文章编号:1671-4598(2024)05-0017-07 DOI:10.16526/j.cnki.11-4762/tp.2024.05.003 中图分类号:TP393 文献标识码:A

基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统设计

顾正祥
(金肯职业技术学院 人工智能与信息工程学院,南京 211156)

摘要:异构网络具有结构复杂、多重覆盖面积大等特征,使得网络入侵检测较为隐蔽,威胁网络运行的安全性;为此,对基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统进行了研究;通过检测 Agent 和通信 Agent 装设主机 Agent,以 Cisco Stealthwatch 流量传感器作为异构网络传感器检测攻击行为,采用 STM32L151RDT6 64 位微控制器传输批量数据,由 MAX3232 芯片实现系统电平转化,实现硬件系统设计;软件部分设计入侵检测标准,采用传感器设备捕获网络实时数据,通过 Agent 技术解析异构网络协议并提取数据运行特征,综合考虑协议解析结果及与检测标准匹配度,实现异构网络多重覆盖节点入侵检测;经实验测试表明,基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统入侵行为的漏检率和入侵类型误检率的平均值仅为 6%和 5%,能够有效提高检测精度,减小检测误差。

关键词:Agent 人工智能;异构网络;多重覆盖网络;入侵检测系统

Design of Intrusion Detection System for Heterogeneous Networks with Multiple Coverage Nodes Based on Agent Artificial Intelligence

GU Zhengxiang
(School of Artificial Intelligence and Information Engineering, Jinken College of Technology, Nanjing 211156, China)

Abstract: Heterogeneous networks have the characteristics of complex structures and large multiple coverage areas, making network intrusion detection more covert and threatening the security of network operations. To this end, a heterogeneous network multi coverage node intrusion detection system based on the Agent artificial intelligence is studied. The communication agents are installed through detecting and installing the agents, The Cisco Stealthwatch traffic sensors are taken as heterogeneous network sensors to detect attack behavior. The microcontroller of STM32L151RDT6 with 64 bits is used to transmit batch data, and MAX3232 chip is used to achieve the level conversion of the system, achieving the system hardware design. The intrusion detection standards are implemented by the software design, sensor devices are used to capture real-time network data, Agent technology is adopted to analyze heterogeneous network protocols and extract data operation characteristics. The protocol analysis results and detection standard matching degree are integrated to achieve multiple coverage node intrusion detection in heterogeneous networks. Experimental results show that heterogeneous network multi coverage node intrusion detection system based on the Agent artificial intelligence has only 6% of intrusion missed detection rate and 5% of intrusion false detection rate, which can effectively improve detection accuracy and reduce detection errors.

Keywords: agent artificial intelligence; heterogeneous network; multiple overlay network; intrusion detection system

0 引言

异构网络是指两个及更多的无线通信系统使用不同的接入技术,或使用同样的接入技术而隶属于不同的无线通信公司的系统网络。将各种无线通信系统充分利用,采用系统间融合的方法,让多个系统相互取长补短,全面发挥它们各自的优势。为实现网络的广泛应用,并保证不同网络之间的独立性,许多异构网络均存在重叠覆盖的情况。通过多模终端的智能化接入手段,使得多种不同类型的网络共同为用户提供随时随地的无线接入,大部分情况下运行在不同的协议上支持不同的功能或应用。由于异构网络的覆盖形式,导致该网络存在多重覆盖的情况,给异构网络的安全运行带来较大隐患。多重覆盖的异构网络给非法用户提供了更为隐蔽的环境,也为非法用户的入侵行为提供了充足条件。为了提高异构网络多重覆盖环境的安全性,设计入侵检测系统。

目前入侵检测系统的研究领域存在较多的研究成果。其中文献[1]根据“一对多”的思想,将多类检测问题分解为若干个二类问题,针对每一个二类问题,基于 AUC 值选取最佳的二类融合算法,解决数据不均衡性问题,并通

收稿日期:2023-09-27; **修回日期**:2023-11-14。
基金项目:高校哲社项目(2023SJYBO860);江苏省高职院校教师专业带头人高端研修项目。
作者简介:顾正祥(1979-),男,高级实验师,硕士。
引用格式:顾正祥.基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统设计[J].计算机测量与控制,2024,32(5):17-23,30.

过类目判定模块，对被测样本的特定类别进行判定，最终实现对网络的入侵检测。该系统中使用 AUC 值虽然可以提高单个二分类器的性能，但是多个二分类器之间的关联性以及它们在综合过程中的权重如何确定都会影响到整体模型的性能表现，不能保证整体模型的泛化性能，检测结果容易存在误差。文献［2］系统采用 SMOTE 与随机抽样相结合的方式，实现对数据的均衡归约，以解决数据失衡的问题。通过综合的方式，从数据中抽取出有意义的特征，以减少处理的维数。使用 BP 神经网络算法，完成数据判别，实现对网络入侵类型的分类与检测。但 BP 神经网络在训练过程中容易陷入局部最优，且对超参数敏感，在分类过程中容易受到限制，导致检测效果不佳。文献［3］系统利用深度卷积产生式对抗网络，从已有的入侵攻击样本中提取内在特征，构造出新的攻击样本，并对其使用的线性整流活化函数进行改进。但通过深度卷积生成对抗网络生成的新攻击样本与现实中的入侵样本存在一定的区别，缺乏真实数据的多样性和复杂性，从而影响系统的真实入侵的检测能力。

