Journal of System Simulation

Volume 30 | Issue 10 Article 13

1-4-2019

# Modeling for Security Protection Capability of Information System Based on CPN

Qiangjun Chen
*1. PLA Information Engineering University, Zhengzhou 450001, China; ;*

Mingqing Zhang
*1. PLA Information Engineering University, Zhengzhou 450001, China; ;*

Hongshan Kong
*1. PLA Information Engineering University, Zhengzhou 450001, China; ;*

Xiaohu Liu
*1. PLA Information Engineering University, Zhengzhou 450001, China; ;*

*See next page for additional authors*

# Modeling for Security Protection Capability of Information System Based on CPN


## Abstract

Abstract: Modeling plays an important role in assessment for security protection capability. Oriented to the features that evaluation has many methods which update quickly, *the analysis frame is proposed based on detect, analyse and respond.* Aimed at the problems that it is difficult to model the intelligent learning and coordination process for protective device, *analysis model is built based on CPN. The colors of message color sets represent the different properties of events. Detect, analysis and respond components which represent different process of security protection capability are defined. Two theorems are proved, and model complexity is analyzed.* The usability of model is verified, and excellent versatility, scalability and analyzability are reached by analyzing the application process. Results show that the model can provide data and model support for the evaluation on security protection capability.



## Keywords

security protection capability, analysis frame, CPN, analysis model



## Authors

Qiangjun Chen, Mingqing Zhang, Hongshan Kong, Xiaohu Liu, and Lianjie Shao



## Recommended Citation

Chen Qiangjun, Zhang Mingqing, Kong Hongshan, Liu Xiaohu, Shao Lianjie. Modeling for Security Protection Capability of Information System Based on CPN[J]. Journal of System Simulation, 2018, 30(10): 3699-3710.

第 30 卷第 10 期 系统仿真学报© Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

# 基于 CPN 的信息系统安全防护能力建模方法

陈强军[1]，张明清[1]，孔红山[1]，刘小虎[1]，邵连杰[2]
(1. 解放军信息工程大学，河南 郑州 450001；2. 解放军 68048 部队，陕西 宝鸡 721000)

**摘要:**建模对安全防护能力评估具有重要作用。结合安全防护能力评估方法多、更新快的特点，*提出了基于监测、分析和响应的安全防护能力分析框架;* 针对防护设备智能学习和协作交互难以建模的问题，*基于 CPN(Colored Petri Nets)构建了安全防护能力分析模型。模型用消息颜色集的颜色表示系统事件的不同属性；建立了监测、分析和响应三种功能组件来表示安全防护能力的不同过程；给出了模型的 2 个定理，分析了模型复杂度。*实例应用验证了模型的有效性，模型分析得出了其良好的通用性、扩展性和可分析性，表明可为安全防护能力的评估提供数据和模型支撑。

**关键词:** 安全防护能力；分析框架；CPN；分析模型
中图分类号：TP391.9A 文献标识码：A 文章编号：1004-731X (2018) 10-3699-12
DOI: 10.16182/j.issn1004731x.joss.201810013

## Modeling for Security Protection Capability of Information System Based on CPN

*Chen Qiangjun*[1], *Zhang Mingqing*[1], *Kong Hongshan*[1], *Liu Xiaohu*[1], *Shao Lianjie*[2]
(1. PLA Information Engineering University, Zhengzhou 450001, China; 2. Unit 68048 of the PLA, Baoji 721000, China)

**Abstract:** Modeling plays an important role in assessment for security protection capability. Oriented to the features that evaluation has many methods which update quickly, *the analysis frame is proposed based on detect, analyse and respond*. Aimed at the problems that it is difficult to model the intelligent learning and coordination process for protective device, *analysis model is built based on CPN. The colors of message color sets represent the different properties of events. Detect, analysis and respond components which represent different process of security protection capability are defined. Two theorems are proved, and model complexity is analyzed.* The usability of model is verified, and excellent versatility, scalability and analyzability are reached by analyzing the application process. Results show that the model can provide data and model support for the evaluation on security protection capability.

**Keywords:** security protection capability; analysis frame; CPN; analysis model

## 引言

由于信息技术的发展，信息系统应用愈来愈广，作用也越来越重要，同时安全威胁和脆弱性也随之呈现出技术含量高、功能种类多、更新快的特点，相应的信息系统安全防护能力(Security Protection Capability of Information System, SPCIS)也呈现出了复杂、多样、快变的特点[1]。由于 SPCIS 是针对已发现安全威胁和脆弱性的，其安全防护措施的部署较威胁和脆弱性存在一定的滞后，所以研究对 SPCIS 较为通用和易于扩展的建模方法很有必要。同时，对防护设备的智能学习、自我更新以及设备间的协作交互等复杂问题的分析，是分析和优化 SPCIS 的重要方法，从而研究支持 SPCIS 复杂性分析的建模方法急为迫切。

收稿日期：2016-09-09 修回日期：2016-11-20;
作者简介：陈强军(1992-)，男，甘肃通渭，硕士生，研究方向为信息系统安全建模与评估；张明清(1961-)，男，湖北孝感，学士，副教授，研究方向为系统建模与仿真；孔红山(1981-)，男，河南濮阳，博士生，讲师，研究方向为系统建模与仿真。



 

## 1 相关工作

SPCIS 的研究范围极为广泛，从信息系统的整体安全性，到信息系统安全策略、措施和方案，以及 SPCIS 的影响因素，再到单个的安全防护设备均有涉及。本文把对 SPCIS 的研究概括为五类：

针对信息系统整体安全性的研究，如风险评估、安全性分析等。Nayot Poolsappasit 等在文献[2]中基于贝叶斯提出了风险动态评估方法，并使安全防护措施的效用最大；万雪莲在文献[3]中从系统攻击和防护两个角度提出了一种综合评估模型；还有利用攻击图[4]、Petri 网[5]进行的研究。

针对信息系统安全策略、措施和方案的研究。You Y 在文献[6]中提出了一种安全测量系统，能有效反映各领域的特点，从而实现有效的信息管理；文献[7-8]中对给定脆弱性环境下的安全措施效用、安全策略进行了建模和分析；文献[9-10]中基于 RBAC 访问控制策略，通过对网络安全的功能定义和建模，给出了一种评估方法；此外还有最优安全策略[11]，防御策略选取[12]等的研究。

