Argus: 基于多源数据驱动的工控安全态势感知系统

朱天晨[1,2]，赵军[3]，李博[1,2,4]，李建欣[1,2,4]
1. 北京航空航天大学计算机学院，北京 100191；
2. 北京市大数据与脑机智能高精尖中心（北京航空航天大学），北京 100191；
3. 山东师范大学信息科学与工程学院，山东 济南 250358；
4. 中关村实验室，北京 100191

摘要
工业控制（工控）系统是国家工业制造与民用基础设施的“大脑”，近年来安全风险日益突出，已成为网络安全中的重点防护目标。针对工控安全数据分散、威胁感知滞后的问题，设计了多源数据驱动的工控安全态势感知系统Argus，提出了工控安全感知链，研发了无状态极速设备扫描、威胁情报精准提取、可疑攻击行为检测等工控安全态势自主感知技术，实现了多通道、立体式工控安全监测与态势感知。实验结果显示，相比传统工控安全态势感知方法，Argus系统的感知精度提升超过10%，效率提升两个数量级，并可前摄性地预警、缓解潜在安全风险。

关键词
工业控制系统；多源数据融合；态势感知；威胁情报

中图分类号：TP311 文献标志码：A doi: 10.11959/j.issn.2096-0271.2023051

Argus: multi-source data-driven industrial control security situational awareness system

ZHU Tianchen[1,2], ZHAO Jun[3], LI Bo[1,2,4], LI Jianxin[1,2,4]
1. School of Computer Science and Engineering, Beihang University, Beijing 100191, China
2. Beijing Advanced Innovation Center for Big Data and Brain Computing, Beijing 100191, China
3. School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China
4. Zhongguancun Laboratory, Beijing 100191, China

Abstract
Industrial control system (ICS) is the brain of national industrial manufacturing and civil infrastructure. However, the security risks associated with ICS have become increasingly prominent, making it a significant target for cybersecurity protection. This paper proposed a solution for the issues associated with ICS security data dispersion and delayed threat perception. Specifically, the paper presented a multi-source data-driven ICS security situational awareness system named Argus, which incorporated an awareness chain for ICS security. Furthermore, the paper developed autonomous

situational awareness technologies for ICS security, such as stateless high-speed device scanning, precise threat intelligence extraction, and suspicious attack behavior detection, to achieve multi-channel and three-dimensional ICS security monitoring and situational awareness. The experimental results indicated that, compared with conventional ICS situational awareness methods, the perception accuracy of the Argus system has improved by over 10%, with efficiency improvements by two orders of magnitude. Additionally, Argus allows for proactive warning and mitigation of potential security risks.

Key words
industrial control system, multi-source data fusion, situation awareness, threat intelligence

0 引言

工业控制系统(industrial control system, ICS, 以下简称工控系统)是工业自动化生产的“神经中枢”, 被广泛应用于能源、轨道交通、电力等民生基础领域。随着工业化与信息化的深度融合, 工控系统正逐步从单机走向互联、从封闭走向开放, 网络空间与物理空间的边界被逐步打破[1]。然而, 近年来网络安全事件频发, 被誉为“工业大脑”的工控系统已成为网络攻击的首选目标, 对工业生产、民生经济以及社会安定造成严重威胁[2]。

目前, 研究者已经在工控安全领域开展了广泛研究。具体地, Feng等人[3]研究了ICS的网络包内容及其时序性, 提出了一种基于堆叠长短期记忆网络的入侵检测模型来实现工业控制系统异常检测。Muna等人[4]基于 TCP/IP 包信息, 设计了基于深度自动编码器和深度前馈神经网络的异常检测框架。Chang等人[5]提出了一种基于 K-Means 和卷积自编码器的工业系统异常检测方法。Demertzis等人[6]提出了Gryphon智能系统, 该系统采用脉冲神经网络(spiking neural network)单分类器检测工控系统异常。Krithivasan等[7]则提出了一种基于超图的异常检测技术, 结合增强的主成分分析和卷积神经网络(EPCA-HG-CNN)来感知系统异常状态。Doshi等[8]提出了一种基于在线差异测试(ODIT)的异常检测算法, 该算法依赖假定的基线和攻击模式来感知工控系统态势。Khan等[9]提出了一种基于深度自编码器的工控入侵检测系统, 通过分析流量时序特征来检测工控入侵事件。

目前, 工控安全防护模型与系统大多仅依赖单源数据, 数据来源有限, 且整合能力差。此外, 它们主要通过对流量层进行被动监控来检测入侵威胁等边界安全问题, 导致威胁感知范围有限, 整体防御关口滞后。为了提升工控安全防护系统对威胁感知的范围与时效性, 将对态势感知、早期预警具有重要意义的多渠道数据(例如设备详情、漏洞舆情等)整合到系统中, 有助于实现对工控系统的态势感知和早期预警。这些多源数据间可相互关联, 触发多点分析, 例如通过监测新闻、论坛中曝出的零时差漏洞的来源、软件、版本、端口等相关信息, 可及时关联并预估潜在影响的工控设备数量, 并整合相关工控设备IP地址发出预警信号。

因此, 本文提出“发现-监测-识别”的工控安全态势感知链, 设计并实现了多源数据驱动的工控安全态势感知系统Argus, 以实现多维度立体式主动防御。Argus系统旨在实时整合和分析联网设备、漏洞威胁、可疑访问等多源多模态数据, 并协同处理设备、漏洞、可疑访问等不

同维度的感知面。针对上述3类感知面，本文提出了基于无状态扫描、多属性图建模等方法的多维度工控安全态势感知技术。具体而言，通过无状态极速扫描技术，Argus系统定期扫描全网段的联网工控设备，获取设备指纹信息，以实现工控设备的高效发现；其次，通过Bi-LSTM+CRF模型从网络公开的新闻、论坛、博客等数据源抽取工控安全威胁情报，完成漏洞威胁的实时监测；最后，Argus系统综合利用采集的设备与漏洞信息，搭建工控设备仿真蜜罐，并部署一套基于多属性图建模的异常流量检测算法，用于识别可疑访问及其源头。通过上述感知链，Argus系统能够在工控网络威胁产生的早期快速感知风险，识别潜在的风险源及其可能影响的工控设备网络，进而评估全网工控安全态势并发出可靠的预警信息。总之，Argus系统能够高效精准地发现、监测并识别工控系统面临的潜在威胁，实现工控网络威胁的早期发现与预警，将工控安全风险感知的关口前移。本文的主要贡献如下。

- 首次提出并构建了一种新型的工控安全态势感知系统Argus。该系统通过建立以“发现-监测-识别”为核心的感知链，实现多维度立体式的前摄性安全态势感知，是对工控安全防护的一种重要补充。
- Argus系统汇聚面向工控安全的网络空间多源大数据，分别从联网设备、漏洞威胁、可疑访问3个感知面对工控网络安全态势进行建模与关联，有效实现多源工控大数据的融合，该系统有助于实现工控网络威胁的早期发现与预警。
- 针对工控设备扫描、漏洞威胁监测、可疑访问识别等工控安全态势感知场景，本文提出无状态极速扫描、多属性图建模学习等优化方法。相比传统设备扫描、可疑访问检测等工控安全态势感知方法，扫描效率提升两个数量级，检测精度提升超过10%。