为了解决上述方法中存在的问题，设计基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统。通过主机 Agent、异构网络传感器、微控制器和系统电路搭建硬件系统，为了提高系统的整体控制能力，设计入侵检测标准，通过传感器设备捕获网络实时数据，提高系统的检测精度，为了进一步降低检测误差，通过 Agent 技术解析异构网络协议并提取数据运行特征，基于检测标准匹配度完成多重覆盖节点入侵检测。

1 总体框架设计

在异构网络多重覆盖节点入侵检测系统总体框架设计中，主要由主机 Agent、异构网络传感器、微控制器和系统电路构成。具体如图 1 所示。

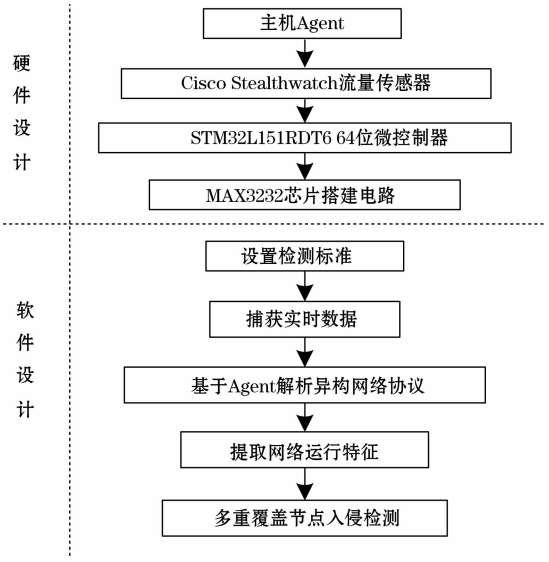

图 1 总体框架设计图

图 1 中，主机 Agent 通过控制管制原则获取主机数据，由异构网络传感器检测网络的入侵行为，经过微控制器进行数据传输，通过 MAX3232 芯片实现系统电平转换。其中，主机 Agent 和 Cisco Stealthwatch 流量传感器通过通信链路进行连接，将采集到的数据发送给微控制器进行处理，利用 MAX3232 芯片将不同硬件设备之间的信号电平进行转换，共同完成硬件系统的设计。

2 异构网络多重覆盖入侵检测硬件系统设计

设计的异构网络多重覆盖入侵检测系统以 Agent 人工智能技术作为支持，因此需要安装相关的硬件设备，为该系统提供硬件支持[4]。在异构网络中装设主机 Agent，根据主机 Agent 的运行要求和系统要求，设计硬件系统中的其他硬件设备。

2.1 主机 Agent

异构网络多重覆盖入侵检测系统中装设的主机 Agent 包括检测 Agent 和通信 Agent 两部分，主机 Agent 结构如图 2 所示。

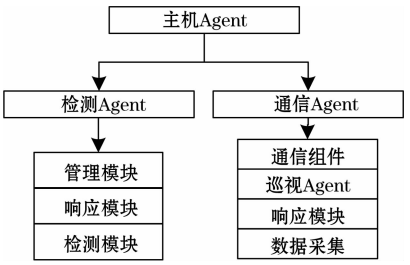

图 2 主机 Agent 结构图

根据图 2 所示，多重覆盖异构网络中每层之间的 Agent 互相通信，不同层次结构的 Agent 之间通过通信 Agent 通信。每一个 Agent 都是一个独立的检测单元，各 Agent 互相协作，共同检测系统和网络的异常或者可疑行为。通信组件分为接收和发送两部分。检测 Agent 拥有系统特权，一旦被突破，会造成较为严重的后果。为了确保 Agent 自身的安全，在通信 Agent 中添加了下属层级巡视 Agent，对其进行定时巡视，或者当 Agent 需要其他层级 Agent 的活动状态时，为其发出请求，由其他层次的通信 Agent 查询后返回结果[5-6]。通信部分以后台服务器模式操作，使用与目录服务相似的机制实现同一层代理通信。在实际操作中，主机 Agent 经由检测器进行数据采集时，采用控制管制的原则，以取得主机数据。

2.2 异构网络传感器

选择 Cisco Stealthwatch 流量传感器作为异构网络传感器。按照用户所选择的或者自定义的规则，对网络中的攻击行为进行检测，从而判断是否存在攻击行为。在异构网络传感器中，为了能够捕获经过网络的所有流量数据，将网卡设置为混杂模式，网卡型号为 Intel Ethernet Server Adapter X520-DA2，在每个网段上均能侦听到报文，并将报文发送给数据分析与预处理模块[7]。当检测到攻击征兆时，立即通知对应的 Agent，再由 Agent 上传给系统终端。同时，通过 Agent 控制并管理网络传感器的工作状态。流量

传感器内部结构及与主机 Agent 的连接如图 3 所示。

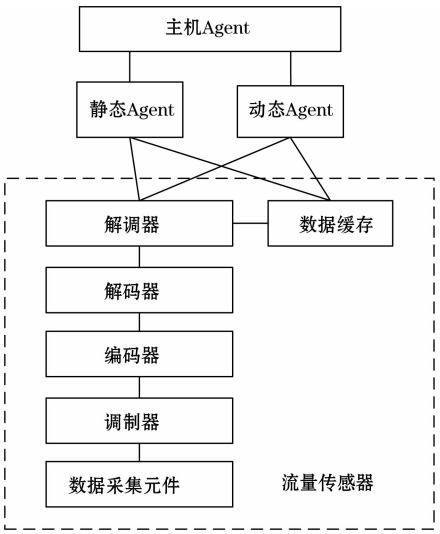

图 3　流量传感器内部结构及与主机 Agent 的连接

装设的 Cisco Stealthwatch 流量传感器能够实现对多重覆盖异构网络节点、网络链路的实时运行数据以及网络流量数据的采集，为异构网络多重覆盖入侵检测系统软件功能的运行提供初始数据支持。

