基于数据驱动的网络安全态势感知预测

吴宝江
（中国电子科技集团有限公司电子科学研究院，北京　100041）

摘　要：云计算和互联网的快速发展引发网络数据的爆炸式增长，随之而来的网络威胁也变得日益复杂，大量的数据给网络带来了巨大的安全风险。传统的安全措施往往不足以抵御这些持续动态变化的网络安全威胁，需要综合应用人工智能和机器学习等技术，基于数据驱动形成数据应用智能化，采用态势数据采集、大数据关联分析、安全威胁研判等手段，实现网络安全威胁实时监测并预测潜在的网络攻击行为，支撑防御策略动态调整，提升网络空间安全防御整体效能。此外，基于数据驱动的网络安全态势感知预测系统能够帮助网络安全管理人员丰富网络风险处理相关专业知识，在实际网络安全威胁场景下做出更好的判断和决策。

关键词：数据驱动；安全态势感知预测；人工智能；机器学习；安全防御
中图分类号：TN918.91；TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.05.003
引用格式：吴宝江. 基于数据驱动的网络安全态势感知预测［J］. 网络安全与数据治理，2025，44(5)：17-20.

Data-driven network security situational awareness and prediction

Wu Baojiang
(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: The rapid development of cloud computing and the Internet has led to the explosive growth of network data, and the ensuing network threats have become increasingly complex. A large amount of data has brought huge security risks to the network. Traditional security measures are often insufficient to resist these constantly changing network security threats. It is necessary to comprehensively apply technologies such as artificial intelligence and machine learning to from data-driven intelligent data applications, using situational data collection, big data correlation analysis, security threat analysis and other means to achieve real-time monitoring of network security threats and predict potential network attack behaviors. It can support dynamic adjustment of defense strategies, and improve the overall effectiveness of network security defense. In addition, data-driven security situational awareness and prediction systems can help network security managers enrich their related professional knowledge of network risks, and make better judgments and decisions in actual network security threat scenarios.

Key words: data-driven; security situational awareness and prediction; artificial intelligence; machine learning; security defense

0　引言

由于日益增长的网络环境威胁和越来越多的网络恶意攻击行为，网络安全已经成为当今互联网世界的一个重要问题。传统的安全解决方案已经不足以抵御当今各个领域持续不断动态发展的网络安全威胁，亟需能够有效感知预测并防御网络安全威胁的创新方法。因此，本文提出基于数据驱动的网络安全态势感知预测方法，它能够提供主动预测策略和实时监测，将为网络安全管理人员针对网络安全事件做出快速、准确决策提供有力支撑，使网络安全管理人员能够有效分配资源，采取应对措施，保护网络环境免受安全威胁。

数据驱动不仅是数据的采集分析，更是数字化时代催生的各类创新技术（人工智能、机器学习等）的综合应用，进而形成数据应用智能化，是利用数据分析来获取有用知识的过程，并最终做出智能决策。由人工智能和机器学习赋能的基于数据驱动的网络安全态势感知预测方法，利用网络日志、系统安全事件和用户行为等众多来源产生的大量数据来预测潜在的网络攻击，这使得积极主动和自适应的网络防御系统成为可能，而不是仅仅依赖预定义的规则和标签来防御网络威胁。此外，网络安全管理人员还可以通过从数据分析中获得的有用知识对网络攻击对手进行分析，深入了解其网络攻击方法、

技术和程序，以便在实际网络安全威胁场景下做出更好的人工判断和决策。

1 相关研究工作

1.1 安全态势感知

网络环境态势是指由网络设备运行条件、网络行为和用户行为等各种因素构成的整个网络空间的现状和趋势。安全态势感知能够获取、理解和展示网络环境的安全要素，是一种科学有效的网络安全态势评估，它利用相关技术对网络安全的变化趋势进行合理预测，预先提醒网络安全管理人员需要对网络设备、网络节点主机和数据资源进行调整、升级和备份，以应对网络环境可能存在的安全风险和威胁，将由此带来的损失降低到能够接受的范围[1]。

