实际场景不够贴近.姜伟等[4-6]提出了攻防随机博弈模型,对网络攻防状态的动态变化进行建模,并应用于防御策略选取等方面,不足之处在于状态转移概率函数不易确定.林旺群等[7]将动态博弈模型引入网络主动防御中,通过"虚拟节点"

收稿日期:2014-10-01 **网络出版时间**:2015-04-14
基金项目:国家自然科学基金资助项目(61303074,61309013);国家重点基础研究发展计划("973"计划)资助项目(2012CB315900)
作者简介:王晋东(1966—),男,教授,E-mail:gzydk2@163.com.
网络出版地址:http://www.cnki.net/kcms/detail/61.1076.TN.20150414.2046.026.html

将网络攻防图转化为网络博弈树,存在的问题在于基于完全信息假设,且未充分地考虑策略收益量化问题.刘玉岭等[8]将不完全信息静态博弈模型运用于蠕虫策略绩效评估方面,存在的问题是未考虑防御者有多种类型的情况,且仅对纯策略贝叶斯均衡进行了分析.Nguyen 等[9]建立了不完全信息静态博弈模型对传感器网络安全防御进行分析,存在的问题是模型未对攻击者类型进行划分,攻防策略简单,且策略收益量化仅为假设,未结合网络的实际情况.Liu 等[10]运用基于动机的方法建立了 AIOS 模型,并运用不完全信息静态博弈来推理该模型,存在的问题是收益量化基于假设而非网络具体情况,且攻击者类型分类简单,仅分为好与坏.Liu 等[11]运用不完全信息博弈对无线 Ad Hoc 网络发生的攻击行为进行分析,存在的问题是未对攻击者详细分类,收益量化简单,且仅对均衡存在的情况进行讨论,并未赋予均衡实际意义.

目前基于博弈模型的最优防御策略选取方法多采用完全信息假设,不贴近网络实际情况,使用场合受限,实用性不强.而基于不完全信息博弈的网络安全防御,多数没有或只简单考虑攻击者的类型,未划分防御者的类型,策略收益量化简单,未结合网络的实际状况.另外,在策略选取时,仅给出混合策略,对防御策略进行选取操作性不强.针对以上问题,笔者的贡献如下:①建立了基于静态贝叶斯博弈的主动防御模型,考虑了多种防御者类型,并全面详细地分析了博弈的混合策略贝叶斯均衡;②提出了基于防御效能的最优策略选取方法,将攻击者混合策略均衡概率分布看成防御者对攻击者可能采取行动的可信预测;③通过防御者对攻击者可能采取行动的可信预测计算防御策略效能,并给出了最优防御策略选取算法,指导防御者进行策略选取.

1　静态贝叶斯博弈主动防御模型

静态贝叶斯博弈是不完全信息同时行动的博弈,其中同时行动是指所有参与者同时选择自己的行动或者是后行动者不知道先行动者采取了什么行动.不完全信息指在博弈时至少有一个参与者不能确定其他参与者的收益函数,参与者的收益函数对应着该参与者的类型.

1.1　模型假设

假设 1　理性假设.假设攻击者和防御者是完全理性的,攻击者不会发动无利可图的攻击,防御者不会不计代价地进行防御.

假设 2　收益假设.攻击者与防御者的目标分别是获取和保护自己的信息资源,因此对于双方收益的各个方面的衡量可依据信息资源的经济价值作为依据.

1.2　模型相关定义

定义 1　静态贝叶斯博弈主动防御模型(Static Bayesian Game Active Defense Model,SBG-ADM)是一个五元组,即 $A_{\text{SBG-ADM}}=(N, T, M, P, U)$,其中:

(1) $N=(N_1, N_2, \cdots, N_n)$,是博弈的参与者集合.参与者是参与博弈的独立决策、独立承担结果的个人或组织,在不同的场合中,参与者的定义是不同的.在本文中,参与者是攻击者和防御者.

(2) $T=(T_1, T_2, \cdots, T_n)$,是参与者的类型集合.$\forall i \in n, T_i \neq \varnothing, T_i=(t_1^i, t_2^i, \cdots, t_k^i)$,表示参与者 P_i 的类型集合,每个参与者都应有 1 种以上的类型,即 $k \geqslant 1$.