2.3　微控制器

异构网络多重覆盖入侵检测系统中微控制器选择 STM32L151RDT6 64 位微控制器。其作用是在大容量存储设备和异构网络传感器之间传输批量数据，同时控制系统入侵检测程序的执行状态[8]。微控制器的工作原理如图 4 所示。

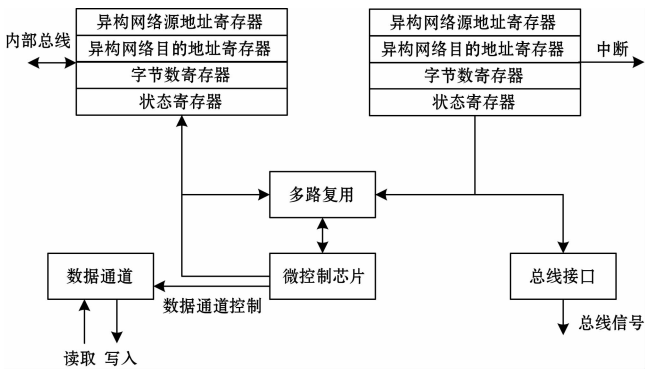

图 4　微控制器工作原理

异构网络传感数据的传输是由微控制器完成的，能够增加系统 CPU 的带宽，使 CPU 在有限时间内执行更多更复杂的算法和任务。微控制器采用双地址传输控制方式，即每次数据传输包括两个步骤，先从源地址读取数据，然后向目的地址写数据[9]。另外，在系统入侵检测程序控制过程中，根据异构网络传感器实时数据的采集情况，判断是否需要执行入侵检测程序。

2.4　系统电路设计

在异构网络多重覆盖入侵检测系统中使用 MAX3232 芯片及其电路进行电平转化，系统电平转化电路如图 5 所示。

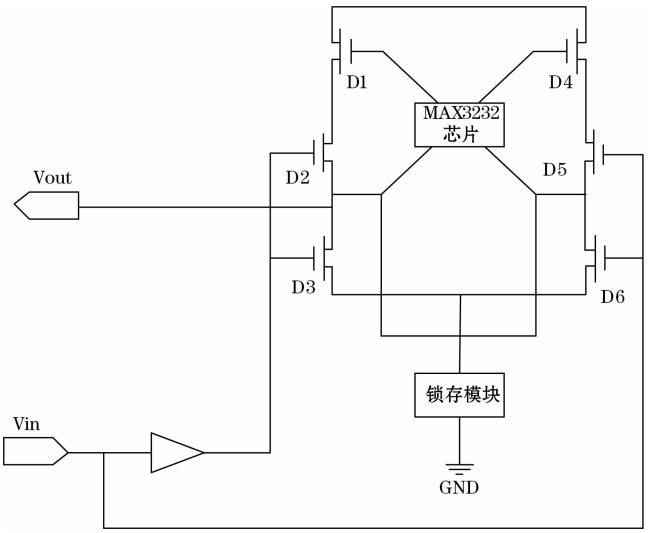

图 5　系统电平转换电路

从图 5 中可以看出，MAX3232 芯片为系统电平转换电路的核心部件，在电平转换电路中添加一个 ESD 元件，为系统中所有硬件设备的输入和输出提供保护，该元件可承受气隙放电、接触放电模式，最大程度地保证系统运行的安全性。

3　异构网络多重覆盖入侵检测系统软件功能设计

在硬件系统的支持下，以异构网络多重覆盖环境为研究对象，对异构网络的入侵情况进行多重覆盖入侵检测，系统软件功能的基本运行原理为：根据不同入侵行为的作用原理与特征，设置异构网络多重覆盖入侵的检测标准，通过当前网络运行特征与入侵检测标准的比对，判断当前异构网络是否存在入侵现象，并针对存在入侵行为的网络，对其入侵强度、入侵位置等内容进行具体检测[10]。为保证系统输出入侵检测结果的精度，利用 Agent 人工智能技术对异构网络的运行协议进行分析验证，判断网络协议运行异常情况，综合网络协议和网络运行特征两个方面，得出异构网络多重覆盖入侵检测结果。

3.1　入侵检测标准设置及数据捕获

多重覆盖异构网络的入侵类型包括：木马病毒入侵、缓冲区溢出入侵、端口扫描入侵等，其中木马病毒入侵是将程序的服务器端植入到目标主机中，通过自己主机上的客户机，实现目标主机完全控制。异构网络多重覆盖木马入侵结构如图 6 所示。

