第36卷 第20期 计 算 机 工 程 2010年10月
Vol.36 No.20 Computer Engineering October 2010
·网络与通信安全技术· 文章编号：1000—3428(2010)20—00125— 文献标识码：A 中图分类号：TP393.08

基于不完全信息动态博弈的网络攻防态势感知

王纯子[1,2]，黄光球[1]
(1. 西安建筑科技大学管理学院，西安 710055；2. 西安工程大学管理学院，西安 710048)

摘 要：为反映网络攻防对峙形势并解决策略相依问题，提出不完全信息的动态攻防博弈模型。通过扩展对象 Petri 网的定义，使变迁及其输出弧上携带攻防策略及其效用信息，定义网络攻防对峙模型。在定义攻防行动顺序的基础上，提出利用攻防对峙模型构建博弈扩展形的方法，据此可得到攻防博弈均衡策略。

关键词：网络安全；扩展对象 Petri 网；攻防对峙模型；动态博弈

Network Attack-defense Situation Awareness Based on Dynamic Game with Incomplete Information

WANG Chun-zi[1,2], HUANG Guang-qiu[1]
(1. School of Management, Xi'an University of Architecture & Technology, Xi'an 710055, China;
2. School of Management, Xi'an Polytechnic University, Xi'an 710048, China)

【Abstract】 To reflect network attack-defense confrontation situation and solve the problem of strategy dependence, an incomplete information dynamic attack-defense game model is proposed. It constructs network attack-defense confrontation model, and based on the definition of attack and defense actions' sequence, the method of conversion from attack-defense confrontation model into extensive form game model is presented, then equilibrium strategy solution can be acquired.

【Key words】 network security; extended object Petri net; attack-defense confrontation model; dynamic game

1 概述

网络攻防对峙问题是一个策略相依的过程，理性的攻防双方可根据对方的行动以及获益来选择应对策略。博弈论在网络攻防领域发挥了重要作用。目前网络攻防的博弈分析尚处于前沿阶段，文献[1-2]通过随机博弈、不完全信息博弈等模型来进行入侵意图、目标和策略的推理。文献[3-6]将博弈论运用于网络安全领域，为该领域的发展做出了极大贡献。但上述研究基本都是针对入侵响应系统进行博弈分析。文献[7]提出了基于主动防御的博弈模型，但该模型必须建立在攻防两方对彼此收益明确获悉的基础上，且无法体现行动的先后顺序，其适用范围受到一定限制。

考虑到以上不足，本文提出一种基于攻防对峙模型的不完全信息动态博弈分析方法，研究网络系统中攻防抗衡全过程以及策略选择情况。本文利用扩展对象 Petri 网构建攻防对峙模型(*A-DCM*)，并提出了基于攻防对峙模型的博弈扩展形构建算法以及策略效用计算方法。在此模型上的动态博弈分析能够描述敌方信息不完备情况下的各种策略对峙情形和趋势，在攻击行为发生前和发生后更及时准确地获得最优主动和被动防御策略。

2 博弈要素分析及 *A-DCM* 的构建

2.1 攻防博弈模型的要素分析

本文将攻击者按攻击能力分为：低水平攻击者 $\theta_{\text{attack}}^{\text{L}}$ 和高水平攻击者 $\theta_{\text{attack}}^{\text{H}}$。$\theta_{\text{attack}}^{\text{H}}$ 能够采取任意难度的攻击策略，而 $\theta_{\text{attack}}^{\text{L}}$ 只能采取攻击复杂度低于 0.5 的攻击行动。这里攻击复杂度 C 的量化参照文献[8]，$C\in[0,1]$。

定义 1 参与人攻击方和防御方分别表示为 A_a 和 A_d。A_a 的类型空间为 Θ_a，$\Theta_a=\{\theta_{\text{att}}^{\text{L}},\theta_{\text{att}}^{\text{H}}\}$。$A_d$ 类型空间为 Θ_d，$\Theta_d=\{\theta_{\text{def}}\}$。

