基于不完全信息静态博弈的工控系统风险评估方法

宋 宇 张春杰 程 超
(长春工业大学计算机科学与工程学院 吉林 长春 130000)

摘 要 针对目前大多数工业控制系统风险评估方法未思考防御者策略以及攻防两者之间的对抗问题,提出一种基于博弈模型的风险评估方法。通过攻击防御图模型,计算攻击收益和防御收益;建立静态贝叶斯攻防博弈模型,计算混合策略贝叶斯纳什均衡,获得攻防两者最优策略概率分布。根据信息安全风险评估的计算方法,以防御者收益和攻击者最优策略选择概率分布为基础进行风险评估计算。通过一个实例证明了该方法的可行性和有用性。

关键词 工业控制系统 风险评估 静态贝叶斯博弈 贝叶斯博弈均衡

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.06.047

RISK ASSESSMENT METHOD OF INDUSTRIAL CONTROL SYSTEM BASED ON INCOMPLETE INFORMATION STATIC GAME

Song Yu Zhang Chunjie Cheng Chao
(*School of Computer Science and Engineering, Changchun University of Technology, Changchun 130000, Jilin, China*)

Abstract At present, most industrial control system risk assessment methods do not consider the defender strategy and the confrontation between attack and defense. Therefore, this paper proposes a risk assessment method based on game model. The attack defense graph was used to calculate attack gain and defense gain. The static Bayesian attack and defense game model was established to calculate the mixed strategy Bayesian Nash equilibrium, and the optimal probability distribution of attack and defense strategies was obtained. According to the calculation method of information security risk assessment, the risk assessment analysis method was calculated based on the probability distribution of the defender's benefit and the attacker's optimal strategy selection. An example was used to illustrate the feasibility and usefulness of the proposed method.

Keywords Industrial control system Risk assessment Static Bayesian game Bayesian game equilibrium

0 引 言

随着工业进程的不断发展,工业控制系统逐渐与信息技术融合,通信方式也逐渐与互联网连通,导致工业控制系统面临越来越多的安全威胁,各种工业信息面临被窃取、篡改、删除等危险,严重的工业控制系统攻击事故时有发生[1]。例如,受“震网”病毒的攻击,伊朗布什尔核电站的核设施无法正常工作,导致国家遭受严重损失;乌克兰电力安全事件,导致全国大区域电力系统故障,引起严重的社会恐慌。因此,如何对工业控制系统进行安全有效的安全防护已变成工业领域的重点研究方面之一。目前,工业控制系统安全研究主要包括深度防御、入侵检测、风险评估等方向。其中,风险评估可以帮助管理者判断系统风险等级,且有针对性地部署防御措施,具有深刻意义[2]。

当前,许多国内外研究人员基于多种理论进行工业控制系统安全风险评估方法研究。文献[3]基于模糊层次分析法,对工业控制系统设备和攻击行为进行层次化建模,评估系统中各个设备的风险值,进而部署

收稿日期:2020-08-10。国家自然科学基金项目(61903047);吉林省发展改革委项目(2019C040-3);吉林省科技厅项目(20200401127GX)。**宋宇**,教授,主研领域:嵌入式系统。**张春杰**,硕士生。**程超**,副教授。

更有效的防御措施。文献[4]运用 D-S 证据理论,基于证据合成方法,整合多个专家的风险评估结果,降低主观影响,利用系统威胁发生可能性的置信区间完成重要性分析,部署有效的防御措施。文献[5]以攻击图为基础,结合工业控制系统的脆弱性量化指标,分析所有可能的攻击路径的脆弱性,得出最佳攻击路径,进行风险分析。文献[6]采用攻击树对工控系统进行建模,利用模糊数计算节点区间概率,得到系统每条攻击路径发生的概率。文献[7]使用了攻击树对 SCADA 系统的信息安全脆弱性进行了风险评估。上述研究方法,主要从工业控制系统结构或攻击者等方面进行风险评估,未思考工业控制系统的防御策略及攻防对抗对风险的影响。文献[8]提出基于攻防博弈的 SCADA 系统信息安全评估方法,建立完全信息静态博弈模型进行风险评估分析。但实际情况是攻防两者之间存在信息的不确定性,就此情况,完全信息博弈模型的实用性显得十分有限。

针对上述研究存在的不足,本文引入博弈理论[9],提出一种基于不完全信息静态攻防博弈模型的风险评估方法。主要内容包括以下几方面:构建攻击防御图模型,根据攻击防御图模型分析攻击者与防御者的攻防策略集合,计算攻防收益函数;建立静态贝叶斯攻防博弈模型,通过不完全信息静态博弈模型分析方法以及攻防双方收益建立攻防博弈树,计算混合策略贝叶斯纳什均衡;根据传统信息系统风险评估方法,以攻防期望收益函数、混合策略贝叶斯纳什均衡为基础,进行工业控制系统风险评估。

