文章编号:1671-4598(2023)12-0244-07 DOI:10.16526/j.cnki.11-4762/tp.2023.12.036 中图分类号:TP309 文献标识码:A

半监督环境下基于 AE-ELM 模型的工业网络安全防御研究

李 媛[1],刘海峰[1],曹博涛[2]
(1.北京市政务信息安全保障中心,北京 100000;
2.陕西科技大学 机电工程学院,西安 710021)

摘要:针对工业网络中存在的入侵风险和安全性防御问题,在半监督网络环境下提出一种基于 AE-ELM 模型的工业网络安全防御方法;通过不同网络环境下攻击程序、恶意数据或恶意代码的攻击原理,设置了适用于工业网络入侵防御与检测的标准;采集符合入侵检测要求的工业网络实时数据并构建数据集,在半监督的网络模式下构建 AE-ELM 模型,并基于该模型提取输入工业网络数据的特征,通过与设置检测标准的对比与匹配,得出工业网络攻击类型的检测结果;根据网络攻击类型,从边界、传输通道、终端等方面进行防御部署,实现工业网络的安全防御;根据与传统防御方法的对比测试结果得出如下结论:综合考虑两种攻击场景,在优化设计方法的防御作用下,工业网络的数据丢失率和篡改率分别降低约 4.36%和 2.35%,即优化设计方法具有更高的安全防御效果。

关键词:半监督环境;AE-ELM 模型;工业网络;安全防御

Research on Industrial Network Security Defense Based on AE-ELM Model in Semi-Supervised Environment

LI Yuan[1], LIU Haifeng[1], CAO Botao[2]
(1. Beijing Municipal Administration Information Security Center, Beijing 100000, China)
(2. School of Mechanical and Electrical Engineering, Shaanxi University of Science and Technology, Xi'an 710021, China)

Abstract: Aiming at intrusion risk and security defense problems in industrial network, in semi-supervised network environment, an industrial network security defense method based on AE-ELM model is proposed. Based on the attack principles of attack programs, malicious data or malicious codes in different network environments, the method sets up the standards for intrusion prevention and detection of industrial networks, collects the real-time data of industrial network meeting the requirements of intrusion detection, constructs the data set. builds the AE-ELM model in the semi-supervised network mode, and extracts the data features of industrial network based on the model. The detection results of industrial network attack types are obtained by comparing and matching with the set detection standards. According to the types of network attacks, the defense is deployed from the aspects of boundaries, transmission channels, and terminals to achieve the security defense of industrial networks. According to the comparison test with traditional defense methods, the test results show that comprehensively considering the two attack scenarios and under the defense function of the optimal design method, the data loss rate and tampering rate of the industrial network are reduced by about 4.36% and 2.35% respectively, that is, the optimal design method has a higher security defense effect.

Keywords: semi-supervised environment; AE-ELM model; industrial network; security defense

0 引言

工业网络指的是安装在工业生产环境中的一种全数字化、双向、多站的通信系统。随着计算机和网络技术的广泛应用,工业网络的发展得到了很大程度上的提高,但是同时也带来了很多的安全问题[1]。由于使用了标准化的部件,传统由私有的解决方案所形成的安全壁垒已经被打破。工业网络不断向开放性和互联性发展,对其安全防护提出了严峻挑战。相对于一般的通信网络,工业网络中的设备数目更多、数据类型更加复杂,使得其安全性问题更加突出,也增加了网络安全防护的难度。工业网络的安全保护是保证网络及其相关业务完整可靠运行的基础,为了最大程度地保证工业网络的运行安全,提出工业网络安全防御方法。

收稿日期:2023-05-23; **修回日期**:2023-06-25。
作者简介:李 媛(1979-),女,硕士,高级工程师。
刘海峰(1975-),男,博士,正高级工程师。
引用格式:李 媛,刘海峰,曹博涛.半监督环境下基于 AE-ELM 模型的工业网络安全防御研究[J].计算机测量与控制,2023,31(12):244-250.

网络安全防御是一种可以提供主动防御的网络安全防护方法，它将访问控制、防火墙、入侵检测等多种安全技术结合在一起，在检测到网络或系统受到入侵攻击行为时，能够及时主动响应，自动拦截并剔除攻击数据，从而实现了对入侵攻击源的直接有效阻断。网络安全防御是一种将检测、响应和防御 3 个方面有机结合的动态、全局、纵深的信息安全防御体系，可以实现对信息系统的实时、主动、智能、自适应的保护。因此，对于网络安全防御的研究是十分必要的。从当前网络安全防御的研究情况来看，发展较为成熟的研究成果主要包括：文献［1］提出的基于时机博弈的网络安全防御方法、文献［2］提出的基于动态伪装技术的网络安全防御以及文献［3］提出的基于高斯增强和迭代攻击的对抗训练防御方法，其中文献［1］提出方法以 SIR 传染病模型为基础并加以改进，构造描述网络安全状态的微分方程，实现对网络安全状况的实时测度，在不同攻守循环策略下，求解纳什均衡，得到最优防御时机对策。文献［2］提出的安全防御方法利用网络动态变化的漏洞和缺陷，以达到发现隐藏漏洞、缺陷和后门的目的。而文献［3］提出方法将高斯干扰加入到纯净的样本中，以增强深度神经网络的泛化性能，利用 ILLC 生成的对抗性样本，对对抗性训练的内极大值进行了近似求解，得出最佳的安全防御方案。然而上述方法在实际运行过程中存在明显的防御效果不佳的问题，为此在半监督环境下，引入 AE-ELM 模型。

