文章编号:1671-4598(2025)03-0167-09 DOI:10.16526/j.cnki.11-4762/tp.2025.03.021 中图分类号:TP309 文献标识码:A

基于访问策略控制的主动式网络信息安全应急联动模型

张 宇[1],万 军[1],陈承斌[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.广东轻工职业技术学院,广州 510300)

摘要:为了应对网络信息安全事件,最大程度的降低入侵攻击对网络信息产生的负面影响,降低网络信息丢包率和错误率,提出基于访问策略控制的主动式网络信息安全应急联动模型。捕获主动式网络数据包,以此作为模型的输入项;采用特征提取与匹配的方式,检测网络信息的安全状态,根据状态检测结果判断模型程序是否启动;根据网络攻击信号的强度特征,追踪主动式网络信息攻击源与路径,从网络节点功率、节点容量、资源可用性等方面设置模型约束条件,通过访问策略控制、信息攻击防御、信息恢复3个步骤,实现模型主动式网络信息安全应急联动功能;通过模型验证实验得出结论:与传统应急联动模型相比,在优化设计模型作用下,主动式静态网络和动态网络的丢包率分别降低3.04%和3.53%,网络信息错误率分别减小5.445%和6.07%,由此证明优化设计的安全应急联动模型具有更高的应用价值。

关键词:访问策略控制;主动式网络;信息安全;应急联动模型

Active Network Information Security Emergency Linkage Model Based on Access Policy Control

ZHANG Yu[1], WAN Jun[1], CHEN Chengbin[2]
(1. Information Center of Guoneng Shuohuang Railway Development Co., Ltd, Cangzhou 062350, China;
2. Guangdong Industry Technical College, Guangzhou 510300, China)

Abstract: In order to respond to network information security incidents, minimize the negative impact of intrusion attacks on network information, and reduce the packet loss and error rates of network information, an active network information security emergency linkage model based on access policy control is proposed. Capture active network packets as inputs to the model. By using feature extraction and matching, the security status of network information is detected, and the model program is determined whether to start based on the state detection results. Based on the strength characteristics of network attack signals, track the source and path of active network information attacks, set model constraints from the aspects of network node power, node capacity, and resource availability. The model's active network information security emergency linkage function is achieved through three steps: access policy control, information attack defense, and information recovery. Through model validation experiments, it is concluded that compared with traditional emergency linkage models, under the optimized design model, the packet loss rates of active static networks and dynamic networks are reduced by 3.04% and 3.53%, respectively, and the network information error rates are reduced by 5.445% and 6.07%, respectively. This proves that the security emergency linkage model of the optimized design has higher application value.

Keywords: access policy control; active network; information security; emergency linkage model

0 引言

主动式网络强调网络中的节点能够主动地参与到网络行为的管理和优化中,不仅具备存储转发等网络功能,同时能够对包含数据和代码的主动包和普通包进行

收稿日期:2024-01-12; **修回日期**:2024-02-27。

作者简介:张 宇(1988-),男,大学本科,工程师。

引用格式:张 宇,万 军,陈承斌.基于访问策略控制的主动式网络信息安全应急联动模型[J].计算机测量与控制,2025,33(3):167-175.

计算处理。在主动式网络中，节点具有智能性，能够自主地执行任务，而不仅仅是被动地接收和转发数据。节点可以主动地与其他节点进行通信，共享信息，并协作完成特定的任务。主动式网络信息安全是网络的重要属性之一，网络信息安全指的是恶意的情况下，不会被破坏、改变、泄漏，系统能够持续、稳定地工作，而不会被打断。受到黑客攻击、病毒软件、内部威胁等因素的影响，导致主动式网络存在严重的信息安全问题，从而使网络信息出现篡改、丢失等现象。由于当前网络空间中威胁与攻击不断增加，对信息系统和网络安全的保护形势变得异常严峻。因此，需要采取一系列措施来加强网络安全保护，减少网络安全事件的发生，保护用户的合法权益和社会公共利益。

现阶段发展较为成熟的网络信息安全方面的研究主要包括：文献［1］提出的基于计算机网络技术的网络信息安全防护方法、文献［2］提出的基于区块链的访问控制模型完成网络信息安全防护、文献［3］提出的基于 IPv6 网络的防御与访问控制融合防护方法以及文献［4］提出的基于攻防博弈模型的网络信息安全防护方法。其中文献［1］提出模型从计算机网络技术视角下，分析网络信息安全问题，在构建复合式网络拓扑结构、优化网络信息安全防护配置、建立多层级协同防护机制、建立身份认证授权系统、建立应急响应机制五方面，构建安全防护体系。当该方法在实际应用中，无法及时地捕获网络信息，导致在面临入侵攻击时多层级协同防护效果较差，网络信息错误率较高。文献［2］提出模型综合考虑 ABAC 模型和区块链的技术原理，对模型中的智能合约进行了具体描述，并在此基础上确定模型的控制工作流程，为域间访问提供标准化的安全、便捷、自主且细粒度的访问控制。该方法虽然对访问进行了控制以对网络信息安全进行防护，但在网络信息安全状态检测方面研究欠缺，实际应用中无法快速检测网络攻击行为和异常情况，导致在防护时存在局限性，仍会有潜在的安全风险发生。文献［3］提出模型提出兼容 IPv6 互联网传输的随机地址生成机制，该机制支持两端时差冗余的随机地址机制，以及支持多线程的无锁随机 IP 地址选取机制旨在辅助移动目标防御所需的随机 IP 地址生成。通过移动目标处理器对原始数据包进行随机地址替换的方法，在标准互联网中传输，结合访问控制技术，可以保护工业互联网设备不受外部设备干扰和攻击。结合访问控制技术，进而保护网络不受外部设备干扰和攻击。但该方法在实现过程中却无法有效追踪网络信息攻击源与路径，导致与访问控制联动性较差，抵御干扰和攻击的效果不佳，产生较高的丢包率。文献［4］依据 CY8C24533 型号处理器，提高系统数据交换与数据处理速度，通过外围底板增强系统的稳定性，并对网络信息安全评估，同时，设定权限管理机制，定义网络攻防博弈的一般策略形式为一个三元组，计算某一个网络区域内被攻击的路径与防御者应选取的防御策略，以此完成基于攻防博弈模型的网络信息安全防护。但该方法在实际应用中，未考虑网络信息攻击源，无法更好地了解攻击者的行为，导致网络信息安全防护效果不佳。因此，针对上述方法在进行主动式网络信息安全防护中所存在的问题，开发了主动式网络信息安全应急联动模型，并引入访问策略控制技术，最大程度的降低入侵攻击对网络信息产生的负面影响，降低网络信息错误率和丢包率。

