图结构下基于通信模式匹配的物联网异常流量检测方法*

靳文京[1]，周成胜[1]，刘美伶[2]

（1. 中国信息通信研究院，北京　100083；2. 北京友坤科技有限责任公司，北京　100195）

摘　要：物联网的广泛应用带来了新的安全风险，为了在不干扰系统正常运行的前提下实时洞察网络的异常状态，基于流量的异常检测方案应运而生，然而当前检测方案普遍存在通用性欠缺、攻击样本依赖性强的问题。基于此，依据物联网系统运行的物理限制与领域规范，创新性地提出了一种图结构下基于通信模式匹配的物联网异常流量检测方法，在通信图构建的基础上利用子图挖掘、同构子图发现等算法分析表征物联网系统中固定、周期、自动运转的通信模式来构建检测基准，并利用社区检测算法高效、精准地发现实时流量中存在的异常数据。在 BoT-IoT 和 IoT-23 数据集上从不同数据集上的效果对比、不同检测方案的效果对比以及不同时间窗口下的实时检测效率三个方面对方案进行了评估，99% 的检测准确率和秒级的实时检测时间充分证明了本方案的高效性和可用性。

关键词：通信模式；物联网；子图挖掘；社区检测；同构子图

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2024. 06. 002

引用格式：靳文京，周成胜，刘美伶. 图结构下基于通信模式匹配的物联网异常流量检测方法［J］. 网络安全与数据治理，2024，43(6)：8 - 15.

An IoT abnormal traffic detection method based on communication pattern matching within a graph structure

Jin Wenjing[1], Zhou Chengsheng[1], Liu Meiling[2]

(1. China Academy of Information and Communications Technology, Beijing 100083, China;
2. Beijing Youkun Technology Co., Ltd., Beijing 100195, China)

Abstract: The wide application of the Internet of Things has brought new security risks. In order to gain a real-time insight into the abnormal state of the network without interfering with the normal operation of the system, the anomaly detection scheme based on traffic came into being. However, the current detection scheme generally has problems such as lack of universality and strong dependence on attack samples. Based on this, according to the physical limitations and domain specifications of the operation of the Internet of Things system, this study innovatively proposed a method of abnormal traffic detection of the Internet of Things based on communication pattern matching under the graph structure. On the basis of the construction of the communication graph, subgraph mining, isomorphic subgraph discovery and other algorithms are used to analyze and characterize the communication mode of fixed, periodic and automatic operation in the Internet of Things system to build the detection benchmark. And the community detection algorithm is used to find the abnormal data in real-time traffic efficiently and accurately. The scheme was evaluated on BoT-IoT data set and IoT-23 data set from three aspects: effect comparison on different data sets, effect comparison of different detection schemes, and real-time detection efficiency under different time windows. The detection accuracy rate of 99% and real-time detection time of seconds fully proved the efficiency and availability of the scheme.

Key words: communication patterns; Internet of Things; subgraph mining; community detection; isomorphic subgraph

0　引言

物联网技术为智慧城市、智能家居、工业自动化等多个领域带来了巨大的变革，但互通互联的网络架构也增加了安全风险的暴露面。例如，Mirai 蠕虫病毒利用物联网设备的漏洞，发动大规模拒绝服务攻击，导致网络

* 基金项目：2022 年工业和信息化部制造业专项（20230049）

拥堵甚至瘫痪。物联网环境所面临的安全问题对个人、企业、国家都构成了严重的威胁，及时发现安全威胁或提前采取防御措施显得尤为关键，各类关于物联网安全防护和异常检测的研究应运而生。然而由于物联网平台在设计开发、通信交互、访问控制等方面缺乏统一标准，设备的运行环境缺乏有效保护，厂商售后不提供补丁和更新服务等因素，使得现有解决方案往往存在应用面狭窄、自动化程度不足等问题。因此，针对物联网特殊的网络环境，提出一种通用的异常检测机制对于保障物联网安全至关重要。

本文基于物联网本身固有的运转特性（各个设备节点按照约定好的行为进行周而复始的工作），提出了一种图结构下基于通信模式匹配的物联网异常流量检测方法。基于物联网设备在通信频率、协议和范围等方面所存在的客观、独特的要求和规范，在通信图构建的基础上利用子图挖掘、同构子图发现等算法挖掘通信模式以构建检测基准，并在此基础上利用社区检测算法高效、精准地发现实时流量中存在的异常数据。具体而言，本研究的创新点主要体现在三个方面：

