

基于攻击特征动态增量聚类的 复合连续网络攻击安全检测方法

王远翔[†]

(湖南省金盾信息安全等级保护评估中心有限公司, 湖南 长沙 410000)

摘 要:复合连续网络中,信息共享残差值过大是网络体系无法准确检测攻击性行为的主要原因。为提升复合连续网络运行安全性,实现对攻击性行为的精准检测,设计了基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法。生成攻击性数据的分布序列,通过转换数据样本格式的方式,完成对复合连续网络中攻击特征的提取。在此基础上,针对复合连续网络进行动态层次实施划分,并在聚类结构中,计算攻击数据的动态增量聚类相异度,实现面向攻击特征的复合连续网络攻击数据动态增量聚类处理。设置必要的安全性攻击检测节点,联合节点内采集到的攻击信息,执行网络攻击数据的安全融合,完成复合连续网络攻击安全检测。测试结果表明,该方法可将信息共享残差控制在0—1.32之内,且能够准确高效地检测攻击性行为,在提升网络体系运行安全性方面具有突出应用价值。

关键词:攻击特征;动态增量聚类;复合连续网络攻击;安全检测;分布序列;格式转化;动态层次;相异度

中图分类号:TP393

文献标识码:A

A Security Detection Method for Composite Continuous Network Attacks Based on Dynamic Incremental Clustering of Attack Features

WANG Yuanxiang[†]

(Hunan Jindun Information Security Classification Protection Evaluation Center, Changsha, Hunan 410000 China)

Abstract: In composite continuous networks, the large residual value of information sharing is the main reason why the network system cannot accurately detect aggressive behavior. To improve the operational security of composite continuous networks and achieve precise detection of aggressive behavior, a dynamic incremental clustering based attack feature based composite continuous network attack security detection method is designed. Generate a distribution sequence of aggressive data, and complete the extraction of attack features in composite continuous networks by transforming the data sample format. On this basis, dynamic hierarchical partitioning is implemented for composite continuous networks, and the dynamic incremental clustering dissimilarity of attack data is calculated in the clustering structure to achieve dynamic incremental clustering processing of attack data for composite continuous networks oriented towards attack features. Set up necessary security attack detection nodes, combine the attack information collected within the nodes, perform security fusion of network attack data, and complete composite continuous network attack security detection. The test results show that this method can control the information sharing residual within 0—1.32, and can detect accurately and efficiently aggressive behavior, which has outstanding application value in improving the operation security of network system.

收稿日期:2023-08-22

基金项目:湖南省自然科学基金资助项目(2019JJ58057)

作者简介:王远翔(1997—),男,四川大邑人,本科,高级工程师,研究方向:信息安全。

[†] 通信联系人, E-mail: wxsly134564@163.com

Key words: attack features; dynamic incremental clustering; composite continuous network attacks; safety testing; distribution sequence; format conversion; dynamic hierarchy; degree of dissimilarity

随着数据样本输入量的增大,复合连续网络对于信息参量的转存速率也会不断增加,而当数据样本累积量达到一定数值标准之后,网络机制的核心数据库主机开始转存信息参量^[1],此时复合连续网络对于外部信息参量的识别敏感性最弱,导致信息共享残差值过大,容易遭受网络攻击,出现不安全事件。因此针对复合连续网络中的攻击行为进行安全性检测,成了一项亟待解决的难题。

现有研究中,基于渗透测试的多层次网络安全入侵检测方法通过提取攻击行为滤波特征参量,定义包含目标信息的纯特征信号集合;再借助检测器装置,完成对数据样本对象的分类处理,完成攻击检测^[2]。基于信息流分析的密码核设计安全验证与漏洞检测方法在密码方面对安全性检测手段进行改进。根据测试向量实际取值,定义完整的密码算法核算机制,又通过形式化验证的方式,实现对攻击性行为的识别与检测^[3]。上述两种方法对于信息共享残差的控制能力有限,在特定情况下无法保证攻击性行为的检测能力。

攻击特征是描述复合连续网络中攻击性行为强度等级的物理参数,主机元件对于攻击特征的判断准确性,决定了主机对攻击性行为的检测与处理能力。动态增量聚类是一种新型的聚类运算思想,在增量值指标的基础上,联合相关物理参数定义全新的聚类处理方案,从而在准确标记信息对象的同时,避免差异化样本对核心数据参数造成覆盖性影响^[4]。文章基于攻击特征动态增量聚类思想设计一种新型的复合连续网络攻击安全检测方法,结合攻击特征与动态增量聚类,提取与识别攻击性行为表现特征,聚合符合检测需求的攻击性数据样本,控制信息共享残差值,提升检测数据样本攻击性行为检测的精准性。

