一种基于广义随机着色 Petri 网的网络攻击组合模型

高 翔* 祝跃飞 刘胜利
(解放军信息工程大学数学工程与先进计算国家重点实验室 郑州 450002)

摘 要：攻击行为建模对网络安全分析与评估具有重要的作用。该文定义了一种基于广义随机着色Petri网的网络攻击组合模型，该模型能清晰表达攻击组合中各组合部分之间的关联关系，给出了攻击行为、攻击组合运算的定义和攻击组合的建立算法，并对组合模型的结构复杂度进行了度量。在此基础上，从系统性能分析的角度对时间代价进行评估。针对网络实例的分析进一步验证了所提出的组合模型及相关计算方法的有效性。

关键词：Petri 网；攻击组合；建模；时间代价
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2013)11-2608-07
DOI: 10.3724/SP.J.1146.2013.00090

Attack Composition Model Based on Generalized Stochastic Colored Petri Nets

Gao Xiang Zhu Yue-fei Liu Sheng-li
(*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: Attack modeling plays an important role in network security analysis and assessment. A Generalized Stochastic Colored Petri Net (GSCPN) model for attack composition is proposed. To each attack, a GSCPN model is constructed to describe the relation of components graphically. Operators to construct attack composition from known ones as blocks are defined formally. The algorithm to construct a composite attack is delivered, and the structural complexity of combination model is measured also. On this basis, the time cost of vulnerabilities is assessed. The network example validates further the effectiveness of the proposed composition model and calculation method.

Key words: Petri net; Attack composition; Modeling; Time cost

1 引言

随着计算机网络的飞速发展，以及大规模、分布式高速网络的被大量的应用，人们对网络的依赖性在不断增加，随之而来的信息安全问题变得尤为突出，不断增长和扩散的计算机病毒和黑客攻击等对广大用户和企业造成了不可估量的损失。因此，面对各种网络威胁，必须采取有效措施来保证计算机网络的安全运行。传统的被动型安全防御技术(入侵检测、防火墙以及用户认证等)已不能满足人们的需要，国内外学者纷纷致力于研究主动的安全分析与评估方法，而网络攻击建模是网络安全评估和全面建立安全防御措施的基础。

目前，在网络攻击的建模方面已取得了一些成果。常见的模型有有限状态机[1]、攻击图模型[2]、脆弱性状态图[3]、威胁传播模型[4]，博弈模型[5]，从不同角度分析和评估系统安全，反映了攻击者和网络系统的状态变化，但这些模型表达能力不足，针对组合式网络攻击，大多欠缺对并发性和协作性攻击过程的描述能力。相比之下，Petri 网是基于图形的数学建模工具，具有语义规范、表达能力强等特点，更利于网络攻击过程的描述。吴迪等人[6]应用有色 Petri 网为系统业务数据流、攻击流等要素建立模型，并且使用层次评价模型评估系统安全措施的效用，但该模型无法评价系统的相关性能。Wang 等人[7]提出了基于随机 Petri 网和博弈模型的网络攻防量化分析方法，可以对攻击成功率、潜在攻击路径等方面进行分析和评价，但是该方法不适于分析并发性攻击行为。

另外，目前基于模型对网络进行安全评估大多采用分析攻击序列成功概率的方法[6–8]，其缺点是计算最大入侵成功概率容易使得分析结果极端化，如果存在概率设置下不合理的情况，将会使分析结果出现很大的偏差。所以研究人员尝试从攻防代价角度对网络安全进行分析。如冯萍慧等人[3]引入可靠

2013-01-18 收到，2013-06-09 改回
国家自然科学基金(60902102, 61272489)和郑州市科技创新团队项目(10CXTD150)资助课题
*通信作者：高翔 feiyu4321@163.com

性原理，从利用成本的角度对攻击代价进行评估。Jiang 等人[9]给出了比较完整的攻防成本敏感模型，有效地应用于网络主动防御中。这些研究成果给了本文研究很大的启发。

针对上述问题，本文给出了一种结合广义随机Petri网[10]和着色Petri网[11]的广义随机着色Petri网(Generalized Stochastic Colored Petri Net, GSCPN)模型，该模型能够清晰表达攻击组合的组成逻辑及明确描述攻击行为之间的关联关系，特别是对并发性和协作性攻击，可用着色Petri网的颜色集来表示攻击相关属性，模型构造方法相对简单。另外，基于随机Petri网评价系统的性能，对网络系统的安全性进行量化评估。这里，特别引入广义随机Petri网，它是随机Petri网的一种扩充，主要表现在将变迁分为瞬时变迁和时间变迁，更适于对网络攻击行为建模。