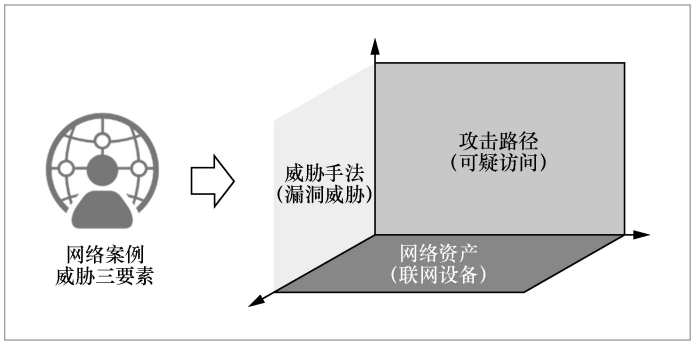

图1 网络空间安全威胁三要素

1 多源数据驱动的工控安全态势感知系统

1.1 系统框架

威胁分析与风险评估 (TARA) 被认为是网络安全分析的核心方法[10]，从TARA的方法论可以看出，网络资产、威胁手法、攻击路径是网络空间安全威胁的三大核心要素（如**图1**所示）。因此，为了全面感知工控网络的安全态势，需要建立以“发现-监测-识别”为核心的感知链，分别从联网设备（网络资产）、漏洞威胁（威胁手法）、可疑访问（攻击路径）3个感知面对工控网络安全态势进行融合建模与感知。

Argus工控安全态势感知系统由三大模块组成：多源数据采集、安全态势分析以及用户交互可视化（如**图2**所示）。系统定期从公开网络和仿真蜜罐上采集工控多源大数据，包括工控设备、安全新闻和访问日志等。系统以“发现-监测-识别”感知链为核心构建工控安全态势感知链路，从联网设备、漏洞威胁和可疑访问3个感知面开展深度分析与融合，以实现工控安全态势的立体式感知与评估。具体而言，首先，Argus系统利用无状态极速扫描技术定期

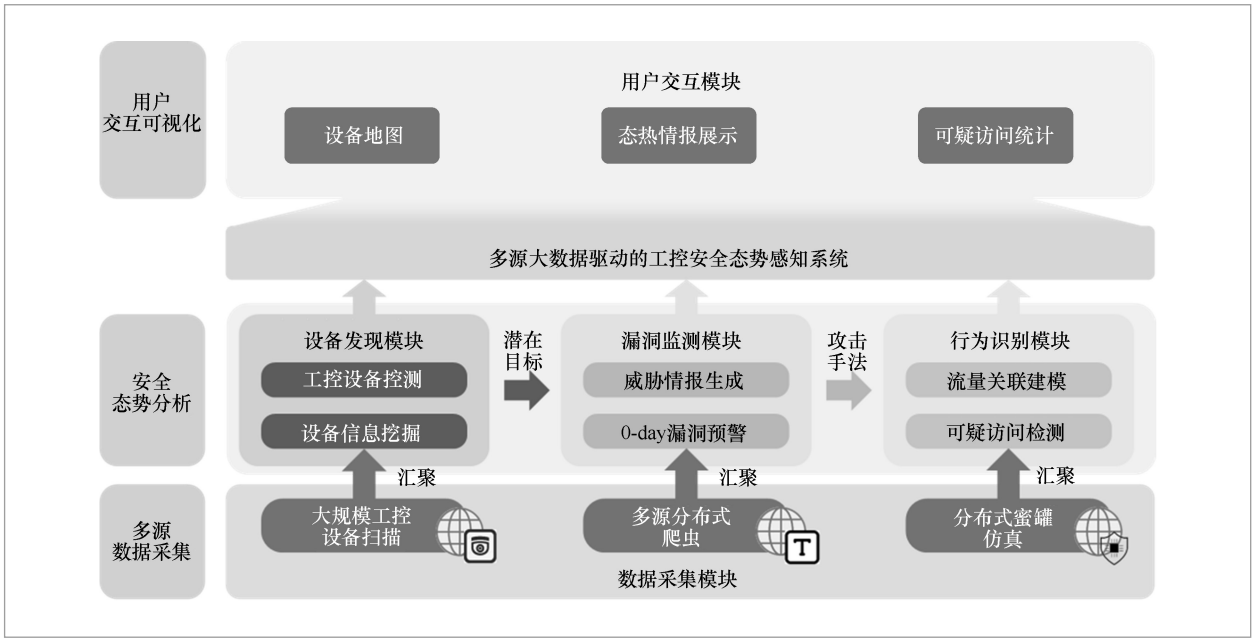

图 2 Argus 系统框架

扫描全网段的联网工控设备，以高效发现工控设备并获取设备指纹信息。其次，通过基于Bi-LSTM+CRF模型的信息抽取模型，从网络公开的新闻、论坛、博客等数据源抽取工控安全威胁情报，完成漏洞威胁的实时监测。最后，Argus系统综合利用采集的设备与漏洞信息，搭建工控设备仿真蜜罐，并部署一套基于多属性图建模的异常流量检测算法，用于识别可疑访问及其源头。通过上述“发现-监测-识别”的感知链，Argus系统能够在工控网络威胁产生早期快速感知风险，识别潜在的风险源及其可能影响的工控设备网络，并发出可靠的预警信息。

1.2 多源数据采集

多项数据采集模块是工控安全态势分析的基础，用于采集多源大数据以提供数据支撑。具体而言，如**图3**所示，该模块包含工控安全认知状态机、工控安全数据源池、工控安全数据仓库3个核心组件，以及4个多源数据采集与高效处理工具，并具备高度相关、动态扩展、循环更新等采集机制。数据采集模块主要用于维护工控安全数据源，定期采集公网暴露的可用工控设备IP地址及端口、最新的新闻博客等工控安全资讯，以及设备访问流量日志等多源工控安全大数据。Argus系统设计并实现了高可靠、可扩展的数据源池，动态采集、更新、融合多源数据，最终形成包括工控安全知识、事件、技术等在内的数据仓库。

1.3 安全态势分析

针对联网设备、漏洞威胁和可疑访问3个工控安全感知面，Argus系统中分别设置了设备发现、舆情监测以及行为识别3个工控安全态势分析模块，建立了以“发现-监测-识别”为核心的感知链，并在此基础上实现了多维感知面融合与综合安全态势评估。

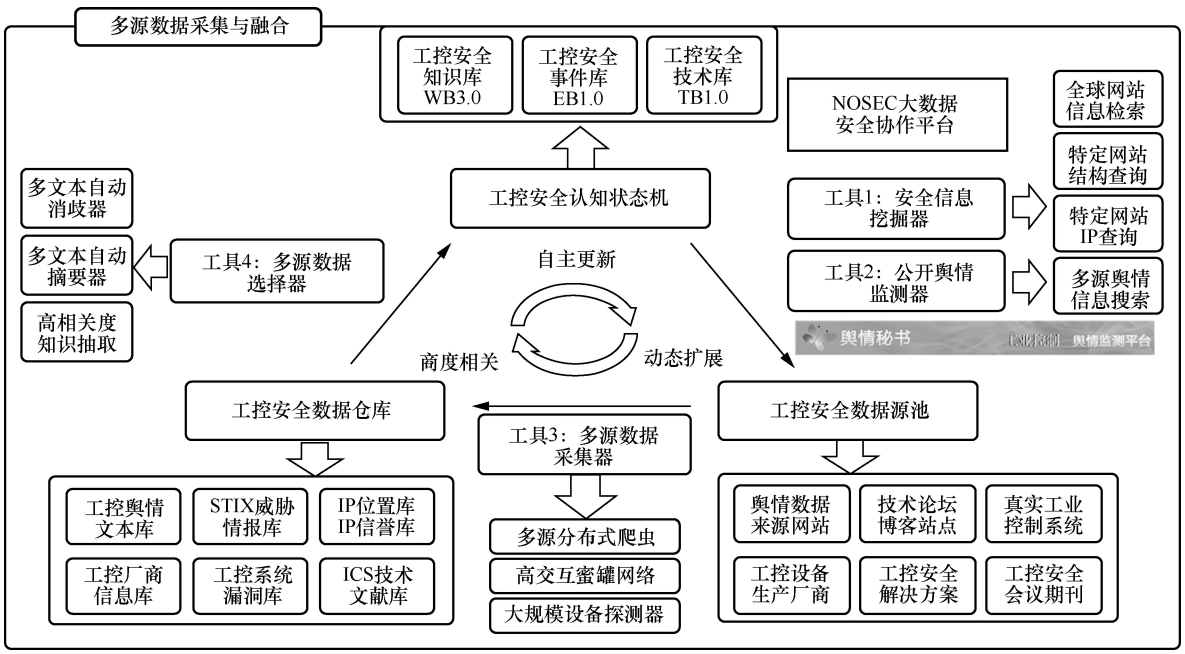

图 3 多源数据采集与融合模块架构

(1)联网设备发现模块

该模块用于扫描联网工控设备信息，建立和动态更新工控设备库。Argus系统周期性地扫描、更新暴露在公网上的海量工控设备，解析工控设备协议，识别相应的设备类型、状态、型号和地理位置等细粒度信息，挖掘不同类型和型号的设备分布，形成并维护工控设备地图与设备库。Argus设计并应用了一种基于无状态扫描与零复制技术的极速扫描算法，可从43亿个可用IP地址中快速、准确地定位暴露在互联网的工控设备和系统，突破了网络端口扫描的效率瓶颈。联网设备发现模块一方面为可疑行为识别模块提供工控设备协议、参数等信息，支撑工控高拟真仿真蜜罐的搭建；另一方面为风险设备分布、风险设备预警、态势指数计算等安全态势分析与可视化提供数据支撑。