1 复合连续网络攻击安全检测方法设计

文章设计的复合连续网络攻击安全检测方法首先提取复合连续网络的攻击特征,然后对特征攻击进行动态层次划分和增量聚类,最后在增强检测节点采集能力的同时,完成攻击行为安全性检测。具体检测流程如图 1 所示。

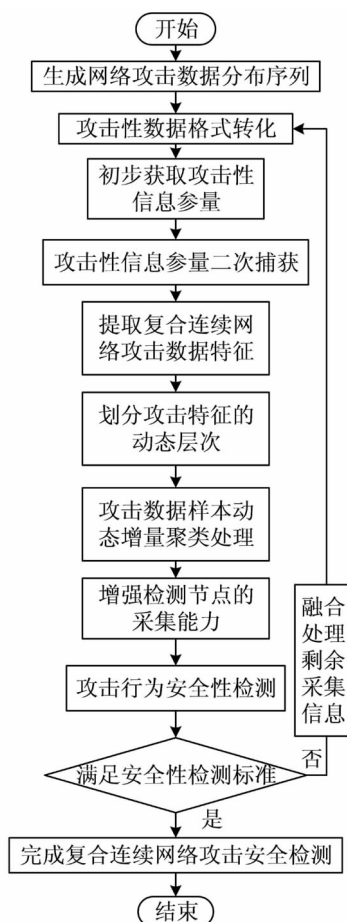


图 1 网络攻击安全检测方法设计

1.1 复合连续网络的攻击特征提取

1.1.1 网络攻击数据的分布序列生成

分布序列是指不满足统一聚合条件的数据检测序列,提取复合连续网络的攻击特征,必须研究网络攻击数据的分布序列。对于复合连续网络中的攻击性数据而言,信息对象的攻击强度等级特征就是数据样本的分布序列^[5]。主机元件如若按照当前序列条件,提取数据样本对象,则可以最大化保证提取所得信息参量的攻击性特征,从而为网络体系内安全性检测指令的实施提供保障^[6]。

χ 表示复合连续网络中攻击数据对象的数值化参数,其定义式为:

$$\chi = 2^{\alpha} \dot{p} (2^{\delta} \bar{O} - \bar{I}) \quad (1)$$

式中: α 、 δ 表示两个随机选取的数据样本数值评定参数,且 $\alpha \neq \delta$ 的不等式取值条件恒成立, $\dot{p}$ 表示数据对象的攻击强度等级评定特征, $\bar{O}$ 表示

攻击数据在复合连续网络中的单位传输均值, $\dot{I}$ 表示攻击数据的关联性数值向量。

利用式(1), 可将网络攻击数据的分布序列表达式定义为:

$$i = \dot{I} \sum_{\epsilon=1} \chi \cdot \left(\frac{|\dot{a}^2|}{\dot{\gamma}} \right)^{\dot{p}} \quad (2)$$

式中: ϵ 表示网络攻击数据的分布式取样系数, $\dot{a}$ 表示网络攻击数据的分布式取样向量, $\dot{\gamma}$ 表示攻击性特征的分布式序列模向量。基于获得的网络攻击数据的分布序列转化攻击性数据格式, 为后续特征提取奠定基础。

1.1.2 针对分布序列的攻击性数据格式转化

针对攻击性数据过量累积的情况, 针对分布序列的攻击性数据格式进行转化。在不考虑其他干扰条件的情况下, 对于上节攻击性数据序列分布的编码采用 One-Hot 机制。以复合连续网络为数据样本的核心存储空间, 在提取攻击特征参量的同时, 完善 One-Hot 机制的运行模式, 从而将重叠在一起的攻击特征参量分离开来, 使得每一网络区域内只存在一个符合提取需求的攻击特征样本, 并以此保证复合连续网络的运行安全性^[7,8]。

针对分布序列, 定义 One-Hot 机制识别量, 具体定义式如下:

$$U = \hat{y} \cdot \frac{\sum_{\epsilon=1} \varphi \times i^e}{|\Delta Y|} \quad (3)$$

式中: $\hat{y}$ 表示网络攻击数据的实时累积特征, ΔY 表示分布序列中网络攻击数据的单位累积量, e 表示分布序列辨识参数, φ 表示基于 One-Hot 机制的网络攻击数据提取系数。

利用式(3), 推导攻击性数据的格式转化过程为:

$$R = R' \frac{(\varphi + 1)^2}{|T_2 - T_1|} \cdot (-\log_U \dot{E}^2) \quad (4)$$

