兰州理工大学

硕士论文

学校代号 10731　　学　　号 202085400105

分 类 号 TP393　　密　　级 公开

兰州理工大学

LANZHOU UNIVERSITY OF TECHNOLOGY

专业学位硕士学位论文

基于 SIG 和 HMM 的工业互联网安全态势预警技术研究

学位申请人姓名　赵映文

培 养 单 位　计算机与通信学院

导师姓名及职称　谢鹏寿 教授

学 科 专 业　计算机技术

研 究 方 向　网络与信息安全

论文提交时间　2023 年 3 月 20 日

学校代号：10731
学　　号：202085400105
密　　级：公　开

兰州理工大学硕士学位论文

基于 SIG 和 HMM 的工业互联网安全态势预警技术研究

学位申请人姓名：赵映文
导师姓名即职称：谢鹏寿教授
培　养　单　位：计算机与通信学院
专　业　名　称：计算机技术
论文提交时间：2023 年 03 月 20 日
论文答辩日期：2023 年 05 月 27 日
答辩委员会主席：刘宗礼　高级工程师

Research on Industrial Internet Security Situation Warning Technology based on SIG and HMM

by

ZHAO Yingwen

B.E. (Hubei University of Engineering) 2018

A thesis submitted in partial satisfaction of the

Requirements for the degree of

Master of Professional

in

Computer Technology

in the

School of Computer and Communication

of

Lanzhou University of Technology

Supervisor

Professor XIE Pengshou

May, 2023

目　录

摘　要

工业互联网已经成为了当今时代的重要基础设施。它在推动工业数字化、智能化、网络化的同时，所面临的安全问题越来越突出。本文在分析工业互联网安全的基础上，建立了基于统计信息网格的工业互联网安全态势预警模型，将态势提取和态势预警引入该模型，深入研究工业互联网安全保护方法，可以有效的避免工业互联网发生安全风险。具体研究内容如下：

1.针对现有的工业互联网安全态势预警模型在受到病毒攻击、网络攻击等手段的影响时，导致预警效果变差以及模型响应能力较差的问题，本文通过引入统计信息网格，建立一种基于统计信息网格的工业互联网安全态势预警模型，该模型引入统计信息网格，不仅解决了匹配滞后于攻击过程的问题，也使得误报率有所降低，增强了本预警模型的响应能力，更有利于预警及时准确的发布。

2. 为了克服传统态势提取方法对非线性的高维数据和多特征数据处理的局限，本文提出一种基于降噪自编码器和改进随机森林的工业互联网安全态势分析要素提取方法，以期获得更精准、更可靠的结果。首先利用降噪自编码器进行特征提取，然后对随机森林算法中的基分类器进行筛选，再采用加权多数投票的方式对原始随机森林算法进行改进，对降维后的数据进行分类训练从而得到最终分类结果。有效解决了传统态势分析要素提取不精准、提取效率不高的问题。

3. 为了解决现有的态势预警技术无法准确检测网络安全状况并且不能及时发现工业互联网潜在威胁的问题。本文首先建立了基于复合攻击的隐马尔可夫模型，然后基于该模型结合复合攻击判别和攻击意图识别等技术来预测入侵者下一次的攻击。该预警技术能够有效的发现和预警工业互联网安全态势变化。

实验结果显示，本文设计的工业互联网安全态势分析要素提取方法和态势预警技术在态势预警模型中，能够准确地将不同的网络攻击进行分类，能够为工业互联网系统争取安全防护的时间，并对外来入侵和攻击做出及时有效的反应，在攻击发生之前就能对攻击的数量和特点进行预测。该研究成果具有理论和现实意义，推动了工业互联网安全态势感知技术的发展。

关键词：工业互联网；安全风险；态势预警模型；态势分析要素提取 ；态势预警技术

Abstract

Industrial Internet has become a critical infrastructure in today's era. While it promotes the digitization, intelligence, and networking of industry, the security problems it faces are becoming more and more prominent. In this thesis, based on the analysis of industrial Internet security, an early warning model of industrial Internet security situation based on a statistical information grid is established, and posture extraction and posture early warning is introduced into this model to deeply study the industrial Internet security protection methods, which can effectively avoid the security risk of the industrial Internet. The specific research contents are as follows:

1.For the existing industrial Internet security situation early warning model when affected by virus attacks, network attacks, and other means, resulting in poor early warning effect and poor model responsiveness, this thesis establishes a piece of statistical information grid-based industrial Internet security situation, early warning model, by introducing a statistical information grid, which not only solves the problem of matching lags behind the attack process, but also makes the false alarm rate reduced, enhances the responsiveness of this early warning model, and is more conducive to the timely and accurate release of early warning.

2.To overcome the limitations of traditional situational extraction methods for processing multi-featured and high-dimensional nonlinear data, this thesis proposes an industrial Internet security situational analysis element extraction method based on noise reduction self-encoder and improved random forest, to obtain more accurate and reliable results. Firstly, the noise reduction self-encoder is used for feature extraction, then the base classifier in the random forest algorithm is filtered, then the original random forest algorithm is improved by using weighted majority voting, and the reduced dimensional data is trained for classification to obtain the final classification results. The problem of imprecise and inefficient extraction of traditional situational analysis elements is effectively solved.

3.To solve the problem that the existing situational warning techniques cannot accurately detect the network security situation and cannot detect the potential threats of the industrial Internet in time. This thesis first established a hidden Markov model based on compound attacks and then predict the next attack of intruders based on this model combined with techniques such as compound attack discrimination and attack intent identification. This early warning technique can effectively detect and warn of the change in the Industrial Internet security situation.

The experimental results show that the situational analysis element extraction method and situational warning technology in the situational and warning model designed in this thesis can

accurately classify different network attacks and predict the number and characteristics of attacks before they occur, to buy time for the security protection of industrial Internet systems and make effective responses to intrusions and attacks on time. The research results have theoretical and practical significance and promote the development of Industrial Internet security situational awareness technology.

Key Words: Industrial Internet; Security risk; Situational early warning model; Situational analysis element extraction; Situational warning technology

插图索引

附表索引

第 1 章 绪 论

1.1 研究背景及意义

工业互联网是将工业系统和互联网技术相结合的概念，是一种将全球工业技术和先进计算机技术、分析技术、传感器技术和网络技术等高度融合的新产品[1]。工业互联网突破了传统工业系统相对封闭的环境，将所有系统和生产设备与外部网络连接起来，并将其应用于新型工业生产系统和基础设施建设当中为世界上各个国家的经济增长和社会发展，带来了新的推动力[2]。

工业互联网未来发展空间广阔，但随之而来的是生产系统中的缺陷也暴露在互联网中。由于生产设备系统通常是连续的，而且使用时间较长，因此所产生的缺陷无法进行定期的维修和更新，就很容易受到网络的攻击，从而对企业的安全构成了越来越大的威胁。如果发生了安全事故，不但会造成巨大的经济损失，而且还会危及公众安全和公家安全[3]。委内瑞拉古里水电站核心计算机网络 2019 年 3 月遭恶意攻击，约 3000 万人受停电影响，经常有不同规模的网络安全事件发生，由此可见解决工业互联网安全问题急如星火。为了实现对工业互联网络安全状况的实时监测与预警，人们对新技术的需求日益强烈[4]。

在复杂多变的工业互联网环境中，尽管防火墙、入侵检测系统等一系列安全组件被部署在关键应用当中，但是这些技术在攻击发生之前都不会做出任何反应。而态势预警技术可以在入侵行为发生或者在入侵造成严重后果之前，预先采取相应的防护措施来加强工业互联网络的安全。因此要想解决这一问题工业互联网必须提供可用的、安全的态势预警模型[5]，因为传统的基于入侵事件的态势预警模型响应能力有限。同时对于在工业互联网环境下，传统态势分析要素提取方法不精确、效率不高等问题以及传统预警技术在检测和预测复合攻击方面不够及时不够准确的问题依然存在。

针对上述问题，本文研究了工业互联网在传统态势预警模型下存在的局限性，并且分析了工业互联网存在的安全风险，结合态势分析要素提取技术、态势预警技术，建立了基于统计信息网格的工业互联网安全态势预警模型，该模型引入了统计信息网格的态势分析方法，实时监控工业网络的恶意入侵行为，增强模型的异常检测能力。在上述模型下，提出了基于降噪自编码器和改进随

机森林的工业互联网安全态势分析要素提取方法以及基于隐马尔可夫模型的工业互联网安全态势预警技术。该成果不仅可以加强安防工作者对工业互联网安全状况的整体感知意识和应急反应能力，而且能够降低安全攻击的危害性，对于企业优质发展的重要推动力——工业互联网安全防护系统的发展具有十分重要的意义。

1.2 国内外研究现状

1.2.1 工业互联网安全态势预警模型研究现状

工业互联网安全态势预警模型对工业互联网信息系统建设具有非常重要的指导作用。国外对工业互联网安全态势预警模型的研究经历了很长一段时间并取得了一定的研究成果，特别是在电力和计算机领域。国外工业互联网安全态势预警模型在防范黑客入侵、保护工业互联网信息安全方面效果明显[6]；相比于国外，我国对工业互联网安全态势预警模型的研究相对较晚，尚未形成完整的预警体系。就国内工业互联网信息安全而言，它对保证工业网络的稳定运行和防止外部入侵具有重要作用。

王超[7]等人提出的基于大数据的安全态势预警模型，利用大数据技术和统计学方法，建立了一套可以对工业互联网安全态势进行实时预警的模型，解决了大数据安全态势模型的研究问题。为了增强信息安全预警的效果，张宁[8]等人提出了一种基于贝叶斯网络的信息安全预警模型，该模型不仅可以有效缩短网络信息数据识别时间，还可以有效地获得最佳适应度值，并最终评估信息安全性能。此外，针对网络安全态势预警模型，黄梁[9]等人提出了一种基于支持向量机的安全态势预警模型，并利用准确率、召回率、F1 值等指标对模型进行评价，实现了安全态势预警模型的评价指标体系。文献[10]中，Ming Yuh 等人提出了一种树模型，该模型使用攻击树来建模攻击意图并预测后续攻击。然而这种方法需要为各种攻击建立树模型，相对复杂，仅对短期网络安全形势预警有效，对长期网络安全形势的预警无能为力。文献[11]中，Herve Dcbar 等人提出了一种聚合和关联入侵报警信息的方法，以减少重复报警并提高报警效率，但实现长期网络安全状况预警也不容易。

文献[12]中，Mu 等人提出了一种安全事件融合和关联预警模型，以实现整个网络中安全事件的集中管理。基于攻击过程和时间参考的纵向事件关联方法

主要用于入侵的早期检测和防止预测的攻击阶段的传播。然而，实施起来很复杂，预警效果不好。

从上述文献中可以看出，网络安全态势预警模型在工业互联网等领域已经取得了一定的研究成果，但现有的工业互联网安全态势预警模型仍存在响应能力有限和误报率较高的问题。面对大量工业网络及主机安全事件，实时性难以满足，仍有大量的技术挑战需要解决。因此，需要建立一个安全的态势预警模型适用于工业互联网环境。

1.2.2 工业互联网安全态势要素提取方法研究现状

态势分析要素提取是整个态势感知的重要组成部分，是工业互联网安全态势感知的基础。整个工业互联网安全系统的性能将直接受到态势分析要素质量的影响。它的提取精确度会对整个工业网络安全保障系统的整体表现带来不可忽视的影响。态势分析要素提取的主要目的是将冗余的数据删除，将具有较高潜力的状况要素提取出来，为下一步的工业互联网安全态势分析提供数据基础并对其进行预警。

王宏彬[13]等人提出了一种基于模糊粗糙集和这组合分类器的态势要素提取方法。首先利用模糊粗糙集理论建立特征与态势要素之间的映射关系，得到模糊规则库。然后采用不同的分类器，来训练多个弱分类器，构建强分类器。最后通过组合分类器和模糊规则库进行分类得到态势要素。研究结果表明，基于模糊粗糙集和组合分类器的态势要素提取方法可以在小数据集和稀疏标注的情况下获得比较好的性能，具有较强的鲁棒性。

曹鲁喆[14]等人提出了一种结合 CNN 和 BiLSTM 的态势要素提取方法。首先利用 CNN 逐层提取数据的局部特征，并在数据包的空间维度上挖掘特征。再利用 BiLSTM 可以长期保留上下文历史信息的特点，提取数据在时间维度上的特征。最后用 Softmax 分类器对 BiLSTM 的输出进行分类。这种方法可以从时间和空间两方面对数据的时间和空间特征进行提取，而且能识别数据包之间隐藏的联系，从而提高了提取态势要素的效率。它解决了传统态势要素提取方法不能完全提取数据特征以及忽略数据包之间隐藏联系等问题。然而，由于数据属性特征的重要性不同，不能为不同的属性分配不同的权重以获得更好的分类结果。

Yongcheng Duan 等人提出了一种基于信息增益的随机森林提取方法[15-16]，

首先，信息增益决定了属性的重要性。在设定一个阈值后，多余的属性被减少和删除。其次，使用随机森林分类器对处理后的数据进行分类。该方法有效地提高了网络安全态势要素的提取精度，但随机森林中决策树的分类精度需要进一步提高。陶晓玲[17]等人在进行态势要素提取的过程当中，数据的有效特性被首先保留下来，同时输入数据维数、存储开销和计算资源也被降低。然而，由于神经网络的层数相对较多，层与层之间存在大量的非线性变换，导致特征信息在态势分析要素的提取过程中丢失。

从上述文献中可以看出，尽管国内外研究人员对网络安全态势要素提取方法进行了大量的研究，为本文的研究工作提供了大量的理论和技术支撑，但是当面对多特征、高维度的非线性数据时由于自身的局限性导致其处理能力有待进一步提升。因此，提出一种基于降噪自编码器和改进随机森林的态势分析要素提取方法对于工业互联网系统非常重要。

1.2.3 工业互联网安全态势预警技术研究现状

目前国内外很多专家为拥有更加准确的预警效果，开展了以下一系列相关研究工作。

Liu Chunju等人提出了一种基于定性微分博弈的实时网络安全威胁预警技术。基于定性微分博弈理论[18-19]，构建了网络攻防博弈模型，推导出安全威胁的动态变化趋势。在此基础上，引入多维欧氏距离度量不同安全状态下的威胁严重度。然后设计了一种预警算法，实现了网络安全威胁的实时预警，但该方法稳定性差。周先春等人提出了一种基于开源工具集的网络安全威胁实时预警方法。基于最新开源数据组件集，将一组采集数据、数据存储、离线分析、实时关联检测[20]、威胁预警等功能构建成一个有机整体，支撑安全事件处理的全过程，最终建立完整的网络安全态势感知与预警架构，实现网络安全威胁实时预警[21]。但在实际应用中，该方法在安全过程中应用较少，可行性较低。考虑到实时性和攻击规模，文献[22]提出了一种攻击预测算法，但该算法只能预测一些高级别、危害性较大的攻击事件。KuoAnKang等人提出了一种网络安全威胁实时预警方法，其依据是大数据[23]。首先提取网络安全基础数据，建立判断实时信息是否安全的网络风险信息识别模型，对提取的数据进行大数据分析。然后，建立用户行为操作序列，对的用户行为操作顺序进行实时信息的提取[24]。并且匹配分析用户库中描述的行为序列，输出匹配结果，判断用户的操作行为

是否存在威胁，根据匹配结果进行分析，但是这种方法有局限，安全性和稳定性不高。

从上述文献中可以看出，目前国内外对网络安全态势预警技术的研究相对较多，但在工业互联网领域，一种基于隐马尔可夫模型的工业互联网安全态势预警技术的提出至关重要，因为网络攻击的复杂性和多样性，态势预警技术在实现上存在一定的局限性。

1.3 存在的问题及分析

在工业互联网安全态势预警模型中，通过态势分析要素提取、态势预警等方案来维护工业互联网系统的安全性。然而，现有的工业互联网安全态势预警模型仍然存在响应能力有限的问题；在受到病毒攻击、网络攻击等手段的影响时，导致预警效果变差的问题。针对现有工业互联网安全态势预警模型在预警效果上的不足，针对现有预警技术中的预测方法依赖网络攻击模型而无法预警长期安全态势的问题，提出一种适用于工业互联网环境的安全态势预警模型。