安全态势主要包括网络、流量、终端、业务系统等几方面的安全态势[2-3]。其中，（1）网络综合安全态势感知：收集汇总网络环境内的网络设备、安全设备等的原始安全事件数据以及分析研判后的安全评估数据，具体包括安全设备的访问控制数据、安全审计数据、边界完整性检查数据、入侵防范数据、恶意代码防范数据，形成网络综合安全态势；（2）流量安全态势：采集原始数据结合分析研判后的评估数据，呈现病毒蠕虫、特种木马、命令控制 C&C、钓鱼邮件、0DAY 漏洞等高级威胁行为，形成流量安全态势，具体包括恶意代码分布统计（病毒蠕虫、特种木马、命令控制 C&C、钓鱼邮件、0DAY 漏洞等）、风险终端列表（终端 IP、租户名称、恶意代码、命令控制 C&C、钓鱼邮件等）、实时告警信息（事件时间、源 IP、源地理位置、目的 IP、目的地理位置、目的单位、事件类型、事件描述、威胁级别）等；（3）终端安全态势：对比分析终端相关的配置是否合规、日志审计是否异常、是否存在安全威胁，形成终端安全态势，具体包括不合规终端总数、不合规终端的告警级别分布、不合规终端的配置类型分布、审计异常终端总数、审计异常终端分布（系统行为审计、拒绝访问审计、系统登录审计、账号变更审计、软件审计、操作审计）、风险终端列表（单位、IP、不合规类型、审计类型、告警时间、告警级别、详情）等；（4）业务系统安全态势：呈现业务系统的安全状态、可用性状态，漏洞、木马、敏感内容、暗链、断链等安全威胁，具体包括业务系统威胁统计（包括漏洞、挂马、暗链等）、实时风险系统（详情包括系统名称、风险分数等）、高风险系统历史趋势、实时扫描任务等。

1.2 基于机器学习的预测方法

机器学习善于处理小样本和非线性数据，能够提供高准确性和易于理解的数据分析结果，因此可以使用机器学习技术来预测网络安全状况。在已有研究中，Hu 等人[4]提出了一种基于 MapReduce 和支持向量机模型（SVM）的网络安全状况预测模型，该模型利用布谷鸟搜索（CS）算法优化 SVM 参数，并通过 MapReduce 进行分布式训练以提高网络安全状况预测模型训练速度。Peshave 等人[5]提出基于隐马尔科夫模型（HMM）预测网络安全威胁事件，并通过最大似然策略评估预测准确度，该策略在恶意网络事件预测方面优于基线预测方法。张婷婷[6]提出运用长短期记忆网络（LSTM）安全预测模型来设定模型超参数，进一步提升网络安全态势预测模型的准确性。陈乾等人[7]提出基于 Transformer 的应用层协议识别方法，通过多注意力机制的模型获取更充足的协议数据时间特征，以此提高信息安全领域协议识别能力。杨莹等人[8]运用图神经网络（GNN）优化图节点特征和边信息提取 GNN 模型，提出无数据模型提取攻击的机器学习安全问题解决方法。

尽管机器学习技术具有显著的优势，但在处理大规模网络安全数据时仍然面临着模型训练和设计方面的挑战。

2 基于数据驱动的网络安全态势感知预测

基于数据驱动的网络安全态势感知预测是一种融合了数据分析、自动学习及预测模型的高级安全分析方法。该技术旨在通过深入分析历史和实时的网络安全数据，识别数据流动、用户行为、系统活动等方面的模式和趋势，构建预测模型来估计未来可能出现的安全态势，包括潜在威胁的发展、攻击行为的演化以及安全漏洞的暴露风险等。

