

基于门控循环单元的信息安全 态势感知系统设计

朱志猛[†]

(中关村硬创空间集团有限公司,北京 100000)

摘 要:随着互联网技术的快速发展,网络在深刻影响了社会生活和生产方式的同时也带来了严峻的信息安全挑战。针对日益复杂的网络攻击带来的信息安全问题,对基于门控循环单元的信息安全态势感知系统进行了分析,设计了基于自适应增强算法和双层门控循环单元的信息安全态势感知模型。结果表明,基于双层门控循环单元的信息安全态势感知模型攻击识别准确率提升至94.01%。在误报率、误警率和漏报率指标上也具有较好的表现,分别为8.35%、5.75%和3.14%。此外,所提模型对于不同类别的网络攻击的识别正确率均较高,且具有较好的信息安全态势感知性能。研究设计的基于门控循环单元的信息安全态势感知模型能够较好地应对复杂多变的网络攻击,对于保护网络信息安全具有一定的应用效果。

关键词:态势感知;信息安全;门控循环单元;自适应增强算法;网络流量探测器

中图分类号:TP393

文献标识码:A

Design of Information Security Situation Awareness System Based on Gated Recurrent Unit

ZHU Zhimeng[†]

(Zhongguancun Hardware Space Group Co., Ltd., Beijing 100000, China)

Abstract: With the rapid development of Internet technology, the network has deeply affected the social life and production mode, but also brought severe information security challenges. In response to the increasingly complex information security issues caused by network attacks, this study analyzed the information security situation awareness system based on gated loop units, and designed an information security situation awareness model based on adaptive enhancement algorithms and double-layer gated loop units. The results show that the attack recognition accuracy of the information security situational awareness model based on double-layer gated loop units has been improved to 94.01%. It also performs well in the indicators of false alarm rate, false alarm rate, and false alarm rate, with values of 8.35%, 5.75%, and 3.14%, respectively. In addition, the proposed model has high recognition accuracy for different types of network attacks and has good information security situational awareness performance. The information security situational awareness model based on gated loop units designed in the research can effectively cope with complex and ever-changing network attacks, and has certain application effects in protecting network information security.

Key words: situation awareness; information security; gate control loop unit; adaptive enhancement algorithm; network traffic detector

随着互联网应用的日益广泛,信息传播的地域限制和时间限制被打破,极大地改变了人们的生活和生产模式。但与此同时,网络攻击也变得越来越复杂多变,为用户的信息安全保护带来了严峻挑战。许多学者对信息安全进行了大量的研究。李伟等针对警务云安全数据的识别和分类问题,利用一维卷积神经网络来对数据进行特征学习和重构,并对 D-S 证据理论进行了改进,以提高安全事件的报警识别率^[1]。谢凯等针对网络安全态势感知问题,设计了一种基于决策树算法的联级网络安全态势感知模型。结果表明,所提模型具有较高的感知准确率和效率^[2]。查德平等为提高网络的安全威胁防范能力,从威胁情报应用角度出发构建了网络威胁情报系统。结果表明,所提方法只存在最大为 0.2 节点密度的误差^[3]。赵冬梅等针对网络安全态势预测准确率较低的问题,引入门控循环单元(Gated Recurrent Unit, GRU)和 Transformer 来搭建网络安全态势预测模型。结果表明,该模型具有较高的预测准确率和效率^[4]。综上所述,尽管有很多学者对信息安全进行了大量的研究,但目前的网络信息安全形势仍然不容乐观,信息泄露的事件频发。在这一背景下,将设计基于自适应增强(Adaptive Boosting, Adaboost)算法和 GRU 的信息安全态势感知模型。研究的创新点在于结合 Adaboost 算法和双层 GRU 设计信息安全态势感知系统,并采用层次化分析方法进行信息安全态势评估。