(3) $M=(M_1, M_2, \cdots, M_n)$,是参与者的行动集合.$\forall i \in n, M_i \neq \varnothing, M_i=(m_1^i, m_2^i, \cdots, m_h^i)$,表示参与者 N_i 的行动集合,每个参与者都应有 1 种以上的行动,即 $h \geqslant 1$.

(4) $P=(P_1, P_2, \cdots, P_n)$,是参与者的先验信念集合.$P_i=P_i(t_{-i} \mid t_i)$,表示参与者 i 在自己实际类型为 t_i 的前提下,对其他参与者类型(若有多个参与者时为类型组合)t_{-i} 的判断.

(5) $U=(U_1, U_2, \cdots, U_n)$,是参与者的收益函数集合.收益函数表示参与者从博弈中可以得到的收益水平,由所有参与者的策略共同决定,参与者不同的策略组合所得到的收益不同.

以上给出了 $A_{\text{SBG-ADM}}$ 的通用模型.为了简化分析,只考虑 $n=2$ 的情况,即 $A_{\text{SBG-ADM}}=\{(N_A, N_D), (T_A, T_D), (M_A, M_D), (P_A, P_D), (U_A, U_D)\}$.其中 N_A 表示攻击者,N_D 表示防御者.攻击者 N_A 类型 T_A 为 $t_A=(t_1^A, t_2^A, \cdots, t_{k_1}^A)$,防御者 N_D 类型 T_D 为 $t_D=(t_1^D, t_2^D, \cdots, t_{k_2}^D)$.文献[11]认为防御者类型为攻击者和防御者的共有信息,即只有一种类型,这并不符合实际.虽然防御者清楚自己的收益情况,但攻击者想通过刺探、收集得到

防御者的全部信息是非常困难的,且信息真实性不能保证,防御者信息对攻击者来说也是不完全的.因此,对攻击者来说,防御者也可根据其收益分为多种类型.一般来说,攻击者的行动集合为其攻击手段集合,$M_A=(m_1^A,m_2^A,\cdots,m_{h_1}^A)$;防御者的行动集合为其防御手段集合,$M_D=(m_1^D,m_2^D,\cdots,m_{h_2}^D)$.$P_A(t_D\mid t_A)$指攻击者的类型为 t_A 时,其对防御者类型 t_D 的一个概率判断;$P_D(t_A\mid t_D)$指防御者类型为 t_D 时,其对攻击者类型 t_A 的一个概率判断.$\forall m_A\in M_A$,$m_D\in M_D$,$t_A\in T_A$,$t_D\in T_D$,$U_A(m_A,m_D,t_A)$表示防御者采用行动 m_D 抵御攻击者的攻击行动 m_A 且攻击者类型为 t_A 时,攻击者的收益;$U_D(m_A,m_D,t_D)$表示防御者采用行动 m_D 抵御攻击者的攻击行动 m_A 且防御者类型为 t_D 时,防御者的收益.

2 博弈均衡分析

在不完全信息的条件下,纯策略贝叶斯纳什均衡表示了攻击者和防御者的最优对策.利用以上定义即可以对静态贝叶斯博弈模型的所有纯策略纳什均衡进行计算.但是,由于博弈的内禀属性,纯策略贝叶斯纳什均衡不可能总是存在的.因此,需要对博弈的混合策略贝叶斯纳什均衡进行分析和存在性证明.

定义 2 混合策略贝叶斯纳什均衡(MSBNE).给定 $A_{\text{SBG-ADM}}=\{(N_A,N_D),(T_A,T_D),(M_A,M_D),(P_A,P_D),(U_A,U_D)\}$,攻击者和防御者的混合策略分别是概率分布 $F_A(t_A)=\{f_1^A(t_A),f_2^A(t_A),\cdots,f_{n_1}^A(t_A)\}$ 和 $F_D(t_D)=\{f_1^D(t_D),f_2^D(t_D),\cdots,f_{n_2}^D(t_D)\}$.若满足 $\sum_{t_D\in T_D}P_A(t_D\mid t_A)U_A(F_A^*(t_A),F_D^*(t_D),t_A)\geqslant\sum_{t_D\in T_D}P_A(t_D\mid t_A)U_A(F_A(t_A),F_D^*(t_D),t_A)$ 和 $\sum_{t_A\in T_A}P_D(t_A\mid t_D)U_D(F_A^*(t_A),F_D^*(t_D),t_D)\geqslant\sum_{t_A\in T_A}P_D(t_A\mid t_D)U_D(F_A^*(t_A),F_D(t_D),t_D)$,则称混合策略 $\{F_A^*(t_A),F_D^*(t_D)\}$ 是贝叶斯纳什均衡.