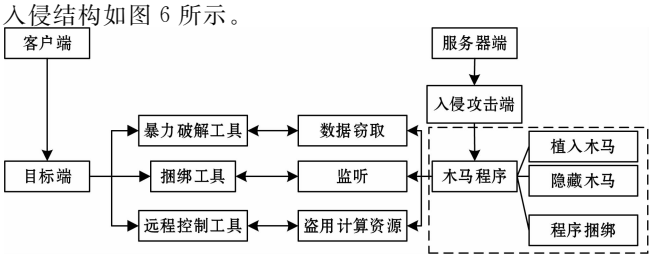

图 6　异构网络多重覆盖木马入侵结构图

异构网络多重覆盖环境中使用的木马病毒大多为特洛伊木马，它在目标计算机中与计算机同步启动，并在某个接口上监听，在辨识收到的数据后，针对目标计算机进行特殊的处理。特洛伊木马本质是一种以端口为通信介质的网络用户服务程序[11]。在木马入侵状态下，多重覆盖异构网络的运行特征可以量化表示为：

$$\tau_T = \kappa_{\text{Trojan horse}} \cdot x \tag{1}$$

式中，$\kappa_{\text{Trojan horse}}$和 x 分别表示异构网络木马入侵攻击强度系数和正常状态下网络的传输数据。另外，缓存溢位攻击是指破坏具有一定权限的程序，从而使攻击者能够对程序进行控制。端口扫描是指对目标系统进行网络扫描，通过主机端口检测，判断目标操作系统的种类和版本[12]，其主要思想是将各种不寻常的数据包传输到目标系统的各个端口，观察系统的响应情况，从而判断远程操作系统的种类。根据缓冲区溢出入侵、端口扫描入侵的作用原理，得出上述两种入侵场景下异构网络数据特征为：

$$\begin{cases} \tau_O = W_{\text{overflow}}(C - W_{\text{overflow}})x \\ \tau_P = \kappa_{\text{scan}}(x - x_{\text{scan}}) \end{cases} \tag{2}$$

式中，W_{overflow}为缓冲区的数据溢出量，C 为缓冲区容量，κ_{scan}和 x_{scan}分别是端口扫描系数和端口数据扫描数量[13]。同理得出其他的入侵方式下异构网络的运行标准特征，以此作为异构网络多重覆盖入侵的检测标准。

在求取异构网络多重覆盖入侵的检测标准后，需要进行多重覆盖异构网络实时数据捕获。上述异构网络多重覆盖入侵检测标准设置中提到了不同入侵类型（如木马病毒入侵、缓冲区溢出入侵、端口扫描入侵等），而多重覆盖异构网络实时数据捕获正是为了捕获这些不同类型入侵行为所产生的网络数据包，实时数据捕获过程可以获取到实际运行中的网络数据，包括上述所提到的不同类型入侵行为所涉及的数据，设置异构网络多重覆盖入侵检测标准可以为异构网络多重覆盖入侵的检测提供数据基础。通过实时捕获的数据，深入分析、提取特征，并应用于入侵检测中。多重覆盖异构网络实时数据捕获主要是对网络数据包进行捕获和监听，同时，通过对采集到的数据进行简单的归类与处理，剔除初始捕获数据中的无效数据包。将数据捕获设备的工作模式调整至混杂模式，保证异构网络数据包捕获的完整性[14]。捕获数据包的流程分为 5 个步骤，即获取指定的侦听网络节点、建立侦听会话、编译过滤规则、设定过滤器、获得数据包和关闭侦听会话，经过上述步骤得出异构网络数据的实时捕获结果为：

$$x_{\text{capture}}(t) = \kappa_{\text{transmission}} x_{\text{network}}(t) f_{\text{capture}} \tag{3}$$

其中：$\kappa_{\text{transmission}}$为数据的传输系数，$f_{\text{capture}}$为网络数据捕获频率，$x_{\text{network}}(t)$ 表示 t 时刻异构网络多重覆盖实际运行数据。按照上述方式得出任意时刻异构网络的数据捕获结果，为保证系统输出的入侵检测质量，需要对初始采集数据进行预处理，从而提高初始采集数据的质量。需要剔除的网络数据包主要为冗余数据包，冗余数据包的识别过程可以表示为：

$$\mu = \sqrt{(x_{\text{capture}}(t) - x_{\text{capture}}(t_j))^2} \tag{4}$$

式中，$x_{\text{capture}}(t_j)$ 表示 t_j 时刻捕获的网络数据。若公式（4）的冗余度 μ 识别结果高于阈值 μ_0，说明对应数据互为冗余数据，需要对其中任意一个数据包进行剔除处理，否则无须执行剔除操作[15]。另外，为降低异构网络中多重覆盖因素对数据包捕获结果的影响，需对初始采集数据进行滤波处理，处理结果为：

$$x_{\text{filtering}} = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x_{\text{capture}}-\mu)^2/2\sigma^2} \tag{5}$$

式中，σ 和 δ 分别表示网络数据的标准差和均值。将公式（3）的输出结果以及公式（4）的冗余度代入公式（5）中，即可得出网络数据的滤波处理结果。重复上述操作，对实时捕获的多重覆盖异构网络数据包进行预处理，得出满足质量要求的数据包捕获结果。