(2)漏洞舆情监测模块

该模块用于采集、抽取与工控漏洞相关的威胁情报。Argus系统在新闻媒体、黑客论坛、暗网帖子等平台上进行长期、定点监测，使用设备库和漏洞库中的关键信息作为触发词，在工控安全相关文本中提取漏洞和攻击行为等威胁信息，抽取威胁情报，从而支持工控系统在遭遇安全威胁之前发出前摄性预警。Argus设计并应用了一种面向工控安全的威胁情报抽取算法，可从海量非结构化、半结构化文本中准确提取零时差漏洞等威胁信息。漏洞舆情监测模块一方面为可疑行为识别模块提供包括固件、版本等在内的漏洞威胁相关信息，支撑工控高拟真仿真蜜罐的搭建；另一方面为风险设备评估、态势指数计算等安全态势分析与可视化提供数据支持。

(3)可疑行为识别模块

该模块用于检测工控蜜罐上的异常流

量，记录可疑访问行为的源头信息。Argus系统通过部署分布式工控蜜罐主动检测可能存在的攻击行为，尤其是有针对性地模拟零时差漏洞或高风险重要设备，实时记录其流量访问日志并加以分析，从中识别可疑访问行为，实现主动式安全态势感知。此外，Argus系统实现了一种基于多属性异构图的可疑行为识别算法，有效提升了对“僵尸”设备的检测精度，对于僵尸网络等攻击的规避与预警具有重要作用。可疑行为识别模块为可疑访问数量统计、态势指数计算等安全态势分析与可视化提供了数据支撑。

1.4 用户交互可视化

该模块整合、汇聚、融合多源数据的分析结果，完成风险设备的评估、预警及分布可视化，记录并展示可疑访问的源IP地址、地理位置及访问次数。此外，该模块根据风险设备数量和可疑访问数量综合计算态势指数，提供设备地图、情报卡片、可疑访问统计、知识图谱、态势指数等方式，实现对工控安全态势的综合评估和交互式可视化。

2 面向工控安全的威胁情报抽取

网络威胁情报是一种实现主动式安全态势感知的有效手段，也是工控安全态势感知链的关键。威胁情报本质上是基于证据的知识，旨在通过从安全博客、黑客论坛、暗网帖子等平台提取漏洞、设备型号等威胁信息，可以协助构建仿真蜜罐，发现风险设备，计算工控安全态势指标，并在设备或系统遭遇威胁前发出预警信息[11]。通常，威胁情报从攻击行为和漏洞入手进行描述，通过提取和分析各个攻击和漏洞的特征，对系统面临的威胁进行警报与预警。与通用领域的语料相比，工控安全领域的语料具有许多特点，例如大量专业术语、缩略语以及工控系统特定的单词和短语。这种多源多域的特殊性和异构性使工控安全威胁情报抽取效果不佳。为了提高抽取精度，本文提出了一种基于Bi-LSTM+CRF模型的工控威胁情报高效精准抽取方法。该方法通过内嵌特定的规则，针对性地优化实体抽取的精度，并利用上下文扩充机制优化关系抽取的精度，可以自动化地从非结构化文本中提取IOC，并准确识别工控安全相关的威胁实体和关系。

2.1 工控威胁情报定义

（1）威胁情报实体定义

本文首先参照STIX2.0协议下的威胁情报实体类别[12]对本文所用的威胁情报实体的类别进行定义。该定义见**表1**。

（2）威胁情报关系定义

对于威胁情报中的实体关系，本文将其进行归纳，见**表2**。

2.2 基于Bi-LSTM+CRF模型的工控威胁情报抽取

工控威胁情报的抽取主要包括两个部分：实体识别和关系抽取。威胁情报实体识别是指从工控安全相关文本中识别具有特定意义的实体，例如设备类型、端口号、漏洞名称和机构名称等。威胁情报关系抽取则是指从工控安全相关文本中抽取实体之间的目标关系。

双向长短期记忆网络（bidirectional-long short-term memory，Bi-LSTM）[13]是一种能够捕捉文本序列中上下文信息的神经网络，它能够提高实体识别

表1 威胁情报实体类别定义

实体类别	详细描述
VEN	VEN实体代表生产软件的厂商，例如Microsoft、Tencent等。在STIX2.0中，该实体对应于Identity
PRO	PRO实体代表厂商生产的软件、硬件产品，例如Word、Office等
VER	VER实体代表产品的版本信息，例如ver3.0、v4.2.0等
MOD	MOD实体代表产品中的某个模块或者产品包含的功能组件，例如插件等
FILE/PATH	FILE/PATH实体代表文件路径或URL超链接地址
FUNC	FUNC实体代表文件中的某个具体函数，例如某个文件中的函数名称、某个模组中的类等
PARAMETER	PARAMETER实体是参数实体。它代表文件中的变量和常量，例如某段代码包含的变量num
ATTACKER	ATTACKER实体代表实行攻击的某个组织、团体或个人
VULTYPE	VULTYPE代表漏洞的分类，例如XSS、Stack Overflow、SQL Injection等
VUL	VUL实体代表具体漏洞名称
PROBLEM	PROBLEM实体代表产品、模组、文件或具体代码中客观存在的可能发生的问题

表2 威胁情报实体关系定义

关系类别	详细描述
OWNERSHIP	OWNERSHIP关系的意义为包含，可表达厂商、产品、版本和组件之间的基本联系
USE	USE关系的意义为使用，可表达黑客团体针对某个软件的攻击路径
TARGET	TARGET关系的意义为目标，可表达安全威胁和产品的关联点，这是威胁情报关系脉络中最重要的信息
RELATED	RELATED 关系意义为相关，可表达不同名称的实体内部联系，进而对比分析出不同安全事件中的更多信息

和关系抽取的准确性。假设文本序列 $\text{text}=(\text{word}_1,\text{word}_2,\cdots,\text{word}_n)$，每个词$\text{word}_i$通过word2vec等特征抽取算法转化为词向量 $\boldsymbol{w}_i$。那么文本序列可以表示为 $\boldsymbol{s}=(\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_n)$，该序列通过LSTM分别从两个方向进行计算，即可得到正向输出 $\vec{\boldsymbol{h}}=(\vec{\boldsymbol{h}}_1,\vec{\boldsymbol{h}}_2,\cdots,\vec{\boldsymbol{h}}_n)$ 以及反向输出 $\overleftarrow{\boldsymbol{h}}=(\overleftarrow{\boldsymbol{h}}_1,\overleftarrow{\boldsymbol{h}}_2,\cdots,\overleftarrow{\boldsymbol{h}}_n)$，将这两个输出中对应的向量 $\vec{\boldsymbol{h}}_i$ 和 $\overleftarrow{\boldsymbol{h}}_i$ 拼接为输出向量 $\boldsymbol{h}_i$，即文本序列的输出向量为 $\boldsymbol{h}=(\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_n)$。由于Bi-LSTM模型并不能学习到标签之间的约束，例如在识别时可能会出现B-PRO后出现I-MOD的情况，而在BIO标注中，I开头的实体必须在同样类型的B实体后。因此，为了解决这一问题，本文在Bi-LSTM[13]模型后添加了一层条件随机场（conditional random field，CRF）层[13]，将 $\boldsymbol{h}=(\boldsymbol{h}_1,\boldsymbol{h}_2,\cdots,\boldsymbol{h}_n)$ 作为输入，利用CRF的全局归一化特点学习标签的约束关系。CRF层能够将Bi-LSTM网络输出的概率序列转化为标注序列，通过考虑标注序列之间的依赖关系，进一步提高序列标注的准确性，从而达到更好的效果。