针对 SPCIS 影响因素的研究。对系统脆弱性的研究，如脆弱性分析[13]，脆弱性定量评估[14]等；对安全威胁的研究，如网络实时威胁的识别与分析[15]，系统漏洞风险评估等[16]。

针对安全防护设备的研究。文献[17-18]中分别对网络防火墙，入侵检测设备进行了分析和评估，是分析单个防护设备的典型案例。

还有一个研究分支，是从攻击者的角度出发，通过分析攻击者策略[19]、权限提升[20]、攻击成本[21]等，进而分析 SPCIS。这种方法通过分析攻击后的效果来分析 SPCIS 可能存在的弱点，是一种好的思路，但由于 SPCIS 在防护过程中是动态变化的，而这种方法不能有效描述 SPCIS 的变化，或者由于变化而出现描述状态空间爆炸等问题。

上述方法多是针对不同的对象采取不同的建模方法，这些方法可分为几个类别，但由于 SPCIS 具有复杂、多样、快变的特点，使得这些方法不能较为普遍的应用，从而降低了方法的可用性；同时，还不能满足 SPCIS 快速变化而带来的分析要求，即扩展性不好；并且一些建模方法不能对防护设备的智能学习、自我更新，以及防护设备间的协作进行建模和研究，即可分析性不强。

本文针对上述问题进行了深入研究。

## 2 信息系统安全防护能力分析

随着信息系统的复杂和智能化，SPCIS 也越来越复杂和智能，影响 SPCIS 的不确定性因素也越来越多。

从 SPCIS 的运行原理来分析。原理为根据已有规则知识对经过的系统事件作出判断，并作出相应的响应，目的是发现已存在或潜在的攻击和脆弱性，从而抵御或降低对系统的危害。

从信息安全技术体系 PDRR(Protection, Detection, Response, Recovery)的角度分析。PDRR 体系考虑了 SPCIS 部署前后所有的过程，包括预先阻止攻击发生的条件产生，检测系统存在的脆弱性和入侵行为，对危及安全的相关行为作出响应，并把系统恢复到安全状态，这些技术组成了一个完整动态的安全循环[22]。

经分析，这里用 Detect，Analyse 和 Respond 抽象出 SPCIS 的 3 个阶段：Detect 按相关规则知识对系统事件监测并作出初步处理；Analyse 依据相关规则知识对监测后的系统事件分析、判断和标记，并把结果传给 Respond；Respond 则根据 Analyse 的标记信息依照相关规则知识作出防护响应。建立如图 1 所示的 SPCIS 分析框架。

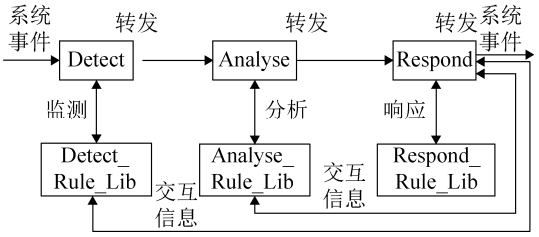


图 1 基于 DAR 的 SPCIS 分析框架

Fig. 1 The analysis framework for SPCIS based on DAR

对框架中的相关概念作如下定义和规范：

**定义 1: Detect** 指 SPCIS 监测的过程。原理为依据监测规则库 *Detect_Rule_Lib* 中的知识，按照相关规则对经过 Detect 中的事件进行处理，将符合规则的予以转发，否则丢弃。

**定义 2: Analyse** 指 SPCIS 分析的过程。原理为依据分析规则库 *Analyse_Rule_Lib* 中的知识，按相关规则对经过 Analyse 的事件分析、判断和标记，并将标记消息传给响应功能组件。

**定义 3: Respond** 指 SPCIS 响应的过程。原理为依据响应规则库 *Respond_Rule_Lib* 中的知识对分析标记后的消息响应。若标记为正常，则直接转发；若为异常，则根据响应规则库中的知识启用相关防护措施，如生成协作消息等。

**定义 4: DAR** 特指 Detect，Analyse，Respond 的合称。表示 Detect，Analyse，Respond 整个运行过程或用其分析问题的过程和方法。

# 3 安全防护能力建模方法

SPCIS 的分析需要研究 DAR 各功能之间的相互作用和并发行为。本节对建立的分析框架应用，把 DAR 3 种功能抽象成 3 类通用的功能组件，并用 CPN tools 作为建模工具构建相应的功能组件，建立 SPCIS 分析模型。

## 3.1 消息建模

统一用颜色集 *Message* 抽象表示经过 DAR 的事件 event。定义如下：

**定义 5: 消息 *Message*** 定义为四元组 $Message ::= \langle Attr\_In, Attr\_Out, Attr\_Oth, MsgCon \rangle$。

*Attr_In* 表示消息的内部属性，如消息是否加密、完整、可用以及脆弱性利用等；*Attr_Out* 表示消息的外部属性，如消息的发送、接收者的 IP 地址，通信端口等；*Attr_Oth* 表示消息的其他属性，如消息在通信机制中的消息类型、消息编号，时间戳等；*MsgCon* 表示消息负载的内容。

信息系统面临的威胁来自系统内部攻击、外部攻击和其他威胁。内部攻击的属性在 *Attr_In* 中体现，如攻击者的攻击行为；外部攻击的属性在 *Attr_Out* 中体现，如攻击者的地址信息；其他威胁在 *Attr_Oth* 中体现，如通信中的通信属性。

*MsgCon* 表示负载在消息中的信息。在 CPN 模型中，其 *token* 均由小写字母表示，如 *Message* 的 *token* 为*(at_in,at_out,at_oth,mc)*。

## 3.2 功能建模

### 3.2.1 Detect 功能组件

Detect 功能组件用来抽象表示对所防护系统的全生命周期监控。监测对象包括系统的信息流、操作行为以及系统的网络连接情况等，监测时不确定是否有攻击。监测是 SPCIS“观察”并作出初步“处理”的过程。组件运行时，不同的消息属性由对应的知识库按照相应的规则函数对其监测，以验证是否符合各属性的要求。

相应的知识库和规则函数定义为：

**定义 6: 监测规则库** 是监测功能组件依据的知识集合，记为 *Det_Rule_Lib*。按消息属性 *Attr_In*，*Attr_Out* 和 *Attr_Oth* 所依据的规则知识，定义三种属性监测规则库：*Det_Rule_In_Lib*={*Det_Rule_In_Lib, Det_Rule_Out_Lib, Det_Rule_Oth_Lib*}，在 CPN 模型中，规则知识存储在监测规则库所中。

