文章编号：2095-4980(2023)11-1370-11

基于贝叶斯网络的攻击事件智能发掘模型

李岳峰，刘　丹

(电子科技大学 电子科学技术研究院，四川 成都 611731)

摘　要：针对目前传统入侵检测系统难以得出网络攻击行为之间存在的关联关系问题，以攻击图表示模型为指引，提出一种基于贝叶斯网络的攻击事件智能发掘模型。本文以先验知识建立贝叶斯攻击行为关联图。基于属性相似度聚合网络攻击行为，针对网络攻击场景设计高效的Ex-Apriori算法发掘攻击行为间的关联规则，并建立攻击行为组集。利用贝叶斯攻击行为关联图的参数对攻击行为组集进行计算，实现对攻击事件的发掘。实验表明，本模型能有效提取网络攻击事件及发现攻击路径，为网络攻击事件的发现与应对措施提供理论支持和技术支撑。

关键词：网络攻击图；贝叶斯网络；关联分析；改进Apriori算法

中图分类号：TN929.5　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021291

Intelligent mining model of attack events based on Bayesian network

LI Yuefeng，LIU Dan

(Research Institute of Electronic Science and Technology，University of Electronic Science and Technology of China，Chengdu Sichuan 611731，China)

Abstract：It is difficult for traditional intrusion detection systems to obtain the relationship among network attack behaviors. Taking an attack graph representation model as a guide，an intelligent mining model of attack events based on Bayesian network is proposed. A Bayesian attack association graph is established based on prior knowledge. The network attack behaviors are aggregated based on attribute similarity. An efficient Ex-Apriori algorithm is designed for network attack scenarios to discover the association rules among the attack behaviors，and the attack behavior group set is established. Finally，the attack behavior group set is calculated by using the parameters of the Bayesian attack association graph to realize the discovery of attack events. Experiments show that this model can effectively extract network attack events and discover attack paths，and provide theoretical and technical support for the discovery and countermeasures of network attack events.

Keywords：network attack graph；Bayesian network；association analysis；improved Apriori algorithm

近年来，不断演变的网络威胁环境让网络攻击情况变得更为复杂，发起网络攻击的入侵者大多不再采用单一的攻击方式，而是在一段时间内通过多种攻击行为的相互配合来达到攻击目的。

在攻击事件的发掘方面，ZHANG等[1]对特定的时间窗口中的告警序列进行分析，然后提取时间窗口内的多阶段攻击行为进而发掘攻击事件，但是时间窗口大小无法确定导致发掘的攻击事件不完全；冯学伟等[2]面向原始告警数据，提出了一种基于Markov性质的发掘方法，通过对因果关系进行建模并利用该方法提取攻击事件，但是该方法输入原始数据会导致检测精确度不高；陆江东等[3]采用Apriori算法对攻击事件进行关联发掘并取得了良好效果；刘文彦等[4]总结了不同的攻击事件发掘模型并分析了不同模型的攻击成功概率。

在发现攻击路径方面，Kumar等[5]分析攻击者可利用的资源构建攻击树进而分析攻击路径；Gadyatskaya等[6]利用ADTool构建攻击树便于对网络攻击进行可视化分析；Bopche等[7]研究动态网络与攻击路径随时间变化的规律；胡浩等[8]提出基于吸收Markov链的攻击路径预测方法，利用节点的被攻击次数和攻击路径长度的期望值来预测攻击步骤；Katarya等[9]通过对系统漏洞进行评估，在提高安全性的同时也构建了存在的攻击路径，但是在真实环境中测试效果不佳。以上几种方法没有深入考虑攻击行为的关联关系，这也导致攻击路径中的一些节点

收稿日期：2021-07-20；修回日期：2021-09-02

出现偏差。

在攻击图的研究方面，Noel 等[10]通过关联事件计算对应的攻击图距离；Liu 等[11]分析告警日志并使用维特比方法构建攻击图从而实现攻击意图识别；杨豪璞等[12]研究面向多阶段攻击的攻击图构建与攻击场景关联方法；Yi 等[13]提出了自动分析网络安全风险并为潜在攻击生成攻击模型的框架；王洋等[14]通过研究攻击图来识别网络入侵的意图。不过，上述几种方法受限于网络规模。

在基于贝叶斯网络分析网络攻击方面，Poolsappasit 等[15]结合贝叶斯网络与攻击图提出一种适用于动态分析的风险评估模型，该方法也将资源可用性用于分析，但是其算法效率不高；Hu 等[16]提出了一种关于贝叶斯攻击图的自适应网络防御的算法，实现了安全风险量化；Matthews 等[17]提出了循环贝叶斯攻击图，能较好地评估攻击者意图，但是该方法仅限于计算单个状态转移概率，无法计算综合转移概率。以上 3 种方法证明贝叶斯网络在分析网络攻击方面能取得较好的效果。

针对以上问题，本文提出一种基于贝叶斯攻击行为关联图(Bayesian Attack Association Graph，BAAG)生成算法与 Ex-Apriori 算法的两阶段攻击事件智能发掘模型(Two-Stage Attack Event Intelligent Mining Model，TAEIM)，主要做了如下工作：

1) 模型的第 1 阶段基于贝叶斯网络与攻击行为关联函数构建贝叶斯攻击行为关联图，通过攻击行为关联函数对包含攻击行为序列的 CICIDS2017 数据集进行处理，再使用 BAAG 生成算法得到攻击行为之间转移的综合概率，并进一步得到贝叶斯攻击行为关联图的详细参数分布，为后续阶段精确发现攻击路径中的各个节点提供可靠图模型。

2) 模型的第 2 阶段针对网络攻击场景设计了高效的 Ex-Apriori 算法，使用基于属性相似度聚合攻击行为的方法与 Ex-Apriori 算法对实际环境下的网络攻击数据集进行处理，剔除非频繁项集，能有效应对大规模网络，同时将攻击行为属性作为参考，发现攻击行为间的关联规则并建立攻击行为组集。最后将贝叶斯攻击行为关联图的参数与攻击行为组集进行计算，以此将不同的攻击行为连接成为置信度更高的攻击序列，达到发掘完整攻击事件的目的，并为进一步发现攻击路径提供支撑。

1　攻击事件相关定义

攻击事件发掘的基础是其递进式的攻击方式，相关定义如下：

定义 1：网络攻击行为(Attack Behavior，Ab)

网络攻击行为是形如 $Ab=(timestamp, Protocol, sIP, dIP, sPort, dPort, msg)$ 的七元组，其中 timestamp 表示这个攻击行为的时间戳，Protocol 表示攻击行为的网络包协议类型，sIP、dIP、sPort、dPort 分别表示源 IP 地址、目的 IP 地址、源端口和目的端口，msg 表示攻击名称。