1 攻击防御图在工控系统中的应用

1.1 攻击防御图模型介绍

攻击图(Network Attack Graph)概念由 Philips 等在 20 世纪 90 年代第一次提出,最初被应用在网络系统安全分析方面。攻击图描述了网络系统中攻击者可能选择的攻击路径,由节点和有向边共同构成。攻击图中系统状态由节点表示,攻击行为由有向边表示,攻击路径由原子攻击组合表示。基本攻击图描述了攻击者可能采取的攻击路径及系统状态,但未考虑防御者的行为及攻防两者的策略收益情况。为了进行更全面地描述工业控制系统中攻击者和防御者的状态。本文引用文献[11]中的攻击防御图模型,描述攻击行为和防御行为,计算攻防收益。

攻击防御图模型 $ADC=(E,V,S)$,如图 1 所示,其中:$E=\{a_1,a_2,\cdots,a_6\}$ 代表攻击者原子攻击集合,攻击收益用原子攻击后的数值表示,每条攻击路径由多个原子攻击组成;$V=\{A,B,C,D,E,F,G,H\}$ 表示状态节点;$S=\{s_1,s_2,s_3\}$ 代表防御行为集合,用防御行为名称和防御收益共同表示。

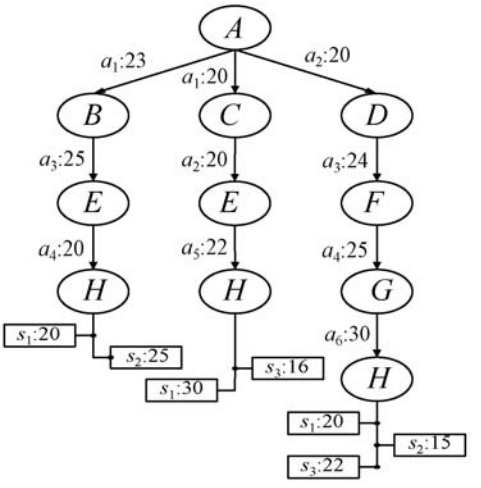

图 1 攻击防御图模型

1.2 攻防双方策略收益量化

博弈论应用中常用经济指标表示参与者的支付函数。本文为了更好地分析攻防博弈模型,引入两个重要经济指标,即防御者收益函数 DPF 和攻击者收益函数 APF。本文将文献[8]和文献[12]结合,改进收益函数计算方法,给出更全面、更合理的收益函数计算公式。

1.2.1 防御者收益函数 DPF

定义 1 防御者收益函数 DPF(Defender Pay of Function)表示攻击者和防御者在博弈过程中防御者的收益函数,如式(1)所示。

$$DPF=[-(1-R_{LR})\times S_L-D_C]\times A_{SR}-(1-A_{SR})\times D_C+I_{OA} \tag{1}$$

式中:S_L 表示系统损失代价,即原子攻击对系统发动攻击后,目标系统的损失;D_C 代表防御成本,即采用某一防御策略花费的成本;R_{LR}代表系统受到攻击后由于部署了防御措施,系统损失降低的比率;A_{SR}表示攻击成功率;I_{OA}表示攻击者信息,即系统受到攻击后可获得的攻击信息,可帮助管理者针对攻击行为做后续分析。

1.2.2 攻击者收益函数 APF

定义 2 攻击者收益函数 APF(Attacker Pay of Function),表示攻击者和防御者在博弈过程中攻击者的收益函数,具体计算公式,如式(2)所示。

$$APF=[(1-R_{LR})\times S_L-A_C]\times A_{SR}-(1-A_{SR})\times A_C+I_{OD} \tag{2}$$

式中:A_C 代表攻击成本,即采用某一攻击行为花费的成本;I_{OD}代表防御者信息,即攻击者进攻目标系统后可得到系统部署的防御信息。

2　构建不完全信息静态攻防博弈模型

博弈论[13]是研究经济领域对抗或竞争问题的重要数学理论,基于博弈模型分析问题,可以对参与者策略选择情况进行推断。工业控制系统中攻击者针对系统的脆弱性攻击,防御者则针对可能存在的威胁部署防御策略,两者之间形成攻防博弈。本文在攻防博弈的基础上考虑攻防两者之间信息的不确定性,构建了不完全信息静态博弈模型进行风险评估研究。

2.1　模型假设

假设 1　理性假设。攻防两者作为理性参与者都希望自己采取的策略是针对另一方的最优策略,此时参与者获得最大收益。因此,为保证参与者收益最大,两者都不会改变此时的策略。

