基于超图 Transformer 的 APT 攻击威胁狩猎网络模型

李元诚，林玉坤
（华北电力大学控制与计算机工程学院，北京 102206）

摘 要：针对物联网环境中高级持续性威胁（APT）具有隐蔽性强、持续时间长、更新迭代快等特点，传统被动检测模型难以对其进行有效搜寻的问题，提出了一种基于超图 Transformer 的 APT 攻击威胁狩猎（HTTN）模型，能够在时间跨度长、信息隐蔽复杂的物联网系统中快速定位和发现 APT 攻击痕迹。该模型首先将输入的网络威胁情报（CTI）日志图和物联网系统内核审计日志图编码为超图，经超图神经网络（HGNN）层计算日志图的全局信息和节点特征；然后由 Transformer 编码器提取超边位置特征；最后对超边进行匹配计算相似度分数，从而实现物联网系统网络环境下 APT 攻击的威胁狩猎。在物联网仿真环境下的实验结果表明，提出的 HTTN 模型与目前主流的图匹配神经网络相比均方误差降低约 20%，Spearman 等级相关系数提升约 0.8%，匹配精度提升约 1.2%。

关键词：高级持续性威胁；威胁狩猎；图匹配；超图
中图分类号：TN92
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2024043

APT attack threat-hunting network model based on hypergraph Transformer

LI Yuancheng, LIN Yukun
School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China

Abstract: To solve the problem that advanced persistent threat (APT) in the Internet of things (IoT) environment had the characteristics of strong concealment, long duration, and fast update iterations, it was difficult for traditional passive detection models to quickly search, a hypergraph Transformer threat-hunting network (HTTN) was proposed. The HTTN model had the function of quickly locating and discovering APT attack traces in IoT systems with long time spans and complicated information concealment. The input cyber threat intelligence (CTI) log graph and IoT system kernel audit log graph were encoded into hypergraphs by the model, and the global information and node features of the log graph were calculated through the hypergraph neural network (HGNN) layer, and then they were extracted for hyperedge position features by the Transformer encoder, and finally the similarity score was calculated by the hyperedge, thus the threat-hunting of APT was realized in the network environment of the Internet of things system. It is shown by the experimental results in the simulation environment of the Internet of things that the mean square error is reduced by about 20% compared to mainstream graph matching neural networks, the Spearman level correlation coefficient is improved by about 0.8%, and improved precision@10 is improved by about 1.2% by the proposed HTTN model.

Keywords: advanced persistent threat, threat-hunting, graph matching, hypergraph

0 引言

物联网的发展正推动国家数字化、智能化和自动化转型，使各种设备能够通过互联网进行数据传输和交换，从而实现智能化的监测、控制和决策。据《中国互联网发展报告（2022）》，全国各地在建“5G+工业物联网”项目超 800 个，覆盖航空、矿山、钢铁、港口、电力等 22 个重要行业，然而这

收稿日期：2023−09−06；**修回日期：**2023−11−29
基金项目：国家电网有限公司科技基金资助项目（No.5700-202199539A-0-5-ZN）
Foundation Item: Science and Technology Project of STATE GRID Corporation of China (No.5700-202199539A-0-5-ZN)

些物联网系统的网络空间涉及多种设备、传感器和通信网络的交互，其复杂性导致系统容易受到恶意攻击的侵害。攻击形式主要包括网络入侵、信息窃取、数据篡改等，尤其是高级持续性威胁（APT, advanced persistent threat）成为最重要的威胁。

近年来，针对工业物联网的 APT 攻击事件层出不穷[1-2]，攻击者通过 APT 攻击侵入国家工业控制网络，对国家工业系统造成巨大破坏。

目前，国内外对物联网系统中 APT 攻击的检测工作大多通过提取 APT 攻击的特征，并在特定 APT 攻击的检测上获得良好效果。例如，APT-Dt-KC 方法[3]利用网络杀伤链模型中的模糊特征，采用贝叶斯分类算法和模糊层次分析法的混合检测方法实现对 APT 攻击的检测；Abdel-Basset 等[4]提出了一个名为 Fed-TH（federated threat-hunting）的联邦深度学习模型，通过捕获网络数据的时间和空间表示，引入一种探索性的微服务放置方法来追踪工业信息物理系统中的 APT 攻击；文献[5]利用因果关系分析、自然语言处理和机器学习的组合构建出一种序列模型，实现从因果图建立攻击和非攻击行为，结合威胁情报事件，确定因果图的 APT 攻击节点。但这些检测模型大多局限于已知的 APT 攻击，且需要大量的攻击样本来提取特征。

另外，APT 组织在发起网络攻击时，为了绕开安全防御系统，大多采用零日攻击[6]。由于缺少大量的样本数据，现有方法对这些未知的 APT 攻击检测效果较差。威胁狩猎是一种新型主动防御技术，以安全假设为起点，主动持续地搜索能绕开安全检测或产生危害的威胁行为[7]，以便及时发现可能的安全威胁。相对于传统的被动检测方法，威胁狩猎方法可以在系统中积极地搜索和追踪威胁行为，从而能够更早地发现攻击者的活动。

综上所述，本文提出了一种基于超图 Transformer 的威胁狩猎网络（HTTN, hypergraph transformer threat-hunting network）模型。该模型能够在构建日志图时，针对 APT 攻击长期潜伏性的特点最大限度地保留物联网系统 APT 攻击痕迹，同时能够利用网络威胁情报（CTI, cyber threat intelligence）生成的威胁情报日志图自适应地不断更新变化的 APT 攻击，并且不需要大量的攻击样本就可进行 APT 攻击的威胁狩猎。该模型以威胁情报和系统日志为输入，对其进行编码和构建超图，再经过超图神经网络层处理后，利用 Transformer 多头注意力机制完成特征提取，最后利用超边匹配算法计算相似性分数，实现威胁情报在物联网日志库中的匹配，完成物联网系统 APT 攻击的威胁狩猎。

