文章编号:1671-4598(2026)02-0135-08 DOI:10.16526/j.cnki.11-4762/tp.2026.02.018 中图分类号:TP309 文献标识码:A

基于回声状态网络识别的网络安全设备联动系统设计

梁 雄[1],杨 煊[1],梁才志[2]
(1.国能朔黄铁路发展有限责任公司 信息中心,河北 沧州 062350;
2.广东轻工职业技术大学 计算机中心,广州 510300)

摘要:网络环境具有复杂性和变化性,使得系统难以及时发现网络中的异常行为或攻击,且联动系统不同设备间无法有效实现数据共享,从而使网络安全设备联动系统无法有效应对新型恶意攻击,导致阻断响应时间长、丢包率高的问题;因此,采用回声状态网络识别对网络安全设备联动系统设计进行研究;在网络安全设备联动系统硬件设计中,为确保联动系统不同设备间可有效实现数据共享,采用开放接口方式,将各自独立的防火墙、入侵检测系统等各设备通过接口连接,实现信息的共享,确保有效实现联动,并使用 NetFlow Collector、Apache Spark 和 Snort 处理模块进行信息采集、处理和检测;然后通过 Cobalt Strike 设备联动决策装置,触发联动控制机制,并通过利用 WatchGuard 联动控制平台,实现网络设备联动防御;在软件设计中,为提高异常检测的准确性,在 Snort 处理模块中引入回声状态网络展开各设备数据异常检测,并在此过程中利用二进制粒子群算法对回声状态网络储备池参数进行优化,以提升其检测性能;最后,基于检测结果,为提高关联的全面性和准确性,先利用贝叶斯网络对检测获得的来自不同安全设备的异常数据结果进行融合,以此作为输入在 Cobalt Strike 设备中采用改进 FUP 算法进行网络安全事件关联挖掘,以发现潜在攻击信息,并提交给决策层的策略判决点进行策略触发,通过检索相应处理策略完成策略触发,最终策略判决点将安全事件处理策略命令下达给 WatchGuard 联动控制平台,从而完成联动操作;由测试结果可知,该系统总体阻断响应时间仅为 184 s,系统丢包率最小值为 0.05,具有高效联动效果。

关键词:HTTP 包识别;网络安全;设备联动;联动控制机制

Design of Network Security Equipment Linkage System Based on Echo State Network Recognition

LIANG Xiong[1], YANG Xuan[1], LIANG Caizhi[2]
(1. Information Center, Guoneng Shuohuang Railway Development Co., Ltd., Cangzhou 062350, China;
2. Computer Centre, Guangdong Industry Polytechnical College, Guangzhou 510300, China)

Abstract: The complexity and variability of network environments make it difficult for systems to detect abnormal behaviors or attacks in a timely manner, and the linkage system between different devices cannot effectively share data, which makes the network security device linkage system unable to effectively respond to new malicious attacks, resulting in long blocking response time and high packet loss rates. Therefore, a network security device linkage system using echo state network recognition is designed. In the hardware design of the network security device linkage system, to ensure effective data sharing between different devices in the linkage system, an open interface method is adopted, which connects independent firewalls, intrusion detection systems, and other devices through interfaces to achieve information sharing and ensure effective linkage. The NetFlow Collector, Apache Spark, and Snort processing modules are used for information collection, processing, and detection. Then, through the Cobalt Strike device linkage decision-making device, the linkage control mechanism is triggered, and the WatchGuard linkage control platform is used to achieve the linkage defense of network devices. In its software design, to improve the accuracy of anomaly detection, an echo state network is introduced into the Snort processing module to carry out the anomaly detection of various device data. During this process, the binary particle

收稿日期:2025-04-16; **修回日期**:2025-06-19。
作者简介:梁 雄(1982-),男,大学本科,工程师。
引用格式:梁 雄,杨 煊,梁才志.基于回声状态网络识别的网络安全设备联动系统设计[J].计算机测量与控制,2026,34(2):135-142,150.

swarm optimization algorithm is used to optimize the parameters of the echo state network reserve pool to improve its detection performance. Finally, based on detection results, in order to improve the comprehensiveness and accuracy of the association, the Bayesian network is first used to fuse the abnormal data results obtained from different security devices. As an input, an improved FUP algorithm is used in the Cobalt Strike device for network security event association mining to discover potential attack information and submit it to the policy decision point of the decision-making layer for policy triggering. The corresponding processing strategy is retrieved to complete the policy triggering. Finally, the policy decision point issues the security event processing strategy command to the WatchGuard linkage control platform, thereby completing the linkage operation. The test results show that the overall blocking response time of the system is only 184 s, and the minimum packet loss rate of the system is 0.05, indicating an efficient linkage effect.

Keywords: HTTP packet recognition; network security; equipment linkage; linkage control mechanism

0 引言

互联网普及与信息科技的飞速发展，使得网络安全性也随之凸显出来。各种网络攻击手段不断出现，给企业和个人带来了巨大的安全威胁。为了应对这些攻击，各种网络安全设备被广泛应用于企业网络中，如防火墙、入侵检测系统、反病毒软件等。这些设备各自具备不同的功能和特点，但它们之间的联动和协同作战能力却往往被忽视了。在传统的网络安全管理系统中，各种设备之间的信息共享和协同作战能力有限，无法充分发挥整体效能。例如，当入侵检测系统检测到一次攻击时，它只能独立地进行响应，而不能与其他设备进行联动，共同抵御攻击。这不仅影响了防御效果，也增加了管理员的管理难度和维护成本。因此，设计一种网络安全设备联动系统，实现各种设备之间的信息共享和协同作战，提高整体防御能力，已成为网络安全领域亟待解决的问题。