半监督学习是一种融合有监督和非监督的学习方式，是当前模式识别、机器学习等领域的热点问题。半监督学习利用了大量无标签的数据和有标签的数据，在模式识别中发挥了重要作用。在采用半监督学习的情况下，在保证精度的前提下，最大程度的降低人员消耗。AE-ELM 模型也就是自编码器－极限学习机模型，其中自动编码器是一种用于半监督学习的人工神经网络，它的作用是把输入的信息当作一个学习对象来表示。极限学习机是以前向神经网络为基础建立起来的一种机器学习系统或方法。自编码器－极限学习机模型能够在保持样本多子空间结构的同时，捕获样本的深层特征。利用 AE-ELM 模型优化设计工业网络安全防御方法，以期能够提升工业网络的安全防御效果，间接的提高工业网络的运行安全性。

1　工业网络安全防御方法设计

优化设计工业网络安全防御方法的基本运行思路为：根据工业网络的实时运行特征，检测工业网络当前的安全性，若发现存在入侵攻击，则判断网络攻击类型，针对当前工业网络攻击类型的检测结果，在 AE-ELM 模型的支持下，部署相应的安全防御策略，结合工业网络的攻击力度，实现工业网络的安全防御功能。

1.1　设置工业网络入侵攻击检测标准

结合工业网络的运行机理，运用对象 Petri 网的模拟工业网络的攻击过程，将入侵攻击程序下工业网络的运行特征，作为入侵攻击检测的比对标准。从工业网络结构方面来看，采用自顶向下的逻辑结构，因此工业网络的入侵方式也采用自顶向下的结构[2]。顶层 Petri 网模型能够描述工控网络中各终端设备之间的攻击顺序关系，在此基础上，拓展上层 Petri 网中每个终端节点，建立由终端目标状态及其变化所表示的变化所构成的子 Petri 网模型，从而实现适用于全工业网络的网络攻击描述。工业网络入侵攻击过程的描述主体包括网络初始状态对象、网络终端设备节点对象和网络攻击行为对象，网络攻击主体可以量化描述为：

$$\begin{cases} Q_{\text{Initial state}} = \{G, L, V\} \\ Q_{\text{terminal equipment}} = \{ID, M, IP, S\} \\ Q_{\text{aggressive behavior}} = \{ID, M, P, E\} \end{cases} \tag{1}$$

式（1）中，G、L 和 V 分别对应的是工业网络中的攻击者集合、攻击者掌握的漏洞信息以及工业网络存在的管理缺陷信息，ID、M、IP 和 S 对应的是网络节点 ID、名称、IP 地址以及状态，另外 P 和 E 分别表示攻击行为的起点对象和攻击目标终端[3]。工业网络的入侵攻击过程描述了在一个终端设备的节点中，出现的各种各样的攻击行为，会导致这个终端设备的状态发生变化。工业网络的入侵攻击过程可以量化表示为：

$$U = Q_{\text{Initial state}} \rightarrow Q_{\text{aggressive behavior}} \tag{2}$$

工业网络在实际运行过程中，容易受到的入侵攻击类型包括蠕虫病毒攻击、拒绝访问攻击和 U2R 攻击等，网络蠕虫是一种以病毒为载体，在未经使用者许可的情况下，任意地进行病毒复制或扩散的方式进行攻击。拒绝访问攻击利用了网络协议中固有的缺陷，通过不断地向服务器发送数据包的方式，从而导致了服务器无法正常提供服务。拒绝访问攻击原理如图 1 所示。

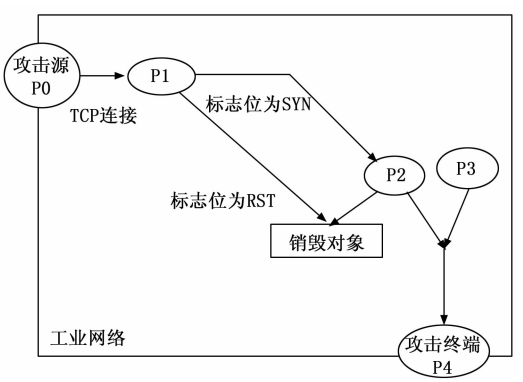

图 1　工业网络拒绝访问攻击原理图

而 U2R 则是以普通用户的身份发起，通过系统漏洞来获得普通用户的权限[4]。按照上述方式即可完成工业网络在不同类型攻击下的模拟，在不同的攻击状态下收集工业网络的运行数据，并利用式（3）提取攻击状态下工业网络实时流量的波动特征：

$$\tau_{\text{standard-fluctuate}}(i) = w_{\max} - w_{\min} \tag{3}$$

其中：w_{max} 和 w_{min} 分别为工业网络流量的最大值和最小值，式（3）的计算结果即为第 i 类攻击作用下流量波动特征的提取结果，同理可以得出工业网络的其他特征提取结果，最终通过多特征的融合得出工业网络入侵攻击检测标准的设置结果。