式中: R 表示转化后的攻击性数据格式, R' 表示转化前的攻击性数据格式, $\dot{E}$ 表示网络攻击数据的过量累积特征, φ 表示基于 One-Hot 机制所定义的攻击数据识别阈值, T_1 、 T_2 表示两个不为零的攻击性数据格式转化周期时长, 且当 $T_2 \neq T_1$ 的不等式条件恒成立时, 可以进行数据格式的转化。

1.1.3 转化后网络攻击数据的特征提取

完成攻击性数据的格式转化后, 对于复合连续网络攻击特征的提取, 就等同于按照数据格式转化条件, 完成对攻击性信息参量的初步获取与二次捕获处理。

(1) 攻击性信息参量的初步获取

攻击性信息进入复合连续网络的所有传输与转化行为都会在 i 中表现出来, 其中包括端口信息、攻击性强度等级等。在 $T_2 \neq T_1$ 的条件下, 借助 MySQL 与 sebek 软件, 可以完成对风险项参数的处理, 初步获取复合连续网络主机对攻击性信息参量^[9]。

(2) 攻击性信息参量的二次捕获

复合连续网络对于攻击性信息参量的处理就是在网络主机中设立一道“防御屏障”, 在 $T_2 \neq T_1$ 的条件下, 判断屏障体系对信息攻击行为的承载能力, 并从中选择具有明显攻击特征的信息参量完成二次捕获处理, 从而实现对复合连续网络攻击特征的提取^[10]。

提取的复合连续网络攻击数据特征满足如下表达式:

$$W = \dot{q} \times \frac{r \cdot \sum_{-\infty}^{+\infty} \vec{P}}{\left(\frac{R}{\tilde{Q}}\right)^2 + 1} \quad (5)$$

式中: W 表示转化后网络攻击数据特征提取结果, $\dot{q}$ 表示攻击特征的初步获取参量, $\tilde{Q}$ 表示攻击特征的二次捕获参量, r 表示复合连续网络中攻击特征的取样权重, $\vec{P}$ 表示数据格式转化条件下的攻击性数据传输向量。由此完成复合连续网络的数据攻击特征提取, 根据特征进行聚类分析, 为后续检测奠定基础。

1.2 面向攻击特征的复合连续网络攻击数据动态增量聚类

1.2.1 复合连续网络的动态层次划分

在划分复合连续网络动态层次结构前, 需要结合上节提取的复合连续网络攻击数据特征 W , 确认攻击特征的动态层次划分标准 A , 具体过程为:

$$A = \frac{W}{\lambda a} \sum_{\iota_1=1} \sum_{\iota_2=1} |\kappa \cdot \hat{S}| \quad (6)$$

式中: a 表示协议文本连接参数, λ 表示复合连续网络的动态化评级系数, ι_1 、 ι_2 表示两个不相等的的数据样本动态分配系数, $\hat{S}$ 表示满足攻击特征条件的数据样本取样对象, κ 表示网络体系的动态性划分阈值。

复合连续网络的动态层次划分标准与常规网络体系基本相同, 都是将完整的网络空间分割成应用层、表示层、会话层、运输层等 7 类结构单元, 并在每一单元结构中设置一种或几种协议文件及端口组织, 以便于主机元件能够根据 A 对攻击性数

据对象进行动态查询与处理。

1.2.2 动态增量聚类处理

动态增量聚类是将检测所需复合连续网络攻击数据样本聚合在一起的处理过程。聚类处理之前,攻击性数据、非攻击性数据混合在一起,因此在检测攻击行为之前,复合连续网络主机必须先根据上节获得的攻击特征动态层次划分标准 A ,将攻击性数据筛选出来^[11-13]。

在复合连续网络中,搭建聚类结构的过程就是完成数据动态增量聚类处理的过程。但在进行聚类处理前,需要结合 A 划分攻击性数据对象的特征,确认动态增量聚类结构对于攻击性数据对象的处理原则 D ,通过数据样本的分布区间,实现动态增量聚类处理。具体过程如下表达式:

$$D = \frac{1}{A} \sqrt{|\mu_1 d_1|^2 + |\mu_2 d_2|^2 + \dots + |\mu_n d_n|^2} \quad (7)$$

式中: d_1 、 d_2 、 $\dots$ 、 d_n 表示满足特征取样条件的 n 个攻击性数据对象,且 $d_1 \neq d_2 \neq \dots \neq d_n$ 的不等式取样条件恒成立, μ_1 、 μ_2 、 $\dots$ 、 μ_n 分别表示与攻击性数据对象匹配的增量聚类识别参数,其取值属于 $[1, +\infty)$ 的数值区间。

复合连续网络攻击安全检测方法在完成对攻击数据对象的动态增量聚类处理时,还要求相同信息对象的差异化水平即聚类相异度指标必须指向同一个数值参量。对于网络检测主机而言,相异度指标的计算数值越大,就表示攻击性数据对象之间的差异化水平越高^[14-16]。