2　攻击组合模型

2.1 基本概念

定义 1　广义随机着色 Petri 网是一个 9 元组 $\mathrm{GSCPN}=(\Sigma,P,T,F,C,G,E,\lambda,M_0,I)$。其中：$\Sigma$ 是一组有限非空数据类型的集合，又称为颜色集；P 是有限库所集；T 是有限变迁集，$T=T_t\cup T_i$，$T_t\cap T_i=\phi$，T_t 表示时间变迁集合，T_i 表示瞬时变迁集合；F 是有限弧集，$F\subseteq P\times T\cup T\times P$，且弧仅存在于 P 和 T 之间；C 是颜色函数集，$C:P\to\Sigma$；G 是条件函数的集合，$G:T\to$ BoolExpression，表示变迁到变迁表达式的映射函数，满足：$\forall t\in T:[\mathrm{Type}(G(t))=\mathrm{Boolean}\wedge\mathrm{Type}(\mathrm{Var}(G(t)))\subseteq\Sigma]$；$E$ 是弧函数的集合，$E:F\to FE$，FE 为弧表达式，满足：

$$\forall f\in F:[\mathrm{Type}(E(f))=C(p)_{MS}\wedge\mathrm{Type}(\mathrm{Var},(E(f)))\subseteq\Sigma]$$

$C(p)_{MS}$ 表示 $C(p)$ 上的多重集的集合；λ 是时间变迁的平均实施速率或瞬时冲突变迁之间优先级集合；M 是标识集合，常用 M_0 表示初始标识，代表攻击开始的位置。I 为初始化函数，$I:P\to\Sigma$ 为每个库所赋初始颜色。

上述定义中，$\mathrm{Type}(x)$ 函数表示 x 的值的类型，Boolean 表示布尔类型，其值为 True 或 False，$\mathrm{Var}(x)$ 函数表示 x 为一个变量。

定义 2　Σ (颜色集)定义为

颜色　Host = string；

颜色　Vul = string；

颜色　AttackCons = SrcHost* DstHost* Vul* Perms；

颜色　SrcHost = Host；

颜色　DstHost = Host；

颜色　Perms={anonymous, guest, root/admin}；

颜色　AttackRes={root access, crash, confident, compromised…}；

颜色　Conditions = BoolExpression；

颜色　Boolean = {true, false}。

其中，攻击条件 AttackCons 由源主机 SrcHost、目的主机 DstHost、攻击利用漏洞 Vul 和攻击发起时用户权限 Perms 组成。其中，用户权限 Perms 由匿名 anonymous，授权用户 guest，超级用户 root/admin 组成。攻击结果 AttackRes 由获得主机 root 访问权限(root access)、被攻陷(compromised)、瘫痪(crash)等组成。Conditions 是布尔表达式类型，用来表示攻击行为需要的条件。Boolean 则表示逻辑常量 true 和 false。

定义 3　攻击行为是一个 11 元组 $\mathrm{Attack}=(\Sigma,P,p^i,p^o,T,F,C,G,E,\lambda,I)$，其中 $\Sigma,P,T,F,C,G,E,\lambda,I$ 的含义与定义 1 相同，$p^i\in P$ 是输入库所，其前集为空；$p^o\in P$ 是输出库所，其后集为空。当 Attack 表示原子攻击行为时，库所集 $p=\{p^i,p^o\}$。p^i 表示攻击者发起时所在的设备的名称以及状态，p^o 表示在实行攻击行为后可能所处的位置和状态。$T=T_t\cup T_i$，其中，T_t 是时间变迁，代表攻击行为的变迁集合。本文假设攻击行为服从指数分布。

为描述方便，可将攻击行为划分为原子攻击和组合攻击两类。图 1 表示了一个原子攻击行为模型。变迁 t 表示攻击行为，攻击行为的平均实施速率在图中没有标识。

定义 4　如果攻击者在实施了攻击行为 A 后，能够使用新获得的攻击资源，继续实施攻击行为 B，那么我们就说攻击行为 A 到攻击行为 B 存在关联性。这里的攻击行为 A 和 B 可以针对同一台主机，也可以是不同主机。