（1）通过分析物联网的各类应用场景，总结得到物联网的运行特点："有限的设备节点按照确定的业务逻辑定期运转"。在此基础上基于图结构提出从通信模式的角度对物联网的正常网络运转特性进行表征和刻画，并采用社区检测的方法实现智能化的异常发现。

（2）从事物固有的时空属性角度深入剖析物联网通信过程，发现不同网络在节点类型、节点通联关系、节点通信特征以及频率上都有其稳定、规律的表现。基于此结合通信图的理念，提出基于图的通信模式表征方法，定义为不同时间窗口的通信图中存在的频繁出现的子图。

（3）基于 BoT-IoT 数据集[1]、IoT-23 数据集[2]对本文所提方案进行实验评估，对比基于统计、机器学习、深度学习的不同检测方案的效果以及两个数据集下的检测效果，99% 的检测准确率充分证明了本方案的可行性和优越性，同时，不同滑动时间窗口下秒级的实时检测效率验证了本方法的高效性。

1 国内外研究现状

根据检测方法的不同，基于流量的物联网异常检测方案可以分为基于统计的、基于机器学习的和基于深度学习的检测方案。

基于统计的检测方案采用规则直接判定的方式发现异常，Ma[3]等人设计并实现了一种基于流量特征识别的安全管控系统，通过提取物联网设备的 IP、MAC、身份指纹等多种流量特征采用白名单的思想实现身份认证和异常行为检测。实验环境下设备识别准确率为 96.6%，异常检测准确率为 97.7%，可以有效检测 DoS、端口扫描和其他网络攻击。余建疆[4]提出了基于多特征融合的 IoT 设备异常检测方法 IoT-MFF，从通信量、周期、报头字段取值分布等多个维度提取了统计特征、信息熵特征、小波分解系数特征三个方面的多个特征，结果表明该方法具备较高的检测准确率和较好的实时性。此种方案虽然简单高效但受到规则的限制无法发现新型网络攻击，且规则更新成本高，难以实时跟进日益高级、隐蔽的网络威胁现状。

基于机器学习的检测方法[5]采用数据驱动的思想通过对攻击样本的自主学习智能建立检测基线。刘祥军等[6]针对物联网设备频遭僵尸网络攻击的问题，提出了基于随机森林的特征选择方法，通过降低数据维度提升了模型的检测效率。随后，刘祥军[7]又提出了一种集成学习的个体学习器选择算法，利用相关系数整合差异大的个体学习器，并通过投票方式进行决策。Diallo[8]提出了基于智能流量分类技术的物联网异常检测和攻击识别，通过在数据集上对比多种机器学习检测方案来发现最优解。基于机器学习的检测方案在一定程度上摆脱了规则的限制，具备良好的自主性和智能性，但存在海量不均衡数据上检测准确率低下、数据异构导致模型泛化能力弱等问题。

深度学习由于其强大的特征自主挖掘能力能够解决机器学习面临的样本不均衡、特征提取主观性强的问题，在现有研究中被广泛应用[9-10]。张月等人[11]提出了基于联邦学习的物联网设备异常检测算法。丁庆丰等[12]则提出了一种基于图神经网络的分布式异常流量检测方案。杨威超等人[13]结合物联网系统特点，设计了基于设备型号分类和 BP 神经网络的流量异常检测模型，实现了高检出率。Zou[14]等人提出了一种特征参与的多流长短期记忆（FAMF-LSTM）方案，采用一种基于关系的特征分组算法将特征分类为若干组，并学习每个流内部的时间相关性及其对输出的影响，实现高效的异常检测。

基于机器学习和深度学习的检测方案虽然在自主学习、智能检测上表现良好，但数据驱动的方案需要大量的攻击样本来进行预先学习，在当前网络攻击呈现高级、隐蔽、持续的环境下，获取实时、大量的攻击样本变得非常困难，因此如何摆脱攻击样本训练的依赖实现异常发现成为亟需解决的问题。