假设 2　类型假设。实际工业控制系统中,由于防御策略的复杂性和攻击信息、行动的隐蔽性,攻防两者不能完全了解对方的策略收益情况。因此,假定可以将其中一方收益的不确定性转换为对其类型的不确定性,类型的不确定性可以通过参与者对类型可能性的推断来表示。

2.2　建立静态贝叶斯攻防博弈模型

静态贝叶斯博弈[13]是不完全信息静态博弈模型,表示参与者在不完全信息情况下同时行动的博弈。本文构建符合工业控制系统实际攻防环境的静态贝叶斯攻防博弈模型,参与者包括攻击者和防御者,即参与者数目 $n=2$。

静态贝叶斯攻防博弈模型可表示为一个五元组 $SBA\text{-}DGM=((N_A,N_D),(T_A,T_D),(B_A,B_D),(P_A,P_D),(U_A,U_D))$,其中:

(1) $N=(N_A,N_D)$代表攻防博弈模型中参与者集合。N_A,N_D分别表示攻击者、防御者。

(2) $T=(T_A,T_D)$代表攻防博弈模型中参与者类型集合。其中 $T_A=(t_1^A,t_2^A,\cdots,t_{j_1}^A)$表示攻击者 N_A的类型集合;$T_D=(t_1^D,t_2^D,\cdots,t_{j_2}^D)$表示防御者 N_D的类型集合。在实际系统中,攻防两者之间一方对另一方收益情况并不完全了解。因此,静态贝叶斯攻防博弈模型分析时,利用"海萨尼转换"的方法,假定一个虚构的参与人——自然,由虚构参与人先决定其他参与者的不同类型,用类型的不确定替代信息的不确定。

(3) $B=(B_A,B_D)$代表博弈模型中参与者的行动集合。其中 $B_A=(b_1^A,b_2^A,\cdots,b_{k_1}^A)$代表不同类型攻击者 N_A的行动集合;$B_D=(b_1^D,b_2^D,\cdots,b_{k_2}^D)$代表不同类型防御者 N_D的行动集合。

(4) 代表攻防博弈模型中参与者的先验概率集合。其中 $P_A=P(t_D\mid t_A)$表示攻击者在类型 t_A的情况下,判断防御者类型 t_D的概率;$P_D=P(t_A\mid t_D)$表示防御者在类型 t_D的情况下,判断攻击者类型 t_A的概率。

(5) $U=(U_A,U_D)$代表攻防博弈模型中参与者收益函数集合。$\forall b_A\in B_A,b_D\in B_D,t_A\in T_A,t_D\in T_D$,$U_A(b_A,b_D,t_A)$表示攻击者是类型 t_A时,攻击者采取行动 b_A,防御者采取行动 b_D时,攻击者的收益函数;$U_D(b_A,b_D,t_D)$表示防御者是类型 t_D时,攻击者采取行动 b_A,防御者采取行动 b_D时,防御者的收益函数。根据文中给出的攻防收益量化计算方法,攻击者和防御者的收益函数可表示为 $U_A(b_A,b_D,t_A)=APF(b_A,b_D,t_A)$,$U_D(b_A,b_D,t_D)=DPF(b_A,b_D,t_D)$。

2.3　攻防博弈模型均衡分析

博弈均衡分析[13]是博弈理论研究的重点内容,从工业控制系统管理者角度思考,对攻击者策略选择的预测有助于管理者部署最佳防御措施,提高系统防御能力。由此,下文给出两个重要概念。

2.3.1　贝叶斯博弈下的混合策略

定义 3　混合策略[13]在 SBA-DGM 中,$S_A(t_A)=\{s_1^A(t_A),s_2^A(t_A),\cdots,s_n^A(t_A)\}$为攻击者在类型 $t_A\in T_A$下的纯策略集,若攻击者的纯策略 $s_k^A(t_A)$以概率 $f_k^A(t_A)$进行选择,则 $F_A(t_A)=\{f_1^A(t_A),f_2^A(t_A),\cdots,f_{n_1}^A(t_A)\}$称为攻击者在类型 t_A下的一个混合策略,简记为 $F_A(t_A)=\{f_1^A,f_2^A,\cdots,f_{n_1}^A\}$,同理可得防御者混合策略为 $F_D(t_D)=\{f_1^D(t_D),f_2^D(t_D),\cdots,f_{n_2}^D(t_D)\}$,简记为 $F_D(t_D)=\{f_1^D,f_2^D,\cdots,f_{n_2}^D\}$。