定义 2：网络攻击阶段(Attack Stage，AS)

通过对网络攻击行为的不同特征进行分类可以将 AS 分为 5 个部分，分别为：信息收集阶段、入侵提权阶段、潜伏扩展阶段、数据窃取阶段、攻击退出阶段。Ab_{ij} 表示 AS 中 i 阶段的第 j 个网络攻击行为。

定义 3：网络攻击事件(Attack Event，AE)

网络攻击事件是将若干个网络攻击行为根据时间顺序或者逻辑顺序构建的一个完整的网络攻击流程，可以用向量 $\boldsymbol{AE}=\{Ab_{11}, Ab_{21}, \cdots, Ab_{mn}\}$ 表示。

定义 4：攻击行为组集(Attack Group，AG)

攻击行为组集由若干个包含多个网络攻击行为的集合所组成，且对于任意 $\boldsymbol{AE}$，均有 $\boldsymbol{AE} \in \boldsymbol{AG}$。

定义 5：攻击行为全集合(Attack Collection，AC)

攻击行为全集合由多个攻击行为组集 $\boldsymbol{AG}$ 组成，且对于任意 $\boldsymbol{AG}$，均有 $\boldsymbol{AG} \in AC$。

网络攻击行为、网络攻击阶段与网络攻击事件三者对应的关系如图 1 所示，图中左侧文字表示不同的网络攻击阶段，右侧的单个圆为单个网络攻击行为，例如 Ab_{11} 代表信息收集阶段的第 1 个攻击行

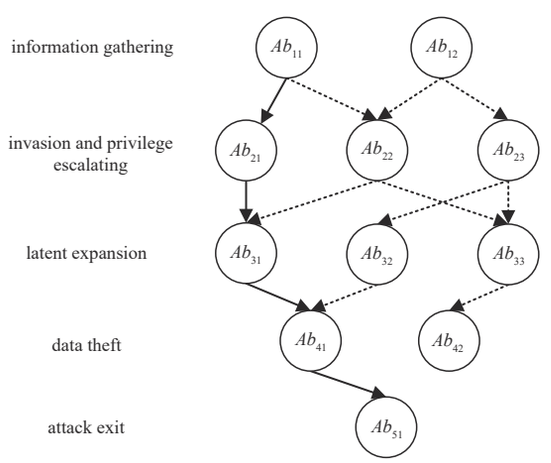

Fig.1 Relationship among attack behavior, attack stage and attack event

图 1　网络攻击行为、网络攻击阶段、网络攻击事件的关系

为，图中所有的网络攻击行为构成了攻击行为全集合，箭头代表不同的攻击行为之间存在的攻击顺序关系，多个互不相同的攻击行为顺序组合形成了攻击行为组集，图中由实线连接的向量集合$\{Ab_{11},Ab_{21},Ab_{31},Ab_{41},Ab_{51}\}$表示1个攻击事件。

2 TAEIM模型

本节详细介绍了TAEIM模型，首先说明了模型结构，包括模型2个阶段的处理流程，然后描述了BAAG算法的具体实现过程，并介绍了基于Ex-Apriori算法提取攻击行为组集与关联规则的方法，最后通过TAEIM模型实现对攻击事件的发掘。

2.1 模型结构

TAEIM模型由两阶段组成。在第1阶段首先使用攻击行为关联函数对包含先验知识的数据集进行处理，并基于BAAG生成算法构建贝叶斯攻击行为关联图，作为后续阶段的输入。在第2阶段首先收集网络攻击行为并进行预处理，采用基于属性相似度聚合的方法将收集的攻击行为进行相似度判断并删除冗余信息，得到攻击行为全集合，接着使用Ex-Apriori算法发现攻击行为间的关联规则，从而获取攻击行为组集。最后将已构建的贝叶斯攻击行为关联图与攻击行为组集进行匹配与计算，对于存在映射关系的攻击行为组集，发掘出完整的攻击事件，TAEIM模型如图2所示。

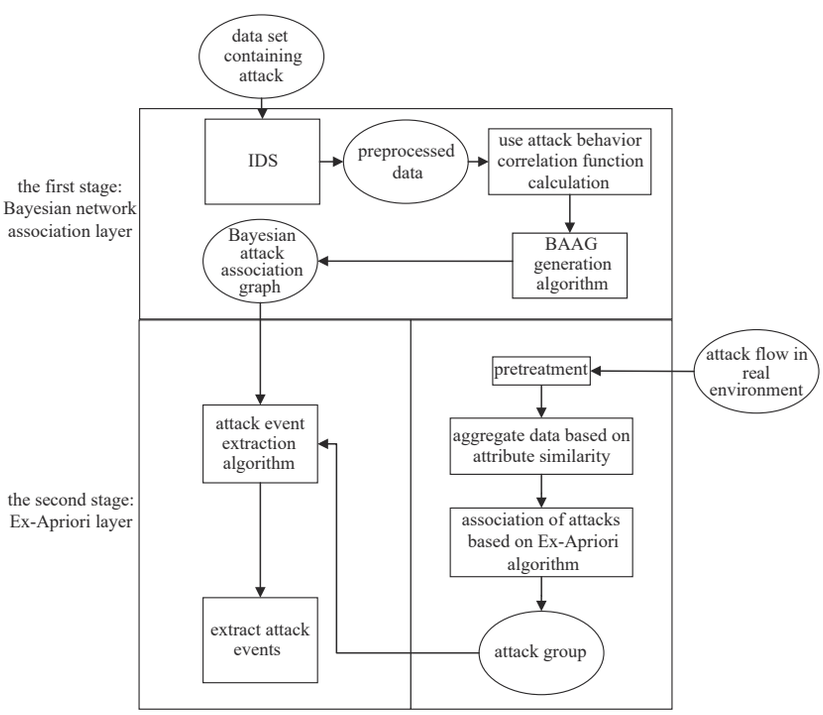

Fig.2 TAEIM model
图2 TAEIM模型

2.2 BAAG生成算法

贝叶斯网络和攻击事件同属于有向无环图，图中的边代表相连的2个节点存在因果关系，因此基于该特点可以将攻击事件的整个流程以贝叶斯网络的形式展示，生成基于贝叶斯网络的攻击行为关联图。

2.2.1 基本定义

构建贝叶斯攻击行为关联图之前，首先对相关要素进行定义：

定义6：贝叶斯攻击行为关联图(BAAG)是由多个网络攻击行为组成的网络拓扑结构，表示为$BAAG=(G,E)$，具体定义如下：

1) G为节点集合，每一个节点代表一个网络攻击行为，表示为$G=\left\{Ab_{11}\cup Ab_{21}\cup\cdots\cup Ab_{mn}\right\}$。