定理 1 贝叶斯纳什均衡存在性.给定 $A_{\text{SBG-ADM}}=\{(N_A,N_D),(T_A,T_D),(M_A,M_D),(P_A,P_D),(U_A,U_D)\}$,如果攻击者和防御者策略集 $S_A(t_A)$ 和 $S_D(t_D)$ 是有限集合,则此博弈模型存在一个混合策略贝叶斯纳什均衡.

证明 因为 $A_{\text{SBG-ADM}}$ 中攻击者和防御者类型集合 T_A 和 T_D,行动集合 M_A 和 M_D,收益值 U_A 和 U_D,策略集 $S_A(t_A)$ 和 $S_D(t_D)$ 都是有限的,所以,$A_{\text{SBG-ADM}}=\{(N_A,N_D),(T_A,T_D),(M_A,M_D),(P_A,P_D),(U_A,U_D)\}$,是一个有限博弈.研究证明,每一个有限博弈都存在一个纯策略或混合策略的贝叶斯纳什均衡,且由于纯策略贝叶斯纳什均衡是混合策略贝叶斯纳什均衡的特例,所以此博弈模型存在一个混合策略贝叶斯纳什均衡.

笔者提出的方法基于博弈理论,防御者综合考虑攻击者的行为进行收益量化、博弈分析,考虑更加全面,所得结果更加科学合理.笔者提出的博弈模型及后续博弈分析都是基于上述模型假设的.由上可知,攻击预测模型总是存在一组混合策略 $F_A^*(t_A)=\{f_1^{A*}(t_A),f_2^{A*}(t_A),\cdots,f_{n_1}^{A*}(t_A)\}$ 和 $F_D^*(t_D)=\{f_1^{D*}(t_D),f_2^{D*}(t_D),\cdots,f_{n_2}^{D*}(t_D)\}$,相比其他混合策略,能使攻击者和防御者收益最大.在不清楚对方策略的情况下,在可预见的未来双方都会倾向于选择这一组混合策略.文献[3,12]采用混合策略中 $F_D^*(t_D)$ 指导防御者进行防御策略选取,防御者分别以 $f_1^D(t_D),f_2^D(t_D),\cdots,f_{n_2}^D(t_D)$ 的概率选择各防御策略.但由于防御者一次只能选择一种防御策略,以概率形式给出的策略选取方案对于用户来说是不好理解和实施的.因此,笔者采用混合策略中的概率分布 $F_A^*(t_A)=\{f_1^{A*}(t_A),f_2^{A*}(t_A),\cdots,f_{n_1}^{A*}(t_A)\}$,作为防御者对攻击者各种行为在理性假设下的预测,在此基础上计算防御策略的防御效能,为选取防御策略提供依据.

3 最优防御策略选取

3.1 最优防御策略的选取方法

防御策略选取是一个非常复杂的过程,需要在双方并不完全知道对方信息的情况下综合考虑攻击者的攻击行动及防御者的防御行动的成本和代价.基于静态贝叶斯博弈进行最优策略选取可以很好地处理这一

类的问题.

将策略成本和收益进行量化后构建攻防博弈树,并将其输入 $A_{\text{SBG-ADM}}$,计算可得到混合策略贝叶斯纳什均衡$\left(F_A^*(t_A),F_D^*(t_D)\right)$.由上可知,由于防御者一次只能选择一种防御策略,传统博弈以概率形式给出的策略选取方案对于用户来说是不好理解和实施的.笔者提出了一种基于防御效能的最优防御策略选取方法,通过对攻击者采取各种行为的可信预测来计算防御策略的防御效能.

