ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.9, September 2010, pp.2376−2386
doi: 10.3724/SP.J.1001.2010.03632

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

贝叶斯推理在攻击图节点置信度计算中的应用*

张少俊[1,2+], 李建华[1,2], 宋珊珊[1], 李 斓[1,2], 陈秀真[1,2]

[1](上海交通大学 信息安全工程学院,上海 200240)

[2](上海市信息安全综合管理技术研究重点实验室,上海 200240)

Using Bayesian Inference for Computing Attack Graph Node Beliefs

ZHANG Shao-Jun[1,2+], LI Jian-Hua[1,2], SONG Shan-Shan[1], LI Lan[1,2], CHEN Xiu-Zhen[1,2]

[1](School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

[2](Shanghai Key Laboratory for Information Security Integrated Management Technology Research, Shanghai 200240, China)

+ Corresponding author: E-mail: zshaojun@sjtu.edu.cn

Zhang SJ, Li JH, Song SS, Li L, Chen XZ. Using Bayesian inference for computing attack graph node beliefs. *Journal of Software*, 2010,21(9):2376−2386. http://www.jos.org.cn/1000-9825/3632.htm

Abstract: Network attack graphs are widely used as templates to extrapolate network security state by analyzing observed intrusion evidence. Existing attack graph node belief computation methods are suffering from generality problems, high computational complexity, or the overuse of empirical formulas to solve problems. This paper improves one of the Bayesian network inference algorithms—the likelihood weighting algorithm into a novel graph node belief computation algorithm, which supports the temporal partial ordering relationship among intrusion evidences. Experiment results show that the method can achieve high computation accuracy in linear computational complexity, a feature making it feasible to be used to process large scale attack graphs in real-time.

Key words: network security; attack graph; belief; Bayesian inference; likelihood weighting

摘 要: 网络攻击图是根据观测到的攻击证据推测网络安全状态的理想模板.现有的攻击图节点置信度计算方法或在模型通用性、计算复杂度方面存在一定不足,或又过多依靠经验公式进行推理而缺乏严密的数学理论支撑.为此,提出一种基于贝叶斯推理的攻击图节点置信度计算方法.方法对似然加权法进行了改进,以支持攻击证据之间的时间偏序关系.实验结果表明,该方法能够有效提高节点置信度的计算准确性,且具有线性计算复杂度,适合于处理大规模攻击图节点置信度的实时计算问题.

关键词: 网络安全;攻击图;置信度;贝叶斯推理;似然加权

中图法分类号: TP393 **文献标识码**: A

网络攻击技术与计算机网络一样,经历了一个从简单到复杂的发展过程.互联网发展的早期,网络攻击以展

* Supported by the National Natural Science Foundation of China under Grant Nos.60605019, 60803145 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant Nos.2007AA01Z473, 2008AA01Z409 (国家高技术研究发展计划(863)); the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant No.20070248002 (高等学校博士学科点专项科研基金)

Received 2009-01-04; Revised 2009-02-24; Accepted 2009-03-31

示个人技能的无目的攻击为主,限于破解口令和利用操作系统已知漏洞等有限的几种方法,攻击与攻击间的关联性较弱.时至今日,网络攻击已演化为一种复杂的多步骤过程,单次攻击往往包含一组紧密关联的基本攻击环节,如目标系统信息收集、弱点信息挖掘分析、目标使用权限获取、攻击行为隐蔽、攻击实施、开辟后门及痕迹清除等.

攻击技术的复杂化对网络安全分析提出了更高的要求.在众多技术手段中,网络攻击图[1−4]由于包含攻击者为达到攻击目标所能选择的所有路径,成为安全分析的重要工具之一.近年来,网络攻击图的自动化生成技术已经成为国内外学术界的研究热点.通过综合攻击、漏洞、目标、主机和网络连接关系等因素,可以利用计算机程序模拟网络安全状态之间的可行变迁,得到所有可能出现的变迁序列,最终整合形成简洁、完备的网络攻击图.

攻击图构建、分析技术早期主要应用于离线网络安全评估领域,目标是预先找出所有可能导致系统受损的状态变迁序列,进而找到成本最低的补救措施.此后,随着网络攻击图更多地应用于告警关联[5,6]、态势感知[7]、应急响应等实时网络安全管理技术领域,如何根据动态观测到的数据判断网络当前状态——计算、更新攻击图节点置信度成了亟待解决的问题.然而,现有的攻击图节点置信度计算方法在模型通用性、计算复杂度及合理性方面存在着一定的问题.为此,本文提出一种基于贝叶斯推理的攻击图节点置信度计算方法,对现有置信度计算方法进行了改进,提升了其计算合理性.同时,方法具有线性计算复杂度,适合于处理大规模攻击图节点置信度的实时计算问题.

1 相关的研究工作

Sheyner 等人[3,4]最早在网络攻击图分析处理过程中引入概率方法.该方法假设:1) 攻击图的部分状态节点到其后继节点的条件转移概率为已知,称为确定性(deterministic)节点,其余节点条件转移概率则为未知,称为非确定性(nondeterministic)节点;2) 在非确定性节点上,攻击者选择最有利于达到攻击目标的路径完成状态转移.