1.2 采集工业网络实时数据

工业网络数据采集是网络攻击防御的重要环节之一，是进行数据分析和攻击检测的前提，工业网络数据的采集能力与质量是影响网络安全防御小姑的关键因素[5]。工业网络实时运行数据的采集结果可以量化表示为：

$$x = f_{\text{gather}} \times \Delta t_{\text{gather}} \tag{4}$$

式中，f_{gather} 和 Δt_{gather} 分别为数据采集频率和采集时间[6]。为保证工业网络实时数据的采集质量，进而提升网络安全的防御效果，需要对初始采集的网络数据进行预处理，预处理步骤具体包括：平滑处理、归一化处理等，其中平滑处理过程如下：

$$\begin{cases} x(t_i) = \dfrac{(g_{\text{GET}}(num,t_i) - g_{\text{GET}}(num,t_0))}{(g_{\text{RSP}}(num,t_i) - g_{\text{RSP}}(num,t_0))} \\ x'(t_i) = \dfrac{(g_{\text{GET}}(byte,t_i) - g_{\text{GET}}(byte,t_0))}{(g_{\text{RSP}}(byte,t_i) - g_{\text{RSP}}(byte,t_0))} \end{cases} \tag{5}$$

其中：$g_{\text{GET}}(num,t_i)$、$g_{\text{GET}}(byte,t_i)$、$g_{\text{RSP}}(num,t_i)$ 和 $g_{\text{RSP}}(byte,t_i)$ 分别对应的是在 t_i 时刻统计的 GET 请求包个数和字节数、RSP 响应包个数和字节数，式（5）的输出结果 $x(t_i)$ 和 $x'(t_i)$ 分别表示时间区间 $[t_0,t_i]$ 内的数值平滑结果[7]。另外工业网络实时数据归一化处理结果为：

$$x_{\text{normalization}} = \frac{x - \bar{x}}{\sigma} \tag{6}$$

式中，$\bar{x}$ 和 σ 分别为工业网络实时数据的平均值和标准差。最终将数据预处理结果幅值给初始采集数据，重复上述流程对工业网络数据进行实时更新，完成数据的采集工作。

1.3 半监督环境下利用 AE-ELM 模型检测网络攻击类型

以实时采集的工业网络数据为研究对象，在半监督环境下，利用 AE-ELM 模型提取数据特征，通过特征匹配的方式确定当前工业网络是否存在攻击行为，针对存在攻击行为的工业网络需要进一步检测攻击类型[8]。半监督学习流程如图 2 所示。

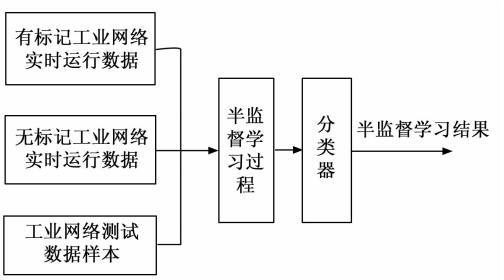

图 2 半监督学习流程图

在提取工业网络运行特征之前，首先需要构建 AE-ELM 模型，AE-ELM 模型由自编码器和极限学习机两部分组成，构建的 AE-ELM 模型结构如图 3 所示。

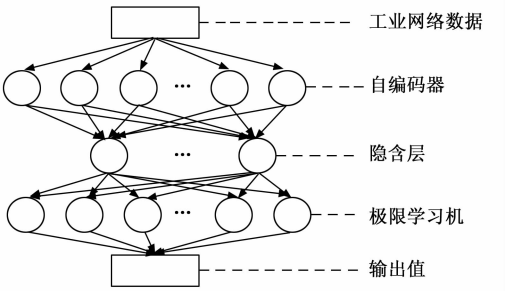

图 3 AE-ELM 模型结构图

其中，自编码器是一种用于高效编码的深度学习网络，其主要目的是为高维、复杂的数据提供一个恰当的表示，特别是在降维、特征学习等方面。自编码器自身也是一个神经网络模型，它包括输入层、隐藏层和输出层，且输入层和输出层的神经元数目相等[9]。具体地说，自编码器使得模型的输出值等于或者尽可能地接近于模型的输入值。自编码器的训练算法，主要是使用后向传播的无监督学习算法，以使得目标输出和模型输入之间的偏差最小为目标进行优化[10]。将工业网络数据设定为自编码器的输入值，并使用编码器将其确定地转换成一组二进制的隐含表达，执行前向传播过程，自编码器在前向传播过程中任意一层的输出结果可以表示为：

$$r^{(l)} = \bar{\omega}^{(l)} f_{\text{activation}}(x^{(l)}) + b^{(l)} \tag{7}$$