文献［1］提出了基于协议特征的检测方法，通过分析网络流量中的协议特征，检测异常行为，进而触发网络安全设备的联动。但该方法在实际应用中，其协议特征在正常的网络通信中也可能出现，但并不一定代表异常行为，导致过多的虚警，增加了管理员的处理负担，降低了系统的可信度；文献［2］提出基于行为的电力网络安全事件联动响应及协同处置方法。利用DoS/DDoS攻击检测方法，关联所有防御方式检测电力网络中的安全事件。根据攻击行为的具体IP位置，启动联动响应及协同处置平台，实现电力网络安全事件联动响应及协同处置。然而，在实际应用中，由于网络环境的复杂性和多样性，该方法的丢包率较高，导致各设备间联动性较差。文献［3］提出了基于深度特征融合网络的网络安全设备联动方法，利用深度特征融合网络，对网络流量进行多层次特征提取和融合，以检测异常行为。当检测到异常行为时，联动系统会触发防御和响应功能。但该方法在实际应用中未考虑特定网络环境和场景的特点，导致在面对新型恶意攻击时，存在较高的丢包率；文献［4］提出了基于BP神经网络的监测系统，采用BP神经网络训练并学习网络流量，并利用该模型对实时网络流量进行异常检测，进而触发联动系统。由于网络环境和威胁形势不断变化，当该方法在应对新型恶意攻击时，BP神经网络的模型需要及时更新和调整，以适应新出现的威胁和攻击方式，导致阻断响应时间较长。文献［5］提出基于蜜网技术的网络安全监控系统。通过引入特征生成算法对单个与多个多态蠕虫病毒进行特征生成，实现了对网络流量模式的建模。在分析网络管控特点的基础上，采用数据挖掘技术实现网络对数据的识别、分析、存储，并允许管理人员实时管控。尽管蜜网技术在检测和分析网络攻击方面表现出优越性，但仅仅依赖蜜网技术可能会面临单一技术带来的局限性。例如，蜜网系统主要侧重于吸引和捕获攻击者，但对于已经渗透到网络内部的威胁可能检测能力有限，影响最终的效果。文献［6］中提出网络安全多层协同联动控制系统。利用图灵计算模型设计协同联动控制子系统形式，构建该子系统存储模块，接口模块与协同联动引擎模块，完成多层联动控制系统设计。在多层协同联动控制系统中，可能需要处理大量的网络数据以进行威胁检测和响应，导致检测效果不佳，影响最终的联动效果。

回声状态网络（ESN，echo state networks）具有良好的泛化能力，能够学习识别数据中的模式，即使该数据与训练数据略有不同。这使得ESN能够较为准确地根据日志数据的攻击类型进行分类，提高异常检测的准确性。且具有在线学习能力，无需在每次看到新数据时都重新训练。这对于网络安全领域尤为重要，因为新的攻击模式可能随时出现，需要系统能够实时学习和适应。此外，网络安全设备的日志数据长度可能不一致，ESN能够处理不同长度的输入数据，这使得它非常适合处理这类数据。因此，在上述文献方法所存在问题的基础上，为提高异常检测准确性，以提升阻断响应速度，降低丢包率，以提升网络安全设备联动，以应对快速变化的网络威胁，设计了基于回声状态网络识别的网络安全设备联动系统。

1　网络安全设备联动系统设计

当前网络深度应用网络中的日志数据量越来越大，其中包含着网络运行、安全和状态等关键信息，因此，为了高效地利用这些数据，需要设计网络安全设备联动系统[7]。因此该系统主要基于对各网络安全设备日志数据的采集，并对源数据进行异常检测，以进一步提高后期关联分析和决策的准确性，提升网络安全设备联动效果，降低丢包率。然后基于预先处理过的数据进行关联性分析，对网络系统中的异常行为进行实时监测和预警，同时对运行的各类设备进行联动，保障整个网络系统的安全。

1.1　网络安全设备联动系统框架

在网络安全设备联动系统中，关键在于对各网络安全设备日志数据的异常检测，其检测的准确性，则直接影响后续事件的关联和联动决策。因此，在网络安全设备联动系统设计中，采用开放接口方式，将各自独立的防火墙和入侵检测系统通过接口连接，在连接点加入联动控制台，通过接口调用的方式实现信息的共享，进而实现一体化防御。在此方式中，联动控制台成为整个系统的中心，防火墙和入侵检测系统等的消息均汇集于此，待做出全面分析后，根据各自结果采取一定的措施，从而实现主动的联动防御。则网络安全设备联动系统框架如图 1 所示。