1　问题描述

物联网具有终端数量多、种类多、连接多、系统多等特点[8]，给系统网络边界带来了极大的复杂性和安全风险。海量终端节点的存在使物联网系统的网络拓扑变得错综复杂，增加了攻击者渗透和横向移动的机会。此外，物联网系统中的多样性还涉及不同类型的终端设备、通信协议、数据格式等，这也增加了系统的脆弱性和受到 APT 攻击的风险。在第一批 APT 报告中，安全公司 Mandiant[9]揭示了全球 APT 攻击参与者的行为，这些攻击者从各领域至少 141 个组织中窃取了数百 TB 的敏感数据；同时估计了 APT 攻击在目标系统的平均存在时间为 365 天。

当前物联网的网络结构正朝着分布式方向发展，其中涉及的网络设备呈现海量增长趋势，这种网络的分布式特性导致物联网系统的边界变得更加复杂，攻击者可以通过外部网络入侵并潜伏到物联网信息网络中，篡改物联网业务层，最终造成对物联网系统的严重破坏。物联网分布式网络结构如图 1 所示。鉴于 APT 组织在进行 APT 攻击时经常利用零日漏洞，而这些漏洞由于样本数量极少，难以通过传统的机器学习方法对其进行有效的检测。因此，如何有效地挖掘系统的日志库，并主动发现长期潜伏的 APT 零日漏洞攻击，成为一项关键性的研究课题。

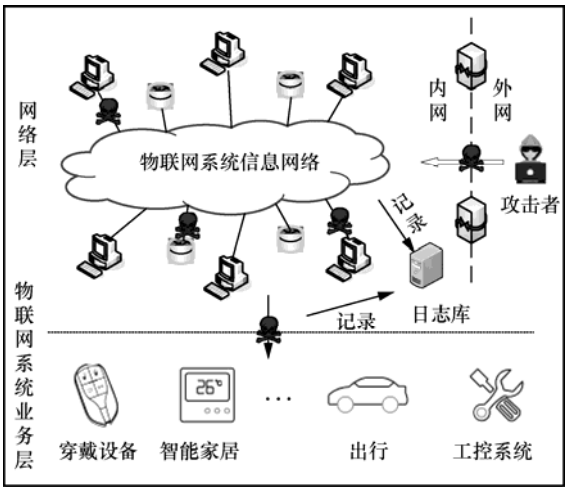


图 1　物联网分布式网络结构

网络威胁情报[10]作为一种威胁信息集合，已经应用于多个领域。本文针对物联网服务器日志库与网络威胁情报库，通过构建图相似性学习模型，计算相似性分数确定威胁情报的匹配程度，从而完成物联网系统中对于 APT 攻击的威胁狩猎。

2 基于超图 Transformer 的威胁狩猎网络模型

2.1 基于 HTTN 模型的威胁情报搜索

物联网系统中针对威胁情报的 APT 攻击狩猎流程如图 2 所示。该模型的最终目的是探测时间跨度大、信息隐蔽复杂的物联网系统内核审计日志库中是否存在与威胁情报相似的 APT 攻击，从而完成威胁狩猎。具体过程如下。

1) 通过各种类型操作系统内核审计引擎实现对物联网系统内核审计日志流的采集，日志流经过相应系统日志处理模块构建物联网系统日志图。

2) 人为收集各种开源或私有威胁情报库中的网络威胁情报，经过威胁情报处理模块生成威胁情报日志图。

3) 将物联网系统日志图与威胁情报日志图一同输入 HTTN 模型中，通过对日志图相似性匹配，计算物联网系统日志图与威胁情报日志图的相似度分数。

4) 威胁狩猎专家通过对 HTTN 模型设置相似度分数阈值，获取物联网系统日志库中所有与威胁情报相匹配的操作系统日志，通过 HTTN 模型发现未知 APT 攻击，完成 APT 攻击的威胁狩猎。

2.2 HTTN 模型设计

本文提出的 HTTN 模型由图信息输入层、超图构造层、超图神经网络层、超图 Transformer 编码层、超边匹配层和相似度分数计算层组成，模型架构如图 3 所示。

2.2.1 图信息输入层

HTTN 模型的数据输入由 N 个日志图对组成，日志图对集合可以表示为 $G=\{(G_{1,1},G_{1,2}),(G_{2,1},G_{2,2}),\cdots,(G_{n,1},G_{n,2})\}$，图 $G_{i,1}$ 或 $G_{i,2}$ 可以有任意的节点和边。对于任意一个日志图对 $(G_{i,1},G_{i,2})$，$G_{i,1}=(V_{i,1},E_{i,1},\boldsymbol{X}_{i,1})$，$n_{i,1}=\left|V_{i,1}\right|$ 和 $e_{i,1}=\left|E_{i,1}\right|$ 分别表示节点数和边数；邻接矩阵 $\boldsymbol{A}_{i,1}\in R^{n_{i,1}\times n_{i,1}}$ 表示图 $G_{i,1}$ 的连接信息；$\boldsymbol{X}_{i,1}\in R^{n_{i,1}\times f}$ 表示图 $G_{i,1}$ 节点的特征矩阵，其中 f 是节点的维度。图 $G_{i,2}$ 的表示方法与图 $G_{i,1}$ 相同。