上述假设将网络攻击图转化为马尔可夫决策过程,利用相关理论,不难计算任意状态节点下攻击者最终变迁到目标状态节点的概率,进而评估网络的可靠性.该方法本质上是一种离线网络安全性评估技术,虽然引入了状态转移概率,但还未完整提出节点置信度的计算、更新问题.

Zhai 等人[8]提出一种利用贝叶斯推理计算网络攻击证据置信度的方法.该方法将攻击证据分为两类:1) 通过观测攻击行为本身获得的事件型证据(如入侵检测系统的告警等);2) 通过观测攻击影响而获得的状态型证据(反病毒系统告警、漏洞扫描报告等).状态型证据一般是可信的,定义其置信度为 1;事件型证据则由于所对应的攻击可能并不成功,因而是不完全可信的,需为每种事件型证据类型定义先验概率 $Pr(T)$,用以表征证据出现情况下攻击真正成功的概率.根据因果关系知识库,可将已观测到的攻击证据链接为有向无圈图,并结合条件概率 $Pr(T)$形成贝叶斯网,最后利用贝叶斯推理使证据之间互相印证,得到更为准确的证据置信度.但由于该方法完全依靠已观测到的攻击证据构建网络攻击图,而非事先根据原子攻击、主机漏洞、网络连接关系等因素得到攻击者可能选择的所能潜在攻击路径,因而方法限于解释处理已观测到的攻击证据,不适合用于预测尚未发生的攻击行为.此外,在事件型证据漏警率较高的情况下,方法计算复杂度过高.

Yu 等人[9]提出了一种用隐彩色 Petri 网对攻击建模以实现告警关联及攻击预测的方法.该方法把资源状态(即攻击者是否占有某资源)、攻击行为及攻击证据作为彩色 Petri 网的不同类型节点,并将其互相关联.同时,引入条件概率:1) 对于攻击行为 d_i,资源状态前件 $I(d_i)$满足时,d_i 以概率 $z(d_i|I(d_i))$发生;2) d_i 发生时,攻击证据 O_j 以概率$\gamma(O_j|d_i)$被观测到.

方法给出了一组经验公式,旨在解决以下问题:

1) 给定资源状态节点置信度分布,如何计算攻击行为 d_i 的发生概率及其影响;
2) 给定资源状态节点置信度分布,当观测到攻击证据 O_j 时,如何计算攻击行为 d_i 发生概率并更新置信度分布.

但是,该方法在更新置信度分布时,采用经验公式仅对攻击行为后继状态节点(而非 Petri 网所有资源状态

节点)进行置信度更新,存在一定的改进空间.

2 基于贝叶斯推理的攻击图节点置信度计算

2.1 攻击图定义和节点置信度计算问题

网络攻击是一种复杂的多步骤过程,包含一组紧密关联的基本攻击行为.基本攻击行为的实施改变了网络状态,使攻击者占有更多的资源,最终实现其攻击目标.同时,攻击行为的实施有可能被安全防护设备(如入侵检测系统)检测到并触发告警,形成攻击证据.一般情况下,管理员能够根据观测到的攻击证据推断网络的当前状态,进而采取应对措施.

网络攻击图描述了上述 3 种因素(资源状态、攻击行为、攻击证据)及其相互关系.一般地,网络攻击图包含了攻击者实现攻击目标的所有潜在攻击路径,具有简洁性和完备性[3].此外,根据单调性假设[10],攻击者不会放弃已经占有的资源.因此,当占有某个资源后,不会再为占有该资源实施攻击.根据以上分析,给出如下定义:

定义 1. 网络攻击图为有向无圈图 $AG=(S,S_0,G,A,O,E,\Delta,\Phi,\Theta,\Pi)$,其中:

- $S=\{s_i|i=1,\ldots,N\}$为资源状态节点集合.节点变量 s 的取值可为 *True* 或 *False*,分别表示当前攻击者已占有或未占有资源 s_i;
- $S_0\subseteq S$ 为 AG 根节点集合,表示初始状态下,攻击者以一定概率占有的资源;
- $G\subseteq S$ 为攻击目标节点集合;
- $A=\{a_i|i=1,\ldots,N_a\}$为攻击行为节点集合.节点变量 a_i 的取值可为 *True* 或 *False*,分别表示当前攻击行为 a_i 已发生或未发生;
- $O=\{o_i|i=1,\ldots,N_o\}$为攻击证据节点集合.节点变量 o_i 的取值可为 *True* 或 *False*,分别表示当前已观测到或未观测到攻击证据 o_i(由于观测到的攻击证据往往经底层传感器归并处理,其出现次数与实际数量可能存在差异,故本文不考虑攻击证据出现的具体次数,仅根据其是否出现进行推理);
- $E=(E_1\cup E_2\cup E_3)$为关联各类节点的有向边集合.其中,$E_1\subseteq S\times A$ 表示只有当攻击者占有某些资源,攻击行为才能发生;$E_2\subseteq A\times S$ 表示攻击行为可导致攻击者占有某些资源;$E_1\subseteq A\times O$ 表示攻击行为可触发某些攻击证据.一般地,记 Pre(n)为节点 n 的前件节点集合,Con(n)为节点 n 的后件节点集合;
- Δ为攻击行为发生的条件概率分布.

$$\Delta=P(\text{攻击行为 } a_i \text{ 发生}|\text{攻击行为 } a_i \text{ 前件满足})=\{\delta:(\mathrm{Pre}(a_i),a_i)\to[0,1]\}.$$