2) E为有向边集合，表示图中不同节点之间的转移概率，用$E=\left\{e_i|i=1,2,\cdots,k\right\}$表示。

定义7：概率分布表(Conditional Probability Table，CPT)

表示了在贝叶斯攻击行为关联图中，父节点向其不同子节点转移的概率分布。

定义 8：概率转移矩阵(Transition Probability Matrix，TPM)

将所有概率分布表中的数据用概率转移矩阵表示，横向和纵向表示的是攻击行为，矩阵中每一个值表示从横向攻击行为到纵向攻击行为的转移概率，如图 3 所示，其中 P_i 代表转移概率。

attack behavior	sniff	port scan	Trojan horse implantation	backdoor connection	remote command	file access
sniff		P_1	P_2			
port scan			P_3			
Trojan horse implantation				P_4	P_5	
backdoor connection					P_6	P_7
remote command				P_8		
file access				P_9		

Fig.3 Transition probability matrix

图 3　转移概率矩阵

2.2.2 构建贝叶斯攻击行为关联图

构建贝叶斯攻击行为关联图分为 3 个步骤，分别是数据集预处理、攻击行为关联度计算、BAAG 生成。

第 1 步的数据集预处理需要对重复或者无用的数据进行删除，此步骤主要为了降低后续处理冗余数据所造成的资源浪费。

第 2 步的攻击行为关联度计算是基于攻击行为关联函数(Attack Behavior Correlation Function，AF)来对数据集中的攻击行为对添加参数。

第 3 步使用 BAAG 生成算法生成贝叶斯攻击行为关联图，此步骤是构建 TAEIM 模型第一阶段的主要部分。

AF 函数主要通过计算 2 个攻击行为在不同属性上的关联度来得出总的关联程度，描述如下：

$$F\left(Ab_{ij},Ab_{mn}\right)=\sum_{i}^{k}\delta_k F_k\left(Ab_{ij},Ab_{mn}\right) \tag{1}$$

式中：Ab_{ij},Ab_{mn} 为 2 个攻击行为；δ_k 为第 k 个属性的权重；$F_k\left(Ab_{ij},Ab_{mn}\right)$ 为第 k 个属性的关联度函数，攻击行为关联度的属性包括攻击行为、IP、时间戳。

对于攻击行为属性关联度，首先要将攻击行为基于攻击阶段分类，然后对于 2 个攻击行为 Ab_{ij},Ab_{mn}，其攻击行为关联度为：

$$F_{\text{Ab\_msg}}(Ab_{ij},Ab_{mn})=\begin{cases}1/\gamma^2, & \gamma>1\\ 0, & \gamma=0\end{cases} \tag{2}$$

$$\gamma=\Lambda(Ab_{ij},Ab_{mn}) \tag{3}$$

式中 $\Lambda(Ab_{ij},Ab_{mn})$ 为 2 个攻击行为所属网络攻击阶段的差值。

对于 IP 的属性关联度，IP 作为网络中的地址认证，在攻击行为关联度的计算中极为重要，采用式(5)来定义 2 个攻击行为之间 IP 地址的关联度：

$$F_{\text{Ab\_IP}}(Ab_{ij},Ab_{mn})=\max\left\{A(sIP_{ij},sIP_{mn}),A(dIP_{ij},dIP_{mn})\right\} \tag{4}$$

$$A(IP_{ij},IP_{mn})=\sum_{i}^{h}\frac{\tau_h e}{PB} \tag{5}$$

式中：$A(IP_{ij},IP_{mn})$ 为 Ab_{ij} 与 Ab_{mn} 两个攻击行为的 IP 关联程度；τ_h 为 IP 地址中按字节顺序排列的部分的相同程度；P 为 IP 地址中按字节排序的位置；B 为 IP 地址的总字节数。

对于时间戳的属性关联度，在包含多阶段攻击行为的攻击事件中，若 2 个攻击行为所处的攻击阶段相同，则时间间隔 ΔT 相对较短，对于处在不同攻击阶段的 2 个攻击行为，ΔT 可能大得多。因此将时间戳属性的关联度函数定义如下：

$$F_{\text{Ab\_time}}(Ab_{ij},Ab_{mn})=\mathrm{e}^{\frac{1}{\Delta T+1}} \tag{6}$$

$$\Delta T=\left|T\left(Ab_{ij}\right)-T\left(Ab_{mn}\right)\right| \tag{7}$$

式中：$T(Ab_{ij})$为Ab_{ij}发生的时间；$T\left(Ab_{mn}\right)$为Ab_{mn}发生的时间。

利用AF函数可以得出任意2个攻击行为的关联度，进一步可以基于贝叶斯网络构建贝叶斯攻击行为关联图，从而为TAEIM模型的第2阶段提供可靠的图模型，BAAG生成算法如下：

algorithm 1 BAAG generation algorithm

input:data set L, relevance threshold ∂

output:Bayesian attack association graph *BAAG*

BEGIN

1. Algorithm initialization
2. Unify and standardize L and obtain the preprocessed data A
3. for $l \in A$,get source IP address *SrcIP*,destination IP address *DstIP*,time *T*,Attack name *msg*
4. for each $(Ab_{ij}, Ab_{mn}) \in A$ do
5. if $F(Ab_{ij}, Ab_{mn}) > \partial$ and Ab_{ij} or Ab_{mn} not in G:
6. add Ab_{ij} or Ab_{mn} as a node to G
7. end for
8. for each $(Ab_{ij}, Ab_{mn}) \in G$ do
9. add edge to E, the weight is (Ab_{ij}, Ab_{mn}) support degree of the child node to the parent node
10. end for
11. delete useless edges and nodes
12. generate $BAAG=(G,E)$
13. generate CPT and TPM
14. end for

END

2.3 基于Ex-Apriori算法的攻击行为组集提取

Ex-Apriori算法是针对Apriori算法在网络攻击场景下效率低下且精确度不高的问题而设计的。通过拆分数据集提高处理效能，对攻击行为全集合设置合适的支持度来不断提取频繁项集，同时利用置信度进一步筛选得到攻击行为间的关联规则，其后使用提升度得到具有不同的相关性的各类频繁项集，最后通过对项集进行剪枝获取攻击行为组集。

2.3.1 要素定义

关于Ex-Apriori算法的要素定义如下：

定义9：支持度(Support)