态势要素提取方法的研究已经比较成熟，目前存在的很多态势要素提取方法在对特征较多，维度较高的非线性数据处理能力上存在一定的局限性。由于神经网络的层数相对较多，并且在层与层之间存在的大量的非线性变换，导致特征信息在态势分析要素提取过程当中造成了特征信息的丢失。因此，本文在第四章，引入了降噪自编码器的概念，提出了一种工业互联网安全态势分析要素提取方法，该方法基于降噪自编码器，并对随机森林进行了改进，使态势分析要素提取的结果更加准确。

由于网络攻击的复杂性导致现有的态势预警技术在根据复合攻击的部分报警信息来预测攻击存在一定的困难。例如，从报警信息序列中无法很好地发现其对应的攻击场景，在发现报警信息对应的复合攻击场景后，对其隐含的攻击意图序列也无法很好地发现。因此，本文利用隐马尔可夫模型的概念，在其基础之上结合复合攻击判别技术和攻击意图识别技术来进行下一步攻击预测，实现工业互联网安全态势预警。

1.4 论文的主要研究内容及创新点

论文主要对工业互联网安全态势预警模型、态势分析要素提取方法以及态势预警技术三个方面进行了研究，并且分析了其在工业互联网领域存在的问题

和不足，针对上述问题，本文开展了以下研究工作：

1. 建立了基于统计信息网格的工业互联网安全态势预警模型。

为了解决在受到病毒攻击、网络攻击等手段的影响时，预警模型的预警效果变差的问题。本文建立了一种基于统计信息网格的工业互联网安全态势预警模型，该模型引入了聚类分析方法，实时监控工业互联网系统的异常行为，增加了异常监测能力，不仅可以提高态势分析要素提取方法的准确性，而且还可以实现态势预警技术的时效性。

2.提出了基于降噪自编码器和改进随机森林的工业互联网安全态势分析要素提取方法。

为了解决态势分析要素提取过程中，特征信息的损失问题。本文提出了一种基于降噪自编码器和改进随机森林的工业互联网安全态势分析要素提取方法。通过分析工业互联网的安全状况，建立了工业互联网安全态势分析要素提取模型，利用降噪自编码器增强对大量数据的特征学习能力，有效选择重要属性删除冗余属性。然后通过对随机森林算法中基分类器的选择等方面进行改进，提高整体的分类精度，有效提高了工业互联网态势分析要素提取方法的准确性。

3.提出了基于隐马尔可夫模型的工业互联网安全态势预警技术。

为了解决传统网络安全态势预警技术不能准确检测和预测复合攻击的问题。提出了基于隐马尔可夫模型的工业互联网安全态势预警技术，它将复合攻击辨别和攻击意图识别等技术与隐马尔可夫模型相结合。警报技术使用前馈算法来计算复合攻击的隐马尔可夫模型产生警报信息的概率，然后使用增强的维特比算法来识别入侵者的攻击意图。最后，两者结合起来，预测入侵者的下一次攻击，提高了预警的准确率，对于工业互联网安全态势预警技术的研究具有重要的理论贡献。

1.5 论文组织结构与安排

针对工业互联网领域存在的安全问题，主要从三个方面进行研究，即建立基于统计信息网格的工业互联网安全态势预警模型、提出基于降噪自编码器结合改进随机森林的工业互联网安全态势分析要素提取方法以及提出基于隐马尔可夫模型的工业互联网安全态势预警技术。本文主要包含五个章节，内容如下：

第 1 章 绪论。本章首先对工业互联网的研究背景进行了简要的描述，然后对传统的态势预警模型、态势分析要素提取方法还有态势预警技术的国内外研

究现状，进行了总结和分析，同时还阐述了这三个方面的研究内容在动态多变的工业互联网环境中存在的问题以及不足，最后对本文的研究内容和创新性进行了简单概述。

第 2 章 相关理论知识。本章首先简单介绍了工业互联网和传统互联网的区别，接着介绍了态势要素提取方法中用到的相关算法，最后介绍了态势预警技术、隐马尔可夫模型等相关理论知识。

第 3 章 基于统计信息网格的工业互联网安全态势预警模型。本章首先介绍了传统的态势预警模型在工业互联网环境下的局限性，然后在表格中总结了三种传统态势预警模型的优缺点，接下来介绍了基于统计信息网格的工业互联网安全态势预警模型及其几个主要组成部分，最后简单介绍了工业互联网安全态势分析部分的主要内容。

第 4 章 基于降噪自编码器结合改进随机森林的工业互联网安全态势分析要素提取方法。本章首先对工业互联网安全态势分析要素提取进行系统建模，然后设计了一种基于降噪自编码器和改进随机森林的态势分析要素提取方法，最后分别从不同层次降噪自编码器结构的特征提取性能、不同态势分析要素提取方法的分类效果及不同提取方法对攻击类型提取效率这三个方面进行算法性能分析。

第 5 章 基于隐马尔可夫模型的工业互联网安全态势预警技术。本章主要介绍了基于隐马尔可夫模型的工业互联网安全态势预警技术。首先，把复合攻击和隐马尔可夫模型相结合建立一种基于复合攻击的隐马尔可夫模型，该模型主要由报警信息层、攻击意图状态层这两部分组成，他们分别研究了三部分预测算法:识别复合攻击，识别攻击意图和预测攻击。其中，攻击预测将前向算法和改进的维特比算法有机的结合在一起来预测下一步可能进行的攻击。最后，通过实验进行验证和分析。

总结与展望。本章首先总结了工业互联网安全态势预警模型、态势要素提取方法和态势预警技术的主要工作内容，然后对当前阶段存在的不足简单进行了介绍，最后为下一步研究工作制定了计划。

第 2 章 相关理论知识

2.1 工业互联网与传统互联网的区别

工业互联网[25](Industrial Internet)是指工业互联的网络，是连接人、数据和机器，它能够连接和整合工业生产过程当中的所有元素，从而推动整个行业的发展。传统互联网主要就是指互联网网络，适用于各行各业，具有实时传播效率较高的特点。但是由于工业互联网的飞速发展，而其又有相当复杂的网络结构因此与传统的工业互联网系统有着很大不同。具体的不同主要有以下三点：

(1)它们所连接的物体是不一样的。传统互联网通过电脑和手机等数字产品连接普通消费者，而工业互联网则是通过大数据、物联网和人工智能等新兴技术力量连接工厂和工业生产中的人、机器和物体，通过连接来协调生产中各个环节的运作。

(2)它们连线的量级不可同日而语。传统互联网连接的是数以十亿计的人，而工业互联网连接的是数以百亿计的生产装置。

(3)它们对网络实时响应的要求是不同的。我们在互联网上往往会有一些延迟，但不会对我们造成太大影响，所以对网络的实时响应要求不高，而工业互联网需要实时响应，以确保生产线上的工作不间断，有时甚至达到毫秒级别。

2.2 深度神经网络

神经网络主要由两部分组成：传统神经网络和深度神经网络。在传统神经网络中，通常使用 BP 算法使神经网络模型从大量样本数据中学习规则。神经网络具有很强的非线性建模能力和自适应学习能力。深度神经网络也称为深度学习。在互联网安全工业要素的提取中，基于 BP 神经网络的许多研究得到了改进，在一定程度上提高了提取性能[26]。

神经网络主要研究的是输入数据的隐藏信息。主要是为了达到信息处理的目的，它透过调整内部神经元间的连结权重来归类后期输入的数据。神经网络是由若干个神经元组成的，它是处理神经网络数据的基本单位。所有的神经元都能够收到其他神经元从不同层发出的输出作为输入，并给予其权重。神经网络要提高辨识的精准度，需要大量的训练和重新调制。神经元的结构模型如图

2.1 所示。

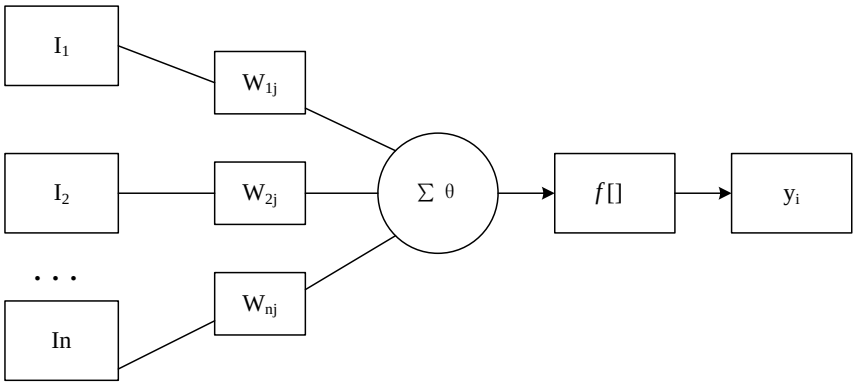


图 2.1 神经元结构模型

在图 2.1 中，$I_1,I_2,\cdots,I_n$表示不同神经元的输入，$W_{1j},W_{2j},\cdots,W_{nj}$表示不同神经元节点间的连接权值，权值不同就表明其对神经元节点的影响也不同。$\sum\theta$表示对神经元阈值进行求和运算。$f[\ ]$是激活函数，O_i是神经元的输出。其中$f[\bullet]$的运算过程如下。

$$v_i=\sum_{j=1}^{n}I_iW_{ij} \tag{2.1}$$

$$u_i=v_i+\theta_i \tag{2.2}$$

$$O_i=f[u_i] \tag{2.3}$$

首先利用公式(2.1)对神经元中不同的输入结果进行求和，其次再根据公式(2.2)中的u_i值来判断神经元是否被激活，最后利用公式(2.3)中的激活函数对神经元进行输出。

在神经网络中，一个神经元的相邻节点的输入和输出之间的关系被称为激活函数。激活函数的作用是保留神经元的特性并将其映射到整个函数中，即将神经元的输入映射到输出。神经网络中使用的激活函数也因所需的结构和层次类型而不同。最常用的激活函数是 sigmoid 函数、Relu 函数和 tanh 函数。sigmoid 函数主要用于将拟合曲线的最终结果转换为隐藏层（0,1）区间内的神经元输出。较大负数在 0 附近无限接近，较大正数在 1 附近无限接近。这样，0 和 1 就可以代表不同的档次分类结果了。其公式如下所示。

$$sig(x)=\frac{1}{e^{-x}+1} \tag{2.4}$$

其中x代表神经元的输入。

因为传统的神经网络在态势感知上的应用有很大的局限性，比如 BP 算法，它是梯度递减的算法，递减的速度比较快，这样就很容易把它引到一个局部最小值的问题上去，所以大家在态势感知的研究上就开始逐步的应用深度学习。

深度学习又被称为深度神经网络，是神经网络的进一步发展。传统神经网络一般有 1 至 2 层的隐藏层，而深层神经网络则有 2 层以上甚至更多的隐含层数[27-28]。深度学习是一种通过采用多层次分析和计算的方式来学习数据内在规律和用来表示层次最后得到输出结果的方法。

与传统的神经网络不同，深度学习使用的是分层结构，包括一个输入层、几个隐藏层和一个输出层。相邻层的节点之间的连接方式与传统神经网络的分层结构类似，但同一层的节点之间和不同层节点之间的连接方式则不同。传统的神经网络是通过一个迭代算法来训练的，该算法计算网络的当前输出，在随机设置初始值后，最终修改参数，直到收敛，主要是基于当前输出和标签之间的误差。

深度学习整体采用层层训练机制，其训练过程包括自下而上的无监督学习和自上而下的监督学习，从而避免了梯度扩散问题的出现。其中由下往上的训练，即由下往上逐层展开，再对各层参数进行分层训练，直至最上面一层，此过程采用无监督训练。而自上而下的监督学习，每一层的参数都是由上往下经过监督训练后得出的。这个过程不像传统的神经网络，在设定初始化值时不是随机的，而是透过输入数据的结构来获得整体上最优的初始化值，从而获得较佳的效果[29]。

2.3 随机森林算法

随机森林(Random Forest, RF)是一种基于统计学的算法，RF 有两个研究方向，一个以组合分类为研究方向，另一个以回归分析为研究方向。它通过集成多个决策树的分类或回归结果来提高模型的准确度和泛化能力。其中，“随机”指的是在构建多个决策树的过程中引入了随机性，以避免过拟合现象的发生[30]。相比于单个决策树，随机森林的优势在于可以处理高维数据，不需要进行特征选择、而且它是一种非常稳定的算法，能够有效地避免过拟合现象的发生、它还能够处理缺失值和异常值等问题，具有较强的鲁棒性。

为了详细介绍随机森林的算法思想，我们首先介绍一下超平面的概念。如图 2.2 所示，该样本数据集包括四种不同类型的样本，已知该数据集是线性可分割的。从图中可以看出超平面可以分割这四种不同类型的样本，分割后的数据集一定是在不相交的区域。在原始样本空间中不同类型的样本会因为每次超平面的使用被分割成两部分，而随机森林算法生成超平面的过程类似于生成二

叉树。这种使用超平面来划分原始样本空间的方法，在随机森林算法中被称为决策树。决策树如图 2.2(a)所示，分割后的数据空间如图 2.2(b)所示。

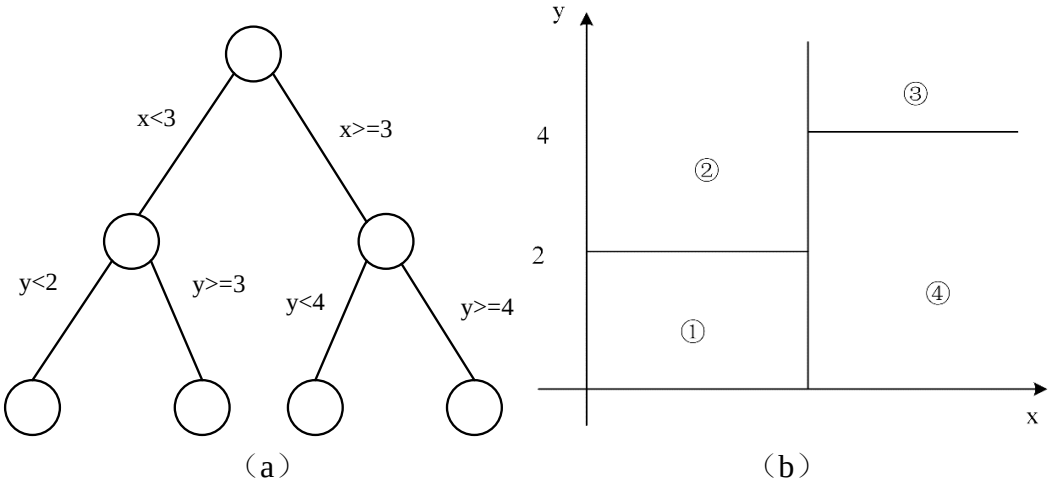


图 2.2 随机森林决策树

随机森林理论的原理是单个子分类器属于弱分类器，弱分类器的分类容易出错，而多个子分类器组成强分类器，强分类器中的子分类器相互补充可以减少误差，各子分类器之间不同特征的相互作用可以提高准确性。随机森林是一种优秀的非线性分类器，对于二分法分类和多分类等问题有较好的分类效果。大量的理论和实例表明，随机森林的分类精度非常高，而且受噪声的影响较小。

2.4 隐马尔可夫模型

隐马尔可夫模型(Hidden Markov Model, HMM)主要是用来描述随机过程统计的概率模型 [31]。主要由描述状态转移的基本随机过程和描述状态与观察值的统计关系的两个随机过程组成。观察者除了看到它的观察值外，不能直接看到它的状态。因此，观察者可以通过外部观察序列感知到内部状态的存在及其属性，当马尔可夫的状态隐藏在内部时。Markov 过程是隐藏 Markov 模型的基础，首先介绍 Markov 链条，以便更好的了解隐藏的 Markov 模型。

马尔可夫链是随机马尔可夫过程的一个特例，即马尔可夫链是一个具有离散状态和时间参数的马尔可夫过程，它的数学描述如下所示：随机序列 X_n，在任意时刻 n，它所处的状态在 $S=\{S_1,\cdots,S_N\}$ 范围之中，所对应的状态序列是 $\{q_1,\cdots,q_n\}$，时刻 t 模型处于某一个状态 $X_t=q_t$，且它在 $m+k$ 时刻所处的状态是 q_{m+k}，其所处状态的决定因素仅仅与它在时刻 m 的状态 q_m 相关，而与 m 时刻之前它所处的状态无关。概率的表示形式如下：