定义 5　不依赖其它攻击行为，且可单独实施的攻击行为称为原子攻击；通过关联关系调用其它攻击行为，完成自身目标的攻击行为称为组合攻击。

2.2 攻击组合运算及时间代价分析

原子攻击可构造成组合攻击，组合攻击又可作

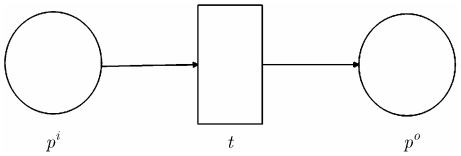

图 1 原子攻击行为模型

为攻击构造成更复杂的攻击。根据关联关系，将多个攻击行为组合为一个攻击的组合方式称为攻击行为的运算。

定义 $1/\lambda = E(C)$ 为攻击成功所花费时间代价的期望值，可以用平均攻击时间(Average Time of Attack, ATA)表示攻击者成功利用系统脆弱性达到目标所需花费时间代价的期望。这里借鉴工作流模型时间性能分析的结果[12]，通过计算组合运算的 $1/\lambda$ 来评估攻击成功所需代价，瞬时变迁的延迟时间可以忽略不计。在攻击过程中，若原子攻击行为 A 发生了 n 次，且存在时间序列 $\{X_t, t \in n\}$，则攻击行为的平均实施时间可以通过式(1)进行求解。

$$\frac{1}{\lambda_i} = \overline{X} = \frac{1}{n}\sum_{t=1}^{n} X_t \tag{1}$$

原子攻击行为之间通过顺序、并发、选择运算构成组合攻击。攻击行为组合可按如下方法进行形式化定义：

$$A ::= (A \cdot A) \,|\, (A \,||\, A) \,|\, (A \oplus A)$$

式中 A 表示攻击行为，“$\cdot$”表示顺序运算，$||$ 表示并发运算，$\oplus$ 表示选择运算。

设有两个攻击行为 $A_1 = (\Sigma_1, P_1, p_1^i, p_1^o, T_1, F_1, C_1, G_1, E_1, \lambda_1, I_1)$ 和 $A_2 = (\Sigma_2, P_2, p_2^i, p_2^o, o_2, T_2, F_2, C_2, G_2, E_2, \lambda_2, I_2)$。

2.2.1 顺序运算 图 2 中的攻击由攻击行为 A_1 和 A_2 经过顺序运算组合而成，瞬时变迁 t_c 的作用是连接前后两个攻击行为。时间变迁 t_1 和 t_2 的攻击平均实施速率分别为 λ_1 和 λ_2。

$A = A_1 \cdot A_2 = (\Sigma, P, p^i, p^o, T, F, C, G, E, \lambda, I)$，其中“$\cdot$”为攻击行为组合的顺序运算符，顺序运算的平均攻击时间为

$$\mathrm{ATA}^{\mathrm{seq}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} \tag{2}$$

这里由攻击行为 $A_1, A_2, \cdots, A_n$ 经过顺序运算组合而成的攻击，时间变迁 $t_1, t_2, \cdots, t_n$ 的攻击平均实施速率分别为 $\lambda_1, \lambda_2, \cdots, \lambda_n$，该组合攻击的平均攻击时间为

$$\mathrm{ATA}^{\mathrm{seq}} = \sum_{i=1}^{n} \frac{1}{\lambda_i} \tag{3}$$

2.2.2 并发运算 图 3 中的攻击由攻击行为 A_1 和 A_2 经过并发运算组合而成，库所 p^i 和 p^o 分别是组合攻击的输入和输出库所。瞬时变迁 t_i 的作用是依据输入生成攻击行为 A_1 和 A_2 的初始条件，瞬时变迁 t_o 的作用是汇总 A_1 和 A_2 输出生成总输出结果。时间变迁 t_1 和 t_2 的攻击平均实施速率分别为 λ_1 和 λ_2。

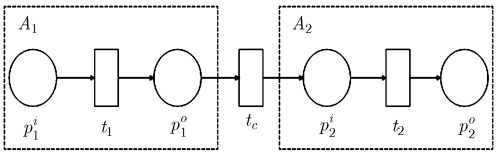

图 2 攻击行为的顺序运算

$A = A_1 \,||\, A_2 = (\Sigma, P, p^i, p^o, T, F, C, G, E, \lambda, I)$，其中 $||$ 为攻击行为组合的并发运算符，并发运算的平均攻击时间为

$$\mathrm{ATA}^{\mathrm{con}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \tag{4}$$

这里由攻击行为 $A_1, A_2, \cdots, A_n$ 经过并发运算组合而成的攻击，时间变迁 $t_1, t_2, \cdots, t_n$ 的攻击平均实施速率分别为 $\lambda_1, \lambda_2, \cdots, \lambda_n$，该组合攻击的平均攻击时间为

$$\begin{aligned}\mathrm{ATA}^{\mathrm{con}} = &\sum_{i=1}^{n}\frac{1}{\lambda_i} - \sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\frac{1}{\lambda_i + \lambda_j} \\ &+ \sum_{i=1}^{n-2}\sum_{j=i+1}^{n-1}\sum_{k=j+1}^{n}\frac{1}{\lambda_i + \lambda_j + \lambda_k} \\ &+ \cdots + (-1)^{n-1}\frac{1}{\sum_{i}^{n}\lambda_i}\end{aligned} \tag{5}$$

