文章编号:1000-582X(2011)04-118-07

CPN 攻击建模及警报相关性算法设计

杜建军,吴中福,陈 明
(重庆大学 计算机学院,重庆 400044)

摘 要:为提高当前入侵检测系统的预警质量和分析预测能力,用染色 Petri 网(colored petri net, CPN)构造了攻击模型,系统性地设计了警报信息相关性分析算法。通过把"警报"和"攻击"作为 2 个不同实体参与模型运算,将目前主要采用的过滤观察信息为基础的关联方法提升为信息推理的演算方法。应用 CPN 模型转换、极小覆盖集命题等方法,对本领域中的难点问题即复合攻击、合作攻击进行了理论分析和算法设计。在此基础上开发了警报信息相关性分析(alerts correlation analysis system, ACAS)实验系统,实验结果表明算法系统对于提高入侵检测系统的警报质量和分析预测能力是可行、有效的。

关键词:入侵检测;染色 Petri 网;攻击建模;警报相关性;合作攻击
中图分类号:TP393 **文献标志码**:A

Attack modeling using colored petri net and alerts correlation algorithms design

DU Jian-jun, WU Zhong-fu, CHEN Ming
(College of Computer Science and Engineering, Chongqing University, Chongqing 400044, P. R. China)

Abstract: In order to improve the alerts quality and prediction capability of traditional intrusion detection systems (IDS), the advanced alerts correlation algorithms are proposed, which is based on attack scenarios modeling using colored petri net (CPN). The current analysis approach information filtering is updated to messages logic deduction by reasoning under the model. The alert and the attack are converted to two different parameters for computation. By means of transforming CPN model and calculating the minimal covering set, the algorithms for multi-step attack and cooperative attack are designed. The experimental alerts correlation analysis system (ACAS) is programmed. That experiment results indicate that these algorithms could be applied to improve the alerts quality and prediction ability of IDS effectively.

Key words: intrusion detection; petri net application; attack modeling; alerts correlation; cooperative attack

伴随互联网应用的高速发展,入侵检测在网络安全中的作用日益突出。入侵检测主要包括基于检测对象正常行为统计结果的异常检测和捕捉已知攻击和系统漏洞的误用检测等。目前的研究主要致力于 2 个方面:1)提高受网络位置差异、潜在误用敏感等严重影响的而只有 1%正确攻击预警的警报[1]质量,即减少大量误报、重复报和漏报。这类研究以相似度、序列性等指标采用过滤模型的方法寻找"真

收稿日期:2010-09-10
基金项目:国家科技支撑计划资助项目(2008BAH37B04)
作者简介:杜建军(1974-),男,重庆大学博士研究生,主要从事计算机安全、网络应用及计算机体系研究,(Tel)67778319;(E-mail)dujianjun@cqu.edu.cn。

实”警报，如法国的 Cuppens[2]、美国爱达荷州立大学的 Deborah[3]等均采用这种方法。2)针对入侵过程的复杂性、多样性和分布性，从大量基础攻击的单一检测警报信息中提取、分析攻击间逻辑关系进而掌握入侵规律提高检测、预报能力。有以北卡罗莱纳大学计算机防御实验室[4]、斯坦福国际系统设计实验室[5]等为代表根据攻击间依赖关系建立的原因关联法和以时间戳、目的地址等建立相似特征的聚类关联法。这些方法在计算量、关联可信度及对未知攻击的检测方面还待进一步完善。

近年蓬勃发展的 Petri 网对离散、并行事件具有很强的描述能力，能很好地建立攻击模型。染色 Petri 网(colored petri net，CPN)是在 Petri 网基础上发展出的高级网系统，引入染色概念来描述多种不同性质的资源。当前主要出现的应用 Petri 网进行入侵检测的研究[3-8]从逻辑上没有摆脱传统过滤型模型的限制，其主要目的仍在追求警报信息过滤规则的匹配。用一种全新的角度处理警报信息：将“警报”和“攻击”作为 2 个不同运算实体参与模型计算，力求通过警报信息推理出实际攻击的发生，进而提高警报质量和分析预测能力。在此基础上对该领域难点的复合攻击、合作攻击进行了探讨和算法设计，开发了警报信息相关性分析 ACAS 实验系统。

1　CPN 攻击建模及工作原理

1.1　模型参数

研究中所用 CPN 模型是 1 个 11 元组：$\mathrm{CPN}=(\sum,Q,D,A,O,G,E,\prod_0,Z,\Gamma,\Xi)$，其中：

