2023 IEEE 第二届电气工程，大数据和算法国际会议(EEBDA) - 978-1-6654-6253-2/23/$31.00©2023 IEEE - DOI: 10.1109 / EEBDA56825.2023.10090710

基于计算机人工智能技术的网络信息安全模型研究

秦文君肖*
北京工业大学珠海分校
中国广东省珠海市
02062@bitzh.edu.cn

李易峰北京工业大学珠海分校
广东省珠海市
中国省
l13829828383@126.com

北京工业大学珠海分校
广东省珠海市
中国省
tianyan2022@126.com

利华国际李
北京工业大学珠海分校
中国广东省珠海市
02062@bitzh.edu.cn

***摘要*提出了一种基于粗糙集理论的 DDoS 攻击安全评估方法。 实现了对安全威胁的实时定量评估。以 FTGUI-20003-1B 处理器和预警信号灯为例，设计了网络通信预警系统的硬件结构。本文引入传感器技术来获取通信网络的状态特征。引入粗糙集理论对网络安全状态进行识别。它将通信网络链路划分为由多个节点组成的通信通道，并识别通信网络的安全状态。仿真结果表明，该方法的入侵检测能力强，安全检测的可靠性和稳定性好。**

关键词:计算机，人工智能，网络信息安全，粗糙集算法，态势感知

I. 介绍

近年来，随着威胁网络安全事件的频繁发生，大量计算机受到病毒、木马的入侵，计算机网络安全面临严峻挑战，网络安全形势不容乐观。为了增强计算机网络的安全防护能力，网络管理者虽然通过安装入侵检测系统、防火墙、杀毒软件等措施来构筑一道安全防线，但随着网络复杂性和不确定性的增加，这些防护单元只是被动地或以某种方式用单一的方法进行隔离防护，而不能协同工作，很难在大规模网络中产生良好的防护效果;同时，在防护过程中不断产生大量的安全日志和告警信息，使得管理人员无法快速高效地分析网络安全的重要变化，也无法预测未来的攻击和潜在威胁[1]。如何在动态复杂的网络环境下将被动的网络安全防护转变为主动的网络安全防护，从而快速有效地分析和评估网络安全的变化，是未来网络安全研究的重点。以粗糙集为分析工具，对空中交通管制安全风险进行整理总结，并对预警指标的选择进行优化基于粗糙集的属性约简，从而降低主观性，提高预警精度。

II. 网络信息安全系统设计

A. 硬件设计

为了满足系统的高性能运行要求，本次设计选用的处理器型号为 FTGUI-20003-1B，是第 12 代 Intel 酷睿的衍生版本。其结构、综合性能和能效均明显优于早期版本，在实际应用中可实现多路径任务的协同处理。该处理器集成了一个特殊的人工智能引擎，具有>14.0 的核心硬件线程。当它与 Windows11 操作系统连接时，可以在任务处理过程中实现动态任务的均衡处理和负载，保证运行中的高效率和低耗能。在 FTGUI- 20003-1B 处理器现有组件的基础上，内置 AI 加速芯片，保证处理器能够及时处理多链路网络通信数据，即使数据链路传输信息超出其预期，也可以避免处理器过载[2]。为了满足系统的预警要求，通常选用阻值较大的指示电阻，以保证通过预警信号灯的电流保持在小的状态。通常情况下警示灯是由灯座、灯罩、灯具、线路等元件连接而成，信号由 led 等组成，需要与前端 TG - 200 传感器通信连接，并放置在仪表板明显等位置，以确保警示灯在使用中能够起到或警示作用。

B. 软件设计

在硬件设备的支持下，引入传感器技术获取通信网络的状态特征。在此过程中，需要保证所获得的状态信息具有高质量的特点。只有满足这一特征，才能保证后续通信网络异常预警的可靠性。目前，有许多技术可用于提取其

978-1-6654-6253-2/23/$31.00©2023 ieee

状态信息，其中大多数在应用中可能有一定的干扰。然而，传感器技术
本文所选取的算法可以剔除一些无效的
状态信息和冗余信息
信息在最初的收集阶段，即使收集到的信息仍然不可避免地带有噪声
信息。但是，这部分信息也可以在后续处理中解决[3]。因此，在初步获取状态信息后