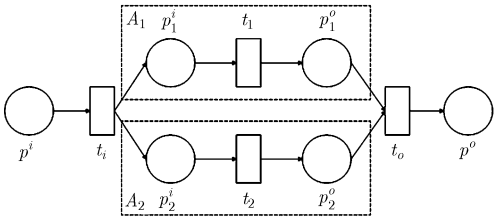

图 3 攻击行为的并发运算

2.2.3 选择运算 图 4 的攻击由攻击行为 A_1 和 A_2 经过选择运算组合而成，库所 p^i 和 p^o 分别是组合攻击的输入和输出库所，瞬时变迁 $t_{i1}, t_{i2}, t_{o1}, t_{o2}$ 的作用是将输入库所的标记传输到输出库所，其中引发 t_{i1}, t_{i2} 的概率分别为 $\alpha, 1-\alpha$。时间变迁 t_1 和 t_2 的攻击平均实施速率分别为 λ_1 和 λ_2。

$A = A_1 \oplus A_2 = (\Sigma, P, p^i, p^o, T, F, C, G, E, \lambda, I)$，其中 $\oplus$ 为攻击行为组合的选择运算符，选择运算的平均攻击时间为

$$\mathrm{ATA}^{\mathrm{sel}} = \frac{\alpha}{\lambda_1} + \frac{1-\alpha}{\lambda_2} \tag{6}$$

这里由攻击行为 $A_1, A_2, \cdots, A_n$ 经过选择运算组合而成的攻击，时间变迁 $t_1, t_2, \cdots, t_n$ 的攻击平均实施速率分别为 $\lambda_1, \lambda_2, \cdots, \lambda_n$，该组合攻击的平均攻击时间为

$$\mathrm{ATA}^{\mathrm{sel}} = \sum_{i=1}^{n} \frac{\alpha_i}{\lambda_i} \tag{7}$$

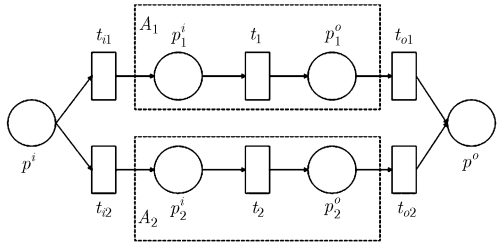

图 4 攻击行为的选择运算

以上 3 种组合运算时间计算公式的证明过程可参考文献[12]，则任何一个组合攻击的总平均攻击时间可以表示为

$$\mathrm{ATA}^{\mathrm{sum}}=\sum_{i=1}^{n}\mathrm{ATA}_i^{\mathrm{seq}}+\sum_{j=1}^{n}\mathrm{ATA}_j^{\mathrm{con}}+\sum_{\mathrm{k}=1}^{\mathrm{n}}\mathrm{ATA}_k^{\mathrm{sel}} \quad (8)$$

2.3 攻击组合模型构建

将需要解决的问题划分成若干个部分，针对各个部分进行详细的分析和建模，之后再组合各个部分。这样既减小了建模的难度，也便于实现。构建组合模型的基本思想为：

(1)收集网络中存在弱点的设备信息，包括主机的漏洞信息和服务信息等；收集网络中设备的连接关系。

(2)对每一个构成组合攻击的原子攻击行为，生成原子模型，并严格定义变迁发生时需要的条件。

(3)定义网络系统的初始状态，并从初始状态出发，根据网络信息以及攻击行为之间的关联关系，用顺序、并发、选择 3 种运算来描述组合攻击流程。其中，攻击行为之间的关联关系可通过关联关系挖掘算法获得。

(4)利用模型的相关性质，或引入层次化思想，使用复合变迁表示一个原子攻击行为或者组合攻击，对模型进行化简达到降低复杂度的目的。

(5)验证模型的有效性，如用可达树来进行验证[13]，若不正确，则修改上述图形模型。

在实际应用中，如果网络规模过大或者较复杂时，会遇到结点数过多的问题，为了减少状态的空间，可引入层次化思想，用一个复合变迁表示一个原子攻击行为或者组合攻击。上述 3 种组合运算多次组合而成的攻击行为都可以通过分层用图 1 的简单结构来表示，具体等价化简过程可参考文献[12]中的方法。

攻击行为关联关系挖掘算法描述如下所示。其中， AS 表示攻击行为集合，集合中的元素 A_m 为原子攻击行为； REL 表示攻击行为关联关系集合，$\mathrm{REL}=(\mathrm{ASS},E,\mathrm{LAS})$，其中， ASS 为有序列关系的攻击行为集合， E 为连接两个原子攻击行为的边集合，LAS(last attacks) 为最近一次加入的攻击行为集合， REL.ASS , REL.E , REL.LAS 的初值均为空集； First 和 Second 为两个队列，初值也为空。