**定义 7: 监测规则 *DetectRule*** 定义五元组 $DetectRule ::= <ID_D, Attr\_D, Equip\_D, Rule\_D, Time\_D>$，其元素分别表示规则的 ID，规则对应的消息属性，规则依附的防护设备，具体的规则知识，以及规则的最近更新时间。

**定义 8: 监测规则函数** 是监测功能组件执行监测的具体行为。同样按消息属性所依据的监测知识库，定义三种监测规则函数：*D_Rule_In*( )，*D_Rule_Out*( )和 *D_Rule_Oth*( )。

在 CPN 模型组件中，监测规则函数定义在变迁的 Guard 函数中或指向库所 *A* 的输出弧上。

构建的 Detect 的功能组件如图 2 所示。

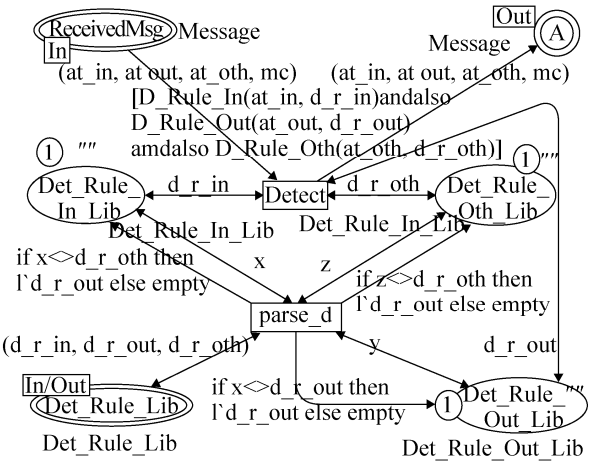


图 2 Detect 功能组件
Fig. 2 Detect component

该功能组件包含 3 个监测知识子库所：*Det_Rule_Out_Lib*，*Det_Rule_In_Lib* 和 *Det_Rule_ Oth_Lib*，分别存储各属性威胁所对应的规则知识；消息库所 *ReceivedMsg* 和 *A* 分别表示接收的消息和监测通过后发送的消息。变迁 *Detect* 用属性的监测规则函数将接收的消息属性和相关属性监测知识进行匹配。

### 3.2.2 Analyse 功能组件

Analyse 功能组件表示对监测后的消息作出记录、分析、判断和标记，即该组件判断是否有异常。分析是 SPCIS“智能学习”并“分析标记”消息的过程。

同 Detect，Analyse 功能组件相关定义如下：

**定义 9：分析规则库** 是分析功能组件依据的知识集合，记为 *Ana_Rule_Lib*。同样，定义 3 种属性分析规则库：*Ana_Rule_Lib* ={*Ana_Rule_In_Lib, Ana_Rule_Out_Lib,Ana_Rule_Oth_Lib*}，库所中的知识即为分析规则。

**定义 10：分析规则 *AnalyseRule*** 定义五元组 *AnalyseRule::=<*$ID_A$*,Attr_A,Equip_A,Rule_A,Time_A>*。

**定义 11：分析规则函数** 是分析功能组件执行分析行为的具体动作。同样有 *A_Rule_In*( )，*A_Rule_Out*( )和 *A_Rule_Oth*( )，分别记录和分析相应的消息属性，并标记结果。标记的消息用颜色集 *MsgTab* 定义。

**定义 12：标记消息 *MsgTab*** 定义四元组 *MsgTab::=<Attr_In_Tab,Attr_Out_Tab,Attr_Oth_Tab ,MsgCon>*，其元素分别表示经 Analyse 功能组件后各消息属性的标记信息。

在 CPN 模型中，分析规则函数定义在变迁的 Code Segments 中，或用替代变迁实现其功能。

构建的 Analyse 功能组件如图 3 所示。

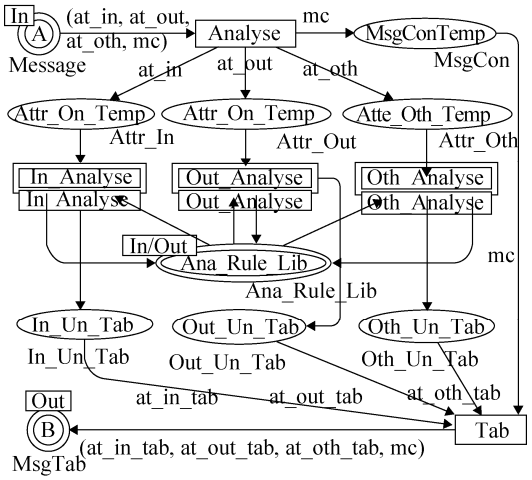


图 3 Analyse 功能组件
Fig. 3 Analyse component

库所 *A* 存储 Analyse 功能组件接收的消息，*B* 存储经过该功能组件转发的标记消息。该功能组件有两个功能：对本组件的分析知识规则库学习更新，以及对经过的消息属性分析标记。*Attr_In_Temp, Attr_Out_Temp,Attr_Oth_Temp* 3 个库所对经过 Analyse 功能组件的消息按属性分类和缓存；替代变迁 *In_Analyse,Out_Analyse*，*Oth_Analyse* 分别分析和标记消息的不同属性，并更新其对应的知识规则库。

图 4 是替代变迁 *In_Analyse* 的 CPN 模型，其他属性的模型同 *In_Analyse*。分析功能组件的三个分析知识库所 *Ana_Rule_In_Lib, Ana_Rule_Out_Lib, Ana_Rule_Oth_Lib* 分别存储消息不同属性的分析规则知识；库所 *In_Un_Tab,Out_Un_Tab,Oth_Un_ Tab* 分别存储消息属性的标记信息。