具体而言，首先对Bi-LSTM的输出结果做线性变换：

$$\boldsymbol{P}=\boldsymbol{W}\boldsymbol{H} \tag{1}$$

其中，矩阵 $\boldsymbol{H}$ 是由向量 $\boldsymbol{h}$ 组成的矩阵，$\boldsymbol{H}\in\mathbb{R}^{d\times n}$，参数矩阵 $\boldsymbol{W}\in\mathbb{R}^{k\times d}$，$\boldsymbol{P}\in\mathbb{R}^{k\times n}$ 即为CRF模型的状态特征矩阵。其中k为标签的总类型数，n为词向量的总数，则 $\boldsymbol{P}_{i,j}$ 表示文本序列中的第j个词作为第i个标签的得分，因此整个序列的得分情况如式（2）所示：

$$S(X,Y)=\sum_{i=0}^{n}\boldsymbol{A}_{y_i,y_{i+1}}+\sum_{j=i}^{n}\boldsymbol{P}_{j,y_j} \tag{2}$$

其中，$X=(x_1,x_2,\cdots,x_n)$ 是输入序列，$Y=(y_1,y_2,\cdots,y_n\}$ 是输出序列，$\boldsymbol{A}\in\mathbb{R}^{(k+2)\cdot(k+2)}$ 是状态转移矩阵，其中 $A_{i,j}$ 表示第i种标签转移到第 j 种标签的得分。对该得分进行归一化即可得到概率模型：

$$p_\theta(Y\mid X)=\frac{\mathrm{e}^{S(X,Y)}}{\sum_{\tilde{Y}\in Y_X}\mathrm{e}^{S(X,\tilde{Y})}} \tag{3}$$

其中，Y_X表示输入文本序列所对应的所有可能标签序列集合，则CRF的目标函数为：

$$\underset{\theta}{\operatorname{argmax}}(\log(p_\theta(Y\mid X))) = \operatorname{argmax}(S(X,Y)) - \log\left(\sum_{\tilde{Y}\in Y_X} e^{S(X,\tilde{Y})}\right) \quad (4)$$

为了有效应对互联网公开文本信息的不确定性、时效性和脏数据等问题，并提升传统Bi-LSTM+CRF模型在工控安全领域语料上的实体抽取和关系抽取方面的性能，本文提出了一种数据预处理方式及两种模型优化方法。针对公开语料资源的不确定性，本文采用数据跨源认证的交叉处理方法，通过整合多个高信誉数据源的信息来提高信息的可信度和准确性。同时，为了保证抽取结果的可靠性，本文还采用了多源数据交叉验证机制，通过抽取算法对包含同一威胁事件的多源数据进行分析，并对抽取结果进行交叉验证和确认，从而提高了提取结果的准确性和可靠性。具体方法如下。

（1）数据跨源认证的数据交叉处理

在工控威胁情报提取过程中，原始语料数据中存在的不确定性、时效性和脏数据等问题会严重影响提取结果的准确性和可靠性。为了解决上述问题，本文建立了一个工控威胁情报源的信誉库，动态维护、更新威胁情报来源的信誉度评分和可靠性评分。通过对来源的认证和评估，可以提高提取结果的可靠性和准确性。在此基础上，为了保证抽取结果的可靠性，本文采用多源数据交叉验证机制，通过抽取算法对包含同一威胁事件的多源数据进行分析，并对抽取结果进行交叉验证和确认，从而提高提取结果的准确性和可靠性。

（2）内嵌规则匹配的实体抽取优化

传统Bi-LSTM+CRF模型在抽取格式化实体（如URL、版本号和一些厂商名称）时，可能会出现误差。这是因为这些实体的字符串通常没有任何规律，并且在分词时可能会被拆分为多个单词，导致它们被错误地识别为无关实体。为了解决这个问题，本文在实体识别过程中嵌入了特殊的正则规则，对具有特定模式的实体进行预处理，从而避免了Bi-LSTM+CRF等模型的误判。例如对于VER和VUL实体，本文分别嵌入了**表3**所示的正则规则，从而提高了实体抽取的准确性。

（3）上下文扩充制的关系抽取优化

经典的关系抽取模型[14]通常将两个实体间的文本序列作为上下文信息，并混合词嵌入和实体嵌入等向量作为关系抽取模型的输入。然而，这些方法通常需要在实体抽取阶段学习到精确的向量表示，这导致在涉及误判实体的关系抽取任务上表现不佳。为了解决这个问题，本文设计了一种新的上下文扩充机制，对于待识别关系类型的两个实体，在原文中分别以这两个实体为起点双向扩散，直到遇到距离最近的其他实体为止，采样这一段文本序列并将其加入上下文信息，用于关系的抽取。通过扩大上下文信息至邻近的其他实体，可有效提升误判实体的关系抽取精度。

综上，通过分析互联网上的一些公开文本信息，抽取以漏洞（特别是一些零时差漏洞）和安全事件为中心的威胁情报，并形成漏洞知识库，有效支撑对漏洞威胁程度的研判，辅助构建仿真蜜罐，发现风险设备，计算工控安全态势指标。此外，

表3 威胁情报实体抽取嵌入规则示例

实体类型	正则规则	抽取示例
VER	(v|ver|version)[\.\-]?[\dx]+([\.\-][\dx]+)*[\.\-]?	“version1.0” “ver1.x”
	[\dx]+([\.\-][\dx]+)+[\.\-]?	“1.5.2”
	[\da-z]{32}	32位的commit id
	…	…
VUL	cve-.+	cve-2018-11693
	cwe-.+	cwe-665
	…	…
…	…	…

综合利用设备发现模块中动态更新的设备库信息，可以对具有相关漏洞的工控设备发出前摄性预警，以提高工控系统的安全性。

3 基于多属性异构图的可疑访问行为识别

僵尸网络已成为发动大规模DDoS攻击的重要途径，也是威胁工控网络安全的重要因素。因此如何精准检测僵尸（机器人）流量，在系统边界识别可疑访问行为，是防范僵尸网络等攻击的重要问题，也是工控安全态势感知链的核心。传统基于入侵检测的可疑访问识别模型通常部署在单一的工控系统边界，只能被动地监控针对当前设备的攻击行为，并且无法建模访问行为间的复杂关联，识别精度低且一旦系统面临攻击很难有充足的调整时间。针对上述问题，Argus系统设计了“关联+检测”的可疑访问行为识别框架。该框架一方面搭建了工控蜜罐，广泛模拟各类工业控制设备（如不同种类的PLC和SCADA）来吸引远程攻击，记录访问流量日志用于提前发现可疑的主机与流量并产生预警；另一方面提出了基于多属性异构图关联建模的检测算法，从蜜罐访问日志中建模可疑行为的复杂关联，从而精准检测可疑访问流量及其“僵尸”主机源头，进而为真实的工控设备、系统的防御策略提供调整方向，提升系统的主动防御能力。