$p\left[S_{m+i}=q_{m+k}\middle|S_m=q_m,S_{m-1}=q_{m-1},\cdots,S_1=q_1\right]=p\left[S_{m+k}=q_{m+k}\middle|S_m=q_m\right]$，其中，$q_i\in\{S_1,\cdots,S_N\}$，于是把 X_n 称为马尔可夫链，马尔可夫链的 k 步转移概率能够表示为 $p_{ij}[m,m+k]=p\left[q_{m+k}=Z_j\middle|q_m=Z_i\right]$ $1\le i,j\le T$。当 $p_{ij}[m,m+k]$ 与 m 没有关系时就把这个马尔可夫链称作奇次马尔可夫链，则有 $p_{ij}[m,m+k]=p_{ij}[k]$。如果 $k=1$ 时，$p_{ij}[1]$ 称作是一步转移概率，简称为转移概率，记作 a_{ij}。所有的状态转移概率可以构成一个状态转移矩阵 A：

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix}$$

其中，$0\le a_{ij}\le 1$，$\sum_{j=1}^{N}a_{ij}=1$。因为 $p_{ij}[k]$ 可以通过转移概率 a_{ij} 得到，所以状态转移矩阵 A 可以作为描述马尔科夫链的重要参数，但是，要是想完全描述马尔科夫链，还需要引入初始概率向量 $p=(p_1,p_2,\cdots,p_N)$，其中 $p_i=p[q_i=S_i]$，$i=1,2,\cdots,N$。显然有：$0\le p_i\le 1$，$\sum_{i=1}^{N}p_i=1$。

马尔可夫链中观察值与其所处的状态是相对应的，也就是说由观察值可以直接知道此时所处的状态。而在马尔可夫模型当中不是如此，观察者只能通过随机过程来实现其状态的感知，也就是说在观察值序列已知的前提下，要想知道实际的状态序列，只能根据其观察值的分布情况、状态初始概率、状态转移概率来推断。

定义 2.1.1 隐马尔可夫模型（HMM）具有下列元素及含义。

1.有限个状态，用集合 S 表示，且 $S=\{S_1,S_2,\cdots,S_N\}$。在 t 时刻的状态为 q_t，状态是被隐藏的信息。

2.在不同的状态下，状态以概率的形式表现不同的观察值，用集合 O，$O=\{O_1,O_2,\cdots,O_T\}$,观察值相当于状态的产生值。

3.状态之间以概率的形式转换，称为状态转换概率，定义为 $a_{ij}=p\left[q_{t+1}=S_j\middle|q_t=S_i\right]$，$1\le i,j\le N$，$A$ 表示状态转换矩阵。

4.观察值由所属的状态以不同的概率产生，称为观察值产生概率，定义为 $b_j(k)=p\left[O_k\middle|q_t=S_j\right]$，其中，$1\le j\le N,1\le k\le T$。状态和观察值间的关系，用观察值产生概率矩阵 B 来表示。

5.在时刻 $t=1$ 时，每个状态不同的初始概率，定义为 $\pi_i=p[q_1=S_i]$，$1\le i\le N$，初始状态概率向量，用集合 π 表示。

一个完整的隐马尔可夫模型(HMM)包含了以上 5 个要素，为了使用方便，

可以用 $\lambda=(A,B,\pi)$ 来表示一个完整的隐马尔可夫模型[32]。隐马尔可夫模型的研究对象是称为观察值的每一个序列的数据。隐马尔可夫模型认为另一个表示一系列状态的序列隐藏在该序列背后，每个观察值发生在某种状态，由概率模型规定观察值和状态的变化，但在观察值背后隐藏着观察不到的状态序列。

2.5 统计信息网格聚类算法

统计信息网格（Statistical Information Grid, SIG）是一种基于网格的聚类算法[40]，该算法的主要思想是将数据集划分为若干个网格，然后在每个网格内进行聚类操作最终得到所有网格的聚类结果。 该算法的优点是可以处理大规模数据集，同时可以有效地处理噪声数据和异常值。此外，该算法还可以自适应地调整网格大小，以适应不同的数据分布情况。 统计信息网格聚类算法的基本步骤如下：

1.将数据集划分为若干个网格，每个网格的大小可以根据数据集的特点进行调整。

2.在每个网格内进行聚类操作，可以使用任何一种聚类算法，如 K-means 算法、层次聚类算法等。

3. 将每个网格的聚类结果合并，得到整个数据集的聚类结果。

4.对于噪声数据和异常值，可以将其分配到最近的网格中进行处理。

总之，统计信息网格聚类算法是一种简单而有效的聚类算法，它可以处理大规模数据集，并且可以自适应地调整网格大小，以适应不同的数据分布情况。该算法在实际应用中具有广泛的应用前景。

2.6 复合攻击

复合攻击是一种综合利用多种攻击手段的攻击方式，其理论和技术涉及多个领域，包括网络安全、信息安全、计算机科学等。在网络安全理论方面，网络安全理论是复合攻击的基础，包括网络攻击、网络防御、网络安全策略等方面的理论。网络安全理论的研究可以帮助防御者更好地理解攻击者的攻击手段和攻击方式，从而采取更有效的防御措施。在信息安全技术方面，信息安全技术是复合攻击的重要组成部分，包括加密技术、身份认证技术、访问控制技术等。这些技术可以帮助防御者保护敏感信息，防止攻击者获取敏感信息。在计

算机科学技术方面，计算机科学技术是复合攻击的基础，包括操作系统、网络协议、编程语言等方面的技术。攻击者可以利用这些技术来攻击受害者的系统，防御者需要了解这些技术，从而采取相应的防御措施。在人工智能技术方面，人工智能技术在复合攻击中也扮演着重要的角色，包括机器学习、深度学习、自然语言处理等方面的技术。攻击者可以利用这些技术来进行更加智能化的攻击，防御者需要利用这些技术来提高防御的智能化程度。 综上所述，复合攻击涉及多个领域的理论和技术，防御者需要综合考虑各种攻击手段，采取多层次的防御措施，才能有效地防范复合攻击。

2.7 本章小结

本章首先对工业互联网系统与传统互联网系统的区别进行了简单的介绍，其主要目的是为了加深对工业互联网相关知识的了解，为后面论文的开展奠定基础；然后，对工业互联网安全态势预警模型、工业互联网安全态势要素提取方法以及工业互联网安全态势预警技术中要用到的相关理论知识进行了介绍。

第 3 章 基于 SIG 的工业互联网安全态势预警模型

3.1 引言

随着工业互联网技术的迅速发展，工业互联网面临着诸多挑战，其中安全被认为是最困难的挑战之一。因为工业互联网系统的动态性和异构性的特点，使得这个问题变得更为复杂，工业互联网安全态势预警模型对工业互联网系统的建设有着举足轻重的作用。为了解决传统预警模型响应差预警效果不够好的问题，需要建立一个安全的工业互联网安全态势预警模型适用于工业互联网环境。基于 SIG 的工业互联网安全态势预警模型是一种应对工业互联网安全威胁的重要手段。该模型基于大数据分析和机器学习技术，利用各种数据源（如设备数据、网络数据、应用程序数据等）进行实时监测和分析，以提前发现并预警潜在的安全风险。

3.2 传统的态势预警模型在工业互联网环境下的局限性

3.2.1 基于工业流量监控的态势预警模型

传统的基于工业流量监控的态势预警模型 [33]的预警过程大致可分为以下四个步骤：首先，利用数据收集设备将目前通过工业网络的所有流数据收集起来，存储到缓存当中，并以特定格式发送到指定的服务器。然后，一般情况下，工业网络的流量变化是平滑的、规律性较强的。可用简单的线性或指标走势图来构造。我们可以在某一时间区间内，对网络流量值进行一次采集，再取历史流度值的前 M 倍以内的值作为观测序列。这样，工业网络流量的预测值 f_{m+1} 就可以根据某种方法在下一时刻得出。所以在每一个相同的时间区间可以得到工业网络流量在当前时间的真实值和工业网络流量在下一个时间的估计值。最终工业网流量状况形成了工业网流量真实值序列 $x_1, x_2, \cdots, x_m$ 和工业网流量估计值序列 $f_2, f_3, \cdots, f_{m+1}$ 两个随时间变化的序列。其次，从工业网络中发现异常入侵方式，通过对采集到的工业网络流量数据进行分析，识别出该方式。再通过观测工业网络流量测量值的调整程度和预测值，并作出是否预警的反应，以此来判断当前工业网络流量是否正常。最后，如果出现类似波峰、波谷这种工业网络流量

异常的情况。这一异常状况将在未来一段时间内影响工业网络流量的预测，波峰会造成预测结果偏高于真实结果，而波谷会造成预测结果偏低于正常结果。最后利用模式识别的方法来判断和分析该异常情况是否属于入侵信息，若属于入侵信息，则发出报警，若不属于入侵信息，则进行系统调整。如图 3.1 所示为基于工业流量监控的预警模型。

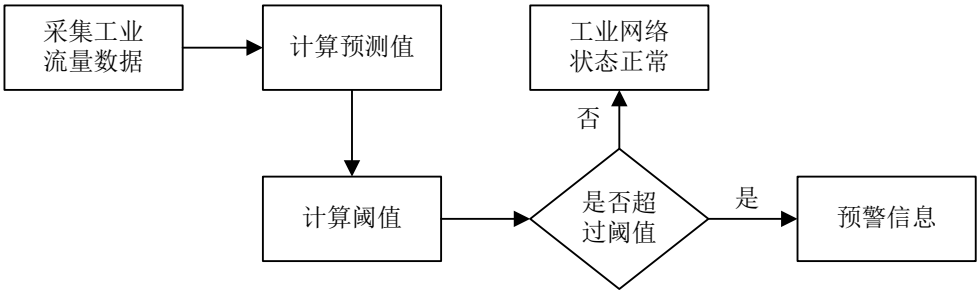


图 3.1 基于工业流量监控的态势预警模型

在对工业网络流量监控数据进行分析时，采用时间序列分析的方法，该方法采用的是选择合适的数学模型分别对应给定的时间序列[34]。

常用的数学模型表示如公式（3.1）所示：

$$v_t = f(v_{t-1}, v_{t-2}, \cdots, v_{t-m}) \tag{3.1}$$

其中，f 表示选定的函数，v_t 表示预测值，$v_{t-1}, v_{t-2}, \cdots, v_{t-m}$ 表示按时间顺序进行排列的参数。

假设工业流量观测序列可以表示为 $x_1, x_2, \cdots, x_t, \cdots, x_{t-m+1}$，取正整数 $m < T$，工业网络流量的变化状况会随着时间 t 的推移而得到一系列数据。$m+1$ 观测值是利用 m 连续观测值的平均值来预测的。

$$F_{t+1} = \frac{1}{m}(x_t + x_{t-1} + \cdots x_{t-n+1}) \tag{3.2}$$

由公式（3.2）得到的 F_{t+1} 就可作为 x_{t+1} 的预测值，其预测的误差可以表示为：$e_{t+1} = x_{t+1} - F_{t+1}$。假设工业网络流量历史观测序列可以表示为 $x_1, x_2, \cdots, x_t, \cdots, x_T$，取正整数 $m < T$，则工业网络流量实际测量值和预测值之间的调整偏离度的计算如公式（3.3）可表示为：

$$D_t = \sqrt{\frac{1}{m}\sum_{t=0}^{m-1}(x_{t-1} - F_{t-1})^2} \tag{3.3}$$

此时，工业互联网系统可以利用工业网络目前所收集到的流量数值与预测值的偏差与计算出 D_t 的关系，从而确定预警等级信息。当该模型应用在工业互联网环境中时，会有以下问题出现：预警效率不高，时间较长；实现过程比较

复杂，而且无响应。

3.2.2 基于攻击过程的态势预警模型

基于攻击过程的态势预警模型可以基于相关分析方法，将这些入侵序列与已知的入侵序列进行比较，以接收来自实时检测设备的原始预警数据，并比较下一个攻击步骤或即将发生的攻击事件，形成一个入侵序列的预警数据。这个模型是在相关处理技术中使用预警数据的延伸[35]。一个基于攻击过程的态势预警模型如图 3.2 所示。

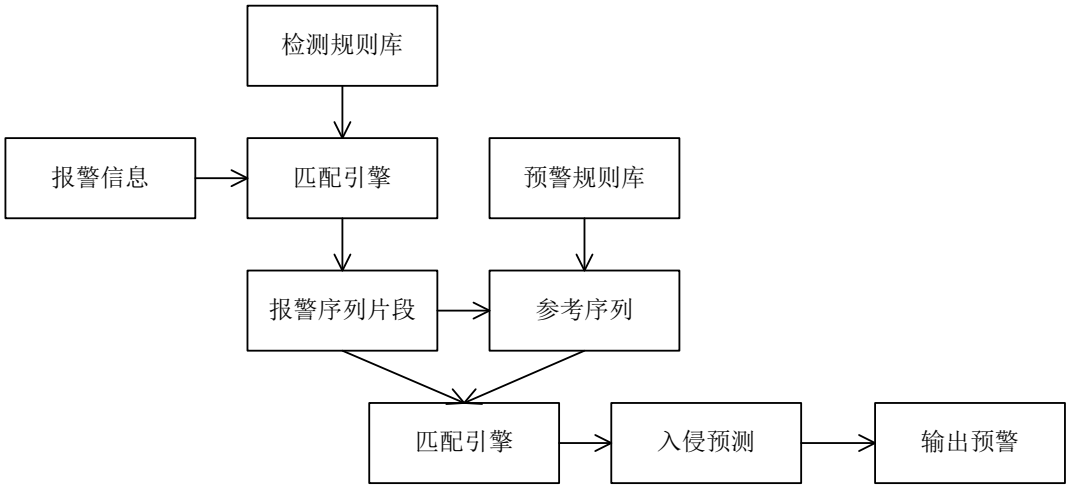


图 3.2 基于攻击过程的态势预警模型

工业互联网系统在对同一主机进行攻击过程预警的步骤如下：首先动态建立被攻击的主机链表，并将其作为链表节点的主键，其 IP 地址作为唯一标识。链表节点的结构主要由以下三个域构成：被攻击主机的 IP 地址；攻击序列 $(Matchstring)$；下一个节点指向。

在收到第一个预警数据包后，工业互联网系统为这个 IP 地址建立了第一个表结点，并在被攻击的主机链表中加入了这个表结点。对于后期接收到的预警数据包，工业互联网系统首先要做的是提取 IP 地址，然后将主机链表遍历一遍，如果这个 IP 地址对应的节点不存在，那么系统将会重新创建一个新的结点，并在 *Matchstring* 字段中写入预警信息；这个 IP 地址如果有对应节点，接下来就直接进入下一步；然后给正在被攻击的主机生成一个攻击序列 Match string；再将上一步生成的攻击序列 Match string 与预警规则库中的规则链表进行逐项匹配；最后进行预警。如果这个节点的攻击序列 Match string 字段与预警规则库中规则链表上的任意一个规则相匹配，这就表明工业互联网系统已经发现了预先定义的入侵，此时系统就会立即采用工业互联网安全策略规定的方式向安全管理人

员发出预警。

这种预警模型目前在应用领域已经相当广泛，但在应用到工业互联网环境中还存在以下不足：

1. 最终匹配的都是一些较短的序列，因为原始预警数据是按照一定的次序获得的。

2. 更多可能的匹配结果可能会随着后续相关预警数据的陆续到来而出现在与数列集合比较的过程中，这样才能逐步获得与之相匹配的完整进攻进程。若等到匹配完成后，攻击过程已经结束，此时预测就失去了意义。

3. 只能建立在已知攻击基础之上，响应能力差。

3.2.3 基于入侵事件的态势预警模型

基于工业网络入侵事件的安全态势预警模型，其主要目的是为了在安全人员采取相应防护措施的情况下，对其进行预警，直到实际发生工业网络入侵事件，最后即时反应，减少误报率[36]。