式中，$\bar{\omega}^{(l)}$ 和 $b^{(l)}$ 分别为第 l 层的权重值和偏置，$x^{(l)}$ 为输入到 l 层的工业网络运行数据，$f_{\text{activation}}$（）为激活函数，其函数表达式为：

$$f_{\text{activation}}(x) = \frac{1}{1+e^{-x}} \tag{8}$$

为了实现对训练样本的拟合，需要最小化网络输出值和对应标签值之间的差值[11]。由此构建自编码器的损失函数为：

$$J(\omega,b) = \frac{\sum_{i=1}^{m_{\text{Autoencoder}}} \frac{1}{2} \left\| r(x^{(i)}) \right\|_2^2 + \frac{\lambda}{2} \| \omega \|_2^2}{m_{\text{Autoencoder}}} \tag{9}$$

式中，参数 λ 为超参数。自编码器反向传播的目的是实现式（9）表示损失函数的最小化，ω 和 b 的更新结果为：

$$\begin{cases} \omega_{\text{new}}^{(l)} = \omega^{(l)} - \mu \dfrac{\partial J(\omega,b)}{\partial \omega^{(l)}} \\ b_{\text{new}}^{(l)} = b^{(l)} - \mu \dfrac{\partial J(\omega,b)}{\partial \omega^{(l)}} \end{cases} \tag{10}$$

式中，μ 为学习率。对给定的训练样本，通过正向传递操作，逐个求出各层的激活数值，其中包含输出层的激活数值。然后，针对某一自编码器节点，通过计算其剩余量来表示其对输出节点残差量的影响程度。利用输出层激活值与真实样本标记值之差，获得输出层各结点的残差值，并根据各结点的残差值加权平均，获得各结点的残差值[12]。当自编码器的学习程序满足设定的迭代条件时，退出自编码器

模块，进入极限学习机程序，极限学习机的输出结果为：

$$y_j = \sum \boldsymbol{\beta}_j f_{\text{extreme learning machine}}(\omega_j x + b_j) \tag{11}$$

其中：$f_{\text{extreme learning machine}}$（）表示极限学习机的迭代函数，$\boldsymbol{\beta}_j$ 为隐含层输出矩阵的广义逆矩阵参数。最终得出的 AE-ELM 模型的输出结果为：

$$z = \sum r^{(l)} \otimes y_j \tag{12}$$

将式（7）和式（11）的计算结果代入到式（12）中，即可得出 AE-ELM 模型的输出结果[13]。在工业网络攻击类型的实际检测过程中，利用 AE-ELM 模型提取工业网络的运行特征，具体的特征提取过程如图 4 所示。

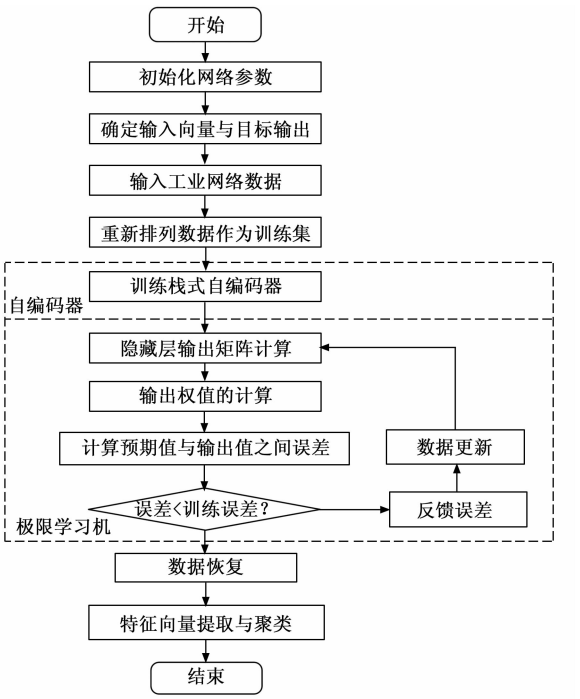

图 4　AE-ELM 模型下的工业网络特征提取流程图

按照图 4 所示的流程，将工业网络实时运行数据的采集结果输入到 AE-ELM 模型中，设置 AE-ELM 模型的最大迭代次数为 $N_{\text{iteration}}$，初始化当前迭代次数为 1，针对工业网络数据特征样本集样本进行 $N_{\text{iteration}}$ 轮训练，AE-ELM 模型的输出结果即为工业网络特征的提取结果，将其标记为 τ_{extract}[14]。根据工业网络入侵攻击检测标准的设置情况，通过特征匹配判断当前工业网络的入侵攻击类型，特征匹配结果为：

$$\psi(i) = \frac{\tau_{\text{extract}} \cdot \tau_{\text{standard-fluctuate}}(i)}{\|\tau_{\text{extract}}\| \cdot \|\tau_{\text{standard-fluctuate}}(i)\|} \tag{13}$$