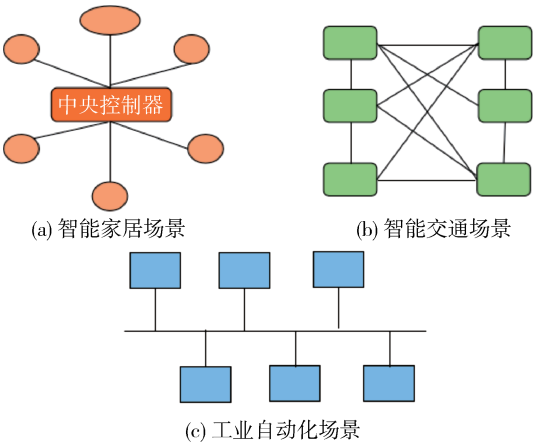
2 通信模式分析

本节通过深度分析物联网运转的网络特性总结了物联网通信模式存在的特点以及表征方法，不仅揭示了物联网设备通信行为的规律性和可预测性，也为后续的异

常流量检测提供了重要基础。

2.1 网络架构分析

图 1 所示是不同应用场景下物联网的网络架构。



(a) 智能家居场景　(b) 智能交通场景

(c) 工业自动化场景

图 1　不同应用场景下的物联网网络架构

智能家居场景中，通常以一个中央控制器（家中的 Wi-Fi 路由器等）为中心，其他设备与之相连，实现集中管理和控制；智能交通场景中由于需要处理大量的实时数据并确保数据传输的可靠性和稳定性，则通过节点之间的直接相互链接实现高度的互联；工业自动化领域则通过一条主要的电缆链接所有节点，实现数据的集中传输和处理。虽然不同场景下的网络结构大相径庭，但如果从网络通信的角度分析物联网设备的运转逻辑，则会表现出相同的特点，具体如下：

（1）网络通信过程（空间）：从组成结构分析，它们都是由限定范围和类型的网络节点以及节点之间的通联关系组成的；从通信过程来看，考虑物联网固定、自动、周期运转的业务特性，网络节点的空间分布、连接固定，且同类设备节点网络通信的特征表现具备相似性和周期、频繁出现的特性。如网络中两个从来没有通信过的设备突然建立了链接或传感器突然上报了一个远超过平常上报字节大小的数据包，就可以发出异常告警提醒可能存在的安全风险。

（2）网络通信频率（时间）：物联网设备的通信频率往往受到其应用场景、设备功能以及能源供应等多种因素的制约。例如，一些传感器设备可能需要定期上报数据，而另一些设备则可能仅在特定事件发生时才进行通信。通过对大量物联网设备的通信频率进行统计分析，可以有效学习通信行为的周期性和规律性，从而为异常检测提供时间维度的判定依据。如门锁在短时间内频繁开启或摄像头突然停止传输数据，就可以发出异常告警提醒可能存在的安全风险。

综上所述，从网络通信的角度分析，不同应用场景下的物联网架构均具备以下几个特点：

（1）设备节点类型固定，节点间的通联关系固定；

（2）同类设备节点的网络通信特点表现相似；

（3）网络通信具备周期性和规律性。

2.2 通信模式表征

基于 2.1 节对不同应用场景下物联网网络运转逻辑的分析，发现不同的物联网网络在节点类型、节点通联关系、节点通信特征以及频率上都有其独特的表现。如果可以自主挖掘并形式化这种特点，则可以为物联网网络建立正常的行为基线并基于此实现准确的异常检测。

基于此，本文作出如下定义：

定义 1　通信图（Communication Graph）：一个通信图 G 是一个有向图，表示为 $G=(V, E, A)$，其中：

V 是节点的集合，每个节点（$v \in V$）代表一个物联网中的通信实体。

E 是边的集合，每条边（$e \in E$）连接两个节点，表示它们之间的通信关系。

A 是边的属性集合，每个属性（$a \in A$）与边（$e \in E$）相关联，并描述了该边所代表的通信的某些特征。

定义 2　通信模式（Communication Pattern）：一个通信模式 P 是通信图 G 的一个子图，$P=(V_P, E_P, A_P)$，其中：

$V_P \in V$ 是参与该模式的一组通信实体的节点集合。

$E_P \in E$ 是这些节点之间通信关系的边集合。

A_P 是与 E_P 中的边相关联的属性集合，表示这些边所代表的通信的特征。

定义 3　边的属性（Edge Attributes）：边的属性集合 A 包含了一系列键值对，用于描述通信的特征。在本文中包括：

数据大小（Data Size）：表示通过该边传输的数据量。

通信频率（Communication Frequency）：表示该边代表的通信发生的次数或速率。

每条边 $e \in E$ 关联一个属性集合 $a \in A$，该集合包含了描述该边所代表通信的特定特征。

定义 4　时间窗口内的通信模式实例（Communication Pattern Instance within a Time Window）：在时间窗口 TW 内，通信模式 P 的一个实例是一个通信图 $G_{|TW|}$ 的子图，$P_{|TW|}=(V_{P_{|TW|}}, E_{P_{|TW|}}, A_{P_{|TW|}})$，其中：