2.3.2　混合策略贝叶斯纳什均衡

定义 4　混合策略贝叶斯纳什均衡[14],给定 $SBA\text{-}DGM=((N_A,N_D),(T_A,T_D),(B_A,B_D),(P_A,P_D),(U_A,U_D))$,$F_A(t_A)=\{f_1^A(t_A),f_2^A(t_A),\cdots,f_{n_1}^A(t_A)\}$表示攻击者混合策略概率分布,$F_D(t_D)=\{f_1^D(t_D),f_2^D(t_D),\cdots,f_{n_1}^D(t_D)\}$表示防御者混合策略概率分布。若同时满足以下条件:

$$\sum_{t_D\in T_D}P_A(t_D\mid t_A)U_A(F_A^*(t_A),F_D^*(t_D),t_A)\geqslant\sum_{t_D\in T_D}P_A(t_D\mid t_A)U_A(F_A(t_A),F_D^*(t_D),t_A)$$

$$\sum_{t_A \in T_A} P_D(t_A \mid t_D) U_D(F_A^*(t_A), F_D^*(t_D), t_D) \geqslant \sum_{t_A \in T_A} P_D(t_A \mid t_D) U_D(F_A(t_A), F_D^*(t_D), t_D)$$

则称混合策略$(F_A^*(t_A), F_D^*(t_D))$是贝叶斯纳什均衡。

静态贝叶斯攻防博弈模型一定存在以下两个混合策略 $F_A^*(t_A) = \{f_1^{A^*}(t_A), f_2^{A^*}(t_A), \cdots, f_{n_1}^{A^*}(t_A)\}$ 和 $F_D^*(t_D) = \{f_1^{D^*}(t_D), f_2^{D^*}(t_D), \cdots, f_{n_2}^{D^*}(t_D)\}$，使得攻防两者同时得到最大收益。根据理性假设，攻防双方在收益最大时，双方不会改变策略。因此，攻防两者都将采用最佳收益情况时的策略，从而达到博弈均衡。这时，攻击行为概率分布 $F_A^*(t_A) = \{f_1^{A^*}(t_A), f_2^{A^*}(t_A), \cdots, f_{n_1}^{A^*}(t_A)\}$ 表示为防御者对攻击者策略的预测，并以此作为风险评估的基础。

3 方法设计

传统信息安全风险评估方法以资产、威胁、脆弱性三个要素为基础进行风险值计算[12]。计算公式如下：

$$R = (A, V, T) = R(I(A, V), L(V, T)) \tag{3}$$

式中：R 表示风险；A 表示资产；V 表示资产脆弱性；T 表示威胁；I 表示威胁导致的损失；L 表示威胁发生的可能性。

分析信息安全风险评估和工业控制系统风险评估的共通性，基于传统信息安全风险计算式(3)，以工业控制系统中威胁发生的可能性 L 和威胁导致的损失 I 为基础，进行风险值计算。

本文通过第 2 节中式(1) - 式(2)计算攻击收益，防御收益后，构建工控系统博弈树。分析工业控制系统攻防两者的历史数据，分别获得防御者对攻击者的先验概率 $P_D = P(t_A \mid t_D)$、攻击者对防御者的先验概率 $P_A = P(t_D \mid t_A)$。将攻防两者收益输入 SBA-DGM 模型，进行攻防博弈分析，计算获得博弈均衡 $F_A^*(t_A)$、$F_D^*(t_D)$。依据攻防博弈模型的理性假设，防御者和攻击者会选择最优策略并保持不变。由此，系统中防御者对攻击者攻击策略预测可由攻防博弈模型的混合策略贝叶斯纳什均衡 $F_A^*(t_A) = \{f_1^{A^*}(t_A), f_2^{A^*}(t_A), \cdots, f_{n_1}^{A^*}(t_A)\}$ 表示，$F_A^*(t_A)$ 为威胁发生的可能性。威胁造成的损失为防御收益 $U_D(b_A, b_D, t_D)$。根据文献[12]观点，风险评估过程中防御者部署的防御措施是管理者已确定的，假定确定的防御者策略为 b_0^d，系统风险值可用式(4)表示，管理者根据不同防御策略，进行系统风险评估分析，计算系统风险值，判断系统风险等级，部署最优防御策略。

$$R_i = \sum_{i_2=1}^{n} P(t_A \mid t_D) \sum_{i_1=1}^{m} f_i^{A^*}(t_A) \frac{U_D(b_A, b_D, t_D)}{U_D^{\max}(b_A, b_D, t_D)} \tag{4}$$