式（13）的输出结果表示的是当前工业网络特征与第 i 类入侵攻击类型的匹配程度，若式（13）的计算结果高于阈值 ψ_0，证明当前工业网络存在 i 类入侵攻击行为，否则认为当前工业网络不存在 i 类入侵攻击行为，进行下一类入侵攻击类型的检测，当满足阈值条件时，退出攻击类型检测程序，并输出检测结果[15]。如果检测得出当前工业网络特征不与任何攻击类型特征相匹配，则认为当前工业网络无入侵攻击行为。

1.4　工业网络安全防御部署

在工业网络安全防御部署过程中，将工业网络分为 3 个防御区域，即网络边界、传输通道和终端装置。在网络边界范围内，建立一个清晰的网络边界，防止外界的攻击侵入到网络内部[16]。在传输通道方面，它通过监测网络中所传送的数据的内容，来及时地检测到网络中的异常情况，并做出相应的反应。在终端设备区域，通过监控终端设备的运行情况，可以及时发现并回应网络中出现的可疑终端设备或终端设备内部出现的异常行为。工业网络安全防御区域的边缘部署情况如图 5 所示。

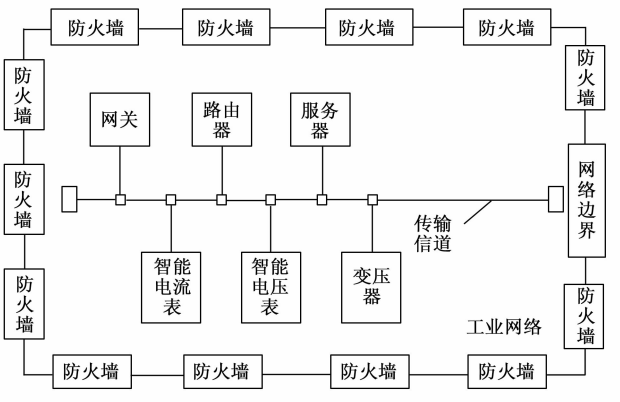

图 5　工业网络安全防御区域边缘部署示意图

针对检测存在入侵攻击行为的工业网络，进行安全防御部署，工业网络安全防御可以分为边界防御、重点防御等多个部分。边界防御技术能够对数据流中的各类恶意代码进行实时拦截。在网络入口和出口以外的地方对攻击进行防御，从某种意义上说，可以提高网络的防御能力[17]。为了应对来自内部的攻击，利用办公区和重要服务器的出入口“串联”的入侵防御模块，实时截获数据传输中的各类恶意攻击，筛选出工作区中的病毒和间谍软件，从而避免对整个网络的安全性和流控的破坏，保障重要服务器和其他重要的信息资源。为应对内外两方面的攻击，利用网络入侵防御体系，将重要的网络链接“串联”起来，实现对数据流中各类恶意攻击的实时截获。同时，还可以通过“旁路”的方法，将其应用于网络中的关键位置。

1.5　实现工业网络安全防御

工业网络的安全防御可以分为攻击响应、攻击阻断和防御执行 3 个步骤，攻击响应的任务是对报文的反馈。根据对入侵事件的报告，按照危险程度的不同，分别采取封锁、隔离、报警和记录的方法来处理。对攻击的响应有两种，一种是主动响应，另一种是被动响应。积极的响应就是在发现有人侵入时，立即采取相应的行动来进行响应，而封闭、隔离的响应则是积极的响应。阻断响应指的是对入侵的攻击源进行跟踪，并利用防火墙等手段将其与网络

的连接切断[18]。隔离是指确定攻击发生的位置，并对其进行隔离，从而能够有效地抑制攻击造成的负面影响。工业网络防御隔离数据量可以表示为：

$$N_{\text{isolate}}=\begin{cases}\dfrac{N_{\text{Industrial network}}}{1-\left[umod\left(\dfrac{1}{N_{\text{Industrial network}}}\right)\right]}*\dfrac{\xi_i}{\xi_{\text{are}}}, & \psi\geqslant\psi_0\\ 0, & \psi<\psi_0\end{cases} \tag{14}$$

其中：ξ_i 和 ξ_{are} 分别表示工业网络中各节点所承载的平均数据量和网络中数据经过多次检测后的剩余数据，$N_{\text{Industrial network}}$ 为工业网络的实时传输数据量，u 为阻断速率。被动响应就是系统仅将信息反馈给管理者，让其自行判断，而报警与记录就是被动响应[19]。在实际的工业网络安全防御过程中，根据网络攻击类型确定防御区域与节点位置，工业网络的安全防御强度为：

$$\delta=\vartheta\times A \tag{15}$$

式中，ϑ 和 A 分别表示网络的攻击强度和攻击范围。按照上述流程完成工业网络的安全防御程序，当检测到工业网络中的无入侵攻击行为时，退出安全防御程序。

2 安全防御效果测试实验分析

以测试优化设计的半监督环境下基于 AE-ELM 模型的工业网络安全防御方法的安全防御效果为目的，采用对比测试的方式设计效果测试实验。此次测试实验的基本思路为：在布设的工业网络测试环境下，编写多个不同类型的攻击程序，在不同攻击条件下运行优化设计的安全防御方法，判断优化设计方法是否能够成功实现攻击指令的防御。最终通过与多个传统安全防御方法的效果对比，体现出优化设计方法的优势。