$V_{P_{|TW|}} \in V_{G_{|TW|}}$ 是时间窗口内通信图中的节点子集。

$E_{P_{|TW|}} \in E_{G_{|TW|}}$ 是时间窗口内通信图中的边子集。

$A_{P_{|TW|}}$ 是与 $E_{P_{|TW|}}$ 中的边相关联的属性集合，描述了这些边在时间窗口 TW 内所代表的通信的特征。

图 2 所示是本文所提出的通信模式表征的抽象图。

通过对比不同时间窗口的通信图 G 来找出跨多个时间窗口都频繁出现的子图，也就是本文所提出的通信模式。

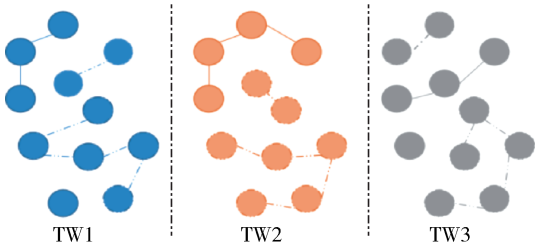


图 2　通信模式抽取抽象图

3　框架

图 3 所示是本文所提出的基于通信模式图匹配的物联网异常流量检测方法框架，包括离线学习和实时检测两个部分。

离线学习阶段通过输入一段时间内物联网通信的正常流量数据，自主学习其中包含的通信模式，构建异常检测的行为基线。具体包括以下步骤：

（1）数据预处理：将网络通信数据按照时间、源 IP、目的 IP、源端口、目的端口、通信包长进行整理，并基于时间窗口对原始序列数据进行划分，每个时间窗口内的数据构成一个子集。

（2）通信图构建：对于每个时间窗口内的数据子集，构建通信图。

（3）子图挖掘：使用 gSpan 图挖掘算法找出每个通信图中的频繁子图。

（4）模式对比与发现：对比不同时间窗口内的通信图，找出跨多个时间窗口都频繁出现的子图。这些子图就是物联网中稳定的通信模式。

（5）通信模式存储：将离线学习阶段得到的所有通信模式存储在图数据库中以便于进行后续的异常检测。

实时检测阶段则是通过旁路部署的方式实时采集物联网的通信流量，抽取出与离线学习阶段相同的特征（包括构建通信图、计算通信频率、提取通信路径等），随后采用图匹配的方法来发现异常的网络流量数据并进行告警。具体包括如下步骤：

（1）预处理实时流量数据：采用滑动时间窗口机制缓存少量的实时数据，并将实时采集的网络流量数据序列转换为通信图的形式。

（2）实时社区检测：基于社区检测算法发现实时流量数据中的社区信息。

（3）异常评分与检测：对于每个实时检测到的社区，计算其与预期通信模式之间的差异或异常评分。设定一个阈值，将异常评分超过该阈值的社区标记为异常。

（4）异常数据提取与报告：从标记为异常的社区中提取具体的流量数据，即不符合通信模式图集合的数据。生成报告或警报，列出这些异常数据及其相关信息（如时间、源 IP、目的 IP 等），以便进一步分析和处理。

3.1　模式提取

通信模式的提取本质上是通过对比不同窗口内的通信图来发现频繁出现的子图的过程，包括子图挖掘和模式对比两个核心步骤。子图挖掘指的是在给定的图集中找出频繁出现的子图结构，是否频繁通过支持度阈值筛选。在本文中选择如算法 1 所示的 gSpan 算法进行实现。

算法 1：gSpan 算法

输入：图集合 G，最小支持度 min_support
输出：频繁子图集合 FS

```
1. 初始化频繁子图集合 FS 为空
2. 初始化 DFS 树 T 的根节点为 null
3. 使用深度优先搜索生成候选子图
   function DFS (current_node):
   for each extension e of current_node:
      new_node = create_new_node (current_node, e)
      if is_frequent (new_node, G, min_support):
         FS.add (new_node)
         DFS (new_node)
4. 调用 DFS (root) 开始搜索
```