2.2.2 超图构造层

为了完成对物联网系统日志图的超边匹配，需要对图信息输入层输入的日志图数据构建超图。日

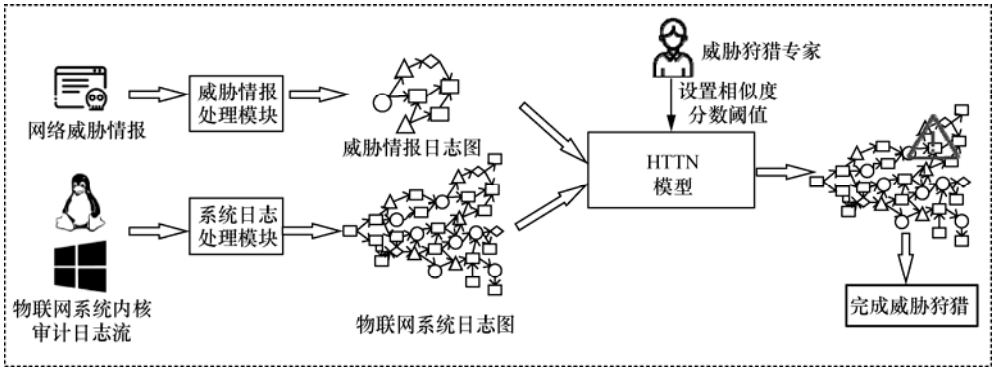


图 2 物联网系统中针对威胁情报的 APT 攻击狩猎流程

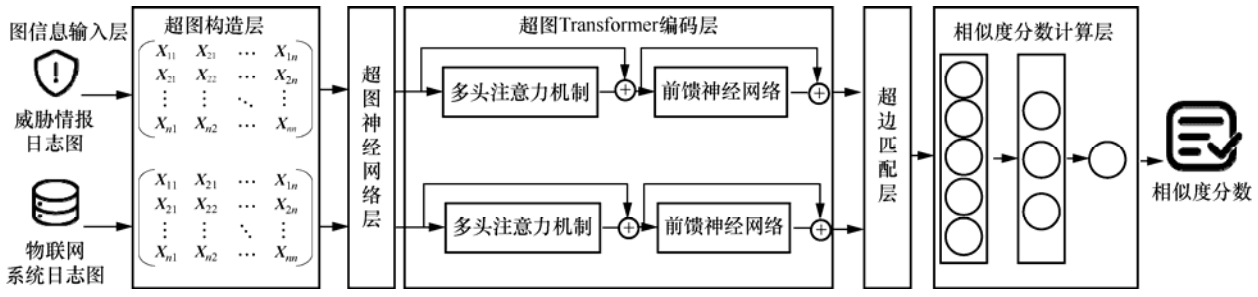


图 3 HTTN 模型架构

志超图定义为 $\mathrm{HG}=(V_{\log},E_{\log},\boldsymbol{X},\boldsymbol{W})$[11]，由日志节点集 $V_{\log}$、日志边集 $E_{\log}$、日志节点特征矩阵 $\boldsymbol{X}$ 和日志对角边权重矩阵 $\boldsymbol{W}$ 组成。与普通图 G 不同，超图的每条超边包含 2 个或多个节点；超图 HG 使用关联矩阵 $\boldsymbol{H}\in R^{|V|\times|E|}$ 来建模非成对节点关系，HG 的关联矩阵 $\boldsymbol{H}$ 的元素定义如下

$$h(v,e)=\begin{cases}1, v\in e\\ 0, v\notin e\end{cases} \tag{1}$$

节点 v 的度数为 $d(v)=\sum_{e\in E}w(e)h(v,e)$，边 e 的度数为 $d(e)=\sum_{v\in V}h(v,e)$。节点度对角线矩阵和超边度对角矩阵分别为 $\boldsymbol{D}_v$ 和 $\boldsymbol{D}_e$。

在超图构造层中，本文采用了随机游走方法构建物联网系统日志超图，能够模拟日志图中节点的传播和转移过程，在局部范围内探索节点之间的关系，同时还可以控制游走参数（如步长等），以调整节点遍历的倾向性，从而适应不同的场景。对于每个日志节点 v，选择在步长为 K 的普通图 G 上进行随机游走，然后将采样节点序列作为超边，得到 $|E|$ 超边矩阵。图 4 表示了 APT 攻击的 Trojan 攻击场景下日志超图的构造过程。其中，节点 A 表示不受信任的外部地址；节点 B 表示浏览器；节点 C 表示 Trojan 文件；节点 D 表示被执行的 Trojan 进程；节点 E 表示 dash 脚本命令行；节点 F 表示显示服务器网络配置的命令；节点 G 表示显示主机名称的命令；节点 H 表示监控服务器 TCP/IP 网络连接的命令；节点 I 表示服务器内包含账号、密码等敏感信息的配置文件，这些配置文件的泄露可以直接导致攻击者侵入物联网业务层、篡改业务层数据等。