### 3.2.3 Respond 功能组件

Respond 功能组件表示对 Analyse 功能组件标记的消息按响应规则进行相关响应的过程。经响应功能组件的消息根据类型有正常和异常消息。响应

是 SPCIS 对标记后的异常消息“处理”和防护功能“实施”的过程。相应的定义为：

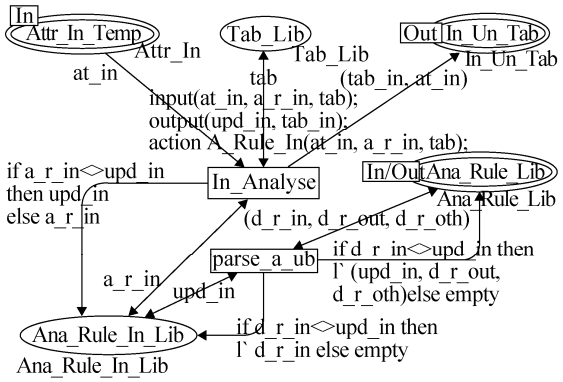


图 4 In_Analyse CPN 模型
Fig. 4 CPN model for In_Analyse

**定义 13: 响应规则库** 是响应功能组件依据的知识集合，记为 *Res_Rule_Lib*。同样有三种属性响应规则库 *Res_Rule_Lib*= {*Res_Rule_In_Lib, Res_Rule_Out_Lib,Res_Rule_Oth_Lib*}。

**定义 14: 响应规则 *RespondRule*** 定义五元组 *RespondRule::=<ID_R,Attr_R* ， *Equip_R,Rule_R* ， *Time_R>*。

**定义 15: 属性响应规则函数** 是响应功能组件对消息属性响应的具体行为。同样，定义 3 种属性响应规则函数：*R_Rule_In*( )，*R_Rule_Out*( )和 *R_Rule_Oth*( )，这里仅作出响应行为的标记，具体的响应由消息响应规则函数执行。

**定义 16: 消息响应规则函数** 是响应功能组件对消息响应行为的具体动作。这里定义两种函数 *R_Rule_M_J*( )和 *R_Rule_M_R*( )，分别表示对标记的属性信息进行综合判断以及对判断后的消息作出具体的响应。前者依据标记消息作出综合判断，后者则具体执行。如 *R_Rule_M_J*( )判断消息丢弃或转发，而 *R_Rule_M_R*( )则执行具体的诸如反向追踪、协作交互等防护功能。

构建的 Respond 功能组件如图 5 所示。响应功能组件完成两个功能：正常消息转发，异常消息处理。变迁 *judge_NE* 解析出正常和异常消息，库所 *NormalMsg* 存储正常消息，变迁 *Send_Nor* 完成转发；库所 *ExceptionMsg* 存储异常消息，替代变迁 *respond* 完成消息属性的响应。变迁 *execute* 中 Guard 函数 *R_Rule_M_J*( )完成异常消息属性的综合处理，Code Segements 中 *R_Rule_M_R*( )函数作出最终响应。替代变迁 *update* 和 *inquire* 共同完成知识库间的具体协作。

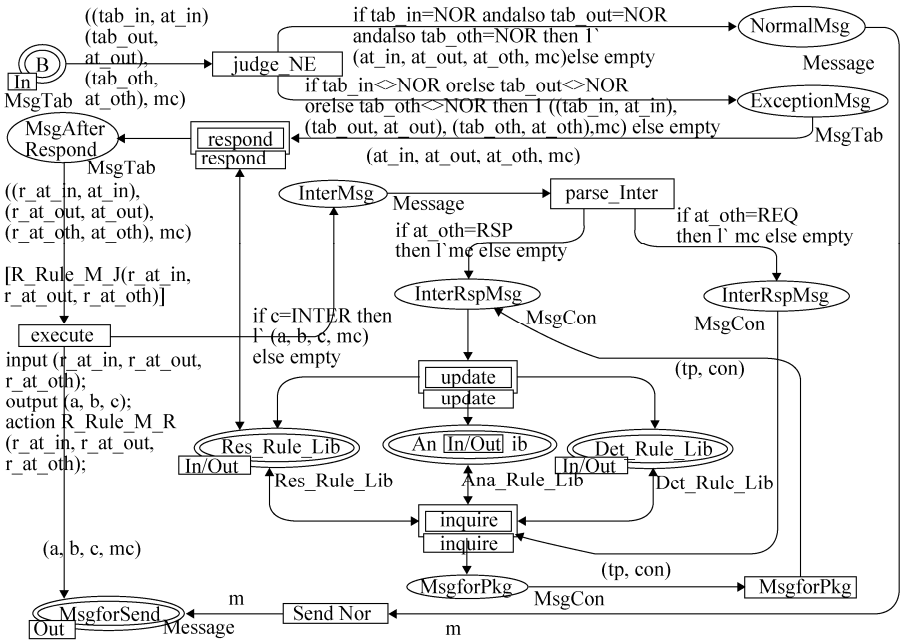


图 5 Respond 功能组件
Fig. 5 Respond component

根据建立的功能组件，基于 DAR 的 SPCIS 分析框架，构建 SPCIS 分析模型，如图 6 所示。

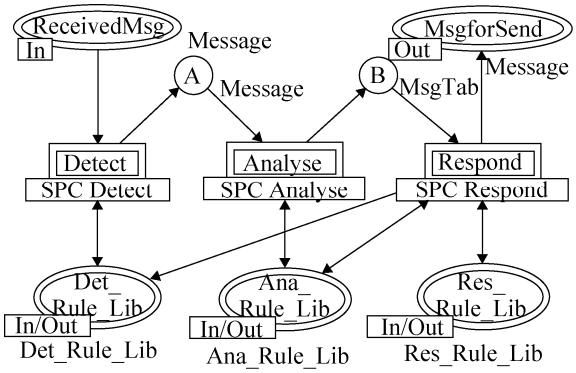


图 6 SPCIS 分析模型

Fig. 6 Analysis model for SPCIS

## 3.3 模型复杂度分析

Petri 网的可达图可穷尽 Petri 网的所有可能，故传统的 CPN 模型一般采用可达图分析。下边给出的定理表明本文建立的分析模型和功能组件在有限步仿真后一定进入死状态，且在死状态时的 SPCIS 为当前防护策略下的最优执行。

**定理 1.** 在特定时间段内，Detect、Analyse 和 Respond 功能组件在有限步仿真后一定进入死状态，并且有且仅有一个死状态，同时在死状态时其组件能力在该时段内分别得到了最优执行。

下面证明定理 1 中的 Detect 功能组件，Analyse 和 Respond 同理。

证明：在有限步仿真后，库所 *ReceivedMsg* 中的 *token* 终将被消耗，故该组件进入死状态；又该组件中不存在可能导致多个变迁竞争的库所，且 *ReceivedMsg* 中元素按时间顺序存储，因此只有一个死状态；又到达死状态时，该组件对 *ReceivedMsg* 中的 *token* 进行了所有可能的尝试，故此时监测能力是该时间段内执行最优的。