在复合连续网络中,选择一个攻击数据的动态增量参数 $\tilde{g}$,其定义式为:

$$\tilde{g} = \frac{(\nu |f \times \dot{h}|^2)^{\frac{1}{\omega}}}{D} \quad (8)$$

式中, $\dot{h}$ 表示攻击数据对象的动态化取样特征, f 表示数据样本的增量等级平均参数, ν 表示基于攻击特征的数据样本增量态势评估向量, ω 表示复合连续网络中攻击数据对象的量化值系数^[17,18]。

利用式(8),推导攻击数据动态增量聚类相异度 H 的计算公式为:

$$H = \frac{\theta \cdot \vec{j}}{g(k_{\max} - k_{\min})} \quad (9)$$

式中, $\vec{j}$ 表示攻击数据动态增量行为的描述向量, θ 表示攻击性数据样本之间的异度极化水平评

价参数, $k_{\max}$ 表示数据信息相异化指征的最大取值, $k_{\min}$ 表示数据信息相异化指征的最小取值。由此完成动态增量的聚类处理,混合状数据对象被复合连续网络完全区分开来。按照 D 将攻击性数据聚合成一个包状结构体,以供主机元件的直接调取与利用。

1.3 基于攻击特征动态增量聚类的攻击行为安全性检测

1.3.1 检测节点采集能力增强

如果复合连续网络检测基站对于簇头节点及普通节点的调节能力有限,则会出现攻击信息采集量过少的情况;反之,若复合连续网络检测基站对簇头节点及普通节点的调节能力过强,则会出现攻击信息采集量过多的情况^[19,20]。因此在攻击行为安全性检测前需要基于上节的聚类结构,增强检测节点的采集能力。

设 ΔL 表示复合连续网络检测基站内攻击信息样本的单位累积量,联立式(9),计算检测节点的攻击信息采集参量 J :

$$J = H \times \left(\frac{\vartheta - 1}{\sigma - 1} \right)^2 \times \beta \quad (10)$$

式中: β 表示复合连续网络中节点的检测距离,该参量需要满足 $T_2 \neq T_1$ 且取值在 $k_{\min}$ 至 $k_{\max}$ 中, ϑ 表示簇头节点与普通节点之间的稳定性连接系数, σ 表示簇头节点与普通节点之间的连贯性连接系数。

1.3.2 攻击行为安全性检测实现

主机元件在安全检测复合连续网络攻击行为时,要求所采集到信息参量必须保持上节攻击特征动态增量聚类后获得的包状存储结构,所以在完成节点采集增强步骤后,必须针对增强采集后获得的 J 实施安全性融合处理,计算攻击数据样本之间的连接间隙,使其小于主机元件所能承载安全性检测距离^[21,22],完成复合连续网络攻击安全的检测。

假定 $\hat{C}$ 表示网络攻击数据在连续检测区间内的融合处理向量,且其取值恒属于 $(0, +\infty)$ 的数值区间,推导网络攻击数据的安全融合过程,连续检测区间结果为:

$$Z = \int_{-\infty}^{+\infty} \left| \hat{C} \xi \cdot J \right|^{-1} |dj| \quad (11)$$

式中, Z 为网络攻击数据间的连接间隙; ξ 表示针对攻击特征动态增量聚类采集信息的数据样本标记参数, X 表示复合连续网络中攻击数据对

象的阶段性融合特征。

当一次融合处理后,网络攻击数据的取样结果并不满足安全性检测标准即 $Z > \beta$ 且 $Z \notin k_{\min} \cdots k_{\max}$,那么为需要联合剩余采集信息,再次进行融合处理,直至 $Z < \beta$ 且 $Z \in k_{\min} \cdots k_{\max}$ 后,数据取样结果能够完全符合复合连续网络主机的安全性检测需求,完成复合连续网络攻击安全检测。

针对复合连续网络攻击安全检测,在攻击数据分布序列的基础上,联合数据格式转化标准,提取网络主机所需的必要特征参量。根据提取特征确认攻击数据提取原则,划分网络体系的动态层次,并联合关键聚类结构,求解聚类相异度指标的具体数值,对于攻击数据动态增量进行聚类处理。基于攻击特征动态增量聚类完成检测节点设置,采集关键攻击信息和检测距离,通过安全融合数据样本的方式,对攻击信息进行融合处理,获取网络攻击数据间的连接间隙,当该参数符合检测距离时,即可实现复合连续网络攻击安全检测。

2 实验与分析

本次实验选择基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法(本文方法)、基于渗透测试的多层次网络安全入侵检测方法(文献[2])、基于信息流分析的密码核设计安全验证与漏洞检测方法(文献[3])三组不同的实验方案,通过对比实验的方式,验证不同实验方案对于信息共享残差值指标的控制能力。