在突发事件发生时，应急联动是各有关部门或组织之间进行协调和合作的一种协作模式。在应对突发事件的过程中，各有关部门通常通过应急通讯系统或即时信息分享平台相互沟通和协作。网络信息安全涉及多个部门和领域，应急联动模型的运行旨在实现跨部门、跨领域的协同作战，形成合力，提高应对安全事件的能力，并实现快速响应安全事件的目标，从而减少损失。而访问策略控制是一种网络安全技术，用于管理和控制网络用户对资源的访问权限。它建立在特定的策略和规则基础上，用于维护网络数据和资源的安全，确保只有经过授权的用户才能访问和使用这些资源。凭借访问策略控制技术的支持下，可以优化主动式网络信息安全应急联动模型，从而最大限度地提升主动式网络的信息安全水平。因此，提出了基于访问策略控制的主动式网络信息安全应急联动模型研究，旨在增强主动式网络信息安全防护效果。

1 主动式网络信息安全应急联动模型设计

在访问策略控制技术的支持下，优化设计主动式网络信息安全应急联动模型，将主动式网络作为研究对象。该模型实时检测当前网络中是否存在安全风险，并以安全风险检测结果作为启动条件。同时，结合网络信息安全入侵源和入侵路径的追踪结果，确定安全应急联动模型的作用对象[5-8]。考虑主动式网络的工作原理和节点属性，设定应急联动模型的约束条件，通过调动网络设备、用户等对象，执行网络攻击防御操作，实现模型的主动式网络信息应急联动功能，完成有效的动式网络信息安全防护。

1.1 捕获主动式网络数据包作为模型输入项

为了给后续的安全状态检测提供可靠的网络信息数据，并及早发现并应对潜在的安全风险，在这一过程中进行主动式网络数据捕获。将捕获实时运行数据作为输入，可以提高应急响应的效率和准确性。采用网络爬虫算法对主动式网络中的实时数据进行捕获[9-10]，具体的捕获流程如图 1 所示。

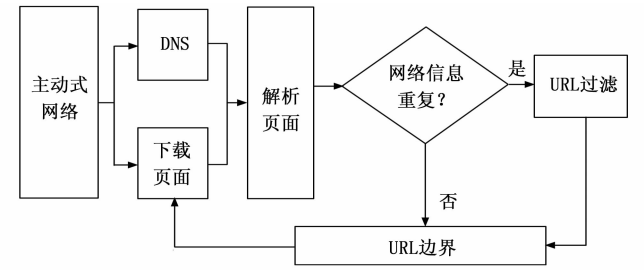

图 1　网络数据包捕获流程图

在实际的主动式网络信息采集过程中，根据 ed2k 网络协议和 Kad 网络协议，并行采集网络中节点及共享文件的索引信息，并将其存入网络信息数据库。数据分析模块从数据库提取服务器信息和节点信息，并根据服务器当前拥有的节点数对服务器进行排名，同时根据网络连接成功率对节点进行排名。这些排名信息将被发送给系统反馈模块。反馈模块根据服务器信息和节点信息调整网络入口节点集合，并生成新的网络入口配置文件。任意时刻网络数据包的捕获结果可以表示为：

$$x(t) = \kappa_{\text{capture}} \times \sum_{i=1}^{n_{\text{node}}} x_t(i) \times f \tag{1}$$

式中，κ_{capture} 表示的是数据包的捕获系数，f 为爬虫对数据包的采集频率，$x_t(i)$ 表示的是主动式网络中第 i 个节点在 t 时刻的实际运行数据，n_{node} 表示的是主动式网络环境中包含的节点数量。为了保证网络数据包的捕获质量，需要对初始采集的数据包执行清洗、补充等预处理操作。数据清洗的目的是检测并处理初始捕获数据包中的错误、重复、异常和不一致数据。在清洗错误数据时，只需判断初始采集的数据是否为错误数据，若属于错误数据，则直接删除；否则，无需执行删除操作。对于重复数据，需要利用公式（2）计算任意两个网络运行数据之间的重复属性：

$$\xi_{ij} = \frac{x_i(t) \cdot x_j(t)}{\| x_i(t) \| \cdot \| x_j(t) \|} \tag{2}$$

式中，$x_i(t)$ 和 $x_j(t)$ 表示的是初始采集的第 i 和 j 个网络数据包。将公式 2 的计算结果与重复度阈值 ξ_0 进行比对，若 ξ_{ij} 证明当前网络数据包为重复数据，需要对其中任意一个进行剔除，完成对重复数据的清洗操作，否则保留上述两个网络数据包，直至所有采集网络数据均比对完成为止。除此之外，还需要采用独立成分分析方式对初始捕获的网络数据包进行降维处理，处理过程可以量化表示为：

$$x_J = \min_U y_{\text{internal}}(\boldsymbol{U}^S \boldsymbol{X} \boldsymbol{X}^S \boldsymbol{U}) - \sum_{i=1}^{N_U} \lg(|\boldsymbol{U}^S x_i(t)|^2) \tag{3}$$

式中，$\boldsymbol{U}$、$\boldsymbol{S}$ 和 $\boldsymbol{X}$ 分别表示的是非奇异矩阵、相互独立基信号和网络数据包集合，N_U 表示的是非奇异矩阵中包含元素数量，y_{internal}（）表示的是联合分布函数。由此重复上述操作，利用公式（1）～（3）完成对主动式网络数据包的捕获与预处理操作。