2.1 数据驱动建模

有效的建模技术对于提取和解释网络安全态势感知中有用的知识是至关重要的，运用各种数据预处理和可视化技术，以及高级建模人工智能和机器学习算法，完成有用知识的提取。基于数据驱动的网络安全态势感知预测包括数据收集、数据预处理、数据特征提取、模型构建、模型开发与训练和模型综合评估等部分，实现网络安全威胁实时监测并预测潜在的网络攻击行为，支撑防御策略动态调整，提升网络空间安全防御整体效能，同时帮助网络安全管理人员提高对网络风险的专业认识，丰富相关专业知识，使其在实际网络安全威胁场景下做出更好的判断和决策。基于数据驱动的网络安全态势感知预测具体组成部分如图 1 所示。

广泛全面地收集网络安全相关数据，包括日志、网络流量、系统安全威胁警报和历史攻击事件等，对收集到的数据进行预处理、清洗、转换。

运用统计分析或机器学习算法[9]，从预处理后的数据

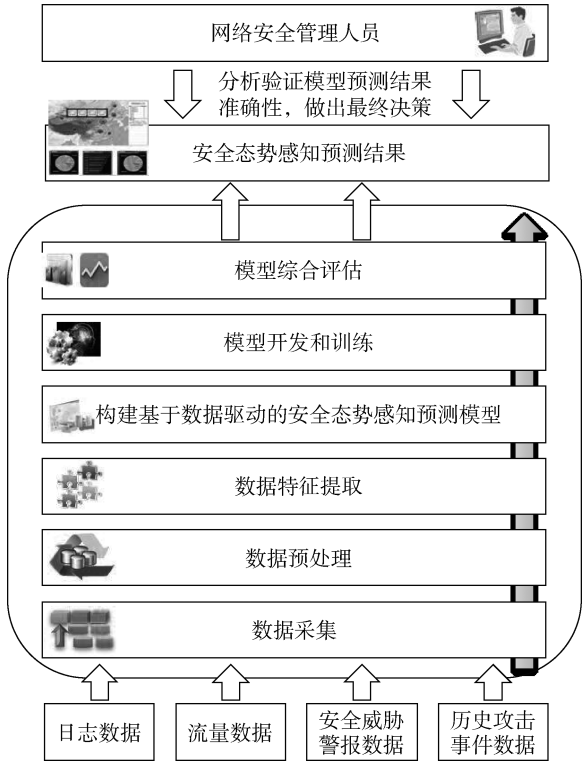

图 1　基于数据驱动的网络安全态势感知预测

中选择或提取有意义的特征信息，用于构建基于数据驱动的安全态势感知预测模型。在某些情况下，需要基于上下文信息和对网络风险及漏洞的专业知识进行特征提取。

在进行高级建模和决策之前，可以运用不同的统计和可视化工具，如散点图、柱状图、热图等对数据的分布、相关性和结构进行分析，以此进一步深入理解数据结构和模式，并识别与网络安全威胁相关的行为模式。而后运用人工智能和机器学习技术（如决策树、随机森林、神经网络等）[10-11]建立网络安全态势感知预测模型。为提高模型性能和泛化能力，需要对模型参数进行优化，开发或集成多个基础模型，通过聚合来自多个基础模型的分析结果来训练安全态势感知预测模型，以提高最终模型的鲁棒性、通用性和总体准确性。

利用相关网络数据建立和训练完模型后，需要对模型进行综合评估。利用 K 倍交叉验证等方法对模型准确性、精度进行评估。运用网络安全态势感知预测模型能够检测到各种网络威胁，但感知预测结果并不是百分之百准确的，需要网络安全管理人员运用专业知识对模型预测结果进行分析和验证，并最终做出关键性的决策。

评估结果令人满意的安全态势感知预测模型可以部署在网络安全环境中，并不断评估其性能、检出率、错报率等，通过定期更新、再训练来适应不断变化的网络安全威胁。整合运用数据分析、机器学习技术和网络安全专业知识，使基于数据驱动的安全态势感知预测模型具有适应性和弹性，以应对不断演变的网络安全威胁。