$\sum=\{c_i \mid i=1,\cdots,N_c\}$ 颜色集合，是标识(token)即攻击源的非空有限集；

$Q=\{q_i \mid i=1,\cdots,N_q\}$ 库所集合，是 1 个有限状态集合表示被攻击资源；

$D=\{d_i \mid i=1,\cdots,N_d\}$ 变迁集合，是可发生事件即攻击事件的有限集；

$A=A_1\cup A_2$ 是弧集，其中 $A_1\subseteq(Q\times D)$ 表示变迁的前集的弧集，$A_2\subseteq(D\times Q)$ 表示变迁后集的弧集。用 $I(d)$ 来表示变迁 d 的前集及弧 $<q,d>\in A_1$，(d) 表示变迁 d 的后集及弧 $<d,q>\in A_2$；

$O=\{o_i \mid i=1,\cdots,N_o\}$ 观察信息即警报的集合；

$G=\{g:A_1\rightarrow S_{M(\sum)}\}$ 是弧集 A_1 相关联的函数集合，表示变迁发生的条件限制，$S_{M(\sum)}$ 是多重集 $M(\sum)$ 的超集；

$E=\{e:A_2\rightarrow S_{M(\sum)}\}$ 是弧集 A_2 相关联的函数集合，表示变迁发生后对资源的占有状况；

$\prod_0=P_0(Q,S_{M(\sum)})=\{\pi:(Q,S_{M(\sum)})\rightarrow[0,1]\}$ 表示初始时标识对资源的占有率；

$\Delta=\{P(d\in D \text{ will fire next} \mid d \text{ is enabled})\}=\{z:D\rightarrow[0,1]\}$，$Z$ 是变迁的前集条件满足后(使能)变迁发生的概率集

$\Gamma=P(O\mid D)=\{\gamma:(O,D)\rightarrow[0,1]\}$ 表示变迁发生能被观察到的概率集；

Ξ 是状态转换的阈值函数；

1.2　建立攻击模型

利用经典的 local-to-root(L2R)攻击场景[9]来说明如何通过 CPN 建立攻击模型。

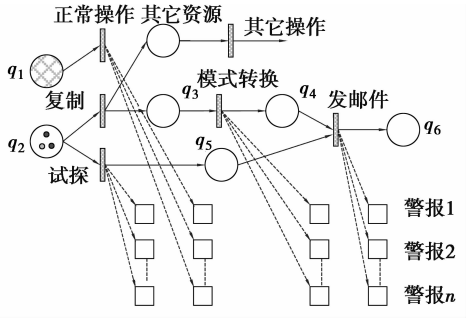

图 1　L2R 攻击 CPN 模型

如图 1，L2R 攻击场景由 copy、chmod、touch 和 mail4 个攻击事件组成，normal 表示合法操作。q_1 代表所有标识都可以访问的资源，如 mail 事件的发生就必须具有 q_4 和 q_5 库所中资源的权限，当某标识完成 mail 攻击事件后，就具有了 q_6 的资源能力。每个攻击事件的发生都可能被 IDS 的感应器鉴别为不同警报 alert 1 to n，计算的目的就是收到 IDS 的警报信息后进行反向推导，实际发生的 L2R 攻击在模型中必然存在一条完整的通路。

CPN 模型为每个标识赋予了 1 个资源占有的概率值，在描述攻击步骤、警报信息和实际攻击发生时是相对独立的。过滤型模型是在警报和攻击间采取逐条类比、匹配的关联，而 CPN 用 1 个观察概率 Γ 来表示事件发生后能被警报信息正确发布的概率，Γ 是 1 个包含误报率、漏报率的统计值。模型将在当前数据状态下结合 CPN 的变迁发生条件、概率及 Γ 推导出“攻击”的发生，进而判定是否更新模型状态。如果观察层改为如下定义

$$P(o_i \mid d_j)=\begin{cases}1, i=j,\\ 0, \text{otherwise}。\end{cases}$$

表示警报和攻击事件在逻辑上具有一致性，并且 $\Delta=1$ 即攻击事件的前集条件满足后必然发生，那么 CPN 模型就与一般的过滤型方法类似了。所以采用 CPN 模型是过滤型方法的超集，同时具有了更强的推理能力。

2 警报信息相关性算法系统

2.1 警报分析系统构造算法

应用CPN建模构成的警报分析系统有1个初始状态 $\prod_0$，算法核心思想是：①针对每条警报，系统首先需要确定代表该攻击事件的变迁，然后根据警报中的信息与当前模型参数推理出该变迁实际发生的可能性；②如果表示攻击事件的变迁发生的可能性值超过设定阈值即确认了该攻击事件的实际发生，系统在预警的同时动态更新相应CPN模型参数至 $\prod_t$。本节算法中省略了标识 c，即算法的对象是同一性质的标识。