定义 2 攻击效用 U_{att} 和防御效用 U_{def}：

$$U_{\text{att}}(s,\theta_i)=AI-AC \tag{1}$$

$$U_{\text{def}}(s)=-SD+DI-DC \tag{2}$$

其中，$U_{\text{att}}(s,\theta_i)$ 为 θ_i 类型的攻击方在攻防博弈局势 s 下的效用函数，$U_{\text{def}}(s)$ 为防御方在攻防博弈局势 s 下的效用函数，AI、AC 为攻击收益和成本，DI、DC 为防御收益与成本，SD 为系统损失，它们的量化可参照文献[6]。

攻防双方的行动顺序为：防御者在攻击尚未发生前从主动防御集中选取行动策略，然后攻击者选择可实施的攻击方式发起攻击。针对某种特定的攻击行为，防御方选择被动防御策略来应对，双方如此往复，轮换决策。在 2 种情况下博弈结束：(1)防御方所采取的防御手段能够完全堵截各条攻击路径；(2)攻击者已达到攻击目标。

2.2 基于扩展对象 Petri 网的攻防对峙模型

在博弈分析之前需建立攻防对峙模型来描述攻击者各个攻击行动和路径。本文将网络中各主机节点定义为对象，节点遭受攻击后所呈现的各种脆弱状态为对象的接口库所。为

基金项目：陕西省重点学科建设专项基金资助项目；陕西省自然科学基金资助项目(2007E217)；陕西省教育厅专项基金资助项目(09JK524)

作者简介：王纯子(1983－)，女，博士研究生，主研方向：网络安全，网络攻防技术；黄光球，教授、博士生导师

收稿日期：2010-09-06 **E-mail：**pure326@126.com

了体现攻防策略的对峙情形，针对各攻击变迁定义防御策略集，并将攻防行动实施的成本、收益、攻击复杂度和防御阻止率等因素引入到模型中。

定义 3 *A-DCM* 定义为一个 9 元组：

$A\text{-}DCM=(O, P, T, \lambda, OA, S, O(p_i), I(t_i), O(t_i))$

其中：

(1)$O=\{O_0,O_1,\cdots, O_N\}$是网络中的节点对象集。

(2)$P=\{O_0.p_0, O_1.p_1,\cdots, O_N.p_n\}$是库所的有限集合，$O_i.p_j$ 表示 O_i 对象上的库所 p_j。

(3)$T=\{t_1, t_2,\cdots, t_m\}$是变迁的有限集合，$P\cup T=\Phi$。

(4)$\lambda=\{\lambda_1, \lambda_2,\cdots, \lambda_m\}$与 T 中元素一一对应，$\lambda_i=<C, SD, AC, AI>$。

(5)$OA=\{\delta_{ij}\}$为变迁的输出弧集合，δ_{ij} 表示从变迁 t_i 到库所 $O_k.p_j$ 的弧。

(6)$S=\{s_{ij}\}$与 IA 中的元素一一对应，$s_{ij}=\{s_{ij}^1, s_{ij}^2,\cdots, s_{ij}^g\}$，表示对攻击行为 t_i 所导致的脆弱状态 p_j，防御方可采取的防御策略集。$s_{ij}^x=<DC, DI, pr, dr>$，其中，$pr$ 为 s_{ij}^x 对 t_i 的后继攻击行为的阻止率，$pr\in[0,1]$；dr 为防御方对攻击行为 t_i 的检测率，$dr\in[0,1]$。

(7)$O(p_i)$表示库所的输出变迁集合。

(8)$I(t_i)$表示变迁的输入库所集合。

(9)$O(t_i)$表示变迁的输出库所集合。

A-DCM 的生成可采用模型检测、prolog 逻辑推理机或定制的搜索算法来寻找到达某一攻击目标的攻击路径 Petri 网，在此基础上增加防御策略集以及攻防效用因素即可。本文将防御策略分为主动防御策略集(ADS)和被动防御策略集(PDS)，以便后续的博弈建模与分析。