考虑工控系统中包含多个子系统，进行整体系统风险评估时，要思考各个子系统风险值占整体系统风险值的权重，权重向量表示为 $W = (W_1, W_2, \cdots, W_n)$，子系统风险值表示为 $R = (R_1, R_2, \cdots, R_n)$。系统的整体风险值公式如下：

$$R_{\text{all}} = \sum_{j=1}^{n} R_j W_j \tag{5}$$

子系统权重可以通过多种方法计算得到，本文利用模糊层次分析法[15]计算子系统权重。多个专家对各子系统进行重要性赋值，构建判断矩阵，并依据式(6) - 式(7)完成一致性转化，判断矩阵化成满足一致性条件的模糊判断矩阵，最后利用式(8)得到子系统权重。

$$r_i = \sum_{k=1}^{n} r_{ik} \tag{6}$$

$$f_{ij} = \frac{r_i - r_j}{2} + 0.5 \tag{7}$$

$$W_i = \frac{1}{n} - \frac{1}{2\alpha} + \frac{1}{n\alpha} \times \sum_{j=1}^{n} f_{ij} \tag{8}$$

算法流程如算法 1 所示。

算法 1 不完全信息静态博弈风险评估算法

输入：SBA-DGM。

输出：工控系统安全风险值。

BEGIN

1. Initialize( )
2. 建立攻防双方类型集合 $T = (T_A, T_D)$
3. 建立攻防双方行动集合 $B = (B_A, B_D)$
4. for all $s_i^A(t_A) \in S_A(t_A)$
5. 分别计算攻击收益 APF、防御收益 DPF
6. $\sum_{t_D \in T_D} P_A(t_D \mid t_A) U_A(F_A^*(t_A), F_D^*(t_D), t_A) \geqslant \sum_{t_D \in T_D} P_A(t_D \mid t_A) U_A(F_A(t_A), F_D^*(t_D), t_A)$
7. $\sum_{t_A \in T_A} P_D(t_A \mid t_D) U_D(F_A^*(t_A), F_D^*(t_D), t_D) \geqslant \sum_{t_A \in T_A} P_D(t_A \mid t_D) U_D(F_A(t_A), F_D^*(t_D), t_D)$
8. 得到混合贝叶斯均衡，$F_A^*(t_A) = \{f_1^{A^*}(t_A), f_2^{A^*}(t_A), \cdots, f_{n_1}^{A^*}(t_A)\}$
9. $R_i = \sum_{i_2=1}^{n} P(t_A \mid t_D) \sum_{i_1=1}^{m} f_i^{A^*}(t_A) \frac{U_D(b_A, b_D, t_D)}{U_D^{\max}(b_A, b_D, t_D)}$
10. 调用算法 2，计算子系统权重。
11. $R_{\text{all}} = \sum_{i=1}^{n} R_i W_i$

12. return R_{all}

END

算法 2　子系统权重计算算法

输入:子系统模糊判断矩阵。

输入:子系统权重。

BEGIN

1. Initialize( )

2. 利用公式 $r_i = \sum_{k=1}^{n} r_{ik}$, $f_{ij} = \frac{r_i - r_j}{2} + 0.5$,完成一致性转化

3. $W_i = \frac{1}{n} - \frac{1}{2\alpha} + \frac{1}{n\alpha} \times \sum_{j=1}^{n} f_{ij}$

4. return W_i

END

4　实际应用及分析

为了说明文中所提工业控制系统风险评估方法的可行性。本文以工业控制系统中的一个子系统——数据采集与监视控制(SCADA)系统为例,利用文中所提出的方法,进行风险评估分析。SCADA 系统结构图如图 2 所示,SCADA 系统主要构成部分有安全防御设备、工程师站、SCADA 服务器、可编程控制器和客户端等。

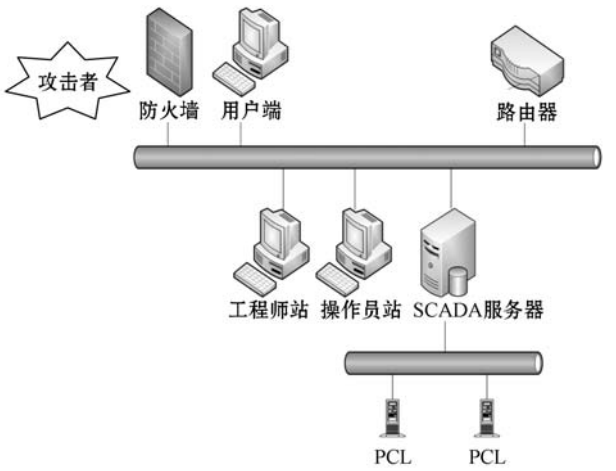

图 2　SCADA 系统拓扑结构

依据系统管理者对攻击信息的分析,将攻击者策略分类为两种类型,由 t_A = {冒险型攻击者,保守型攻击者}表示,具体信息如表 1 所示,其中不同原子攻击组合表示不同类型的攻击策略,攻击行为存在不确定性,因此攻击者信息也存在不确定性。依据防御策略成本,系统影响以及管理者经验等方面的思考,防御者策略也可分为两类,由 t_D = {高等级防御者,低等级防御者}表示,具体信息如表 2 所示,根据攻防两者所采用的行动策略构建系统的攻击防御图模型,如图 3 所示。