2.2　关键技术分析

基于数据驱动的安全态势感知预测能够识别网络各种活动的安全风险，并从宏观角度进行威胁意图理解和影响评估，预测网络安全的发展趋势，从而为网络安全管理人员提供合理的决策支持，其关键技术主要包括安全态势数据采集、态势评估和态势预测。

2.2.1　安全态势数据收集

安全态势数据收集是基于数据驱动的安全态势感知预测的前提。在大多数情况下，安全态势数据包括网络拓扑、漏洞和状态数据以及通过各种防御措施和分析技术获得的日志数据和威胁数据，这些数据的有效整合为态势感知预测的高维理解和分析提供了基础。

现在的信息网络具有高度灵活性和动态性，安全态势数据的生成速度快、规模大、格式复杂，必须采用有针对性的多源数据采集、清洗、转换方法，以提高数据采集提取效率和准确性。运用分布式日志采集处理框架 Logstash 或者 Fluentd 进行日志收集、过滤和转发，通过基于零拷贝技术的采集引擎 DPDK 实现实时网络数据采集，然后进行链路层、网络层、传输层的预处理解析，根据会话流（IP 地址、端口、协议）的 Hash 进行负载均衡式分发。但是上述方法均有其局限性，造成的数据缺失将会为数据融合和冗余处理带来问题，因此改进数据收集、提取技术仍然是一个热门的研究领域。

2.2.2　安全态势评估

采用 HDFS、HBase、ElasticSearch 等技术实现告警、事件、日志的存储、统计和检索，建立知识数据库，以此运用基于知识推理的方法进行安全态势评估。但由于收集大量的推理规则和先前经验信息是十分困难的，因此该方法具有很大的限制性。

通过应用机器学习构建安全态势情景模板，使用模式匹配和映射对态势情景进行划分，这种模式识别评估方法比知识推理更为复杂，但对专业知识和先前经验信息的依赖较少，具有处理能力强大且不完全依赖专家知识的优点。不过，该方法在模式提取步骤中需要处理日益复杂的数据，这降低了安全态势评估的有效性。

2.2.3　安全态势预测

网络安全态势评估的最终目标是安全威胁风险预测，使网络安全管理由被动变为主动。机器学习的出色自学习和自适应能力能够提供快速收敛和高容错性，提升安全态势预测准确性。但是机器学习获得参数，必须有足够的训练参数，即使马尔科夫模型能够预测不同的时间序列，但仍然需要一组训练数据。

在短期安全态势预测中，灰色理论可以提供少量的样

本数据，无需任何训练数据即可提高态势预测的准确性，但网络样本数据庞大且复杂，灰色理论的局限性也是显而易见的。另外支持向量机（SVM）模型具有很强的泛化能力以及良好的适应性、快速收敛速度和强大的数学理论支持，可以将训练集按照类别分开，或是预测新的训练点所对应的类别。利用 K 倍交叉验证法快速计算粒子适应度，在提高预测模型精度的同时不失模型可靠性和稳定性。总之需要构建“数据－模型－技术－评估”的闭环优化体系形成技术迭代来不断提升安全态势预测准确性。

3 面临的挑战

虽然基于数据驱动的网络安全态势感知预测对网络安全管理提供了有效决策支持，但研究人员和网络安全管理人员仍然面临着很多挑战，主要挑战如下：

（1）算法可解释性：在网络安全环境下，理解人工智能和机器学习算法如何做出相关决策和输出数据是至关重要的，研究人员需要专注于开发可解释的人工智能技术，为算法背后的推理提供解释，使网络安全管理人员能够验证模型的预测结果。

（2）隐私保护问题：研究人员需要开发隐私保护技术，如差异隐私、联邦学习、数据匿名化等方法，以确保网络中个人和敏感数据的隐私得到保护。可以运用联邦学习支持多个设备上训练模型，而不需要共享原始数据，从而保护数据隐私。