1 基于 GRU 的信息安全态势感知系统

1.1 基于双层 GRU 的信息安全态势感知模型搭建

为提高模型对网络攻击进行识别的准确性,研究从时间维度出发,对网络流量数据中的时间特征进行分析。因此,研究采用具有较强的时间长序列处理能力的 GRU 搭建态势感知模型。在进行信息安全态势感知之前,要先对原始流量信息进行预处理。数据预处理能够为后续的网络数据挖掘工作提供可靠和高质量的数据,便于计算机的运算。首先,通过在网络中部署网络探测器来进行流量探测,现有的网络探测器分为网络流量探测器和入侵检测探测器^[5]。研究采用性能损耗较小,且能够对网络数据进行高精度监测的 Tranalyzer 网络流量探测器来进行流量探测。然后,研究选择一位有效编码和最大-最小归一化来对 N 个状态进行编

码,并将数据缩放到一个给定的范围。最后,融合不同探测器的探测结果,得到信息安全态势感知模型的输入。

在完成了对数据的预处理后,研究利用 GRU 来挖掘网络流量的时间信息。GRU 是循环神经网络的一种变体,旨在解决传统循环神经网络中存在的长依赖和梯度问题。GRU 有重置门和更新门两个门,且相较于传统的循环神经网络而言参数较少,具有更强的记忆能力和运行效率,具体结构如图 1 所示。

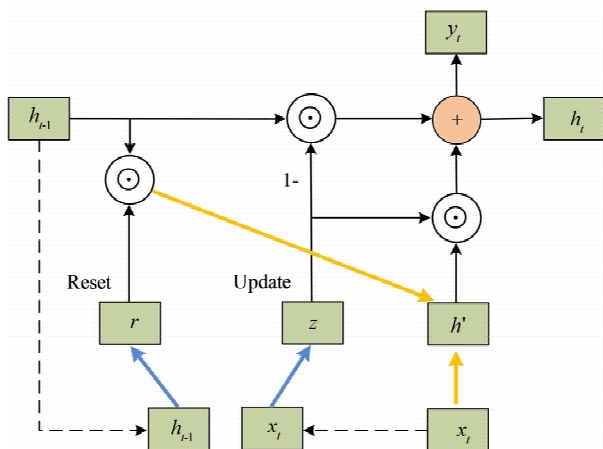


图 1 GRU 的结构图

GRU 的原理与长短时记忆网络类似,即用门控机制控制输入、记忆等信息而在当前时间步做出预测。GRU 有更新门和重置门两个门,其中更新门决定了前一时刻的状态信息的更新和丢弃,用于控制前一时刻的状态信息被带到当前状态中的程度。重置门决定了前一时刻状态信息的写入,即如何将新的输入信息与前面的信息相结合^[8]。更新门 z_t 和重置门 r_t 的计算如式(1)所示。

$$\begin{cases} z_t = \sigma(W_z \cdot [h_{t-1}, x_t]) \\ r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \end{cases} \quad (1)$$

式中, σ 表示 sigmoid 激活函数, W_z 表示更新门的权重矩阵, x_t 表示第 t 个时间步的输入向量, h_{t-1} 表示第 $t-1$ 个时间步的隐藏状态, W_r 表示重置门的权重矩阵。当前的流量记忆信息 $\tilde{h}_t$ 如式(2)所示。

$$\tilde{h}_t = \tanh(W_{\tilde{h}} \cdot [r_t * h_{t-1}, x_t]) \quad (2)$$

式中, $\tanh$ 表示非线性激活函数, $W_{\tilde{h}}$ 表示候选状态的权重矩阵。隐藏状态 h_t 的计算如式(3)所示。

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t \quad (3)$$

整个双层 GRU 网络的训练流程分为前向传播和反向传播两个部分。反向传播计算不同神经元间误差并更新权重和偏置。在前向传播中,将 k

个时刻的样本输入到神经元中,并计算该时刻真实值与预测值之间的误差。随后,为进一步提升模型对于各种网络攻击的识别准确率,研究利用 Ada-boost 算法来更新样本的权值,计算攻击识别模型的权重。Adaboost 算法是一种集成式机器学习方法,通过迭代更新权重将一定数量的弱分类器集合形成强分类器,并通过深挖弱分类器的性能减少误差率^[6]。首先,对训练集 $S = \{(x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)\}$ 中的各个样本的权值进行初始化,赋予相同的权值 w_m, i , 如式(4)所示。