由上可知,在一个网络博弈场景中,防御者在理性假设下对攻击者的各种行为进行预测,这个预测结果就为混合策略中的概率分布 $F_A^*(t_A)=\left\{f_1^{A*}(t_A),f_2^{A*}(t_A),\cdots,f_{n_1}^{A*}(t_A)\right\}$.可以通过各类型防御者的先验概率及收益函数得到该博弈场景下防御者防御策略 $s_j^D(t_D)$ 的效能期望:

$$E_D\left(s_j^D(t_D)\right)=\sum_{t_A}P(t_A\mid t_D)\sum_i U_D\left(m_i^A,s_j^D(t_D),t_A\right)F_A^*(t_A)\quad .\tag{1}$$

将防御者所有防御策略 $s_j^D(t_D)\in S_D(t_D)$ 的防御效能期望进行求解后,则可以将各个防御策略按照防御效能的高低进行排序,防御者可按照效能从高到低的顺序对最优防御策略进行选择.

3.2　相关工作比较

如表 1 所示,文献[8-10]采用不完全信息静态博弈.相比它们,笔者考虑了防御者的类型,收益量化详细,可操作性好.收益量化是指文献给出的方法对攻防双方收益量化是否结合网络实际,且步骤详细、可行,部分文献中收益量化仅通过作者假设得出,简单但可行性差.可操作性是指文献给出的方法或算法为用户所选取的最佳防御策略是否具有较强的实用性.攻击者和防御者一次只能选取一种攻击或防御策略,相比以混合策略形式给出的策略选取方案,通过策略效能计算,以纯策略形式给出的策略选取方案具有更好的可操作性,较差则表示文献未给出具体策略选取方案.

表 1　相关工作比较

文献	信息需求	攻击者类型	防御者类型	可操作性	时间复杂度
文献[3]	完全信息	1	1	一般	Polynomial Time; PPAD-Complete
文献[8]	不完全信息	k_1	1	一般	$O\left(\lvert S_A(t_A)\rvert\lvert S_D(t_D)\rvert\lvert T_A\rvert\right)$
文献[9]	不完全信息	1	1	较差	$O\left(\lvert S_A(t_A)\rvert\lvert S_D(t_D)\rvert\right)$
文献[10]	不完全信息	2	1	一般	文献未给出算法
本文	不完全信息	k_1	k_2	较好	$O\left(\lvert S_A(t_A)\rvert\lvert S_D(t_D)\rvert\lvert T_A\rvert\lvert T_D\rvert\right)$; PPAD-Incomplete

4　应用实例与分析

通过部署如文献[7]所示的网络信息系统拓扑结构进行模拟实验.

根据攻击者的历史行为,防御者可将攻击者的类型划为 T_A,$t_A=\{$冒险型攻击者,保守型攻击者$\}$.本实例设定防御者的类型为 T_B,$t_B=\{$一级防御,二级防御,三级防御$\}$.冒险型攻击者为了达到目的不惜采用高代价攻击方式,成功率较高,具有较大风险;保守型攻击者攻击时更愿意使用代价较小的方式实施攻击,成功率较低,风险也较低.防御者自一级防御到三级防御,力度越来越小,消耗越来越小.服务器弱点信息请见文献[7].

由于弱点间存在相互依赖的关系,攻击者可以通过一系列的原子攻击来获得访问数据库的权限.攻击者的原子攻击信息请见参考文献[13].参考 MIT 林肯实验室攻防分类,对网络拓扑进行分析可得到不同类型攻击者采取的各类攻击行动,如表 2 所示.

表 2　不同类型攻击者行动

攻击者类型	攻击行动	攻击者类型	攻击行动
冒险型攻击者	$m_1^A:\{a_9,a_6,a_2\}$	保守型攻击者	$m_4^A:\{a_5,a_{10}\}$
	$m_2^A:\{a_{10},a_5,a_8\}$		$m_5^A:\{a_{14},a_{11},a_6\}$
	$m_3^A:\{a_7,a_1\}$		$m_6^A:\{a_{13},a_5\}$

防御者选取的防御策略常常是各项防御措施的集合,不同类型的防御者选取的行动是不相同的.从防御行为库选出可用的防御行动后,经过对成本、影响及专家建议等方面的考虑,不同类型可供选取的防御行动如表 3 所示.