2.2.3　超图神经网络层

超图神经网络（HGNN, hypergraph neural network）[12-13]是一种考虑高阶节点关系而不是成对节点关系的神经网络模型，由于物联网系统内核审计日志图节点之间关系具有复杂性以及 APT 攻击具有阶段性的特点，仅仅对日志图成对节点之间进行匹配训练无法充分提取日志图之间节点的相关性，因此训练出来的模型对于 APT 攻击威胁情报日志的匹配效果不佳。又由于 HGNN 在编码日志节点位置相关性方面展现出比传统的图卷积网络（GCN, graph convolutional network）[14]更好的性能，为了更好地捕捉日志超图中复杂的节点关系，在 HTTN 模型中添加了 HGNN 层。对于 HGNN 层中的第 l 层，它以超图 HG 的关联矩阵 $\boldsymbol{H}$ 和隐藏表示矩阵 $\boldsymbol{X}^l$ 作为输入，计算下一层的节点表示为

$$\boldsymbol{X}^{l+1}=\mathrm{HGNN}(\boldsymbol{X}^l,\boldsymbol{H},\boldsymbol{\theta}^l)=\sigma\left(\boldsymbol{D}_v^{-\frac{1}{2}}\boldsymbol{H}\boldsymbol{W}\boldsymbol{D}_e^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{D}_v^{-\frac{1}{2}}\boldsymbol{X}^l\boldsymbol{\theta}^l\right) \tag{2}$$

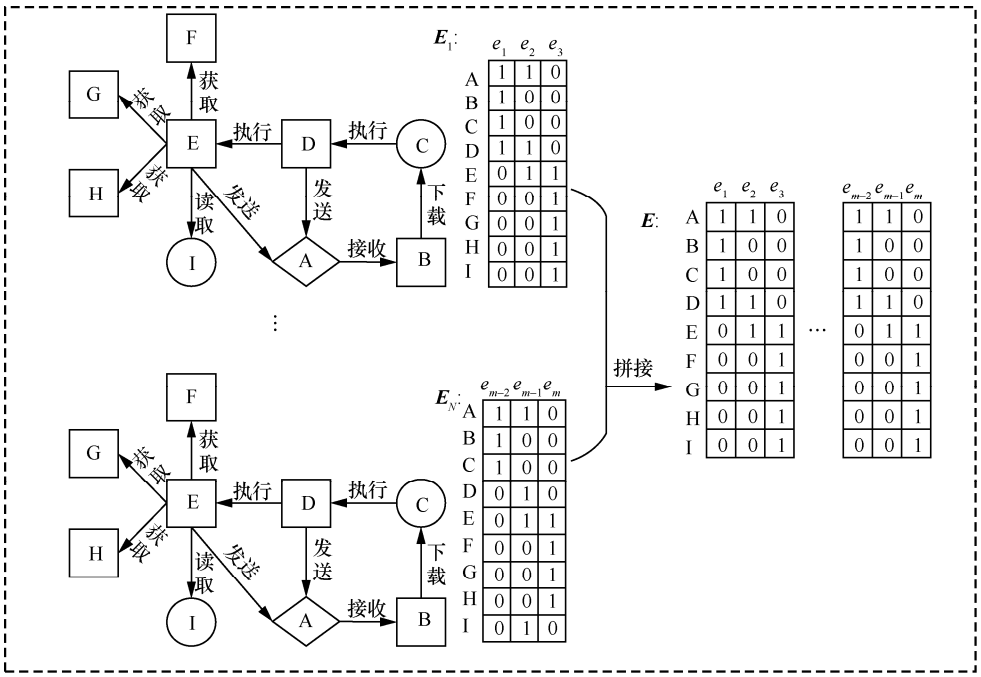


图 4　Trojan 攻击场景下日志超图的构造过程

其中，$\sigma(\cdot)$ 为非线性激活函数，$\boldsymbol{D}_v$、$\boldsymbol{D}_e$、$\boldsymbol{W}$ 分别为对角节点度、边度和边权重矩阵，$\boldsymbol{\theta} \in R^{d_l \times d_{l+1}}$ 为可训练参数矩阵。

HGNN 层可以执行日志图节点–边–节点转换，让日志超图结构更好地细化日志的超边特征。而在 HTTN 模型中，为了提高后续模块中超边匹配层中对超边的匹配效果，对物联网系统日志图采用了节点–边转换的方法，从而将节点特征嵌入超边矩阵中。HTTN 模型中初始日志节点 X^1 可以学习处理 $\boldsymbol{\theta}^0$ 参数矩阵特性，然后根据超边收集日志节点特征，形成超边特征矩阵 $\boldsymbol{R}_e^{|E|\times|N|}$，由 $\boldsymbol{H}^{\mathrm{T}} \in \boldsymbol{R}_e^{|E|\times|N|}$ 实现，最后通过与矩阵 $\boldsymbol{H}$ 的相乘，聚合其相关超边特征，HGNN 层可以充分提取物联网系统与威胁情报日志图中节点的位置与特征信息，提高后续超边匹配的相似度分数。

2.2.4 超图 Transformer 编码层

将经过超图神经网络层处理后的日志超边矩阵 $\boldsymbol{E}$ 输入 Transformer 编码层。Transformer 编码层可以提取日志超边矩阵中的核心特征，弱化日志超边之间的依赖问题。Transformer 编码层主要由以下 2 种结构组成。

1) 多头注意力机制。自注意力机制是对原有注意力机制的改进，是 Transformer 模型中的核心技术。自注意力计算如式(3)所示。

$$\begin{aligned}\boldsymbol{E}\times\boldsymbol{W}^{\boldsymbol{Q}}&=\boldsymbol{Q}\\ \boldsymbol{E}\times\boldsymbol{W}^{\boldsymbol{K}}&=\boldsymbol{K}\\ \boldsymbol{E}\times\boldsymbol{W}^{\boldsymbol{V}}&=\boldsymbol{V}\\ \mathrm{attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})&=\mathrm{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_k}}\right)\boldsymbol{V}\end{aligned}\tag{3}$$