$$w_m, i = \frac{1}{n}, \quad i = 1, 2, \dots, n \tag{4}$$

使所有样本的初始权值为相同数值。然后,训练弱分类器。计算误差率来衡量弱分类器在此次分类中的加权错误率,每次选择误差率最低的分类器加入最终线性分类器中。更新各个样本的权重,具体而言,降低被准确分类的样本点的权重,提高没有被准确分类的样本点的权重。最后,将训练得到的多个弱分类器组合为强分类器 $f(x)$, 如式(5)所示。

$$f(x) = \sum_{i=1}^T \alpha_i h_i(x) \tag{5}$$

式中, T 表示弱分类器的数量, α_i 表示第 t 个弱分类器在强分类器中所占权重的数值, $h_i(x)$ 表示样本 x 的第 t 个弱分类器。综上所述,研究设计的 Adaboost-GRU 算法的流程如图 2 所示。

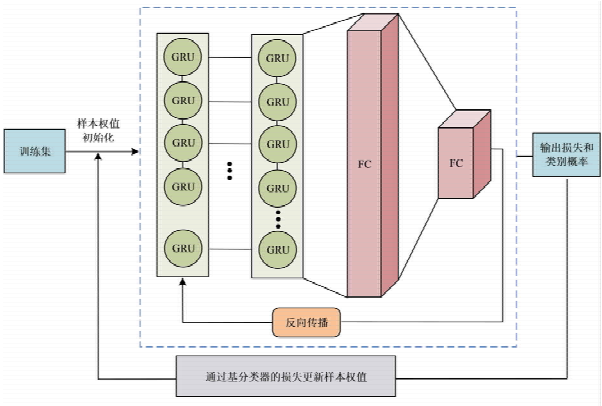


图2 Adaboost-GRU 算法的流程

1.2 信息安全态势评估模块

对信息安全态势进行评估是安全态势感知任务中的重难点和关键环节,是指通过对设备产生的安全事件进行过滤、汇总和关联分析,建立合适的数学模型来评估网络系统在整体上遭受安全威胁的程度,从而全面掌握网络整体的安全状况。通过

信息安全态势评估可以尽早地发现网络中的安全隐患和威胁,向网络安全管理人员提供直接的网络状况判断依据,进而采取有效的应对措施^[9]。研究采用层次化分析方法来计算网络的安全态势值,构建安全态势感知模型中的态势评估模块^[10]。层次化分析方法能够从网络的不同层次对网络安全状况进行分析,因此能够提供更加细致准确的网络安全信息。威胁等级量化是风险评价和权重分配的基础,研究采用权系数理论来对攻击的威胁等级进行量化,权系数 W_i 如式(6)所示。

$$W_i = \begin{cases} \frac{1}{2} + \frac{\sqrt{-2\ln \frac{2i}{n}}}{6}, & 1 \leq i \leq \frac{n}{2} \\ \frac{1}{2}, & i = \frac{n}{2} \\ \frac{1}{2} - \frac{\sqrt{-2\ln \frac{2i}{n}}}{6}, & \frac{n}{2} < i < n \end{cases} \tag{6}$$

式中, n 表示威胁等级的个数, i 表示威胁等级的排列顺序。研究采用层次化分析方法来进行安全态势评估,层次化分析方法将网络分为网络层、主机层和服务层,具体结构如图 3 所示。