2.1 复合连续网络连接

选择公开数据集 UNSW-NB15 数据集作为测试对象。UNSW-NB15 数据集是一项面向网络入侵检测的公开数据集,由澳大利亚网络安全中心实验室提供。该数据集模拟了真实的网络环境中的流量情况,并包含各种常见网络攻击和正常流量,广泛应用于网络入侵检测任务中。选取真实网络流量数据 3.5 GB 和网络攻击数据 115 MB。网络攻击数据中包含 DDoS 攻击、僵尸网络攻击、恶意软件传播攻击、漏洞利用攻击、数据泄露攻击五种攻击类型。对于信息共享残差值的实验要求数据样本只能在复合连续网络中传输,因此为保证实验结果的真实性,需利用 RVS 双绞线,将网络体系的各个终端节点连接起来,具体连接情况如图 2 所示。

表 1 为本次实验所选设备元件的具体型号。

为最大化避免突发性事件对实验结果真实性的影响,实验开始前,必须多次调节设备元件之间的连接关系,以确保实验设备的稳定运行状态。

表 1 实验设备选型

项目	设备名称	型号
1	网络响应主机	DE2-115 Cyclone IV 型单片机设备
2	数据触发器	PDIP40 89C51 型集成元件
3	数据分类装置	STM32F103 LQFP100 微处理器
4	双绞线	RVS 型多通路光纤线缆
5	处理器	STC89c52 型集成处理芯片
6	防火墙	冰盾抗 DDOS 防火墙
7	局域网主机	TX-1C 增强型单片机



图 2 复合连续网络连接

2.2 实验流程

提取数据特征后获得的复合连续网络动态层次如图 3 所示。

应用层	TELENT、FTP、SMTP等应用协议文件
表示层	
会话层	
运输层	TCP或UDP文本
网络层	网络IP端点
数据链路层	网络连接端口
物理层	

图 3 复合连续网络动态层次

由图 3 可知,应用层、表示层、会话层共享 TELENT、FTP、SMTP 等应用协议文件,负责将处于传输状态的攻击性数据导入网络主机,以便于主机设备对其进行后续的聚类处理。运输层结构对攻击性数据的传输遵循 TCP 或 UDP 文本,当复合连续网络对数据样本攻击特征进行识别时,这两类文本协议的存在,可以有效避免数据覆盖行为的

出现,从而保障了网络主机对于攻击行为的安全性检测需求。网络层提供了处于开放状态的网络 IP 端点,可以在数据链路层、物理层组织的配合下,建立网络检测端口与 IP 端点之间的实时连接关系。

在复合连续网络保持连续开放状态的情况下,具体的安全性攻击检测节点设置结构如图 4 所示。

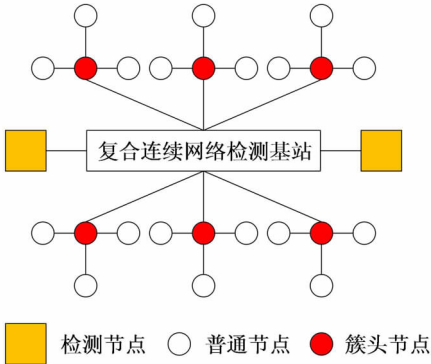


图 4 复合连续网络中安全性攻击检测节点设置结构

图 4 中,检测节点作为主机元件与检测基站之间的过渡设备,可以为数据样本的传输提供较为稳定的端口节点组织。

复合连续网络中,信息共享残差值过大会使网络体系无法准确检测攻击性行为。为保证复合连续网络的攻击行为得到准确检测,必须将信息共享残差控制在较低的数值水平。因此,将信息共享残差值作为方法功能的测试指标。本次实验的具体执行流程如下。