其中，$\boldsymbol{E}$ 为超图 HG 的超边矩阵；$\boldsymbol{Q}$、$\boldsymbol{K}$ 和 $\boldsymbol{V}$ 分别是 Query、Key 和 Value 向量，均来自 $\boldsymbol{E}$；d_k 代表向量 $\boldsymbol{Q}$、$\boldsymbol{K}$ 的维度；$\boldsymbol{W}^{\boldsymbol{Q}}$、$\boldsymbol{W}^{\boldsymbol{K}}$、$\boldsymbol{W}^{\boldsymbol{V}}$ 为随机初始化矩阵，可以让模型在反向传播中学习到合适的参数。

多头注意力机制可以发现日志超边中的位置特征，同时实现多套权重同时计算，并且彼此之间不共享权重，通过对注意力层的堆叠，使日志超图中每个超边的节点注意周围节点的特征。多头注意力机制通过 h 个不同的线性变换对 $\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$ 进行投影映射，如图 5 所示，最后将各个自注意力计算结果拼接起来，如式(4)所示，首先初始化多组权重矩阵 $\boldsymbol{W}_i^{\boldsymbol{Q}}$、$\boldsymbol{W}_i^{\boldsymbol{K}}$、$\boldsymbol{W}_i^{\boldsymbol{V}}$，其中$1 \leqslant i \leqslant h$，分别计算各自的 $\boldsymbol{Q}_i$、$\boldsymbol{K}_i$、$\boldsymbol{V}_i$，再根据注意力机制计算式得到 $\boldsymbol{E}_i^{\mathrm{mha}}$，mha 表示多头注意力机制，将各组 $\boldsymbol{E}_i^{\mathrm{mha}}$ 拼接后与权值矩阵 $\boldsymbol{W}^0$ 相乘，最后映射到原来的空间当中，得到和原来超边矩阵输入维度相同的 $\boldsymbol{E}^{\mathrm{mha}}$，即

$$\begin{aligned}\boldsymbol{E}_i^{\mathrm{mha}}&=\mathrm{attention}(\boldsymbol{E}\boldsymbol{W}_i^{\boldsymbol{Q}},\boldsymbol{E}\boldsymbol{W}_i^{\boldsymbol{K}},\boldsymbol{E}\boldsymbol{W}_i^{\boldsymbol{V}})\\ \boldsymbol{E}^{\mathrm{mha}}&=\mathrm{Concat}(\boldsymbol{E}_1^{\mathrm{mha}},\boldsymbol{E}_2^{\mathrm{mha}},\cdots,\boldsymbol{E}_h^{\mathrm{mha}})\boldsymbol{W}^0\end{aligned}\tag{4}$$

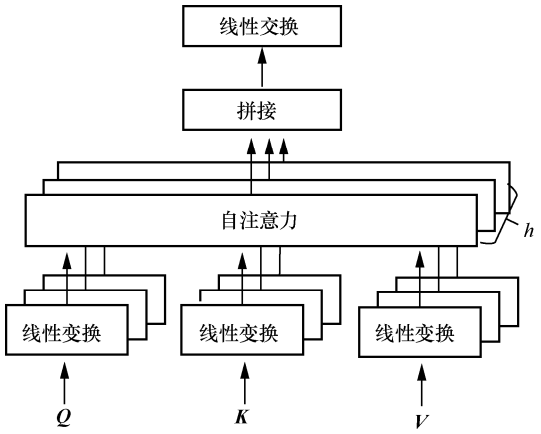


图 5 多头注意力机制

2) 前馈神经网络。超图 Transformer 编码层的前馈神经网络主要解决多头注意力机制对于超图神经网络层处理后的数据拟合程度不够的问题，以便更好地泛化函数，由激活函数为 ReLU 的全连接层和线性激活函数的全连接层构成。

2.2.5 超边匹配层

由于日志超边之间的相关性对图匹配模型非常重要，因此本文在 HTTN 模型中采用了超边匹配机制。传统的图匹配问题大多采用逐个节点进行匹配的方法，由于 APT 攻击隐蔽性、长期纠缠性的特点，仅考虑日志图节点或者单条边的相关性会导致 APT 攻击的威胁情报在物联网系统日志库中的匹配效果不佳。因此，HTTN 模型并没有使用节点特征匹配，而是使用超边匹配的方法，这与将整个图中所有节点进行匹配相比计算效率和计算准确度更高。

超边匹配层的核心部分是计算超图对 H_1 和 H_2 超边之间的相似度分数。首先构建该图对的相似分数矩阵 $\boldsymbol{S}^{n_1\times n_2}$，对于 H_1 中每个超边 e_i^1，计算它与图对中另一个图 H_2 的所有超边的高斯核函数计算分数，即

$$S_{i,j}=\mathrm{e}^{-\frac{\left\|e_i^1-e_j^2\right\|^2}{2\sigma^2}},\ j\in 1,2,\cdots,\left|\varepsilon_2\right|\tag{5}$$

其中，$|\varepsilon_2|$是H_2中超边的数目，e_i^1和e_j^2表示超图H_1和H_2中的超边，σ控制高斯核函数的作用范围，其值越大，高斯核函数的局部影响范围就越大。

2.2.6　相似度分数计算层

在获得日志图相似度分数矩阵之后，需要使用全连接层神经网络来逐步降低日志图相似度矩阵的维度，进而拟合出一个函数实现对日志图的相似度分数计算。全连接层的原理是通过矩阵的向量乘积，实现由一个特征空间线性变换到另一个特征空间，最终实现矩阵的降维。全连接层如图 6 所示。