为便于推导,本文假设 Pre(a_i)元素之间存在“与”关系,即攻击行为所有前件都满足时攻击行为才可能发生;

- Φ为攻击行为成功的条件概率分布.由于当且仅当攻击成功时,攻击行为将改变资源状态,因而攻击成功的概率即等于攻击行为将其后件节点变量值置为 *True* 的概率.即有

$$\Phi=P(\text{攻击行为 } a_i \text{ 成功}|\text{攻击行为 } a_i \text{ 发生})=\{\phi:(a_i,\mathrm{Con}(a_i))\to[0,1]\}.$$

此外,本文假设当资源状态节点 s_i 作为两个或两个以上攻击行为的后件时,Pre(s_i)元素之间存在“或”关系,即任何攻击行为的成功都将独立地把 s_i 置为 *True*;

- Θ为观测到攻击证据的条件概率.$\Theta=P(\text{观测到攻击证据 } o_j|\text{攻击行为 } a_i \text{ 发生})=\{\theta:(a_i,o_j)\to[0,1]\}$;同样,当 o_j 作为两个或两个以上攻击行为的后件时,Pre(o_j)元素之间存在“或”关系,即任何攻击行为的发生都可能独立地触发 o_j;
- $\Pi=\{\pi:S\cup A\cup O\to[0,1]\}$为攻击图节点置信度分布.其中,$\pi(s_i)$表示攻击者当前占有资源 s_i 的概率,$\pi(a_i)$表示攻击行为 a_i 当前已发生的概率,$\pi(o_i)$表示当前已观测到攻击证据 o_i 的概率.特别地,Π_0 为攻击图初始节点置信度分布.此时,攻击者以一定概率占有 S_0 中的元素,任何攻击行为尚未发生,故有:

$$\pi_0(n_i)\geqslant 0,\ n_i\in S_0,$$
$$\pi_0(n_i)=0,\ n_i\notin S_0.$$

符合定义 1 的网络攻击图可通过如下方法生成:首先,改进文献[10]提出的攻击图生成方法,显式标出攻击行为节点及其与资源状态节点之间的有向边(在原方法中,该部分信息以标签形式记录在资源节点所附带的列

表中),以生成目标网络攻击图的主干结构;而后,列出所有可能出现的攻击证据,将其加入攻击图,并标识攻击行为与攻击证据之间的触发关系;最后,根据专家经验定义条件概率分布Δ,Φ和Θ,并结合目标网络的安全状态估计初始节点置信度分布Π_0.

根据以上方法生成的网络攻击图的一般形态如图 1 所示.

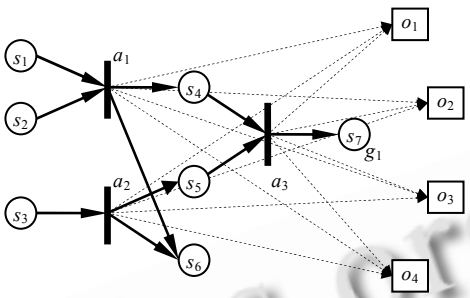


Fig.1 A typical network attack graph

图 1 网络攻击图一般形态

图 1 中初始状态节点置信度分布为Π_0使攻击者以一定概率占有资源 s_1,s_2 和 s_3.而后,攻击行为 a_1,a_2 和 a_3 将遵循条件概率分布Δ发生,并导致攻击者以条件概率分布Φ占有资源 s_4,s_5,s_6 和 s_7.攻击行为发生的同时,以条件概率分布Θ触发攻击证据 o_1,o_2,o_3 和 o_4.

如前所述,攻击图关注攻击证据是否出现,但不具体记录各个攻击证据的出现次数及出现时间.为弥补缺失这部分信息对后验推理造成的影响,可定义攻击证据之间具有一定的时间偏序关系.证据时间偏序关系 $o_m \rightarrow o_n$ 是指:证据 o_m 在证据 o_n 首次出现以后就没有再出现过.换言之,o_m 所有出现的时间点都要早于 o_n 出现的时间点.图 2 给出一个例子,说明时间偏序关系对后验推理的作用.

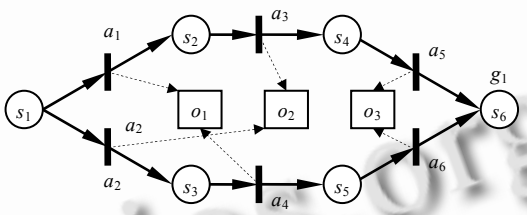


Fig.2 A simple network attack graph

图 2 简单网络攻击图

图 2 中,假设攻击者初始状态下以概率 1.0 占有资源节点 s_1,攻击目标为节点 s_6(即 g_1),分布Δ和Φ的概率取值均为 0.5,分布Θ的概率取值均为 1.0,攻击过程中观测到证据序列 $o_2 \rightarrow o_1 \rightarrow o_3$.

分析:为达到目标,攻击者有两条攻击路径可以选择:

① $s_1 \rightarrow a_1 \rightarrow s_2 \rightarrow a_3 \rightarrow s_4 \rightarrow a_5 \rightarrow s_6$;

② $s_1 \rightarrow a_2 \rightarrow s_3 \rightarrow a_4 \rightarrow s_5 \rightarrow a_6 \rightarrow s_6$.