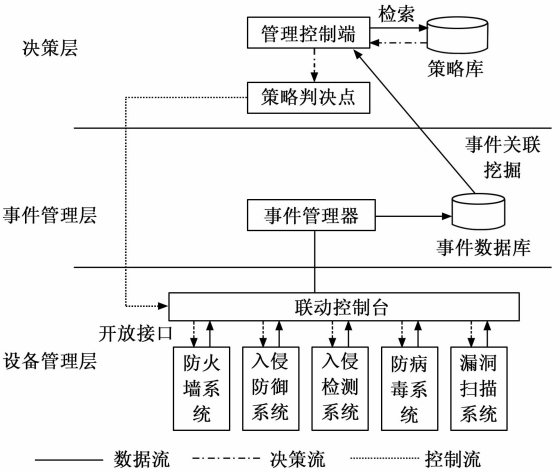

图 1　网络安全设备联动系统框架图

由图 1 可知，安全设备联动体系中主要包括设备管理层、事件管理层和决策层 3 层架构，以及事件流、决策流两类数据传输流。

在设备管理层，在连接点加入联动控制台，在该平台中由适配器代理程序分别采集防火墙、入侵防御系统、漏洞扫描器、防病毒系统等需要联动的安全设备日志，将设备原始日志初步过滤并去除冗余后，按照 Syslog 标准进行格式统一，上传至事件管理层的事件管理器中。事件管理器对接收到的安全事件进行关联分析与合并，将安全事件存储到安全事件数据库中。决策层的条件触发器接收来自事件数据库中的触发条件，然后到策略知识库中查询相应的安全策略，最终安全策略通过动作执行器向各个安全设备的适配器代理程序下发，由代理根据策略的命令改变各设备的相关配置从而完成联动操作。

1.2　网络安全设备联动系统硬件设计

1.2.1　网络安全设备联动信息采集与处理模块

在设备管理层使用 NetFlow Collector 的数据采集器，能够从网络设备（如路由器和交换机）中收集日志数据信息[8]。并将网络安全设备的日志数据信息进行汇总，并将其转化为信息处理模块。

然后使用 Apache Spark 大规模数据处理工具，来对数据进行快速并行处理。将采集到的原始日志数据进行清洗、归并和格式转换等操作，以便后续处理。这个过程可以通过 Spark Core 进行分布式处理，利用其强大的计算能力和并行处理能力，可以高效地处理大规模的数据[9-10]。

同时采用 Fiddler 网络调试代理，定时将安全装置的工作状况、统计资料，以及收集代理的工作状况等信息传输给信息处理中心[11-12]。最后，通过 Snort 轻量级的开源入侵检测与防御系统（IDS/IPS），对各类网络设备的数据进行检测，以对攻击进行实时监测，并基于关联规则完成对网络攻击的有效防御[13]。则网络安全设备联动信息采集与处理模块架构如图 2 所示。

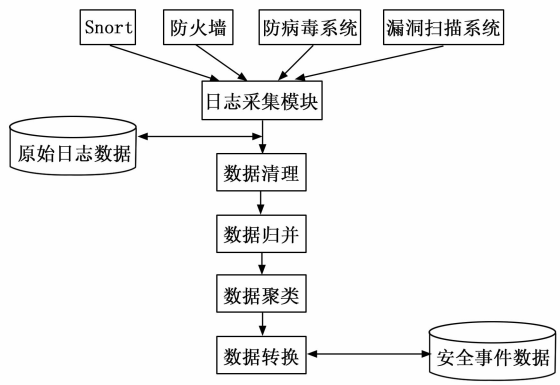

图 2　信息采集与处理模块架构示意图

1.2.2　网络设备安全分析与设备联动决策模块

在事件管理层网络设备安全分析模块主要是通过对网络安全状态的综合分析，通过关联算法对各事件进行关联，来判定网络中存在的威胁程度，从而发现安全保护体系中的弱点。在联动数据库支撑下，设备联动决策模块利用人工智能方法，对网络攻击种类及威胁程度进行了分析，以帮助网络安全管理者作出决策。

使用 Cobalt Strike 设备联动决策装置，该设备是一种高级的渗透测试工具，它可以模拟真实的网络攻击场

景，并提供实时的防御建议和联动控制建议[14-15]。Cobalt Strike 具有攻击模拟、防御建议、联动控制等功能，可以快速地评估网络的安全性和防御能力。

Cobalt Strike 通过与 Snort 等安全分析装置的集成，可以获取实时安全事件信息。它对收集到的安全事件与事件数据库进行关联分析，识别出潜在的安全威胁和攻击行为，触发联动控制机制。以使其在面对新型恶意攻击时，具有较好的联动防御效果。

网络设备安全分析与设备联动决策模块结构如图 3 所示。

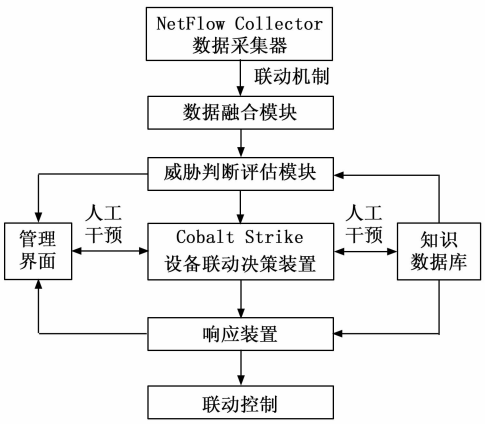

图 3 网络设备安全分析与设备联动决策模块结构

由图 3 可知，当 Snort 检测到异常数据包时，它会将警报信息发送给 Cobalt Strike，Cobalt Strike 根据接收到警报信息进行关联分析，得出潜在的安全威胁和攻击行为。利用联动机制对每一种安全设备采取一种联动机制，阻止攻击，启动杀毒进程[16]。同时，对事件进展进行实时追踪，并对相应措施调整。网络设备根据接收到的建议和措施执行相应的操作，如关闭受攻击的服务、隔离攻击源等，以保护网络的安全。

1.2.3 联动控制平台

采用 WatchGuard 联动控制平台，可有效实现防火墙入侵检测、内容过滤等一系列安全措施[17]。联动控制平台通过连接各个代理程序，对具体的事件进行推理整合，然后传给 Snort 进行异常检测。并可通过联动控制功能，将 WatchGuard 可与其他安全设备和系统进行集成，依据决策层所给出的安全事件处理策略命令以及设备联动决策模块的联动机制，实现各设备的相关配置的改变，从而完成联动防御操作。该平台结构如图 4 所示。