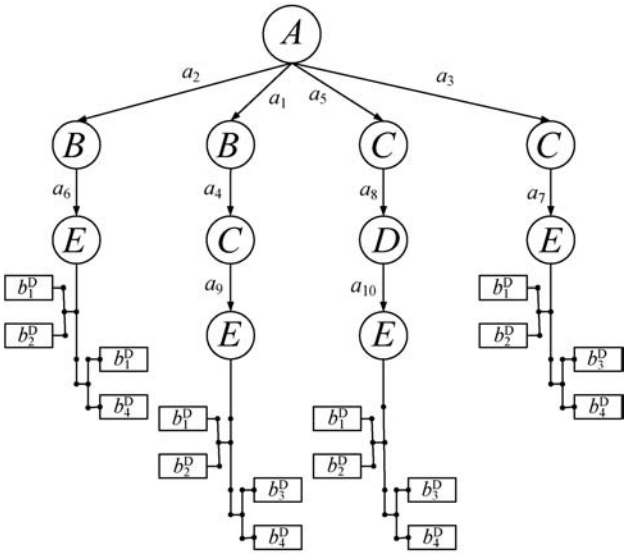

图 3　攻击防御图模型

表 1　攻击者攻击行动描述

分类	原子攻击	冒险型攻击者		保守型攻击者	
		b_1^A	b_2^A	b_3^A	b_4^A
Root	a_1 Destroy Data base		√		
	a_2 Shutdown server	√			
	a_3 Remotebuffer over flow				√
User	a_4 Request DNS sending special response		√		
	a_5 Ftp. rhost			√	
	a_6 Stealortamper with datas	√			
Data	a_7 Steala ccountand crack it				√
	a_8 Sendspecial LPC requestto LSASS process			√	
Dos	a_9 UDPFlood		√		
	a_{10} TCP-SYNFlood			√	

表 2　防御者防御行动描述

防御子策略	高等级防御者		低等级防御者	
	b_1^D	b_2^D	b_3^D	b_4^D
Limit packets fromports		√		√
Install 0547 patches	√	√		
Reinstall Listener program			√	√
Unistall deletee Trojan		√		
Add physical ressource			√	
Correc thomepage	√			√
Renew data		√		√
Delete suspiciousa ccount			√	

确定参与者的策略集合,建立攻击防御图模型后,利用第 2 节中的式(1) – 式(2)计算参与者的策略收

益。通过分析工业控制系统的攻击历史记录和防御历史记录,获得防御者对攻击者类型的先验概率:(冒险型攻击者,保守型攻击者) = (0.55,0.45),攻击者对防御者其类型的先验概率:(高等级防御者,低等级防御者) = (0.6,0.4)。然后,建立攻防博弈树如图 4 所示。通过均衡公式计算得到混合策略贝叶斯纳什均衡,计算结果如表 3 所示。

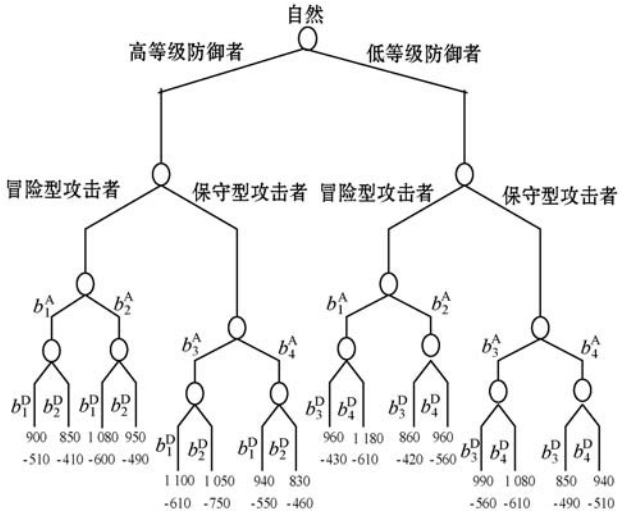

图 4 攻防博弈树

表 3 混合策略贝叶斯纳什均衡

混合策略均衡	攻击者/防御者类型	混合策略贝叶斯纳什均衡概率分布
$F_A^*(t_A)$	冒险型攻击者	$\{F_1^{A*}(t_A),F_2^{A*}(t_A),\} = \{0.475\,5,0.524\,5\}$
	保守型攻击者	$\{F_3^{A*}(t_A),F_4^{A*}(t_A),\} = \{0.231\,4,0.768\,6\}$
$F_D^*(t_D)$	高等级防御者	$\{F_1^{D*}(t_D),F_2^{D*}(t_D),\} = \{0.614\,5,0.385\,5\}$
	低等级防御者	$\{F_3^{D*}(t_D),F_4^{D*}(t_A),\} = \{0.495\,2,0.504\,8\}$