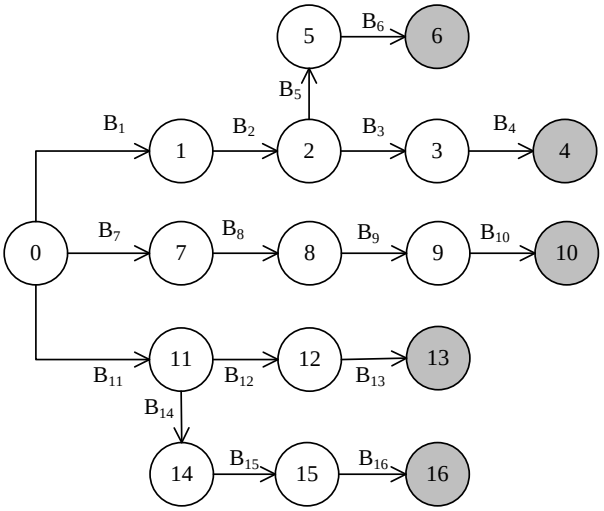


图 3.3 基于入侵事件的安全态势预警模型

在工业互联网系统中，大多数网络入侵的攻击行为都是有明确计划、分具体步骤来进行实施的，假设把入侵行为的每一个具体步骤分别对应一个相应的安全事件，不妨用函数 $B_i=(B_{i1},B_{i2},\cdots,B_{ij},\cdots,B_{im})(j=1,2,\cdots,m)$ 来表示，其中 B 代表一个相应的安全事件。把所有入侵攻击行为对应的安全事件序列结合在一起形成一个安全态势预警模型，基于入侵事件的安全态势预警模型结构如图 3.3 所示，其中白色圆圈代表工业互联网系统的安全状态，箭头代表的是安全事件，灰色圆圈代表的是一个入侵行为攻击过程的结束，假设模型中状态 0 代表工业

互联网系统的初始状态，往下以此类推，每个事件到达灰色圆圈代表一个完整的入侵行为的攻击过程的结束。

基于上述入侵事件的安全态势预警模型，我们可以针对已有的入侵行为进行阐述。在分析攻击事件序列时，不仅能检测到正在发生的入侵攻击行为，还能预测到入侵攻击行为在未来是否可能会发生。当攻击行为到达某一状态时，入侵状态追踪就可以实现，侦测其对应的全部输出状态。例如当入侵状态到达状态 11 时，之后可能会进入到状态 12 或者状态 14 这两个状态，进而最终到达状态 13 或者状态 16，所以当入侵行为到达 11 时，为了对以后的状态进行预测，我们要选取安全事件 B_{12} 和安全事件 B_{14} 对其进行入侵过程的追踪，进而提前对最后可能出现的状态进行预测。该模型应用于工业互联网环境中时，明显的存在以下几个缺点：

1. 在预警的实时性方面，该模型在面对工业互联网中大量主机安全事件，实时性很难满足；

2. 在预警的误报率方面，工业互联网系统不能从海量的报警事件中判断出真正的入侵事件；

3.在响应能力方面，安全管理人员在分析报告和采取防护行动的这段事件间隔内，给攻击者留下了一段可能随意攻击时间间隔。

3.3 基于 SIG 的工业互联网安全态势预警模型

目前的工业互联网安全态势预警主要是针对特定的攻击类型，仅作短期趋势预测，通过对上一节中常见的网络安全态势预警模型在工业互联网环境中的局限性的研究，了解到此类预警模型不具备适应性。响应能力有限[37]。因此本章提出了一种基于统计信息网格的工业互联网安全态势预警模型，该模型不但可以适用于不同的攻击类型，而且可以对工业互联网安全报警事件进行长期的安全态势预警，而且在预警技术的选择上，采用具有响应能力的算法，可以有效提高算法的时效性和预警的准确率。因为它采用了基于 SIG 和 HMM 方法，不但解决了传统预警模型在预警效果上的不足，与此同时，由于两种算法的使用还解决了基于攻击过程的安全态势预警模型中出现的匹配过程滞后于攻击过程的普遍性问题。基于 SIG 的工业互联网安全态势预警模型如图 3.4 所示。上述态势预警模型主要有四个模块，态势分析要素提取模块、态势分析模块、预警模块以及态势可视化模块。

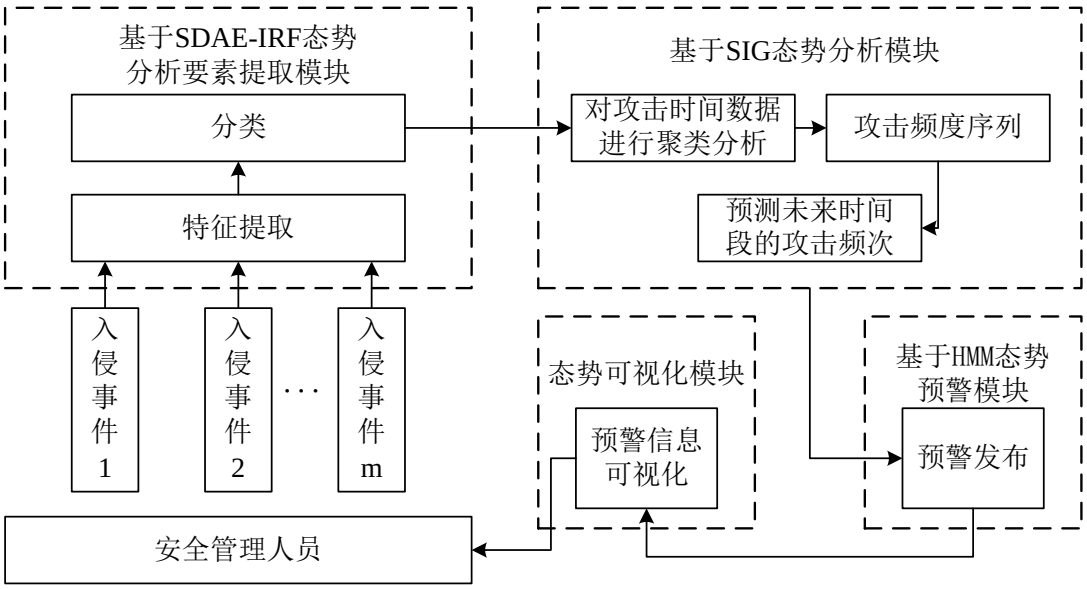


图 3.4 基于 SIG 的工业互联网安全态势预警模型

其中，态势要素提取模块以及预警模块是该预警模型的主要内容，态势要素提取是进行大规模工业互联网安全态势感知的重要前提和基础。而预警技术可以及时预测攻击态势，监测工业互联网各网络节点网络流量的实时变化情况。在态势分析模块，基于 SIG 的态势分析方法可以在遇到空间复杂度较大的问题时将其非常快地解决。然而，在态势预警模块中，基于 HMM 的预警技术使其反应能力得到加强，有利于预警更准确、更及时的发布，实现态势预警技术的及时性，从而轻松解决了工业互联网安全态势预警模型检测预测复合攻击困难的难题。

该工业互联网安全态势预警模型的主要工作流程可以描述为：

(1)由报警事件收集器收集来自入侵检测系统、防火墙以及工业网络安全实时监控系统等报警日志的报警事件；

(2)对不同格式的报警事件进行特征提取，提取出统一的、适于聚类分析的报警事件；由于不同安全设备的报警日志各不相同，对异构事件进行统一处理是进行下一步分析的前提和要求；

(3)采用基于 SIG 的聚类方法，对上一步提取出的攻击时间数据进行聚类分析，取得攻击频度值序列；

(4)根据入侵事件的频度值序列，采用 HMM 预测算法预测未来时间段的攻击频次；

(5)根据预测结果进行预警。

采用基于 SIG 的工业互联网安全态势预警模型与上述传统预警模型在进行

工业网络信息数据识别的完成时间测试，工业互联网信息数据识别的完成时间将直接影响工业互联网安全态势预警的及时性，测试结果如表 3.1 所示。

表 3.1 工业互联网信息数据识别的完成时间测试结果

实验次数	工业互联网信息数据识别的完成时间/s			
	文献[33]	文献[35]	文献[36]	本章预警模型
1	3.40	3.31	3.26	2.15
2	3.42	3.29	3.27	2.17
3	3.33	3.25	3.19	2.08
4	3.35	3.23	3.18	2.18
5	3.38	3.22	3.21	2.11

由表 3.1 的结果可以看出，基于 SIG 的工业互联网安全态势预警模型与其他三种传统态势预警模型相比，工业网络信息数据识别完成时间最短，这是因为该模型在识别工业网络信息的过程中，由于先自适应分类处理了信息数据样本，使得工业网络信息数据非常容易被识别，提高了网络信息数据的识别速度。因此可以证明该态势预警模型可以有效识别工业互联网络信息，保证工业互联网安全态势预警的及时性。该模型不依赖于特定的攻击类型，即只要有攻击频率的历史信息，就可以根据攻击频率进行预警，它不但能够对工业互联网的短期安全状况进行预警，而且能够对长期安全状况进行预警，具有自学能力和较高灵活性，时间复杂性较低等特点。

3.4 工业互联网安全态势分析

3.4.1 基于 SIG 的报警事件聚类分析

基于统计信息网格的报警事件聚类分析可以帮助工业网络安全人员更好地了解网络安全事件的分布规律和特点，从而采取更加有效的预防和应对措施。具体步骤如下：

(1)将网络空间划分为网格单元。可以根据实际情况选择不同的网格大小和形状，例如正方形、矩形、六边形等。

(2)在每个网格单元中记录统计信息。可以记录该网格单元内的报警事件数量、报警类型、报警时间等信息。

(3)对每个网格单元进行聚类分析。可以使用聚类算法，例如 K-means 算法、

DBSCAN 算法等，将相邻的网格单元聚类为一个簇。

4. 分析聚类结果。可以根据聚类结果，找出簇内报警事件的共性和规律，例如某个簇内报警事件类型相似、发生时间相近等。

5.根据分析结果采取相应措施。可以根据聚类结果，采取相应的预防和应对措施，例如加强某些区域的网络安全防护、增加监控等。

总之，基于统计信息网格的网络安全报警事件聚类分析可以帮助网络安全人员更好地了解工业互联网安全事件的分布规律和特点，从而采取更加有效的预防和应对措施。

3.4.2 攻击频率序列获取

定义：设 $D_1,D_2,\cdots,D_n$ 是数据集 $S=\{S_1,S_2,\cdots,S_m\}$ 中数据对象的 n 个属性的有界定义域，那么 $D=D_1\times D_2\times\cdots\times D_n$ 就是一个 n 维空间，我们将 $D_1,D_2,\cdots,D_n$ 看作是 D 的维（属性、字段），则对于一个包含 m 个数据点的 n 维空间中的数据集 $l=\{l_1,l_2,\cdots,l_m\}$，其中 $l_i=\{l_{i1},l_{i2},\cdots,l_{in}\}(i=1,2,\cdots,m)$，$S_i$ 的第 j 个分量 $S_{ij}\in D_j$。将 D 中的每一维 M 等分，即把 D 分割成 M^m 个网格单元。

SIG 是一种基于网格的多分辨率聚类技术，它采用多分辨率的网格数据结构，将空间量化为有限数量的矩形单元，构成网格结构，并在整个网格内进行聚类。对于不同级别的分辨率，矩形单元通常存储多个级别。该算法预先计算并存储每个网格单元的属性的统计信息，包括平均值、最大值和最小值[40]。

利用 SIG 进行预警事件聚类分析的过程主要如下：将入侵事件的属性（时间、攻击类型、源地址、目的地址、请求的服务类型）视为 N 维空间 S 的维度，并分别定义一个有界定义域。输入的入侵事件是 N 维空间中的一组点。

以考察三维入侵事件为例，讲解聚类分析的全过程(时间、目标地址、攻击类型)。先把参数定下来，把最小的频次数值定到 5。

在一维空间当中，只考虑工业网络安全事件的发生时间，如果在某一时间间隔内发生的入侵次数大于等于 5，那么就把这个事件记录下来，并将其记录并存入到 $S_{[1]}$ 中：$S_{[1]}=\{e_{t1},e_{t2},\cdots,e_{tn}\}$。

在二维空间当中，需要在 $S_{[1]}$ 的基础之上，继续检查安全事件的目标地址，如果在某个目标地址上的入侵事件发生的次数大于等于 5，则把这个事件并记录下来并存入到 $S_{[2]}$ 中：$S_{[2]}=\{e_{(t,d)}\}$。

在三维空间当中，在 $S_{[2]}$ 基础上，继续检查安全事件的攻击类型，如果某个

攻击类型的入侵事件次数大于等于5，则将此类事件记录下来并存入到$S_{[3]}$中，$S_{[3]}=\left\{e_{(t,d,l)}\right\}$。其中，$e$表示入侵事件，$S_{[i]}$表示i维空间上满足最小支持度（它是该属性频次与总次数的比值）要求的事件集。

通过以上方法分析报警事件，得出攻击频率序列。需要选择合适的预警技术，根据获取的攻击频率序列预测未来的攻击事件。

3.5 本章小结

本章分析了在工业互联网环境下，传统的态势预警模型存在的不足，并在此基础之上，建立了基于统计信息网格的工业互联网安全态势预警模型，然后介绍了该模型框架的几个主要组成部分，描述了态势分析部分的主要内容。

第 4 章 基于 SDAE-IRF 的工业互联网安全态势分析要素提取方法研究

4.1 引言

由于传统态势分析要素提取方法的局限性，导致其在处理多特征和较高维度的非线性数据时，出现态势分析要素提取不准确和低效率的问题。为了能够更好的解决上述问题，本章针对工业互联网领域的安全态势分析要素提取方法，提出了一种基于降噪自编码器和改进随机森林算法的工业互联网安全态势分析要素提取方法。该方法在参考传统网络安全态势要素提取模型和提取方法的基础上，分析工业互联网安全现状，并建立工业互联网安全态势分析要素提取模型，利用降噪自编码器(Stacked Denoising Auto Encoders, SDAE)通过一系列非线性变换对原始输入数据进行特征提取，利用改进随机森林算法(Improved Random Forest, IRF)对基分类器进行筛选，然后采用加权多数投票的方式对原始随机森林算法进行改进，对降维后的数据进行分类训练从而得到最终分类结果。

4.2 工业互联网安全态势分析要素提取模型及方法

4.2.1 态势分析要素提取模型

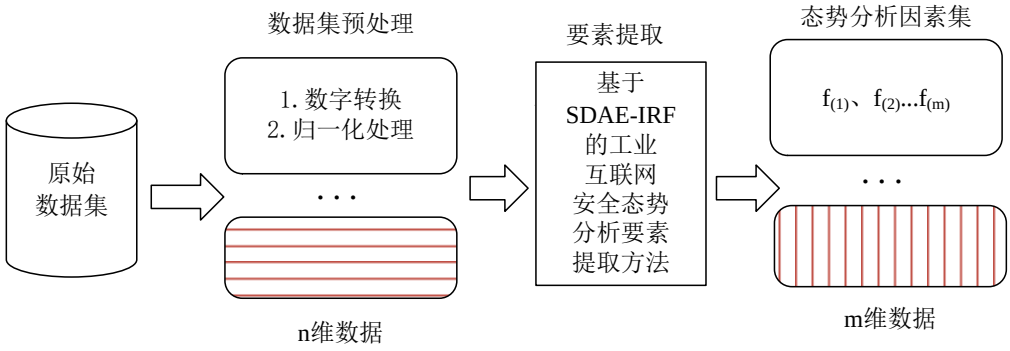


图 4.1 工业互联网安全态势分析要素提取模型

根据工业互联网安全态势分析要素提取的工作原理，本章建立的工业互联网安全态势分析要素的提取模型如图 4.1 所示。该模型首先要获得工业互联网的原始数据，并对其进行预处理操作，对数据进行数字转换、归一化处理。因为该数据集包括三种非数字数据类型，而数据集中各个特征计数之间通常存在

大量的极差，直接用原始数据进行实验会降低寻找最优算法方案的速度，并降低分类精度。再利用本章提出的基于 SDAE-IRF 的态势分析要素提取方法对预处理过的数据进行特征提取和分类，最后得到态势分析所需的因素集。

4.2.2 态势分析要素提取方法

由于 SDAE 有很好的复杂函数逼近能力，它针对大量的数据有很好的特征学习能力，能够有效选择重要属性，删除冗余属性。而且 IRF 能够从基分类器的分类精确度和多样性两个方面对基分类器进行筛选，从而提高整体的分类精确度和泛化能力，因此本章将两种算法结合进行工业互联网安全态势分析要素提取。具体提取流程如图 4.2 所示。