1.3 网络安全设备联动系统软件设计

基于上述分析可知，该系统主要是通过联动控制平台进行源数据异常检测，然后由事件管理器进行数据关联性分析，完成设备联动，保障整个网络系统的安全。其关键是各网络安全设备日志数据的精准异常检测，来

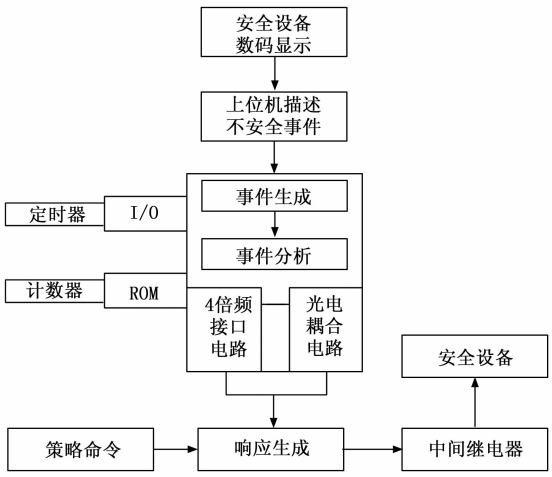

图 4 联动控制子系统结构

提升网络安全设备联动效果，降低丢包率。因此，针对源数据异常检测来展开对网络安全设备联动系统的软件设计。

1.3.1 基于回声状态网络识别的网络设备源数据异常检测

为了进一步提高后期关联分析和决策的准确性，确保网络安全设备联动效果，使用回声状态网络对日志数据进行聚类分析，将日志划分为数个聚类数据集，来完成异常检测。

回声状态网络核心结构是网络中的储备池，储备池是由随机稀疏连接的神经元组成，可以对输入的数据进行高维和非线性的表示的结构[18-19]。回声状态网络的训练过程和储备池的生成过程是两个相互独立的过程，因此，储备池至输出层的权值只需要采用线性方法训练即可得到，这在很大程度上简化了其训练过程。同时回声状态网络在稳定性、全局最优性、收敛速度和训练复杂度等方面相对于传统神经网络算法有了很大提高和改善，因此，将其应用于日志预处理中，实现了日志数据的聚类分析，以完成异常检测[20-21]。回声状态网络的典型网络结构如图 5 所示，由输入层、储备池、输出层图中组成，其中储备池对应传统神经网络模型的隐含层，但内部连接权值的生成方式不同。

图 5 中实线连接权值表示 ESNs 的基本连接权值，是 ESNs 中必不可少的；虚线连接权值表示 ESNs 的可选连接权值，可根据具体问题确定是否选择。

假设系统具有 K 个输入单元，N 个内部处理单元，同时具有 L 个输出单元，则在第 t 个时刻，输入层状态 $u(t)$、储备池状态 $x(t)$、输出层状态 $y(t)$ 由公式 (1) 来计算获得：

$$\begin{cases} u(t) = [u_1(t), u_2(t), \cdots, u_M(t)]^T \\ x(t) = [x_1(t), x_2(t), \cdots, x_K(t)]^T \\ y(t) = [y_1(t), y_2(t), \cdots, y_L(t)]^T \end{cases} \tag{1}$$

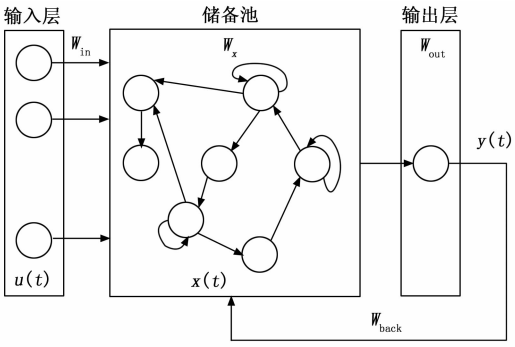

图 5　ESNs 的网络结构

ESN 的储备池状态 $x(t)$ 和 $t+1$ 时刻的输出层状态 $y(t+1)$ 由公式（2）和公式（3）计算：

$$x(t+1) = f[\boldsymbol{W}_{\text{in}}u(t+1) + \boldsymbol{W}_x x(t) + \boldsymbol{W}_{\text{back}}y(t)] \quad (2)$$

$$y(t+1) = f_{\text{out}}\{\boldsymbol{W}_{\text{out}}[x(t+1);u(t+1);y(t)]\} \quad (3)$$

其中：$\boldsymbol{W}_x$、$\boldsymbol{W}_{\text{in}}$，$\boldsymbol{W}_{\text{out}}$ 分别为储备池状态矩阵，输入层到储备池的连接权值矩阵和储备池到输出层的连接权值矩阵；$\boldsymbol{W}_{\text{out}}$ 为唯一需要训练的变量，而其他变量，如，$\boldsymbol{W}_x$ 和 W_{in} 都在训练过程中保持不变；f 和 f_{out} 分别是动态储备池和输出层的激活函数，通常使用 Sigmoid 函数和双曲正切函数来表示。ESN 的动态储备池类似于复杂的非线性动态滤波器，会随着输入而发生变化。

