设计研究与应用

多源异构数据融合的网络安全态势评估体系研究

王帅
（吉林司法警官职业学院，吉林长春 130000）

摘 要：为保障网络安全运行，降低网络遭受攻击的几率，本文对多源异构数据融合的网络安全态势评估体系进行深入研究，提出了一个包括流量解析模块、属性提炼模块、决策引擎模块、多源融合模块、网络安全态势评估模块的网络安全态势评估体系，实现了网络流量的全面解析、网络攻击特征及其核心属性的读取、核心属性至攻击类型的映射、多决策引擎输出结果的融合，有效提升了网络安全态势评估效果。

关键词：多源异构数据；网络安全；态势评估；威胁量化
中图分类号：TP393.08 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2023.06.035
本文著录格式：王帅.多源异构数据融合的网络安全态势评估体系研究[J].软件,2023,44(06):141-143

Research on Network Security Situation Assessment System Based on Multi-source Heterogeneous Data Fusion

WANG Shuai
(Jilin Judicial Police Vocational College, Changchun Jilin 130000)

【Abstract】：In order to ensure the safe operation of the network and reduce the probability of network attacks, this paper conducts in-depth research on the network security situation assessment system of multi-source heterogeneous data fusion, and proposes a network security situation assessment system that includes traffic analysis module, attribute extraction module, decision engine module, multi-source integration module, and network security situation assessment module, which realizes the comprehensive analysis the reading of network attack features and their core attributes, the mapping of core attributes to attack types, and the integration of multiple decision engine output results effectively improve the effectiveness of network security situation assessment.

【Key words】：multi-source heterogeneous data;network security;situation assessment;threat quantification

0 引言

基于通信技术的快速发展，社会经济发展逐渐进入互联网经济体制中，网络在为社会公众带来便利条件的同时，也产生了一定的安全风险，对社会稳定发展带来了不利影响[1]。对此，本文以网络运行安全要求为切入点，提出能够满足网络安全态势动态评估的运行体系，以对多源数据进行融合、威胁量化等，旨在提升网络安全态势评估精准性，为网络安全运行提供保障。

1 流量解析模块

流量解析模块主要是通过网络探测器，以多视角解析网络流量，以全面、精准掌握流量特征[2]。现阶段，用于流量解析的网络探测器主要有网络流量解析器与恶意流量分析器。

网络流量解析器的应用可以根据 TCP/IP 协议解析流量包[3]，获取包的个数、发包速率等信息，能够帮助管理人员全面了解流量特征。同时，网络流量解析器可以对网络流量特征进行长期监测，为网络安全运行提供保障。