1个攻击事件即变迁是使能的当且仅当它的前集条件都已满足，这是Petri网的基本假设，也与攻击必须具备特定资源的条件是一致的。用式(1)来计算在 t 时刻变迁 d 使能的概率。显然，前集条件没有满足的变迁其值为0。

$$P(E(d) \mid \prod_t) = P(\text{disenabled} \mid \prod_t) = P\Big(\bigwedge_{q\in I(d)}(\prod_t(q) \geqslant G(a=(q,d)))\Big) \approx \prod_{q\in I(d)} P(\prod_t(q) \geqslant G(a=(q,d))) = \prod_{q\in I(d)} \pi_t(q)。 \tag{1}$$

状态 $\prod_t$ 下，1个变迁使能后可能发生的概率用式(2)来计算。同1个标识在同一时刻可能具有触发多个变迁的能力，但是变迁之间具有相对独立性。

$$\delta_t(d) = P(D=d \mid \prod_t) = P(d \text{ will firenext} \mid E(d))P(E(d) \mid \prod_t) = z(d)\prod_{q\in I(d)} \pi_t(q)。 \tag{2}$$

1个库所 q 中某标识即攻击源 c 具有了该资源的能力当且仅当标识 c 已经获得了该资源或者包含标识 c 的变迁确实发生且 q 属于该变迁的后集。用式(3)来计算在没有报警信息的条件下标识 c 具有资源 q 的概率。

$$P(\{(q,c)\} \leqslant M_t \mid S_{t-1}) \approx 1-(1-\pi_{t-1}(q))\cdot\prod_{q\in O(d)}(1-\delta_t(d))。 \tag{3}$$

引入观察集 O_t 后，在 t 时刻收到1条警报信息，系统状态为 $\prod_{t-1}$，用式(4)计算该警报事件相关变迁实际发生的可能性。

$$P(D_t=d \mid S_{t-1},O_t) = \frac{P(D_t=d,O_t \mid S_{t-1})}{P(O_t \mid S_{t-1})} = \frac{P(D_t=d \mid S_{t-1})P(O_t \mid D_t=d,S_{t-1})}{P(O_t \mid S_{t-1})}。 \tag{4}$$

由于 $P(D_t=d|S_{t-1})=\delta_{t-1}(d)$，并且 O_t 仅仅依赖于 D_t，式(4)可改写为

$$\frac{\delta_{t-1}(d)P(O_t \mid D_t=d)}{P(O_t \mid S_{t-1})} = \frac{\delta_{t-1}(d)\gamma_t(O_t \mid d)}{\sum_{d'\in D}\delta_{t-1}(d')\gamma_t(O_t \mid d')} = \frac{\delta_{t-1}(d)\gamma(O_t \mid d)}{\sum_{d'\in D}\delta_{t-1}(d')\gamma(O_t \mid d')}。 \tag{5}$$

式(5)中，d' 表示所有警报信息中与变迁 d 相关的事件，包括正确与误报为 d 的事件。

t 时刻收到一条警报信息，系统状态为 $\prod_{t-1}$，在完成对该警报事件的推理计算后，用式(6)和(7)计算系统更新后的状态 $\prod_t$。

$$P(\{(q\in O(d),c)\} \leqslant M_t \mid S_{t-1},O_t,D_t=d) \approx 1-(1-\pi_{t-1}(q))\times\left(1-\frac{\delta_{t-1}(d)\gamma(O_t \mid d)}{\sum_{d'\in D}\delta_{t-1}(d')\gamma(O_t \mid d')}\prod_{q'\in O(d)}\pi_{t-1}(q')\right)。 \tag{6}$$

$$P(\{(q\notin O(d),c)\} \leqslant M_t \mid S_{t-1},O_t,D_t=d) = \pi_{t-1}(q\notin O(d))。 \tag{7}$$

系统的初始化过程需依次读入已有的IDS观察(警报)信息和Petri网模型参数。$N_o=|O|$ 表示读入的观察信息总和，则系统初始化的算法时间复杂度为 $O(N_o)$。系统运行过程中，每接收到一条新的IDS警报信息，先进行事件(变迁)匹配，其时间复杂度为 $O(N_d)$，$N_d=|D|$ 为变迁总和。匹配后根据变迁参数和前集条件计算该警报实际发生概率进而选择更新系统状态，其总的算法时间复杂度概括为 $O(\max(Q_d \cup M_d))$，其中 $Q_d=\{q_0,q_1,\cdots q_{d-1}\}$ 是各变迁前集条件(库所)数量的集合，$M_d=\{m_0,m_1,\cdots m_{d-1}\}$ 是各变迁后集库所数量的集合。由于攻击模型建立时变迁及库所条件的数量都不大，所以相关性算法具有很高的效率。