首先,根据图 5 调节复合连续网络,待攻击数据样本累积量达到 100 MB 后,开始实验。

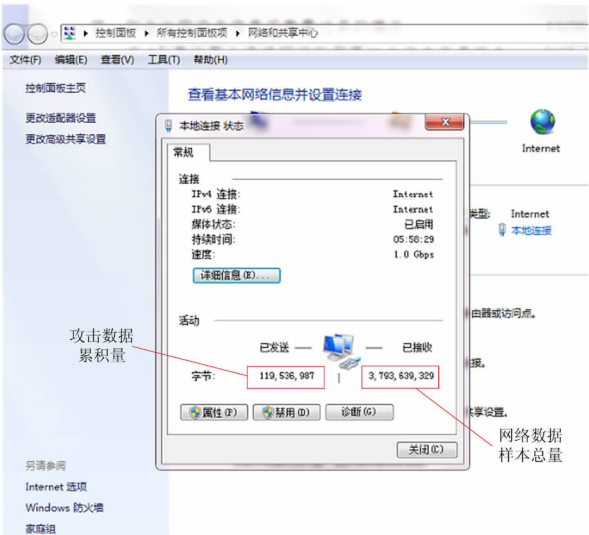


图 5 复合连续网络调试

然后,分别记录实验组(基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法)、对照

A 组(文献[2]提出的基于渗透测试的多层次网络安全入侵检测方法)、对照 B 组(文献[3]提出的基于信息流分析的密码核设计安全验证与漏洞检测方法)检测方法作用下,信息共享残差的数值变化情况,以及攻击安全检测准确率和检测效率。

2.3 实验结果分析

检测本文方法对复合连续网络攻击数据动态增量聚类的性能。聚类处理前待检测数据样本的分类形式如图 6 所示。

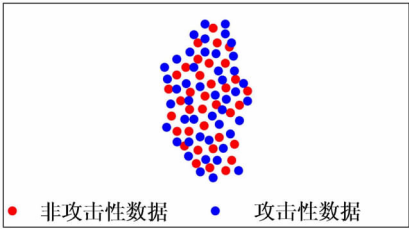


图 6 动态增量聚类前的数据样本

完成聚类处理后待检测数据样本的分类形式如图 7 所示。

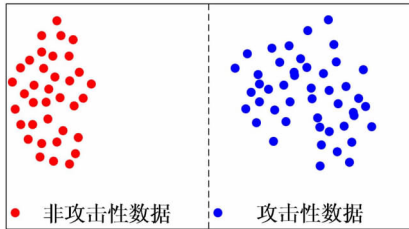


图 7 动态增量聚类后的数据样本

对比图 6 和图 7 可知,由于动态增量聚类是一项连锁性处理行为,所以在完成对攻击性数据对象的聚合处理后,非攻击性数据对象也会表现出聚合分布状态,且复合连续网络主机会自发将两类数据样本存储于不同的终端体系之中,以保证网络体系的安全性运行能力。

实验过程中,对取样所得攻击数据进行完全检测,记录信息共享残差指标的极限数值,所得结果为预期最大值,再缩小攻击数据对象取样量,分别应用实验组、对照 A 组、对照 B 组方法进行实验。

图 8 反映了实验组、对照 A 组、对照 B 组信息共享残差指标的具体实验数值。

分析图 8 可知,与信息共享残差的预期最大值相比,对照 A 组、对照 B 组实验残差的数值水平相对较高,前者最大值达到了 2.14、后者最大值达到了 2.00。实验组信息共享残差的实验数值水平相对较低,整个实验过程中,其最大值只能达到 1.32,与对照 A 组最大值相比,下降了 0.82,与对照

B组最大值相比,下降了 0.68。在本次实验所选的三组检测方法中,基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法的应用能力最强,可以将信息共享残差控制在较低的数值水平,能够较好地解决由残差值过大引起的网络体系无法准确检测攻击性行为的问题。