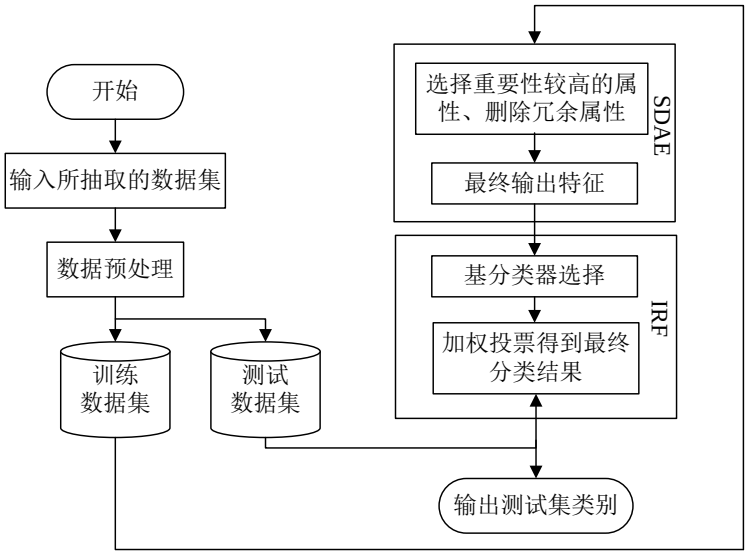


图 4.2 SDAE-IRF 提取方法框图

由图 4.2 可知，将上述处理过的数据分为训练数据集合测试数据集，然后将其输入到特征提取模块中的降噪自编码器算法当中，进行降维和特征提取，得到重要性较高的属性，去除了互补性较差的冗余属性。随后将这些特征信息输入到改进随机森林算法中生成一定数量的基分类器，然后筛选出分类精度较高的基分类器，然后对基分类器做加权投票得到最终分类结果。

4.3 基于 SDAE-IRF 的工业互联网安全态势分析要素提取方法

4.3.1 基于 SDAE 的特征提取

自编码器（AE）是一种无监督神经网络结构，它有三层结构，以隐藏层为

界，下面输入层为编码器（encoder），上面输出层为解码器（decoder）。其结构如图 4.3 所示。在隐藏层中，首先对输入信息进行编码，然后对输出数据进行重构。使得输出信息与输入信息之间的重构误差接近最小值，以此来获得数据的抽象表示[41]。

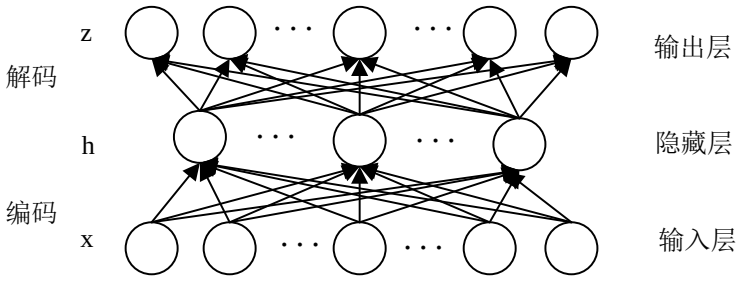


图 4.3 用于特征提取的 AE 架构

假设编码器的输入层与隐藏层的神经元数目分别为 D_i 和 D_h。给定一组未标记的数据集 $X=\{x_1,x_2,\cdots x_n\}$，$x_i \in R^n$。训练过程包括两部分：编码器和解码器[42]。在编码过程中，编码器利用映射函数 f_θ 通过一系列非线性映射变化将输入向量 x_i 转换为隐藏层向量 h 如公式（4.1）所示。

$$h(x_i)=f_\theta(x_i)=f(W_1x_i+b_1) \tag{4.1}$$

其中，参数集合 $\theta=(W,b)$，$W_1 \in R^{D_i \times D_h}$ 是编码权重矩阵，$b_1 \in R^{D_h}$ 是偏移向量。在解码过程中，同样利用映射函数 g_θ 通过对隐藏层向量 h 进行线性映射，重构输入向量 x_i，得到输出向量 z 如公式（4.2）所示。

$$z_i=g_\theta(h(x_i))=W_2h(x_i)+b_2 \tag{4.2}$$

其中，参数集合 $\theta=\{W_2,b_2\}$，$W_2 \in R^{D_h \times D_i}$ 是解码权重矩阵，$b_2 \in R^{D_i}$ 表示偏移向量。

从上述训练模型来看，自编码器的主要任务是通过调节编码器和解码器的相关参数，使得输入向量 x 和输出向量 z 的重构误差最小化，即输入输出的代价函数最小化[43]。代价函数定义如公式（4.3）所示。

$$J(W,b)=\left[\frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{2}\left\|z_i-x_i\right\|^2\right)\right]+\frac{\lambda}{2}\sum_{l=1}^{m_l-1}\sum_{i=1}^{m_l}\sum_{j=1}^{m_l+1}(W_{ij}^{(l)})^2 \tag{4.3}$$

上式的第一部分为均方误差项，第二部分为正则化项，其目的是减小权值的大小防止过拟合。λ 是正则化系数。通过最小化代价函数 $J(W,b)$ 可得到相关权重矩阵 W 和偏移向量 b。

传统的自编码器实质上就是通过学习非线性映射，使得原始输入数据与重建输出数据等价。这类直接从编码解码中得到的映射所存在的最大问题是当被

测样本与训练样本之间的特征并非完全处于某一特征空间中，特别是主特征并不是处于同一个特征空间中，则训练出的结果相对较差、泛化能力也较差[44]。与传统自编码器相比, SDAE 样本空间遭到破坏，其在学习消除噪声数据重构原始样本空间训练中获得了更好的特征表达和泛化能力[45]。

在参数调整方面，本章对 SDAE 模块中隐含层节点的数量的选取进行了研究，确定了最优参数，提高了特征提取的效率。如图 4.4 所示，SDAE 通过叠加多个降噪自编码器实现原始数据的抽象特征表示，重构输入。这意味着它通过输入数据训练第一个隐藏层，然后将第一个隐藏层的输入作为第二个隐藏层的第一个输入，直到所需的数据表示完成[46]。

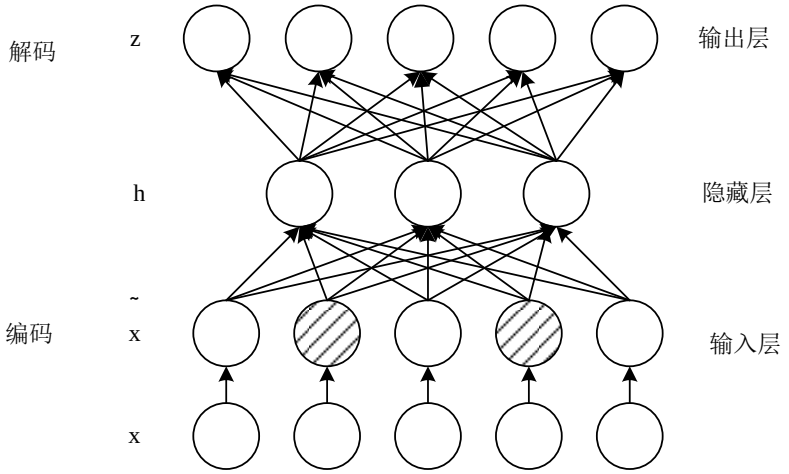


图 4.4 用于特征提取的 SDAE 架构

通过随机映射向原始输入数据添加噪声： $x \to q(x|x)$，并将其映射到一个隐藏层表示如公式（4.4）所示。

$$h = f_\theta(x) = f(W_1 x_i + b_1) \tag{4.4}$$

使用与自编码器相同的重构方法对输入数据进行重构如公式（4.5）所示。

$$z_i = g_\theta(h) = W_2 h + b_2 \tag{4.5}$$

同样，通过最小化代价函数得到降噪自编码器参数 $\{\theta, \theta'\}$ 如公式（4.6）所示。考虑到 SDAE 是一个多层降噪编码器的堆栈，W_{all} 表示堆栈降噪自编码器网络的权值矩阵，b_{all} 表示偏移向量矩阵。

$$W_{all}, b_{all} = \arg\min_{\theta_l, \theta'} J(W, b) \tag{4.6}$$

$l \in \{1, \ldots, L\}$ 代表 SDAE 的隐藏层数，h_l 表示 l 层的输出向量，W_l 为 l 层的权值，

b_l 表示 l 层的偏移量，利用 SDAE 预训练就可得到最终输出特征如公式（4.7）所示。

$$h_{l+1} = f(W_{l+1} + b_{l+1}) \tag{4.7}$$

其中 $f(x)$ 为激活函数，h_{l+1} 表示最终的输出特征。

以上内容是单层降噪自动编码器的训练过程，本章的特征提取模块是通过叠加多个自动降噪编码器来训练的，其训练过程类似于单层自动降噪编码器。在重建第一层特征后，将其作为隐藏层引入下一层进行信息训练，重复这一过程直到训练结束。经过多级训练，该模型获得了足够好的特征来代表原始输入数据，但降噪自分类器还没有处理分类问题的能力，通常需要在其底部添加特定的分类器进行分类。

4.3.2 基于 IRF 的分类

SDAE 算法完成了工业互联网安全态势分析要素提取的第一步，特征提取。然而要素提取最终要处理的是分类问题，因此模型需要在 SDAE 的底层设计分类器。本章采用 IRF 作为底层分类器，主要基于以下几点：传统的准确率较高的分类算法对于大规模数据处理能力不高；处理时间较优的算法往往对数据预处理有较高的要求[47]。而 IRF 算法将大规模数据的分类问题分解为各个子分类器处理的小规模问题，从而实现了快速准确的分类。并且该算法从基分类器的选取以及投票方式两个方面对原始随机森林算法做出了改进，相比于原始随机森林算法其筛选的基分类器分类精度更高，对基分类器的投票方式更加科学，实现相对简单，应用领域广泛[48]。随机森林算法的整体分类步骤如图 4.5 所示。首先，把原始的数据集，按照一定的原则一分为二，分别为训练集和测试集。训练数据集为 $D = \{(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)\}$，采用 BOOTSTRAP 算法，从样本集中随机抽取与原始数据量相同的样品，实行有放有回的随机抽样，得到 m 组训练子集。其次，从每组训练子集的全部属性特征中，随机抽取 K 个特征，选出最优秀的分枝树。建立 M 决策树作为其节点，每个决策树之间没有相关性；然后，对生成的每一棵决策树重复上述操作，使得每棵决策树都能产生更好的分类结果；最后，对这 M 棵决策树进行投票，使其形成一个随机森林，决定数据的分类。投票机制包括一票否决和加权多数投票等 [49]。其中多数投票法如公式（4.8）所示。

$$H(X)=\arg\max\sum_{i=1}^{k}I(h_i(X)=Y) \tag{4.8}$$

其中$H(X)$为最终的态势分析要素，h_i为单棵决策树的投票结果，$I(.)$为示性函数。

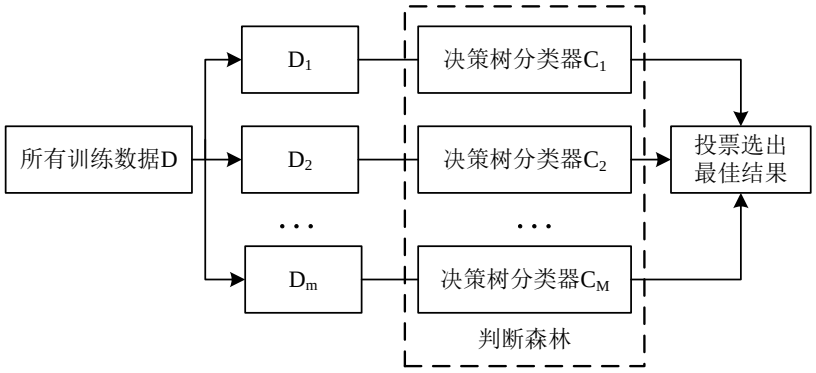


图 4.5 原始随机森林分类图

对于改进的随机森林算法来说，每组基分类器之间的互补性和独立性，对其分类效果、分类效率等均有影响。因此基分类器的选择首先要解决的问题是如何去除分类结果相似的分类[50]。这里采用成对多样性度量的方法，只考虑两组分类器的分类差异样本的比例。首先引入如下符号：假设K个基分类器成立，其中C_i和$C_j(i,j=1,2,3...K,i\neq j)$是基分类器中任意两个不同的基分类器，如表 4.1 为二分类器分类结果表。$N_{11}(N_{00})$是态势分析要素在分类中都对（都错）的个数，$N_{10}(N_{01})$是分析要素在分类中一对一错（一错一对）的个数。

表 4.1 二分类器分类结果

C_i	C_j 1	C_j 0
1	N_{11}	N_{10}
0	N_{01}	N_{00}

由表 4.1 可计算出这两个基分类器态势分析要素的总量如公式（4.9）所示。

$$K=N_{11}+N_{00}+N_{10}+N_{01} \tag{4.9}$$

分类器分类结果的不一致度量关心的是两个分类器C_i和C_j在同一特征分类中所产生的不同分类结果的样本，其不一致公式如(4. 10)所示。

$$C_{ij}=(N_{10}+N_{01})/K \tag{4.10}$$

由上式可知，两个基分类器分类结果不同的数据点越多，则两个基分类器之间的互不相似度就越大，其取值范围为[0,1]。其中C_{ij}为分类结果相似的分类器。在通过对随机森林分类器不一致性指标进行选择后，就能得到分类性能更

好的基分类器。因此，从整体上提高了随机森算法的分类精度。

传统随机森林算法中使用的投票方法是以相同的权重对所有的基础分类器进行投票。这样一来，不同基础分类器之间的差异性就被忽略了，总会有一个表现不佳的基础分类器没有正确投票，这将会影响随机森林算法的最终分类结果[51]。加权多数投票法是一种最直观也是最常用的综合方法，将更大的话语权通过加权投票法分配到一个表现更好的分类器上[52]。各基分类器的权重与对应的分类精度的关系如公式（4.11）所示。

$$W = \ln \frac{p_i}{1-p_i}, (i = 1...K) \tag{4.11}$$

其中 p_i 为第 i 个基分类器的分类精度，W 是 p_i 精确度所对应的权重。本章采用上述公式求出各基础分类器选取后的权重，最终分类结果和权重之间对应关系用(4.12)表示。

$$f_{inal}(x) = \arg\max \left\{ \sum_{m \in K, f_{tree}, m(x)=i, i=1,2,...,n} W_m \right\} \tag{4.12}$$

其中 f_{inal} 为最终分类结果，i 为类别数，m 为基分类器，通过改变基分类器的投票方式来提升整体的分类效果。

4.4 实验及结果分析

本章实验编程环境为 Windows10 环境下的 Python3.6，编程平台选用 PyCharmCommunity2017。Intel 酷睿 i7-6500UCPU2.50GHz 内存 16GB 运行内存。借助机器学习库 SCIKIT-LEARN 实现相关算法。数据集选取了公开的天然气管道 SCADA 系统数据，其中包含 26 个维度特征的 274628 个实例和一个包含 7 种不同攻击的类目标签的标签列[53]。

由于数据集的数据样本数量庞大，实验研究难度较大，因此，本章对原始数据集中的 5000 个数据进行了随机筛选，作为实验数据集。选取五分之四的实验数据作为训练集，五分之一的实验数据作为测试集。从中提取了 3137 个正常数据、158 个简单的恶意响应注入攻击、783 个复杂的恶意响应注入攻击、42 个恶意状态命令攻击、406 个恶意参数命令注入攻击、19 个恶意功能命令注入攻击、87 个拒绝服务攻击和 368 个检测攻击。该数据集中数据的种类与标签之间对应的关系如表 4.2 所示。

为验证本章工业互联网安全态势分析要素提取方法的有效性，选取准确率（Accuracy）、误报率（Error）为性能指标。其中分类准确率指的是正确划分样本数量与所有样本数量之间的比值，分类准确率越高，表示方法性能越好。

表 4.2 数据种类与标签对应关系

攻击种类	具体描述	标签
Normal	正常数据	0
NMRI	简单的恶意响应注入攻击	1
CMRI	复杂的恶意响应注入攻击	2
MSCI	恶意状态命令注入攻击	3
MPCI	恶意参数命令注入攻击	4
MFCI	恶意功能命令注入攻击	5
DoS	拒绝服务攻击	6
Recon	侦察攻击	7

误报率指的是检测出正样本数量中错误样本的数量与全部样本数量的比值，误报率数值越低，表明方法性能越好[54]。正确率和误报率的计算如公式（4.13）（4.14）所示。

