基于贝叶斯网络的网络攻击威胁评估分析研究

孙立健，王培超，周鋆，张维明

摘　要：近年来，随着互联网的发展，网络威胁不断加深，网络异常行为分析变得十分重要。目前主流的网络异常行为分析本质上为贝叶斯网络模型。本文基于贝叶斯网络，对网络威胁要素进行建模，利用评分搜索算法对模型进行结构学习，之后利用贝叶斯网络推理来对整体威胁进行风险分析和计算。

关键字：贝叶斯网络 网络异常行为 威胁评估 风险分析

Research on Risk Analysis of Cyber Attack Threat with a Bayesian Network

Sun Lijain,Wang Peichao,Zhou Yun,Zhang Weiming

Abstract：In recent years, with the development of the Internet, network threats have deepened and network anomaly behavior analysis has become very important. The current mainstream network anomaly behavior analysis is essentially a Bayesian network model. Based on the Bayesian network, this paper models the network threat elements, uses the scoring search algorithm to build the structure of the model, and uses Bayesian network inferringto analyze and calculate the overall threat.

Key words：Bayesian Network ; Network Anomaly Behavior ;Threat Assessment ;Risk Analysis

一、 前言

近年来，随着互联网的发展，网络威胁不断加深，如何对网络攻击威胁进行评估分析已经成为了当前的热点研究问题。针对网络攻击进行威胁评估是为了评估威胁可能的原因与影响程度，为信息系统的建立、安全策略的确定，以及系统的安全运行提供保障。目前国内外对网络攻击越来越重视，针对其威胁程度和原因开展了多项研究，主要有层次分析法、模糊综合评判法、状态转移算法、贝叶斯网络分析法[1]。其中，层次分析法和模糊综合评判法主观性强，并且是静态分析，不能对整个系统的威胁原因进行动态分析。而状态转移法通过对模型进行构建，利用内部采集的数据或外部获取的信息计算不同状态间的条件转移概率。这种状态转移图模型利用状态间的相关性或因果关系对用户在网络空间中的行为进行描述，本质上还是属于有向的概率图模型，即贝叶斯网络模型。另外，这种半自动的模型构建方式，过多依赖于领域专家的输入，无法适用于大规模网络及大数据的环境条件，无法应对未知的高级可持续性威胁（APT）攻击的挑战。因此，需要研究如何自动的从已有数据和知识中获取模型的结构和参数，实现高效的网络攻击威胁评估计算，即研究贝叶斯网络的学习和推理过程[2-4]。

二、 贝叶斯网络

贝叶斯网络是一个有向无环图，其节点代表随机变量，节点间的箭线代表随机变量间的依赖关系[1]。假设用θ表示节点（变量）在集合$\boldsymbol{X}$中的联合概率分布，用G=(U,E)表示有向无环图（DAG）。令$\boldsymbol{X}=\{X_1,\ldots,X_n\}$代表一个随机变量（连续或离散）的集合，集合中每个变量

第一作者：孙立健
单位：国防科技大学重点实验室
职称：研究生在读
联系电话：18569033686
通讯地址：湖南省长沙市国防科技大学系统工程学院
电邮地址：yzzxnblbq@163.com

X_i都取有限值或在一定的范围内取值。网络结构中的节点集$\boldsymbol{X}=\{X_1,\ldots,X_n\}$与模型中的随机变量一一对应，网络结构中的边$E$表示变量间的条件依赖关系。如果$(G,\theta)$满足局部马尔科夫条件（Local Markov condition），即已知父节点时，X_i与其非子节点条件独立，那么这里就可以称(G,θ)模型为一个 BN 模型。结构学习的任务就是在给定标注数据的基础上，自动智能地学习出准确的贝叶斯网络拓扑结构G。基于评分搜索的方法是一种常用的结构学习方法，分为评分函数和搜索算法两部分，其核心思想是把结构学习问题处理为模型选择问题，即基于评分规则，评价候选结构与标注数据D的拟合度，在候选结构组成的空间上搜索评分最高的结构。

$$\hat{G}=argmax_{G\in\Omega}\ell(G,D)$$

这里，$\ell(G,D)$是标注数据拟合候选结构的对数似然度（log-likelihood），拟合越好，则$\ell(G,D)$越高；Ω是用来存放所有可能候选结构对应邻接矩阵的集$\Omega=\{A\in\mathbb{Z}^{n\times n}\}$。

贝叶斯网络可以用一个二元组$(G,\boldsymbol{P})$进行形式化的表示，其中G代表贝叶斯网络的结构，该结构蕴含了存在于$\boldsymbol{X}$中的变量的间的关系，$\boldsymbol{P}$ 是与每个变量相关的条件概率分布的集合。进一步地，$\boldsymbol{P}=\{P_i\}$，$P_i=P(X_i|\pi(X_i))$，其中$\pi(X_i)$代表节点集合$\boldsymbol{X}$中X_i的父节点，节点满足马尔科夫性质的联合概率分布如下所示：

$$P(\boldsymbol{X})=\prod_i P(X_i|\pi(X_i))$$

对于一个节点代表离散变量的贝叶斯网络来说，每一个节点的概率分布情况由条件概率表（Conditional Probability Table，CPT）给出，相应节点的 CPT 包含了在给定父节点取值的情况下，当前节点取特定值的概率大小[错误!未找到引用源.]。在获取了特征和原始数据后，便可以利用贝叶斯结构学习算法对模型进行构建。