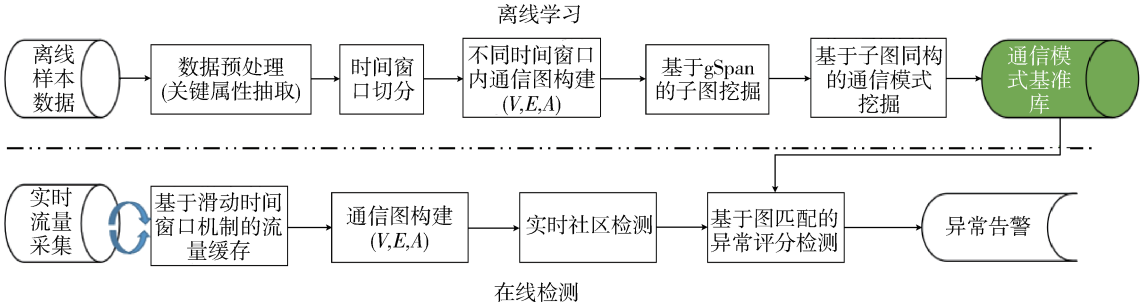


图 3　基于通信模式图匹配的物联网异常流量检测框架

模式对比与发现则涉及在不同时间窗口内的频繁子图之间找出相似的子图结构，本文通过对比子图的节点、边以及边上的属性共同来判定子图是否同构。考虑到物联网节点的量级、子图数量的庞大等，选用 VF2 算法来进行子图模式的对比，具体实现逻辑如算法 2 所述。

算法 2：VF2_SubgraphIsomorphism（大图 G，子图 H）

输入：大图 G；子图 H（包含节点集合和边集合）

输出：存在同构返回映射关系 Map，否则返回空

1. 初始化：
   Map = 空映射
   Cand = V_G　// 候选节点初始为 G 的所有节点
2. while Cand 非空 do
3. 从 Cand 中选择一个节点 v
4. for 每个节点 $h \in V\_H$ do
5. if h 的属性与 v 的属性匹配 then
6. Map［h］= v
7. 更新 Cand：对于 h 的每个邻居 n，查找 v 的邻居中属性匹配且未映射的节点 u，将 u 加入 Cand
8. if 递归判断同构返回成功 then
9. return Map
10. 撤销 Map［h］的映射
11. return 空

// 递归调用时传入当前映射 Map 和更新后的候选节点集合 Cand 到本算法中

3.2　异常检测

为了保证异常检测的实时性和准确性，通常无法留存长时间的实时流量来学习其中的通信模式并与基准库进行匹配，因此在进行异常检测时需要考虑如何利用实时流量中体现的模式局部信息来进行匹配。基于社区的异常匹配方法通过利用图中对象之间的局部关系将图划分为不同的社区或集群来检测那些与社区内其他对象差异显著的节点或边，能够适应本场景的需求。

图 4 所示是本方案中异常检测详细实现流程。具体来说，通过引入滑动时间窗口缓存一定时间段的流量数据并将其转换为图中的节点和边，在此基础之上，使用社区检测算法在图 G 上进行社区划分得到社区集合。在计算异常评分时，从图结构（节点数量、边数量、连接关系）和属性特征（边属性）两个层面综合比较一个社区与预期通信模式的差异。Louvain 算法[15]是一种基于模块度的社区发现算法，其基本思想是网络中节点尝试遍历所有邻居的社区标签，并选择最大化模块度增量的社区标签。该算法是目前研究中最常用的社区发现算法之一。本文采用 Louvain 算法实现实时社区集合的划分。