算法　攻击行为关联关系挖掘算法

输入： 攻击行为集合 AS

输出： 攻击行为关联关系集合 REL

步骤 1　遍历集合 AS，将初始 $M_0(p_m^i)=1$ 的攻击行为 A_m 放入队列 First，其余的放入队列 Second；

步骤 2　分析队列 First 第 m 个元素 A_m 与队列 Second 第 n 个元素 A_n 之间的关系，若 A_m 为 A_n 发生的前提条件， 则 $\mathrm{REL.ASS}=\mathrm{REL.ASS}\cup\{A_n\}$ ，$\mathrm{REL}.E=\mathrm{REL}.E\cup\{(A_m,A_n)\}$ ， $\mathrm{REL.LA}=\mathrm{REL.LA}\cup\{A_n\}$；

步骤 3　对于 REL 中 LAS 的每一个元素 LA_r，分析 LA_r 与队列 Second 中元素 $A_k(A_k\notin\mathrm{REL.ASS})$ 之间的关系，若 LA_r 为 A_k 发生的前提条件，则 $\mathrm{REL.ASS}=\mathrm{REL.ASS}\cup\{A_k\}$ ， $\mathrm{REL}.E=\mathrm{REL}.E\cup\{(\mathrm{LA}_r,A_k)\}$；否则，转入步骤 4；

步骤 4　算法结束。

2.4 模型的结构复杂度度量

引入面向对象的设计度量相关思想对组合模型的 3 种组成结构进行复杂度度量，这里可以将由一个输入库所、一个输出库所和一个时间变迁组成的原子攻击行为抽象为一个模块。组合模型的结构复杂度 S_{com} 可以表示为

$$S_{\mathrm{com}}=|F|/|A| \quad (9)$$

其中 F 为模型中的流关系，$|F|$ 为模型中有向弧的数目。 A 为原子攻击行为，$|A|$ 为原子攻击 A 中元素的数量。

在图 2 中，$|F|=6$, $|A|=3$，顺序运算的结构复杂度为 $S_{\text{com-seq}}=2$。

在图 3 中，$|F|=10$, $|A|=3$，并发运算的结构复杂度为 $S_{\text{com-seq}}=10/3$。

在图 4 中，$|F|=12$, $|A|=3$，选择运算的结构复杂度为 $S_{\text{com-seq}}=4$。

从以上分析可知，攻击组合模型中选择运算的结构复杂度最高，并且可以得出结论：在一定的系统规模范围内，有向弧的数量变化是影响模型结构复杂性的主要因素，因此降低有向弧数量是优化模型的有效途径，可以通过 2.3 节中提到的层次化思想减少有向弧数量。

3　实验结果

3.1 实验环境

为了验证前面所提出的网络攻击组合模型，根据林肯实验室提供的 2000 DARPA 评估数据集[14]构造了一个实验网络环境，网络拓扑结构如图 5 所

示。该数据集提供了两个攻击场景 LLDOS 1.0 和 LLDOS 2.0.2，其中，攻击场景 LLDOS 1.0 包括 5 个攻击阶段：第 1 阶段：攻击者预探测网络，对网络进行 IP 扫描，产生了大量的 echo 请求和回应包。第 2 阶段：攻击者实施 sadmind 漏洞查寻。第 3 阶段：攻击者多次尝试 sadmind 缓冲区溢出攻击，通过 sadmind 漏洞分别闯入主机(mill, locke, pascal)。第 4 阶段：攻击者分别对主机(mill, locke, pascal)安装 mstream DDoS 木马软件。第 5 阶段：向目标主机 www.af.mil 实施 DDoS 攻击。

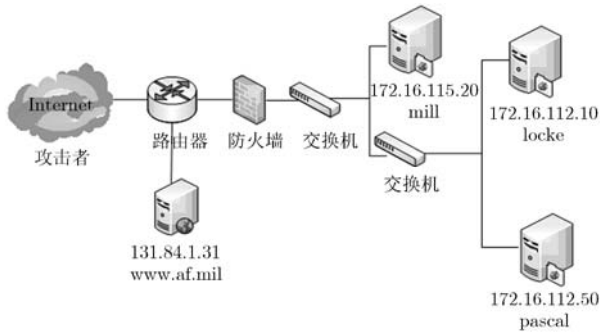

图 5 网络拓扑图

实验网络中主机的漏洞和服务信息如表 1 所示。

3.2 系统建模与结构复杂度度量

假设 $A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9$ 是原子攻击行为，分别代表预探测网络、sadmind 漏洞查寻、通过漏洞闯入主机(mill, locke, pascal)、主机(mill, locke, pascal)被安装木马软件、对目标主机实施 DDoS 攻击。组合后的目标攻击为 $A=(A_1\cdot A_2\cdot (A_3 \,||\, A_4 \,||\, A_5)(A_6 \,||\, A_7 \,||\, A_8)\cdot A_9)$，攻击场景 LLDOS 1.0 可用图 6 表示，*符号表示各个网段上存在的主机。另外，为了图形显示的简洁，我们略去了图中一些弧上的弧函数以及变迁的 G 函数。