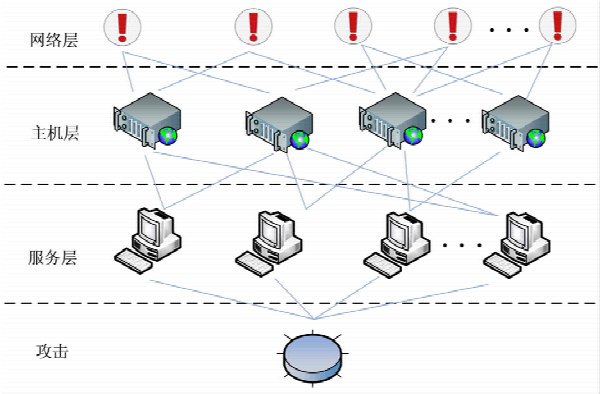


图3 层次化分析方法的架构图

网络层态势通过评估该区域边界防护措施的有效性进行确定,网络态势值 $N(t)$ 的计算如式(7)所示。

$$N(t) = f(\mathbf{H}(t), \mathbf{W}(t)) = \mathbf{H}(t) \cdot \mathbf{W}(t) \tag{7}$$

式中, $\mathbf{H}(t)$ 表示 n 个主机态势生成的向量, $\mathbf{W}(t)$ 表示 n 个主机的权值向量。主机发生网络攻击事件所带来的威胁即为该主机所有端口发生网络攻击事件的威胁总和。主机层态势值 $h_k(t)$ 与受到的威胁程度成正比,能够体现主机的安全状态,其计算如式(8)所示。

$$h_k(t) = f(\mathbf{S}_k(t), \mathbf{V}(t)) = \mathbf{S}_k(t) \cdot \mathbf{V}(t) \tag{8}$$

式中, $\mathbf{S}_k(t)$ 表示第 k 个主机上 m 个服务器的态势值向量, $\mathbf{V}(t)$ 表示 m 个服务器的权值向量。

由此可知,服务态势和服务重要性影响决定了主机层态势。主机的权值向量 $\tau w_k(t)$ 的计算如式(9)所示。

$$\tau w_k(t) = \frac{h_{u_k} h_{f_k}}{\sum_{k=1}^n h_{u_k} h_{f_k}} \quad (9)$$

式中, h_{u_k} 表示主机 k 上的用户数量, h_{f_k} 表示主机 k 的使用频率。服务层态势能够体现服务的安全状态,呈动态变化。服务层态势的评估以端口作为单位,首先考虑威胁因素,即在该端口上发生的攻击的影响力和数量。然后考虑脆弱性,即在该端口上发生攻击事件的频率。服务层态势值 $S_{kj}(t)$ 的计算如式(10)所示。

$$S_{kj}(t) = \sum_{i=1}^l p(\text{attacki}) \cdot 10^{f(\text{attacki})} \quad (10)$$

式中, $p(\text{attacki})$ 和 $f(\text{attacki})$ 分别表示第 i 条攻击发生的概率和威胁值, l 表示第 j 类服务在第 t 个时间窗口上遭受攻击的总数。服务权重 $v_{kj}(t)$ 的计算如式(11)所示。

$$v_{kj}(t) = \frac{su_{kj} s f_{kj}}{\sum_{j=1}^m su_{kj} s f_{kj}} \quad (11)$$

式中, su_{kj} 和 $s f_{kj}$ 分别表示主机 k 启用第 j 类服务的用户数量和使用频率, m 表示服务的数量。为了更好地衡量所提算法对攻击的识别性能,研究选取准确率(Accuracy)、漏报率(False Negative Rate, FNR)、误报率(False Positive Rate, FPR)和误警率(False Alarm Rate, FAR)作为评价指标^[11-12]。准确率是指预测正确的样本数量占总量的百分比。FNR 是预测错误的阳性样本在实际阳性样本中的占比。FPR 是阴性样品中被分类器预测为正样本的比例,反映了检测方法或诊断系统的准确性。FAR 是指被错误地判断为正样本的比例,表示系统中错误地触发报警的概率。四种指标的计算如式(12)所示。

$$\begin{cases} \text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \\ \text{FNR} = \frac{\text{FN}}{\text{FN} + \text{TP}} \\ \text{FPR} = \frac{\text{FP}}{\text{TN} + \text{FP}} \\ \text{FAR} = \frac{\text{FPR} + \text{FNR}}{2} \end{cases} \quad (12)$$