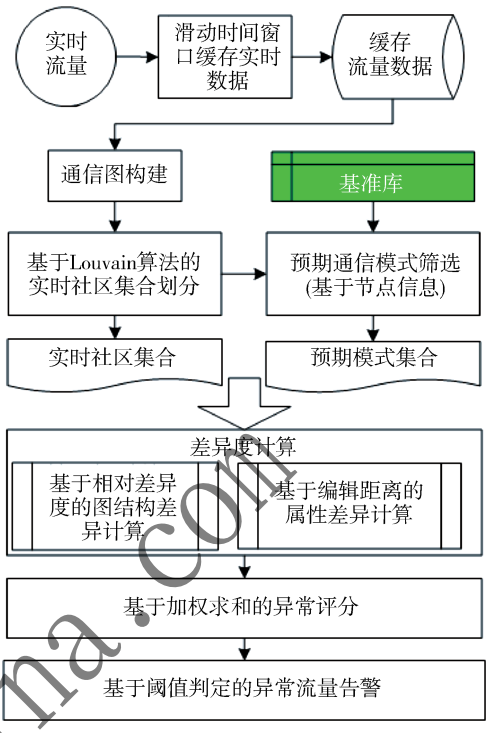


图 4　基于实时社区检测的异常发现流程

4　实验与分析

4.1　数据集

本文的核心思想在于正常网络环境中通信模式的表征学习，因此数据集中需要包含物联网的正常流量和攻击流量，通过调研，本文选择下述两个数据集对所提方案进行验证评估：

（1）BoT-IoT 数据集。该数据集包括正常流量和包含 DDoS、DoS、数据泄露等的攻击流量，其中 pcap 文件大小为 69.3 GB，包含超过 72 000 000 条记录。为了简化数据集的处理，提取了原始数据集的 5%（大约 300 万条记录）进行实验。

（2）IoT-23 数据集。该数据集由不同 IoT 网络流量的 23 个捕获（或称为场景）组成，分为来自受感染 IoT 设备的 20 个网络捕获（pcap 文件）和来自真实 IoT 设备网络流量的 3 个网络捕获。恶意和良性场景都在具有无限制互联网连接的受控网络环境中运行，就像任何真正的物联网设备一样。

两个数据集中的正常流量用于离线训练，攻击流量和正常流量的 10% 组合形成测试集验证模型效果。

4.2　评价指标

本研究本质上是一个二分类任务，因此采用机器学习的常用指标对本文所提方案进行有效性评估。具体计

算指标如下：

（1）准确率（Accuracy）：计算测试集中被正确判定为攻击的流量样本占测试集总样本数量的比例。

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

（2）精确率（Precision）：计算被正确判定为攻击的流量样本在实际攻击流量样本中的比例。

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

（3）召回率（Recall）：计算被正确判定为攻击的流量样本在所有被判定为攻击流量样本的比例，主要体现误报情况。

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

（4）$F1$ 分数（$F1$ Score）：是精确率和召回率的调和平均数，用于综合考虑精确率和召回率的表现。

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

4.3 实验结果

本文设计了三个实验来验证方案的有效性、优越性和高效性。

（1）模型有效性实验：在不同数据集下对比模型的检测准确率来验证模型的有效性和泛化性；

（2）模型优越性实验：在同一数据集下执行不同的异常检测方案，通过对比各类模型的检测效果来验证模型的优越性；

（3）模型高效性实验：对比不同时间窗口下模型的实时执行时间验证模型用于异常检测的高效性。

4.3.1 模型有效性实验

为保证攻击流量样本的随机性，将 BoT-IoT 数据集和 IoT-23 数据集中的测试集均随机均分为 10 份，在基于正常流量完成离线训练后，分别在 10 份不同的攻击流量上计算模型的各类指标。

图 5、图 6 所示分别是本文所提模型在 BoT-IoT 数据集、IoT-23 数据集的检测准确率。根据结果可以看出，在两个数据集下的平均检测准确率、召回率、精准率等都达到了 98% 以上，甚至在某些测试集上达到了 100%，说明本模型对于正常流量、异常流量的识别均很准确，不会出现较高的误报，证明了本文所提方案的有效性和可用性。

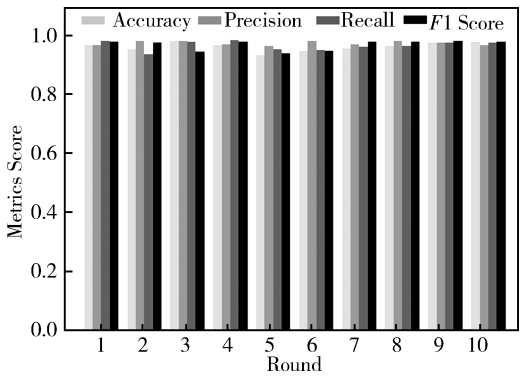


图 5　BoT-IoT 数据集下的模型检测结果

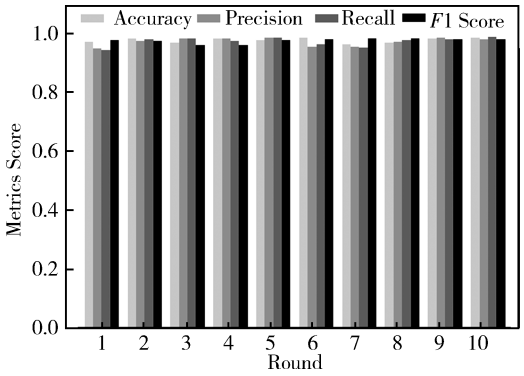


图 6　IoT-23 数据集下的模型检测结果

4.3.2 模型优越性实验

实验选择传统基于统计的异常检测、基于简单机器学习的异常检测、基于深度学习的异常检测与本文所提出的基于通信模式匹配的异常检测方法对比，验证本文所提方案的有效性和精准性。本实验数据集采用的是 BoT-IoT 数据集。