1.2　检测主动式网络信息安全状态作为模型启动条件

通过对捕获并处理完成的网络数据包进行特征提取和匹配，以检测网络的安全状态，判断当前主动式网络是否存在信息安全问题。以此作为主动式网络信息安全应急联动模型的启动条件[12]。在网络信息安全检测之前，首先需要确定不同入侵状态下网络信息的标准特征，以 DDoS 入侵方式为例，该入侵原理如图 2 所示。

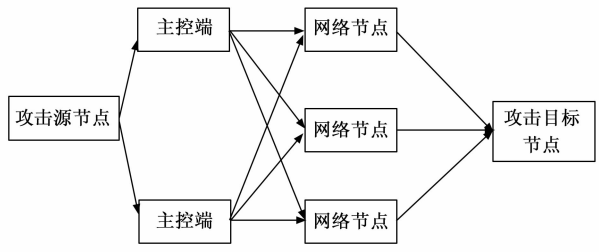

图 2　DDoS 入侵攻击原理图

DDoS 入侵攻击的目标是使目标系统或网络资源耗尽，导致服务中断或不可用。攻击者通常通过控制多个存在漏洞的主机作为傀儡机，同时攻击目标主机或服务器，造成其瘫痪。在网络攻击过程中，攻击者利用攻击工具攻陷主机，并植入恶意程序以自动控制其他主机，使大量主机成为傀儡机，通过协同合作达到预期攻击效果和破坏力。根据上述 DDoS 入侵攻击的执行原理，可以得出在这种攻击下主动式网络信息的标准特征为 $\zeta_b(D)$，同时按照上述方式可以得出其他网络攻击作用下信息的标准特征。

根据网络数据包的捕获结果，提取网络特征，具体包括网络流量、平均数据包大小、数据包分布等向量，其中网络流量特征的提取结果可以表示为：

$$\zeta_{\text{flow}} = \int_{i=1}^{N} v_i \, \mathrm{d}t \tag{4}$$

式中，v_i 表示的是网络信息的传输速率。另外平均数据包大小和数据包分布特征向量的提取结果如下：

$$\begin{cases} \zeta_{\text{size}} = \dfrac{\zeta_{\text{flow}}}{n_{\text{capture}}} \\ \zeta_{\text{distribution}} = \dfrac{n_{\text{capture}}}{B} \end{cases} \tag{5}$$

式中，n_{capture} 和 B 分别表示网络信息的捕获量和网络贷款。会将相关数据代入到上述公式中，即可得出网络信息特征的提取结果。采用加权融合的方式，对采集的特征向量进行融合处理，得出网络信息综合特征的提取结果为：

$$\zeta_c = \bar{\omega}_1 \zeta_{\text{flow}} + \bar{\omega}_2 \zeta_{\text{size}} + \bar{\omega}_3 \zeta_{\text{distribution}} \tag{6}$$

式中，$\bar{\omega}_1$、$\bar{\omega}_2$ 和 $\bar{\omega}_3$ 分别对应的是网络流量、平均数据包大小、数据包分布 3 个特征向量的加权融合权重系数。

那么，主动式网络信息安全状态的检测结果为：

$$s = \sqrt{[\zeta_c - \zeta_b(i)]^2} \tag{7}$$

最终计算得出 s 取值越大，证明对应网络存在入侵攻击风险越大，若计算得出 ζ_c 的值高于 0.9，则认为当前主动式网络存在 i 类入侵攻击。重复上述操作，分别将不同入侵攻击类型作用下主动网络的标准特征代入到公式（7）中，得出满足阈值条件的匹配结果，判定当前主动式网络处于入侵攻击状态，并确定入侵攻击类型。若所有攻击标准特征的匹配度计算结果均不满足阈值条件，则认为当前网络无入侵攻击现象。如果检测得出主动式网络信息处于安全状态，则不启动安全应急联动模型，否则需立即启动模型的应急联动程序。

1.3 追踪主动式网络信息攻击源与路径

针对存在入侵攻击的主动式网络，需要确定网络中攻击源的位置，并推演出具体的攻击路径[13-14]。网络攻击源的定位主要是根据上述状态检测获得入侵攻击类型结果来得知网络攻击信号的强度特征和传播特征，从而得到已知网络节点位置上的攻击源定位结果为：

$$\begin{cases} x_{\text{attack}} = x_k \mathrm{d}_x \\ y_{\text{attack}} = y_k \mathrm{d}_y \end{cases} \tag{8}$$

式中，d_x 和 d_y 分别表示已知网络节点与攻击源节点之间距离在水平和竖直方向上的分量，(x_k, y_k) 为主动式网络中的已知网络节点位置坐标。公式（8）中变量 d_x 和 d_y 的计算公式如下：

$$\begin{cases} d_x = \dfrac{Q_{s\_k}}{Q_{\text{s\_attack}} \kappa_{\text{s\_transfer}} \kappa_{\text{s\_attenuation}}} \cdot \cos\theta \\ d_y = \dfrac{Q_{s\_k}}{Q_{\text{s\_attack}} \kappa_{\text{s\_transfer}} \kappa_{\text{s\_attenuation}}} \cdot \sin\theta \end{cases} \tag{9}$$

式中，Q_{s_k} 和 $Q_{\text{s\_attack}}$ 分别为主动式网络信息安全状态的检测结果对应的网络节点和攻击源节点实际接收的攻击信号强度值，$\kappa_{\text{s\_transfer}}$ 和 $\kappa_{\text{s\_attenuation}}$ 表示的是攻击信号在主动式网络中的传递系数和衰减系数，θ 为已知节点接收攻击信息的偏角。在已知网络信息攻击源位置的情况下，对主动式网络的攻击路径进行推演，推演原理如图 3 所示。