恶意流量分析器的应用可以获取网络恶意流量特征，并根据协议封装格式，对流量包进行解析，再通过数据比对分析，最终获取数据包中的恶意流量，具体流程如图 1 所示。

2 属性提炼模块

属性提炼包括日志数据预处理、核心属性提炼，主要是对流量解析模块解析出的信息进行处理，并提炼出能够提升攻击类型判断精准度的数据信息。通过属性提

作者简介：王帅（1983—），女，吉林长春人，硕士，副教授，研究方向：计算机网络安全、信息安全、计算机攻击与防护。

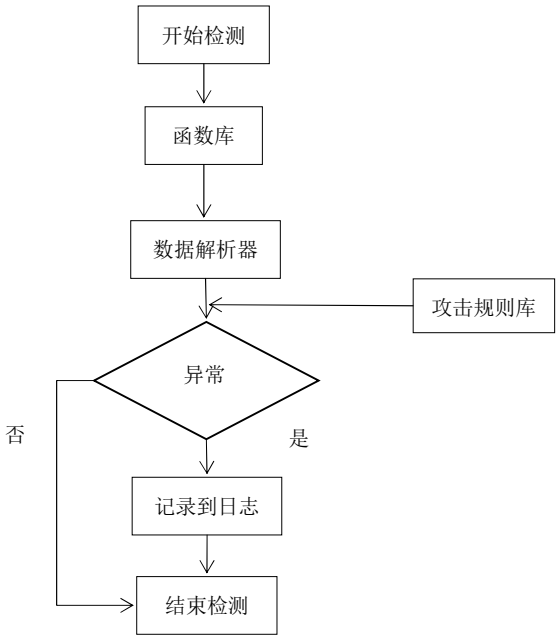

图 1 恶意流量解析流程

Fig.1 Malicious traffic resolution process

炼处理，能够精准提取出网络的核心属性，查找到与网络攻击有关的数据，为网络遭受攻击的情况分析提供依据。

数据预处理的应用可以有效避免值域范围较大的属性在训练过程中覆盖值域范围较小的属性，导致其属性失去意义。在网络安全态势预测过程中，计算机本身无法对非数值的数据进行处理。因此，需要对非数值型数据进行编码，为处理非数值型数据奠定基础。整体而言，现阶段常用的编码方式有 Label 编码、One-hot 编码 [4]。两种编码方式相比，One-hot 编码不会为各类攻击添加序列关系，能够满足实际使用需求。

核心属性提炼主要是对网络攻击相关性较强的属性进行提炼，以便更清晰地掌握网络遭受攻击的情况。与其他属性提炼不同，核心属性提炼可以综合时间属性、IP 地址属性、应用服务属性、端口号属性等，生成网络连接属性，并生成新的网络连接属性，以便更精准地分析网络遭受攻击的情况。

3 决策引擎模块

决策引擎模块可以通过训练，建立起核心属性到攻击类型的映射，可以提炼模块输出的数据，进而检测各类网络攻击。决策引擎模块包括攻击检测模型、多分类检测。

攻击检测模型可以提炼出核心属性，输出网络攻击类型。现阶段，攻击检测模型有决策树、BP 神经网络、支持向量机等。其中，决策树本质上是一种判断规则组成的树状分类模型，在实际应用中，可以通过信息增益等，提取属性，对网络攻击进行判断；BP 神经网络由多个神经元组成，能够模拟生物神经大脑，对网络运行环境进行判断 [5]。每个神经元可以收集上一层信号，并在信号处理后，传输给下一层神经元。

多分类检测可以将多种攻击类型转化为二分类问题。多分类检测的方法可以使用 One-vs-One 等方法 [6]。One-vs-One 方法是通过两种攻击类型数据训练获得的二分类模型，当数据中含有 n 种攻击类型时，需要训练 c_n^2 个二分类模型。在攻击检测过程中，可以将网络特征数据分别输入到二分类模型中进行检测，通过投票等方法得到最终结果。

4 多源融合模块

多源融合是将多个决策引擎输出的结果进行融合后，以全局性视角，对网络的运行状况进行分析，以提升网络攻击类型提取的效果 [7]。若各决策引擎输出结果存在冲突，则对冲突证据进行修正，然后再进行多源数据融合。

冲突证据修正可以减少证据之间的矛盾，确保多源数据融合后的结果更符合实际情况。

多源数据融合常用的算法主要是 D-S 证据理论，该理论可以通过相同事件关联和融合，得出一致性结论，公式表示如式（1）、式（2）所示：

$$m(A)=\frac{\sum_{B_i\cap C_j=A} m_1(B_i)m_2(C_j)}{1-k} \tag{1}$$

$$k=\sum_{B_i\cap C_j=\varnothing} m_1(B_i)m_2(C_j) \tag{2}$$

式（1）、式（2）中，k 表示冲突系数；B_i、C_j 表示焦元；$m(A)$ 表示多源数据融合结果；m_1、m_2 分别表示决策引擎输出的结果（存在冲突）。

在某次实验中，出现 m_1(0.99,0.01,0)、m_2(0,0.01,0.99) 冲突证据，攻击类型如表 1 所示。

表 1 攻击类型

Tab.1 Attack types

	DOS	Backdoor	Shellcode
m_1	0.99	0.01	0
m_2	0	0.01	0.99

现阶段，常用的数据修正主要是置信度法与加权平均法。在实验中，应用 $M=\{\overrightarrow{m_i}\,|\,1\le i\le n\}$ 表示原始数据，$M'=\{\overrightarrow{m_i}'\,|\,1\le i\le n\}$ 表示修正后的数据，其中，n 表示数据量。

通过决策引擎模块，输出结果，如表 2 所示。

表 2 输出结果

Tab.2 Output results

	DOS	Backdoor	Shellcode
决策引擎 1	0.75	0.15	0.1
决策引擎 2	0.8	0.2	0
D-S 证据理论的多源数据融合	0.95	0.05	0