3.2 解析异构网络协议并提取数据特征

Agent 是一种在异构网络中自主地从一台主机迁移到另一台主机，并且能与其他 Agent 或资源进行交互的计算机系统。它是一门源于人工智能的新兴学科，是分布式人工智能与网络技术相结合的产物。Agent 能够解释为来自环境并反映环境中发生的事件的数据，同时通过一定的行为来影响环境。Agent 技术具有自主性、自发行为、反应性和社会性等特点。3.1 小节中得到的数据包捕获结果提供了 Agent 人工智能技术解析异构网络协议所需的原始数据。在数据包捕获结果中，可以获取到异构网络的传输数据包，这些数据包反映了网络中的各种协议结构和通信行为，通过对这些数据包进行解析和处理，可以提取出异构网络协议的特征信息，高质量的数据包捕获结果可以提供准确的网络协议，为 Agent 人工智能提供充足的数据样本。为此，利用主机 Agent，在 Agent 人工智能技术的支持下进行 Agent 的移动与交互，从而判断任意两个异构网络主机 Agent 节点之间的协议状态。Agent 人工智能技术原理如图 7 所示。

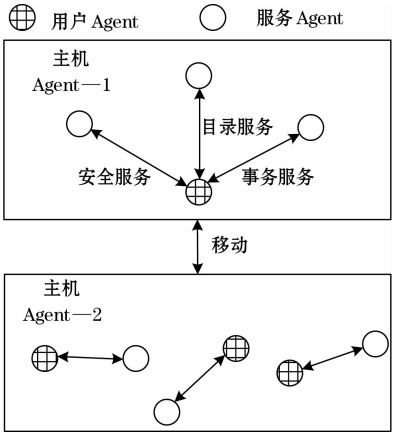

图 7 Agent 人工智能技术原理

Agent 可分为数据状态、执行状态和代码状态，如果一个移动代理包含多个线程，则要求每一个线程从一个端点启动。一般来说，智能体的运行状态较为活跃，尤其是多

线程 Agent，导致产生了强大的移动代价。Agent 在进行弱移动时，在目的地执行主线程的某一入口函数，不需要从断点开始执行，只需要按照实际需求，将部分的执行状态保存到数据状态中，并随着 Agent 一起移动。为此，进行传输的数据量较小，开销较小，执行效率较高[16]。Agent 要实现某个任务，必须在多台主机间来回穿梭，并与这些主机进行互动，充分利用这些主机提供的资源和服务，实现该任务目标。为 Agent 规划最优的移动路径，进而提升系统的工作效率。在异构网络中，移动策略效果直接反映了异构网络传输协议的运行情况。异构网络协议主要是利用 Agent 人工智能技术对捕获数据包结构进行解析[17]，根据数据包结构的解析结果，得出当前异构网络协议运行状态的识别结果。异构网络协议的解析结果可以量化表示为：

$$\gamma_{\text{agreement}} = \left(\sum_{i=1}^{n_{\text{data packet}}} \varphi_i x_{\text{filtering}} \mid J_{\text{capture}} - J_{\text{agreement}} \mid \right)^{1/\varphi_{\text{Agent}}} \tag{6}$$

其中：$n_{\text{data packet}}$为异构网络中第 i 条信道的数据包的捕获量，φ_i 为主机 Agent 的移动效率，J_{capture}和 $J_{\text{agreement}}$分别为捕获异构网络数据结构和网络协议正常运行状态下运行数据的结构系数[18]。按照上述方式完成异构网络协议的解析工作。

Agent 人工智能技术通过分析异构网络中的捕获数据包结构，得到数据包结构的解析结果，而数据包结构中存在多重覆盖异构网络的运行特征信息，通过获得协议的具体细节，从而提取出多重覆盖异构网络的运行特征，有助于更好地理解和分析异构网络的协议运行状态。提取的多重覆盖异构网络运行特征具体包括：网络流量峰值、不同网络信道流量偏差、网络流量溢出量、网络流量均值等，其中网络流量峰值的提取结果为：

$$\tau_{\text{peak value}} = \gamma_{\text{agreement}} y_{\max} \tag{7}$$

其中：$y_{\max}$ 为最大值求解函数。同理多重覆盖异构网络中的信道流量偏差、网络流量溢出量、网络流量均值的提取结果分别为：

$$\begin{cases} \tau_{\text{deviation}} = \sum_{i=1}^{n_{\text{channel}}} \mid n_i - \bar{n}_i \mid \\ \tau_{\text{overflow}} = n_i - C_{\text{channel}} \\ \tau_{\text{mean value}} = \dfrac{n_i}{\Delta t} \end{cases} \tag{8}$$

式中，n_{channel}、n_i 和 $\bar{n}_i$ 分别为异构网络中第 i 条信道的数据捕获量、网络总捕获量和捕获数据的平均值，C_{channel}为异构网络信道容量，Δt 表示异构网络的运行时长[19]。最终对提取的网络特征分量进行融合处理，得到综合网络特征为：

$$\tau_{net} = \frac{\kappa_{\text{screen}} (\tau_{\text{peak value}} \tau_{\text{deviation}} - \tau_{\text{overflow}} \tau_{\text{mean value}})^2}{(\tau_{\text{peak value}} + \tau_{\text{mean value}})(\tau_{\text{overflow}} + \tau_{\text{deviation}})(\tau_{\text{peak value}} + \tau_{\text{overflow}})} \tag{9}$$

其中：κ_{screen}为特征筛选系数，由此得出多重覆盖异构网络的综合特征提取结果。

3.3　实现异构网络多重覆盖节点入侵检测

在实现异构网络多重覆盖节点入侵检测的过程中，可以将综合网络特征作为输入，利用多重覆盖异构网络的综合特征提取结果获取异构网络多重覆盖环境特征与入侵标准特征之间的匹配度，通过综合网络协议和特征匹配度两个方面判断当前异构网络多重覆盖环境是否存在入侵行为，入侵行为判定条件为：

$$\begin{cases} \gamma_{\text{agreement}} \leqslant \gamma_0 \\ s_\tau \geqslant s_0 \end{cases} \tag{10}$$