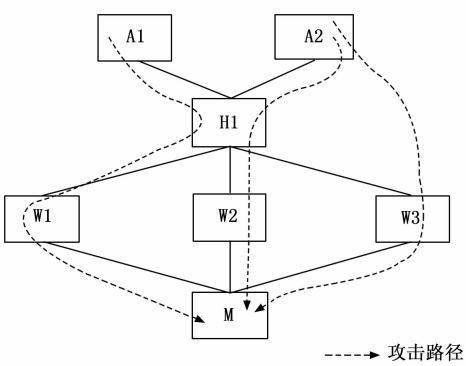

图 3 主动式网络攻击路径推演原理图

图 3 中 A、H、W 和 M 分别表示的是攻击源节点、网络交换机节点、普通网络节点和攻击目标节点，采用概率计算的方式确定攻击目标节点在攻击任意环节的节点选择情况，其中攻击源选择任意节点的概率可以表示为：

$$P = p(H_i)[1 - p(W_j)]^{n_{\text{node}} - i - j} \tag{10}$$

式中，$p(H_i)$ 和 $p(W_j)$ 表示的是攻击源选择第 i 个交换机和第 j 个普通网络节点的概率，由此即可得出主动式网络信息攻击路径的追踪结果为：

$$L = l_{\text{pace}} \frac{(x - x_M)(y_{\text{attack}} - y_M)}{x_{\text{attack}} - x_M} + y_M, P(M) = \max P \tag{11}$$

式中，(x_M, y_M) 表示的是攻击目标节点的位置坐标，$\max P$ 为节点选择概率的最大值，l_{pace} 为步距。在实际的路径追踪过程中，分别生成攻击源与交换机、交换机与普通节点以及普通节点与攻击目标节点之间的攻击路径分量，并通过路径分量的首尾连接，完成对主动式网络信息攻击路径的追踪。

1.4 设定主动式网络信息安全应急联动模型约束条件

为了确保访问的安全性、保护系统和数据的完整性、有效预防网络攻击并优化资源利用，从主动式网络节点功率、节点容量、资源可用性、恢复时间等方面设置安全应急联动模型的约束条件。这些约束条件使模型更加智能和灵活，增强网络信息安全的应急联动功能。网络节点功率是指网络中节点设备在网络中的发射功率，其大小决定了数据传输的距离和范围。网络节点容量包括处理能力和存储能力两个方面。处理能力表示节点能够同时处理的数据量和处理速度。处理能力强的节点可以更快地处理数据，提高网络的传输效率。而存储能力则是指节点能够存储的数据量。存储能力强的节点能够承载更多的数据，从而支持更多的业务和应用。

网络节点功率、节点容量约束条件的设置情况如下：

$$\begin{cases} P_{\text{linkage}} \leqslant 0.9P(i) \\ R_{\text{linkage}} \leqslant 0.8R_{\text{residue}}(i) \end{cases} \tag{12}$$

式中，$P(i)$ 和 $R_{\text{residue}}(i)$ 为网络节点 i 的标准功率和剩余容量值。另外资源可用性约束和恢复时间约束条件的设置结果为：

$$\begin{cases} \varphi \leqslant B\lg(1+\sigma) \\ \lambda \leqslant T_{\max} \end{cases} \tag{13}$$

式中，σ 为网络信道资源中信号和噪声之间的功率比，$T_{\max}$ 为恢复时间的最大限制。按照上述方式可以得出安全应急联动模型中其他约束条件的设置结果，并保证模型运行过程中各个网络节点的运行均满足设定的约束条件。

1.5　实现模型主动式网络信息安全应急联动功能

主动式网络信息安全应急联动模型的实现涉及协调中心、应急响应组、客户等多个主体，模型的运行机理如图 4 所示。

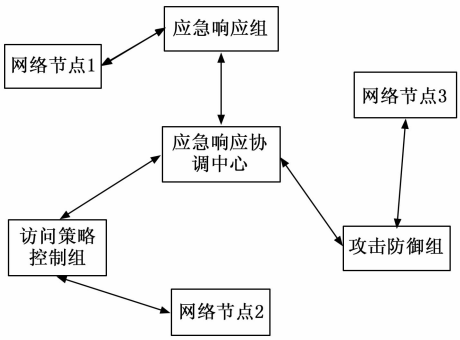

图 4　主动式网络信息安全应急联动模型运行机理图

应急响应协调中心不仅负责保障体系的正常运行，还作为信息共享、交换和分析的核心场所，在联动系统中占据至关重要的地位[15-18]。应急响应组的主要任务是直接应对网络安全事件，其组织结构可以根据实际的技术力量和资源状况与协调中心保持一致，或者进行适当的合并，甚至在某些情况下可以承担部分协调中心的功能。根据应急联动模型的运行机理，基于上述的追踪结果和设定的主动式网络信息安全应急联动模型约束条件，从访问策略控制、攻击防御、信息恢复等方面，进行主动式网络信息安全应急联动，以最快速度解决主动式网络信息的安全问题，并最大程度的提升网络信息的准确性和完整性。

1.5.1　访问策略控制

针对主动式网络存在的信息安全问题，生成实施访问控制的主体对接受控制课题所作出的行为动作集合，生成的网络访问策略可以表示为：

$$Z(G,\psi,\tau,V,F)\rightarrow K \tag{14}$$

式中，G、ψ、τ、V 和 F 分别表示的是规则模式、实施访问控制策略的主体和课题、触发策略规则执行事件、策略生效条件，K 为访问控制策略的行为。在应急联动模型中，网络安全设备所采用的访问控制策略可分为应用级策略和网络级策略两种[19]。应用级策略主要涉及用户和角色管理代理的权限，包括它们可以访问哪些资源以及在发生安全问题时应采取的措施等，呈现出一种相对粗粒度的访问控制[20-21]。而网络级策略则主要体现在防火墙、入侵检测系统、VPN 网关等网络安全设备上，通过一系列包过滤规则对通信流进行精细控制，实现了一种更为细粒度的访问控制。在实际的访问策略控制过程中，需要对策略之间的冲突进行检测，并消解访问策略执行过程中的冲突现象。访问策略冲突的检测过程如图 5 所示。

针对存在冗余冲突的访问策略，在特定规则和逻辑的约束下，随意选择一个访问策略执行，同时考虑其他策略的影响，在策略执行过程中确保不会引入新的冲突。针对存在泛化冲突的访问策略，将其限定在特定范围内执行，例如对部分具有较高可信度的用户赋予访问权限，满足访问权限的可执行访问操作，否则不能进入主动式网络。用户可信度可以表示为：

$$\mu=|\vartheta_{\text{behaviour}}-\vartheta'_{\text{behaviour}}|\otimes|\vartheta_{\text{identity}}-\vartheta'_{\text{identity}}| \tag{15}$$