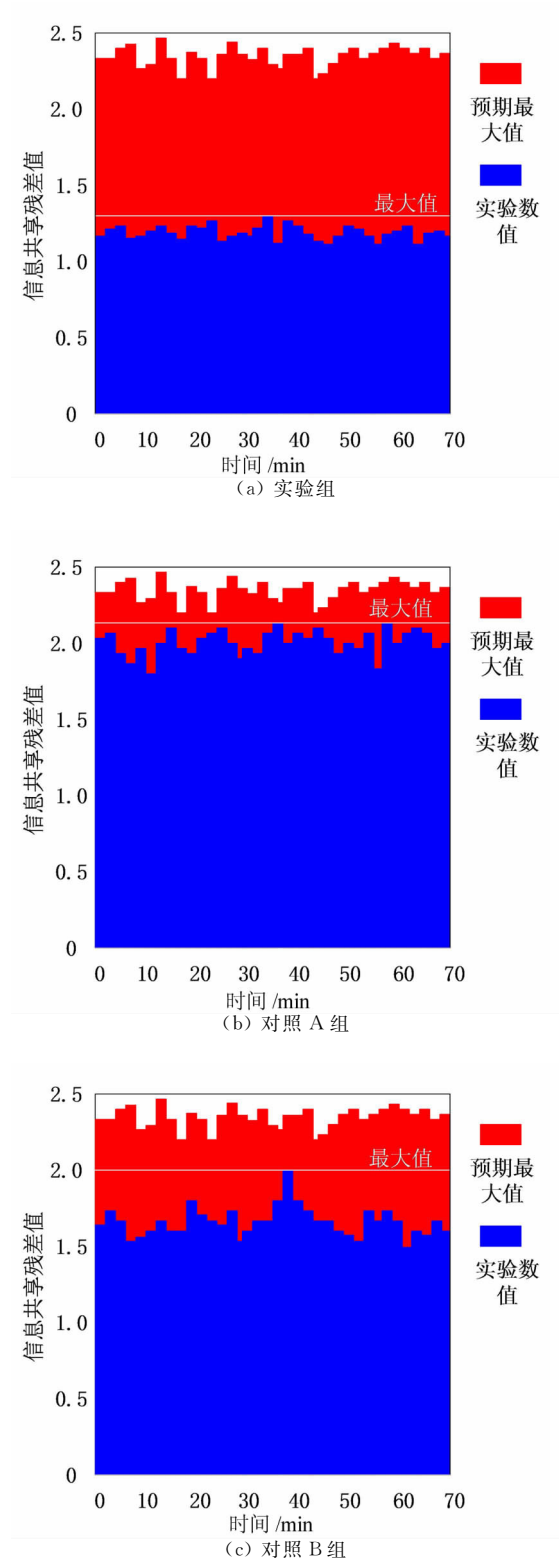


图 8 信息共享残差值

以检测准确率和检测效率为指标,进一步测试三种方法的网络攻击检测性能。检测准确率计算公式为:

$$F = \frac{n}{N} \times 100\% \tag{12}$$

式中, n 表示与实际攻击类型一致的测定值个数, N 表示网络攻击总测定个数。

利用三种方法对输入网络的 DDoS 攻击、僵尸网络攻击、恶意软件传播攻击、漏洞利用攻击、虚假响应攻击进行检测。将检测结果与实际数据对比,通过式(9)获得三种方法的检测准确率,同时记录三种方法的检测时间。三种方法的检测准确率和检测效率的测试结果如图 9 和图 10 所示。

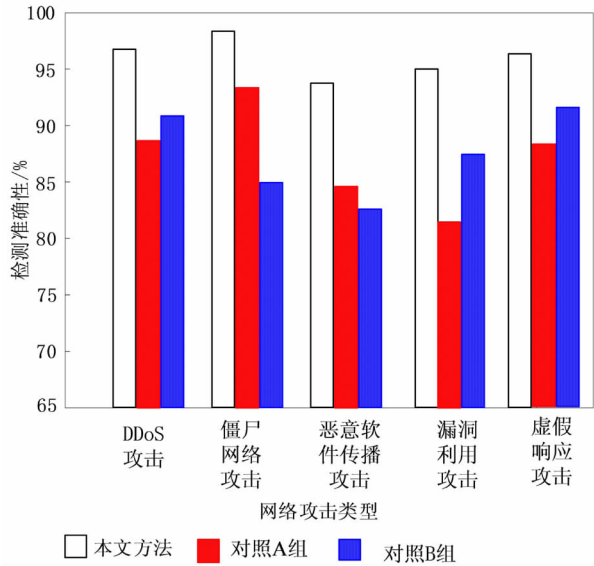


图 9 攻击检测准确率

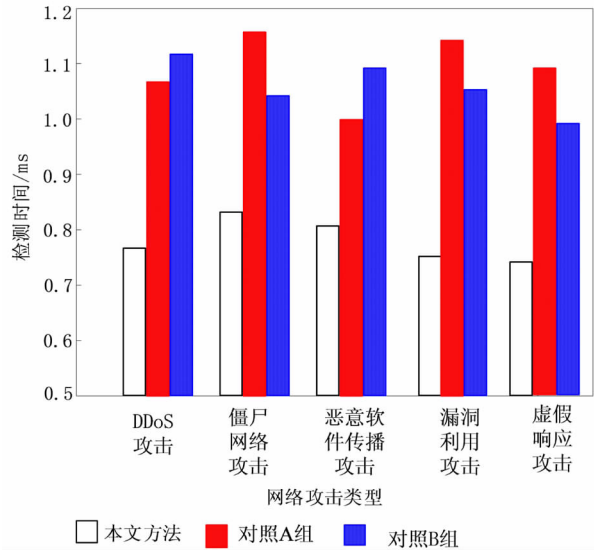


图 10 攻击检测效率

由图 9 可知,面对五种攻击类型,基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法的检测准确率高于 95%,检测时间低于 0.9 ms,而其他两种方法的检测准确率和检测效率均低于复合连续网络攻击安全检测方法。由此可知基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法能够准确检测攻击性行为,符合提升复合连续网络运行安全性、精准检测攻击性行为的实际应用需求。