式中，s_τ 表示异构网络多重覆盖环境特征与入侵标准特征之间的匹配度，γ_0 和 s_0 分别为网络协议解析与特征匹配度阈值[20]。其中变量 s_τ 的计算公式为：

$$s_\tau = \frac{\tau_{sd} \cdot \tau_{\text{net}}}{(\tau_{sd} + \tau_{\text{net}})} \tag{11}$$

其中：τ_{sd} 表示网络入侵的标准特征，将相关参数代入到公式（11）中，得出特征匹配度的计算结果，将公式（10）和公式（11）进行联立，即可得出当前多重覆盖异构网络入侵状态的检测结果。通过公式（10）的计算结果判定当前异构网络存在入侵异常，则网络入侵类型与 τ_{sd} 一致。在此基础上，对存在入侵行为的异构网络进行入侵强度检测与入侵位置检测，并将检测参数以可视化的形式输出，实现异构网络多重覆盖入侵检测功能。

4　系统测试

以测试设计的基于 Agent 人工智能的异构网络多重覆盖节点入侵检测系统的入侵检测性能为目的，采用白盒测试的方式进行系统测试。白盒测试的基本原理是在已知运行结果的情况下，对比测试目标的输出结果与已知结果之间的差距。此次系统测试的基本思路为：通过设置异构网络多重覆盖环境及其入侵方式，确定异构网络的入侵状态、入侵类型以及入侵强度，在此基础上，利用设计的入侵检测系统输出相应的入侵检测结果，并与设置的入侵参数进行对比，得出反映优化设计系统入侵检测性能的测试结果，并验证系统运行功能是否满足预期效果。

4.1　布设系统测试环境

根据基于 Agent 人工智能的异构网络多重覆盖节点入侵检测硬件系统的设计结果，安装相关的硬件设备，并配置两台型号相同的计算机，其型号为 Dell XPS 17，处理器为 Intel Core i9 11th generation，内存为 32 GB RAM。其中一台计算机作为主测计算机，主要用来运行异构网络多重覆盖入侵检测软件 Suricata，另一台计算机用来模拟攻击设备。由于设计的入侵检测系统以 Agent 人工智能作为技术支持，为保证该技术能够在实验环境中正常运行，需要对系统运行环境进行相应配置。系统以 IBMAglet 为智能体的工作环境，并以此为基础，将其设置在各节点主机上，为 Agent 的工作提供了必要条件。同时，还为移动代理系统的开发提供更多的类库和界面。Aglet 具有跨平台的特性，使得 Agent 可以在不同的环境下工作。选择 ASDK 作为开发工具，创建、管理并发送移动代理到远程计算机去执行。Agent 的开发语言使用的是 Java，以完成跨平台的连接，将对象序列化的功能和 RMI 接口直接集成在一起，为移动 Agent 提供了强大的支持。在系统开始工作之前，需要在每一

个操作系统平台上运行 Aglets 虚拟机。在运行过程中，在虚拟机端口上实现彼此之间的通信。通过这种方式，每个 Aglets 都能在虚拟机中跨越不同的平台。与此同时，Aglets 之间还可以利用这个环境中所提供的功能互相传递消息。

4.2 配置异构网络多重覆盖入侵检测对象

通过多个网关、路由器、交换机以及计算机的组合，构建多重覆盖的异构网络，以此作为系统的入侵检测对象。图 8 表示的是构建异构网络的基本拓扑结构。

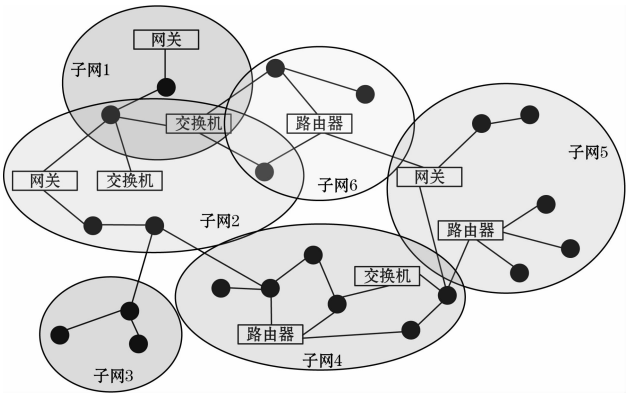

图 8 异构网络拓扑结构图

从图 8 中可以看出，异构网络由 21 个节点组成，共生成了 6 个不同结构的子网，各子网之间存在多重覆盖的情况，导致网络节点同时出现在不同的子网环境中。异构网络中子网 1、子网 3 和子网 5 中设置的网络传输协议为 TCP-IP 协议，其他子网设置的是 IPX/SPX 协议。

4.3 编写异构网络入侵攻击程序

为实现对异构网络入侵场景的模拟，在系统测试环境的模拟攻击设备设备中导入入侵攻击程序。编写的入侵攻击程序类型包括木马病毒入侵、缓冲区溢出入侵、端口扫描入侵、DOS、DDoS 等，其中木马病毒入侵攻击程序的运行界面如图 9 所示。