基于传感器技术的通信网络，有必要通过状态划分来描述其特性
网络安全与网络安全的等级。本研究采用了粗糙集算法。

模糊集理论和粗糙集理论是经典集合理论在处理不确定性和不精确问题方面的扩展。两种理论的比较与融合一直是一个有趣的话题。
假设(U, *R)* 是近似空间，R 是
在 U 域上的等价关系，则 F 是一个模糊集
∝*F*∈ *ℱ(U)*上下近似
*空间*上*模*糊集*F 的*aprR (F)和 aprR (F)
(U, R)*是*一对模糊集:

$$\overline{apr}_R(F)(x) = \sup_{y\in U}\{\min[\mu_F(y), \mu_R(x,y)]\} \quad (r-f)\ (1)$$

$$\underline{apr}_R(F)(x) = \inf_{y\in U}\{\max[1-\mu_F(y), \mu_R(x,y)]\}$$

(aprR *(F)*, *aprR (F))称*为 *u* 上模糊集 F 的粗糙模糊集。rough - fuzzy 模型将近似对象从清晰集 X 扩展到模糊集 F。

如果将等价关系 R 进一步推广为模糊相似关系 R，则存在一个模糊相似关系
近似空间(U,R)。∝*F*∈ *(ω)* ，上部
下近似 *aprR (F)* 和 *apr* (F)
空间(U,R)上的模糊集 *F* 是一对模糊集:

$$\overline{apr}_R(F)(x) = \sup_{y\in U}\{\min[\mu_F(y), \mu_R(x,y)]\} \quad (f-r)\ (2)$$

$$\underline{apr}_R(F)(x) = \inf_{y\in U}\{\max[1-\mu_F(y), \mu_R(x,y)]\}。$$

(4 *月* (F), aprR (F))*称为*的模糊粗糙集
模糊粗糙模型不仅将近似对象从清晰集 X 扩展到模糊集 F，而且将理论域上的等价关系 R 扩展到模糊相似关系 R。

从公式(R-F) (F-R)很明显，粗糙
模糊集是模糊粗糙集的一种特殊情况。经典粗糙集也是粗糙模糊集的一种特殊情况，其近似对象是清晰集。为了更好地理解这个结论，让我们看一下粗糙集的另一个定义。

如前所述，粗糙集由上下近似描述，有时称为粗糙集的弱-强成员函数。使用
$\mu_{\overline{XR}}$ ，$\mu_{\underline{XR}}$表示 X 和 R 的成员函数，请注意
集合描述的特征函数表示(即: $\mu_X(y) = 1$，如果 y ∈X。

上述方程也是一对模糊集。由式(R)和(R-f)可知，当近似对象为清晰集 x 时，经典粗糙集显然是粗糙模糊集的一种特殊情况。由于粗糙集、粗糙模糊集和模糊粗糙集都是模糊集，那么它们一定可以用-切集的形式表示