这里强调特定时段是必须的，因为库所 *Det_Rule_Lib* 中的 *token* 会随仿真运行而更新，所以对于库所 *ReceivedMsg* 中的同一组 *token*，Detect 在不同时段会得到不同的死状态，但在 *Det_Rule_Lib* 中的 *token* 未更新这一特定时段的死状态是一定的。

根据功能组件的建立过程知，该组件的任一库所均有界，因此组件对应的可达图节点数量均有限。该组件有两个变迁：变迁 *parse_d* 用来解析知识规则，设库所 *Det_Rule_Lib* 中 *token* 有 *m* 个，由于变迁 *parse_d* 不存在环路，所以最多经过 *m* 次，变迁 *parse_d* 进入非使能状态；同理，在变迁 *Detect* 中，设库所 *ReceivedMsg* 中的消息流 *token* 的平均数量为 *n*，则 *ReceivedMsg* 中的 *token* 最多经过 *n* 次将流向库所 *A* 或者被丢弃。所以该组件最多经过 $m+n$ 次进入死状态，又 *m*,*n* 为常数，故 Detect 组件的复杂度为 $O=(m+n)$。

同理，Analyse 和 Respond 组件的复杂度也为 $O=(m+n)$。

**定理 2.** 在特定时间段内，SPCIS 分析模型在有限步仿真后一定进入死状态，并且有且仅有一个死状态，且在死状态时 SPCIS 为当前防护策略下的执行最优。同时，存在消息 *M*，使得该消息在不同时段有不同的死状态。

证明：因为该分析模型由功能组件按一定顺序构成，上述已证明在特定时段内各功能组件必进入死状态，故构建的分析模型在有限步仿真后也一定进入死状态且唯一。下边证明存在消息 *M*，使得该消息在不同时段有不同的死状态：

假设分析模型的知识库初始状态为 $Lib_1$。由分析模型知，存在消息 $M_1$，使得 Analyse 组件中的智能学习功能在 $T_1$ 时被调用，因此存在消息 $M_2 \subseteq M_1$，使得 Respond 组件中的知识更新功能在 $T_2(T_2>T_1)$时被调用，故在 $T_3(T_3>T_2)$时可得到更新后的知识库，设为 $Lib_2$。

令消息 $M=M_1 \cap M_2$，在 $T_{21}$ 及知识库初始状态 $Lib_1$ 时，对消息 *M* 进行防护分析，由定理 2 前部分知在有限步仿真后一定进入死状态，记为 $S_1$，得到 $S_1$ 的时间设为 $T_{22}$，因智能学习和知识更新，知识库被更新，记为 $Lib_2$；在时间 $T_{23}(T_{23}>T_{22})$时对消息 *M* 进行同样的分析，记有限步仿真后进入的死状态为 $S_2$，而此时的 $S_2$ 是由知识库 $Lib_2$ 得到的，所以必然和 $S_1$ 不同。故得证。




DOI: 10.16182/j.issn1004731x.joss.201810013

# 4 仿真验证与分析

## 4.1 实例场景

图 7 所示的信息系统中：(1) 防火墙 Filter 3 将系统分为可信区、DMZ 和外网，而 Filter 1 和 Filter 2 分别对经过 DMZ 和可信区的事件按规则转发或过滤；(2) 入侵检测设备 Detector 1 和 Detector 2 分别分析经过 DMZ 和可信区的事件；(3) Investigator 1 和 Investigator 2 分别对检测出的异常响应。表 1~2 为该系统设备属性和通信规则。

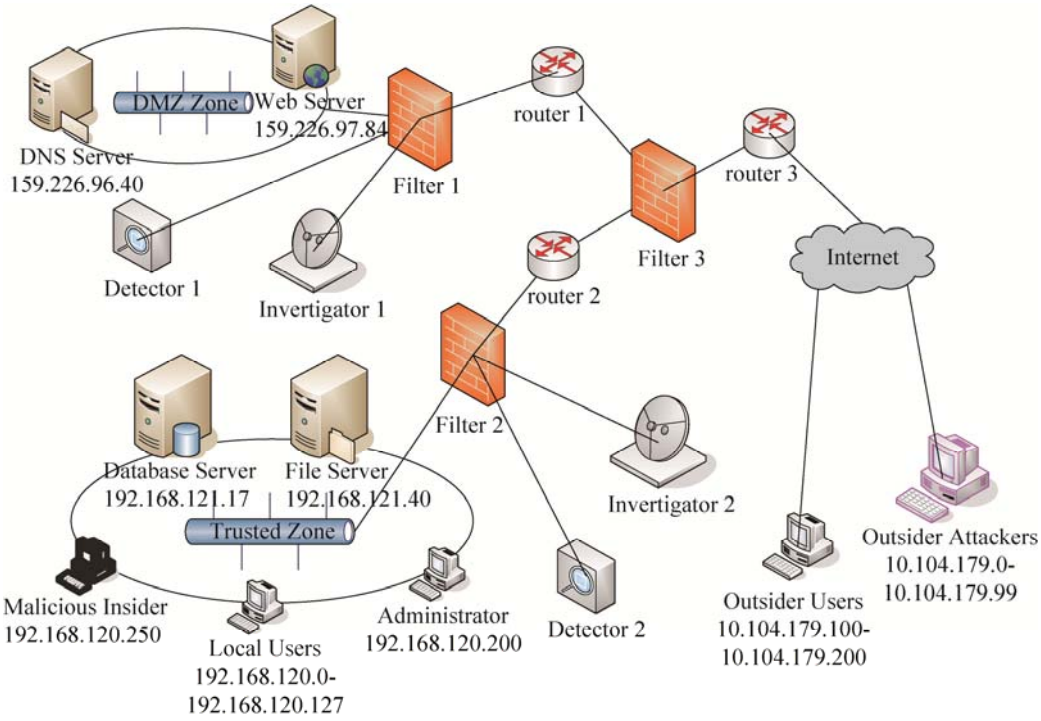


图 7　Web 信息系统
Fig. 7　Web information system

表 1　Web 信息系统设备属性表
Tab. 1　Web equipment attribute

| 通信实体 | 行为 |
|---|---|
| Local and Outsider Users | 向 Web 或 DNS Server 发请求消息 |
| Malicious Insider | 获取系统管理员权限并非法操作 |
| Outsider Attackers | 向攻击目的发送攻击信息 |
| WebServer | 响应请求并发送响应消息 |