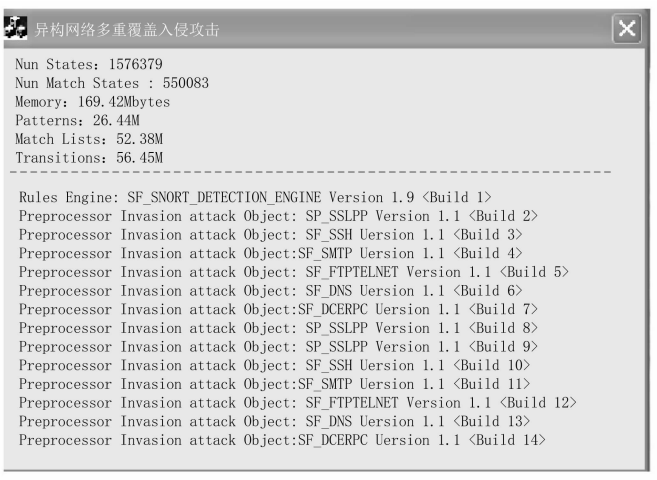

图 9 异构网络多重覆盖入侵攻击程序运行界面

同理得出其他入侵攻击程序的编写结果，在攻击程序编写与运行过程中，需要保证入侵攻击程序相对独立，不会出现异构网络同时被两种入侵方式攻击的情况。另外，由于木马入侵攻击、DOS、DDoS 等入侵攻击方式的可控性较低，为降低入侵攻击程序对多重覆盖异构网络中信息产生的实质影响，在攻击程序编写过程中增加一个强制终止条件，当异构网络或入侵攻击程序运行满足强制终止条件时，入侵攻击程序自动停止运行。

4.4 系统测试过程

在配置完成的系统测试环境下，利用编程工具将设计基于 Agent 人工智能的异构网络多重覆盖入侵检测系统的软件部分转换成程序代码，将其导入到主测计算机中。准备多重覆盖异构网络的通信任务，将网络调整至运行状态，并生成相应的网络运行数据。将布设的异构网络接入到系统软件运行程序中，通过实时数据采集、协议分析、特征提取与匹配等步骤，输出异构网络多重覆盖的入侵检测系统输出结果，如图 10 所示。

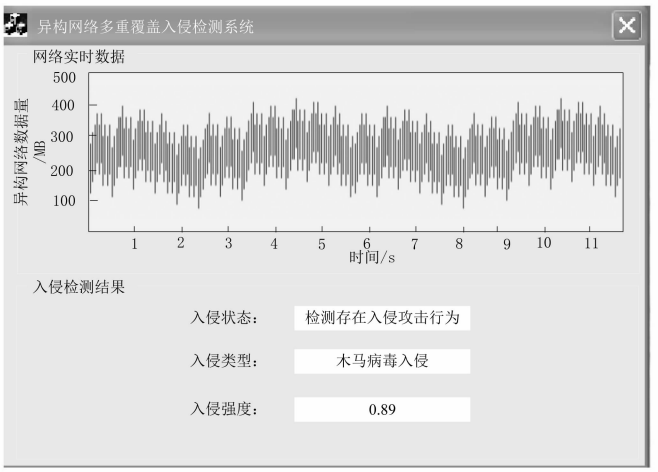

图 10 异构网络多重覆盖入侵检测系统输出结果

图 10 表示的是木马入侵攻击程序运行状态下的入侵检测结果，同理得出其他入侵攻击状态下的入侵检测结果。系统测试设置基于采样集成算法的入侵检测系统（文献［1］系统）、基于特征优化和 BP 神经网络的入侵检测系统（文献［2］系统）以及基于改进深度卷积生成对抗网络的入侵检测系统（文献［3］系统）作为对比系统，对比系统的主要实验环境及参数设置如下。

文献［1］系统算法设计一种 OSECGIDS 工作流程图，以 NSL-KDD 为测试数据集，该数据集中 Probe、R2L 和 U2R 的样本分别占总数的约 9.2%、0.7%和 0.04，并将多分类问题转换为二分类问题；文献［2］系统同样以 NSL-KDD 为测试数据集，利用 SMOTE 技术采集 16 055 条实验数据，随机抽取 Normal 10%、DoS 13%、Probe50%，并将 R2L 和 U2R 分别扩大 50 倍和 100 倍；文献［3］系统以 CIC-IDS-2017 为测试数据集，该数据集中包含 83 个特征和 3 119 345 个实例，设置 Adam 学习率为 0.000 2，循环数为 60 000，批处理为 128。

基于上述研究环境和研究参数设置，重复上述操作完

成系统开发，得出系统入侵检测结果，并与设计的基于 Agent 人工智能的异构网络多重覆盖入侵检测系统进行对比。

4.5　设置系统测试指标

设置入侵行为漏检率、入侵类型误检率和入侵强度检测误差 3 个指标反映系统的入侵检测功能，其中入侵行为漏检率是异构网络存在入侵行为但未被检测出的概率，入侵类型误检率是异构网络入侵类型检测错误次数的占比，上述两个指标的数值结果为：

$$\begin{cases}\eta_{\text{leak}}=\dfrac{Num_i-Num_d}{Num_i}\times 100\%\\ \eta_{\text{mistake}}=\dfrac{Num_{\text{correct}}}{Num_i}\times 100\%\end{cases}\tag{12}$$