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4.13}$$

$$Error = \frac{FN}{TP + FN} \tag{4.14}$$

其中 TP 为阳性，表示此次分级结果为阳性，而实际为阳性；FP 是假阳性，说明分级结果是正样本，其实是负样本；TN 为真阴性，代表分级结果为负值，实际为负值；FN 为假阴性，表示分级结果为负数，实际为正数。本章将数据集中的异常攻击设为正样本。

4.4.1 特征提取性能

文献[17]中探讨了深度神经网络的训练策略，指出网络层数的增加可以提高降噪自动编码器的表征学习能力，但是层数过多也会导致网络的泛化能力下降。因此，选择适当的层数来构建 SDAE 网络结构是非常重要的。本章分别采用不同隐藏层的 SDAE 结构来对原始数据集进行特征提取，编码层数分别为 2 层、3 层和 4 层。不同层 SDAE 结构算法及 BP 特征提取方法性能比较如图 4.6 所示其中 2-SDAE-BP 表示含有两个隐藏层的 BP 算法，3-SDAE-BP 表示含有三个隐藏层的 BP 算法，4-SDAE-BP 表示含有四个隐藏层的 BP 算法。

由该图可知，当隐藏层数为 2 时，其算法的优势相较于 BP 算法并不明显，这是因为当隐藏层数较少时，该算法的学习数据重构能力不高，导致无法充分提取态势分析要素的特征信息。

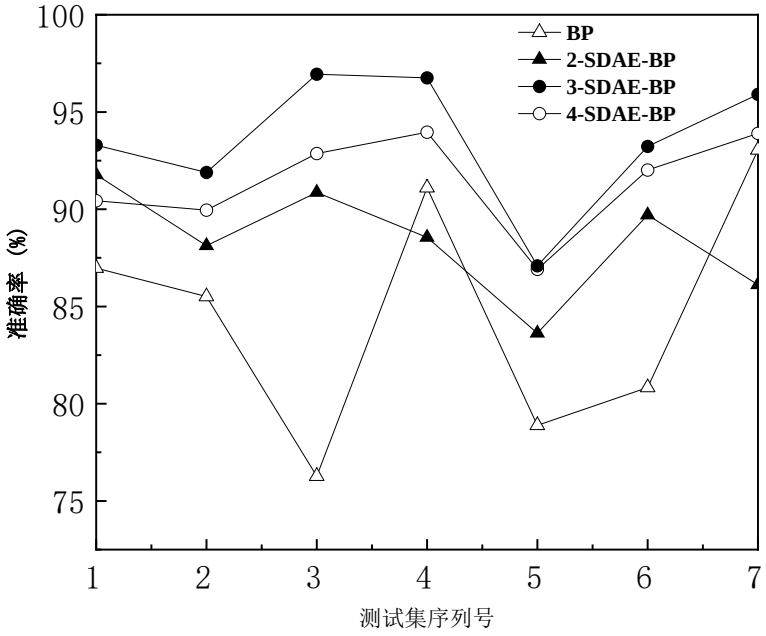


图 4.6 不同层次 SDAE 特征提取方法对比图

由于隐藏层数的增加，很明显可以看出其算法的特征学习能力在增强，提取的精度也有了明显的改进。但是图中 4-SDAE-BP 算法的提取精度较 3-SDAE-BP 算法略低，这是因为当隐藏层的数量增加时，层与层之间存在的大量非线性转换，导致态势分析要素的特征信息出现一定的损失，这是无法避免的。因此，就造成了特征提取准确率的降低。故本章使用含有三个隐藏层的 3-SDAE-BP 算法对原数据集进行态势分析要素提取。

4.4.2 分类方法性能

为验证本章 IRF 分类方法的有效性，表 4.3 和表 4.4 分别对比了不同分类方法所得到的分类准确率和误报率两个评价指标。

表 4.3 不同方法的分类正确率数据

属性个数	分类正确率（%）		
	文献[15]	文献[16]	本章方法
5	93.19	95.83	98.80
11	93.08	92.94	98.64
13	92.62	94.46	96.02
17	91.87	93.20	97.51

由表 4.3 中的数据可知，当属性个数为 17 时，文献[15]的平均分类正确率为 82.46%，文献[16]的平均分类正确率为 85.78%，而本章分类方法 IRF 的平均

分类正确率高达 94.52%，主要原因在于，在原始随机森林的基础上对产生的基分类器进行了筛选，去除了分类结果相似的基分类器，从而在整体上提高了分类方法的分类精度。

表 4.4 不同分类方法的误报率数据

类别	分类误报率（%）		
	文献[15]	文献[16]	本章方法
Normal	12.6	13.2	2.1
NMRI	0.9	0.7	0.4
CMRI	0.8	0.6	0.5
MSCI	1.4	1.2	1.1
MPCI	2.8	4.7	1.6
MFCI	4.7	3.5	2.3
DoS	16.0	18.0	17.8
Recon	7.6	5.3	4.1
Weighted Avg	9.5	8.2	6.7

由表 4.4 中的数据可知，本章分类方法 IRF 对数据集中不同类别的攻击分类的误报率相较于文献[15]和文献[16]都较低，这是因为本章方法在对分类器的投票上也做了从原始的相同权重投票到加权多数投票的改进，从而有效的降低了误报率。

4.4.3 态势分析要素提取性能

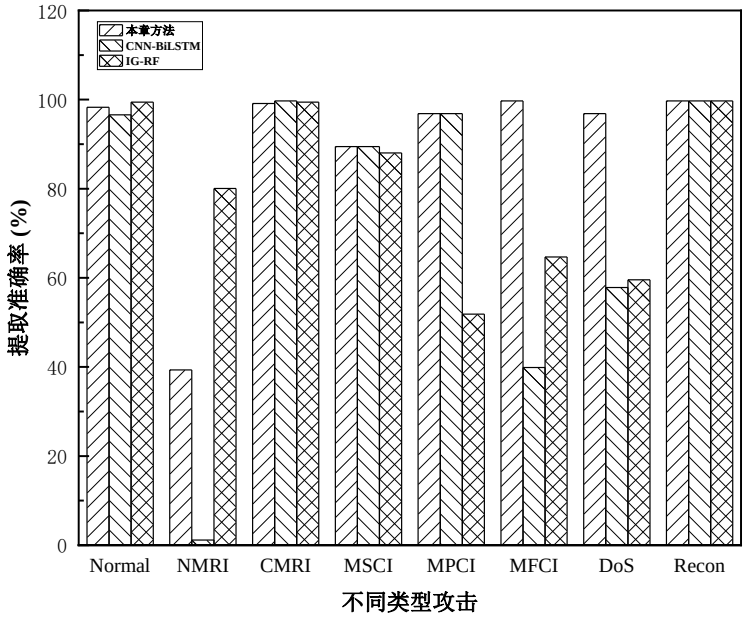


图 4.7 不同种类攻击提取正确率

如图 4.7 表示的是采用文献[14]、文献[16]、本章方法等三种态势分析要素提取方法对无攻击流量（正常数据）、NMRI(简单恶意响应注入攻击)、CMRI(复杂恶意响应注入攻击)、MSCI(恶意状态命令注入攻击)、MPCI（恶意参数命令注入攻击）、MFCI（恶意功能命令注入攻击）、DoS（拒绝服务攻击）、Recon（侦察

攻击)的提取情况。条形图中的不同形状代表不同的方法。横坐标表示不同的攻击类型，纵坐标表示情况分析要素的正确提取率。

图中三种不同的柱状图分别代表本章态势分析要素提取方法和文献[14]和文献[16]的态势要素提取方法。从上述实验图中可以看出本章的态势分析要素提取方法 SDAE-IRF，对 Normal、CMRI、MSCI、MPCI、MFCI、DoS、Recon 的提取效果较好，仅对 NMRI 这一个攻击类别的提取不太理想。这是因为这一类型的攻击对所采集的样本数据值比较敏感，因此导致提取效果不佳。从整体趋势来看本章提出的 SDAE-IRF 态势分析要素提取方法，在以上三种方法中提取的精确度更高，能够对各种不同的网络攻击进行准确的分类。证明了本章提出的方法的可靠性。

4.5 本章小结

本章首先对工业互联网安全态势分析要素提取进行系统建模，从本章的提取模型图中可以得出，态势分析要素提取方法性能的好坏将直接影响态势分析要素集的维度，而且对工业互联网安全态势分析结果有着关键影响。因此本章设计了一种基于 SDAE-IRF 的态势分析要素提取方法，分别从不同层次 SDAE 结构特征提取方法的性能、不同分类器的分类效果及不同态势分析要素提取方法提取性能进行对比分析。实验结果表明，本章采用的方法为一种有效的态势分析要素提取方法，该方法突破了传统的态势要素提取的方法在多特征和高维度的非线性数据处理上的局限性，解决了传统态势分析要素提取方法不准确、效率较低等问题。本章为工业互联网安全态势分析要素提取的研究提供了一种新思路，为接下来工业互联网安全态势分析和态势预警工作提供了数据支持。

第 5 章 基于 HMM 的工业互联网安全态势预警技术

5.1 引言

预警技术当中最核心的问题是攻击预测。由于工业互联网攻击的复杂性，传统的互联网安全态势预警技术存在以下两个问题：一是其对应的复合攻击场景如何从大量的报警信息组合而成的报警信息序列中找到；二是找到与报警信息序列相应的复合攻击场景之后，背后所隐藏的攻击意图序列是如何被发现的。为了解决上述问题，本章采用基于 HMM 的工业互联网安全态势预警技术。首先，把这些已完成的复合攻击步骤相对应的报警信息形成一个报警信息序列，然后将其输入到预先建立的基于复合攻击 HMM 态势预警模型当中，推断出隐藏在报警信息序列中的攻击意图序列，最后预测出攻击者可能的下一个攻击意图和攻击行为。

5.2 基于复合攻击的 HMM 态势预警模型

随着网络攻击手段的不断升级和复杂化，传统的单一攻击预警模型已经无法满足网络安全的需求。复合攻击已经成为一种常见的攻击方式，攻击者通过多种攻击手段相互配合，以达到更高的攻击效果。为了有效地应对复合攻击，需要开发一种能够及时预警的态势预警模型。HMM 是一种常用的序列建模方法，可以用于对时间序列数据进行建模和预测[55]。在本章中，提出了一种基于复合攻击的 HMM 态势预警模型如图 5.1 所示。

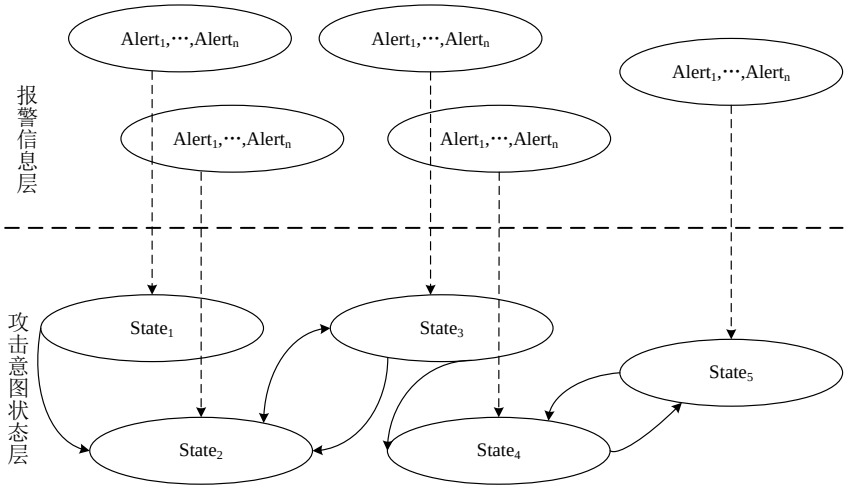


图 5.1 基于复合攻击的 HMM 态势预警模型

上述预警模型主要包括两部分：报警信息层和攻击意图状态层。其中报警信息层是由入侵检测系统产生的报警信息组成，而这些报警信息是我们唯一能直接观察到的信息。入侵者为了完成攻击任务，会尽可能小的代价，充分利用一些可以利用的信息和手段。无论最终攻击结果的成败与否，由入侵检测系统所产生的报警信息为入侵者攻击意图的进一步认定提供了基础。攻击意图状态层由复合攻击的每个攻击意图抽象而成，这里蕴含着攻击者真正的攻击意图信息，从外部无法直接观察到。在对复合攻击的各个攻击步骤进行分析时，在隐马尔可夫模型的攻击意图状态层中的状态也随之确定，只要提取到对应攻击意图的各个攻击步骤阶段。这种复杂的报警信息与攻击意图之间的关系，导致观察者为了感知复合攻击的进展，只能根据报警信息对入侵者的攻击意图进行推断[56]。

该模型将复合攻击看作是一种隐含状态，通过对攻击行为序列进行建模，可以预测出未来可能发生的攻击行为。具体来说，我们将攻击行为序列分为多个时间段，并将每个时间段看作是一个观测状态。同时，我们将复合攻击看作是一个隐含状态，通过对观测状态和隐含状态进行建模，可以得到一个 HMM 模型。在该模型中，我们可以通过观测状态来预测隐含状态，从而预测未来可能发生的攻击行为。该模型的优点在于，它能够对复合攻击进行有效的建模和预测，能够及时发现并预警未来可能发生的攻击行为。同时，该模型还可以根据实际情况进行调整和优化，以提高预测的准确性和可靠性[57]。

5.3 基于 HMM 的工业互联网安全态势预警技术

5.3.1 复合攻击判别

复合攻击判别可作如下描述：首先将入侵检测系统产生的报警信息，经过报警信息的预处理后，形成报警信息序列；然后利用 HMM 中的 Forward 算法，计算出各种复合攻击模型产生报警信息序列的概率；再根据概率值的大小来判断攻击者可能会进行的复合攻击，哪个复合攻击产生的概率值大，就表示入侵者可能会进行哪个复合攻击[58]。报警信息序列会随着复合攻击的深入而增加，概率值也会随之增加，也就是判断复合攻击发生的精确度会越来越高。由此可见，选择复合攻击的 HMM 模型，也将与攻击者复合攻击的轨迹越来越接近。复合攻击判别如图 5.2 所示。

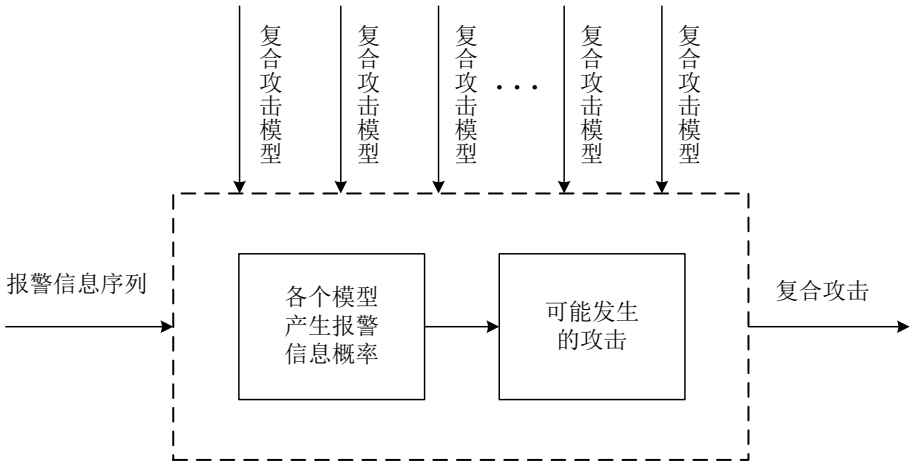


图 5.2 复合攻击判别

图中的输入部分为经过预处理之后的报警信息组成的报警信息序列。根据特定的复合攻击所建立的 Malkov 模型 $\lambda=(A,B,\pi)$，计算每一种攻击 Malkov 模型产生警报信息序列的机率，再根据每一种模型产生警报系统信息序列的机率，选出最容易发生的复合攻击。图中输出部分为入侵者可能性最大的复合攻击。

前向算法主要用于求概率 $P(O|\lambda)$，首先给定一个报警信息序列 $O=\{Alert_1,Alert_2,\cdots,Alert_n\}$ 及 HMM 模型 λ，然后在复合攻击的 HMM 模型中代入收集到的报警信息。最后，报警信息序列最有可能包含的复合攻击，可以根据得到的概率值的大小，自动进行分析[59]。