ESN 的实现过程分为 4 个阶段，分别为网络初始化、网络更新和采集、网络训练阶段以及网络测试阶段。

1）网络初始化：

初始化 ESN 的储备池规模 N、储备池谱半径 R、稀疏度 C 以及输入变换因子 S 等参数。初始化网络连接权值矩阵 $\boldsymbol{W}_x$、$\boldsymbol{W}_{\text{in}}$、$\boldsymbol{W}_{\text{back}}$。此外，还需设置储备池的初始状态 $x(0)=0$。为更好地适应特定任务或降低过拟合和病态的可能性，现利用优化的二进制粒子群算法（BPSO，binary particle swarm optimization）对储备池规模 N、储备池谱半径 R、稀疏度 C 进行确定，完成网络初始化，具体如下：

步骤 1：初始化

ESN 参数设置：定义 ESN 的初始参数，储备池规模 N、储备池谱半径 R、稀疏度 C。

BPSO 参数设置：定义粒子群的大小、迭代次数、惯性权重、加速系数等。

初始化粒子群：每个粒子代表 ESN 的一组参数配置，随机初始化粒子的位置和速度。

步骤 2：计算适应度值

使用当前粒子的参数配置训练 ESN，选用均方误差（MSE）作为适应度函数，获得每个粒子的适应度值，以此结果评估每个粒子的性能。

步骤 3：迭代优化

对于每个粒子，如果当前位置的适应度值优于其历史最优解，则更新个体最优解。在所有粒子中找出适应度值最优的粒子，更新全局最优解。接着根据个体最优解和全局最优解，以及粒子的当前速度和位置，更新粒子的速度和位置。粒子 i 的速度 v_i 更新公式如下：

$$v_{i+1} = wv_i + c_1 r_1(p_{\text{Best}_i} - x_i) + c_2 r_2(p_{\text{Best}} - x_i) \quad (4)$$

式中，w 为惯性权重，c_1 和 c_2 学习因子，r_1 和 r_2 为 $[0,1]$ 之间的随机数，p_{Best_i} 为历史最优解，p_{Best} 全局最优解。由于这是二进制粒子群算法，速度和位置的更新需要采用二进制编码的特定方式，如使用 Sigmoid 函数将速度转换为 0～1 之间的概率，然后依据概率决定位置的二进制位是否翻转。则使用 Sigmoid 函数将速度 v_i 转换为位置更新的概率具体表示如下：

$$S(v_{i+1}) = \frac{1}{1+e^{-v_{i+1}}} \quad (5)$$

对于粒子 i 的每个二进制位 x_i，根据 Sigmoid 函数的输出 $S(v_{i+1})$ 来决定是否翻转该位，表示如下：

$$x_{i+1} = \begin{cases} 1, \text{if} \quad random() < S(v_{i+1}) \\ 0, \text{otherwise} \end{cases} \quad (6)$$

步骤 4：终止条件

如果全局最优解的适应度值达到了最小，则提前终止算法，输出全局最优解对应的 ESN 参数配置。否则，继续重复上述步骤 3 内容。

综上，完成网络初始化，并在此基础上，进行后续的网络更新和采集。

2）网络更新和采集：

ESN 根据公式（2）更新储备池状态，并且采集网络的状态信息，注意在采集网络 时要舍弃初始阶段的网络状态，这是为了避免初始状态的随机性对 ESN 产生影响。假设训练样本个数为 M 个，舍弃的前 I 个样本，从 $(I+1)$ 输入样本开始采集，则采集的内部状态矩阵 $\boldsymbol{P}$ 如下所示：

$$\boldsymbol{P}\begin{bmatrix} x_1(1) & x_1(2) & \cdots & x_1(M-1) & x_1(M) \\ x_2(1) & x_2(2) & \cdots & x_2(M-1) & x_2(M) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_K(1) & x_K(2) & \cdots & x_K(M-1) & x_K(M) \end{bmatrix} \quad (7)$$

3）网络训练阶段：

ESN 通常采用岭回归法求解输出权值矩阵 $\boldsymbol{W}_{\text{out}}$，具体的求解过程如下：

$$T = \boldsymbol{W}_{\text{out}} * \boldsymbol{P} \quad (8)$$

$$\boldsymbol{W}_{\text{out}} = T\boldsymbol{P}^{-1} \quad (9)$$

其中：T 为目标值。由于 $\boldsymbol{P}$ 不一定是方阵，因此 ESN 一般采用 $\boldsymbol{P}$ 的伪逆 $\boldsymbol{P}^{+}$ 代替 $\boldsymbol{P}^{-}$，在 Matlab 中提供了伪求逆函数 $pinv$。

4）网络检测阶段：

训练得到输出矩阵后，将其代入公式（3）中，然后根据公式（3）完成网络设备源数据异常检测。

综上，在设备管理层完成对所采集的各个设备源数据的异常检测，以为后续网络安全事件关联奠定基础，提高关联的准确性，以确保决策的有效性，提升网络安全设备联动效果。

1.3.2 基于改进 FUP 算法的网络安全事件关联挖掘

接下来，事件管理层在安全设备日志数据进行异常检测的基础上运用关联分析，对将要发生的安全风险事件与事件数据库中的事件进行关联，发现其中的攻击信息，可以进行警示和自动防护处理。