2.2 模型参数评估

参数评估的目标是在已知警报信息 $O_1,O_2,\cdots,O_t$ 的条件下，计算。1)变迁的前集条件满足后该变迁发生的概率 z；2)变迁发生能被观察到的概率 γ。2个参数都是IDS的性质，计算域是全集而非特定标识，计算结果作为模型参数输入系统。

γ 的计算采用最大相似度原则[10]，其定义 $\gamma(o|d)$ 为

$$L(\gamma,d) = \sum_i \ln(P(O_i \mid \gamma,d)) = \sum_{O_i=o}\ln\gamma + \sum_{O_i\neq o}\ln(1-\gamma) = N\ln\gamma + L\ln(1-\gamma), \tag{8}$$

式(8)中，N 是变迁发生IDS预警的次数，而 L 是未发布警报的次数，可以推导出式(9)，即 γ 代表

了 IDS 正确预警的频率。

$$\frac{\partial L(\gamma,d)}{\partial \gamma}=\frac{N}{\gamma}-\frac{L}{1-\gamma}=0\Rightarrow$$
$$(N+L)\gamma=N\Rightarrow \tag{9}$$
$$\gamma=\frac{N}{(N+L)}。$$

z 的计算采用求最大期望的方法[11]，其定义 $z=z(d)$ 为

$$L(z)=\sum_i \ln(P(D_i\mid z,E_i(d)))=$$
$$\sum_{D_i=d}\ln(z\cdot E_i(d))+\sum_{D_i\neq d}\ln(1-z\cdot E_i(d)), \tag{10}$$

式(10)中，$E_i(d)$ 表示变迁 d 在 i 步使能的概率，可推导出

$$\frac{\partial L(z)}{\partial z}=\sum_{D_i=d}\frac{1}{z}-\sum_{D_i\neq d}\frac{E_i(d)}{1-z\cdot E_i(d)}=0\Rightarrow$$
$$z=\frac{N}{\sum_{D_i\neq d}\frac{E_i(d)}{1-z\cdot E_i(d)}}。 \tag{11}$$

式(11)中 N 是变迁发生的次数，结合计算 $E_i(d)$ 的式(1)通过叠代收敛可求解出 z。

2.3　警报分析系统结构

图 2 是应用 CPN 建模的警报相关性分析系统结构，如不进行虚线标注的“系统学习”，即当前状态直接等于 $\prod_0$ 而未进行过任何的推理运算，其初始工作状态就近似于过滤性模型。系统接收从 IDS 发布的警报信息进行运算，输出最后经系统确认的警报和预测分析信息。

3　复合、合作攻击算法设计

3.1　复合攻击算法

现实中攻击大多数是由许多具时间、空间跨度的分散行为构成的复合攻击[12]。算法对于复合攻击的推导目标是：用 CPN 建模并在模型状态参数 λ 下，对于 1 个警报事件序列 $O=O_1,O_2,\cdots,O_t$，怎样的变迁发生序列 $D=D_1,D_2,\cdots,D_t$ 最大可能导致该警报序列的产生，其数学描述为

$$\max_D[P(D\mid O,\lambda)]=\max_D\left[\frac{P(O\mid D,\lambda)P(D\mid\lambda)}{P(O\mid\lambda)}\right]。 \tag{12}$$

由于观察概率 $P(O|\lambda)$ 与变迁集合 D 不相关，所以式(12)的最优解等价于式(13)的最优解。

$$\max_D[P(O\mid D,\lambda)P(D\mid\lambda)]=\max_D P(O,D\mid\lambda)。 \tag{13}$$

为动态计算该值定义 $\omega_t(j)$：对于 1 个长度为 t 的警报序列，结束事件为 j 且事件序列长度为 t 的最优解，即

$$\omega_t(j)=\max_{D_1\cdots D_{t-1}}P(O_1,\cdots,O_t,D_1,\cdots,D_{t-1},D_t=j\mid\lambda)。 \tag{14}$$

那么式(14)即是求最优的 $\omega_t(j)$

$$\max_D P(O,D\mid\lambda)=\max_j\omega_t(j)=$$
$$\max_j\max_{D_1\cdots D_{t-1}}(O_1,\cdots,O_t,D_1,\cdots D_{t-1},D_t=j\mid\lambda)。 \tag{15}$$