支持度表示关联的数据集合在AC中出现的次数N在AC中所占的比例，对于关联的集合$\left\{Ab_{ij}, Ab_{mn}\right\}$，其对应的支持度如式(8)所示。

$$Support\left(Ab_{ij}, Ab_{mn}\right)=N\left(Ab_{ij}, Ab_{mn}\right)/N\left(AC\right) \tag{8}$$

式中：$Support\left(Ab_{ij}, Ab_{mn}\right)$为攻击行为$Ab_{ij}$与$Ab_{mn}$的支持度；$N\left(Ab_{ij}, Ab_{mn}\right)$为$Ab_{ij}$与$Ab_{mn}$在数据集$AC$中出现的次数；$N\left(AC\right)$为总数据集的大小。

定义10：置信度(Confidence)

置信度表示在攻击行为Ab_{ij}发生的情况下攻击行为Ab_{mn}发生的概率，即Ab_{ij}和Ab_{mn}同时发生的次数占Ab_{ij}发生的次数的比例，如式(9)所示。

$$Confidence(Ab_{ij} \rightarrow Ab_{mn})=P\left(Ab_{mn}|Ab_{ij}\right)=P\left(Ab_{ij}, Ab_{mn}\right)/P\left(Ab_{ij}\right) \tag{9}$$

式中：$Confidence(Ab_{ij} \rightarrow Ab_{mn})$为攻击行为$Ab_{ij}$对$Ab_{mn}$的置信度；$P\left(Ab_{mn}|Ab_{ij}\right)$为在$Ab_{ij}$已经发生的情况下$Ab_{mn}$发生的概率。

定义11：提升度(Lift)

提升度代表置信度$Confidence(Ab_{ij} \rightarrow Ab_{mn})$与$Ab_{mn}$攻击行为发生概率之比，如式(10)所示。

$$Lift(Ab_{ij} \rightarrow Ab_{mn})=Confidence(Ab_{ij} \rightarrow Ab_{mn})/P\left(Ab_{mn}\right) \tag{10}$$

$Lift(Ab_{ij} \to Ab_{mn})$ 为 Ab_{ij} 与 Ab_{mn} 的提升度，若 $Lift(Ab_{ij} \to Ab_{mn}) > 1$，则随着 $Lift(Ab_{ij} \to Ab_{mn})$ 的增加，Ab_{ij} 与 Ab_{mn} 的正相关性也越高；若 $Lift(Ab_{ij} \to Ab_{mn}) < 1$，则随着 $Lift(Ab_{ij} \to Ab_{mn})$ 的减小，Ab_{ij} 与 Ab_{mn} 的负相关性越高；若 $Lift(Ab_{ij} \to Ab_{mn}) = 1$，表示 Ab_{ij} 与 Ab_{mn} 无相关性。

定义 12：攻击行为频繁项集 F

攻击行为频繁项集表示在发生多个网络攻击行为时，支持度大于等于最小支持度的多个攻击行为。

2.3.2 基于属性相似度的攻击行为聚合

使用基于属性相似度的攻击行为聚合方法处理实际环境下的网络攻击流数据，可以减少冗余信息，而经过该方法输出的攻击行为全集合可以作为 Ex-Apriori 算法的输入。

基于属性相似度的攻击行为聚合是指如果在一定时间内实施的多个攻击行为之间存在属性相似度且高于阈值 h，则可以将这些攻击行为聚合。基于单位时间内不同攻击行为的属性，将攻击行为之间的相似度定义如下：

定义 13：攻击行为相似度(SIM)

若 2 个攻击行为的 $(sIP, dIP, sPort, dPort, msg)$ 完全相同，为同一个攻击行为，SIM 为 1；对于其他的任意 2 个攻击行为 Ab_{ij} 与 Ab_{mn} 的相似度计算如式(11)所示。

$$SIM(Ab_{ij}, Ab_{mn}) = \sum_{1}^{k} wSIM_k(Ab_{ij}, Ab_{mn}) \tag{11}$$

式中：$SIM(Ab_{ij}, Ab_{mn})$ 为 Ab_{ij} 与 Ab_{mn} 的总相似度；$Sim_k(Ab_{ij}, Ab_{mn})$ 为 Ab_{ij} 与 Ab_{mn} 在第 k 个属性上的相似度(取值 0 或 1)；w 为不同属性值的权重，经过大量实验后得出 w 的值如表 1 所示。

表 1 不同属性的权重值

Table1 Weights of different attributes

attributes	weights
msg	0.60
sIP	0.15
dIP	0.15
sPort	0.05
dPort	0.05

如果 $SIM(Ab_{ij}, Ab_{mn}) = 1$，表示攻击行为 Ab_{ij} 与 Ab_{mn} 完全相同，可以聚合为同一个攻击行为；如果 $SIM(Ab_{ij}, Ab_{mn}) = 0$，则表示攻击行为 Ab_{ij} 与 Ab_{mn} 完全不同，不做处理；如果 $0 < SIM(Ab_{ij}, Ab_{mn}) < 1$，表示攻击行为 Ab_{ij} 与 Ab_{mn} 可能存在关联关系，将其聚合为超集合 Z。基于属性相似度的攻击行为聚合能压缩数据量，将得到的攻击行为全集合作为 Ex-Apriori 算法的输入可以有效地提高 TAEIM 模型第 2 阶段的处理效率。

2.3.3 Ex-Apriori 算法描述

本节将攻击行为全集合拆分为多个子集，通过对不同子集内的网络攻击行为进行分析，可以发现攻击行为间的关联规则并提取攻击行为组集。

通过 Ex-Apriori 算法拆分处理数据集的流程如图 4 所示，在网络攻击场景中，所采集的数据集是按照时间顺序存储的，因此基于属性相似度聚合后的攻击行为全集合同样是按照时间顺序依次排列的，选择合适的周期 T 对攻击行为全集合进行拆分，进而利用多线程对拆分的子集进行处理，最后合并为新的频繁项集集合。