3 基于攻防对峙模型的博弈扩展形构建方法

要在攻防对峙模型上进行博弈分析必须先将攻击路径网转化为博弈扩展形，它明确定义了攻防行动在时间上的先后顺序以及各阶段双方可采取的策略集。

定义 4 攻防对峙博弈的扩展形记为：

$A\text{-}DCGEF=\{I, \Theta_a, A, X, pre(x), act(x), a(x), h(x), p, u\}$

其中：

(1)$I=\{A_a, A_d\}$为攻防博弈局中人。

(2)$\Theta_a=\{L, H\}$为 A_a 的类型。

(3)$A=\{A_a, A_d\}$表示攻击方和防御方的行动空间。

(4)$X=\{x_j^k\}$为博弈树中所有节点的集合，x_j^k 表示第 k 个攻防阶段中的第 j 个节点。

(5)$pre(x)$表示每一个节点 $x\in X$ 的最近前列点。任何节点的最近前列点必然唯一，即$|pre(x)|=1$。

(6)$act(x)$表示每一个节点 $x\in X$ 的前继动作。

(7)$a(x)$：$X\rightarrow A$，代表在决策点 x 上，所有可供攻击者或防御者选择的行动集合。

(8)$h(x)$代表攻击方或防御方在决策点 x 上的信息集。

(9)$p\in[0,1]$表示自然选择攻击者类型的概率分布。

(10)收益函数集合 $u=\{u_a, u_d\}$表示当到达某个结束点时，局中人 A_a 和 A_d 所获得的效用。

本文通过从攻防对峙模型中不断提取博弈信息，按照攻防行动顺序来模拟攻防场景，将攻防对峙模型转换为博弈扩展形。构造算法如下：

算法 1 A-DCGEF_generation()

输入 *A-DCM*

1. 初始化。创建节点集 X、行动集 a(x)、节点队列 nq；创建初始节点 $x_0^0\in X$ ； $a(x_0^0)=\{L,H\}$ ；

2. 创建节点 x_1^1, x_2^1 ； $pre(x_1^1)=x_0^0$ ， $pre(x_2^1)=x_0^0$ ；

3. $a(x_1^1)=a(x_2^1)=\{a_d^1,a_d^2,\cdots,a_d^n\}$ // a_d^i 为 A_d 在攻击发生前的主//动防御策略， $a_d^i\in$ADS

4. for(对应每个防御动作 a_d^i)

5. 创建节点 x_i^2, x_{n+i}^2 ； $pre(x_i^2)=x_1^1$, $pre(x_{n+i}^2)=x_2^1$ ；

6. 将 x_i^2, x_{n+i}^2 加入队列 nq；

7. flag=1；

8. while(nq≠∅)

9. { if(flag==0) // nq 中的节点为防御决策点

10. {从 nq 的尾部取出一个节点 x_j^k ；

11. 在 A-DCM 中搜索 $act(x_j^k)$ 对应的变迁 t_i；

12. while($\forall s_{ib}^x\in s_{ib}$)

13. $a(x_j^k)\leftarrow a_d^i$ ；创建节点 x_b^a , $pre(x_b^a)=x_j^k$ ； $act(x_b^a)=a_a^i$ ；

14. 将 x_b^a 加入队列 nq；

15. flag=1；}

16. if (flag==1) // nq 中的节点为攻击决策点

17. { 从 nq 的尾部取出一个节点 x_j^k ；

18. 在 A-DCM 中搜索 $act(pre(x_j^k))$ 对应的变迁 t_i；

19. if($act(x_j^k).pv<1$)

20. if($pre(x_j^k)$ 为主动防御决策点) st=$O(O_0.p_0)$ ；//st 为可选的后继攻击变迁集

21. st=$O(O(t_i))\cup(O(I(t_i))-t_i)$；

22. else if($act(x_j^k).pv=1$)

23. if($pre(x_j^k)$ 为主动防御决策点) st=$O(O_0.p_0)-t_i$；

24. st=$O(I(t_i))-t_i$；

25. while(在 A-DCM 中$\forall t_y\in st||\forall t_y\in O(O_0.p_0)$)

26. { if(x_j^k 属于 L 分枝&&$t_y.C\geq0.5$) continue；

27. $a(x_j^k)\leftarrow a_a^y$ ；创建节点 x_b^a， $pre(x_b^a)=x_j^k$ ； $act(x_b^a)=a_a^y$ ；

28. 将 x_b^a 加入队列 nq；}

29. flag=0；}

30. }

通过上述算法可以得到攻防行动交替进行的博弈树结构，对每一个终止节点 x_j^k，根据式(1)~式(2)并结合防御阻止率和攻击检测率计算攻防期望效用 $u(x_j^k)$，算法如下：