式中，Num_d、Num_{correct}和 Num_i 分别表示成功检测出的存在入侵行为实验次数、实验设置的入侵行为总次数以及入侵类型检测正确的次数。入侵强度测试误差指标的测试结果如下：

$$\varepsilon_{\text{strength}}=|Q-Q_{\text{set}}|\tag{13}$$

其中：Q 和 Q_{set}分别为入侵攻击强度的检测值和设定值，由此得出漏检率和误检率越低、入侵强度检测误差越小，对应系统的检测功能越优。

4.6　系统测试实验结果与分析

统计不同异构网络多重覆盖入侵检测系统的输出结果数据，通过公式（12）计算得出入侵行为漏检率、入侵类型误检率指标的测试结果。系统入侵行为漏检率、入侵类型误检率测试结果如图 11 所示。

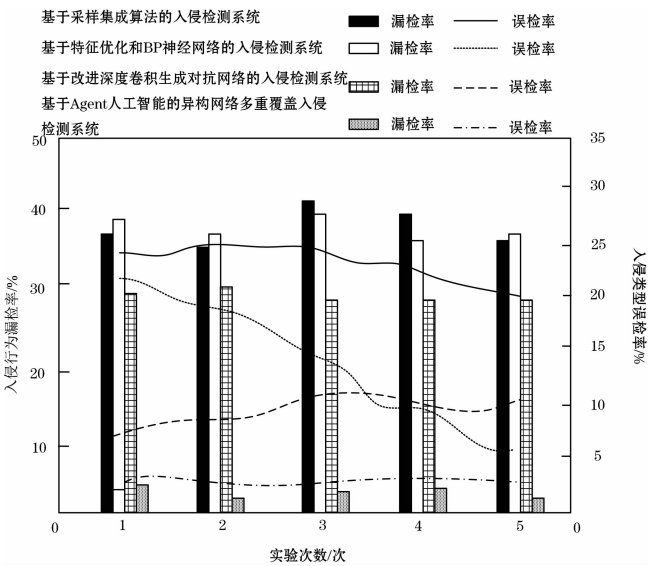

图 11　系统入侵行为漏检率、入侵类型误检率测试结果

从图 11 中可以看出，3 种对比系统的平均入侵行为漏检率分别为 38%、38%和 30%，平均入侵类型误检率分别为 29%、20%和 15%，设计系统入侵行为漏检率和入侵类型误检率的平均值分别为 6%和 5%，设计基于 Agent 人工智能的异构网络多重覆盖入侵检测系统的漏检率和误检率始终低于对比系统，能够提高检测精度。这是因为设计系统使用 Agent 人工智能技术对捕获的数据包进行解析，分析数据包的结构和内容，提取数据特征，这些特征可以用于评估和监测网络的运行状态、优化网络性能、识别异常行为，有效提高入侵检测精度。

异构网络多重覆盖入侵强度检测误差指标测试结果，如表 1 所示。

表 1　异构网络多重覆盖入侵强度检测误差测试结果

实验编号	入侵攻击类型	入侵强度	采样集成检测系统	特征优化的检测系统	生成对抗网络的检测系统	设计系统
1	木马病毒入侵	0.89	0.81	0.83	0.86	0.89
2	木马病毒入侵	0.67	0.75	0.72	0.70	0.68
3	缓冲区溢出入侵	0.74	0.62	0.67	0.71	0.73
4	缓冲区溢出入侵	0.82	0.74	0.78	0.80	0.82
5	端口扫描入侵	0.79	0.89	0.85	0.83	0.80
6	端口扫描入侵	0.68	0.62	0.64	0.65	0.67
7	DOS	0.47	0.41	0.44	0.45	0.47
8	DDoS	0.56	0.50	0.51	0.53	0.55

将表 1 中的数据代入到公式（13）中，计算得出 3 种对比方法入侵强度检测误差的平均值分别为 0.08、0.05 和 0.03，而设计基于 Agent 人工智能的异构网络多重覆盖入侵检测系统输出的平均入侵强度检测误差为 0.01，说明设计系统的入侵检测性能更优。为了进一步测试设计系统的优越性，采用同一攻击方法测试不同攻击强度下，4 种系统的检测能力，测试结果如表 2 所示。

表 2　同一攻击方法下不同入侵强度检测误差测试结果

实验编号	木马病毒入侵强度	采样集成检测系统	特征优化的检测系统	生成对抗网络的检测系统	设计系统
1	0.2	0.11	0.23	0.26	0.2
2	0.3	0.35	0.32	0.33	0.3
3	0.4	0.42	0.47	0.41	0.41
4	0.5	0.54	0.58	0.56	0.49
5	0.6	0.69	0.65	0.53	0.5
6	0.7	0.72	0.74	0.65	0.6
7	0.8	0.81	0.84	0.75	0.79
8	0.9	0.95	0.91	0.83	0.9

由表 2 可以看出，设计系统的检测结果与实际攻击强度基本一致，验证了设计系统的检测性能。这是因为设计系统通过获取的多重覆盖异构网络的综合特征，设定描述入侵行为的标准特征，计算了网络综合特征与入侵标准特征之间的匹配度，通过分析入侵行为的特征、异常流量来源，计算入侵的强度，降低了检测误差。

5　结束语

异构网络多重覆盖是通信网络的必然发展趋势，在工作与生活场景中得到广泛应用，入侵检测系统作为一种积极主动的网络安全防护手段，对异构网络多重覆盖环境中的内部攻击、外部攻击、错误操作等问题进行实时防护，对

（下转第 30 页）