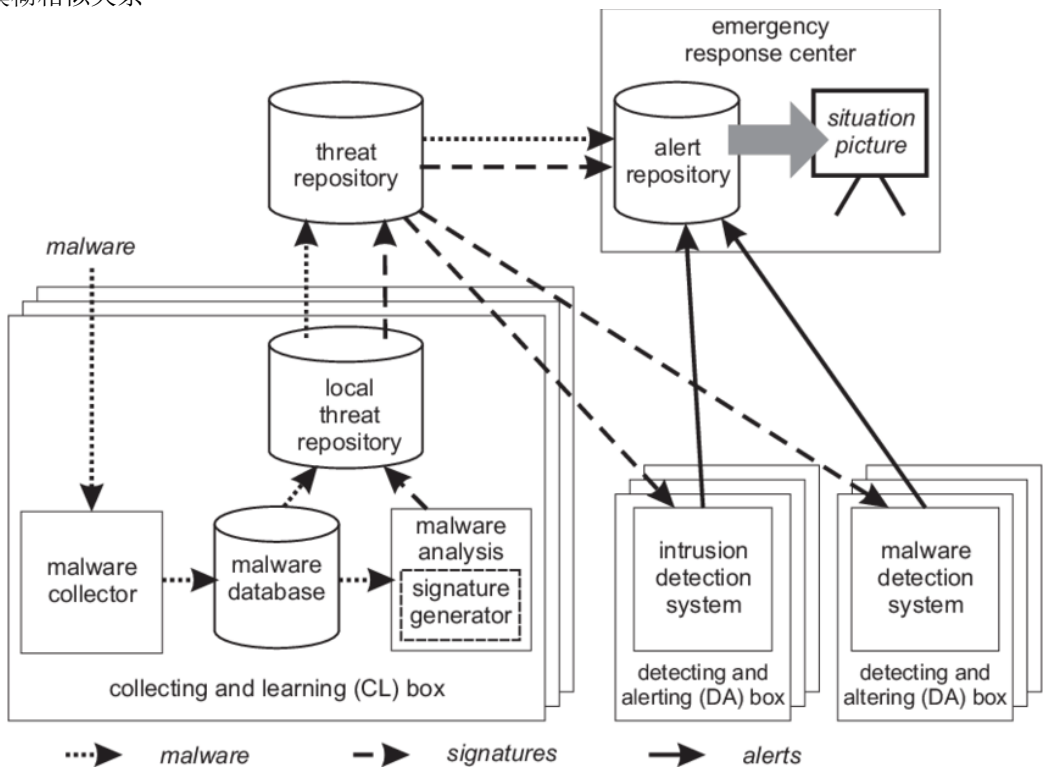


图 1 所示。通信网络异常及报警过程

III. 建立通信网络异常预警机制

在完成上述设计后，建立通信网络异常预警机制，进行通信网络异常预警。异常和早期预警过程如图 1 所示。

按照上图 1 所示的流程进行通信网络异常预警。当通信网络异常和风险被识别后，需要提取风险信息，并且通过细化风险信息来划分预警级别和类别。网络安全态势架构的建立是网络安全态势技术应用的关键，直接影响网络安全态势系统性能的应用效果[4]。本文将 JDL 模型与 Endsley 给出的网络安全态势感知模型相结合，对体系结构组件之间的关联管理进行定量研究，设计了网络安全态势感知的系统框架，如图 2 所示。系统结构以层次化结构为主，直观简单。

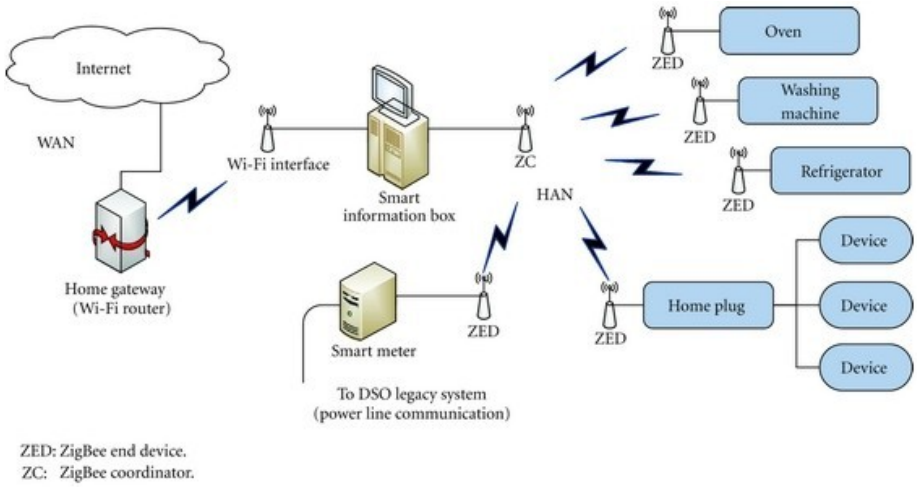


图 2 所示。网络安全架构

A. 原始数据的采集和预处理

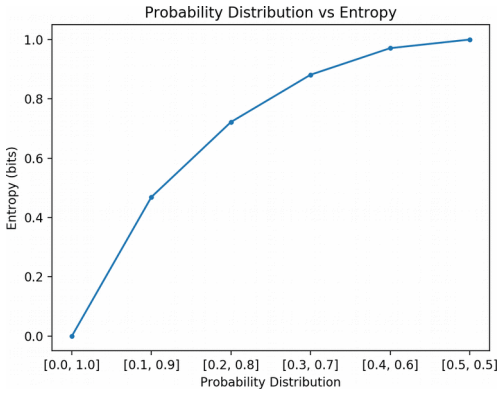
网络安全态势感知系统收集分布在网络系统中的各种网络防护软件(如防火墙、入侵检测系统、杀毒软件等)的各种相关日志数据。然而，这些数据中含有大量冗余数据、错误和虚警信息，且数据格式不同，不可能直接利用这些数据进行信息挖掘和分析[5]。预处理技术应筛选和减少来自不同软件的不同数据信息，并对异构数据格式的数据进行统一转换和存储，为未来的安全评估和预警做好数据准备。

B. 事件关联

数据融合与挖掘技术是对采集到的数据进行关联分析，剔除冗余的数据信息，提取并整合对网络安全构成威胁的关联数据信息。

C. 响应和警告

根据网络安全形势的态势结果，不仅对即将发生的网络安全事件进行响应和防御措施，相应地实现主动防御的功能，而且还通过对网络安全态势感知历史和当前网络安全态势感知数据的对比和分析，得出安全态势分析的趋势



对形势进行预测，为今后的网络安全管理提供决策和参考。

D. 网络安全态势可视化

传统的文本数据形式不能直接、清晰地向用户反馈网络安全状况结果。网络安全态势系统通过可视化显示功能，将大量抽象枯燥的当前网络安全态势数据以动态图形的形式显示出来，方便用户查看，提高了数据显示的可见性和直观性。

IV. 系统检查

图 3 为企业信息化网络传输的样例信息。选取前 200 个采样点，进行 300 次蒙特卡罗实验，防御企业信息化的网络安全[6]。采用最小二乘法和深度卷积神经方法作为实验对比方法，得到病毒入侵信息的检测输出，如图 4 所示。