根据图 2,攻击行为 a_1 和 a_4 将触发攻击证据 o_1;a_2 和 a_3 将触发 o_2;a_5 和 a_6 将触发 o_3.此时:

- 若不考虑证据之间的时间偏序关系,将 3 个证据节点简单取值为 *True*,经后验推理可以发现,所有节点置信度均大于 0,即两条攻击路径都有可能被实施;
- 若考虑时间偏序关系,则容易发现证据序列存在时间偏序关系 $o_2 \rightarrow o_1$.根据假设,分布Θ取值均为 1.0,即 a_1 必触发 o_1,a_3 必触发 o_2,故攻击路径①的实施将打破偏序关系 $o_2 \rightarrow o_1$,所以攻击者实施路径①的可能性应被排除.

根据以上分析,攻击图节点置信度计算问题可描述为:

定义 2. 攻击图节点置信度计算问题是指:给定网络攻击图 AG,当观测到攻击证据序列$\alpha=o_{i1},o_{i2},\ldots,o_{ik}$,且具有时间偏序关系$\Omega=\{o_m\rightarrow o_n\}$时,求相对应的 AG 节点置信度分布序列$\beta=\Pi_0,\Pi_1,\ldots,\Pi_k$.

2.2 贝叶斯近似推理——似然加权法的改进

贝叶斯网[11]起源于20世纪80年代中期对人工智能领域中不确定性问题的研究,目前已经成为人工智能的一个重要领域.贝叶斯网为后验概率推理提供了极大的方便.一般地,只要设定一组证据变量的取值,即可通过消元、团树传播或近似推理等方法计算节点后验概率分布.下面给出贝叶斯网及后验推理的一般定义.

定义 3. 贝叶斯网是一个有向无圈图,其中,节点代表随机变量,节点间的边代表变量之间的直接依赖关系.每个节点都附有一个概率分布,根节点 X 所附的是它的边缘分布 $P(X)$,非根节点 X 所附的是条件概率分布 $P(X|\mathrm{Pre}(X))$.后验推理则是指已知贝叶斯网中某些变量的取值,计算另外一些变量后验概率分布的问题.

对比定义 1 和定义 3 容易发现,网络攻击图本质是一张贝叶斯网.唯一的区别是,网络攻击图攻击证据之间可能具有时间偏序关系,不应通过传统的贝叶斯推理方法简单设定证据节点取值进行后验推理.为解决该问题,本文提出一种对贝叶斯近似推理——似然加权法的改进,在后验推理过程中加入对证据节点时间偏序关系的支持.

似然加权法是逻辑抽样法的一个发展.逻辑抽样法按照贝叶斯网的拓扑序对其中的变量逐个进行抽样:对待抽样变量 X,若它是根节点,则按分布 $P(X)$进行抽样;若是非根节点,则按分布 $P(X|\mathrm{Pre}(X)=r)$进行抽样(这里,r 是 X 的父节点的抽样结果,在对 X 抽样时是已知的).假设通过顺序抽样过程获得了 m 个独立样本,其中满足证据节点取值 $O=o$ 的有 m_o 个,而在这 m_o 个样本中,进一步满足查询变量 $Q=q$ 的有 $m_{q,o}$ 个,则 $P(Q=q|O=o)\approx m_{q,o}/m_o$.似然加权法的主要目的是避免逻辑抽样法舍弃大量不符合证据变量取值的样本所造成的浪费:当 X 不是证据变量时,抽样方式与逻辑抽样法一样;当 X 是证据变量时,以 X 的观测值作为抽样结果,同时将抽样到该值的概率作为该样本的权重.最后计算 $P(Q=q|O=o)$近似值时,仅需把样本个数 m_o 与 $m_{q,o}$ 用相应的样本权重和替换即可.

为支持证据节点之间的时间偏序关系,本文对似然加权法进行了改进,其基本思路为:当 X 为证据变量且取值为真时,先按条件概率产生一种导致其值为真的成因**,而后检验该成因与其他证据变量的成因是否符合时间偏序关系.若符合,则将抽样到该值的概率计入样本的权重,并继续处理其他节点;反之则抛弃样本.这种处理方式可以保证所得样本每一个证据节点取值均为观测值,且不违背证据节点间的时间偏序关系.改进后算法伪代码见算法 1.

算法 1. 似然加权法改进.

PartialLikelihoodWeighting($\boldsymbol{AG},m,\boldsymbol{O},\boldsymbol{o},\boldsymbol{\Omega},\boldsymbol{Q},\boldsymbol{q}$)

输入: $\boldsymbol{AG}$——贝叶斯网(即攻击图);m——有效样本量;$\boldsymbol{O}$——证据变量集合;$\boldsymbol{o}$——$\boldsymbol{O}$ 的取值;

$\boldsymbol{\Omega}$——$\boldsymbol{O}$ 上的一个偏序关系;$\boldsymbol{Q}$——查询变量;$\boldsymbol{q}$——查询变量的取值;

输出: 对 $P(\boldsymbol{Q}=\boldsymbol{q}|\boldsymbol{O}=\boldsymbol{o},\boldsymbol{\Omega})$的近似.