式中, FN 表示假阴性, FP 表示假阳性, TN 表示真阴性, TP 表示真阳性。综上所述,为保障信息安全,研究设计了基于 Adaboost-GRU 的信息安全态势感知模型,并采用层次化分析方法进行信息安全态势评估,实现服务态势、主机态势和网络态势的可视化。

2 基于 GRU 的信息安全态势感知系统有效性分析

为验证所提信息安全态势感知模型的有效性,研究使用 Linux 操作系统,采用 UNSW-NB15 数据集进行实验。首先在系统中部署流量探测器进行探测,并将预处理后的数据经过采样处理后作为所提算法决策集成模块的输入。将 GRU 网络层数设置为 2,将隐藏层神经元个数设置为 256,选取 5 个基学习器。并传统的 D-S 证据理论、基于决策树算法的联级网络安全态势感知模型和基于威胁情报的网络安全态势感知模型进行对比^[13-14]。四种方法的指标对比结果如图 4 所示。从图 4(a)中可以看出,所提 Adaboost-GRU 算法在准确率方面的表现最好,准确率为 94.01%。其次是基于决策树算法的联级网络安全态势感知模型,准确率为 93.51%,D-S 证据理论的表现最差。从图 4(b)中可以看出,Adaboost-GRU 算法的 FPR 值最小,为 8.35%。从图 4(c)中可以看出,Adaboost-GRU 算法的 FAR 值最小,为 5.75%。从图 4(d)中可以看出,Adaboost-GRU 算法的 FNR 值最小,为 3.14%。结果表明,研究所提 Adaboost-GRU 算法在准确率、FPR、FAR 和 FNR 四种指标上均具有较好的表现,具有一定的可行性和优越性。

为进一步验证所提信息安全态势感知模型的攻击识别性能,进一步分析所提算法与基于决策树算法的联级网络安全态势感知模型对于不同攻击的识别正确率。结果如图 5 所示。从图 5 中可以看出,除了在 Exploits、Fuzzers 和 Shellcode 三种攻击上 Adaboost-GRU 算法的识别正确率略低于基于决策树算法的联级网络安全态势感知模型以外,其余类别的攻击均是 Adaboost-GRU 算法的识别正确率更高。结果表明,所提 Adaboost-GRU 算法的攻击识别正确率在整体上的表现更好,对于不同攻击的识别正确率均较高,具有较好的攻击识别性能。

为验证所提算法的实际应用效果,研究分别选取了 IP 为 117.176.24.12(host1),117.176.24.13(host2)和 117.176.24.14(host3)的 3 台主机为研究对象进行安全态势分析。服务层态势选取了 DNS、HTTP 和 SMTP 三种服务类型进行展示。以 5 min 为一个时间窗口,在网络的第 11 个时间窗口设置一次较大的网络攻击,在第 46 个时间窗口设置一次中等的网络攻击。在 host1 的第 8 个时间窗口设置一次较大的网络攻击,对 host2 给予三次中等的网络攻击,在 host3 的第 46 个时间窗

口设置一次中等的网络攻击。分别计算层次化分析方法中网络的三个层次的态势值,结果如图 6 所示。从图 6(a)中可以看出,在第 11 和第 46 个时间窗口,该网络分别受到了较大和中等的网络攻击,与实际情况一致。因此,网络在这两个时间窗口上较为危险,网络管理人员应该在这两个时间窗口对网络进行密切监督,并采取适当的保护措施。从图 6(b)中可以看出,在第 8 和第 109 个时间窗

口,host1 分别受到了较大和中等的网络攻击。host2 在第 11、36、61 和 79 个时间窗口受到了中等的网络攻击。host3 在第 46 个时间窗口受到了中等的网络攻击。从图 6(c)中可以看出,HTTP 服务在第 46 个时间窗口受到了较大的网络攻击。结果表明,所提 Adaboost-GRU 算法具有较好的信息安全态势感知性能。