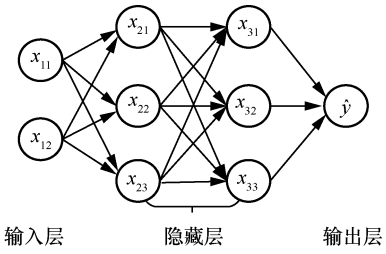


图 6　全连接层

相似度矩阵经过全连接层处理后会计算出日志图相似分数$S_i \in R$，并用式(6)所示的均方误差损失函数与实际相似性分数进行比较，衡量模型对于物联网系统日志图与威胁情报日志图的匹配效果。

$$L = \frac{1}{|G|}\sum_{i=1}^{n}(s_i - s(G_{i,1}, G_{i,2}))^2 \tag{6}$$

其中，并且$s(G_{i,1}, G_{i,2})$表示日志图$G_{i,1}$和日志图$G_{i,2}$之间的实际相似性分数。

3　实验与分析

为了验证 HTTN 模型对 APT 攻击威胁狩猎的准确率与高效性，本文采用 Linux 内核审计日志与多种 APT 攻击场景[15]混合的数据集，并与 SimGNN[16]、GraphSim[17]、H2MN[18]、HGMN[19]等主流图回归模型进行对比实验，最终证明本文所提出的 HTTN 模型在 APT 攻击威胁情报的匹配中具有更好的表现。

3.1　实验准备与实验环境

本文实验的服务器版本为 Ubuntu16.04，设备配置了 4gNVIDIA TITAN RTX 2080 Ti 显卡及 10.2 版本的计算统一设备架构（CUDA）。实验环境为 Python3.7 版本，使用 PyTorch 框架编写，基于网格搜索实验确定 HTTN 模型超参数，如表 1 所示。在 HTTN 模型的训练过程中，使用一阶优化算法 Adam 对模型参数进行优化，来代替传统的梯度下降过程，使训练过程所需内存更少、计算更高效，解决物联网系统内核审计日志数据规模大的问题。

表 1　　HTTN 模型超参数

超参数名称	超参数数值
批大小	256
学习率	1×10^{-3}
权重衰减	5×10^{-4}
层数	5
维度	100
随机步长	5
随机失活	0.1
多头数量	5
训练轮数	1 000

3.2　评价方法

为了对本文提出的 HTTN 模型匹配效果进行准确的评估，本文参照文献[18]中图回归模型实验指标，采用均方误差（MSE, mean square error)、Spearman 等级相关系数ρ和精度@10（简称p@10）分别衡量模型性能。其中，MSE 用来衡量预测相似度分数与真实相似度分数的平均方差；ρ评估预测排名结果与真实排名结果之间的排名相关性；p@10 表示模型结果的匹配精度。

3.3　数据集介绍与预处理

本文实验数据集来自某些 APT 攻击场景[16]下的 Linux 内核审计日志，实验中使用 Mininet+Docker 搭建一个分布式物联网仿真环境以收集物联网环境下的各种日志信息。Mininet 是由虚拟终端节点、交换机、路由器连接而成的一个网络仿真器，采用轻量级的虚拟化技术使系统与真实网络相似；Docker 是一个开源的容器化平台，用于轻量级、快速和可靠地构建、发布和运行应用程序，通过 Docker 可以快速在 Mininet 生成的虚拟终端节点上搭建主机并收集内核审计日志。物联网系统属于分布式架构，其中各项服务大多部署在 Linux 服务器中，因此对服务器安全性要求极高，而内核审计日志基于 Linux 底层对用户系统程序、进程、操作进行记录，可以对 APT 攻击的各个阶段日志信息进行收集。日志图中的一个节点代表一条命令或者程序，一条边代表命令或者程序之间的相关性。

本文在数据集中随机选择了 5 000 个日志图对，按照 60%、20%和 20%划分为训练集、测试集和验证集。由于 APT 攻击隐蔽性的特点，因此威胁情报所生成的日志图节点数量一般不会超过 15 个，对此参照文献[19]对数据集使用了 A*算法生成日志图对的相似度分数。

3.4　不同模型实验结果分析

实验将本文所提出的 HTTN 模型与传统的 SimGNN、GraphSim、HGMN 和 H2MN 图回归模型进行对比实验，实验结果如表 2 所示，各模型训练过程效果对比如图 7～图 9 所示。从表 2 可知，在包含 APT 攻击的 Linux 日志数据集中，本文提出的 HTTN 模型在均方误差上较 SimGNN、GraphSim、HGMN、H2MN 模型分别降低了约 0.807、0.270、0.166 和 0.046；在 Spearman 等级相关系数方面，HTTN 模型相较于 SimGNN、GraphSim、HGMN、H2MN 模型分别提高了 0.061 7、0.022 6、0.007 6 和 0.012 6；在 p@10 指标方面，HTTN 模型相较于 SimGNN、GraphSim、HGMN 和 H2MN 模型分别提高了 0.098 3、0.015 7、0.014 7 和 0.011 8。由图 7～图 9 可以看出，HTTN 模型性能明显优于 SimGNN 模型，取得了良好的效果；与 GraphSim、HGMN 和 H2MN 模型相比，在均方误差和 Spearman 等级相关系数方面，均是在训练 500 轮后开始取得良好效果，而在 p@10 指标方面，则是在模型训练 100 轮之后获得明显提高；关于模型收敛性方面，所有模型的均方误差均是在训练 800 轮之后开始趋近收敛，Spearman 等级相关系数方面开始趋近收敛轮数在 700 左右，p@10 的收敛轮数也在 700 左右。通过对 MSE、ρ 和 p@10 指标的对比，可以充分证明 HTTN 模型中对日志图超边矩阵添加 Transformer 编码层多头注意力的有效性，相较于其他几种模型在威胁情报匹配性能方面取得了提高，若为了得到更高的匹配精度，后续将尝试在超图构造阶段进行改进。