算法:
01: $\rho\leftarrow\boldsymbol{AG}$ 的一个拓扑序;
02: $i\leftarrow 0$; $w_{o,\Omega}\leftarrow 0$; $w_{q,o,\Omega}\leftarrow 0$;
03: while ($i<m$)
04: $\boldsymbol{D}_i\leftarrow\varnothing$; $\boldsymbol{Z}_i\leftarrow\varnothing$; $w_i=1$;
05: for (ρ中的每一个变量 X)
06: if ($X\in\boldsymbol{O}$) then
07: $x\leftarrow X$ 的观测值;
08: if ($x=True$)

** 本文中,成因是指攻击证据成立(即出现)的原因.需注意的是:若攻击行为 a_i 是攻击证据 o_j 的前件,当$\theta(a_i,o_j)<1$ 时,即使 $a_i=True$,a_i 也可以不是 $o_j=True$ 的成因.一般地,节点 $o_j=True$ 的成因是$\{x|x\in\mathrm{Pre}(o_j)\text{ and }x=True\}$的一个子集,未必是该集合本身.

09: C_X,w_X←RandomSelectCausation($\boldsymbol{AG},X,\boldsymbol{D}_i$);
10: for ($\boldsymbol{Z}_i$ 中的每一组(Y,C_Y))
11: if (IsPartialSatisfied($\boldsymbol{AG},\boldsymbol{\Omega},X,Y,C_X,C_Y$)=*false*) then goto 28;
12: end for (10)
13: w_i←w_i*w_X;
14: $\boldsymbol{Z}_i$←$\boldsymbol{Z}_i$∪{(X,C_X)};
15: else (08)
16: w_i←w_i*$P(X|\text{Pre}(X))|_{Di}$;
17: end if (08)
18: else (06)
19: x←从 $P(X|\text{Pre}(X))$抽样的结果;
20: end if (06)
21: $\boldsymbol{D}_i$←$\boldsymbol{D}_i$∪{$X=x$};
22: end for (05)
23: $w_{o,\Omega}$←$w_{o,\Omega}$+w_i;
24: if ($\boldsymbol{Q}=\boldsymbol{q}\in\boldsymbol{D}_i$) then
25: $w_{q,o,\Omega}$←$w_{q,o,\Omega}$+w_i;
26: end if (24)
27: i←i+1;
28: end while (03)
29: return $w_{q,o,\Omega}/w_{o,\Omega}$;

算法 1 首先选择攻击图的任意一个拓扑序ρ,而后进入循环直到生成预定义的 m 个有效样本.第 4~22 行是抽样过程,按照拓扑序ρ对每个变量 X 进行抽样.抽样时,若 X 为证据变量,以 X 的观测值作为抽样结果(第 7 行),同时,将抽样到该值的概率计入该样本的权重(第 13 行、第 16 行);若 X 不是证据变量,则按分布 $P(X|\text{Pre}(X))$进行抽样.该过程与传统的似然加权法的区别是:1) 当X为证据变量且取值为真时,除了以X的观测值作为抽样结果外,需要调用成因选择方法 RandomSelectCausation(见算法 2)根据概率分布决定样本中的哪一个(或一些)攻击行为导致了 X 为真(第 9 行);2) 确定证据节点成因之后,调用偏序关系检查方法 IsPartialSatisfied(见算法 3)检查证据时间偏序关系与拓扑偏序关系是否一致,以决定样本的有效性(第 11 行.这里定义若节点 a 到节点 b 存在一条有向路径,则它们具有拓扑偏序关系 $a\rightarrow b$).

算法 2. 成因选择方法.

RandomSelectCausation($\boldsymbol{AG},X,\boldsymbol{D}$)

输入: $\boldsymbol{AG}$——贝叶斯网(即攻击图);X——$\boldsymbol{AG}$ 中的某个证据节点,其取值为 *True*;
$\boldsymbol{D}$——$\boldsymbol{AG}$ 中含 Pre(X)在内的部分节点的取值集合;

输出: C_X——取值集合 $\boldsymbol{D}$ 下使 X=*True* 的一个成因集合;w_X——P(成因集为 $C_X|\boldsymbol{D},X$=*True*).

算法: 01: Φ←∅; Θ←{$Y|Y\in\text{Pre}(X)$且$(Y=True)\in D$};
02: p_Σ←0;
03: for (Θ的每一个非空子集θ)
04: p_θ←$\Pi_{Y\in\theta}P(X=True|Y=True)$
*$\Pi_{Y\in(\Theta-\theta)}P(X=False|Y=True)$;
05: Φ←Φ∪{(θ,p_θ)};
06: p_Σ←p_Σ+p_θ;
07: end for (3)

08: for (Φ中的每一个元素(θ,p_θ))

09: $p_\theta \leftarrow p_\theta / p_\Sigma$;

10: end for (8)

11: (θ_r, p_{θ_r})$\leftarrow\Phi$中元素以 p_θ为概率分布的抽样结果;

12: $C_X \leftarrow \theta_r$; $w_X \leftarrow p_{\theta_r}$;

13: return C_X, w_X;

算法 3. 偏序关系检查方法.