2.1 布设工业网络测试环境

选择符合国际 ISO11519 标准的工业网络作为实验的安全防御环境，从组成架构方面来看，布设的工业网络包含智能电流表、智能电压表、变压器等设备。在工业网络测试环境的布设过程中，除基本的智能工业设备之外，需要设置一个服务器和多个网络终端节点，其中网络服务器的配置为：Celeron CPU2.66 GHz、256 M 内存、10 M/100 M 的自适应网络卡。在工业网络服务器上安装了 WEB Server 2003，并使用 IIS6.0 实现了特定的应用程序服务。为了表现工业网络的差异性，在工业网络服务器上架设两套网络系统，分别为工业网络环境和安全防御运行环境，由此能够保证基于 AE-ELM 模型的工业网络安全防御方法的运行不会影响工业网络的正常执行程序[20]。为模拟工业网络在受到攻击时的大规模并发连接，取消对网络服务器的带宽与连通性等约束，并将请求队列从有限数目变为最大数目。与此同时，对最大的工作进程数量进行了调整，为了降低在动态访问过程中，同一会话 ID 在不同进程之间不能共享所造成的影响，只开启了 2 个工作进程，这样既可以避免出现网站访问错误，又可以提升工业网络服务器的运行性能。除网络服务器外，还需要设置多个网络节点，所有网络节点的主机采用 WindowsXP，其主要配置有：1.0 GHz、384 M 存储空间、10/100 M 网络适配卡；CeleronCPU2、0 GHz、512 M 存储、10/100 M 网络适配卡；AMDAthlon3000＋1.8 GHz，512 M 存储器，10/100 M 的适配网卡。

2.2 编写工业网络入侵攻击程序

编写的入侵攻击程序包括恶意代码植入、拒绝服务两种。图 6 为恶意代码植入攻击程序的具体运行情况。

图 6 恶意代码植入攻击程序运行界面

在恶意代码植入攻击程序执行过程中，将恶意代码输入到工业网络中，启动工业网络后，恶意程序开始对网络进行扫描，利用工业网络中存在的安全漏洞，对操作员站的控制权，并在其上安装了组态软件。在获得操作者站的控制权之后，在操作者站控制软件的进程中植入配置好的恶意代码，并通过这个过程将断开开关命令发送给测控设备。由于测控设备在操作人员站发出的命令下，将开关切断并造成停电事故。同时，在开关操作中没有采取有效的消弧措施，造成了一些设备的烧坏。利用对电力设备的攻击，实现了对工业网络的间接攻击，并对工业网络的正常运行造成直接影响，实现了恶意代码植入攻击的目标。同理对拒绝服务入侵程序进行编写并添加到布设的工业网络中，又攻击节点执行攻击程序。为保证网络攻击程序的可控性，在攻击程序的起始位置加设强制中断指令，降低攻击指令对工业网络产生的实际损伤。在攻击程序执行过程中需要注意的是，不同类型的攻击程序不在同一攻击节点上执行，保证攻击程序之间互不干扰。

2.3 准备工业网络运行数据样本

实验开始之前，通过对工业网络中各个节点添加通信任务，产生工业网络的运行数据，并得出运行状态下工业网络的实时数据。准备的数据样本可以分为两个部分，第一部分就是无攻击条件下的运行数据，即不启动编写的攻击程序获取的网络实时运行数据，在此基础上，逐一启动编写的攻击程序，按照相同方式得到第二部分的样本准备结果。无攻击条件下产生的运行数据为网络安全的比对标

准数据，而攻击条件下准备的数据样本为实验的测试数据集。

2.4　设定 AE-ELM 模型运行参数

为保证优化设计的工业网络安全防御方法能够成功调用半监督环境下的 AE-ELM 模型，对模型的运行参数进行设定。根据工业网络运行数据样本的准备情况设定 AE-ELM 模型的学习速率参数为 0.002，在保证算法不陷入局部极小化的前提下，使算法快速收敛。在执行恶意代码植入攻击安全防御程序时，将批大小设置为 128，而在执行拒绝服务安全防御程序时间，批大小分别设置为 512。另外，工业网络训练集特征提取次数设置为 3，隐含层节点数为 500，退化率为 0.1，最大迭代次数设置为 200 次。