（3）对抗攻击和防御：网络攻击对手可以操纵数据或使用中毒数据来误导机器学习算法，导致错误的决策或绕过检测机制。研究人员需要研究异常检测技术，识别不寻常的网络行为，检测以前未知的或看不见的威胁和零日攻击。将数据驱动的机器学习和专家知识相结合形成混合模型算法，以提高安全态势感知预测模型的整体有效性。

（4）通用化和可扩展化：基于数据驱动的安全态势感知预测模型在网络安全方面的有效性可能因不同环境和不断演变的网络威胁而不同，因此，需要确保模型的通用性和普遍适应性。研究人员需要研究迁移学习技术以帮助模型保持较高的检测精度，并适应新的网络攻击威胁模式。同时，由于网络安全数据呈指数级增长，还需要开发可扩展的算法、分布式计算框架和优化处理决策，以保证模型的弹性和预测效率。

综上所述，基于数据驱动的安全态势感知预测涉及数据质量、模型鲁棒性、隐私保护等多方面问题，应对这些挑战是未来研究和改进的关键重点。

4 结束语

由于信息网络环境日益复杂，网络环境威胁和网络恶意攻击行为越来越多，传统的安全措施已经无法满足网络安全防御体系的需求。基于数据驱动的网络安全态势感知预测的研究和应用为提高网络安全主动防御能力提供了新方法。综合应用人工智能和机器学习等先进技术，基于数据驱动构建网络安全态势感知预测模型，提取、研究网络威胁特征，及时发现潜在网络威胁因素，预测安全风险发展趋势，能够为网络安全管理人员提供决策支持，建立起更安全的网络主动安全防御体系。

参考文献

[1] LIN Y L, HSIEH J G, WU H K. Three parameter sequential minimal optimization for support vector machines [J]. Neuro Computing, 2011, 72: 3467－3475.

[2] 朱坤莹. 网络安全态势感知及其应用实践研究 [J]. 软件, 2023, 44 (7): 157－159.

[3] 李泽慧, 徐沛东, 邬阳, 等. 基于大数据的网络安全态势感知平台应用研究 [J]. 计算机应用与软件, 2023, 40 (7): 337－341.

[4] HU J, MA D, LIU C, et al. Network security situation prediction based on MR-SVM [J]. IEEE Access, 2019, 7: 130937－130945.

[5] PESHAVE A, GANESAN A, OATES T. Predicting network threat events using HMM ensembles [C]//International Conference on Advanced Data Mining and Applications. Springer, 2022.

[6] 张婷婷. 机器学习支持下的网络安全态势感知分析 [J]. 信息与电脑, 2024, 36 (8): 198－200.

[7] 陈乾, 洪征, 司建鹏. 融合 SENet 和 Transformer 的应用层协议识别方法 [J]. 计算机科学与探索, 2024, 18 (3): 805－817.

[8] 杨莹, 郝晓燕, 于丹, 等. 面向图神经网络模型提取攻击的图数据生成方法 [J]. 计算机应用, 2024, 44 (8): 2483－2492.

[9] SARKER I H. CyberLearning: effectiveness analysis of machine learning security modeling to detect cyberanomalies and multiattacks [J]. Internet of Things, 2021, 14: 100393.

[10] LUNDBERG H, MOWLA N I, ABEDIN S F, et al. Experimental analysis of trustworthy in vehicle intrusion detection system using explainable artificial intelligence [J]. IEEE Access, 2022, 10: 102831.

[11] SARKER I H, COLMAN A, HAN J, et al. Context-aware machine learning and mobile data analytics: automated rule-based services with intelligent decision-making [M]. Cham, Switzerland: Springer, 2021.

（收稿日期：2025－04－09）

作者简介：

吴宝江（1979－），男，博士，高级工程师，主要研究方向：安全保密、体系总体设计、无线通信。

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