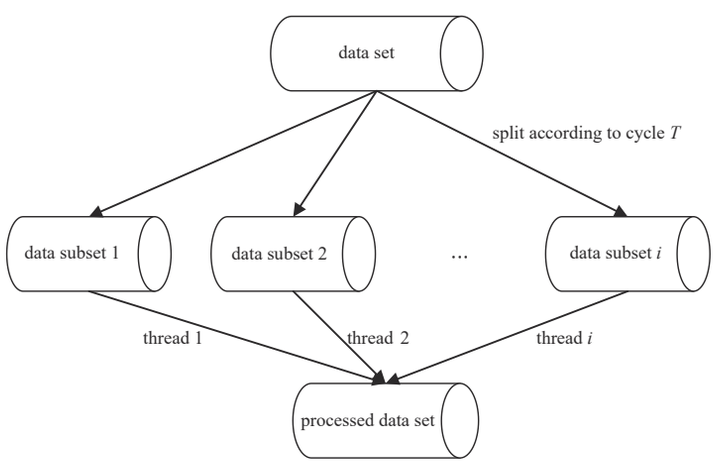

Fig.4 Split the data set through the Ex-Apriori algorithm

图 4 通过 Ex-Apriori 算法拆分处理数据集

对于某个项集 I_s，在数据集 D_s 下 I_s 是非频繁项集，但是在将 D_s 按照时间顺序拆分后得到的数据子集 D_{st} 中，I_s 是频繁的，那么根据网络攻击场景的特点，说明 I_s 中的网络攻击行为在该时间段中发生的次数较多，I_s 仍然是频繁项集。因此 Ex-Apriori 算法在解决了候选集太多以及频繁扫描数据库造成的效率问题的同时，也避免了 Apriori 算法由于单一地采用全局支持度作为过滤条件而删除了有用的数据，提高了准确度。同时针对网络攻击行为的属性特点，在将支持度与置信度作

为判断基础的前提下加入攻击行为属性的分类，使最终结果更加合理。

通过 Ex–Apriori 算法对攻击行为全集合进行提取，输出攻击行为组集，算法描述如下：

Algorithm 2 Ex–Apriori algorithm

Input: Attack collection AC, Number of groups k, Support threshold $min\_support$, Confidence threshold $min\_confidence$, Minimum number of frequent item sets Num, Super collection Z

Output: Attack group AG

```
BEGIN
    Algorithm initialization
    divide AC into k groups and get item_1 to item_x
    for group L_1 to L_k do
      for item set item_1 to item_x do
        if support_x > min_support and number of itemsets N > Num
          add to frequent itemsets F_kx
      end for
    end for
    create a confidence set C={}
for F_11 to F_kx do
  if support_F > min_support and conf_F > min_confidence
    add to AG
end for
add Z to AG
END
```

2.4 基于 TAEIM 模型发掘攻击事件

通过 2.2 节内容可以获取贝叶斯攻击行为关联图 BAAG，通过 2.3 节的方法可以获取攻击行为组集 AG。因此基于 TAEIM 模型的攻击事件发掘算法如下：

Algorithm 3 Attack event extraction algorithm

Input: Bayesian attack association graph $BAAG$, Attack group AG, Conditional probability table CPT, Transition probability matrix TPM

Output: Attack events extracted $BAAG–AE$

```
BEGIN
Algorithm initialization
Initialize BAAG–AE
for Ab_mn in AG do
  if Ab_mn match Node_i which is in BAAG
    add Node_i to BAAG–AE
    generate edge e for Node_i
end for
for e in BAAG–AE
    generate the weight of e according to CPT and TPM
 end for
END
```

3 实验与分析

3.1 数据集与评价指标

目前关于网络安全研究使用的公开数据集大多是 DARPA98、KDD99 和 NSL–KDD，但是这些数据集距今时间较长，导致数据集中缺少某些攻击种类进而无法反映最新的网络攻击情况。考虑到该问题，实验数据集采用加拿大网络安全研究所发布的 CICIDS2017，该数据集由正常流量以及包含了多种攻击行为的流量所组成，持续时间从星期一到星期五，其中周一全部为正常流量。实施的网络攻击方式有暴力破解、DoS、DDoS、渗透、Heart–bleed 和 Scan 等，详细信息如表 2 所示。

表2 数据集详细信息

Table2 Details of CICIDS2017 dataset

date	types of attack	size
Tuesday	FTP−patator、SSH−patator	11 G
Wednesday	DoS slowloris、DoS slowhttptest、DoS hulk、DoS goldeneye、Heart−bleed	13 G
Thursday	brute force、XSS、Sql injection、infiltration	7.8 G
Friday	Botnet ARES、port scan、DDoS LOIT	8.3 G

实验采用的评价指标包含 3 部分，第 1 部分是对于包含攻击行为的数据集，通过聚合率来判断基于属性相似度的攻击行为聚合的效果；第 2 部分是将 Ex−Apriori 算法与普通 Apriori 算法的效率进行比较；第 3 部分是通过 BAAG 生成算法构建贝叶斯攻击行为关联图，并结合模型 2 个阶段的实验结果构建 TAEIM 模型，通过对比实际攻击事件来测试模型的合理性与精确度。

3.2 实验结果及分析

在通过聚合率判断基于属性相似度聚合攻击行为的效果方面，首先在 Ubuntu 系统中安装 Snort 并对 CICIDS2017 的 pcap 文件进行检测，获得了包含原始攻击行为数据的 alert.csv 文件，将其导入到数据库后如图 5 所示。