对 $\omega_t(j)$ 建立递推公式为

$$\omega_t(j)=\max_{D_1\cdots D_{t-1}}P(O_1,\cdots,O_t,D_1,\cdots D_{t-1},D_t=j\mid\lambda)=$$
$$\max_{D_1\cdots D_{t-1}}[P(O_1,\cdots O_t,D1,\cdots D_{t-1}\mid\lambda)\cdot$$
$$P(D_t=j\mid S_{t-1},\lambda)P(O_t\mid D_t=j,\lambda)]=$$
$$\max_{D_{t-1}=i}[\max_{D_1\cdots D_{t-2}}P(O_1,\cdots,O_{t-1},D_1,\cdots,D_{t-1}=$$
$$i\mid\lambda)\cdot P(D_t=j\mid S_{t-1},\lambda)P(O_t\mid D_t=j,\lambda)]\approx$$
$$\max_{D_{t-1}=i}[\omega_{t-1}(i)\delta^i_{t-1}(j)\gamma(O_t\mid j)], \tag{16}$$

式(16)中：$\delta^i_{t-1}(j)\approx P(D_t=j\mid S'_{t-1},\lambda)$，$S'_{t-1}$ 是与 $\omega_{t-1}(i)$ 相对应的系统状态。由 $\omega_t(j)$ 的递推公式可以发现，在计算 $[\omega_{t-1}(i)\delta^i_{t-1}(j)\gamma(O_t\mid j)]$ 时必须对所有的事件 N_d 和所有的警报信息 N_o 进行计算，从中挑选出最优解，即该算法的时间复杂度是 $O(N_d^2\cdot N_o)$。由于攻击事件类型的相对集中，有很多事件的观察概率 $\gamma(O_t\mid j)$ 都非常小，可以设定一个阈值来去掉这些计算，时间复杂度可降为 $O(N_d\cdot N_o)$。

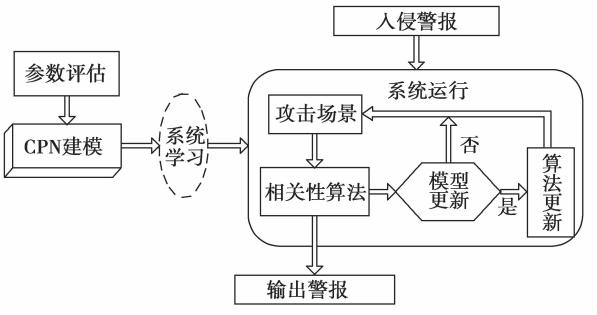

图 2　警报相关性分析系统结构

3.2　合作攻击算法设计

合作攻击是指多个攻击者共享资源能力相互协作完成整个入侵活动，仅从 IDS 收到的警报信息上很难建立攻击者之间的逻辑合作关系，所以合作攻击一直是入侵检测研究的难点。

研究中把 3 种类型：1）同一个攻击者实时篡改源 IP 地址达到伪装的目的；2）同一个攻击者在不同的网络位置发起攻击；3）不同的攻击者在不同的网络位置共享信息发起攻击，统称为合作攻击。因为从 CPN 模型的角度看，3 种类型都源于不同性质的标识共享资源能力，所以处于合作关系的所有标识在模型中的能力等价于所有标识能力的合集。根据

CPN的局部性原理，用局部结构图进行讨论。图3中标识直接用源IP表示，省略目的IP、时间戳、资源占有概率等，即所有攻击针对同一目的主机进行。

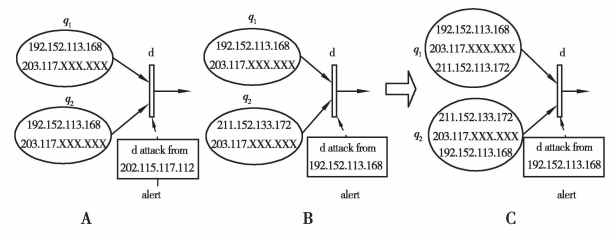

图3 CPN局部结构图

图3的A中系统根据变迁发生规则推断出该警报是误报，但是却很可能漏掉了类型1的情况。B中如果存在类型2、3的情况该警报也是成立的。C就是B中具有合作关系的标识在模型中的完整表示。所以必须回答2个问题：1)哪些标识具有合作攻击的能力。2)如何计算这些标识发起合作攻击的可能性。