算法 2 utility_calculate()

输入 *A-DCGEF*

1.while(对所有终止节点 x_j^k)

2.{ if($pre(x_j^k)$ 为攻击决策点)

3. { cn=$pre(x_j^k)$ ；// cn 存储当前节点

4. $u_a(x_j^k)=act(x_j^k).AI-act(x_j^k).AC$ ；

5. $u_d(x_j^k)=-act(x_j^k).SD$ ；

6. if($pre(x_j^k)$ 为防御决策点)

7. { cn=$pre(pre(x_j^k))$ ；

8. $u_a(x_j^k)=(1-act(x_j^k).dr)\times(act(pre(x_j^k)).AI-act(pre(x_j^k)).AC)$ ；

9. $u_d(x_j^k)=(1-act(x_j^k).dr)\times(-act(pre(x_j^k)).SD+act(x_j^k).DI-act(x_j^k).DC)$ ；}

10. while(pre(cn)!=主动防御决策点)

11. { $u_a(x_j^k)=(1-act(cn).dr\times act(cn).pr)\times u_a(x_j^k)+$

act(pre(cn)).AI-act(pre(cn)).AC;

12. $u_d(x_j^k)$ =(1-act(cn).dr×act(cn).pr)× $u_d(x_j^k)$ +act(cn).dr × (-act(pre(cn)).SD+act(cn).DI-act(cn).DC)；

13. cn=pre(pre(cn))；temp_node=pre(cn)；}

14. if(防御动作 act(cn)对攻击动作 act(temp_node)有阻止作用)

15. $u_a(x_j^k)$×=1-act(cn).pr ；

16. $u_d(x_j^k)$=(1-act(cn).pr)× $u_d(x_j^k)$-act(cn).DC ；

17. else $u_d(x_j^k)$=$u_d(x_j^k)$+Q×(1-e^{-block_num})-act(cn).DC ；

18. 输出 $u(x_j^k)$=($u_a(x_j^k)$,$u_d(x_j^k)$) ；}

上述算法第(17)行中 $Q\times(1-e^{-block_num})$为路径堵截获益，表示当某主动防御策略虽然无法完全阻止攻击者的后继攻击，但能够堵截部分攻击路径时防御者所获得收益。*block_num* 为防御动作 *act*(*cn*)堵截的攻击变迁个数，*Q* 为一常数，依实际情况确定。

攻防博弈模型的完美贝叶斯均衡需在逆推归纳法的基础上，根据已观察到的行动不断修正对攻击者类型的信念，结合“信念”与均衡策略的相互依存关系来综合求解，具体求解方法这里不再详述。

4 实例验证与分析

为了说明和验证攻防对峙博弈分析方法，构建攻击场景如图 1 所示。

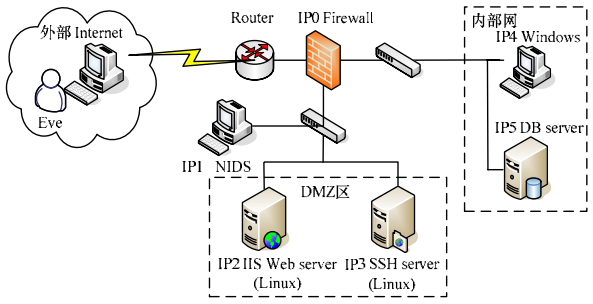


图 1 网络拓扑结构

外部主机只能访问 DMZ 区域的主机。各主机漏洞(Bugtraq ID)为：IP2-18858，IP3-8628，IP4-8152，IP5-4845。IP2 上的 WWW 服务能够向 IP5 中读写信息，且对 IP3 有信任关系。假设攻击者企图获取 IP5 上的机密信息或 Root 权限，根据以上网络信息可建立如图 2 所示的网络攻防对峙模型。