表 2　Web 信息系统通信规则配置表
Tab. 2　Web communication rule configuration

| From | To |
|---|---|
| - | Web Server<br>DNS Server |
| Local Users, Web Serever and Administrator | Database Server<br>File Server |

根据 3.1 节消息建模分析可知，该系统中 Web Server 会受到 3 方面的安全威胁。本文建立的模型可为这 3 类威胁的分析和评估提供模型支撑，限于篇幅，本文只对外部攻击进行仿真验证。

设置 Outsider Attackers 对 Web Server 发起 DoS 攻击，用本文提出的方法建立该系统的 SPCIS 分析模型，通过分析该系统应对 DoS 攻击的过程验证本文所提模型的有效性。

## 4.2 模型构建

### 4.2.1 消息建模

因实例未考虑内部威胁，故根据该系统的业务功能，可按定义 6 给出该系统的消息定义：*Message::=<(SrcIP,SrcPort,DesIP,DesPort),(MsgID, MsgType),MsgCon>*。

式中 *SrcIP* 和 *SrcPort* 表示消息发送者的 IP 地址和端口号，*DesIP* 和 *DesPort* 表示接收者的 IP 地址和端口号；*MsgID* 表示消息的 ID，*MsgType* 表示消息的类型；*MsgCon* 表示消息负载内容。

其中，*MsgType* 定义为正常消息 NOR 和协作消息 INTER，具体取值如表 3 所示。*MsgCon* 进一步定义为 *MsgCon::=<Type,Content>*，*Type* 为消息负载内容的类型，*Content* 为具体内容。

表 3 消息类型
Tab. 3 Message type

| 序号 | 消息类型 | 符号表示 | 序号 | 消息类型 | 符号表示 |
|---|---|---|---|---|---|
| 1 | 业务消息 | NOR | 3 | 协作请求 | InterReq |
| 2 | 协作消息 | INTER | 4 | 协作回复 | InterRsp |

#### 4.2.2 功能建模

分析该系统的防护功能，对功能组件中的 3 类规则库、规则知识颜色集和规则函数用该系统的相关属性赋值，便得到该系统的 DAR 功能组件。该系统 DAR 功能组件中，除规则库、规则知识颜色集和规则函数与 3.2 节中各功能组件不同外，其他方面如工作原理和过程均相同，下面给出赋值的过程和其表示的具体物理意义。

对规则库赋值。由于实例只考虑 *Attr_Out*，故赋值 *Det_Rule_SI_Lib,Det_Rule_SP_Lib*，*Det_Rule_DI_Lib,Det_Rule_DP_Lib* 给属性监测规则库；赋值 *Ana_Rule_SI_Lib,Ana_Rule_SP_Lib*，*Ana_Rule_DI_Lib*，*Ana_Rule_DP_Lib* 给属性分析规则库；赋值 *Res_Rule_SI_Lib,Res_Rule_SP_Lib*，*Res_Rule_DI_Lib,Res_Rule_DP_Lib* 给属性响应规则库。这些属性规则库分别用来存储该系统消息 *SrcIP*，SrcPort，*DesIP*，*DesPort* 的属性监测、属性分析、属性响应规则知识。

对规则颜色集分别赋值。按定义 8 分别为：*DetectRule::=<$ID_D$,Attr_D,Equip_D,(Zone,Rule),Time_D>*，*Zone* 为规则所在区域，如 DMZ，Trusted Zone 和 Internet 外的区域；*Rule* 为具体规则，如 IP 地址或端口等。*AnalyseRule::=<$ID_A$,Attr_A,Equip_A,(Freq,MsgTime),Time_A>*，*Freq* 表示消息属性在时间 *MsgTime* 接收的频次。*RespondRule::=<$ID_R$,Attr_R,Equip_R,(Atk,Pro,Lib)Time_R>*，其中 *Atk* 为攻击类型，*Pro* 为该攻击的防护方式，*Lib* 为协作规则库(若无为空)。

对规则函数赋值。监测规则函数即表 2 中的通信规则，定义在指向库所 *A* 的输出弧上。分析规则函数在替代变迁 *SI_Analyse*，*SP_Analyse*，*DI_Analyse*，*DP_Analyse* 中，定义为在时间段 *SI_JCP* 内收到消息频次超过 *SI_CriPoint* 则认为攻击发生，则标记相应的属性。响应规则函数分别定义在替代变迁 *respond*，*update* 和 *inquire* 中。

最后，用已构建的该系统 DAR 功能组件，构建 Web 信息系统的 SPCIS 分析模型。

### 4.3 仿真验证

仿真配置：库所 *ReceivedMsg* 按表 4 所示发送消息包，仿真时间为 500 个时间单位，通过 CPN tools 中 Monitor 统计库所 *MsgForSend* 在仿真时间内接收的消息包数量。

表 5 所示为 3 组测试中各规则知识颜色集。表 3 里 Business 1 和 Business 2 为仿真测试的业务消息，Attack 为攻击消息，并按表中时间以相应速率发送消息包。表 5 分别表示各规则知识颜色集，其物理意义见 4.2.2 节规则颜色集赋值。

得到库所 *ReceivedMsg* 发包速率(单位时间内发送消息的数量，如图中 Sender)和 *MsgForSend* 的收包速率(单位时间收到消息的数量，如图中 Receiver)如图 8 所示。

Test 1 中不设置攻击，图 8 中 Test1 显示，接收包速率由 0 开始上升，并在 5 时刻达到 55 左右，并保持至仿真结束。这表明 Business 2 的消息包被过滤，因为 Outsider Users 无权访问 Trusted Zone 中的 Database Server，故被 Filter3 过滤，从而可验证 Detect 功能组件的有效性。

Test 2 设置攻击，攻击时刻为 200~300，且 *Ana_Rule_Lib* 中规则为空。图 8 中 Test 2 显示，在

208 时刻接收包速率急剧上升，并保持 100 左右达 100 个时间单位，至 307 时刻才回到 55 左右。这是因为分析规则为空，故对接收的异常消息不作分析和标记，故接收包和发送包速率基本一致。