式中，$\vartheta_{\text{behaviour}}$ 和 $\vartheta_{\text{identity}}$ 分别表示访问用户行为和身份安全性，$\vartheta'_{\text{behaviour}}$ 和 $\vartheta'_{\text{identity}}$ 对应的是用户行为与身份的安全阈值。根据公式（15）的计算结果对用户的访问等级进行划分，完成泛化冲突访问策略的冲突消解。若访问策略存在屏蔽冲突，可以根据其重要性、紧急性等因素进行优先级排序。优先级高的策略优先执行，以避免对业务的影响。另外，针对存在关联冲突的访问策略，将其进行分阶段执行，以避免同时执行多个策略导致的冲突。可以根据策略的优先级、紧急程度等因素，将策略分为不同的阶段，并按照阶段顺序依次执行。

1.5.2　主动式网络信息攻击防御

根据主动式网络信息攻击源与路径的追踪结果，采

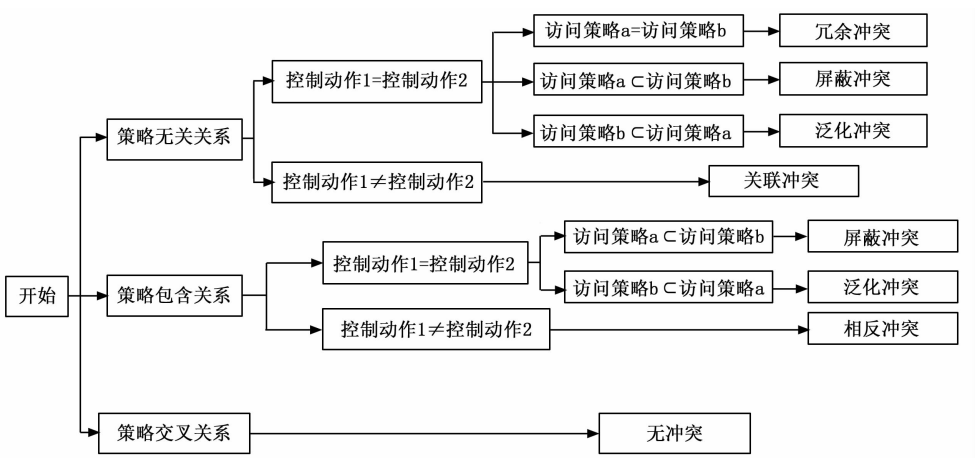

图 5　访问策略冲突检测过程图

用攻击源隔离、攻击路径断开、网络流量控制等方式，实现网络攻击防御操作。攻击源隔离可分为物理隔离和防火墙隔离两种方式，以追踪的网络攻击源为隔离对象，通过物理手段将攻击源与受保护的网络隔离开来，即在网络安全设备上设置过滤规则，阻止来自特定 IP 地址或网络段的流量进入受保护网络。而防火墙隔离是通过配置防火墙规则，可以阻止来自特定 IP 地址、端口或协议的流量进入受保护网络。攻击路径断开防御操作就是将追踪攻击路径中任意一个网络节点调整至关闭状态，迫使攻击源无法按照原路径执行攻击操作。另外，网络流量控制就是通过限制网络流量的速度和数量，防止攻击者利用大量的流量进行攻击，网络防御隔离数据量为：

$$N_{\text{isolate}}=\frac{N_t}{1-R_{\text{linkage}}\left[P_{\text{linkage}}\upsilon_{\text{block}}\bmod\left(\frac{K}{N_t}\right)\right]}*\mu\frac{\bar{\zeta}}{\zeta_{\text{residue}}} \tag{16}$$

式中，N_t 为主动式网络实时传输数据量，υ_{block} 为流量阻断速率，$\bar{\zeta}$ 和 ζ_{residue} 分别为网络各节点承载的平均数据量和网络中数据经过访问策略控制后的剩余数据。根据主动式网络攻击源发出的信号强度，确定网络的防御强度，进而得出流量阻断速率的具体取值，完成对主动式网络的攻击防御操作。

1.5.3 主动式网络信息恢复

在进行上述两方面联动操作的同时，在满足上述资源可用性约束 φ 的基础上，通过定期备份网络数据，来确保有可用的备份资源。以在发生网络故障时，可迅速启动恢复计划，定位故障点并进行隔离，以防止故障扩散。并根据备份策略，在满足恢复时间约束条件 λ 的基础上，从备份中恢复丢失或损坏的数据。最后，通过容错技术和分布式恢复等方式，确保恢复的数据能够正确地接管业务，并尽快恢复网络的正常运行。整个操作流程需要快速、准确地进行，以减少网络故障对业务的影响。

由此，通过上述 3 个方面实现模型主动式网络信息安全应急联动功能，完成有效的主动式网络信息安全防护。

2 模型验证测试实验分析

为了测试基于访问策略控制的主动式网络信息安全应急联动模型的应用性能，设计模型验证测试实验。此次实验的基本原理为：构建静态和动态两种主动式网络作为实验环境，编写网络攻击程序，对主动式网络信息安全产生威胁。利用优化设计的应急联动模型，对存在信息安全风险的主动式网络进行应急处理，模型运行结束后，对主动式网络中的信息完整性、正确性进行度量，得出反映模型应用性能的测试结果。

2.1 构建主动式网络测试对象

模型测试实验中构建的主动式网络由外网区、隔离区和内网区 3 个部分组成，3 个区域通过防火墙进行隔离，隔离区中的服务器型号为 Apache 服务器，能够提供 Web 服务、Smtpd 服务、Sshd 远程服务、Ftpd 服务。内网服务器型号与隔离区相同，提供数据库服务，并为主机提供 SshdService 和 FtpdService。由于工作需要，SQLServer 同时提供 RPCService 供外网区域访问。根据组成主动式网络节点的移动属性，将网络分为静态和动态两种类型，静态环境中所有节点均为固定节点，而动态网络中的节点处于实时运动状态，移动方向与速度均不相同。初始状态下，主动式网络处于正常运行状态，但组成网络节点的脆弱程序存在差异。