而在网络安全设备联动系统中，事件数据库是不断变化的，因此需要使用增量关联算法（FUP，fast update algorithm）对事件进行关联[22-23]。在此之前，为提高关联的全面性和准确性，现利用贝叶斯网络对上述检测的来自不同安全设备的异常数据结果进行融合，以此作为输入，进行网络安全事件关联挖掘。根据上述检测所得数据，来提取其关键特征，包括事件的时间戳、源 IP 地址、目的 IP 地址、端口号、协议类型、事件类型（如扫描、攻击尝试等）等。基于此，构建贝叶斯网络。在贝叶斯网络中，节点代表特征，边代表特征之间的依赖关系。使用贝叶斯定理来结合不同数据源的概率信息，来对来自不同安全设备的异常数据进行融合，通过计算后验概率，可以评估不同事件之间的关联性，并整合多个数据源的信息。具体如下：

$$P(X)=\frac{P(X\mid A)P(A)+P(X\mid B)P(B)}{P(A)+P(B)} \tag{10}$$

式中，$P(X\mid B)$ 为数据源 B 发生时事件 X 发生的概率，$P(X\mid A)$ 为数据源 A 发生时事件 X 发生的概率，$P(A)$ 和 $P(B)$ 分别是数据源 A 和 B 的先验概率。

将融合后的数据输入到 FUP 算法中进行事件关联分析。FUP 算法可以帮助识别和分析事件之间的潜在联系，从而发现复杂的攻击模式或异常行为。FUP 算法的基本流程包括多个循环，在第一次循环中，算法会扫描数据集，计算各项的支持度，并根据支持度阈值筛选出频繁项集。在后续的循环中，算法会进一步处理非频繁项集，并更新频繁项集。然而，FUP 算法需要进行频繁的事务数据库扫描，当数据量很大时，这可能会成为算法的性能瓶颈。因此，减少计算量，提高增量关联规则挖掘的计算效率，将 FUP 算法与压缩布尔矩阵相结合，来完成网络安全事件关联挖掘。算法的基本思想：要充分利用原数据库的检测结果，缩减原始数据库的扫描次数，同时不断的压缩事务数据库，去除与频繁项集无关的项目集，减少挖掘过程中产生候选项集的数目，从而降低算法的复杂度，改善算法的性能。具体实现过程描述如下：

在原始数据库中新增异常事件数据集 db 后，数据库 $DB\cup db$ 的频繁项集 X 可以分为 3 种情况：1）X 在 DB 和 db 中均是频繁的；2）X 为 DB 中的频繁项集，db 中的非频繁项集；3）X 为 db 中的频繁项集，DB 中的非频繁项集。

接下来，基于上述情况展开关联挖掘，令项集为 $I=\{i_1,i_2,\cdots,i_n\}$，事务数据库为 $D=\{t_1,t_2,\cdots,t_m\}$，此时，事务矩阵 $\boldsymbol{TM}$ 的每一个元素 $\{A_{ij}\}$ 定义为：

$$\{A_{ij}\}=\begin{Bmatrix}1 & \text{若 } i_j\in t_i\\ 0 & \text{若 } i_j\notin t_i\end{Bmatrix},$$
$$i=1,2,\cdots,m,j=1,2,\cdots,n \tag{11}$$

则事务矩阵中，定义项 I_j 的向量为 $\boldsymbol{TM}_j=(A_{1j},A_{2j},\cdots,A_{mj})$，而 I_j 的支持度计算公式如下：

$$supp(I_j)=\sum_{i=1}^{m}A_{ij} \tag{12}$$

由此，根据上述步骤可构建一个 $m+1$ 行 $n+1$ 列的布尔矩阵 $\boldsymbol{TM}_{(m+1)\times(n+1)}$，其中，$m$ 代表事务数，n 代表总项目个数。设最小支持度是 $support_{\min}$，则根据公式（12）来计算事务矩阵 $\boldsymbol{TM}_{(m+1)\times(n+1)}$ 中每一行向量的支持度，并与最小支持度进行比较。

如果事务矩阵 $\boldsymbol{TM}_{(m+1)\times(n+1)}$ 某行的支持度小于等于最小支持度是 $support_{\min}$，则将其从矩阵中删除。最后，重新计算新的最小支持度并重复此过程，直到没有事务被删除为止。

经上述压缩过程，当频率 $k>1$ 时，设压缩后的事务矩阵为 $\boldsymbol{TM}_{s\times r}$，对 $\boldsymbol{TM}$ 的前 $r-1$ 列任意 k 个列进行组合，共有 C_{r-1}^{k} 种组合。对每个组合相应的列进行预运算，若结果中 1 的个数大于等于 $support_{\min}$，则此组合对应的项集为频繁 k-项集。

综上，完成对将要发生的安全风险事件与事件数据库中的事件的关联挖掘，以能够实现安全事件的预警。由此，将关联结果提交给决策层的策略判决点进行策略触发，管理控制端通过检索相应处理策略完成策略触发，并将触发策略返回给策略判决点。最后，策略判决点将安全事件处理策略命令下达给设备管理层中联动控制平台的各个代理，代理根据策略的命令改变各设备的相关配置从而完成联动操作。

2 系统性能测试

2.1 测试环境搭建及测试步骤

为了验证基于回声状态网络识别的网络安全设备联动系统设计合理性，必须对多台网络安全设备进行监控。

所涉及的安全设备主要有防火墙、交换机、Snort 服务器和主机。在搭建的实验平台中，采用思科 PIX-506E 防火墙作为内网和外网的安全设备，思科 WS-C2960 交换机作为汇聚层的数据传输设备，在交换机的网段内安装了一台 Snort 入侵检测系统服务器。