利用前向算法在进行复合攻击判别时，将执行以下操作：

1.计算攻击意图 $intent_i$ 产生报警信息 $Alert_1$ 的概率；

$$\alpha_1(i)=\pi_i \bullet b_i(Alert_1) \tag{5.1}$$

其中 π_i 表示第 i 时刻的初始状态概率向量，b_i 表示第 i 时刻的观察值产生概率。

2.计算 $t+1$ 时刻，产生报警信息序列 $\{Alert_1,\cdots,Alert_{t+1}\}$ 且 $q_{t+1}=intent_j$ 的概率；

$$\alpha_{t+1}(j)=\left[\sum_{i=1}^{N}\alpha_t(i)\alpha_{ij}\right]b_j(Alert_{t+1}) \tag{5.2}$$

其中 $1\le t\le T-1;1\le j\le N$；$\alpha_{ij}$ 表示状态 i 到状态 j 的转换概率，b_j 表示观察值处在状态 j 时刻的产生概率，N 表示攻击意图的个数。

3.计算复合攻击的隐马尔可夫模型 λ 产生报警信息序列 $O=\{Alert_1,Alert_2,\cdots,Alert_T\}$ 的概率；

$$P(O|\lambda)=\sum_{i=1}^{N}\alpha_T(i) \tag{5.3}$$

判断最有可能发生的复合攻击是根据上述前向算法进行的。假设 n 个复合

攻击隐马尔可夫模型是事先建立的，每个模型产生告警信息序列的概率是 $P(O|\lambda)=\{P(O|\lambda_1),P(O|\lambda_2),\cdots,P(O|\lambda_n)\}$，最大概率 $P(O|\lambda^*)$ 是从中选择出来的。于是复合攻击 Malkov 模型 $\lambda^*=(A,B,\pi)$ 就表明复合攻击的可能性最大。

5.3.2 攻击意图识别

每一个特定的攻击步骤(攻击意图)，入侵者在进行复合攻击时，都有不同的攻击方式，而且每个攻击方式的攻击目的都可能不一样。与此相对应的是，同样的攻击步骤，所产生的报警信息也可能是千差万别的。因此，在预测攻击时，研究入侵者哪个攻击意图序列的可能性最大，需要根据报警信息集合来进行识别[60]。

本章采用改进维特比（Viterbi）算法精细攻击意图的识别：首先确定一个报警信息序列 $A=\{Alert_1,Alert_2,\cdots,Alert_n\}$ 和一个隐马尔可夫模型 $\lambda=(A,B,\pi)$，然后通过计算得到复合攻击 HMM 模型产生报警信息的概率，最后找到所隐藏的最佳攻击意图序列 $I=\{intent_1^*,intent_2^*,\cdots,intent_T^*\}$ [61]。具体执行操作如下：

1.计算产生报警信息 $Alert_1$，并且当前处于攻击意图 $intent_i$ 的概率；

$$\xi(i)=\pi_i \bullet b_i\left(Alert_{c_1}\right) \tag{5.4}$$

其中 c_1 表示在 $t=1$ 时刻所处的中心点，且有 $center_1(i)=c_1$。

2.计算产生报警信息 $\{Alert_1,Alert_2,\cdots,Alert_t\}$ 且处于攻击意图 $intent_j$ 的概率；

$$\xi_t(j)=\left[\max_{1\le i\le N}\{\xi_{t-1}(i)\alpha_{ij}\}\right]\bullet\max_{c_t\in\Omega_{pred_t(j)}}\left\{b_i\left(Alert_{[c_t]}\right)\right\} \tag{5.5}$$

$$center_t(j)=\arg\max\left\{b_j\left(Alert_{[c_t]}\right)\right\}\ (1\le j\le N,2\le t\le T) \tag{5.6}$$

$$pred_t(j)=center_{t-1}\left(\arg\max_{1\le i\le N}\{\xi_{t-1}(i)\bullet\alpha_{ij}\}\right) \tag{5.7}$$

其中 Ω_i 表示以 i 为中心的领域范围，$pred_t(j)$ 表示最佳部分报警序列中最后一个报警信息所对应的中心点，即 t 时刻处于攻击意图 $intent_j$ 并产生报警信息 $Alert_t$ 的中心前驱点。

3.计算最佳攻击意图序列 $Q^*=\{intent_1^*,intent_2^*,\cdots,intent_T^*\}$；

$$intent_t^*=center_{t+1}\left(intent_t^*\right)\ t=T-1,T-2,\cdots,1 \tag{5.8}$$

入侵者在进行网络攻击的时候，其攻击意图时常具有隐蔽性的特征，它的真正攻击意图通常隐藏在入侵检测系统产生的报警信息中。识别入侵者的攻击

意图就是在报警信息预处理后，根据报警信息序列得出入侵者真正的攻击意图。如图 5.3 所示为攻击意图识别图。

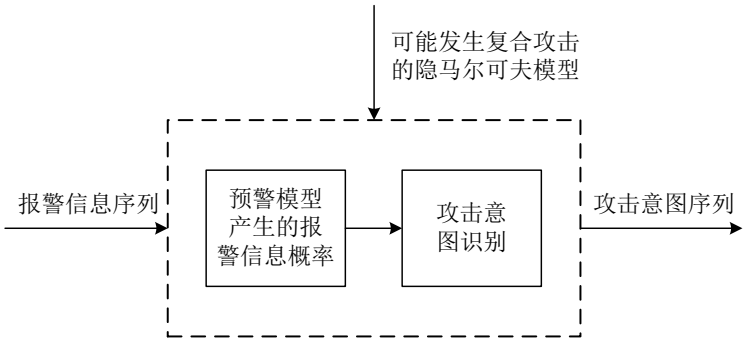


图 5.3 攻击意图识别

根据图 5.3 可以看出， 攻击意图识别部分的输入部分是报警信息序列和可能出现复合攻击的隐马尔可夫模型，由预处理后的报警信息组成。识别过程首先通过计算隐马尔可夫模型产生告警信息序列的概率，然后根据最大概率原则，选择最佳攻击意图，最后得出攻击意图序列。

5.3.3 攻击预测

攻击预测阶段主要是将以上两种算法合并在一起，应用在基于 HMM 的攻击预测算法的攻击预测中[62]。首先，将攻击最开始的阶段收集到的攻击报警信息视为观察值序列G，将所有经过训练的复合攻击 HMM 模型作为备选模型，然后将每个模型中产生的观察值序列的概率G按照一定的次序进行计算，从中挑出的最大概率表明该报警信息最有可能来自于哪一种特定的复合攻击场景[63]。

把报警信息序列$A=\{Alert_1, Alert_2, \cdots, Alert_n\}$代入到建立好的复合攻击 HMM 模型当中，判别出接下来最有可能发生的复合攻击并且识别出入侵者最有可能的攻击意图序列以后，然后要进行的操作就是预测入侵者的攻击步骤[64]。根据攻击意图识别得到的攻击意图序列，求出复合攻击 HMM 模型$\lambda^*=\theta(A,B,\pi)$最有可能发生的全部攻击意图后。预测入侵者下一步可能的攻击意图具体执行操作如下：

$$Q=S-Q^* \tag{5.9}$$

其中S表示复合攻击 HMM 模型λ^*中的攻击意图，Q^*代表已完成攻击的攻击意图序列。

由于这一部分是预警技术当中比较重要的一个环节，它主要负责的是根据

报警信息、入侵者已经完成的攻击意图来预测入侵者的行动路线，入侵者下一步的行动路线是预警技术的主要内容[65]。如图 5.4 所示为攻击预测图。

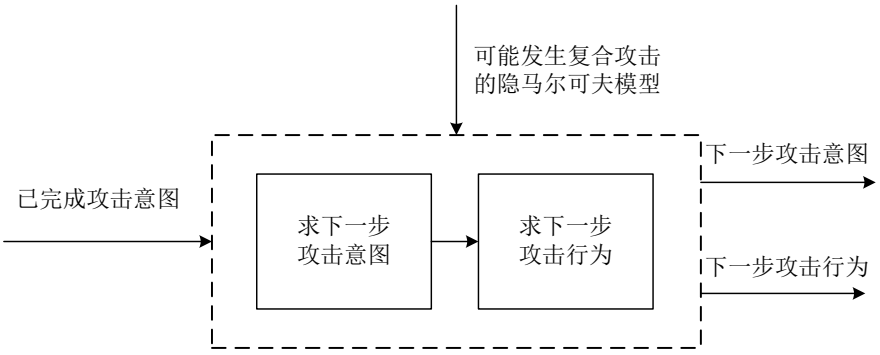


图 5.4 攻击预测

从图 5.4 可以看出， 在攻击预测过程中的输入部分，有入侵者已经完成的攻击意图，还有可能会发生复合攻击的隐马尔可夫模型。这一过程主要有以下两个内容：第一个内容是对入侵者的下一步攻击意图进行求索，这一部分主要负责对入侵者的第一步行动路线进行预测。内容二是对入侵者的下一步攻击行为进行求索，这部分主要负责入侵者具体的攻击方式进行预判。

5.4 实验及结果分析

本章实验编程环境为 Windows7 环境下的 MATLAB2010a，Intel 酷睿 i7-6500U CPU2.50GHz 内存 16GB 运行内存，实验工具用到 WEKA3.9。数据集选 NSL-KDD，NSL-KDD 数据集是一种用于评估入侵检测系统的标准数据集，它是对原始 KDD Cup 99 数据集的改进版本，去除了其中一些问题并添加了更多的样本，使得该数据集更适合于现代网络安全环境的实际应用。

该数据集包含 41 个网络连接属性和 1 个网络连接的类标签，其中 41 个网络连接属性按照数据的含义可以分为 4 类，分别是 9 个网络连接的基本特征、13 个网络连接的内容特征、9 个基于时间的网络流量统计特征以及 10 个基于主机的网络流量统计特征。根据数据类型每个网络连接分为 9 个离散属性和 32 个连续属性。而 1 个网络连接类标签又包括异常类型和正常类型两种，其中异常类型中的 39 种攻击类型分为四类，这四种异常类型的数据以及正常类型数据分布如表 5.1 所示。

为验证本章工业互联网安全态势预警技术的性能，分别选取平均绝对误差（Mean Absolute Error，MAE）和均方根误差（Root Mean Square Error, RMSE）

作为评价预警技术中攻击预测算法的性能指标[66]，误差值越小，表示攻击预测算法精度越高，说明态势预警更准确。其中两种误差的计算公式定义如下：

表 5.1 NSL-KDD 数据集的数据分布

类标签	训练集	测试集
正常数据	67343	9711
Dos	45927	7456
Probe	11656	2421
U2R	52	200
R2L	995	2756

$$MAE = \frac{1}{N}\sum_{i=1}^{N}\left|y_i - \tilde{y}_i\right| \tag{5.10}$$

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - \tilde{y}_i\right)^2} \tag{5.11}$$

其中 N 表示训练样本个数， y_i 表示实际值， $\tilde{y}_i$ 表示预警模型的预测值。

5.4.1 预警精度

为了对不同预警技术进行精确评估，表 5.2 计算了不同预警技术的平均绝对误差和均方根误差。根据本章选取的两个测评指标来衡量预警结果，这两个测评指标分别表示预测值与真实值的偏离程度和拟合度，数值越小表示预警效果越好。从表 5.2 可以看出，本章提到的预警技术中攻击预测方法与其他方法相比，在两个误差方面的优势更大一些。

表 5.2 预警误差指标对比

预警方法	MAE	RMSE
本章方法	0.0015	0.0026
SVM	0.1128	0.1542
BP	0.0084	0.0096
LSTM	0.0052	0.0068
RNN	0.0072	0.0079

表 5.3 是在进行预警时，不同预警方法在各连续时间点上的绝对误差对比，

本章提出的基于 HMM 的工业互联网安全态势预警技术，从表中可以得出结论，总体来看效果还是比较不错的。在所有随机抽取的连续时间段内的时间点上，它们的绝对误差都控制在 0.4%以内，剩下的绝大多数时间点上的绝对误差都比其他方法低，由此可见，本章的基于 HMM 的工业互联网安全态势预警技术有较好的预警效果。

表 5.3 不同预警方法各时间点预警绝对误差对比

序号	本章方法	SVM	BP	LSTM	RNN
1	0.00062	0.00294	0.01058	0.00268	0.00548
2	0.00248	0.01826	0.00796	0.00209	0.00549
3	000266	0.03912	0.00812	0.00284	0.00708
4	0.00118	0.01424	0.01152	0.00648	0.00512
5	0.00036	0.01568	0.01086	0.00365	0.00424
6	0.00015	0.01189	0.01567	0.00451	0.00563

将本章方法同 SVM、BP、LSTM、RNN 等传统预警方法进行预警精度比较，结果如图 5.5 所示。

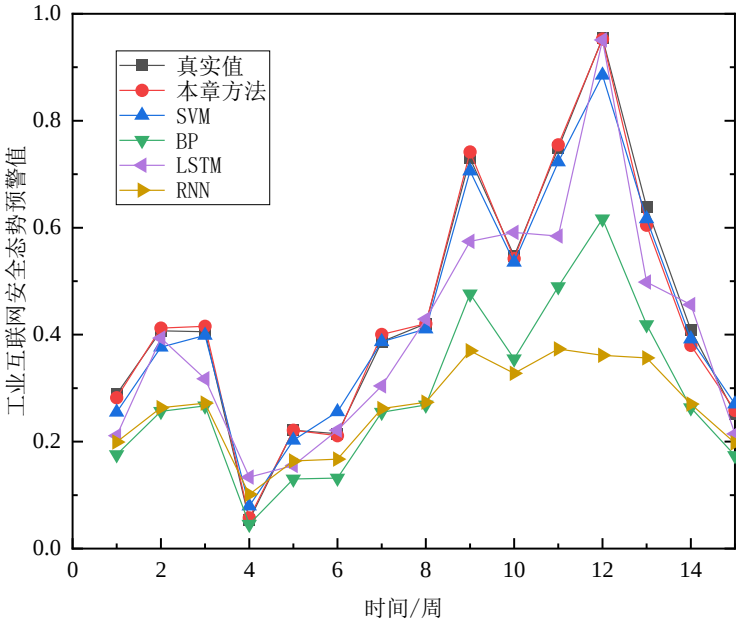


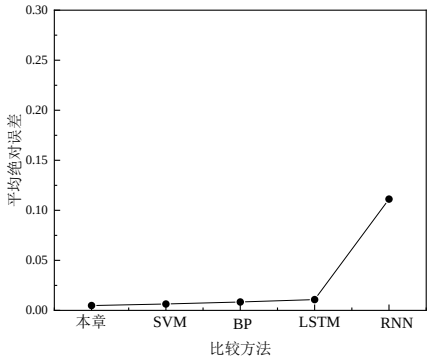
图 5.5 不同预警方法对比

图中所有的预警方式都具有一定的预测攻击能力，对工业互联网安全状态的基本趋势都能进行预测，但每一种预警方式对攻击的预测精确度却各不相同。其中，SVM 主要用于大样本的回归预测，因此其预警精确度并不十分精确，而 BP 神经网络又不能对情况序列的时间相关性进行捕捉，容易陷入局部最优状况，

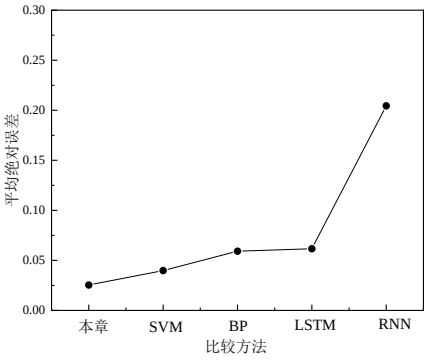
因此预警误差较大。而本章提出的 HMM 工业互联网安全态势预警技术具有最高的预警精度，从图中可以看到，每个预测点的预警值同实际值几乎完全重合。从而证明了 HMM 对于态势预警的积极作用。