2.5　描述测试实验过程

在布设的工业网络中选择任意一个计算机作为安全防御方法的主测计算机，且在选择时保证主测计算机的选择结果与攻击程序的执行主机不为同一设备。在主测计算机中布设半监督环境，利用编程工具实现对基于 AE-ELM 模型的工业网络安全防御方法的开发与运行，并将设定的 AE-ELM 模型运行参数输入到安全防御方法的运行程序中。同时启动安全防御方法与编写的攻击程序，以准备的工业网络运行数据样本为处理对象，实现优化设计方法的安全防御功能。图 7 为工业网络安全防御方法的执行界面。

图 7　工业网络安全防御方法的执行界面

按照上述方式切换工业网络的攻击方式，得出不同攻击场景下的安全防御结果，统计攻击与防御程序作用下工业网络的实际运行结果。为体现出优化设计方法在安全防御效果方面的优势，设置传统的基于时机博弈的网络安全防御方法和基于动态伪装技术的网络安全防御方法作为实验的对比方法，重复上述流程得出不同攻击场景下的安全防御结果。

2.6　设置安全防御效果测试指标

工业网络安全攻击的最终目的是实现对网络数据的窃取或篡改，而安全防御效果的测试则是判断防御方法作用下是否能够阻断攻击源的数据窃取与篡改程序，最大程度的保证工业网络数据的完整性和正确性，因此可以设置工业网络数据的丢失率和篡改率作为反映安全防御效果的量化测试指标，其中工业网络数据丢失率的数值结果如下：

$$\eta_{\text{loss}} = \frac{N_{\text{set}} - N_{\text{net}}}{N_{\text{set}}} \times 100\% \tag{16}$$

式中，N_{set} 和 N_{net} 分别表示工业网络设置的运行数据以及防御方法作用下工业网络的实际运行数据，其中 N_{set} 的具体取值与准备的无攻击条件下的数据样本一致。另外篡改率指标的测试结果为：

$$\eta_{\text{distort}} = \frac{N_{\text{distort}}}{N_{\text{set}}} \times 100\% \tag{17}$$

其中：N_{distort} 为工业网络中的数据篡改量，通过无、有攻击条件下运行网络的对比，即可得出变量 N_{distort} 的具体取值。最终计算得出工业网络数据的丢失率和篡改率越低，证明工业网络数据的完整性和正确性更高，即对应方法的安全防御效果越优。

2.7　实验防御效果测试实验结果与分析

2.7.1　恶意代码植入攻击下的安全防御效果

在恶意代码植入攻击条件下，通过相关数据的统计，得出反映 3 种方法安全防御效果的测试结果，如表 1 所示。

表 1 的测试数据均为工业网络节点在 0.5 h 内产生的数据，将表 1 中数据代入到式（16）中，计算得出 3 种方法的平均数据丢失率分别为 4.41%、1.95% 和 0.47%，通过式（17）的计算得出 3 种方法数据篡改率的平均值分别为 4.32%、

表 1　恶意代码植入攻击下网络安全防御效果测试数据表

工业网络节点编号	设置运行数据量/GB	基于时机博弈的网络安全防御方法		基于动态伪装技术的网络安全防御方法		半监督环境下基于 AE-ELM 模型的工业网络安全防御方法	
		实际运行数据量/GB	篡改数据量/GB	实际运行数据量/GB	篡改数据量/GB	实际运行数据量/GB	篡改数据量/GB
1	14.6	14.0	0.8	14.3	0.3	14.5	0.1
2	23.4	22.6	0.9	23.1	0.5	23.4	0.1
3	22.5	21.7	0.7	22.2	0.6	22.5	0.1
4	18.9	18.0	0.6	18.4	0.4	18.7	0.2
5	20.1	18.8	1.0	19.7	0.5	20.0	0.1
6	16.8	16.1	0.9	16.4	0.6	16.7	0.2

2.50%和 0.72%。

2.7.2 拒绝服务攻击下的安全防御效果

将工业网络的攻击程序切换至拒绝服务攻击，统计该场景下的通过安全防御得出的工业网络实际运行数据，通过式（16）和（17）的计算，得出该场景下反映 3 种方法安全防御效果的测试结果，如图 8 所示。