IsPartialSatisfied($\boldsymbol{AG}$,$\boldsymbol{\Omega}$,X,Y,C_X,C_Y)

输入: $\boldsymbol{AG}$——贝叶斯网(即攻击图);$\boldsymbol{\Omega}$——证据偏序关系;X,Y——任意两个证据节点;

C_X,C_Y——两个使 X=*True*,Y=*True* 的成因集合;

输出: 布尔量 b,成因集合 C_X,C_Y 是否符合偏序关系.

算法: 01: $\psi \leftarrow \boldsymbol{AG}$ 节点的拓扑偏序关系

02: if (($X \rightarrow Y$)$\in\boldsymbol{\Omega}$)

03: for (每一个 $V\in C_X$,$W\in C_Y$))

04: if (($W \rightarrow V$)符合拓扑偏序ψ) return *False*;

05: end for (03)

06: return *True*;

07: else (02)

08: return *True*;

09: end if (02)

上述对似然加权法的改进保证了抽样过程完全依照攻击图的实际概率分布进行,并且通过 RandomSelectCausation 和 IsPartialSatisfied 方法的联合使用使获得的每一个样本都不违背攻击证据之间的时间偏序关系,在计算后验概率时都能被利用.

3 算法验证及分析

为验证算法功能及运行性能,用 Java 语言编制程序实现了改进的似然加权法,并做如下实验:

3.1 功能验证及分析

3.1.1 与传统贝叶斯后验推理的比较

仍以图 2 网络攻击图为例,利用传统贝叶斯推理进行节点置信度计算,计算结果见表 1.

Table 1 Classical Bayesian inference result

表 1 传统贝叶斯后验推理结果

i	$\pi_i(s_1)$	$\pi_i(s_2)$	$\pi_i(s_3)$	$\pi_i(s_4)$	$\pi_i(s_5)$	$\pi_i(s_6)$	$\pi_i(a_1)$	$\pi_i(a_2)$	$\pi_i(a_3)$	$\pi_i(a_4)$	$\pi_i(a_5)$	$\pi_i(a_6)$
0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	1.0	0.0	0.333	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0
2	1.0	0.477	0.477	0.097	0.097	0.0	0.85	0.85	0.29	0.29	0.0	0.0
3	1.0	0.619	0.619	0.524	0.524	0.504	0.746	0.746	0.556	0.556	0.508	0.508

表 1 中,序号 i 对应不同的推理时间点.即:i=0 对应尚未观测到任何攻击证据时对节点置信度所作的推理,i=1 对应观测到证据 o_2 时所作的推理,i=2 对应观测到证据序列 $o_2 \rightarrow o_1$ 时所作的推理,i=3 对应序列 $o_2 \rightarrow o_1 \rightarrow o_3$.

而后,利用本文算法进行节点置信度计算(有效样本数=20 000 个),结果见表 2.

Table 2 Improved likelihood weighting inference result

表 2 改进的似然加权法推理结果

i	$\pi_i(s_1)$	$\pi_i(s_2)$	$\pi_i(s_3)$	$\pi_i(s_4)$	$\pi_i(s_5)$	$\pi_i(s_6)$	$\pi_i(a_1)$	$\pi_i(a_2)$	$\pi_i(a_3)$	$\pi_i(a_4)$	$\pi_i(a_5)$	$\pi_i(a_6)$
0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	1.0	0.0	0.331	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	0.0
2	1.0	0.264	0.582	0.0	0.123	0.0	0.793	1.0	0.0	0.366	0.0	0.0
3	1.0	0.136	1.0	0.0	1.0	0.501	0.429	1.0	0.0	1.0	0.0	1.0

传统贝叶斯后验推理不考虑证据出现的前后次序,因而表 1 中 i>1 时攻击路径①、攻击②的节点置信度是对称相等的,即意味着难以通过分析节点置信度来判断攻击者选取了哪条路径.改进的似然加权法则考虑到证据之间的时间偏序关系,因而攻击路径②上的节点置信度明显高于攻击路径①,明确了攻击路径.

3.1.2 与隐彩色 Petri 网方法[9]的比较

由于避免了依靠经验公式进行后验推理,本文算法对节点置信度的计算合理性明显优于隐彩色 Petri 网方法.为证明这一点,对上面的例子稍作调整,如图 3 所示.

与图 2 相比,图 3 增加了攻击节点 a_7、资源节点 s_7 及证据节点 o_4.同时,调整了部分攻击行为与攻击证据的触发关系,并在各有向边上标识了所对应的条件概率值.设初始状态下攻击者仍以概率 1.0 占有资源节点 s_1,攻击目标仍为节点 s_6.攻击过程中,观测到证据序列 $o_1 \to o_2 \to o_3 \to o_4$.

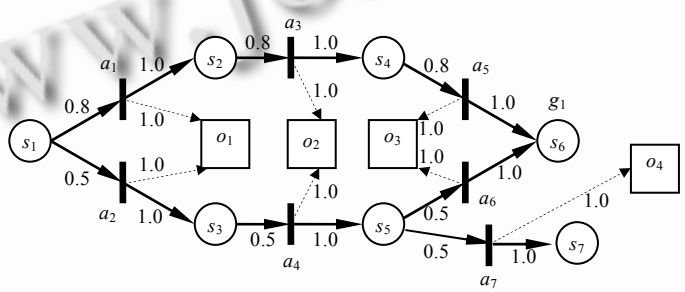


Fig.3 A network attack graph

图 3 网络攻击图

参照隐彩色 Petri 网方法,对状态节点置信度进行计算,计算结果见表 3(由于该方法未定义对其他类型节点置信度计算公式,故仅能得到状态节点置信度).