2.2 编写主动式网络攻击程序

以构建的主动式网络为攻击对象，编写 DDoS、扫描攻击等网络攻击程序。编写攻击程序的运行界面如图 6 所示。

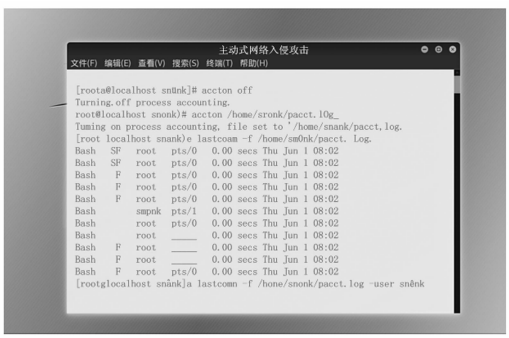

图 6 主动式网络攻击程序运行界面

为体现出应急联动模型在不同网络攻击状态下的作用效果，编写多个不同类型的攻击程序，并保证攻击程序之间的独立性。主动式网络攻击程序的编写与执行情况，如表 1 所示。

表 1 主动式网络攻击程序信息表

攻击程序编号	网络攻击类型	网络攻击强度等级
1	DDoS	II
2	扫描攻击	I
3	口令入侵	III
4	特洛伊木马	I
5	黑客软件	IV
6	安全漏洞	II

表 1 中 I 攻击等级最高，IV 攻击等级最低。攻击程序编写完成后，需要对程序进行调试，并确定的攻击强度。在编写的程序首段加设一个强制中断指令，保证攻击程序的可控性。

2.3 选择模型开发工具

模型验证测试实验的开发环境为计算机的处理器是

Intel（R）Core（TM）3.40 GHz，拥有 16 G 的可用内存，并运行着 Windows7 旗舰版操作系统。其模型功能运行程序所使用的代码是基于 Weka3.6 的开源源代码。Weka3.6 是一款广泛使用的开源机器学习和数据挖掘软件工具，具有直观易用的用户界面和丰富的可视化工具。它支持多种机器学习算法，包括分类、聚类、回归和关联规则挖掘等，可用于解决各种数据挖掘任务。同时，Weka3.6 还提供了多种数据预处理工具，如过滤、编码和变换等，用于清洗数据、处理缺失值、进行特征选择和数据转换等。此外，Weka3.6 还支持插件扩展，用户可以通过编写插件来扩展 Weka 的功能。

2.4　描述模型验证测试实验过程

利用选择的开发工具完成对主动式网络信息安全应急联动模型的开发，将其应用到存在攻击行为的主动式网络中，通过应急联动模型中访问策略控制方法的运行，得出相应的执行结果。在访问策略控制技术的支持下，完成对主动式网络信息安全的应急联动任务，图 7 表示的是 DDoS 攻击下安全应急联动模型的运行结果。

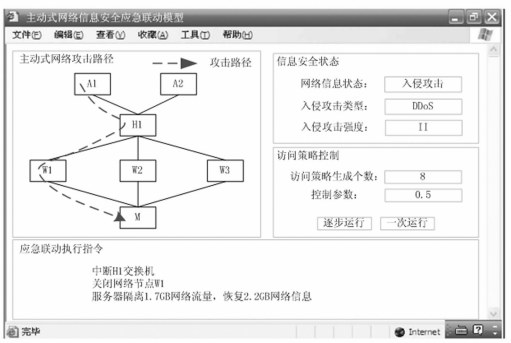

图 7　主动式网络信息安全应急联动模型运行界面

按照上述方式可以得出其他攻击类型作用下，安全应急联动模型的执行结果。为了体现出优化设计模型在应用性能方面的优势，设置基于计算机网络技术的网络信息安全防护模型和基于区块链的访问控制模型作为实验对比项，利用相同的开发工具，完成对比模型的开发，得出对应的应急联动模型执行结果，并对相关数据进行统计。

2.5　设置模型性能测试指标

此次实验分别从网络信息完整性、正确性两个方面对模型的应用性能进行度量，设置的量化测试指标为信息丢包率和误码率，上述指标的数值结果为：

$$\begin{cases}\eta_{\text{loss}} = \left(1-\dfrac{n_{\text{run}}}{n}\right)\times 100\% \\ \eta_{\text{err}} = \dfrac{n_{\text{err}}}{n}\times 100\%\end{cases} \tag{17}$$

式中，n_{run}、n_{err}和 n 分别表示的是主动式网络运行结束后网络中的有效信息量、错误信息量以及初始输入信息量。最终计算得出丢包率和误码率取值越高，证明对应模型作用下网络信息的完整性和正确性越低。

2.6　模型验证测试实验结果与分析

2.6.1　主动式静态网络

在静态网络环境下，通过网络节点数据的统计，得出攻击作用下，主动式网络信息安全应急联动模型的应用性能测试结果，如表 2 所示。

将表 2 中的数据代入到公式（17）中，计算得出 3 种应急联动模型作用下，静态网络信息的丢包率和网络信息错误率如图 8 所示。

根据图 8 所得结果可知，所提基于访问策略控制的主动式网络信息安全应急联动模型的丢包率和错误率均低于其他两种对比项，则 3 种模型的静态网络信息平均丢包率分别为 4.10%、2.42%和 0.22%，而网络信息错误率的平均值分别为 7.35%、4.50%和 0.48%。对比上述结果可得出，所提基于访问策略控制的主动式网络信息安全应急联动模型在主动式静态网络表现良好，可有效实现对入侵攻击的抵挡，降低信息丢包率和错误率。

2.6.2　主动式动态网络

以主动式动态网络作为实验对象，通过 3 种模型的运行，得出模型应用性能测试结果，如表 3 所示。

通过公式（17）的计算，得出两种传统应急联动模型作用下，动态网络的丢包率和网络信息错误率如图 9 所示。

表 2　动态网络信息安全应急联动模型性能测试数据表

攻击程序编号	初始网络数据量/GB	攻击作用下的有效信息量/GB			错误信息量/GB		
		应用基于计算机网络技术的网络信息安全防护模型	应用基于区块链的访问控制模型	应用基于访问策略控制的主动式网络信息安全应急联动模型	应用基于计算机网络技术的网络信息安全防护模型	应用基于区块链的访问控制模型	应用基于访问策略控制的主动式网络信息安全应急联动模型
1	54.7	52.2	52.9	54.5	5.5	2.4	0.4
2	68.9	64.5	66.8	68.7	2.6	2.7	0.2
3	96.4	92.6	93.2	96.3	7.4	3.9	0.6
4	85.5	81.3	83.7	85.4	5.3	4.4	0.5
5	73.1	70.8	72.2	73.0	6.0	3.8	0.1
6	60.0	59.0	59.1	59.8	4.9	2.6	0.3