由图 4 分析可知，最小二乘法对企业信息化网络安全防御检测的输出频率波动较大，主要在-20 ~ 10MHz 之间，而深度卷积神经方法的输出频率主要在 -10 ~ 10MHz 之间，波动较大[7]。采用该方法进行的企业信息网络安全防御检测输出频率稳定在

约 0MHz，稳定性高。由此可见，本文提出的方法可以实现企业信息化网络安全防御系统的稳定运行。在此基础上，测试了三种病毒入侵检测方法的准确率，对比结果如图 5 所示。

图 3 所示。网络传输企业信息化信息

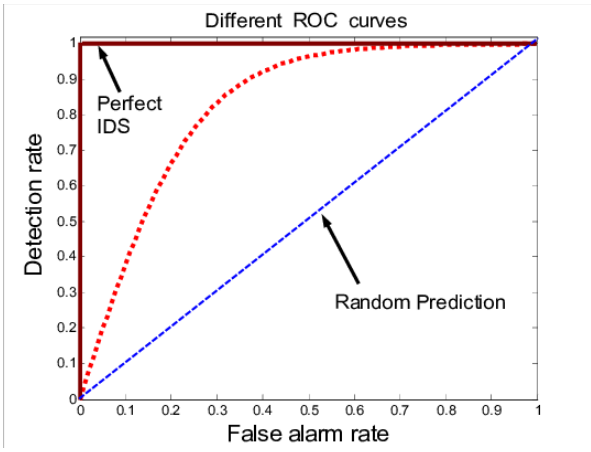


图 4 所示。输出企业信息网络病毒入侵检测

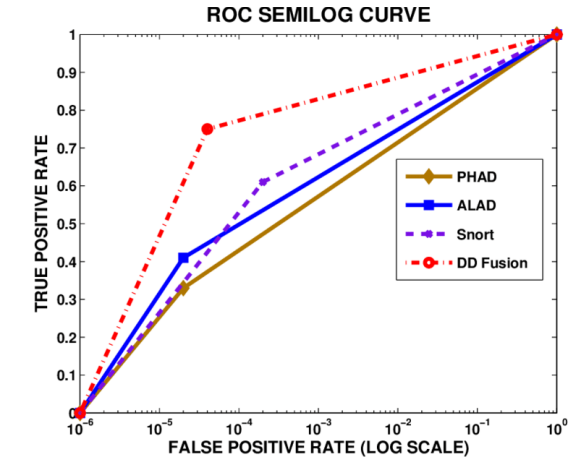


图 5 所示。病毒入侵检测的准确性测试

由图 5 的分析可知，最小二乘法的平均检测准确率为 79%，深度卷积神经方法的平均检测准确率为 75%，本文提出的方法对于企业信息化网络安全防御的平均检测准确率为 96%。 本文提出的方法能够有效检测企业信息网络的病毒入侵，有效提高企业信息网络的安全防御能力。

V. 结论

本文介绍了粗糙集算法应用于 DDoS 攻击的威胁

该程度评估方法可以实时合理地评估系统的安全威胁状态，当攻击开始时，情况值迅速上升，起到及时报警的作用。实证分析表明，该方法的计算结果是准确的，但最小二乘支持向量机模型的精度和性能与运行参数的选择高度相关，以进一步提高算法的精度和运行速度。

确认

本文的研究是省重点平台和广东省高校重大科研项目(No.2021ZDZX3004)资助的。

参考文献

[1] 任正非加威。计算机网络信息安全风险层次分析模型研究。《焊接学报》，第 43 卷，第 49- 51 页，2020 年 9 月。

[2] 张欣，董黎明。基于攻防博弈模型的网络节点信息安全定量仿真。计算机仿真，vol. 037, pp. 18-21,98, 2020 年 6 月。

[3] 连文娟，赵多多，范秀彬。基于 CFL_BLP 模型的 CFL SSL 协议。计算机工程，第 47 卷，第 120- 124 页，2021 年 6 月。

[4] 通 Changwei。计算机网络安全及其防范措施。《经济学》，第三卷，第 25-32 页，2020 年 2 月。

[5] 颜瑞铵，张丽辰。基于焦点损失和卷积神经网络的入侵检测。计算机与现代化，第 7 卷，第 55-61 页，2021 年 1 月。

[6] 刘玉洲，方贤文。基于博弈策略的攻防模型有效变异域验证算法。计算机应用研究，vol. 39, pp. 69-75, 2022 年 7 月。

[7] 张宁，范海涛。基于贝叶斯网络的信息安全预警模型。微型计算机应用，第 44 卷，第 38-44 页，2022 年 6 月。