5 网络安全态势评估模块

网络安全态势评估模块是在融合结果的基础上，结合网络的实际运行情况，对网络的威胁进行量化评估，主要包括网络攻击威胁量化评估、网络威胁态势评估两方面。

（1）网络攻击威胁量化评估是根据网络受到的攻击危害程度，对攻击进行定量分析的方式。网络攻击威胁量化评估是有效评估网络威胁状态的重要基础，是现阶段，网络安全态势评估常用的方法之一。在网络攻击威胁量化评估过程中，主要应用到专家经验量化方法、权系数量化方法。其中，专家经验量化方法主要是通过历史经验提取和分析，对网络的攻击威胁程度、危害结果等进行量化分析的方法；权系数量化方法主要是对网络攻击的威胁等级进行划分和定性分析，以从高到低的威胁等级排序原则，对分析结果进行排序，最终确定排序后的网络攻击威胁值。

（2）网络威胁态势评估是应用层次化方法，对网络各设备的运行状况进行评估。以网络运行视角而言，主要的设备为主机。通过网络威胁态势评估，可以对网络结构的层次关系进行分析，并对各层次进行划分，再对各层次下的网络状态进行评估分析。在网络实际运行中，网络威胁态势评估可以对攻击发生的因素、概率等进行分析，判断出网络遭受攻击威胁的概率。同时，网络威胁态势评估可以根据计算机主机的各模块使用情况、运行情况，确定其服务的权值，对主机态势及网络整体的安全态势进行分析，以全面评估网络安全态势，为保证网络安全运行提供保障。

6 结语

网络安全态势评估是保证网络安全运行的重要保障，为提升网络安全态势评估精准性与全面性，本文对多元异构数据融合的网络安全态势评估体系进行研究。针对网络信息愈加庞大的现实情况、网络安全态势评估的实时性要求分析，构建包括流量解析、属性提炼、决策引擎、多源融合、态势评估五方面的网络安全态势评估体系，以期提升网络安全态势评估质量，为网络安全发展提供技术支持。但从整体视角而言，本研究未对网络攻击防控系统进行深度研究，需要在日后研究中进行补充和完善。

参考文献

[1] 张涛涛.基于异构数据源的网络安全监测平台设计和实现[J].网络安全技术与应用,2022(6):6-8.

[2] 刘琦.多源异构大数据平台的建设及应用[J].软件工程,2021,24(10):54-58.

[3] 陈娜,刘海姣,李今宋,等.配电终端多源异构数据的跨模态聚合算法[J].控制与信息技术,2021(4):1-7.

[4] 孙宇飞.政务云网络安全态势多源异构数据收集与存储模式研究[J].网络安全技术与应用,2021(8):78-80.

[5] 常利伟,田晓雄,张宇青,等.基于多源异构数据融合的网络安全态势评估体系[J].智能系统学报,2021,16(1):38-47.

[6] 苏小玉,徐奎奎.网络安全态势感知中数据融合算法应用综述[J].河北省科学院学报,2020,37(2):37-44.

[7] 刘蓓,禄凯,程浩,等.基于异构数据融合的政务网络安全监测平台设计与实现[J].信息安全研究,2020,6(6):491-498.

…… 上接第106页

些未实现的功能，如账户充值与提现功能、向用户发送订阅消息功能等，还需进行进一步的研究。

参考文献

[1] 方静,曾陈萍,严兆淋,等.基于微信小程序“易助”平台的设计与实现[J].现代信息科技,2021,5(24):32-34.

[2] 陈娜,马炎,龙霞.基于微信小程序的校园快递代取互助平台建设[J].信息记录材料,2019,20(9):165-166.

[3] 李林锦,操守正,颜山明.基于微信小程序的校园互助应用[J].无线互联科技,2020,17(13):28-29.

[4] 兰哲威,周雪芹.小程序实现校园互助与班级管理平台[J].电脑知识与技术,2021,17(35):64-67.

[5] 邓云霞,周沛,孙罡,等.“帮主”小程序的设计研究——基于微信小程序的校园跑腿互助平台[J].投资与合作,2021(2):197-198.