3.1 工控蜜罐搭建

Argus系统选取了部分工控设备和系统进行仿真与参数配置，通过部署分布式高拟真工控蜜罐，模拟存在漏洞的工控设备或系统，用于采集并分析可疑的访问流量。仿真对象的选取遵循两个原则：一是优先选取设备发现模块中应用、分布较为广泛的工控系统或设备；二是优先选取舆情监测模块中存在高危漏洞的系统软件或设备固件。工控蜜罐的部署框架如**图4**所示，其工作流程如下。

（1）网络会话构建

在不同网络端口上维持动态蜜罐节点和攻击者的异常会话，由对应端口上的套接字处理请求和应答。

（2）工控协议解析

解析被广泛应用于工控领域的ModusBus、Bacnet、S7、IEC104、Guardian和Kamstrup 6种工业控制通信协议。云端部署多行业多场景的蜜罐节点来模拟上述6种常用工控协议，并仿真其工业生产工艺流程，动态解析多种工控指令报文，实现对不同场景和应用控制协议的动态解析与恶意行为捕获。Argus系统已在全球部署了10个蜜罐节点来捕获工控攻击行为，其统计信息见**表4**。

（3）设备状态模拟

为了提高蜜罐节点的隐蔽性和迷惑性，模板设置数据区设置被蜜罐节点模拟的工业控制设备的状态信息，包括设备名、编号、厂商等不可修改信息和电压值，以及剩余油量等可改的状态信息。

（4）实时数据回传

采用RabbitMQ消息队列构建云端节点与本地内网连接，当蜜罐产生新的访问流量数据时，直接通过该连接将数据发送到数据队列中，由RabbitMQ向内网主机推送数据，实现日志数据实时回传。

3.2 多属性异构图建模

为了准确描述流量数据中可疑访问行为之间的复杂关联，本文利用多属性图对流量数据进行建模[15]。具体而言，将网络

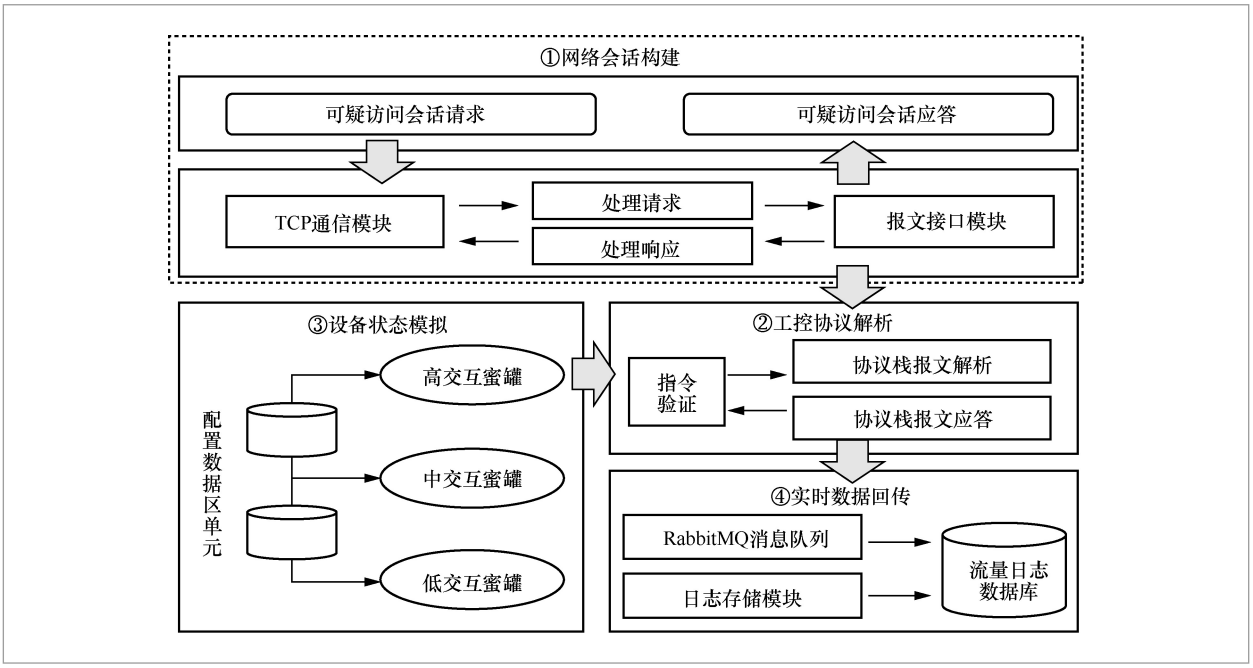

图 4 工控蜜罐部署框架

流数据中报文的6个关键要素定义为图上的节点，将报文之间的传输关联等关系定义为图上的边，将报文中的部分细粒度信息定义为节点的属性。因此可将流量数据形式化建模为多属性图$G=(V, E, A)$，其中V代表节点集合，包含源IP地址、目标IP地址、请求、端口号、协议类型、应答6类节点，节点类型以及属性信息如**图5**所示；E代表边集合，包含的关系类型见**表5**，$A=\bigcup_{i=1}^{m} A_i$ 代表节点的属性集合。

3.3 基于多属性异构图的可疑访问检测

本文将网络流量数据中的源IP地址、端口、请求、目的IP地址、协议类型、响应之间的交互关联建模为多属性异构图$G=(V, E, A)$，并基于此将可疑访问检测的任务转化为异构图上对源IP地址节点的二分类任务，以判定源IP地址对应的主机是否属于可疑的“僵尸”主机[15]。算法流程如**图6**所示，具体流程如下。

表 4 蜜罐节点统计

蜜罐IP	地理位置	采集日志数量/条
114.215.17.58	中国北京	17 356
120.76.53.242	中国杭州	402 068
122.112.235.239	中国杭州	970 783
122.112.235.27	中国杭州	913 285
139.159.221.18	中国深圳	521 352
139.159.221.19	中国深圳	864 532
139.159.221.20	中国深圳	675 277
47.88.212.109	新加坡	4 546 790
47.88.77.143	美国圣马特奥	580 673
47.89.26.43	中国香港	1 124 782

(1) 节点相似性嵌入

由于被劫持的很多“僵尸”主机通常通过脚本等方式批量控制，在进行扫描或网络攻击时，其行为模式具有一定的同源性与相似性，因此可以通过分析访问流量属性之间的关联关系，计算所有主机（即源IP节点）的相似性。本文假设通过重要

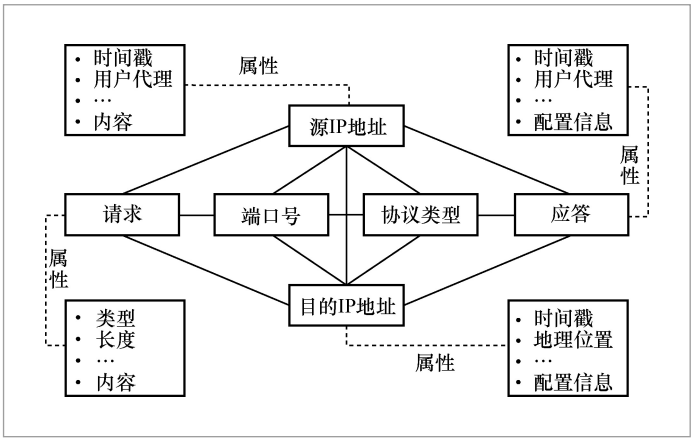

图 5 流量信息建模的多属性异构图概念示意图

表 5 多属性异构图的关系类型

关系编号	对应节点类型	详细信息
R1	源IP地址–目的IP地址	表示从某一源IP地址到某一目的IP地址的连接
R2	源IP地址–协议	表示某一源IP地址通过某一协议发送请求报文
R3	源IP地址–端口号	表示某一源IP地址与其发送请求报文所用端口之间的关系
R4	源IP地址–请求	表示某一源IP地址与其所发送的请求报文之间的关系
R5	源IP地址–应答	表示某一源IP地址与其接收的应答报文之间的关系
R6	目的IP地址–协议	表示某一目的IP地址通过某一协议接收请求报文
R7	目的IP地址–端口号	表示某一目的IP地址与其接收请求报文所用端口之间的关系
R8	目的IP地址–请求	表示某一目的IP地址与其所接收的请求报文之间的关系
R9	目的IP地址–应答	表示某一目的IP地址与其发送的应答报文之间的关系
R10	协议–端口号	表示某一协议利用某一端口进行工作