图4把传统的CPN转化为另一种描述形式。图中A、B、C 3个库所和变迁 d 的逻辑关系没有改变，虚线框表示标识，它所覆盖到的库所表示该库所中具有该标识。

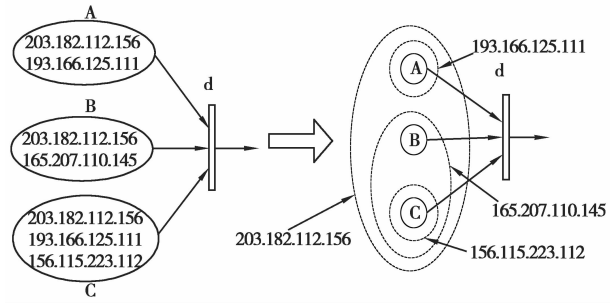

图4 形式转化的CPN描述

根据2个基本原则：1)CPN中变迁发生的基本假设；2)合作者共享资源能力，从图4中可以很清楚地得出具有合作攻击能力的标识：覆盖了变迁前集所有库所的标识集。如标识IP：165.207.110.145和IP：193.166.125.111合作就具备了发起d攻击事件的能力，而即使IP：193.166.125.111和IP：156.115.223.112合作也不可能发起d攻击事件，同时IP：203.182.112.156本身就具备了发起d攻击事件的能力，不再考虑加入其它标识的冗余状态。如果把每类标识作为1个集合，集合中的元素是所有存在该标识的库所，寻找具有合作攻击能力标识组合的问题就转化为寻找标识集对变迁的前集库所的覆盖集问题。排除冗余，就是寻找所有的极小覆盖集。

用反证法很容易证明寻找所有极小覆盖集与最小覆盖集问题一样是NP完全的[13]，其算法时间复杂度为 $O(k^n)$。CPN中变迁前集条件并不多，这样的算法是实用的，图5是用回溯法来解该问题的递归算法。

```
1.所有集合进行编号1-n;
2.求解所有极小覆盖集函数f(编号k)
  {如果k>n,返回;
    与当前临时集合S合并:S=SUk,判定S是否为覆盖集;
    如果S是覆盖集则输出一个解，否则调用f(k+1)寻找所有包含集合k的解;
    恢复S为未合并状态:S=S-k,调用f(k+1)寻找所有不包含集合k的解;
  }
```

图5 求解所有极小覆盖集递归算法

得到了具有合作攻击能力的标识组合后，剩下的问题是计算这些组合发起攻击事件的可能性。一个合作攻击标识组合为 $C=\{c_1,c_2,\cdots,c_n\}$，代表攻击事件的变迁发生概率 z 由IDS性质决定，结合变迁使能概率计算式(2)可以得到：

$$P(E(d)\mid\prod\nolimits_t,C)=P(\text{disenabled}\mid\prod\nolimits_t,C)=P\Big(\bigwedge_{q\in I(d)}(\max_C[\prod\nolimits_t(q,c_i)]\geqslant G(a=(q,d)))\Big)\approx\prod_{q\in I(d)}P(\max_C[\prod\nolimits_t(q,c_i)]\geqslant G(a=(q,d)))=\prod_{q\in I(d)}\max_C[\pi_t(q,c_i)]。\tag{17}$$

式(17)中，对每个前集库所取组合中最大资源能力的标识计算，可以通过警报信息中相关标识优先、阈值设定和最大概率综合判定攻击事件的发生。系统状态更新需要在相关攻击事件的变迁后集中填加 C 中所有标识 c_i 相应参数。

4 ACAS系统实验及分析

用VC6.0开发了CPN建模的警报相关性分析实验系统ACAS(alerts correlation analysis system)，采用离线、自定义格式的警报信息输入且加入可选择合作攻击分析模块。

首先模拟经典的DARPA 2 000攻击场景[14]，其测试数据集LLDOS1.0包含1个完整的复合攻击序列。图6是该攻击场景的Petri网模型，是1个严格的串行模式。

图7的实验过程包含图6的CPN模型参数和自定义格式警报信息2个输入文件，和1个处理完警报信息后的当前模型参数输出文件。CPN模型参数输入文件nodes由变迁和库所2类结点组成，结构如图8(a)和图8(b)所示，输出文件结构一致。