对网络攻击威胁评估的贝叶斯网络进行参数学习，需要利用先前的历史资料和数据，以确定不同属性节点的先验分布，本文利用贝塔分布来模拟先验分布。当没有历史数据时，采用均匀分布拟合先验分布，即贝塔分布的参数取值为 1。后利用入侵检测系统获得的实时攻击数据，结合贝塔先验分布，通过贝叶斯估计进行参数学习与更新。

三、 贝叶斯网络的更新

本文对贝叶斯网络的更新采用联结树推理方法，基本思路是先将贝叶斯网络转换为一种二次结构（Second Structure, SS），再通过对二次结构的推理得到贝叶斯网络的推理的精确结果。这里，SS=(JT,PP)，其中：JT=(C,S)为联结树，C 为贝叶斯网络中的团集，S 为 JT 中的边集；PP 为与团和边相关的概率势，可从每个团中的变量的联合概率分布计算得到。在 SS 上计算联合概率是通过计算 JT 上团和边的 PP 实现的。

无约束贝叶斯网络的更新与推理是 NP 难问题，对于复杂的贝叶斯网络模型，涉及变量多，推理计算很难在多项式时间内完成。在本文中，部分贝叶斯网络结点可能用特殊的概率分布来进行建模，即结点状态空间连续。连续结点和离散结点共存的贝叶斯网络也称为混合贝叶斯网络，其精确推理只支持部分特殊的情况，如条件高斯概率分布。因此，本文引入贝叶斯网络近似推理的方法。

近似推理通过对节点状态进行采样，对采样样本进行统计分析得到一个近似的推理结果。近似推理算法所使用的采样方法在耗费时间和计算复杂程度上都比精确推理的计算过程小很多，特别是应用到复杂的网络，近似推理的优越性明显。这里，本文将采用动态离散的联结树推理算法（Dynamic Discretization Junction Tree Algorithm，DDJT），对单任务下的模型进行近似的计算推理。

动态离散的联结树推理方法核心在于动态离散的过程，即将连续的变量（假设其域值范围是Ω，概率分布函数为f）离散化，离散化的首要步骤是将域值范围Ω分割成一系列间隔小段（intervals）的集$\psi=\{\varpi_i\}$，然后在些间隔小段上定义一个局部连续的概率分布函数$\tilde{f}$。动态离散推理过程就是在Ω中找到高密度区域，并对其进行较为准确的分割，在给定模型和观

测证据的情况下，继续计算新的域值范围分割ψ，并测试离散化后的概率分布函数$\tilde{f}$与真实f之间的差异是否小于一定的条件。如果条件满足则算法停止，如果不满足则在该区域进行进一步的分割，如此往复迭代，直至收敛。

动态离散的联结树推理算法相对于离散的联结树推理算法，它可以处理包含连续结点的贝叶斯网络推理问题。此外，相对于静态离散方法，动态离散能够更好地将连续变量离散化，提高离散后的分布的准确性，从而提高推理精度。

通过对贝叶斯网络进行学习与更新，可以依据数据的实时变化来更新网络攻击威胁模型，进而分析得出网络攻击威胁的成因，为保障信息系统的安全提供保证。

四、 网络攻击威胁模型

根据上一节中构建的贝叶斯网络，本文接下来利用其构建网络攻击威胁评估模型。网络攻击模型的贝叶斯网络受多个因素的影响，对于一个信息系统所遭受的 Web 攻击风险，可以由其自身运行维护情况、自身存在漏洞的情况和其遭受攻击的情况共同确定。通过上述的描述形式，可以构建下图 1 所示的网络攻击威胁模型，其中每个圆形节点代表网络攻击威胁可能的来源，其节点之间相互关联。梳理节点与节点、节点与边、边与边之间的关系，构建得到贝叶斯网络，从而反映一个信息系统遭受 Web 攻击的风险因素之间的关系。