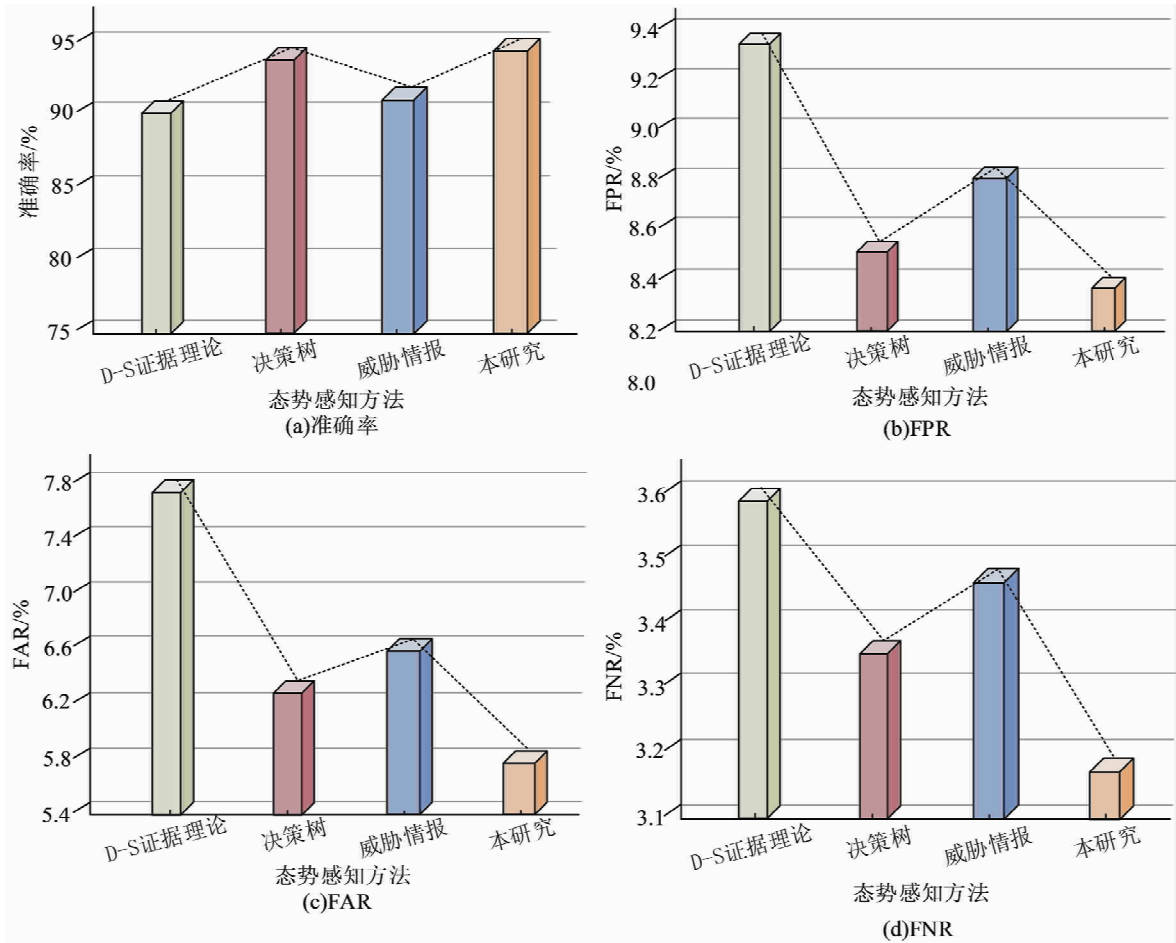


图 4 四种信息安全态势感知方法的对比结果

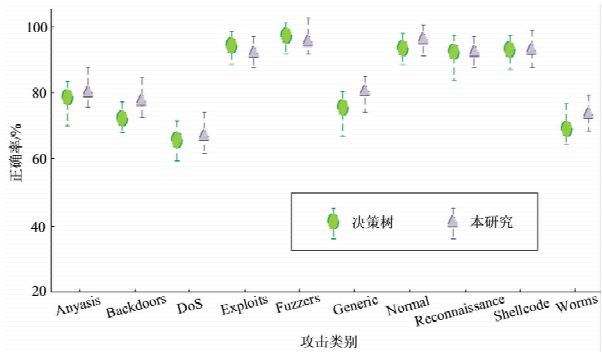


图 5 两种方法的攻击识别正确率对比结果

3 结 论

随着网络攻击的复杂化和多样化,网络信息泄

露的事件频发,网络信息安全也越来越受到重视。为帮助相关网络安全管理人员全面掌握网络的整体安全状况,进而加强对网络安全的监管,研究搭建了基于 Adaboost-GRU 的信息安全态势感知模型。结果表明,研究所提 Adaboost-GRU 算法在准确率、FPR、FAR 和 FNR 四种指标上均具有较好的表现,分别为 94.01%、8.35%、5.75% 和 3.14%。此外,除了在 Exploits、Fuzzers 和 Shellcode 三种攻击上 Adaboost-GRU 算法的识别正确率略低于基于决策树算法的联级网络安全态势感知模型以外,其余类别的攻击均是 Adaboost-GRU 算法的识别正确率更高。此外,所提算法能够较为准确地计算出网络的态势值、各个主机的态势值以及各类服务的态势值,具有较好的信息安全态势感

知性能。综上所述,研究设计的算法具有较好的攻击识别性能,能够有效地评估和感知信息安全态势,具有一定的可行性和有效性。应用在网络中有助于精准地计算网络安全态势,帮助相关人员对网络安全状况进行分析。但研究仅对信息安全态势