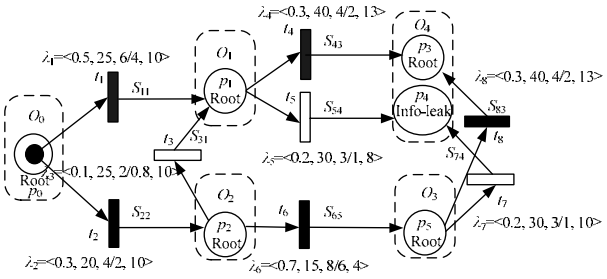


图 2 网络的攻防对峙模型

图 2 中对象 O_i 对应网络主机 IP(i+1)，各变迁的防御策略及其代价获益情况如表 1 所示。表 1 只罗列了部分防御策略集以示说明。按照算法 A-DCGEF_generation()将图 2 所示的攻防对峙模型转换成博弈扩展形，并根据 utility_calculate()得到每个策略组合下终止节点上的攻防效用(Q=10)。

表 1 防御策略集

S	策略描述	策略属性值
s_{11}	s_{11}^1 ：修复漏洞 18858	s_{11}^1 =<3, 25, 1, 0.6>
	s_{11}^2 ：关闭进程	s_{11}^2 =<1, 15, 0.5, 0.6>
	s_{11}^3 ：阻断可疑 IP 地址	s_{11}^3 =<1, 20, 1, 0.6>
s_{22}	s_{22}^1 ：修复漏洞 8628	s_{22}^1 =<3, 20, 1, 0.9>
	s_{22}^2 ：配置权限分隔	s_{22}^2 =<2, 10, 0.8, 0.9>
	s_{22}^3 ：断开网络	s_{22}^3 =<10, 15, 1, 0.9>

本文假设自然选择 L 型和 H 型攻击者的先验概率为 $p(L)=p(H)=0.5$。防御者采取主动防御措施后，观察攻击者的行动来修正对攻击者类型的先验信念。通过计算后验信念 $\tilde{p}_d(L/H\,|\,a_a^i)$ ：$\tilde{p}_d(L\,|\,a_a^1)=0$, $\tilde{p}_d(H\,|\,a_a^1)=1$, $\tilde{p}_d(L\,|\,a_a^2)=0.558$, $\tilde{p}_d(H\,|\,a_a^2)=0.441$ 等，结合逆推归纳法可得到攻防博弈的完美贝叶斯均衡策略(s_{22}^1 , a_a^1 , s_{11}^3)。当攻击行为尚未发生时，防御者选择 s_{22}^1 为最优主动防御策略，这是由于实施 s_{22}^1 可完全封堵低水平攻击者的所有攻击路径，而高水平攻击者只能选取 a_a^1 ，大大降低网络系统被攻击的概率。当防御方检测到攻击动作 a_a^1 时，可实施被动防御策略 s_{11}^3 阻断攻击者 IP 来保护网络系统。

5 结束语

针对主动防御技术中建模与分析的不足，本文提出一种基于不完全信息动态博弈的攻防态势感知方法。该方法能够全面描述各种攻防对峙场景，为防御者预测最优攻击路径以及提前制定防御措施提供了研究基础。由于大型复杂网络中存在多个防御者协作防御的情形，因此下一步的研究工作重点是将合作博弈与本文的竞争博弈相结合，多防御者合作博弈共同对抗攻击者行为。

参考文献

[1] Lye K W, Wing J. Game Strategies in Network Security[R]. Pittsburgh, USA: School of Computer Science, Carnegie Mellon University, Tech. Rep.: CMU-CS-02-136, 2002.

[2] Stakhanova N, Basu S, Wong J. A Taxonomy of Intrusion Response Systems[J]. International Journal of Information and Computer Security, 2007, 1(1/2): 169-184.

[3] 石 进, 陆 音, 谢 立. 基于博弈理论的动态入侵响应[J]. 计算机研究与发展, 2008, 45(5): 747-757.

[4] 石 盼, 连一峰. 基于战略博弈的 DDoS 攻防绩效评估方法[J]. 计算机工程, 2009, 35(3): 195-198.

[5] 郭渊博, 马建峰. 基于博弈论框架的自适应网络入侵检测与响应[J]. 系统工程与电子技术, 2005, 27(5): 914-917.

[6] 刘雪艳, 张 强, 王彩芬. 传感器网络安全投资的演化博弈分析[J]. 计算机工程, 2010, 36(12):190-192.

[7] 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.

[8] 张永铮, 云晓春, 胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报, 2004, 25(7): 107-114.

编辑 顾姣健