的元路径（见**表6**）连接的对象，其关联应当更紧密，并且往往更相似[15-16]，因此如果两个源IP地址节点间拥有大量相似的元路径实例，则它们对应的主机更有可能是相似的类型。具体而言，本文采用基于元路径随机游走的相似性度量算法[15-16]，计算源IP地址节点之间的相似性邻接矩阵，如式（5）所示。

$$\mathrm{sim}_{\mathrm{metapath}}(h_i,h_j)=\sum_m^{M'}\vec{w}_m\frac{2\cdot\left|\left\{h_{i\to j}\in P_m\right\}\right|}{\left|\left\{h_{i\to j}\in P_m\right\}\right|+\left|\left\{h_{j\to j}\in P_m\right\}\right|} \tag{5}$$

其中，$h_{i\to j}\in P_m$ 代表源IP地址节点 h_i 在元路径 P_m 下连通源IP地址节点 h_j 的一条路径实例，$\left|h_{i\to j}\in P_m\right|=\boldsymbol{C}_{P_m}(i,j)$，$\left|h_{i\to i}\in P_m\right|=\boldsymbol{C}_{P_m}(i,i)$，$\left|h_{j\to j}\in P_m\right|=\boldsymbol{C}_{P_m}(i,j)$，$\left|h_{j\to j}\in P_m\right|=\boldsymbol{C}_{P_m}(j,j)$，$\boldsymbol{C}_{P_m}(\cdot)$ 是基于元路径 P_m 下的交换矩阵。$\vec{\boldsymbol{w}}_m$ 是一组可训练的参数，代表元路径 P_m 的权重，M' 代表元路径的数量。进而，通过成对随机游走算法[15]可以得到基于元路径的源IP地址的相似性邻接矩阵 $\boldsymbol{A}\in\mathbb{R}^{N\times N}$ 以及对应节点属性矩阵 $\boldsymbol{X}\in\mathbb{R}^{N\times d}$，其中 N 代表多属性图中源IP节点的数量。

（2）图卷积特征提取

进一步可利用图神经网络来提取图上节点的特征，本文定义图上节点的初始特征为 $\boldsymbol{H}^{(0)}=\boldsymbol{X}\boldsymbol{\Theta}$，其中 $\boldsymbol{\Theta}\in\mathbb{R}^{d\times h}$，$h$ 为图卷积的特征维度，进而使用多层图神经网络来学习多属性图上节点的特征：

$$\begin{aligned}\boldsymbol{H}^{(l+1)}&=f(\boldsymbol{H}^{(l)},\boldsymbol{A})+\boldsymbol{H}^{(l)}=\\&\sigma(\boldsymbol{A}\boldsymbol{H}^{(l)}\boldsymbol{W}^{(l)}+\boldsymbol{H}^{(l)}b^{(l)})+\boldsymbol{H}^{(l)}\end{aligned} \tag{6}$$

其中，$\boldsymbol{W}^{(l)}\in\mathbb{R}^{d\times h}$ 是从图神经网络第 l 层到第 l+1层的参数矩阵，$\boldsymbol{b}^{(l)}\in\mathbb{R}^{d\times h}$ 是图神经网络第层的偏置项参数矩阵，σ 是激活函数。

（3）非均衡分类优化

由于可疑访问场景下，正负样本存在极端不均衡的情况，本文采用经过非均衡优化的交叉熵损失函数作为目标函数对模型进行优化：

$$\mathrm{Loss}\left(Y_i,Z_i\right)=-\frac{1}{|Y|}\sum_{i\in Y}\lambda_i\sum_{j=0}^{1}Y_{ij}\cdot\log Z \tag{7}$$

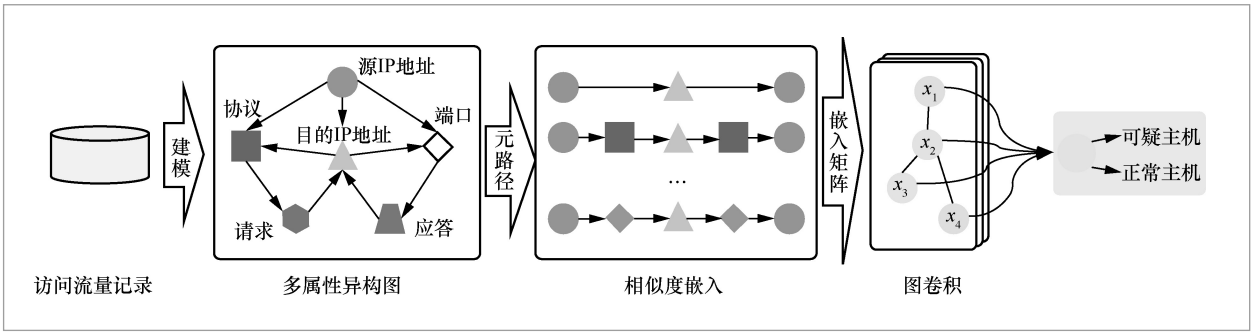

图 6 基于多属性异构图的可疑访问检测算法流程

表 6 多属性异构图的部分元路径示例

对应节点类型	解释
源IP地址–目的IP地址–源IP地址	表示两个源IP地址访问了同一个目的IP地址
源IP地址–协议–源IP地址	表示两个源IP地址使用了相同的协议
源IP地址–端口号–源IP地址	表示两个源IP地址使用了相同的端口
源IP地址–端口–目的IP地址–端口–源IP地址	表示两个源IP地址通过相同的端口访问了同一个目的IP地址
源IP地址–目的IP地址–应答–目的IP地址–源IP地址	表示两个源IP地址通过访问不同的目的IP地址产生了同一应答
…	…

其中，Y_i 表示真实的“僵尸”主机节点，$Z=\sigma(\boldsymbol{HP})$ 表示模型预测的“僵尸”主机节点，$\boldsymbol{P}\in\mathbb{R}^{h\times 1}$ 是输出层的参数矩阵，σ 是输出层的激活函数，λ_i 为对应的样本权重，$|Y|$ 代表全部样本的数量。

4 系统性能验证

4.1 全网设备扫描性能评估

本文利用一台DELL-BQT5132台式机，在100 Mbit/s带宽下对比了传统全连接端口扫描算法[17]与Argus所用的无状态端口扫描算法的性能，实验结果见**表7**。

无状态扫描方法通过提前中断3次握手通信过程，降低了通信双方的会话延迟，并且通信双方不再维护通信状态，节约了系统开销，从而提高了扫描效率。此外，零复制协议栈的引入大幅降低了数据在操作系统内周转的时空消耗，比传统扫描方法整体性能提高86~130倍。在部署有2台DELL-BQT5132台式机1.5 Gbit/s带宽的真实环境下，Argus系统采用的无状态极速扫描方法可以在1 h内完成一次全网工控设备扫描。