表 1 网络主机相关信息

	网络主机	mill	locke	pascal	www.af.mil
漏洞信息	ICMP 配置不当	√	√	√	×
	sunrpc 配置不当	√	√	√	×
	Sadmind 缓冲溢出漏洞	√	√	√	×
	rcp 配置不当	√	√	√	×
	SYN Flood 漏洞	√	√	√	×
服务信息	http	×	√	√	√
	ftp	√	√	√	×
	telnet	√	√	√	×

注：√符号表示主机具有该漏洞或服务，×符号表示主机不具有该漏洞或服务。

如图 6 所示，p_1^i 表示准备预探测网络；p_1^o 表示完成预探测网络；p_2^i 表示准备 sadmind 漏洞查寻；p_2^o 表示完成漏洞查寻；p_3^i, p_4^i, p_5^i 表示准备对主机(mill, locke, pascal)进行 sadmind 缓冲区溢出攻击；p_3^o, p_4^o, p_5^o 表示攻击者进入主机(mill, locke, pascal)并获取 root 权限；p_6^i, p_7^i, p_8^i 表示准备对主机(mill, locke, pascal)安装木马软件；p_6^o, p_7^o, p_8^o 表示攻击者进入主机(mill, locke, pascal)并完成木马安装；p_9^i 表示攻击者处于主机 mill，准备对主机 locke 和 pascal 发送指令共同实施 DDoS 攻击；p_9^o 表示完成攻击。瞬时变迁 t_a, t_b, t_c, t_d 的作用是连接前后两个攻击行为，瞬时变迁 t_e 表示返回初始状态，时间变迁 $t_1 - t_9$ 对应的攻击平均实施速率分别为 $\lambda_1 - \lambda_9$。其中，t_1 表示 IP Sweep 攻击；t_2 表示 Sadmind Ping 攻击；t_3, t_4, t_5 表示 Sadmind Exploit 攻击；t_6, t_7, t_8 表示 DDoS Software 安装完毕；t_9 表示 DDoS 攻击。

根据式(9)，在攻击场景LLDOS 1.0的攻击组合模型中，$|F|=36$，$|A|=3$，因此，该模型的结构复杂度为 $S_{\text{com}}=12$。这里，为了清晰展示整个组合攻击过程，所以不对模型的结构复杂度进行优化。

另外，通过构造该模型的可达树，可以验证该模型是正确和有效的。

3.3 实验结果与分析

据上述时间代价的计算方法，可得该广义随机着色 Petri 网描述图对应的平均攻击时间公式为

$$\begin{aligned}\text{ATA}^{\text{sum}} = &\frac{1}{\lambda_1}+\frac{1}{\lambda_2}+\left(\frac{1}{\lambda_3}+\frac{1}{\lambda_4}+\frac{1}{\lambda_5}-\frac{1}{\lambda_3+\lambda_4}\right.\\ &\left.-\frac{1}{\lambda_3+\lambda_5}-\frac{1}{\lambda_4+\lambda_5}+\frac{1}{\lambda_3+\lambda_4+\lambda_5}\right)\\ &+\left(\frac{1}{\lambda_6}+\frac{1}{\lambda_7}+\frac{1}{\lambda_8}-\frac{1}{\lambda_6+\lambda_7}-\frac{1}{\lambda_6+\lambda_8}\right.\\ &\left.-\frac{1}{\lambda_7+\lambda_8}+\frac{1}{\lambda_6+\lambda_7+\lambda_8}\right)+\frac{1}{\lambda_9}\end{aligned}$$

根据式(1)，由相关领域专家依据数据集[14]估算，可得时间变迁 $t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9$ 的平均攻击时间分别为 $\frac{1}{\lambda_1}=12.875$ s，$\frac{1}{\lambda_2}=0.305$ s，$\frac{1}{\lambda_3}=2.041$ s，$\frac{1}{\lambda_4}=2.047$ s，$\frac{1}{\lambda_5}=2.048$ s，$\frac{1}{\lambda_6}=1.778$ s，$\frac{1}{\lambda_7}=1.713$ s，$\frac{1}{\lambda_8}=1.007$ s，$\frac{1}{\lambda_9}=5.302$ s。