根据实际情况分析,工业控制系统防御过程中,防御者策略是确定的,因此,假定此时防御者采用防御策略是 b_1^D,根据式(4)计算风险值可得:

$$R_i = \sum_{i_2=1}^{2} P(t_A \mid t_D) \sum_{i_1=1}^{2} f_{i_2}^{A*}(t_A) \frac{U_D(b_A,b_D,t_D)}{U_D^{\max}(b_A,b_D,t_D)} = 0.648\,9$$

数据采集与监视控制系统、分布式控制系统、过程控制系统是工业控制系统中几个重要的子系统,本文考虑子系统风险对工业控制系统整体风险的影响。以三个子系统为例,计算得到各个子系统安全风险值为 $(R_1,R_2,R_3,) = (0.648\,9,0.591\,3,0.759\,4)$。依据专家对工业控制系统中三个子系统的重要性评价,利用模糊层次分析法计算子系统的权重向量为 $(\boldsymbol{W}_1,\boldsymbol{W}_2,\boldsymbol{W}_3) = (0.528\,6,0.309\,5,0.261\,9)$。根据式(5)计算工业控制系统整体风险值 $R_{ALL} = 0.724\,9$,依据文献[16]将风险等级分为五个等级,判断该系统风险级别为四级。

同理,可以得到部署其他防御策略时的风险值,如图 5 所示。同时,本文对防御策略收益取绝对值,计算各个防御策略收益的平均值,这时数值小的策略较好,如图 6 所示。

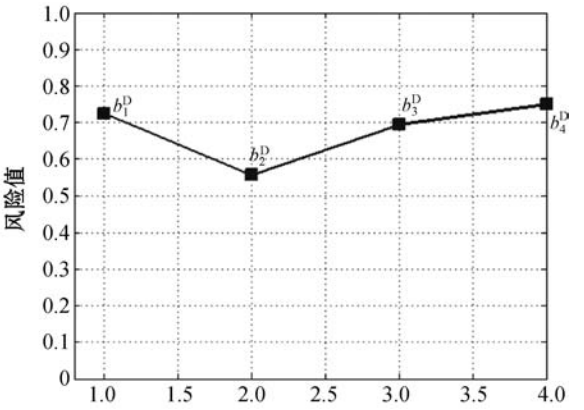

图 5 风险值

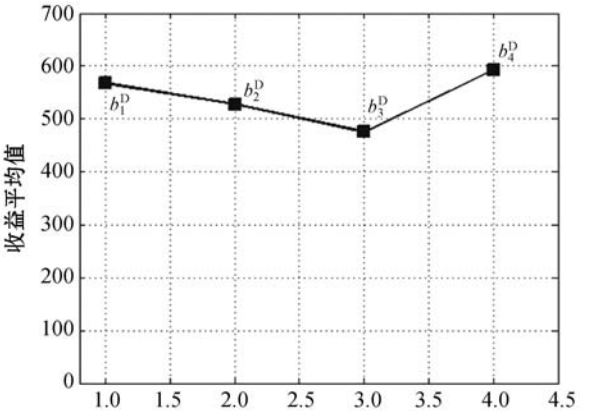

图 6 防御策略收益平均值

可以看出,系统采用防御策略 b_2^D 时,系统风险值最小,并且防御收益函数也相对较为合理。管理者可以根据风险值和收益函数的比较,选择部署最佳的防御策略,提高系统防御能力,降低安全风险。

由此可见本文所提的方法是可行的,本文引入不完全信息静态博弈理论,综合考虑了攻防两者之间的对抗以及两者之间信息的不确定性,更符合实际应用情况。具体比较如表 4 所示。

表 4 方法比较

方法	攻击者类型	信息需求	全面性	可操作性
文献[3]	1	无	一般	一般
文献[17]	1	完全信息	一般	一般
文献[9]	1	完全信息	一般	较好
本文	2	不完全信息	很好	很好

信息需求表示攻击者和防御者所拥有对方信息情况。相比于文献[9]、文献[17]中使用的完全信息博

弈,本文增加了攻防之间信息的不确定性,采用不完全信息博弈更加贴近实际应用场景;全面性表示收益函数和博弈模型分析过程中是否考虑更多的影响因素。相比于文献[3]、文献[17]、文献[9],本文增加了攻防对抗、系统损失、攻防间接收益、信息不确定性、子系统权重等影响因素,提高了风险评估分析的全面性。相比于文献[3]、文献[9],本文给出了具体的风险值计算公式和风险评估算法的步骤,能够更好地完成工控系统安全风险评估,具有更好的可操作性。