表 3 不同类型防御者行动

防御策略	防御者								
	一级防御			二级防御			三级防御		
	m_1^D	m_2^D	m_3^D	m_4^D	m_5^D	m_6^D	m_7^D	m_8^D	m_9^D
Limit packets from ports	√				√		√	√	
Install 0547 patches		√	√		√		√		√
Reinstall Listener program	√		√	√		√		√	√
Unistall delete Trojan						√	√		
Limit access to MDSYS .SDO_CS			√	√					√
Renew data	√	√						√	
Restart server				√	√	√		√	√
Limit SYN/ICMP packets	√	√		√	√				
Add physical resource									
Repair database		√	√		√		√		
Correct homepage		√					√	√	√
Delete suspicious account			√	√		√			

参与者行动集合确定后,利用文献[3]的策略收益量化方法对各类型的参与者行动的成本和收益进行量化.另外,通过对历史数据的分析,防御者可得到攻击者类型的先验信念:(冒险型攻击者,保守型攻击者)=(0.6,0.4);防御者对攻击者历史行为进行分析,可得到攻击者对其类型的先验信念:(一级防御,二级防御,三级防御)=(0.3,0.4,0.3).由于攻击者类型有 2 种,防御者类型有 3 种,因此需要进行 2 次海萨尼转换.由此可得到网络博弈树如图 1 所示.

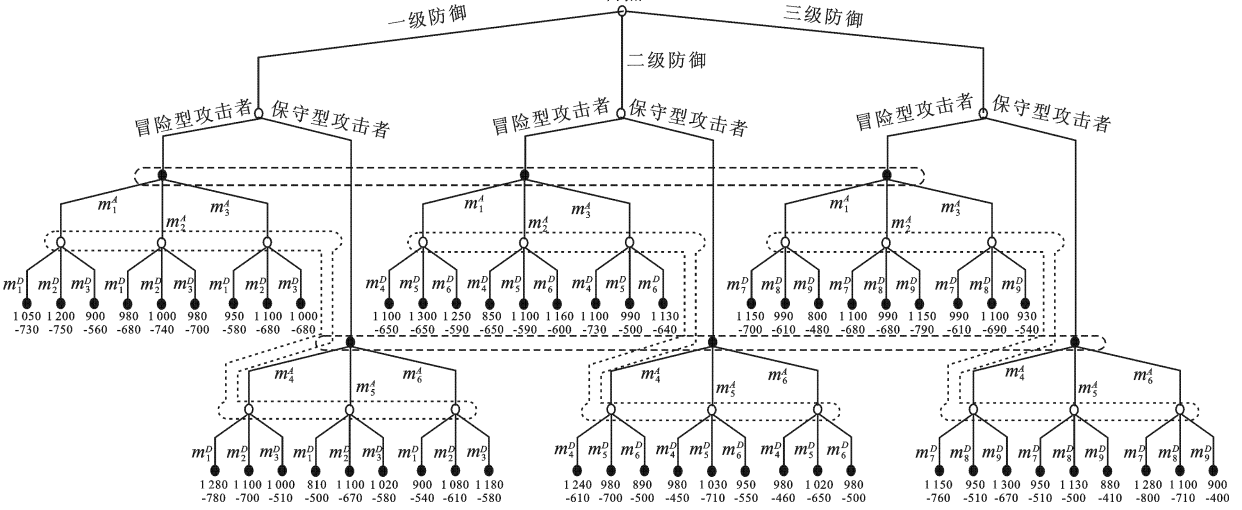

图 1 网络博弈树

利用最优防御策略选取算法可得到均衡如下:冒险型攻击者的混合策略均衡为$\{f_1^{A*}(t_A), f_2^{A*}(t_A), f_3^{A*}(t_A)\}=\{0, 0.3417, 0.6583\}$;保守型攻击者的混合策略均衡为$\{f_4^{A*}(t_A), f_5^{A*}(t_A), f_6^{A*}(t_A)\}=\{0.8547, 0, 0.1453\}$;一级防御的混合策略均衡为$\{f_1^{D*}(t_D), f_2^{D*}(t_D), f_3^{D*}(t_D)\}=\{0,0,1\}$;二级防御的混合策略均衡为$\{f_4^{D*}(t_D), f_5^{D*}(t_D), f_6^{D*}(t_D)\}=\{0, 0.0750, 0.9250\}$;三级防御的混合策略均衡为$\{f_7^{D*}(t_D), f_8^{D*}(t_D), f_9^{D*}(t_D)\}=\{0, 0.1909, 0.8091\}$.