通过基于属性相似度的攻击行为聚合方法对原始攻击行为数据进行聚合，聚合率如表 3 所示。

timestamp	sig_generator	sig_id	sig_rev	msg	proto	src	srcport	dst	dstport	ethsrc	ethdst	ethlen	tcpflags	tcpseq	tcpack	tcplen
07/07-03:58:33.217559	1	254	4	DNS SPOOF query response with TTL o	UDP	192.168.10.3	53	192.168.10.19	8251	18:66:DA:9B:E3	00:23:AE:9B:AD	0x59	(Null)	(Null)	(Null)	(Null)
07/07-03:58:37.213839	1	2925	3	INFO web bug 0x0 gif attempt	TCP	222.158.212.13	80	192.168.10.9	9938	00:C1:B1:14:EB:	B8:AC:6F:1D:1F	0x17	***AP***	0x7F49E1	0x381577	(Null)
07/07-03:58:37.182424	1	853	9	WEB-CGI wrap access	TCP	192.168.10.9	9930	125.1.77.19	80	B8:AC:6F:1D:1F	00:C1:B1:14:EB:	0x199	***A****	0x2EE372	0x7A325	(Null)
07/07-03:58:40.119955	1	402	7	ICMP Destination Unreachable Port Un	ICMP	192.168.10.9	(Null)	192.168.10.3	(Null)	B8:AC:6F:1D:1F	18:66:DA:9B:E3	0xA2	(Null)	(Null)	(Null)	(Null)
07/07-03:58:40.120004	1	402	7	ICMP Destination Unreachable Port Un	ICMP	192.168.10.9	(Null)	192.168.10.3	(Null)	B8:AC:6F:1D:1F	18:66:DA:9B:E3	0xA2	(Null)	(Null)	(Null)	(Null)
07/07-04:01:05.056077	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54055	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x21B	***A****	0x2B8DE	0x870A07	(Null)
07/07-04:01:05.119113	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54055	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C6	***AP***	0x870A07	0x2B8DE4	(Null)
07/07-04:01:05.403630	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54055	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x224	***AP***	0x2B8DE4	0x870A0A	(Null)
07/07-04:01:05.458822	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54055	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C6	***AP***	0x870A0F	0x2B8DE6	(Null)
07/07-04:01:05.457823	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54059	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x222	***A****	0x80D4B	0x5DD63	(Null)
07/07-04:01:05.458341	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54060	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x21F	***A****	0x9734F9	0x18CFE8	(Null)
07/07-04:01:05.462248	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54061	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x23E	***A****	0x6E5216	0x183F58	(Null)
07/07-04:01:05.515061	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54059	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C5	***AP***	0x5DD63	0x80D4B	(Null)
07/07-04:01:05.516196	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54060	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C6	***AP***	0x18CFE8	0x9734FA	(Null)
07/07-04:01:05.524056	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54061	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C5	***AP***	0x183F5B	0x6E5218	(Null)
07/07-04:01:05.932864	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54074	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x21D	***A****	0xAD59C	0xAA673	(Null)
07/07-04:01:05.986126	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54074	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C6	***AP***	0xAA673	0xAD59D	(Null)
07/07-04:01:05.939205	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54073	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x223	***A****	0x80DB6	0x697A11	(Null)
07/07-04:01:05.995833	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54073	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C5	***AP***	0x697A11	0x80DB6	(Null)
07/07-04:01:05.970339	1	1054	7	WEB-MISC weblogic/tomcat .jsp view s	TCP	192.168.10.25	54072	199.59.88.242	80	00:25:00:A8:C4:	00:C1:B1:14:EB:	0x23A	***A****	0x85CA3	0xCE192	(Null)
07/07-04:01:06.026450	1	2925	3	INFO web bug 0x0 gif attempt	TCP	199.59.88.242	80	192.168.10.25	54072	00:C1:B1:14:EB:	00:25:00:A8:C4:	0x2C5	***AP***	0xCE1920	0x85CA3	(Null)
07/07-04:01:35.409536	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58672	104.97.126.55	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50C	***AP***	0x1751C9	0x84316	(Null)
07/07-04:01:35.603174	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58673	52.160.91.170	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50C	***AP***	0x85F9DC	0x713FB	(Null)
07/07-04:01:43.807349	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58689	104.97.126.55	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50C	***AP***	0x9A6DC	0x056C	(Null)
07/07-04:01:43.847922	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58673	52.160.91.170	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50C	***AP***	0x85F9EA	0x713FC	(Null)
07/07-04:01:44.177768	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58691	104.97.126.55	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50E	***AP***	0x2DE20	0x4C8D1	(Null)
07/07-04:01:44.219840	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.5	58673	52.160.91.170	80	B8:AC:6F:36:0A:	00:C1:B1:14:EB:	0x50E	***AP***	0x85F9F9	0x713FD	(Null)
07/07-04:01:55.271928	1	538	15	NETBIOS SMB IPC$ unicode share acce	TCP	192.168.10.25	54150	192.168.10.19	139	00:25:00:A8:C4:	00:23:AE:9B:AD	0xA2	***AP***	0x26586A	0x1495E	(Null)
07/07-04:02:17.478367	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.14	52023	23.210.86.11	80	B8:AC:6F:36:07:	00:C1:B1:14:EB:	0x510	***AP***	0x260E6C	0x98832	(Null)
07/07-04:02:17.597345	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.14	52024	40.112.213.22	80	B8:AC:6F:36:07:	00:C1:B1:14:EB:	0x510	***AP***	0x92F8A6	0x7587E	(Null)
07/07-04:02:17.718698	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.14	52025	23.210.86.11	80	B8:AC:6F:36:07:	00:C1:B1:14:EB:	0x5EA	***A****	0x4E8B71	0xF85EA	(Null)
07/07-04:02:36.235898	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.14	52207	23.210.86.11	80	B8:AC:6F:36:07:	00:C1:B1:14:EB:	0x510	***AP***	0x9DB6E	0xFBC2C	(Null)
07/07-04:02:36.266549	1	1000001	1	COMMUNITY WEB-MISC mod_jrun ove	TCP	192.168.10.14	52024	40.112.213.22	80	B8:AC:6F:36:07:	00:C1:B1:14:EB:	0x510	***AP***	0x92F8B5	0x7587F	(Null)

Fig.5 Raw attack behavior data

图5 原始攻击行为数据

从表 3 可以看出，聚合率都在 72% 以上，星期二的聚合率较高，达到了 82.5%，说明通过基于属性相似度的攻击行为聚合方法可以有效地减少冗余数据，避免冗余数据对后续实验的精确度和效率造成影响。

表3 攻击行为数据聚合率对比

Table 3 Comparison of attack behavior data aggregation rate

date	number of raw data	after polymerization	polymerization rate/%
Tuesday	18 450	3 233	82.5
Wednesday	5 903	1 629	72.4
Thursday	8 518	2 356	72.3
Friday	7 532	1 943	74.2

在对比 Ex−Apriori 算法与普通 Apriori 算法的效率方面，首先在真实网络环境中构建网络攻击流数据，利用不同种类的攻击工具发起多种网络攻击，将攻击流量与正常流量混合后得到约 10 GB 的真实流量(以 pcap 文件保存)，通过对攻击行为数据进行处理后，分别对数据量为 2 000、4 000、6 000、8 000、10 000 的攻击行为数据进行了实验，设置支持度阈值 Support 为 0.1，置信度阈值 Confidence 为 0.5，记录每次处理所需要的时间。图 6 为 2 种算法耗时对比。