5 结　语

本文在已有基于博弈模型的工业控制系统风险评估方法上采用了不完全信息模型,更符合实际系统的应用情况。建立了静态贝叶斯攻防博弈模型,对博弈模型计算混合策略贝叶斯纳什均衡,进行攻击者行为预测,进行风险评估,为管理者部署最优防御措施提供帮助。但是该方法只适用于阶段性风险评估,缺少对工业控制系统的动态性风险评估。因此,下一步将重点研究动态博弈情况,以动态博弈理论为基础进行工业控制系统风险评估研究。

参 考 文 献

[1] 王小山,杨安,石志强,等. 工业控制系统信息安全新趋势[J]. 信息网络安全,2015(1):6 - 11.

[2] 区和坚. 工业控制系统信息安全研究综述[J]. 自动化仪表,2017,38(7):4 - 8.

[3] 贾驰千,冯冬芹. 基于模糊层次分析法的工控系统安全评估[J]. 浙江大学学报(工学版),2016,50(4):759 - 765.

[4] 林云威,陈冬青,彭勇,等. 基于 D-S 证据理论的电厂工业控制系统信息安全风险评估[J]. 华东理工大学学报(自然科学版),2014,40(4):500 - 505.

[5] 黄家辉,冯冬芹,王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报,2016,42(5):792 - 798.

[6] Shang W L, Gong T Y, Chen C Y, et al. Information security risk assessment method for ship control system based on fuzzy sets and attack trees[J]. Security and Communication Networks,2019,2019:2054 - 2210.

[7] Ten C W, Liu C, Govindarasu M. Vulnerability assessment of cybersecurity for SCADA system using attack trees[C]// IEEE Conference on Power Engineering Society General Meeting,2007:1 - 8.

[8] 黄慧萍,肖世德,孟祥印. 基于攻防博弈的 SCADA 系统信息安全评估方法[J]. 计算机工程与科学,2017,39(5):877 - 884.

[9] Wei H, Xia C H, Wang H Q, et al. A game theoretical attack-defense model oriented to network security risk assessment[C]//International Conference on Computer Science and Software Engineering,2008:1097 - 1103.

[10] Phillips C, Swilwr L P. A graph-based system for network vulnerability analysis[C]//Workshop on New Security Paradigms,1998:71 - 79.

[11] Jiang W, Fang B X, Zhang H L, et al. Optimal network security Strengthening using attack-defense game model[C]// 6th International Conference on Information Technology,2009:475 - 480.

[12] 余定坤,王晋东,张恒巍,等. 基于静态贝叶斯博弈的风险评估方法研究[J]. 计算机工程与科学,2015,37(6):1079 - 1086.

[13] Fudenberg D, Tirole J. Game theory[M]. Cambridge: The MIT Press,1991.

[14] Myerson R. Bayesian equilibrium and incentive compatibility: An introduction[M]//Social Goals and Social Organization. Cambridge: Cambridge University Press,1985.

[15] 吕跃进. 基于模糊一致矩阵的模糊层次分析法的排序[J]. 模糊系统与数学,2002(2):79 - 85.

[16] Matuleviius R. Model comprehension and stakeholder appropriateness of security risk-oriented modeling languages[M]. Heidelberg: Spring,2014.

[17] 张树伟,刘文芬,魏江宏. 基于博弈模型的网络风险量化评估方法[J]. 信息工程大学学报,2014,15(2):156 - 162.

(上接第 328 页)

[18] 游静,上官经伦,徐守坤,等. 考虑信任可靠度的分布式动态信任管理模型[J]. 软件学报,2017,28(9):2354 - 2369.

[19] Seo S H, Won J, Sultana S, et al. Effective key management in dynamic wireless sensor networks[J]. IEEE Transactions on Information Forensics and Security,2015,10(2):371 - 383.

[20] 周治平,赵晓晓,邵楠楠. 结合模糊集合与 D-S 证据理论的 WSN 信任评估模型[J]. 系统仿真学报,2018,30(4):1229 - 1236.

[21] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems,2007,43(2):618 - 644.

[22] Marmol F G, Perez G M. TRMSim-WSN, trust and reputation models simulator for wireless sensor networks[C]// IEEE International Conference on Communications, 2009:14 - 18.

[23] Mármol F G, Pérez G M. Providing trust in wireless sensor networks using a bio-inspired technique[J]. Telecommunication Systems,2011,46(2):163 - 180.

[24] Mármol F G, Marín-Blázquez J G, Pérez G M. LFTM, linguistic fuzzy trust mechanism for distributed networks[J]. Concurrency and Computation: Practice and Experience, 2012,24(17):2007 - 2027.