5.4.2 预警时长

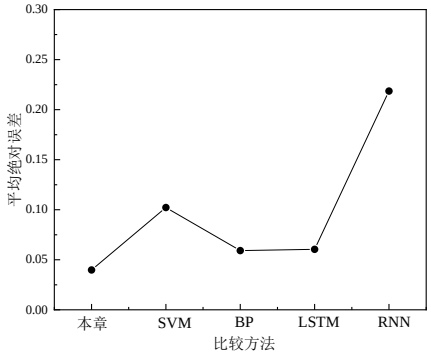
对于序列数据的预警不但需要考虑预警精度，还需要说明预警时长，因此需要在不同的预警时长上进行比较才更有意义。图 5.6 为不同预警方法在不同预警时长下的预警精度比较。所有方法在单步预警中的误差都是最小的，与多个时长的预警精度相比，随着时长的增加，预警误差也在逐渐加大，但在时长不变的情况下，本章的方法误差是最小的，而且随着预警时长的提高也是逐渐平滑的。比如在第五周的时候，本章方法的预警的平均绝对误差最低，相比于 SVM、BP、LSTM 以及 RNN 四种方法。说明本章建立的基于复合攻击的 HMM 态势预警模型具备一定的鲁棒性。证明了本章基于 HMM 的工业互联网安全态势预警技术的可行性和有效性。



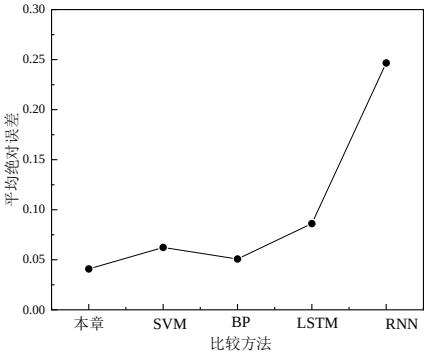
(a)第一周



(b)第五周



(c)第十周



(d)第十五周

图 5.6 不同时长的预警性能对比

5.5 本章小结

本章主要介绍工业互联网安全态势感知预警技术，首先将复合攻击建模方法与基于攻击意图的 HMM 相结合，建立了基于复合攻击的 HMM 态势预警模型提出工业互联网安全态势预警技术。主要对复合攻击的判别预测算法、攻击意图的识别以及攻击预测这三部分内容进行了深入的研究。其中，攻击预测有机地结合了 Forward 算法和经过改进的 Viterbi 算法，对下一步可能发生的攻击进行预测。

总结与展望

本文对工业互联网安全态势预警的相关技术进行了深入研究，分析了目前工业互联网安全态势预警模型的研究现状及面临的主要问题，主要完成的工作如下：

1. 针对现有的工业互联网安全态势预警模型仍然存在响应能力有限，在受到病毒攻击、网络攻击等手段的影响时，导致预警效果变差，引入统计信息网格，建立基于统计信息网格的工业互联网安全态势预警模型，阐述了该模型的基本架构，主要包括态势分析要素提取和态势预警两部分内容，并且概述了该模型的体系结构，利用 SIG 和 HMM 实时跟踪和监控工业系统异常行为，增强了异常监测能力，从而提高了该模型的安全性。

2.针对现有的工业互联网安全态势分析要素提取方法对多特征、高维度的非线性数据处理能力有限，导致其存在提取不精准、效率不高等问题。提出了基于降噪自编码器和改进随机森林的工业互联网安全态势分析要素提取方法。该方法在参考传统网络安全态势要素提取模型和提取方法的基础上，分析工业互联网安全现状，并建立工业互联网安全态势分析要素提取模型，利用 SDAE 通过一系列非线性变换对原始输入数据进行特征提取，利用 IRF 对基分类器进行筛选，然后采用加权多数投票的方式对原始随机森林算法进行改进，对降维后的数据进行分类训练从而得到最终分类结果，提高了态势分析要素提取方法的准确性。

3. 针对现有的态势预警技术主要集中在攻击行为上，而工业互联网复杂多变的环境导致这些态势预警技术无法准确检测网络安全状况并且不能及时发现工业互联网潜在威胁，使得基于攻击行为的态势预警技术在实现上存在一定的局限性。因此，结合复合攻击、攻击意图、隐马尔可夫模型，提出工业互联网安全态势预警技术。复合攻击判断，攻击意图辨识是重点中的重点。最终将两者结合起来，对入侵者下一步的攻击进行预测，从而在工业互联网安全态势预警方面取得成效。

本文主要研究工作是为了提高工业互联网系统的安全性，当然本文所提的基于 SIG 的工业互联网安全态势预警模型以及相关算法的应用也存在着一定的不足，下一步将从以下几个方面继续进行研究：

1. 本章提出的工业互联网安全态势预警模型中的聚类分析算法主要针对了攻击这一种安全事件来进行展开，下一步工作将考虑如何将其进行扩展，比如针对病毒的爆发，用户的误操作等方面。

2. 随着工业互联网数据类型的增加，态势分析要素提取模型的建立更加复杂，如何减少问题的复杂度，提出更加高效的态势分析要素提取算法将是未来研究工作的重点。

3. 本章的预警技术只是对下一步可能发生的攻击进行预测，为达到更加理想的预警效果，下一步研究工作应当基于所提出的预警模型，设计工业互联网安全态势预警系统，并实现其预警功能。

参考文献

[1] Abuhasel K A, Khan M A. A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing[J]. IEEE Access, 2020,8:117354-117364.

[2] Javaid M, Haleem A, Singh R P, et al. Upgrading the manufacturing sector via applications of industrial internet of things (IIoT)[J]. Sensors International, 2021,2: 100129.

[3] Guo H, Li J, Liu J, et al. A survey on space-air-ground-sea integrated network security in 6G[J]. IEEE Communications Surveys & Tutorials, 2021, 24(1): 53-87.

[4] Yang H, Cheng L, Chuah M C. Deep-learning-based network intrusion detection for SCADA systems[C].2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019: 1-7.

[5] Zhang D, Wang S. Optimization of traditional Snort intrusion detection system[C]IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2019, 569(4): 042041.

[6] Xu J, Han J, Qi Z, et al. A Reliable Traceability Model for Grain and Oil Quality Safety Based on Blockchain and Industrial Internet[J]. Sustainability, 2022, 14(22): 15144.

[7] 焦萍萍.大数据挖掘在船舶通信网络安全预警中的应用[J].舰船科学技术,2020,42(6):118-120.

[8] 张宁,范海涛.基于贝叶斯网络的信息安全预警模型[J].微型电脑应用,2022,38(6):135-138.

[9] Liu R. Early Warning Model of College Students' Psychological Crises Based on Big Data Mining and SEM[J]. International Journal of Information Technologies and Systems Approach (IJITSA), 2023, 16(2): 1-17.

[10] Shi C, Tan Y. A BP neural network-based early warning model for student performance in the context of big data[J]. Journal of Sensors, 2022,10:3-8.

[11] Cai J, Xiao D, Lv L, et al. An early warning model for vegetable pests based on multidimensional data[J]. Computers and Electronics in Agriculture, 2019(156): 217-

226.

[12] Sun M. A method for determining parameter weight early warning model based on reinforcement learning[J]. Computer Communications, 2020,157: 417-422.

[13] 王宏彬.基于模糊粗糙集和组合分类器的态势要素提取[D].[硕士论文].河北师范大学,2021.

[14] 曹鲁喆.基于深度学习的校园网络安全态势要素提取与评估方法研究[D].[硕士论文].中国人民公安大学,2021.

[15] 孙磊.基于随机森林的工控网络安全态势要素提取方法研究[D].[硕士论文].长春工业大学,2021.

[16] Duan Y, Li X, Yang X, et al. Network security situation factor extraction based on random forest of information gain[C].Proceedings of the 4th International Conference on Big Data and Computing. 2019: 194-197.

[17] 陶晓玲.基于深度学习的网络安全分域态势评估研究[D].[博士论文].桂林电子科技大学,2021.

[18] CUI A, WANG X. Real-time early warning of network security threats based on improved ant colony algorithm[C].2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA). IEEE, 2019: 309-316.

[19] Luo Y, Mo Y. Research on Dynamic Early Warning Methods of Internet of Things Based on Big Data Mining[C].2021 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS). IEEE, 2021: 145-150.

[20] Xu L, Ding L, Li Q, et al. Study on Risk Assessment and Early Warning Platform for Voltage Sag[C].IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2019, 490(7): 072043.

[21] Zhu B, Zhang L, Zhang Y. The early warning method of drug adverse reaction monitoring based on data mining algorithm was studied[C].Journal of Physics: Conference Series. IOP Publishing, 2021, 1852(3): 032052.

[22] Song X. Research on early warning method of major financial risk based on abnormal detection[C].2022 4th International Conference on Economic Management and Cultural Industry (ICEMCI 2022). Atlantis Press, 2022: 660-664.

[23] Mi H, Zheng Y. Binocular vision vehicle environment collision early warning method based on machine learning[J]. International Journal of Vehicle Information and

Communication Systems, 2020, 5(2): 219-230.

[24] Gupta M, Almomani O, Khasawneh A M, et al. Smart remote sensing network for early warning of disaster risks[M]Nanotechnology-Based Smart Remote Sensing Networks for Disaster Prevention. Elsevier, 2022: 303-324.

[25] Wu Y, Wang Z, Ma Y, et al. Deep reinforcement learning for blockchain in industrial IoT: A survey[J]. Computer Networks, 2021,191: 108004.

[26] Li Z, Liu F, Yang W, et al. A survey of convolutional neural networks: analysis, applications, and prospects[J]. IEEE transactions on neural networks and learning systems, 2021.

[27] Yu S, Li H, Chen X, et al. Multistability analysis of quaternion-valued neural networks with cosine activation functions[J]. Applied Mathematics and Computation, 2023,445: 127849.

[28] Das S, Wahi A. Digital Image Analysis Using Deep Learning Convolutional Neural Networks for Color Matching of Knitted Cotton Fabric[J]. Journal of Natural Fibers, 2022, 19(17): 15716-15722.

[29] Bao R, Sun Y. Top-N recommendation model based on SDAE[C].Journal of Physics: Conference Series. IOP Publishing, 2019, 1168(5): 052036.

[30] Dong Y, Zhang S, Xu J, et al. Random Forest Algorithm Based on Linear Privacy Budget Allocation[J]. Journal of Database Management (JDM), 2022, 33(2): 1-19.

[31] 张晴.基于隐马尔可夫模型的网络安全态势预测方法研究[D].[硕士论文].河北工业大学,2019.

[32] Ilhan F, Karaahmetoglu O, Balaban I, et al. Markovian RNN: an adaptive time series prediction network with HMM-based switching for nonstationary environments[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021,62:32-36.

[33] 罗逸涵,程杰仁,唐湘滟,欧明望,王天.基于自适应阈值的 DDoS 攻击态势预警模型[J].浙江大学学报(工学版),2020,54(4):704-711.

[34] Suo G, Guo R, Du J, et al. Construction of Hierarchical Network Security Situation Early Warning Model Based on Fuzzy Reasoning[C].2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019). Atlantis Press, 2019: 101-106.

[35] 邵宇航,朱小朋,王子良,等.面向 APT 攻击的航天信息网络安全预警模型研究[J].

网络安全技术与应用, 2021,11:14-16.

[36]赵志岩,纪小默.智能化网络安全威胁感知融合模型研究[J].信息网络安全, 2020 (4): 87-93.

[37]江志英,李宇洋,李佳桐,等.基于层次分析的长短记忆网络 (AHP-LSTM) 的食品安全网络舆情预警模型[J]. 北京化工大学学报 (自然科学版), 2021,48(6): 98.

[38]Yan Xiaoshen, Wang Yu. Clustering Analysis Algorithm of Volleyball Simulation Based on Radial Fuzzy Neural Network[J]. Computational intelligence and neuroscience,2022.

[39]Yu Z. Big data clustering analysis algorithm for internet of things based on K-means[J]. International Journal of Distributed Systems and Technologies (IJDST), 2019, 10(1): 1-12.

[40]Vani G, Hema A. Quantum Statistical Information Grid Clustering for Early Esophageal Adenocarcinoma Detection[J]. REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS, 2021, 11(4): 3170-3182.

[41]俞中华,杨晓东.基于深度自编码网络的网络安全态势感知与预警机制[J].广播电视网络,2020,27(6):63-65.

[42]Ko K, Koh Y J, Kim C S. Blind and compact denoising network based on noise order learning[J]. IEEE Transactions on Image Processing, 2022(31): 1657-1670.

[43]Aouedi O, Piamrat K, Bagadthey D. A semi-supervised stacked autoencoder approach for network traffic classification[C].2020 IEEE 28th International Conference on Network Protocols (ICNP). IEEE, 2020: 1-6.

[44]C. Chun, K. M. Jeon, T. Kim, et al. Drone Noise Reduction using Deep Convolutional Autoencoder for UAV Acoustic Sensor Networks,2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), 2019:168-169.

[45]丁红卫,万良,龙廷艳.深度自编码网络在入侵检测中的应用研究[J].哈尔滨工业大学学报 ,2019,51(5):185-194

[46]Kim H, Lee T. Research on Autoencdoer Technology for Malware Feature Purification[C].2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel Distributed Computing (SNPD-Winter). IEEE, 2021: 236-239.

[47] Mishra S, Mallick R K, Gadanayak D A. Islanding detection of microgrid using EMD and random forest classifier[C].2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE). IEEE, 2020: 1-5.

[48] Miah M O, Khan S S, Shatabda S, et al. Improving detection accuracy for imbalanced network intrusion classification using cluster-based under-sampling with random forests[C].2019 1st international conference on advances in science, engineering and robotics technology (ICASERT). IEEE, 2019: 1-5.

[49] Lu T, Huang Y, Zhao W, et al. The metering automation system based intrusion detection using random forest classifier with smote+ enn[C].2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT). IEEE, 2019: 370-374.

[50] Liu Y, Liu L, Gao Y, et al. An improved random forest algorithm based on attribute compatibility[C].2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2019: 2558-2561.

[51] Dong R H, Shui Y L, Zhang Q Y. Intrusion Detection Model Based on Feature Selection and Random Forest[J]. International Journal of Network Security, 2021, 23(6): 985-996.

[52] Wang W, Bai B, Wang Y, et al. Bitstream protocol classification mechanism based on feature extraction[C].2019 International conference on networking and network applications (NaNA). IEEE, 2019: 241-246.

[53] Liu D, Yu H, Wang W, et al. Multi-source Log Comprehensive Feature Extraction Method Based on Restricted Boltzmann Machine in Power Information System[C].2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN). IEEE, 2019: 503-508.

[54] Na G S, Chang H. Unsupervised Subspace Extraction via Deep Kernelized Clustering[J]. ACM Transactions on Knowledge Discovery from Data (TKDD), 2021, 16(1): 1-15.

[55] 罗逸涵,程杰仁,唐湘滟,等.基于自适应阈值的 DDoS 攻击态势预警模型[J]. 浙江大学学报(工学版), 2020, 54(4): 704-711.

[56] Luo Y, Mo Y. Research on Dynamic Early Warning Methods of Internet of Things

Based on Big Data Mining[C].2021 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS). IEEE, 2021: 145-150.

[57]陈晓军,姚浩浩,王月领,等.基于 DNS 日志的恶意域名态势预警研究[J]. 信息技术与信息化, 2021,07:99-101.

[58]王跃,武茂浦,刘鑫宇等.船舶工控网络安全态势监测预警关键技术研究[J].科技和产业,2022,22(9):330-334.

[59]Long Y, Huang S, Peng L, et al. Internal and External Defects Discrimination of Pipelines Using Composite Magnetic Flux Leakage Detection[C].2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). IEEE, 2021: 1-6.

[60]Khattak A, Habib A, Asghar M Z, et al. Applying deep neural networks for user intention identification[J]. Soft Computing, 2021,25: 2191-2220.

[61]Du G, Liu Z, Lu H. Application of innovative risk early warning mode under big data technology in Internet credit financial risk assessment[J]. Journal of Computational and Applied Mathematics, 2021,386: 113260.

[62]王其文.面向多源数据融合的网络攻击预警技术研究[D].[博士论文].中国科学院大学,2021.

[63]吴璐瑶.天然气管道泄漏的数值模拟与预警技术研究[D].[硕士论文].安徽理工大学,2019.

[64]郑贤斌,周锡河,郭志红,等.基于风险分析和 GIS 的油气管道安全预警技术研究[J]. 石油规划设计, 2019, 18(1): 6-9.

[65]Sajjad M, Khan Z A, Ullah A, et al. A novel CNN-GRU-based hybrid approach for short-term residential load forecasting[J]. Ieee Access, 2020, 8: 143759-143768.

[66]Munkhdalai L, Munkhdalai T, Park K H, et al. An end-to-end adaptive input selection with dynamic weights for forecasting multivariate time series[J]. IEEE Access, 2019, 7: 99099-99114.