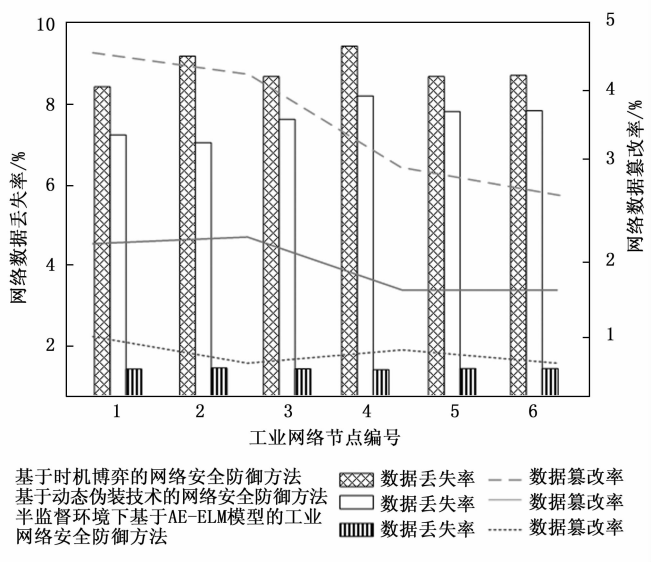

图 8 拒绝服务攻击下安全防御效果测试对比结果

从图 8 中可以看出，与两种对比方法相比，在优化设计方法的安全防御下，工业网络的数据丢失率和篡改率明显降低，降低量约为 6%和 2%。

3 结束语

安全防御的核心功能是精准拦截与深层防御，在保证安全的前提下，改善检测技术以提高其对入侵的探测准确率，并在此基础上进一步提升自身的性能，是未来工业网络的发展方向。安全防御的重点是确保网络环境的可信性、网络状态的可知性和网络的可控制性。工业网络安全防御有助于进一步明确网络的安全防护目标，为整个网络的安全防护问题提供了一个完整的解决方案，并将推动行业内对工业互联网的安全防护意识的转变。针对目前工业网络安全防御的不足，在半监督环境下优化设计的安全防御方法，并构建了相应的防御措施，从实验结果中可以看出，优化设计方法能够成功实现对恶意代码植入和拒绝服务对工业网络的攻击，对于工业网络的安全发展起到正面作用。

参考文献：

[1] 孙鹏宇，张恒巍，谭晶磊，等．基于时机博弈的网络安全防御决策方法［J］．计算机工程，2022，48（11）：145－151.

[2] 丁朝晖，张 伟，杨国玉．基于动态伪装技术的网络安全防御系统研究［J］．电子技术应用，2022，48（1）：129－132.

[3] 王丹妮，陈 伟，羊 洋，等．基于高斯增强和迭代攻击的对抗训练防御方法［J］．计算机科学，2021，48（S1）：509－513.

[4] 王 翡．基于大数据的计算机网络安全防御系统探究［J］．数字通信世界，2023（3）：155－157.

[5] 孙凯祺，邱 伟，李可军，等．面向快速频率响应系统的网络攻击防御控制策略［J］．中国电机工程学报，2021，41（16）：5476－5486.

[6] 贾 焰，方滨兴，李爱平，等．基于人工智能的网络空间安全防御战略研究［J］．中国工程科学，2021，23（3）：98－105.

[7] 赵 伟，周颖杰，李政辉，等．一种基于少量异常标签的 SQL 注入攻击检测方法［J］．四川大学学报（自然科学版），2022，59（6）：39－47.

[8] 张晓琴，汪云飞，胡春强．基于改进极限学习机的数据采集与监控系统攻击检测模型［J］．南京航空航天大学学报，2021，53（5）：708－717.

[9] 王振东，刘尧迪，杨书新，等．基于天牛群优化与改进正则化极限学习机的网络入侵检测［J］．自动化学报，2022，48（12）：3024－3041.

[10] 丑义凡，易 波，王兴伟，等．IPv6 网络中基于 MF-DL 的 DDoS 攻击快速防御机制［J］．计算机学报，2021，44（10）：2047－2060.

[11] 赵玉明，顾慎凯．融合残差密集块自注意力机制和生成对抗网络的对抗攻击防御模型［J］．计算机应用，2022，42（3）：921－929.

[12] 潘 刚，米士超，郭荣华，等．基于攻击树和 CVSS 的网络攻击效果评估方法［J］．电子技术应用，2022，48（4）：76－80.

[13] 李元诚，杨珊珊．基于改进自注意力机制生成对抗网络的智能电网 GPS 欺骗攻击防御方法［J］．电力自动化设备，2021，41（11）：100－106.

[14] 刘向举，刘鹏程，路小宝，等．基于 SD-IoT 的 DDoS 攻击防御方法［J］．计算机工程与设计，2021，42（11）：3001－3008.

[15] 陈晋音，胡书隆，邢长友，等．面向智能渗透攻击的欺骗防御方法［J］．通信学报，2022，43（10）：106－120.

[16] 马 吉，杜永文，夏金棕．基于独立监督网络的选择性转发攻击检测［J］．传感技术学报，2022，35（4）：538－544.

[17] 王晓鹏，罗 威，秦 克，等．一种针对快速梯度下降对抗攻击的防御方法［J］．计算机工程，2021，47（11）：121－128.

[18] 张恩宁，王 刚，马润年，等．采用双异质群体演化博弈的网络安全防御决策方法［J］．西安交通大学学报，2021，55（9）：178－188.

[19] 张春花，马竟宵．车联网中基于短期标识的 Sybil 攻击防御方法［J］．小型微型计算机系统，2021，42（8）：1727－1734.

[20] 刘广睿，张伟哲，李欣洁．基于边缘样本的智能网络入侵检测系统数据污染防御方法［J］．计算机研究与发展，2022，59（10）：2348－2361.