接着依据上述测试环境，采用 Syslog 采集方式采

集防火墙、交换机和主机日志数据。通过在 windows 系统上建立日志服务器，Syslog 日志服务器选用 kiwi syslog daemon。其中日志服务器负责接收各网络设备发来的日志数据，接收到的日志数据以文本格式储存。对接收的日志文本文件进行分解，将数据存入数据库中。然后利用回声状态网络对数据进行异常检测，并在此基础上，采用改进 FUP 算法对所检测到将要发生的安全风险事件与事件数据库中的事件的关联挖掘，以发现潜在攻击信息。接着，将关联结果提交给决策层的策略判决点进行策略触发，管理控制端通过检索相应处理策略完成策略触发，并将触发策略返回给策略判决点。最后策略判决点将安全事件处理策略命令下达给设备管理层中联动控制平台的各个代理，代理根据策略的命令改变各设备的相关配置，完成联动操作。最后，将测试体系结构部署在网络侧集线器和客户机端的交换器，根据相应指标对所设计系统进行测试。由此，依据上述步骤来完成本文所设计系统的测试，以验证其确保网络安全的有效性。

2.2　指标设置

针对上述设置，将阻断响应时间和丢包率作为测试指标，对比分析基于协议特征的网络流量异常行为检测方法、基于深度特征融合网络的网络安全设备联动方法、基于 BP 神经网络的监测系统和基于回声状态网络识别的网络安全设备联动系统的联动效果。其中，阻断响应时间是指网络安全设备在检测到异常流量或威胁后，从触发阻断机制到实际执行阻断操作所需的时间。这个指标是评价网络安全设备联动系统性能的关键参数之一。在网络安全设备联动系统设计中，阻断响应时间的快慢直接影响到系统对威胁的应对能力。较短的阻断响应时间意味着系统能够更快速地隔离和阻断威胁，减少潜在的损失和风险。相反，如果阻断响应时间过长，那么威胁可能会在系统中持续存在并造成更大的损害。

丢包率是指在网络传输过程中，由于各种原因导致数据包丢失的比例。在网络安全设备联动系统测试中，丢包率是一个重要的性能指标，它反映了系统在网络异常检测以及联动方面的稳定性和可靠性。丢包率的高低直接影响到网络数据传输的安全性。较高的丢包率意味着大量数据包在网络传输过程中丢失，使得很多数据未被网络安全设备检测到，那么这些潜在威胁就可能在网络中隐匿并持续传播。这削弱了网络安全设备的防护能力，增加了被攻击的风险。且网络安全设备联动系统依赖于各个设备之间的信息共享和协同工作。如果丢包率过高，那么设备之间的通信可能受到严重影响，导致联动机制无法有效执行。这削弱了整个系统的联动防护效果，使得单一设备难以应对复杂的网络威胁。因此，在网络安全设备联动系统设计中，需要尽可能降低丢包率，以确保数据在网络中的稳定传输，实现有效的网络安全设备联动操作，保障网络安全。

综上所述，阻断响应时间和丢包率是网络安全设备联动系统设计中两个重要的测试指标。因此，通过对这两个指标进行测试，来验证联动系统的性能。

2.3　测试结果与分析

2.3.1　阻断响应时间结果分析

不良信息可能会携带恶意软件，这些软件可能会感染企业的系统，造成数据泄露、系统崩溃等严重后果。为了保护企业的信息安全和维护网络的正常运行，不同方法采取了不同的阻断方式，其中基于协议特征的网络流量异常行为检测方法是通过对比正常流量和异常流量的特征差异进行阻断的；基于深度特征融合网络的网络安全设备联动方法是通过使用深度学习模型对网络流量异常检测而进行阻断的；基于 BP 神经网络的监测系统通过反向传播算法优化参数，最小化预测误差来进行阻断的；基于回声状态网络识别系统通过回声状态网络展开各设备数据异常检测，并采用改进 FUP 算法进行网络安全事件关联挖掘，发现潜在攻击信息，由策略判决点将安全事件处理策略命令下达给 WatchGuard 联动控制平台，进行联动操作完成阻断。

不同方法阻断响应时间对比结果如图 6 所示。

由图 6（a）可知，使用该方法对第 9 行第 1～9 列位置的不良信息进行阻断时，响应时间均为 50 s，共

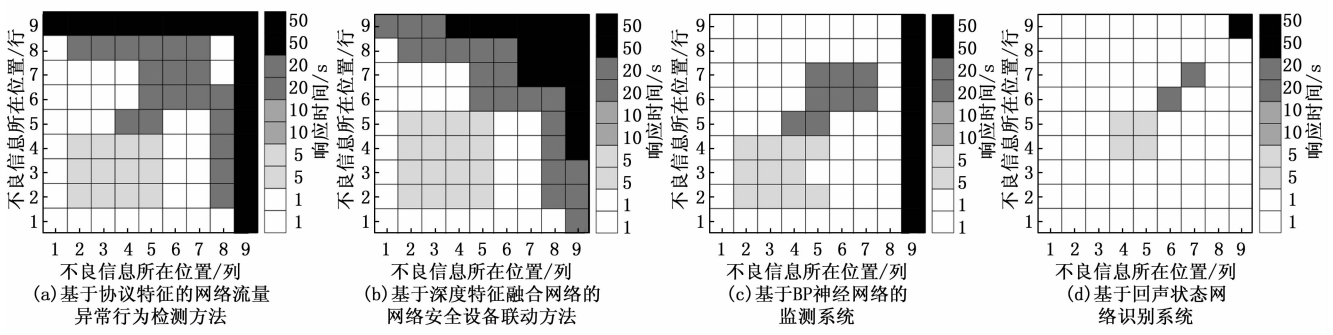

图 6　不同方法阻断响应时间对比结果

850 s。对第 8 行第 2～7 列、第 6、7 行第 5～7 列、第 2～6 行第 8 列、第 5 行第 4～5 列位置的不良信息进行阻断时，响应时间均为 20 s，共 380 s。对第 2～4 行第 2～5 列位置的不良信息进行阻断时，响应时间均为 5 s，共 60 s。其余位置不良信息阻断响应时间均为 1 s，共 32 s。使用该方法的总体阻断响应时间为 1 322 s。