Table 3 Hidden colored Petri net aposterior inference result

表 3 隐彩色 Petri 网后验推理结果

i	Assumed action	$\pi_i(s_1)$	$\pi_i(s_2)$	$\pi_i(s_3)$	$\pi_i(s_4)$	$\pi_i(s_5)$	$\pi_i(s_6)$	$\pi_i(s_7)$
0	—	1.0	0.0	0.0	0.0	0.0	0.0	0.0
1	a_1	1.0	0.615	0.0	0.0	0.0	0.0	0.0
	a_2	1.0	0.0	0.385	0.0	0.0	0.0	0.0
2	a_3	1.0	0.615	0.0	0.275	0.0	0.0	0.0
	a_4	1.0	0.0	0.385	0.0	0.193	0.0	0.0
3	a_5	1.0	0.615	0.0	0.275	0.0	0.109	0.0
	a_6	1.0	0.0	0.385	0.0	0.193	0.057	0.0
4	a_7	1.0	0.0	0.385	0.0	0.193	0.057	0.057

需要说明的是,隐彩色 Petri 网方法推理时,需引入辅助函数 $\omega_i(a_j)$,以度量、比较在推理时间点 i 上攻击行为 a_j 发生的可能性的相对大小.状态节点置信度的更新是在假设 a_j 为所发生的攻击行为下进行的.为节约篇幅,表 3 仅列出所有 $\omega_i(a_j)$>0 的情况.

而后,利用本文算法进行节点置信度计算(有效样本数=10 000 个),结果见表 4.

Table 4 Improved likelihood weighting inference result

表 4 改进的似然加权法推理结果

i	$\pi_i(s_1)$	$\pi_i(s_2)$	$\pi_i(s_3)$	$\pi_i(s_4)$	$\pi_i(s_5)$	$\pi_i(s_6)$	$\pi_i(s_7)$	$\pi_i(a_1)$	$\pi_i(a_2)$	$\pi_i(a_3)$	$\pi_i(a_4)$	$\pi_i(a_5)$	$\pi_i(a_6)$	$\pi_i(a_7)$
0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
1	1.0	0.705	0.522	0.0	0.0	0.0	0.0	0.705	0.522	0.0	0.0	0.0	0.0	0.0
2	1.0	0.890	0.493	0.822	0.244	0.0	0.0	0.890	0.493	0.822	0.244	0.0	0.0	0.0
3	1.0	0.971	0.467	0.951	0.206	1.0	0.0	0.971	0.467	0.951	0.206	0.931	0.139	0.0
4	1.0	0.866	1.0	0.762	1.0	1.0	1.0	0.866	1.0	0.762	1.0	0.678	0.655	1.0

表 3 对于每一个观测阶段,需假设已发生的是攻击路径①上的攻击行为或攻击路径②上的攻击行为.当 i<4 时,前一种假设所获得的状态节点置信度明显高于后一种假设,这归因于两条路径上条件概率值的差异.而当 i=4 时,由于 o_4 仅可能由 a_7 触发,存在对攻击路径②的"确认效应",故路径①被完全排除,仅有路径②节点置信度大于 0.然而,由于方法所定义的经验公式仅能对攻击行为后继节点进行置信度更新,故路径②节点置信度并未增大.表 4 中,当 i<4 时,攻击路径①上的节点置信度略高于攻击路径②,而当 i=4 时,o_4 对攻击路径②的"确认效应"使得该路径节点置信度均增大为 1.0.同时,o_1,o_2 和 o_3 在观测序列中虽然仅出现一次,但考虑其可能经底层传感器归并处理,故路径①节点置信度虽有一定程度下降,但仍不排除其被实施的可能.

3.2 性能验证及分析

改进的似然加权法主要分为采样及样本统计两个部分,前者的计算量远大于后者,因而本节主要关注算法的采样性能.图 4 为上述两个例子的采样性能曲线.主要运行环境为:Intel Core2 Duo CPU 2.00GHz,2GB DDR2 内存,Microsoft Windows XP Professional 操作系统(service pack 2),Sun JDK 1.6.0_10-rc.

如图 4 显示,对于特定的攻击图,采样时间与有效样本数量成正比.对于图 2 所示攻击图,平均每采集一个有效样本需耗时 0.91s,图 3 攻击图则耗时 0.63s.分析算法不难发现,影响采样时间的主要因素包括:1) 攻击图节点数量 N;2) 证据节点偏序关系 Ω.由于攻击图中每一个节点的前件个数都是有限的,因而一次采样中对单个节点的处理总能在常数时间 $T_{\max}$ 内完成,即单个样本采样时间恒小于 $N\times T_{\max}$.另一方面,证据偏序关系 Ω 确实可能导致采样时丢弃大量的无效样本(这也是图 2 节点个数虽小于图 6,但采样时间却大于后者的原因).为控制其对性能的影响,可设置最大尝试次数 M,当采样次数达到 M 时终止采样过程,并利用已得到的有效样本进行统计计算.综上所述,采样总耗时恒小于 $N\times T_{\max}\times M$,即算法具有线性计算复杂度.