3 结 论

基于攻击特征动态增量聚类的复合连续网络攻击安全检测方法,重新定义了攻击数据的分布序列,通过动态增量聚类处理攻击数据对象的方式,完成对攻击信息的采集,从而实现网络攻击安全性检测。应用所提检测方法,可以较好控制信息共享残差的数值水平、解决网络体系无法准确高效检测攻击性行为的问题。不但提升了复合连续网络的运行安全性,还保障了主机元件对攻击性行为的精准检测能力。未来相关研究可以在该方法的基础上寻求更加有效的检测技术,从而在维护复合连续网络运行能力的同时,更加有效地控制信息共享残差指标的数值水平。

参考文献

[1] 杜峥,刘孟凯,周建勋,等. 高速采样下含网络攻击的信息物理系统 H_{∞} 故障检测[J]. 控制与决策, 2022, 37(5): 1395—1401.

[2] 李群,王超,任天宇. 基于渗透测试的多层次网络安全入侵检测方法[J]. 沈阳工业大学学报, 2022, 44(4):372—377.

[3] 马艺新,唐时博,谭静,等. 基于信息流分析的密码核设计安全验证与漏洞检测[J]. 西北工业大学学报, 2022, 40(1): 76—83.

[4] 史亚文,唐可可,彭伟龙,等. 基于对抗点的局部点云神经网络特征匹配攻击[J]. 计算机辅助设计与图形学学报, 2022, 34(9):1379—1390.

[5] 霍纬纲,梁锐,李永华. 基于随机 Transformer 的多维时间序列异常检测模型[J]. 通信学报, 2023, 44(2):94—103.

[6] 邱禧荷,茹亚军,陈斌,等. 基于 Deep AR 神经网络时间序

列模型的电能消耗预测[J]. 江苏大学学报(自然科学版), 2022, 43(5):599—603.

[7] 张乐瑞,梁钊毓,余顶,等. HDF5 格式多群截面数据库 AX-ELIB 的加工与验证[J]. 哈尔滨工程大学学报, 2021, 42(12):1819—1825.

[8] 任含,邓军勇. 图数据压缩格式对广度优先搜索算法影响的特性化分析[J]. 郑州大学学报(理学版), 2021, 53(2):26—33.

[9] 刘峰,朱颖,张凯,等. 数据挖掘下电网调度信号异常数据提取方法[J]. 湘潭大学学报(自然科学版), 2021, 43(6):74—80.

[10] 张磊,吴颖,杨建常. 基于大数据挖掘的电力通信信号异常数据提取方法[J]. 科技通报, 2022, 38(6):35—38+44.

[11] 李建桂,梁越,高鹏飞,等. 基于层次化类别嵌入的电力 ICT 系统故障分类[J]. 北京邮电大学学报, 2021, 44(4):34—40.

[12] 王礼云,辛月兰. 基于卷积神经网络和层次标签集扩展的文本分类方法[J]. 西北师范大学学报(自然科学版), 2021, 57(2):48—54.

[13] 乔永坚,刘晓琳,白亮. 面向高维特征缺失数据的 K 最近邻插补子空间聚类算法[J]. 计算机应用, 2022, 42(11): 3322—3329.

[14] 卢建云,张蔚,李林. 一种基于动态局部密度和聚类结构的聚类算法[J]. 山东大学学报(工学版), 2022, 52(2):118—127.

[15] 陈鸿杰,何玉林,黄哲学,等. 基于候选中心融合的多观测点 I-nice 聚类算法[J]. 模式识别与人工智能, 2022, 35(4):348—362.

[16] 赵春霞,赵营颖,宋学坤. 基于频繁项集的多源异构数据并行聚类算法[J]. 济南大学学报(自然科学版), 2022, 36(4): 440—443+451.

[17] 兰天,蓝元良,刘伟麟,等. 面向换流阀状态监测用传感器节点电磁取能仿真分析与设计[J]. 电网技术, 2022, 46(4): 1503—1510.

[18] 张孟伦,张希,牛鹏飞. 面向物联网监测节点的集成式微流控传感芯片[J]. 传感技术学报, 2021, 34(2):157—161.

[19] 熊英乔,邱芬. 恶意软件攻击行为的时序逻辑建模分析[J]. 计算机仿真, 2022, 39(06):430—433,438.

[20] 翟雁,郭晓波,王谦. 机床运动轴位置信息高精度高频率实时采集研究[J]. 制造技术与机床, 2021, 706(4):96—100.

[21] 盛裕杰,郭庆来,刘梦洁,等. 多源数据融合的用户充电行为分析与充电设施规划实践[J]. 电力系统自动化, 2022, 46(12):151—162.

[22] 石宜金,谭贵生,赵波,等. 基于模糊综合评估模型与信息融合的电力变压器状态评估方法[J]. 电力系统保护与控制, 2022, 50(21):167—176.