Test 3 中，防护设置同 Test 1，攻击设置同 Test 2。图 8 中 Test 3 显示，在 253 时刻前同 Test 2，而在 253 时刻接收包速率就回到正常水平。这是因为在测试中入侵检测设备通过智能学习发现攻击并作了标记，并在攻击未结束前更新了监测规则库和响应规则库，从而及时地阻断了攻击消息。

所以，Test 2 和 Test 3 的结果可验证 Analyse 和 Respond 智能学习和防护协作功能的有效性。

表 4 仿真测试设置表

Tab. 4 Simulation test settings

| | | Business 1 | Business 2 | Attack |
|---|---|---|---|---|
| Test 1 | DesIP | 192.168.121.17 | | - |
| | SrcIP | 192.168.120.0-127 | 10.104.179.100-200 | - |
| | 速率 | 55 | 45 | - |
| | 时间 | (0，500) | | - |
| Test 2 | DesIP | 159.226.97.84 | | |
| | SrcIP | 192.168.120.0-127 | - | 10.104.179.99 |
| | 速率 | 55 | - | 45 |
| | 时间 | (0，500) | - | (200，300) |
| Test 3 | DesIP | 159.226.97.84 | | |
| | SrcIP | 192.168.120.0-127 | - | 10.104.179.99 |
| | 速率 | 55 | - | 45 |
| | 时间 | (0，500) | - | (200，300) |

表 5 规则库知识设置表

Tab. 5 Knowledge of rule library settings

| | Test 1 | Test 3 | Test 2 |
|---|---|---|---|
| Det_Rule_Lib | 1`(1,"DI","Filter3",("DMZ","159.226.96.40"),0)++<br>1`(2,"DI","Filter3",("DMZ","159.226.97.84"),0)++<br>1`(3,"DI","Filter3",("TRZ","192.168.121.40"),0)++<br>1`(4,"DI","Filter3",("TRZ","192.168.121.17"),0)++<br>1`(5,"SI","Filter3",("INT"," "),0)++<br>1`(6,"SI","Filter3",("TRZ","192.168.120.*"),0) | | |
| Ana_Rule_Lib | 1`(1,"SI","Detector*",(225,5),0)++<br>1`(2,"SP","Detector*",(225,5),0)++<br>1`(3,"DI","Detector*",(225,5),0)++<br>1`(4,"DP","Detector*",(225,5),0) | | —— |
| Res_Rule_Lib | 1`(1,"SI","Investigator*",("DoS","Update","D"),0)++<br>1`(2,"SP","Investigator*",("DoS","Inquire","D"),0)++<br>1`(3,"DI","Investigator*",("DoS","Update","R"),0)++<br>1`(4,"DP","Investigator*",("DoS","Update","R"),0) | | |

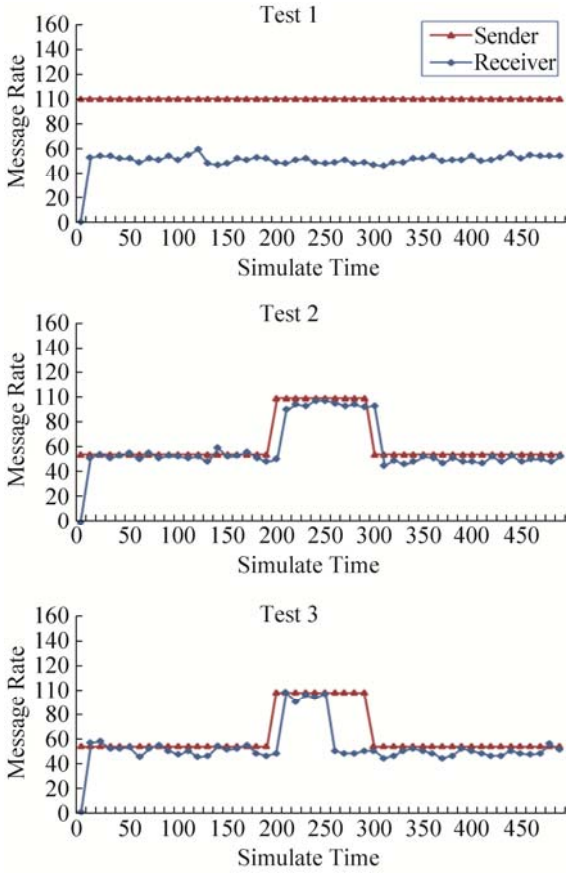


图 8 仿真测试结果图
Fig. 8 Simulation test results

### 4.4 模型分析

实际上在仿真开始前，可基于 CPN tools 中的数据监视器对模型中的库所和变迁设置监视器，以实时收集仿真数据，从而为 SPCIS 后续的分析和评估提供过程数据。仿真结束后，由 3.4 节的定理知，进入死状态时的 SPCIS 为当前防护策略下的最优，故通过采集死状态时库所中的 *token*，可用来分析和评估执行最优时的安全防护策略。与传统方法相比，本文方法具有以下优势：

文献[9]中建立的终端信息流、传输、过滤和转换功能 CPN 模型适用于给定的网络拓扑，当网络拓扑变化时，需要重新分析网络拓扑来构建模型，而本文方法通过抽象事件属性和防护规则，便可快速构建分析模型，具有较好的通用性。

针对某一脆弱性的攻击会随着技术的成熟衍生出多种攻击方法，传统的建模方法[4-7]往往需要重新分析攻击原理，再建立分析模型，而本文方法可通过扩展消息的相关属性和防护规则，并调整规则函数来建立分析模型，具有良好的扩展性。

文献[7]攻击者能力分析模型中，威胁代理和脆弱性利用 CPN 模型是在给定脆弱性下的分析，且不能描述攻击者的交互作用，而本文方法除了可分析已给定的脆弱性，还能通过智能学习和自我更新描述 SPCIS 的协同防护，从而可进一步分析 SPCIS 的协作交互，具有良好的可分析性。

同时，为说明本文构建的 CPN 模型具有较高的分析效率，本文定量对比了相关文献建立的模型复杂度，如表 6 所示。

表 6 模型复杂度对比
Tab. 6 Comparability of model complexity

| 模型 | 复杂度 | 说明 |
|---|---|---|
| 文献[7] | $O=\left((k\times n+p)\times m\times n\right)$ | $k,n,p,m$ 均为常数 |
| 文献[19] | $S_{com}=\lvert F\rvert/\lvert A\rvert$ | $\lvert F\rvert$为有向弧数目<br>$\lvert A\rvert$为原子攻击数 |
| 本文 | $O=(m+n)$ | $m$ 为规则数<br>$n$ 为消息数 |