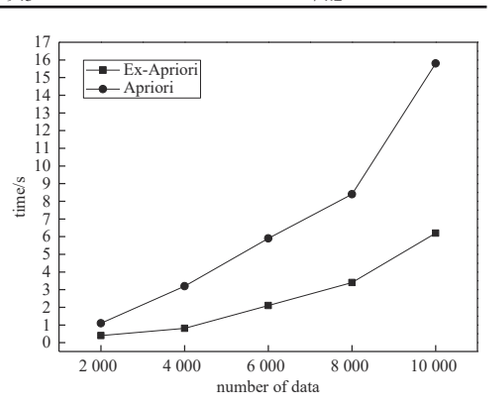

Fig.6 Time consumption comparison of two algorithms

图6 两种算法耗时对比

从图 6 可以发现在数据量不大的时候，2 种算法耗时并无太大区别，而随着数据量的增大，2 种算法的耗时差从 2 000 条的

0.6 s到10 000条的9.6 s，说明随着数据集的扩大，Ex-Apriori算法相比普通Apriori算法提升的效率更加明显。

通过BAAG生成算法处理CICIDS2017数据集得到贝叶斯攻击行为关联图，截取部分展示如图7所示。

结合两阶段的实验结果，构建TAEIM模型提取的攻击事件如图8所示。

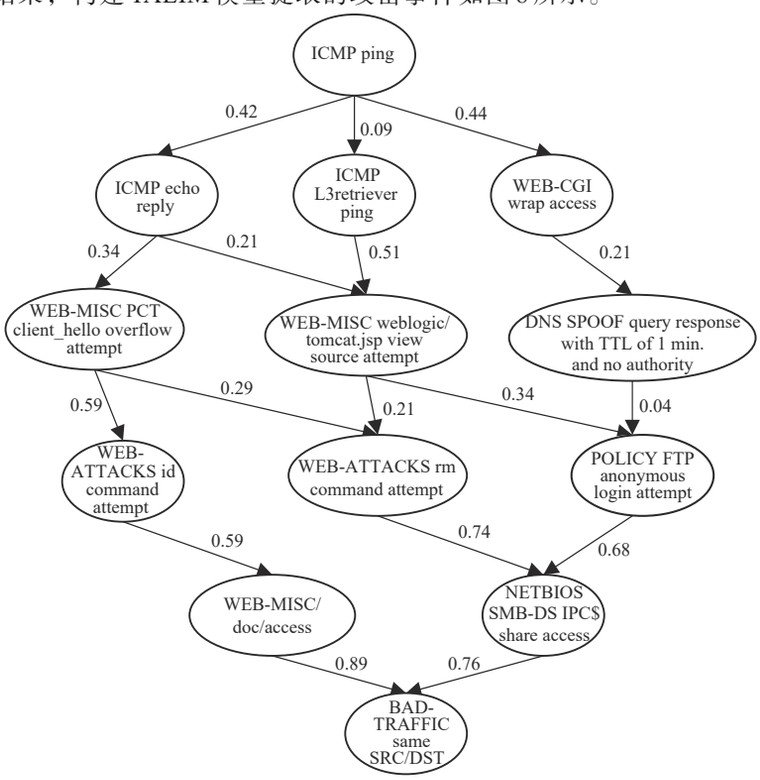

Fig.7 Bayesian attack association graph

图7 贝叶斯攻击行为关联图

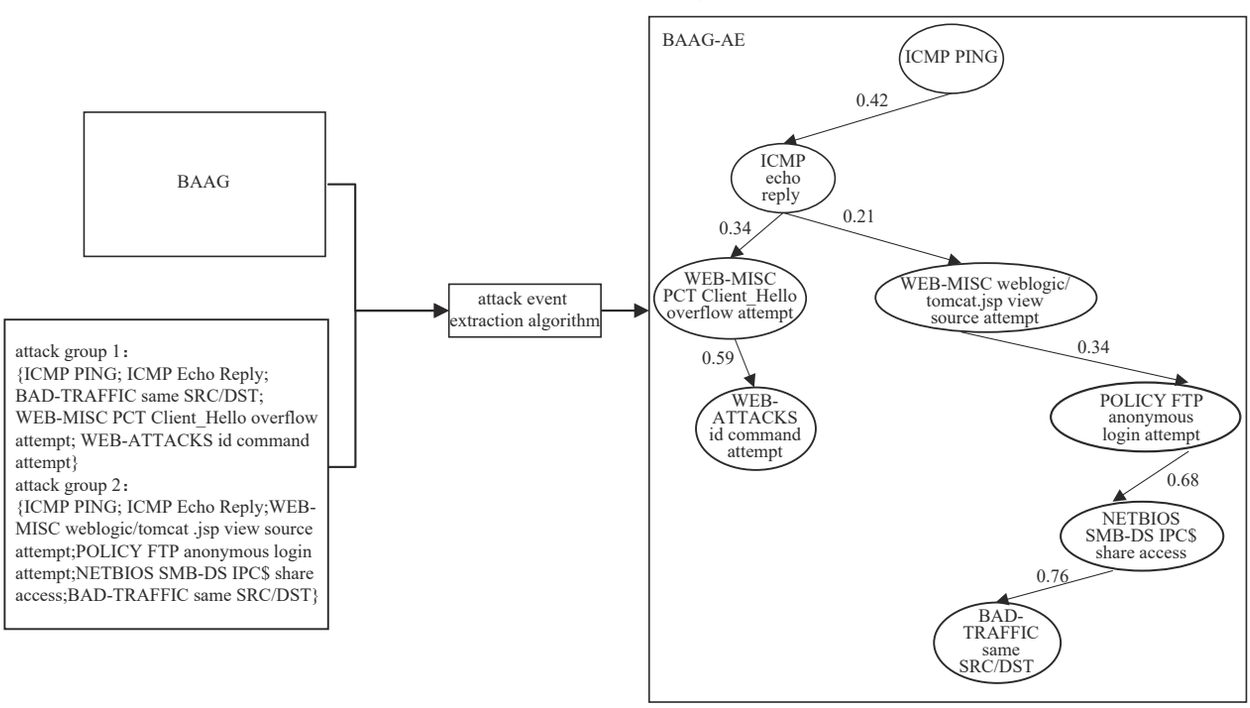

Fig.8 Attack discovered

图8 发掘的攻击事件

将采用攻击工具发起的实际攻击事件与图 8 的结果进行对比，所发掘的攻击事件的匹配率用公式(12)表示。

$$P_e = \frac{Num(DisEvents)}{Num(RealEvents)} \tag{12}$$

式中：P_e 为攻击事件的匹配率；$Num(DisEvents)$ 为成功发掘的攻击事件数目；$Num(RealEvents)$ 为实际的攻击事件数目。由于文献[16]与文献[17]同样基于贝叶斯网络构建了攻击图，因此为了验证本模型的有效性，在同样的测试情况下复现文献[16]与文献[17]的方法，并对比了攻击事件的匹配率，从图 9 可以看出本文提出的 TAEIM 模型明显优于另外 2 种方法。

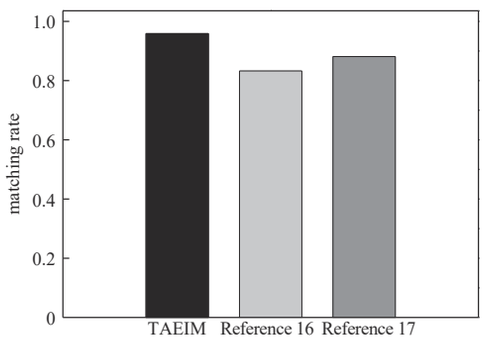

Fig.9 Comparative results
图 9　结果对比

通过以上实验测试结果表明，基于贝叶斯网络的攻击事件智能发掘模型是可行有效的，能够准确地识别出攻击事件的整个攻击流程，为发掘攻击事件与发现攻击路径提供了依据和支撑。