之后利用算法通过式(1)计算各防御策略的防御效能:$\left(E_D(s_1^D(t_D)),E_D(s_2^D(t_D)),E_D(s_3^D(t_D)),E_D(s_4^D(t_D)),E_D(s_5^D(t_D)),E_D(s_6^D(t_D)),E_D(s_7^D(t_D)),E_D(s_8^D(t_D)),E_D(s_9^D(t_D))\right)=$ (−666.553 2, −695.070 4, −620.168 8, −656.880 4, −595.545 8, −595.548 2, −686.676 2, −627.573 8, −627.562 6). 按大小排列为:$\left(E_D(s_5^D(t_D)),E_D(s_6^D(t_D)),E_D(s_3^D(t_D)),E_D(s_9^D(t_D)),E_D(s_8^D(t_D)),E_D(s_1^D(t_D)),E_D(s_4^D(t_D)),E_D(s_7^D(t_D)),E_D(s_2^D(t_D))\right)$. 由上可知,防御策略 $s_5^D(t_D)$ 的防御效能最大. 在实际应用中,在资源受限的前提下,可按照效能排序优先选取靠前的策略,所以防御者的最优防御策略是策略 $s_5^D(t_D)$:选择二级防御中的防御行动 m_5^D.

5　结束语

为帮助、指导防御者进行防御策略的选取,笔者提出了静态贝叶斯博弈主动防御模型,并对该模型进行了详细的形式化定义. 该模型将攻击者和防御者划分为多种类型,对博弈的均衡情况进行了分析和证明. 笔者认为攻击者的混合策略概率分布是防御者对攻击者可能采取行动的可信预测,对各个防御策略的防御效能进行了计算. 笔者还提出了基于静态贝叶斯的主动防御策略选取算法,可用于指导防御者采取最优防御策略进行主动防御. 实例分析说明了笔者提出的模型和算法在攻击预测及主动防御策略选取方面的合理性和有效性.

参考文献:

[1] ZONOUZ S A, KHURANA H, SANDERS W H. RRE: A Game-theoretic Intrusion Response and Recovery Engine [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 395-406.

[2] LIANG X N, XIAO Y. Game Theory for Network Security [J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 472-486.

[3] 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): 817-825.
JIANG Wei, FANG Bingxing, TIAN Zhihong, et al. Evaluating Network Security and Optimal Active Defense Based on Attack-defense Game Model [J]. Chinese Journal of Computers, 2009, 32(4): 817-825.

[4] 姜伟,方滨兴,田志宏,等. 基于攻防随机博弈模型的防御策略选取研究[J]. 计算机研究与发展, 2010, 47(10): 1714-1723.
JIANG Wei, FANG Bingxing, TIAN Zhihong, et al. Research on Defense Strategies Selection Based on Attack-defense Stochastic Game Model [J]. Journal of Computer Research and Development, 2010, 47(10): 1714-1723.

[5] YU M, LIU C, QIU X L, et al. Modelling and Analysis of Phishing Attack Using Stochastic Game Nets[C]// International Conference on Cyberspace Technology. London: IET, 2013: 300-305.

[6] WANG C L, MIAO Q, DAI Y Q. Network Survivability Analysis Based on Stochastic Game Model[C]//Proceedings of the 4th International Conference on Multimedia Information Networking and Security. Washington: IEEE Computer Society, 2012: 99-104.

[7] 林旺群,王慧,刘佳宏,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.
LIN Wangqun, WANG Hui, LIU Jiahong 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.