通过定量对比可知，文献[7]中建立的攻击者能力 CPN 模型，和文献[19]中基于广义随机 CPN 的网络攻击组合模型复杂度均为非线性阶，而本文构建的 CPN 分析模型复杂度为线性阶，从而具有较高的分析效率。

## 5 结论

本文结合现阶段 SPCIS 分析和建模的易通用、可扩展和可分析需求，提出了基于 DAR 的概念框架，并利用 CPN 建立了分析模型。最后，仿真实验验证了所构建模型的有效性；模型分析对比说明了本文方法的优越性；同时还可通过设置并收集仿真开始前后的数据，为 SPCIS 的分析和评估提供模型和数据支撑。

本文方法是按 SPCIS 的防护功能和原理来建模，而不对具体的设备建模，从而一定程度上避免了复杂系统中大量设备的建模问题，但同时会因为


https://dc-china-simulation.researchcommons.org/journal/vol30/iss10/13
DOI: 10.16182/j.issn1004731x.joss.201810013

大量的设备使得构建的模型功能可能不够精确，并且抽象建模过程相对困难，下一步将在模型应用过程中进一步优化建模方法。

## 参考文献:

[1] 360 互联网安全中心. 2015 年中国互联网安全报告 [EB/OL]. (2016-02-29)[ 2016-09-06]. http://www.360.cn/weishi/2015_sr.html.
360 Center for Internet Security: 2015 Chinese Internet Security Report [EB/OL]. (2016-02-29) [2016-09-06] http://www. 360.cn/weishi/2015_sr.html.

[2] Nayot Poolsappasit, Rinku Dewri, Indrajit Ray. Dynamic Security Risk Management Using Bayesian Attack Graphs [J]. IEEE Transactions on Dependable and Secure Computing (S1941-0018), 2012, 9(1): 61-74.

[3] 万雪莲, 张京河. 基于攻、防的信息系统安全综合评估方法的研究 [J]. 计算机科学, 2016, 43(S1): 322-327.
Wan Xuelian, Zhang Jinghe. Research on Comprehensive Assessment Method of Information System Security Based on System Attack and Defense [J]. Computer Science, 2016, 43(S1): 322-327.

[4] 戴方芳. 基于攻击图理论的网络安全风险评估技术研究 [D]. 北京: 北京邮电大学, 2015.
Dai Fangfang. Research on Network Security Risk Assessment Technology Based on Attack Graph Theory [D]. Beijing, China: Beijing University of Posts and Telecommunications, 2015.

[5] 高翔, 刘洋, 贺筱媛. 基于 GSCPN 模型的网络安全加固措施制定方法 [J]. 系统仿真学报 (S1004-731X), 2016, 28(5): 1009-1016.
Gao Xiang, Liu Yang, He Xiaoyuan. Method for Network Security Reinforcement Based on GSCPN Model [J]. Journal of System Simulation (S1004-731X), 2016, 28(5): 1009-1016.

[6] You Y, Cho I, Lee K. An advanced approach to security measurement system [J]. The Journal of Supercomputing (S0920-8542), 2016, 72(9): 3443-3454.

[7] 吴迪, 冯登国, 连一峰, 等. 一种给定脆弱性环境下的安全措施效用评估模型 [J]. 软件学报, 2012, 23(7): 1880-1898.
Wu Di, Feng Dengguo, Lian Yifeng, et al. An efficiency evaluation model of system security measures in the given vulnerabilities set [J]. Journal of Software, 2012, 23(7): 1880-1898.

[8] Roland Rieke. Modelling and Analysing Network Security Policies in a Given Vulnerability Setting [M]// Critical Information Infrastructures Security. Germany: Springer Berlin Heidelberg, 2006: 67-78.

[9] Laborde R, Nasser B, Grasset F. A formal approach for the evaluation of network security mechanisms based on RBAC policies [J]. Electronic Notes in Theoretical Computer Science (S1571-0661), 2005, 121(0): 117-142.

[10] Laborde R, Nasser B, Grasset F, et al. Network security management: A formal evaluation tool based on RBAC policies [M]// Network Control and Engineering for QoS, Security and Mobility, III. USA: Springer US, 2005: 69-80.

[11] 陈小军, 时金桥, 徐菲, 等. 面向内部威胁的最优安全策略算法研究 [J].计算机研究与发展, 2014, 51(7): 1565-1577.
Chen Xiaojun, Shi Jinqiao, Xu Fei, et al. Algorithm of Optimal Security Hardening Measures Against Insider Threat [J]. Journal of Computer Research and Development, 2014, 51(7): 1565-1577.

[12] 李志, 单洪, 马春来, 等. 基于攻防图的网络主动防御策略选取研究 [J]. 计算机应用研究, 2015, 32(12): 3729-3734.
Li Zhi, Shan Hong, Ma Chunlai. Network active defense strategy selection based on attack-defense graph [J]. Application Research of Computers, 2015, 32(12): 3729-3734.

[13] Feng, Nan, Wang, et al. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis [J]. Information Sciences (S0020-0255), 2014, 256(1): 57-73.

[14] Ghani H, Luna J, Suri N. Quantitative assessment of software vulnerabilities based on economic-driven security metrics [C]// Risks and Security of Internet and Systems (CRiSIS), 2013 International Conference on. USA: IEEE, 2013: 1-8.

[15] 吕慧颖, 彭武, 王瑞梅, 等. 基于时空关联分析的网络实时威胁识别与评估 [J]. 计算机研究与发展, 2014, 51(5): 1039-1049.
Lü Huiying, Peng Wu, Wang Ruimei, et al. A Real-time Network Threat Recognition and Assessment Method Based on Association Analysis of Time and Space [J]. Journal of Computer Research and Development, 2014, 51(5): 1039-1049.

[16] 张恒巍, 张健, 王晋东, 等. 基于连通度算子的系统漏洞风险评估 [J]. 计算机工程与设计, 2015, 36(1): 65-70.
Zhang Hengwei, Zhang Jian, Wang Jindong, et al. System vulnerability risk evaluation based on connectivity operator [J]. Computer Engineering and Design, 2015, 36(1): 65-70.

(下转第 3716 页)