表 7 发包速率对比

方法	发包速率
传统全连接端口扫描[17]	9~14 kbit/s
Argus系统	1 000~1 200 kbit/s

4.2 威胁情报性能评估

(1) 数据集

CVE数据集：本文从截止到2019年

9月的CVE平台上爬取了111 868条与漏洞相关的文本并进行标注，并以8:2的比例进行训练集与测试集的划分。

（2）实验结果

图7展示了Argus系统与基线方法Bi-LSTM+CRF分别在工控威胁情报实体抽取与关系抽取任务上的实验对比结果。Argus系统使用威胁情报提取方法在准确率和Micro-F1指标上都取得了最优性能，其性能提升主要归结于以下原因：首先，设计的内嵌规则匹配的实体抽取优化算法能够提升对驳杂无规律的厂商、网址、版本号等实体识别的准确率；其次，提出的上下文扩充感知的关系抽取优化方法，通过引入实体附近更多的上下文信息，可减小上游命名实体识别模型的错判对关系抽取模型带来的误导。综上所述，本文提出的威胁情报抽取优化算法的优势具体可表述为：①通过嵌入正则规则来特殊处理部分格式化实体，避免了传统模型的误判，并提高了抽取准确率；②通过设计新的上下文采样机制来扩充实体之间的文本序列作为上下文信息，有效提高错判实体的关系抽取精度。与此同时，由于上下文扩充的关系抽取优化需要消耗较多的计算资源和时间，因此本文算法在抽取长距离关系时，算法的性能和效率可能会受到一定程度的影响。

（3）工控威胁情报示例

在**表8**中，本文以“Merry X-Mas Ransomware”勒索病毒为例，选择了部分字段，以展示Argus系统在该勒索病毒方面抽取的威胁情报结果。同时，在**表9**中，本文选取“Heap-Based Buffer Overflow”缓冲区溢出威胁作为示例，展示了罗克韦尔厂商安装有ThinServer特定版本的部分设备存在的安全威胁。通过这些情报的正确提取，Argus系统能够针对相关设备、漏洞等发出有效的预警信息。例如，在“Heap-Based Buffer Overflow”威胁情报中，采用“Rockwell”“ThinServer”以及版本号等信息作为关键词进行匹配，就可以在Argus系统的设备库中检索到符合要求的相关设备的数量、IP地址、地理位置分布等信息，并进行可视化，进一步可辅助计算各项安全态势风险指标。

4.3 可疑访问检测模型性能评估

（1）数据集

● CTU-13数据集是美国科罗拉多理工大学（Colorado Technical University，CTU）于2011年发布的一个常用的僵尸网络流量公共基准数据集[18]，该数据集包含

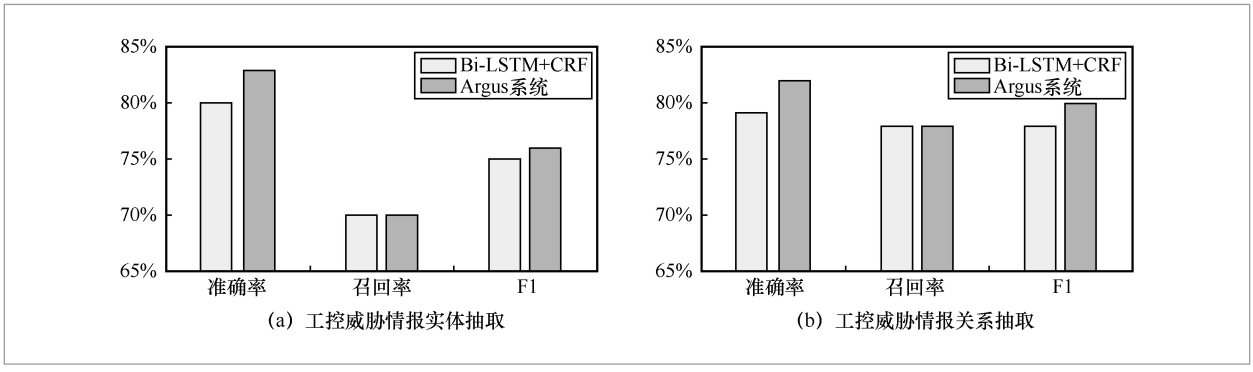

图7 工控威胁情报提取性能对比

13个场景下的78 754条僵尸网络流量和2 743 258条正常流量。

● 蜜罐数据集来源于Argus系统部署的10个模拟不同协议和场景的蜜罐，记录了从2017年6月到2019年6月的流量访问日志，包括但不限于时间戳、源IP地址、目标IP地址、源端口、目标端口、请求、响应、会话持续时间等，该数据集包含5 000多条僵尸网络流量，以及2 738 188条正常流量。

(2)基线方法

● SVM[19]：支持向量机(support vector machine，SVM)是针对分类任务简单而有效的模型，本文将其作为一种可疑访问检测的基线方法。

● Graph-ML[20]：该方法利用图论以及机器学习来解决可疑访问的检测问题，利用有监督和无监督的机器学习方法建立两阶段的基于图的检测方法。

● Graph-Cluster[21]：该方法是一种基于图特征的高效检测方法，通过构建主机之间的拓扑连接图，提取图特征对可疑访问行为进行聚类。

● GCN[22]：图卷积方法是一种处理图数据的先进方法，将主机的拓扑结构和属性信息作为输入。

● HAN[23]：该方法是一种有效的基于注意力的异构图表征方法，可以评估节点级和路径级特征对图表示的重要性。

(3)实验结果

表10展示了不同的可疑访问检测模型的性能对比结果。本文提出的可疑访问检测方法在对可疑访问行为的召回上取得了5%~16%的显著性能提升，这主要得益于两个方面。首先，与Graph-ML[20]等模型不同，本文提出的Argus系统使用了多属性异构图建模工控实体，并学习它们之间的内在交互关系，可以更有效地发现可疑访问源头之间的相似性，从而精准识别“僵尸”主机；其次，相比于基于异构图神经网络的可疑访问检测方法，如GCN和HAN模型[23]，Argus系统采用了元路径双向游走策略，通过学习多种元路径的语义信息得到访问源头的表征向量，并且利用图卷积能够更有效地提取“僵尸”主机的固定行为模式，从而准确识别“僵尸”主机节点。综上所述，本文提出的可疑访问检测模型具有以下优势：①使用多属性图对流

表 8 关于 Merry X-Mas Ransomware 的工控威胁情报示例

字段	值
时间	2019-12-2 19:00:51
漏洞	CVE-2019-7481
厂商	SonicWall
端口	80/TCP
IP地址	192.185.18.204
DNS	neogenomes.com
文件/路径	GET/court/PlaintNote_12545_copy.zip
端口	443/tcp
IP地址	81.4.123.67
DNS	onion1.host:443
文件/路径	GET/temper/PGPClient.exe
端口	443/tcp
IP地址	168.235.98.160
DNS	onion1.pw
文件/路径	POST/blog/index.php
…	…

表 9 关于 Heap-Based Buffer Overflow 的工控威胁情报示例

字段	值
时间	2023-03-21
漏洞	Heap-Based Buffer Overflow
厂商	Rockwell Automation
设备	ThinManagerThinServer
版本	6.x - 10.x 11.0.0 - 11.0.5 11.1.0 - 11.1.5 11.2.0 - 11.2.6 12.0.0 - 12.0.4 12.1.0 - 12.1.5 13.0.0 - 13.0.1
文件/路径	ThinServer.exe
…	…

表 10 可疑访问检测模型性能对比

方法	CTU-13数据集			蜜罐数据集		
	准确率	召回率	F1	准确率	召回率	F1
SVM	84.14	85.32	84.73	82.36	84.21	83.27
Graph-ML	92.31	87.50	88.48	91.04	89.37	90.20
Graph-Cluster	94.17	92.36	93.26	93.21	92.72	92.96
GCN	92.54	91.85	92.20	92.16	91.45	91.80
HAN	93.43	91.89	92.65	93.14	92.81	92.97
Argus系统	92.65	93.47	93.06	93.68	97.71	95.65
提升比例	-1.61%	+1.20%	-0.21%	+0.58%	+5.28%	+2.88%

量数据进行建模，可以更准确地描述流量数据中的可疑访问行为之间的复杂关联，提高了检测的准确性；②采用基于元路径随机游走的相似性度量算法，可以计算源IP地址节点之间的相似性，进一步提高了检测的准确性；③利用图神经网络可以提取多属性图上节点的特征，对高维、复杂的网络流数据有良好的处理能力；④采用经过非均衡优化的交叉熵损失函数作为目标函数，能够处理正负样本极端不均衡的情况。然而，本文提出的模型需要将网络流量数据建模为多属性异构图，并对数据进行预处理和关联提取，因此在处理数据量较大、节点数量较多的场景时训练效率有待提高。