代入上述公式，最终得到该组合攻击的平均攻击时间为 $\text{ATA}^{\text{sum}}=25.047$ s。

使用随机 Petri 网仿真软件(PIPE2.5[15])提供的

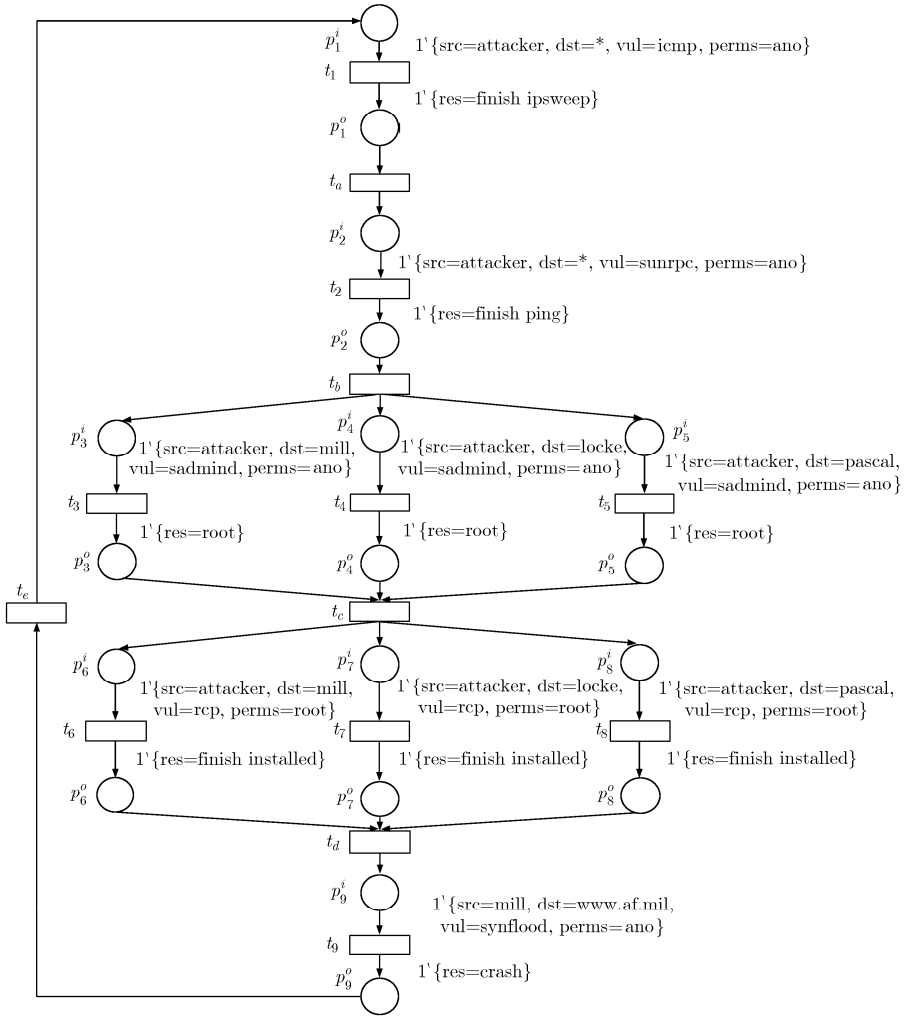

图 6　攻击场景 LLDOS 1.0 的攻击组合模型

基于稳定状态概率的方法求得的平均执行时间为 25.459，两者差别很小。传统的基于马尔可夫链的性能分析方法[16]具有指数时间复杂性，而本文采用的时间性能近似分析方法具有线性时间复杂度，计算方法简单，更具有实际应用价值。表 2 给出了几种网络安全评估模型的比较。

可见，本文所描述的网络攻击组合模型，适于对并发性和协作性攻击建模，能够清晰表示网络中攻击行为的各种属性和类型。另外，可根据组合运算对攻击组合的平均攻击时间 ATA 进行估算，从而为网络脆弱性量化评估提供了可行的方案。

4　结论

本文提出了一种基于广义随机有色 Petri 网的网络攻击组合模型，定义了几种攻击组合运算，并给出了攻击组合的构造算法以及模型结构复杂度的

表 2　几种评估模型的比较

评估模型	形式语义	攻击行为描述	并发性攻击行为建模	系统性能分析
有限状态机[1]	严格	一般	不适合	不可以
Attack Graph[2]	一般	一般	不适合	不可以
脆弱性状态图[3]	一般	一般	适合	不可以
威胁传播模型[4]	一般	一般	不适合	不可以
博弈模型[5]	严格	一般	不适合	不可以
本文的模型	严格	较好	适合	可以

分析方法。组合模型具有描述并发性和协作性攻击过程的能力，能够清晰表达攻击行为之间的关联关系，构造方法相对简单，同时可根据时间代价对网络系统的脆弱性程度进行量化分析，对网络系统安全性的增强提供了理论依据。实验结果表明，本文提出的组合模型及相关计算方法是有效可行的。

参 考 文 献

[1] Porras P A and Kemmerer R A. Penetration state transition analysis: a rule-based intrusion detection approach[C]. Proceedings of the Eighth Annual Computer Security Applications Conference, San Antonio, USA, 1992: 220–229.