表 2　　**各模型实验结果对比**

模型	MSE	ρ	p@10
SimGNN	$0.980\,3\times10^{-3}$	0.926 1	0.856 6
GraphSim	$0.443\,2\times10^{-3}$	0.965 2	0.9392
HGMN	$0.339\,2\times10^{-3}$	0.980 2	0.940 2
H2MN	$0.219\,3\times10^{-3}$	0.975 2	0.943 1
本文模型	$0.173\,3\times10^{-3}$	0.987 8	0.954 9

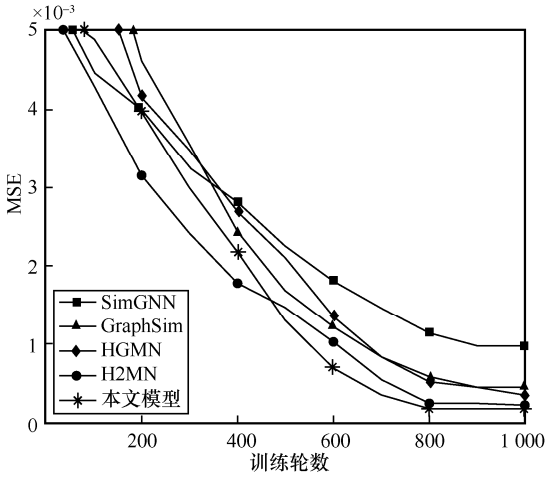


图 7　各模型训练过程 MSE 变化

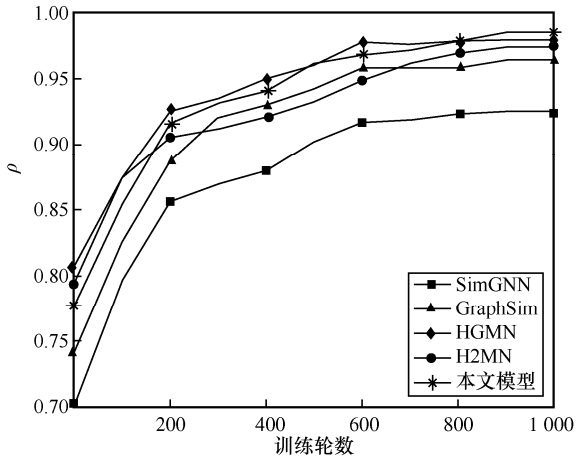


图 8　各模型训练过程 ρ 变化

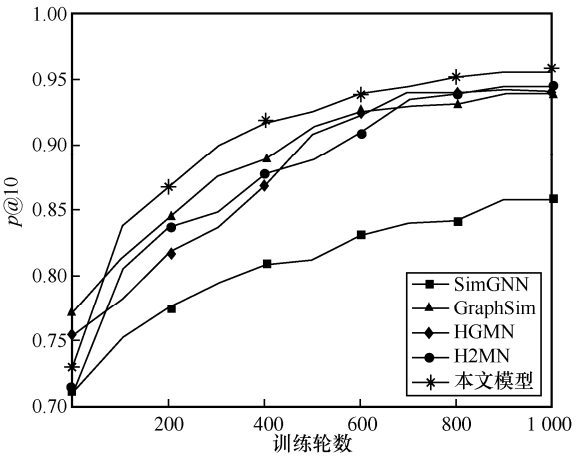


图 9　各模型训练过程 p@10 变化

当物联网系统遭受基于零日漏洞的 APT 攻击时，APT 攻击存在于物联网系统的时间越长，产生的危害也就越大，因此威胁狩猎网络模型的计算时间越短越好，本文进行了不同模型日志图相似度分

数计算时间的对比实验，实验结果如图 10 所示。由图 10 可以看出，HTTN 模型在计算时间上相较于 SimGNN、GraphSim、HGMN 模型分别缩短了 6.14 ms、7.1 ms 和 5.35 ms，与 H2MN 模型的计算时间相差不大，证明 Transformer 中多头注意力机制可以有效提取日志图特征，快速进行相似度分数计算。H2MN 模型所采用的超边池算子方法缩短了相似度分数的计算时间，但匹配精度方面却不如 HTTN 模型。后续 HTTN 模型计算时间的处理上可以尝试做进一步改进。

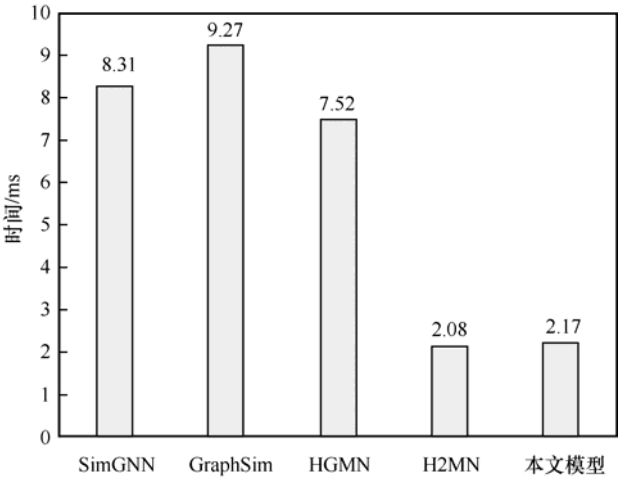


图 10　不同模型日志图相似度分数计算时间的对比

4　结束语

本文提出了一种自适应的超图 Transformer 的威胁狩猎网络模型，将网络威胁情报和物联网系统内核审计日志构建超图，经过 HGNN 层学习超图高阶节点之间的关系，将特征映射到超边矩阵中，采用 Transformer 编码层对超边矩阵添加多头注意力机制，最终通过超边匹配实现对日志图的相似度分数计算，找到与网络威胁情报相匹配的物联网系统内核审计日志。这种模型可以适应不断更新变化的 APT 攻击，完成物联网系统 APT 攻击的威胁狩猎，实现针对 APT 攻击的快速响应和主动防御。