由图 6（b）可知，使用该方法对第 9 行第 4～9 列、第 8 行第 7～9 列、第 7 行第 7～9 列、第 4～6 行第 9 列、位置的不良信息进行阻断时，响应时间均为 50 s，共 750 s。对第 9 行第 1～3 列、第 8 行第 2～6 列、第 7 行第 5～6 列、第 6 行第 5～8 列、第 2～5 行第 8 列、第 1～3 行第 9 列位置的不良信息进行阻断时，响应时间均为 20 s，共 420 s。对第 2～5 行第 2～5 列位置的不良信息进行阻断时，响应时间均为 5 s，共 80 s。其余位置不良信息阻断响应时间均为 1 s，共 29 s。使用该方法的总体阻断响应时间为 1 279 s。

由图 6（c）可知，使用该方法对第 1～9 行第 9 列位置的不良信息进行阻断时，响应时间均为 50 s，共 450 s。对第 6～7 行第 5～7 列、第 5 行第 4～5 列位置的不良信息进行阻断时，响应时间均为 20 s，共 160 s。对第 2～4 行第 2～4 列、第 2、4 行第 5 列位置的不良信息进行阻断时，响应时间均为 5 s，共 40 s。其余位置不良信息阻断响应时间均为 1 s，共 55 s。使用该方法的总体阻断响应时间为 705 s。

由图 6（d）可知，使用该方法对第 9 行第 9 列位置的不良信息进行阻断时，响应时间为 50 s。对第 7 行第 7 列、第 6 行第 6 列位置的不良信息进行阻断时，响应时间均为 20 s，共 40 s。对第 4、5 行第 4～5 列位置的不良信息进行阻断时，响应时间均为 5 s，共 20 s。其余位置不良信息阻断响应时间均为 1 s，共 74 s。使用该方法的总体阻断响应时间为 184 s。

通过上述对比结果可知，使用所设计系统总体阻断响应时间仅为 184 s，具有较快的阻断响应速度。

2.3.2 丢包率结果分析

在网络安全设备联动测试过程中，统计数据丢包率是非常重要的。当网络中出现丢包现象时，通常意味着网络连接不稳定或者网络设备之间存在通信问题，导致设备间联动性较差，影响应对快速变化的网络威胁的效果。

不同方法的丢包率对比结果如图 7 所示。

由图 7 可知，使用基于协议特征的网络流量异常行为检测方法、基于深度特征融合网络的网络安全设备联动方法、基于 BP 神经网络的监测系统均由最高 92%、88%、80%降到 73%、47%、26%；使用基于 HTTP 包识别系统由最高 30%降到 5%。对比上述 4 种方法所得结果，所设计系统丢包率较低。由此可说明，所设计系统具有较好的设备联动性，可有效应对快速变化的网络威胁，对新型威胁具有较好的识别和响应能力，可提供更全面的安全保护。

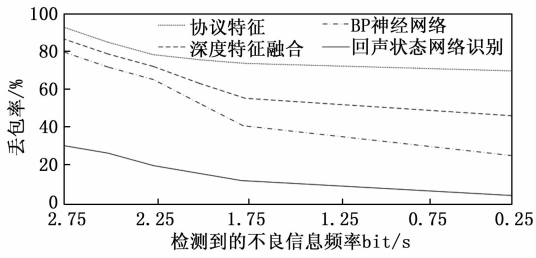

图 7 不同方法丢包率对比结果

3 结束语

传统网络安全方法无法有效应对新型的恶意攻击、无法自适应网络环境的变化，对于未知威胁的检测和防御能力较弱。而设计的基于回声状态网络识别的网络安全设备联动系统，通过引入回声状态网络展开各设备数据异常检测，然后基于检测结果，采用改进 FUP 算法进行网络安全事件关联挖掘，以发现潜在攻击信息，并提交给决策层的策略判决点进行策略触发，最终策略判决点将安全事件处理策略命令下达给 WatchGuard 联动控制平台，进行联动防御操作。相比传统方法，所设计系统当检测到潜在威胁时，可以立即触发相应的安全设备进行防御和响应，能够更准确地识别出恶意攻击和潜在威胁。

总之，基于回声状态网络识别的网络安全设备联动系统提供了一种更智能、更有效的解决方案，解决了传统网络安全方法存在的问题，并提高了网络的整体安全性和防御能力。

参考文献：

[1] 王文博，刘 绚，张 博，等. 基于协议特征的电力工控网络流量异常行为检测方法 [J]. 电力系统自动化，2023，47 (2)：137－145.

[2] 吴荣春，张治兵，蒋 皓，等. 基于行为的电力网络安全事件联动响应及协同处置方法 [J]. 微型电脑应用，2023，39 (1)：53－56.

[3] 周 涛，汪永超，张栩静，等. 基于深度特征融合网络的数模联动随机退化设备剩余寿命预测 [J]. 计算机集成制造系统，2022，28 (12)：3937－3945.

[4] 王志强，彭高辉. 基于 BP 神经网络的矿用设备安全监测系统设计 [J]. 煤炭技术，2022，41 (8)：218－220.

[5] 薛 莹. 基于蜜网技术的网络安全系统设计与实现 [J]. 电子设计工程，2022，30 (13)：142－145.

[6] 翟柱新，严 欣. 电力网络安全多层协同联动控制系统 [J]. 自动化技术与应用，2023，42 (9)：99－102.

（下转第 150 页）