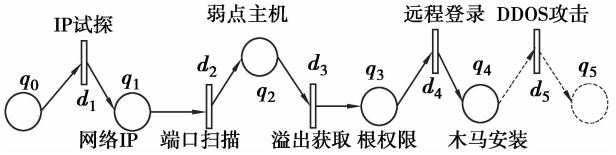

图 6　LLDOS1.0 攻击场景 CPN 建模

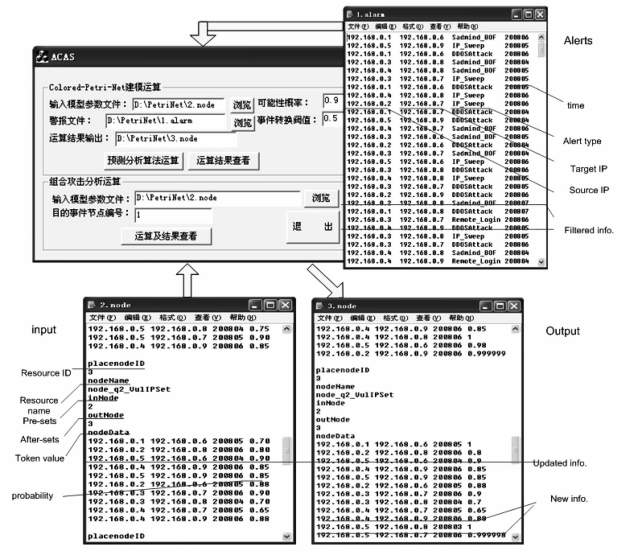

图 7　模拟 DDoS 攻击场景的 ACAS 实验

变迁包含编号、类型名称、前集库所编号数组、后集库所编号数组、发生概率 5 个字段,库所包含编号、名称、前集条件编号数组、后集条件编号数组、数据链表 5 个字段组成,数据链表每个结点又由源 IP、目的 IP、时间戳、资源占有概率 4 个字段组成。自定义警报文件 alarms 格式如图 8(c)所示,包含源 IP、目的 IP、攻击类型名称和时间戳 4 个字段。系统界面控制输入变迁发生概率和过滤阈值,其缺省值分别为 1 和 0.5。

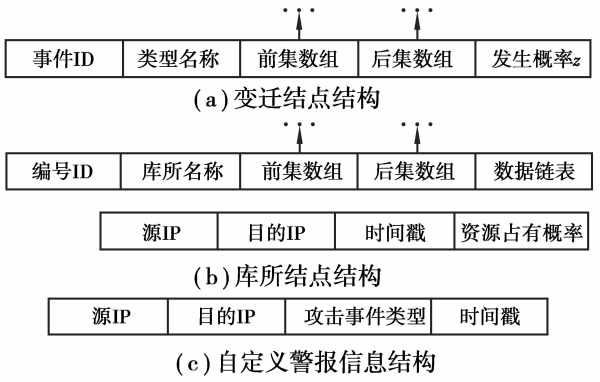

图 8　输入文件信息数据结构

实验图 7 中 ACAS 对 3000 条警报信息进行了逐条处理,反复实验表明 ACAS 在准确实现算法的基础上,有效过滤掉大量误报、重复警报,对有效信息的积累提高了警报的分析预报能力。同时实验发现:1)变迁发生阈值条件的设定对警报信息过滤的影响过高:例如在相同模型参数和警报信息输入下,阈值由 0.5 提高到 0.6,警报过滤率从约 42%提高到了 58%。虽然过滤率很大程度上取决于警报本身,但过高的阈值敏感可能导致有用信息丢失。实验中采用的阈值是攻击场景信息分布的经验统计值,为保留更多分析信息进行了适当降低,基于实验目的在系统界面可以控制调整,而该阈值条件设定理论值的探讨需要作进一步的研究;2)ACAS 中系统模型参数经过多次推理更新后,对同类型警报的敏感性及发生概率有较大提高,源于确认攻击事件实际发生后计算资源占有概率即式(6)时向上取近似值。

由于访问 GCP(grand challenge problem)的数据库[15]有非常严格的限制,为研究合作攻击,在 ACAS 中添加了图 9 的虚拟攻击场景。合作攻击的发生必须是变迁的前集至少包含 2 个以上的库所,显然该场景中 Attack_1 和 Attack_2 上都具有可能性。合作攻击的分析是可选择性模块,其计算结果并没有作为系统状态的更新依据。

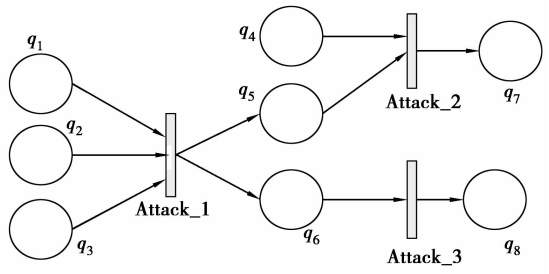

图 9　虚拟合作攻击场景 CPN 模型

图 10 中,文件 minset 是对 Attack_1 的完整分析输出,另有图 9 的 CPN 模型参数输入文件 4.node,图中省略。该实验无需警报文件的输入,是基于模型当前状态的运算,警报信息可以驱动该运算的发生。通过变换模型参数的多次实验表明 ACAS

图 10　虚拟合作攻击场景 ACAS 实验

能完整的发布可能存在的合作攻击情景,仅依靠阈值的限定信息发布显得冗余,现在系统中没有把这些信息作为更新 CPN 模型参数的条件,需要结合警报信息中相关标识、最大概率等才可能达到理想的指标。