[2] Wang Shu-zhen, Zhang Zong-hua, and Kadobayashi Youki. Exploring attack graph for cost-benefit security hardening: a probabilistic approach[J]. *Computers & Security*, 2013, 32(2): 158–169.

[3] 冯萍慧, 连一峰, 戴英侠, 等. 面向网络系统的脆弱性利用成本估算模型[J]. 计算机学报, 2006, 29(8): 1375–1381.
Feng Ping-hui, Lian Yi-feng, Dai Ying-xia, *et al*.. An evaluation model of vulnerability exploitation cost for network system[J]. *Chinese Journal of Computers*, 2006, 29(8): 1375–1381.

[4] 陈锋, 刘德辉, 张怡, 等. 基于威胁传播模型的层次化网络安全评估方法[J]. 计算机研究与发展, 2011, 48(6): 945–954.
Chen Feng, Liu De-hui, Zhang Yi, *et al*.. A hierarchical evaluation approach for network security based on threat spread model[J]. *Journal of Computer Research and Development*, 2011, 48(6): 945–954.

[5] Liang Xian-nuan and Xiao Yang. Game theory for network security[J]. *IEEE Communications Surveys & Tutorials*, 2013, 15(1): 472–486.

[6] 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 Deng-guo, Lian Yi-feng, *et al*.. Efficiency evaluation model of system security measures in the given vulnerabilities set[J]. *Journal of Software*, 2012, 23(7): 1880–1898.

[7] Wang Yuan-zhuo, Yu Min , Li Jing-yuan , *et al*.. Stochastic game net and applications in security analysis for enterprise network[J]. *International Journal of Information Security*, 2012, 11(1): 41–52.

[8] 王永杰, 鲜明, 刘进, 等. 基于攻击图模型的网络安全评估研究[J]. 通信学报, 2007, 28(3): 29–34.
Wang Yong-jie, Xian Ming, Liu Jin, *et al*.. Study of network security evaluation based on attack graph model[J]. *Journal on Communications*, 2007, 28(3): 29–34.

[9] Jiang Wei, Zhang Hong-li, Tian Zhi-hong, *et al*.. A game theoretic method for decision and analysis of the optimal active defense strategy[C]. Proceedings of International Conference on Computational Intelligence and Security, Harbin, China, 2007: 819–823.

[10] Chiola G, Marsan M A, Balbo G, *et al*.. Generalized stochastic Petri nets: a definition at the net level and its implications[J]. *IEEE Transactions on Software Engineering*, 1993, 19(2): 89–107.

[11] Jensen K. Coloured Petri Nets: Basic Concepts Analysis Methods and Practical Use[M]. Berlin: Springer-Verlag, 1997, Vol. 1: 234–240.

[12] 林闯, 曲杨, 郑波, 等. 一种随机 Petri 网性能等价化简与分析方法[J]. 电子学报, 2002, 30(11): 1620–1623.
Lin Chuang, Qu Yang, Zheng Bo, *et al*.. An approach to performance equivalent simplification and analysis of stochastic petri nets[J]. *Acta Electronica Sinica*, 2002, 30(11): 1620–1623.

[13] Barylska K, Mikulski L, and Ochmanski E. On persistent reachability in Petri nets[J]. *Information and Computation*, 2013, 223(1): 67–77.

[14] MIT Lincoln Lab. 2000 DARPA Intrusion Detection Scenario Specific Datasets[OL]. http://www.ll.mit.edu/ IST/ ideval/ data/2000/2000_data_index.html. 2012.10.

[15] Dingle N J, Knottenbelt W J, and Suto T. PIPE2: a tool for the performance evaluation of generalized stochastic Petri nets[J]. *ACM SIGMETRICS Performance Evaluation Review*, 2009, 36(4): 34–39.

[16] Ferscha A. Business workflow analysis using generalized stochastic petri nets[C]. Proceedings of 9th Austrian-Hungarian Informatics Conferencn, Linz, Austria, 1994: 222–234.

高 翔： 男，1984 年生，博士生，研究方向为形式化建模与验证、网络与信息安全.

祝跃飞： 男，1962 年生，教授，博士生导师，研究方向为应用数学、网络与信息安全.

刘胜利： 男，1973 年生，副教授，硕士生导师，研究方向为网络与信息安全.