感知进行了分析,保障信息安全的效果有限。因此,在未来的研究中,应该进一步结合信息安全态势预测模型,共同对信息安全态势进行检测,以更好地保障网络空间的平稳运行。

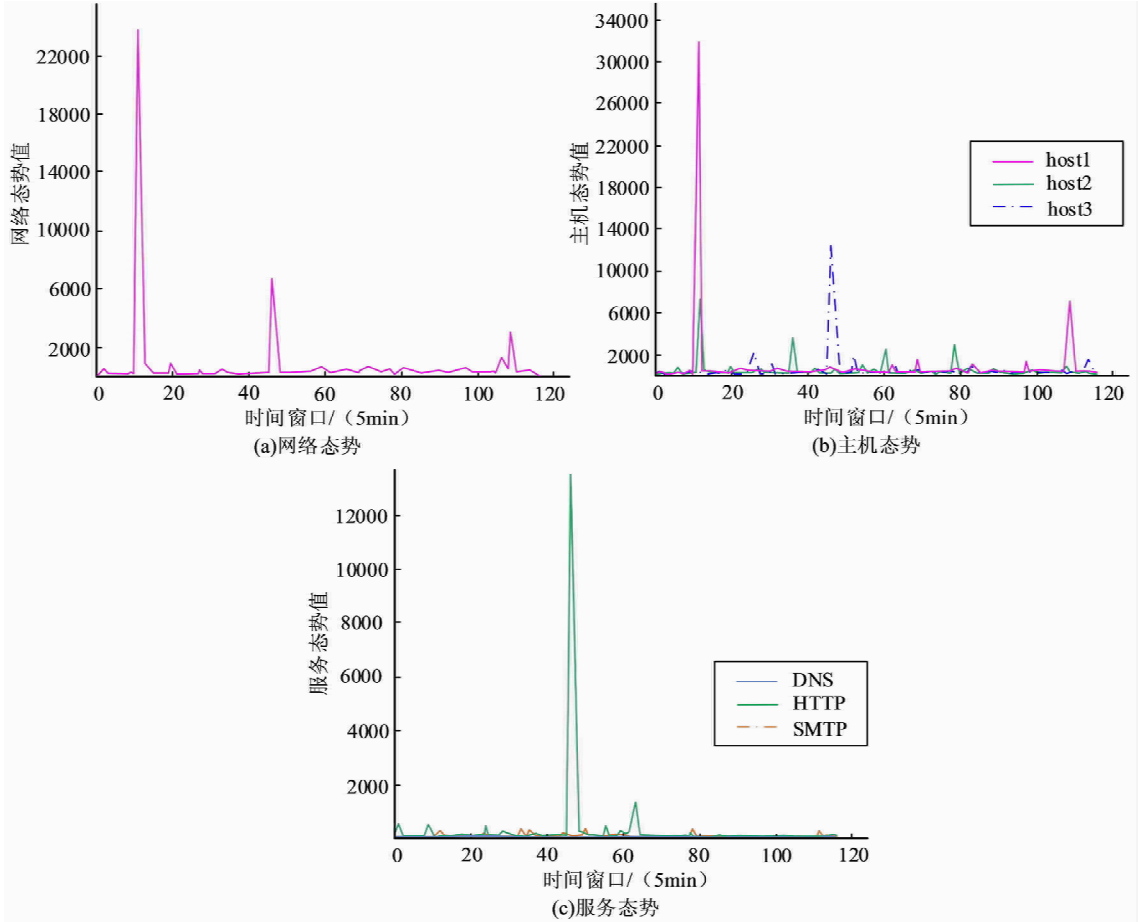


图 6 网络安全态势分析结果

参考文献

[1] 李伟,何明,徐兵,等. 基于一维卷积神经网络与改进 D-S 证据理论的警务云安全数据融合技术[J]. 计算机应用研究, 2022, 39(12):3765—3802.

[2] 谢凯,代康. 基于决策树的联级网络安全态势感知系统设计[J]. 现代电子技术, 2022, 45(17):74—78.

[3] 查德平,徐艺扬,尧玉恒. 基于联防联控架构的网络威胁情报系统设计[J]. 现代电子技术, 2023, 46(14):63—67.

[4] 赵冬梅,李志坚. 基于 Transformer 的网络安全态势预测[J]. 华中科技大学学报(自然科学版), 2022, 50(5):46—52.

[5] 朱铝芬,徐媛媛. 改进 Petri 网故障诊断算法的信道故障诊断与处理[J]. 计算机测量与控制, 2023, 31(6):6—11.

[6] XU M, BARALDI P, LU X, et al. Generative adversarial networks with adaboost ensemble learning for anomaly detection in high-speed train automatic doors[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 23408—23421.

[7] 杨信强,李振华,钟悦,等. 基于变分模态分解和 CNN-GRU-ED 的超短期互感器误差预测[J]. 电力系统保护与控制,