具体而言，基于统计的异常检测方法针对数据集中包含的 DDoS 等攻击建立检测规则（如 1 s 内目的 IP 访问次数、访问频率等特征阈值）；基于机器学习的检测方法则提取常见的如包长、字节长度、平均包长等特征，并选择随机森林作为检测器进行训练和检测；基于深度学习的异常检测方法将原始流量样本输入至 RNN 网络中进行学习和检测。其中基于机器学习和深度学习的方案将 BoT-IoT 数据集中的正常流量和攻击流量按照 1∶1 的比例组成训练集对模型进行初始训练。图 7 所示是不同检测

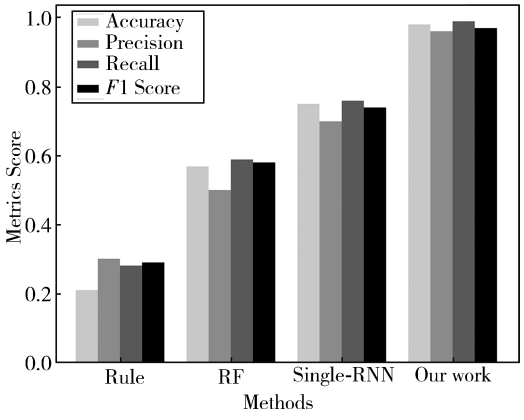


图 7　不同检测方案的检测效果对比

方案下的检测效果，可以看出本文所提检测方案在准确率、精准率、召回率等评价指标上都表现出显著的优势。

4.3.3 模型效率实验

异常检测方法的目标是能够实时、精准地发现网络环境中存在的异常行为，除了准确率，方法的实时执行效率也至关重要。本文提出了基于滑动时间窗口机制的检测方案，考虑系统的实时性要求以及通信图构建需要的缓存数据，一般将时间窗口设置为 1 min、5 min、10 min、15 min、30 min。图 8 所示是本文所提方案在不同滑动时间窗口下的检测执行时间图。同样地，本实验数据集采用的依然是 BoT-IoT 数据集。

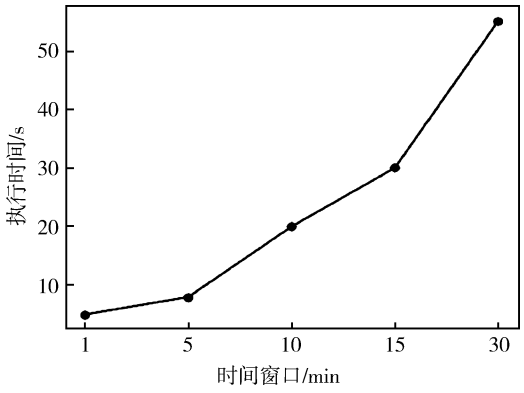


图 8　不同滑动时间窗口下实时检测时间

从图 8 可以看出，即使是 30 min 的滑动时间窗口，在 1 min 内就可以完成图构建、社区检测，充分满足实时性要求。

5　结论

物联网产业的迅猛发展在推动智慧城市、智能家居等领域进步的同时也带了新的安全风险。现有检测方案通用型不足、攻击样本依赖度高等问题使得提出一种通用的异常检测机制对于保障物联网安全至关重要。本文基于物联网运转特性，提出了一种图结构下基于通信模式匹配的物联网异常流量检测方法。该方法深入分析物联网通信机制，利用图结构和算法分析通信模式，构建检测基准，并通过社区检测算法发现异常数据。实验结果表明，本文方法具有高检测准确率和高效性，为物联网安全防护提供了新的思路和手段。

面向不同规模的物联网环境仅需采集一段时间内的正常运行流量就可以建立本模型的检测基线从而实现精准检测，因此该方法具备通用、普适的特点。但是，不容忽视的大规模物联网环境下流量数据的激增会使得离线学习阶段耗时过长，导致检测模型在正式上线运行前期需要漫长的等待，该问题也是后续研究的重点。未来将考虑引入增量、动态的思想将大规模数据背景下的离线学习分割为分段训练，以模式自增的方式来提升效率。

参考文献

[1] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E, et al. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset [J]. Future Generations Computer Systems, 2019, 100: 779 – 796.