5 结 论

不同于大多数过滤性模型研究,笔者提出了以 CPN 建立攻击模型的警报信息相关性分析算法系统,其核心思想是把警报与攻击作为不同实体参与推理运算,进而引入了变迁使能、事件发生、资源占有等概率条件,对系统框架及模型中所涉及的相关性算法进行了详细的阐述和分析。通过 CPN 模型转换、求解极小覆盖集等方法对复合攻击、尤其是合作攻击完成了理论探讨与算法设计。目前开发的实验程序 ACAS 表明应用 CPN 建模及相关算法对于提高 IDS 的警报质量和分析预测能力是可行、有效的。在整个研究过程中,有 2 个基本假设限制了 CPN 模型的能力:1)攻击行为的前提条件和破坏结果在领域内是已知的,即攻击场景的构造问题。当然,这并不是 CPN 模型引入的,基本上所有的过滤性模型都是基于这样的假设;2)初始条件下,资源占有的概率是已知的,这样的假设是完全基于系统的角度,其实对于资源的获取有较多的途径,比如 root ID 的泄露等。

下一步工作包括:1)基础算法系统中变迁发生的阈值条件选取问题;2)继续分析攻击实例,使攻击场景的类别更完整;3)结合警报信息相关标识、优先顺序等方法使合作攻击的判定更加合理。

参考文献:

[1] JULISCH K, DACIER M. Mining intrusion detection alarms for actionable knowledge[C]// The 8th ACM International Conference on Knowledge Discovery and Data Mining, July 23-26, 2002, Edmonton, Alberta, Canada. New York: ACM, 2002: 366-375.

[2] CUPPENS F, AUTREL F, BENFERHAT S, et al. Correlation in an intrusion detection process[C/OL]// Internet Security Communication Workshop, Tunis, September 29, 2002: Computer Network Security [2003]. http://www.lsv.ens-cachan.fr/~goubault/SECI-02/Final/actes-seci02/pdf/014-cuppens.pdf

[3] YU D, FRINCKE D. Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net [J]. Computer Networks, 2007, 5(3): 632-654.

[4] NING P, XU D B, HEALEY C G, et al. Building attack scenarios through integration of complementary alert correlation methods [C]//The 11th Annual Network and Distributed System Security Symposium. (NDSS 2004). [S.l.]: IEEE, 2004: 97-111.

[5] CHEUNG S. LINDQVIST U, FONG M W. Modeling multi-step cyber attacks for scenario recognition[C]// The 3rd DARPA Information Survivability Conference and Exposition (DISCEX III), April 22-24, 2003, Washington D. C. Washington: IEEE Computer Society Press. 2003(1): 284-292.

[6] 严芬, 黄皓, 殷新春. 基于 CTPN 的复合攻击检测方法研究[J]. 计算机学报, 2006, 29(8): 1383 - 1391.
YAN FEN, HANG HAO, YIN XIN-CHUN. A detection algorithm for multi-step attack based on CTPN [J]. Chinese Journal of Computers, 2006, 29 (8):1383-1391.

[7] FRINCKE D, TOBIN D, HO Y. Planning petri nets and intrusion detection [C]//The 21st National Information Systems Security Conference (NISSC'98), 1998, Crystal City, Virginia. [S.l.]: IEEE Computer Society, 2006.

[8] 鲍旭华, 戴英侠, 冯萍慧, 等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报, 2005, 16(12): 2132-2138.
BAO XU-HUA, DAI YING-XIA, FENG PING-HUI, et al. A detection and forecast algorithm for multi-step attack based on intrusion intension [J]. Chinese Journal of Software, 2005, 16(12): 2132-2138.

[9] ILGUN K, KEMMERERER R, PORRAS P. State transition analysis: a rule-based intrusion detection system [J]. IEEE Transactions on Software Engineering, 1995, 21(3): 181-199.

[10] HARRIS J W, STOCKER H. Maximum likelihood method: handbook of Mathematics and computational science [M]. New York: Springer-Verlag, 1998: 824-827.

[11] MOON T. The expectation maximization algorithm [J]. IEEE Signal Processing Magazine, 1996, 13(6): 47-60.

[12] VALDES A, SKINNER K. Probabilistic alert correlation [C]//In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), October 10-12, 2001, Davis, Central America, USA. London: Springer-Verlag, 2001.

[13] WANG X D. Algorithms design and analysis [M]. Beijing: Publishing House of Electronics Industry, 2001.

[14] Lincoln Lab, MIT. DARPA 2000 intrusion detection evaluation datasets[EB/OL]. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.

[15] HAINES J, RYDER D K, TINNEL L, et al. Validation of sensor alert correlators[J]. IEEE Security and Privacy, 2003, 1(1): 46-56.

(编辑 侯 湘)