2023, 51(12):68—77.

[8] ZHAO L, LI Z, QU L, et al. A hybrid VMD-LSTM/GRU model to predict non-stationary and irregular waves on the east coast of China[J]. Ocean Engineering, 2023, 276(15): 1—18.

[9] 凡静,李娜. 基于并行约简的多节点网络安全态势评估方法[J]. 科技通报, 2023(6):35—39.

[10] 孔德玉,陆鑫星,沈海强,等. 基于改进层次分析法的再生骨料生产模式优选评价[J]. 浙江工业大学学报, 2023, 51(5): 504—508.

[11] ZHANG H L, XU Z B, FAN X Q, et al. Fusion of quality evaluation metrics and convolutional neural network representations for ROI filtering in LC-MS[J]. Analytical Chemistry, 2023, 95(2):612—620.

[12] 胡向东,盛顺利. 融合 DBN 和 BiLSTM 的工业互联网入侵检测方法[J]. 重庆邮电大学学报(自然科学版), 2022, 34(1): 134—146.

[13] 周莉,李静毅. 基于决策树算法的联级网络安全态势感知模型[J]. 计算机仿真, 2021, 38(5):264—268.

[14] 张红斌,尹彦,赵冬梅,等. 基于威胁情报的网络安全态势感知模型[J]. 通信学报, 2021, 42(6):182—194.