[2] GARCIA S, PARMISNO A, ERQUIAGA M J. IoT-23: a labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Z/OL]. [2024 – 04 – 01]. http://doi.org/10.5281/zenodo.4743746.

[3] MA Y, LI N, TENG Z, et al. Anomaly detection and blocking based on power IoT sensing layer traffic features identification [C]//2022 14th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Changsha, China, 2022: 15 – 20.

[4] 余建疆. 基于流量的物联网设备识别与异常检测方法研究 [D]. 长沙: 中南大学, 2024.

[5] 王振东, 张林, 李大海. 基于机器学习的物联网入侵检测系统综述 [J]. 计算机工程与应用, 2021, 57 (4): 18 – 27.

[6] 刘祥军, 江凌云. 基于特征选择的物联网设备流量异常检测算法 [J]. 计算机工程与设计, 2022, 43 (8): 2153 – 2161.

[7] 刘祥军, 江凌云. 基于集成学习的物联网设备异常流量检测算法 [J]. 计算机应用研究, 2022, 39 (6): 1785 – 1789, 1804.

[8] DIALLO C. IoT anomaly detection and attack identification using smart traffic classification techniques [C]//2022 7th International Conference on Frontiers of Signal Processing (ICFSP), Paris, France, 2022: 51 – 58.

[9] ASHRAF J, MOUSTAFA N, BUKHSHI A D, et al. Intrusion detection system for SDN-enabled IoT networks using machine learning techniques [C]//2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Gold Coast, Australia, 2021: 46 – 52.

[10] KHAN A, SHARMA I. Tackling Okiru attacks in IoT with AI-driven detection and mitigation strategies [C]//2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023: 336 – 341.

[11] 张月, 唐伦, 王恺, 等. 基于 GB-AEnet-FL 网络的物联网设备异常检测 [J]. 计算机应用研究, 2002, 39 (11): 3410 – 3416.

[12] 丁庆丰, 李晋国. 一种物联网环境下的分布式异常流量检测方案 [J]. 计算机工程, 2022, 48 (8): 152 – 159.

[13] 杨威超, 郭渊博, 钟雅, 等. 基于设备型号分类和 BP 神

经网络的物联网流量异常检测［J］. 信息网络安全，2019（12）：53－63.

［14］ZOU B L，WEI Y，MA L，et al. Feature-attended multi-flow LSTM for anomaly detection in Internet of Things［C］//IEEE INFOCOM 2022－IEEE Conference on Computer Communications Workshops，New York，USA，2022：1－6.

［15］BLONDEL V D，GUILLAUME J L，LAMBIOTTE R，et al. Fast unfolding of communities in large networks［J］. Journal of Statistical Mechanics：Theory and Experiment，2008：P10008.

（收稿日期：2024－04－17）

作者简介：

靳文京（1991－），男，本科，工程师，主要研究方向：网络安全、信息通信。

周成胜（1982－），男，硕士，高级工程师，主要研究方向：网络安全、工业互联网安全、车联网安全、物联网安全。

刘美伶（1991－），通信作者，女，硕士，主要研究方向：网络安全、数据安全。

（上接第7页）

［7］侯辉广. 无线 Mesh 网络中信誉模型研究［D］. 哈尔滨：哈尔滨工业大学，2015.

［8］LATHIA N，HAILES S，CAPRA L. Trust-based collaborative filtering［C］// IFIP International Conference on Trust Management. Springer，2008：119－134.

［9］WANG X S，SU L，ZHOU Q H，et al. Group recommender systems based on members′ preferencefor trusted social networks［J］. Security and Communication Networks，2020，2020：1－11.

［10］黄艳蓉. 基于机器学习的众包参与者信誉评估研究［D］. 武汉：武汉大学，2020.

［11］陈海彪，黄声勇，蔡洁锐. 一个基于智能电网的跨层路由的信任评估协议［J］. 计算机科学，2021，48（S1）：491－497，503.

［12］李稚楹，杨武，谢治军. PageRank 算法研究综述［J］. 计算机科学，2011，38（S1）：185－188.

（收稿日期：2024－04－29）

作者简介：

郑儿（1984－），女，硕士，高级工程师，主要研究方向：网络安全。

陈麓竹（1997－），女，硕士研究生，主要研究方向：网络安全。

赵静（1983－），女，博士，主要研究方向：网络安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部