[8] 刘玉岭,冯登国,吴丽惠,等. 基于静态贝叶斯博弈的蠕虫攻防策略绩效评估[J]. 软件学报, 2012, 23(3): 712-723.
LIU Yuling, FENG Dengguo, WU Lihui, et al. Performance Evaluation of Worm Attack and Defense Strategies Based on Static Bayesian Game [J]. Journal of Software, 2012, 23(3): 712-723.

[9] NGUYEN K C, ALPCAN T, BASAR T. Security Games with Incomplete Information[C]// 2009 IEEE International Conference on Communications. Piscataway: IEEE, 2009: 5199443.

[10] LIU P, ZANG W Y, YU M. Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies[J].

ACM Transactions on Information and System Security , 2005 , 8(1) : 78-118 .

[11] LIU Y , COMANICIU C , MAN H . A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks [C]//Proceedings of the 2006 Workshop on Game Theory for Communications and Networks . New York : ACM , 2006 : 1190198 .

[12] 陈永强 , 付钰 , 吴晓平 , 等 . 基于非零和博弈模型的主动防御策略选取方法[J] . 计算机应用 , 2013 , 33(5) : 1347-1349 . CHEN Yongqiang , FU Yu , WU Xiaoping . et al . Active Defense Strategy Selection Based on Non-zero-sum Attack-defense Game Model [J] . Journal of Computer Applications . 2013 , 33(5) : 1347-1349 .

[13] KAYODE A B , BABATUNDE I G , ISRAEL H D . DGM Approach to Network Attacker and Defender Strategies[C]// 8th International Conference for Internet Technology and Secured Transactions . Piscataway : IEEE Computer Society , 2013 : 313-320 .

(编辑 : 郭 华)

(上接第 74 页)

参考文献 :

[1] JAFAR S , SHAMAI S . Degrees of Freedom Region for the Mimo X Channel [J] . IEEE Transactions on Information Theory , 2008 , 54(1) : 151-170 .

[2] MADDAH-ALI M , MOTAHARI A , KHANDANI A . Communication over Mimo X Channels : Interference Alignment , Decomposition , and Performance Analysis [J] . IEEE Transactions on Information Theory , 2008 , 54(8) : 3457-3470 .

[3] CADAMBE V , JAFAR S . Interference Alignment and the Degrees of Freedom of Wireless X Networks [J] . IEEE Transactions on Information Theory , 2009 , 55(9) : 3893-3908 .

[4] HUANG C , CADAMBE V , JAFAR S . Interference Alignment and the Generalized Degrees of Freedom of the X Channel [J] . IEEE Transactions on Information Theory , 2012 , 58(8) : 5130-5150 .

[5] KOYLUOGLU O , SHAHMOHAMMADI M , EL-GAMAL H . A New Achievable Rate Region for the Discrete Memoryless X Channel [C]//Proceedings of IEEE Intnternational Symposium on Information Theory . Piscataway : IEEE , 2009 : 2427-2431 .

[6] PRASAD P , SRINIDHI N , CHOCKALINGAM A . Bounds on the Sum-rate Capacity of the Gaussian Mimo X Channel [C]//Fiftieth Annual Allerton Conference on Communication , Control , and Computing . Washington : IEEE Computer Society , 2012 : 1238-1245 .

[7] PRASAD P , CHOCKALINGAM A . Capacity Bounds for the Gaussian X Channel [C]//Information Theory and Applications Workshop . Washington : IEEE Computer Society , 2013 : 53-62 .

[8] LI J , GE J H , SUN C Q , et al . On the Capacity of Multiple-input Multiple-output Gaussian X Channels [J] . IET Communications , 2013 , 7(18) : 2084-2091 .

[9] KUMAR V P , BHASHYAM S . MIMO Gaussian X Channel : Noisy Interference Regime [J] . IEEE Communications Letters , 2014 , 18(8) : 1295-1298 .

[10] ANNAPUREDDY V , VEERAVALLI V . Gaussian Interference Networks : Sum Capacity in the Low Interference Regime and New Outer Bounds on the Capacity Region [J] . IEEE Transactions on Information Theory , 2009 , 55(7) : 3032-3050 .

[11] HAJEK B . An Exploration of Random Processes for Engineers [M] . Illinois : University Illinois at Urbana Champaign , 2008 .

(编辑 : 齐淑娟)