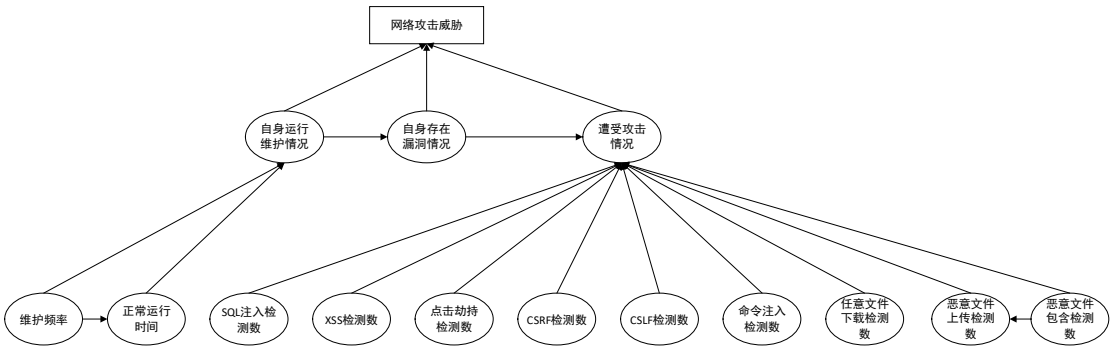

图 1 Web 攻击风险因素图

风险因素的具体说明如下：

（1）自身运行维护情况：代表了一个信息系统自身受到维护的情况，由维护频率和正常运行时长两部分组成，其中维护频率MF是指在某时间段内对该信息系统的维护频率，正常运行时长NT是自系统上次被成功攻击并被修复后正常运行的时长，维护频率的不同对系统正常运行时间产生影响，维护频率越高，系统正常运行时间越长；

（2）自身存在漏洞情况：代表了一个信息系统自身存在的风险情况，通过对信息系统自身存在的未修补漏洞进行扫描，可确定其威胁程度，记作N_{sev}，sev代表相应漏洞的威胁程度，包含高（$high$）、中（$medium$）、低（low）三个等级状态。当自身运行维护情况良好时，可以有效减少系统的漏洞；

（3）遭受攻击情况：代表了一个信息系统目前被攻击者的刺探情况。对不同类型的攻击数量根据特定的时间段进行统计，记为N_{atk}^{α}，atk代表利用相应类型攻击，α代表具体的时间段。在本文中，$atk \in \{sqli, xss, cj, csrf, crlfi, ci,\ mfu, rfd, mfi\}$，分别代表 SQL 注入、XSS、点击劫持、CSRF、CRLF 注入、命令注入、恶意文件上传、任意文件下载和恶意文件包含。时间段需要根据决策者的经验进行决定，例如当决策者将α设定为 2h 时，需统计在 2h 内检测到的相应攻击的数量。当系统存在大量漏洞时，系统遭受攻击的情况会更加严重，系统所遭受的损失也更大。同时，当系统中存在大量的恶意文件时，恶意文件上传检测数也会随之上升。

通过利用上述因素以及数据构建贝叶斯网络，对 Web 攻击的风险进行定量刻画，可以达到网络攻击的威胁进行评估的目的，确定网络攻击威胁的风险程度。

五、 网络攻击威胁评估

网络攻击威胁的目的通常是希望能根据对模型中网络风险的观察，结合已知的模型信息和经验知识，通过计算推理来获得关于可能的网络攻击威胁表现，并对整体威胁进行风险分析和计算，给出网络攻击的威胁来源。

在上一节中对网络攻击威胁模型进行了构建。因此，利用上述模型，对网络攻击的威胁进行评估，对于任意时刻，贝叶斯网络模型中的某个属性节点 X_i,根据其自身节点的条件概率表以及其父节点被获取的概率，可以求得该节点 X_i 被获取的概率 $P(X_i)$,同时根据计算得到的对应网络威胁因素的威胁程度值 A_i，可求得该节点 X_i 被获取的威胁值 R_i 如公式所示：

$$R_i = P(X_i) \times A_i$$

进一步的到系统的网络攻击威胁值如公式所示：

$$R_{total} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} \left(P(X_i) \times A_i \right)$$

通过上式，可以计算得到网络攻击威胁值，对整体威胁进行风险分析和计算。

六、 总结

本文的目标在于通过构建网络攻击威胁模型，以信息系统为研究对象进行系统的网络攻击威胁评估。文中首先引入了贝叶斯网络，然后构建该网络环境下的贝叶斯攻击图结构模型，最后，根据贝叶斯参数学习动态更新节点概率并结合数据动态计算系统的网络攻击威胁值，通过 MATLAB 仿真模拟该系统的动态威胁过程，可以验证本文提出的网络攻击威胁模型及方法的准确性和有效性。

参考文献：

[1] 常昊,秦元庆,周纯杰.基于贝叶斯攻击图的工控系统动态风险评估[J].信息技术,2018,42(10):62-67+72.

[2] Chockalingam S, Pieters W, Teixeira A, et al. Bayesian Network Models in Cyber Security: A Systematic Review [C]// Estonia: Nordic Conference on Secure IT Systems. Springer, 2017: 105~122.

[3] Wu J, Yin L, Guo Y. Cyber Attacks Prediction Model Based on Bayesian Network [C]// Singapore: International Conference on Parallel and Distributed Systems, 2013:730~731.

[4] Kwan M, Chow K P, Lai P, et al. Analysis of the Digital Evidence Presented in the Yahoo! Case [J]. 2009, 306: 241~252.

[5] Zhou Y, Fenton N, Zhu C. An Empirical Study of Bayesian Network Parameter Learning with Monotonic Influence Constraints [J]. Decision Support Systems, 2016, 87: 69~79.

[6] Glover F. Tabu Search: A Tutorial [J]. Interfaces, 1990, 20(4): 74~94.