表 3 静态网络信息安全应急联动模型性能测试数据表

攻击程序编号	初始网络数据量/GB	攻击作用下的有效信息量/GB			错误信息量/GB		
		应用基于计算机网络技术的网络信息安全防护模型	应用基于区块链的访问控制模型	应用基于访问策略控制的主动式网络信息安全应急联动模型	应用基于计算机网络技术的网络信息安全防护模型	应用基于区块链的访问控制模型	应用基于访问策略控制的主动式网络信息安全应急联动模型
1	54.7	51.4	52.6	54.2	5.9	2.7	0.4
2	68.9	64.2	66.2	68.5	3.8	2.9	0.4
3	96.4	92.3	92.8	96.2	7.7	4.5	0.6
4	85.5	81.0	83.3	85.3	5.9	4.9	0.8
5	73.1	70.1	72.1	73.0	6.5	4.0	0.3
6	60.0	58.2	58.4	59.7	5.7	3.7	0.4

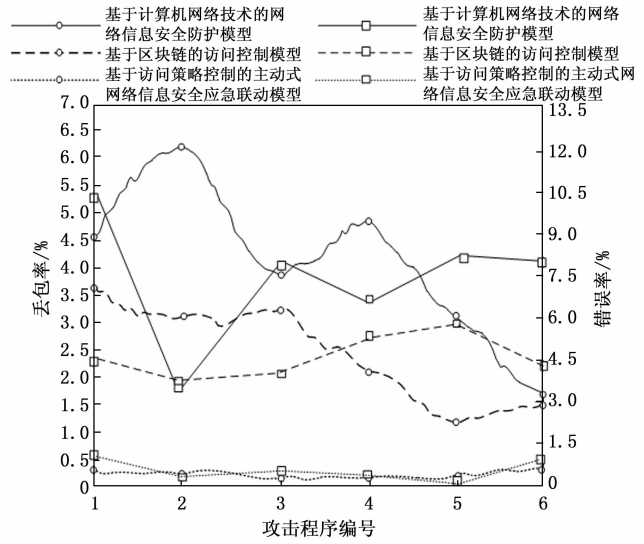

图 8 静态网络信息丢包率和错误率结果

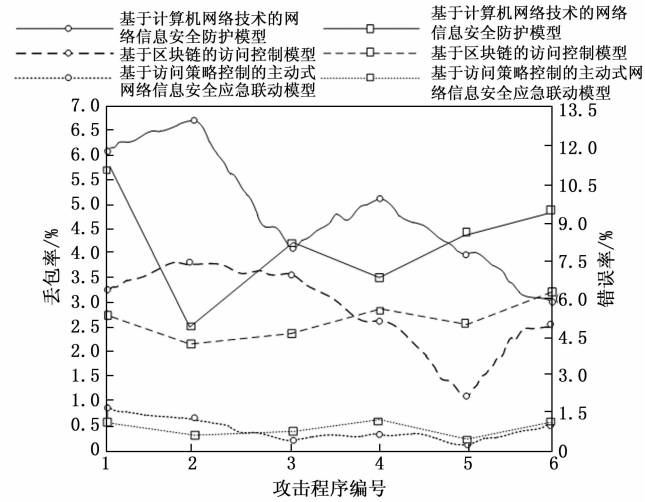

图 9 动态网络信息丢包率和错误率结果

根据图 9 所得结果可知，所提基于访问策略控制的主动式网络信息安全应急联动模型在主动式动态网络中的应用，其丢包率和错误率也低于其他两种对比项。3 种模型的动态网络信息平均丢包率分别为 4.91%、3.01% 和 0.43%，平均信息错误率分别为 8.26%、5.20% 和 0.66%。对比上述结果可得出，所提基于访问策略控制的主动式网络信息安全应急联动模型在主动式动态网络中仍具有较好的表现。综合在上述两种网络情况下的结果说明，所提模型可最大程度的降低入侵攻击对网络信息产生的负面影响，降低网络信息错误率和丢包率。

3 结束语

基于访问策略控制的主动式网络信息安全应急联动模型在保障网络信息安全方面具有重要意义。通过建立科学的应急联动模型，能够实现及时发现和应对网络攻击，有效保护企业核心信息资产，提升网络安全防护水平。在实际应用中，该模型不仅有助于提高网络安全事件的响应速度和处理效率，还能够为企业的信息安全建设提供有力的支持。因此，应该重视并积极推广这种主动式网络信息安全应急联动模型，以应对日益复杂的网络攻击和信息安全挑战。

参考文献：

[1] 陈辉定. 基于计算机网络技术的网络信息安全防护体系构建 [J]. 现代雷达，2023，45 (2)：101－103.

[2] 张建标，张兆乾，徐万山，等. 一种基于区块链的域间访问控制模型 [J]. 软件学报，2021，32 (5)：1547－1564.

[3] 李振宇，丁 勇，袁 方，等. 基于 IPv6 网络的移动目标防御与访问控制融合防护方法 [J]. 计算机研究与发展，2022，59 (5)：1105－1119.

[4] 龙曼丽. 基于攻防博弈模型的网络信息安全防护系统设计 [J]. 现代电子技术，2021，44 (4)：115－118.

[5] 刘宁春，郜 帅，侯心迪，等. 一种信息中心移动自组网中的数据访问控制机制 [J]. 北京邮电大学学报，2021，44 (2)：54－60.

[6] 刘 晶，朱炳旭，梁佳杭，等. 基于主侧链合作的区块链访问控制策略 [J]. 计算机工程，2022，48 (3)：10－16.