(4)可疑访问检测案例分析

Argus系统收集蜜罐系统的访问日志数据，并通过构建多属性图分析，检测包括僵尸流量在内的典型恶意流量。本文列举几个系统检测出的真实流量与源IP地址实例。

● 针对Modbus协议的恶意访问行为。Argus系统检测到大量疑似DDoS攻击的报文，内容为“30840000002d0201076384000000240400 0a01000a010002010002016401010087 0b6f626a656374436c617373308400000000”，这是高风险的连续的访问行为，可影响所有使用Modbus协议的设备。由于这种访问方式发送的信息长度超过了Modbus协议的标准数据包长度，因此这种访问方式会导致拒绝服务。尽管这类报文不包含任何有效信息，但会导致运行Modbus协议的设备崩溃。Argus系统所用多属性图模型成功检测出源IP地址157.56.***.***以固定的、可疑的访问模式向多个蜜罐发送大量上述报文。

● 针对简单网络管理协议(simple network management protocol，SNMP)的可疑访问行为。这是低风险的访问行为，可以向基于SNMP的设备发送报文，目的是嗅探设备信息，包括系统信息、设备名称、开放端口、描述性信息等。**表11**列出了部分检测到的可疑报文内容。

● 针对Kamstrup协议的可疑访问行为。这是低风险的访问行为，旨在获得基于Kamstrup协议的电网设备的信息。通过发送Kamstrup协议指令来请求0104xx数据，该访问行为可以获得电网设备的发电量等其他详细数据。

表 11 针对 SNMP 协议的部分访问行为

源IP	类型	OID	功能
85.105.***.***	Get	1.2.6.1.2.1.1.1	未知
	Get	1.3.6.1	获取OID的描述性信息
	GetNext	1.3.6.1.2.1.1.1	获取SNMP MIB-2的描述性信息
	GetNext	1.3.6.1.2.1.1.2	获取SNMP MIB-2的OID信息
	GetNext	1.3.6.1.2.1.1.5	获取SNMP MIB-2的主机名称
…	…	…	…

5 结束语

本文设计了一种多源数据驱动的工控安全态势感知系统Argus，通过协同分析暴露的工控设备信息、蜜罐访问日志、工控威胁情报等多源数据，实现多维度立体式安全态势感知，主动监测并感知工控系统周边存在的潜在威胁。实验结果显示，Argus系统使用的无状态工控设备极速扫描、工控威胁情报提取及可疑访问行为检测等方法均取得最优性能，能够长期监测和感知工控系统的安全态势。

参考文献:

[1] BHAMARE D, ZOLANVARI M, ERBAD A, et al. Cybersecurity for industrial control systems: a survey[J]. Computers & Security, 2020, 89: 101677.

[2] 周明, 吕世超, 游建舟, 等. 工业控制系统安全态势感知技术研究[J]. 信息安全学报, 2022, 7(2): 101-119.
ZHOU M, LYU S C, YOU J Z, et al. A comprehensive survey of security situational aware-ness on industrial control systems[J]. Journal of Cyber Security, 2022, 7(2): 101-119.

[3] FENG C, LI T T, CHANA D. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks[C]//Proceedings of 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2017: 261-272.

[4] MUNA A L H, MOUSTAFA N, SITNIKOVA E. Identification of malicious activities in industrial Internet of Things based on deep learning models[J]. Journal of Information Security and Applications, 2018, 41: 1-11.

[5] CHANG C P, HSU W C, LIAO I E. Anomaly detection for industrial control systems using K-means and convolutional autoencoder[C]//Proceedings of 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Piscataway: IEEE Press, 2019: 1-6.

[6] DEMERTZIS K, ILIADIS L, BOUGOUDIS I. Gryphon: a semi-supervised anomaly detection system based on one-class evolving spiking neural network[J]. Neural Computing and Applications, 2020, 32(9):

4303–4314.

[7] PRIYANGA S, KRITHIVASAN K, PRAVINRAJ S, et al. Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph–based convolution neural network (EPCA–HG–CNN)[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4394–4404.

[8] DOSHI K, YILMAZ Y, ULUDAG S. Timely detection and mitigation of stealthy DDoS attacks via IoT networks[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2164–2176.

[9] KHAN I A, KESHK M, PI D C, et al. Enhancing IIoT networks protection: a robust security model for attack detection in Internet industrial control systems[J]. Ad Hoc Networks, 2022, 134: 102930.

[10] ISO. Electrical and electronic components and general system aspects: ISO/TC 22/SC 32[S]. 2021.

[11] SCHLETTE D, CASELLI M, PERNUL G. A comparative study on cyber threat intelligence: the security incident response perspective[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2525–2556.

[12] OASIS. Cyber threat intelligence (CTI): TC. STIX 2.0[S]. 2018.

[13] HUANG Z, XU W, YU K. Bidirectional LSTM–CRF models for sequence tagging[J]. arXiv preprint, 2015, arXiv: 1508.01991.

[14] ZHENG S C, HAO Y X, LU D Y, et al. Joint entity and relation extraction based on a hybrid neural network[J]. Neurocomputing, 2017, 257: 59–66.

[15] ZHAOJ, LIU X D, YAN Q B, et al. Multi–attributed heterogeneous graph convolutional network for bot detection[J]. Information Sciences, 2020, 537: 380–393.

[16] SUN Y Z, HAN J W, YAN X F, et al. Pathsim: meta path–based top–k similarity search in heterogeneous information networks[J]. Proceedings of the VLDB Endowment, 2011, 4(11): 992–1003.

[17] LYON G F. Nmap network scanning: the official Nmap project guide to network discovery and security scanning[M]. Sunnyvale: Insecure, 2009.

[18] GARCÍA S, GRILL M, STIBOREK J, et al. An empirical comparison of botnet detection methods[J]. Computers & Security, 2014, 45: 100–123.

[19] HEARST M A, DUMAIS S T, OSUNA E, et al. Support vector machines[J]. IEEE Intelligent Systems and Their Applications, 1998, 13(4): 18–28.

[20] DAYA A A, SALAHUDDIN M A, LIMAM N, et al. A graph–based machine learning approach for bot detection[C]// Proceedings of 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). Piscataway: IEEE Press, 2019: 144–152.

[21] CHOWDHURY S, KHANZADEH M, AKULA R, et al. Botnet detection using graph–based feature clustering[J]. Journal of Big Data, 2017, 4(1): 1–23.

[22] KIPF T N, WELLING M. Semi–supervised classification with graph convolutional networks[J]. arXiv preprint, 2016, arXiv: 1609.02907.

[23] WANG X, JI H Y, SHI C, et al. Heterogeneous graph attention network[C]//Proceedings of WWW'19: The World Wide Web Conference. New York: ACM Press, 2019: 2022–2032.

作者简介

朱天晨（1996- ），男，北京航空航天大学计算机学院博士生，主要研究方向为大数据分析与处理、强化学习、序列决策等。

赵军（1989- ），男，博士，山东师范大学信息科学与工程学院讲师，主要研究方向为工业控制系统安全、网络威胁情报、图神经网络。

李博（1980- ），男，博士，北京航空航天大学计算机学院副研究员，北京市大数据科学与脑机智能高精尖中心高级研究员，主要研究方向为网络安全、工业互联网、大数据安全等。

李建欣（1979- ），男，博士，北京航空航天大学计算机学院教授、党委书记，北京市大数据科学与脑机智能高精尖创新中心研究员，主要研究方向为大数据分析与处理、机器学习和可信计算等。

收稿日期： 2023-02-28
通信作者： 李建欣，lijx@act.buaa.edu.cn
基金项目： 国家自然科学基金资助项目（No.U20B2053）
Foundation Item: The National Natural Science Foundation of China (No.U20B2053)