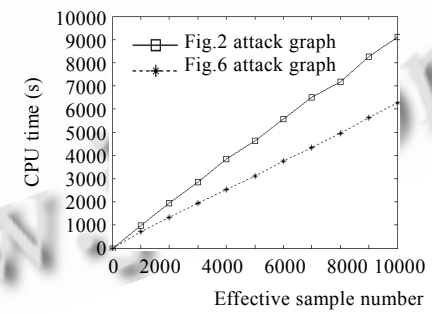


Fig.4 Sampling CPU time curves

图 4 采样 CPU 时间曲线

4 结束语

随着网络攻击图更多地应用于实时网络安全管理技术领域,如何根据攻击证据合理地计算攻击图节点置信度成了亟待解决的问题.本文提出一种基于贝叶斯后验推理的攻击图节点置信度计算方法,对传统的似然加权法进行了改进.

实验表明,算法能够根据观测到的攻击证据合理地计算攻击图节点置信度,且具有线性计算复杂度,适合处理大规模攻击图节点置信度的实时计算更新问题.未来的研究方向包括:

1) 将算法应用于网络安全态势感知领域,根据节点置信度的动态变化找出最有可能已经发生的攻击序列,并预测未来各种后续攻击发生的可能性;
2) 将算法应用于主动安全防御领域,根据后续攻击序列的发生概率,找到性价比最高的防御方案;
3) 与告警关联结合,改进现有基于攻击图图距的告警关联方法[12].

致谢 我们向上海交通大学信息安全工程学院及上海市信息安全综合管理技术研究重点实验室所有参与网络入侵路径协同分析工程的同学和老师表示衷心感谢.

References:

[1] Shi J, Guo S, Lu Y, Xie L. An intrusion response method based on attack graph. Journal of Software, 2008,19(10):2746−2753 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/2746.htm [doi: 10.3724/SP.J.1001.2008.02746]

[2] Wang Y, Xian M, Liu J, Wang G. Study of network security evaluation based on attack graph model. Journal on Communications, 2007,28(3):29−34 (in Chinese with English abstract).

[3] Sheyner O, Haines J, Jha S, Lippmann R, Wing J. Automated generation and analysis of attack graphs. In: Williams D, ed. Proc. of the 2002 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2002. 273−284.

[4] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs. In: Jacobs A, ed. Proc. of the 15th IEEE Computer Security Foundations Workshop. Nova Scotia: IEEE Computer Society, 2002. 49−63.

[5] Valeur F, Vigna G, Kruegel C, Kemmerer R. A comprehensive approach to intrusion detection alert correlation. IEEE Trans. on Dependable and Secure Computing, 2004,1(3):146−169. [doi: 10.1109/TDSC.2004.21]

[6] Noel S, Robertson E, Jajodia S. Correlating intrusion events and building attack scenarios through attack graph distances. In: Proc. of the 20th Computer Security Applications Conf. Tucson: IEEE Computer Society, 2004. 350−359. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01377242.

[7] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems. In: Proc. of the '99 IRIS National Symp. on Sensor and Data Fusion. Laurel: IEEE Computer Society, 1999. 24−27. http://citeseerx.ist.psu.edu/viewdoc/download?doi:10.1.1.51.1753&rep=rep1&type=pdf.

[8] Zhai Y, Ning P, Iyer P, Reeves D. Reasoning about complementary intrusion evidence. In: Proc. of the 20th Annual Computer Security Applications Conf. Tucson: IEEE Computer Society, 2004. 39−48. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.4398&rep=rep1&type=pdf.

[9] Yu D, Frincke D. Improving the quality of alerts and predicting intruder's next goal with hidden colored Petri-net. Computer Networks, 2007,51(3):632−654. [doi: 10.1016/j.comnet.2006.05.008]

[10] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis. In: Atluri V, ed. Proc. of the 9th ACM Conf. on Computer and Communications Security. Washington: Association for Computing Machinery, 2002. 217−224.

[11] Zhang L, Guo H. Introduction to Bayesian Networks. Beijing: Science Press, 2006 (in Chinese).

[12] Zhang S, Li J, Chen X, Fan L. Building network attack graph for alert causal correlation. Computers & Security, 2008,27(5-6):188−196. [doi: 10.1016/j.cose.2008.05.005]

附中文参考文献:

[1] 石进,郭山清,陆音,谢立.一种基于攻击图的入侵响应方法.软件学报,2008,19(10):2746−2753. http://www.jos.org.cn/1000-9825/19/2746.htm [doi: 10.3724/SP.J.1001.2008.02746]

[2] 王永杰,鲜明,刘进,王国玉.基于攻击图模型的网络安全评估研究.通信学报,2007,28(3):29−34.

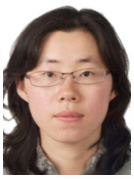
[11] 张连文,郭海鹏.贝叶斯网引论.北京:科学出版社,2006.

张少俊(1978－),男,上海人,博士生,主要研究领域为计算机网络安全综合管理.

李建华(1965－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,信息处理,计算机通信网.

宋珊珊(1985－),女,硕士生,主要研究领域为计算机网络安全综合管理.

李斓(1977－),男,博士,讲师,主要研究领域为计算机系统访问控制.



陈秀真(1977－),女,博士,讲师,主要研究领域为计算机网络风险评估.