对于物联网系统的威胁狩猎研究并没有结束，本文主要研究的是威胁情报在物联网系统的匹配问题，关于如何将网络威胁情报和物联网系统内核审计日志自动化生成日志图部分的研究并不充分，并没有实现针对 APT 攻击威胁狩猎的完全自动化，这将在后续工作中进行深入研究。

参考文献：

[1] 徐震, 周晓军, 王利明, 等. PLC 攻防关键技术研究进展[J]. 信息安全学报, 2019, 4(3): 48-69.
XU Z, ZHOU X J, WANG L M, et al. Recent advances in PLC attack and protection technology[J]. Journal of Cyber Security, 2019, 4(3): 48-69.

[2] 卢英佳. 我国电力信息系统面临的网络安全风险及处置建议[J]. 中国信息安全, 2019(11): 97-99.
LU Y J. Network security risks faced by China’s electric power information system and its disposal suggestions[J]. China Information Security, 2019(11): 97-99.

[3] PANAHNEJAD M, MIRABI M. APT-Dt-KC: advanced persistent threat detection based on kill-chain model[J]. The Journal of Supercomputing, 2022, 78(6): 8644-8677.

[4] ABDEL-BASSET M, HAWASH H, SALLAM K. Federated threat-hunting approach for microservice-based industrial cyber-physical system[J]. IEEE Transactions on Industrial Informatics, 2022, 18(3): 1905-1917.

[5] ALSAHEEL A, NAN Y, MA S, et al. A sequence-based learning approach for attack investigation[C]//Proceedings of 30th USENIX Security Symposium. Berkeley: USENIX Association, 2021: 3005-3022.

[6] YE Z W, GUO Y B, JU A K. Zero-day vulnerability risk assessment and attack path analysis using security metric[C]//Proceedings of International Conference on Artificial Intelligence and Security. Berlin: Springer, 2019: 266-278.

[7] 徐嘉涔, 王轶骏, 薛质. 网络空间威胁狩猎的研究综述[J]. 通信技术, 2020, 53(1): 1-8.
XU J C, WANG Y J, XUE Z. Research on threat hunting in cyberspace[J]. Communications Technology, 2020, 53(1): 1-8.

[8] 李铁根, 郎颂, 赵日红. 面向工业物联网的终端安全新思考与展望[J]. 工业信息安全, 2022(5): 86-93.
LI T G, LANG S, ZHAO R H, et al. new thoughts and prospects on terminal security for industrial Internet of things [J]. Industrial Information Security, 2022(5): 86-93.

[9] Mandiant. Exposing one of China’s cyber espionage units[R]. 2016.

[10] BARNUM S. Standardizing cyber threat intelligence information with the structured threat information expression[J]. Mitre Corporation, 2012, 11: 1-22.

[11] ZHOU D Y, HUANG J Y, SCHÖLKOPF B. Learning with hypergraphs: clustering, classification, and embedding[C]//Proceedings of the 19th International Conference on Neural Information Processing Systems. New York: ACM Press, 2006: 1601-1608.

[12] FENG Y F, YOU H X, ZHANG Z Z, et al. Hypergraph neural networks[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2019, 33(1): 3558-3565.

[13] YADATI N, NIMISHAKAVI M, YADAV P, et al. HyperGCN: a new method of training graph convolutional networks on hypergraphs[J]. arXiv Preprint, arXiv: 1809.02589, 2018.

[14] KIPF T N, WELLING M. Semi-supervised classification with graph convolutional networks[J]. arXiv Preprint, arXiv: 1609.02907, 2016.

[15] MILAJERDI S M, GJOMEMO R, ESHETE B, et al. HOLMES: real-time APT detection through correlation of suspicious information flows[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2019: 1137-1152.

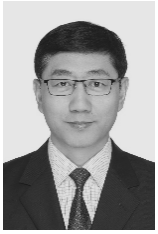
[16] BAI Y S, DING H, BIAN S, et al. SimGNN: a neural network approach to fast graph similarity computation[C]//Proceedings of the Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining. New York: ACM Press, 2019: 384-392.

[17] BAI Y S, DING H, GU K, et al. Learning-based efficient graph similarity computation via multi-scale convolutional set matching[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(4): 3219-3226.

[18] ZHANG Z, BU J J, ESTER M, et al. H2MN: graph similarity learning with hierarchical hypergraph matching networks[C]//Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. New York: ACM Press, 2021: 2274-2284.

[19] LING X, WU L F, WANG S Z, et al. Multilevel graph matching networks for deep graph similarity learning[J]. arXiv Preprint, arXiv: 2007.04395, 2020.

[作者简介]



李元诚（1970− ），男，山东烟台人，华北电力大学教授、博士生导师，主要研究方向为密码学、信息安全等。

林玉坤（1998− ），男，山东烟台人，华北电力大学硕士生，主要研究方向为电力系统网络安全等。