4　结论

本文提出一种基于贝叶斯网络的两阶段攻击事件智能发掘模型，该模型解决了网络攻击行为数据冗余、攻击场景构建不完全、攻击行为关联关系难以提取的问题。以先验知识建立贝叶斯攻击行为关联图，结合基于属性相似度的攻击行为聚合方法减少冗余数据，针对网络攻击场景设计高效的 Ex-Apriori 算法，发现攻击行为间的关联规则并提取攻击行为组集，通过 TAEIM 模型进一步发掘完整的攻击事件并发现攻击路径。从实验结果可知本文提出的方法能够有效提取网络攻击事件及寻找攻击路径。未来将继续研究攻击图的动态生成算法并结合本模型提高发掘的精确度与实时性，为网络安全领域提供更大的实用价值和现实意义。

参考文献：

[1] ZHANG Aifang,LI Zhitang,LI Dong,et al. Discovering novel multistage attack patterns in alert streams[C]// 2007 International Conference on Networking, Architecture, and Storage(NAS 2007). Guilin, Guangxi, China: IEEE, 2007: 115-121. doi: 10.1109/NAS.2007.20.

[2] 冯学伟,王东霞,黄敏桓,等. 一种基于马尔可夫性质的因果知识挖掘方法[J]. 计算机研究与发展, 2014,51(11):2493-2504. (FENG Xuewei,WANG Dongxia,HUANG Minhuan,et al. A mining approach for causal knowledge in alert correlating based on Markov property[J]. Journal of Computer Research and Development, 2014,51(11): 2493-2504.) doi: 10.7544/issn1000-1239.2014.20130854.

[3] 陆江东,郑奋,戴卓臣. 基于改进 Apriori 的网络安全感知方法[J]. 计算机测量与控制, 2017,25(10): 244-246,254. (LU Jiangdong,ZHENG Fen,DAI Zhuochen. Network security situation awareness method based on improved Apriori algorithm[J]. Computer Measurement & Control, 2017,25(10):244-246,254.) doi:10.16526/j.cnki.11-4762/tp.2017.10.062.

[4] 刘文彦,霍树民,陈扬,等. 网络攻击链模型分析及研究[J]. 通信学报, 2018,39(z2):88-94. (LIU Wenyan,HUO Shumin,CHEN Yang,et al. Analysis and study of cyber attack chain model[J]. Journal on Communications, 2018,39(z2):88-94.) doi:10.11959/j.issn.1000-436x.2018271.

[5] KUMAR R, RUIJTERS E, STOELINGA M. Quantitative attack tree analysis via priced timed automata[C]// International Conference on Formal Modeling and Analysis of Timed Systems. Cham: Springer, 2015: 156-171. doi: 10.1007/978-3-319-22975-1_11.

[6] GADYATSKAYA O, JHAWAR R, KORDY P, et al. Attack trees for practical security assessment: ranking of attack scenarios with ADTool 2.0[C]// International Conference on Quantitative Evaluation of Systems. Cham: Springer, 2016: 159-162. doi: 10.1007/978-3-319-43425-4_10.

[7] BOPCHE G S,MEHTRE B M. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks[J]. Computers & Security, 2017(64):16-43. doi:10.1016/j.cose.2016.09.010.

[8] 胡浩,刘玉岭,张红旗,等. 基于吸收 Markov 链的网络入侵路径预测方法[J]. 计算机研究与发展, 2018,55(4):831-845. (HU Hao,LIU Yuling,ZHANG Hongqi,et al. Route prediction method for network intrusion using absorbing Markov chain[J]. Journal of Computer Research and Development, 2018,55(4):831-845.) doi:10.7544/issn1000-1239.2018.20170087.

[9] KATARYA R, JAIN C. Multilayered risk analysis of mobile systems and apps[C]// 2018 Second International Conference on

Computing Methodologies and Communication(ICCMC). Erode,India:IEEE, 2018:64-67. doi:10.1109/ICCMC.2018.8487535.

[10] NOEL S, JAJODIA S. Optimal IDS sensor placement and alert prioritization using attack graphs[J]. Journal of Network and Systems Management, 2008,16(3):259-275. doi:10.1007/s10922-008-9109-x.

[11] LIU Sichao, LIU Yuan. Network security risk assessment method based on HMM and attack graph model[C]// 2016 the 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing(SNPD). Shanghai,China:IEEE, 2016:517-522. doi:10.1109/SNPD.2016.7515951.

[12] 杨豪璞,邱辉,王坤. 面向多步攻击的网络安全态势评估方法[J]. 通信学报, 2017,38(1):187-198. (YANG Haopu,QIU Hui, WANG Kun. Network security situation evaluation method for multi-step attack[J]. Journal on Communications, 2017, 38(1): 187-198.) doi:10.11959/j.issn.1000-436x.2017021.

[13] YI Feng,CAI Huangyi,XIN Fuzheng. A logic-based attack graph for analyzing network security risk against potential attack[C]// 2018 IEEE International Conference on Networking, Architecture and Storage(NAS). Chongqing, China: IEEE, 2018: 1-4. doi: 10.1109/NAS.2018.8515733.

[14] 王洋,吴建英,黄金垒,等. 基于贝叶斯攻击图的网络入侵意图识别方法[J]. 计算机工程与应用, 2019,55(22):73-79. (WANG Yang, WU Jianying, HUANG Jinlei, et al. Network intrusion intention recognition method based on Bayesian attack graph[J]. Computer Engineering and Applications, 2019,55(22):73-79.) doi:10.3778/j.issn.1002-8331.1809-0081.

[15] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2012,9(1):61-74. doi:10.1109/TDSC.2011.34.

[16] HU Zhisheng,ZHU Minghui,LIU Peng. Online algorithms for adaptive cyber defense on Bayesian attack graphs[C]// Proceedings of the 2017 workshop on moving target defense. Dallas, Texas, USA: Association for Computing Machinery, 2017: 99-109. doi: 10.1145/3140549.3140556.

[17] MATTHEWS I, MACE J, SOUDJANI S, et al. Cyclic Bayesian attack graphs: a systematic computational approach[C]// 2020 IEEE the 19th International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom). Guangzhou,China:IEEE, 2020:129-136. doi:10.1109/TrustCom50675.2020.00030.

作者简介：

李岳峰(1997-)，男，在读硕士研究生，主要研究方向为计算机网络安全.email:1139627163@qq.com.

刘　丹(1969-)，男，博士，副教授，主要研究方向为网络安全、自然语言处理.