[7] 王静宇，杨 力. 基于区块链和策略分级的访问控制模型 [J]. 计算机工程与设计，2022，43 (5)：1232－1239.

[8] 巩 坪，王九如，宋万水，等. 基于智能合约的物联网权限传递访问控制模型 [J]. 郑州大学学报 (理学版)，2023，55 (3)：28－33.

[9] SUN YONG，王译霄，宣晓婷，等. 基于机器学习联合网络爬虫算法的果汁鉴伪技术的研究进展 [J]. 华中农业大学学报，2022，41 (1)：269－276.

[10] 刘多林，吕　苗. Scrapy 框架下分布式网络爬虫数据采集算法仿真 [J]. 计算机仿真，2023，40 (6)：504－508.

[11] 李　杨，徐　龙，李研强，等. 基于智能合约的物联网访问控制架构与验证 [J]. 计算机应用，2022，42 (6)：1922－1931.

[12] 邓三军，袁凌云，孙丽梅. 基于信任度的物联网访问控制模型研究 [J]. 计算机工程与设计，2022，43 (11)：3030－3036.

[13] 苗新亮，常　瑞，潘少平，等. 可信执行环境访问控制建模与安全性分析 [J]. 软件学报，2023，34 (8)：3637－3658.

[14] 董江涛，闫沛文，杜瑞忠. 雾计算中基于无配对 CP-ABE 可验证的访问控制方案 [J]. 通信学报，2021，42 (8)：139－150.

[15] 王清旭，董理君，贾　伟，等. 开放式环境下基于向量表征与计算的动态访问控制 [J]. 计算机科学，2022，49 (S2)：727－733.

[16] 丁　滟，王　鹏，王　闯，等. 基于属性的操作系统动态强制访问控制机制 [J]. 计算机工程与科学，2023，45 (10)：1770－1778.

[17] 王　赟，于　尧，赵雨佳，等. 家庭物联网中基于 SDN 的入侵检测防御机制 [J]. 控制工程，2021，28 (5)：1027－1032.

[18] 程雨芊，程中鼎. 基于 LSSVM 的传感器网络安全风险预测与控制 [J]. 沈阳工业大学学报，2022，44 (5)：558－564.

[19] 颜　蔚. 基于卷积神经网络的无线网络安全风险评估及控制 [J]. 沈阳工业大学学报，2022，44 (5)：565－569.

[20] 高春刚，王永杰，熊鑫立. MTDCD：一种对抗网络入侵的混合防御机制 [J]. 计算机科学，2022，49 (7)：324－331.

[21] 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.

(上接第 166 页)

[6] SCHUG E C，AKSTETER J W，HUFF R W，et al. Guidance and control for ship automatic landing using GPS [C] // Proceedings of the 57th Annual Meeting of the Institute of Navigation，ION 2001，Albuquerque NM. USA，2001：852－862.

[7] SOUSA P，WELLONS L，COLBY G，et al. Test results of an F/A-18 automatic carrier landing using shipboard relative global positioning system [R]. ADA417314，Naval Air Warfare Center Aircraft Div Patuxent River MD，2003.

[8] URNES J M，HESS R K. Development of the F/A-18A automatic carrier landing system [J]. Journal of Guidance Control and Dynamics，1985，8 (3)：289－295.

[9] 梁颖茜，常绍平，王青林. 基于 RTK 定位的差分卫星引导技术研究 [J]. 测控技术，2022，41 (8)：22－26.

[10] MISRA P，ENGE P. Global positioning system，signals，measurements，and performance，second edition [M]. USA：Ganga-Jamuna Press，2006.

[11] HEO M-B，PERVAN B. Carrier phase navigation architecture for shipboard relative GPS [J]. IEEE Transactions on Aerospace and Electronic Systems，2006，42 (2)：670－679.

[12] JOERGER M，STEVANOVIC S，KHANAFSEH S，et al. Differential RAIM and relative RAIM for orbit ephemeris fault detection [C] // Proceedings of the 2012 IEEE/ION Position，Location and Navigation Symposium. Myrtle Beach，SC，USA：IEEE，2012：174－187.

[13] PERVAN B，CHAN F-C，GEBRE-EGZIABHER D，et al. Performance analysis of carrier-phase DGPS navigation for shipboard landing of aircraft [J]. Journal of the Institute of Navigation，2003，50 (3)：181－191.

[14] 王官龙，崔晓伟，陆明泉. 北斗三频海基 JPALS 无故障导航算法 [J]. 航空学报，2017，321340，38 (12)，1－9.

[15] 聂　欣，张　朔，高　飞，等. 卫星导航着舰系统完好性分析及性能研究 [C] // 中国卫星导航系统管理办公室学术交流中心，第十四届中国卫星导航年会论文集——S02 卫星导航系统与增强，2023.

[16] SUBRAHMANYAM M B. H∞ design of F/A-18A automatic carrier landing system [J]. Journal of Guidance Control and Dynamics，1994，17 (1)：187－191.

[17] BUTTRILL C S，ARBUCKLE P D，HOFFLER K D. Simulation model of a twin-tail，high performance airplane [R]. NASA-TM-107601，1992.

[18] 何霄阳，张　冬，甄　冲，等. 全自动着舰系统 α-β-γ 滤波器 [J]. 飞机设计，2022，42 (1)：4－10.

[19] NICHOLSON D，HENDRICK C M，JAQUES E R，et al. Scaled experiments in Vision-Based approach and landing in high sea states [C] // Proceedings of AIAA AVIATION 2022 Forum，Chicago，USA，2022.

[20] 张　琳，杜智慧，罗　瑜，等. 舰尾流随高扰动模型对直升机着舰悬停控制的影响研究 [J]. 计算机测量与控制，2022，30 (3)：106－113.

[21] 李　煜，刘小雄，李吉宽，等. 基于 L1 自适应着舰纵向控制与特性分析 [J]. 计算机测量与控制，2018，26 (12)：120－124.

[22] 汪　节，韩　维，王家兴，等. MAGIC CARPET 着舰对甲板运动的控制策略 [J]. 电光与控制：1－8 [2023-10-27]. http://kns.hggfdd.top/kcms/detail/41.1227.TN.20230921.1348.002.html.