基于量子神经形态计算的实时主动防御系统

Real-Time Active Defense System Based on Quantum Neuromorphic Computing

王智明，丁　莹，于　城（中国联合网络通信集团有限公司，北京 100033）
Wang Zhiming，Ding Ying，Yu Cheng（China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：
随着网络安全威胁的日益复杂化和多样化，基于传统冯·诺依曼架构的网络安全防御系统在能效、响应延迟和动态适应性方面，面临严峻挑战。提出一种基于量子神经形态计算的实时主动防御系统，该系统融合了量子计算与神经形态的计算优势，设计了光子—量子融合加速架构，采用量子脉冲神经网络（QSNNs）实现威胁识别，并探索量子纠缠态突触设计在多节点量子网络中的抗干扰性。该系统可深度适配物联网边缘计算场景，通过轻量化节点实现终端级实时防御，其量子纠缠态突触设计还支持跨域分布式防御协同，在多云环境中实现无延迟威胁情报共享与联动响应，为网络安全防御提供创新且有效的解决方案。

关键词：
量子神经形态计算；实时主动防御系统；量子纠缠态突触
doi：10.12045/j.issn.1007-3043.2025.10.005
文章编号：1007-3043（2025）10-0023-07
中图分类号：TN914
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
As cybersecurity threats grow increasingly complex and diverse，traditional defense systems based on the Von Neumann architecture face serious challenges in energy efficiency，response latency，and dynamic adaptability. It proposes a real-time active defense system based on quantum neuromorphic computing，which integrates the advantages of quantum computing and neuromorphic engineering. A photonic-quantum hybrid acceleration architecture is designed，which adopts quantum spiking neural networks （QSNNs） for threat detection. Furthermore，the anti-interference of quantum entangled synapse designs in multi-node quantum networks is explored. The system is highly adaptable to IoT edge computing scenarios，enabling real-time terminal-level defense via lightweight nodes. And the design also supports cross-domain distributed defense collaboration，facilitating zero-latency threat intelligence sharing and coordinated response in multi-cloud environments，which provides a novel and effective solution for cybersecurity defense.

Keywords：
Quantum neuromorphic computing；Real-time active defense system；Quantum entangled synapse

引用格式：王智明，丁莹，于城. 基于量子神经形态计算的实时主动防御系统[J]. 邮电设计技术，2025（10）：23-29.

0　前言

随着网络的复杂化、多样化，新型网络安全威胁不断涌现。传统冯·诺依曼网络安全防御系统面临能效低、响应延迟高、难以应对动态变化攻击等诸多难题。而基于量子计算和神经形态计算技术的新型实时主动防御系统，可以高效解决上述难题。其中，量子计算通过量子叠加、纠缠和干涉等技术特性可实现指数级的计算加速。神经形态计算通过模仿生物神经系统的结构和功能，融合事件驱动脉冲神经网络（SNN）来实现高效信息处理，具有低功耗、高并行性和实时处理的优势[1]，并且神经形态计算算法评估和优化有显著进展，例如 Yik 等人提出的 NeuroBench 就是神经形态计算算法的评估和改进工具，推动了神经形

收稿日期：2025-08-08

态系统在复杂任务中的应用[2-3]。基于量子神经形态计算的实时主动防御系统可快速检测并响应安全威胁,同时高效处理海量网络数据,在网络安全领域具有巨大的发展潜力。本文致力于研究基于量子神经形态计算的实时主动防御系统,以解决传统网络安全防御系统在能效、延迟和动态适应性方面的难题,为网络安全提供更高效的技术保障。

1 量子神经形态计算理论体系

量子神经形态计算融合了量子计算和神经形态计算2门新兴交叉学科。量子计算的理论基础源于量子力学的基本原理,量子比特作为量子计算的基本单元,能够处于0和1的叠加态,这使得量子计算机可以同时处理多种可能的计算状态,从而在特定问题上实现远超经典计算机的计算速度。神经形态计算则模仿生物神经系统的结构与功能,通过事件驱动的SNN实现高效信息处理,具备低功耗、高并行性和实时处理的优势[4]。两者融合后,量子比特用于模拟神经元状态。量子纠缠用于描述多量子比特间的强相关性,为并行处理提供强大支撑[5-6],以实现神经元间的突触连接即量子纠缠态突触,形成兼具量子计算并行加速能力与神经形态计算低功耗实时特性的系统。QSNNs是该体系的重要组成部分,通过将传统SNN的神经元和突触替换为量子版本,实现更高效的模式识别与信息处理。同时,该体系融合量子算法与神经形态学习算法,如脉冲时间依赖可塑性(STDP)与量子算法结合,形成适用于量子神经形态系统的学习机制,持续优化性能提升复杂模式识别能力。光子—量子融合加速架构也是该理论体系的核心内容[7-9]。该架构结合了光子计算高速、低功耗、高带宽的特点与量子计算的并行处理能力,通过合理分配计算任务提升系统整体性能。其中,大规模线性运算交由光子计算处理,复杂的非线性变换和优化问题则由量子计算负责。这种分工协作方式充分发挥2种计算方式的优势,为量子神经形态计算在高效处理海量数据和复杂任务方面提供了架构支撑,成为连接理论与实际应用的关键环节。

2 基于量子神经形态计算的实时主动防御系统

基于量子神经形态计算的实时主动防御系统,充分利用量子神经形态计算的优势,构建一个能够高效、快速、准确应对网络安全威胁的防御体系。该系统从网络安全防御的实际需求出发,结合量子神经形态计算的理论和技术特点,通过数据采集与预处理、量子神经形态威胁检测引擎、威胁响应与决策和系统管理与控制模块之间的协同工作,实现对网络安全威胁的实时检测、准确识别和快速响应。

2.1 系统架构

基于量子神经形态计算的实时主动防御系统架构采用分层设计,将各功能模块有机整合,形成高效协同的整体。该架构从下到上分为基础设施层、数据层、处理层、应用层和管理层,各层间通过标准化接口实现数据交互,保障灵活性与可扩展性。系统架构如图1所示。

基础设施层主要为基于量子神经形态计算的实时主动防御系统架构提供量子计算、光子计算、网络和存储等硬件设备。

数据层是系统的基础,负责数据的采集、存储和管理。采集点覆盖网络关键路径与节点,用于收集网络流量、系统日志等数据。数据传输至采用Hadoop分布式文件系统(HDFS)的存储模块,以满足海量数据存储需求,并保证高可靠性与可扩展性。数据管理模块对存储数据进行组织,建立索引以便于查询,同时可实施生命周期管理,清理过期数据,以节省空间。

处理层即核心计算层,用于实现数据预处理、威胁检测与分析任务。数据预处理模块对数据层数据进行清洗、特征提取和压缩,转换为适合威胁检测引擎处理的标准格式。量子神经形态威胁检测引擎是处理层核心,依托光子—量子融合加速架构,由多个量子脉冲神经网络组成,借助量子计算并行性与神经形态计算高效性,实时分析数据并识别攻击模式[10]。其检测准确率可通过模型:

$$\mathrm{Acc} = \alpha \cdot \mathrm{QSNN}_{\mathrm{out}} + (1-\alpha) \cdot \xi \cdot \mathrm{Entropy}(X) \quad (1)$$

其中,$\mathrm{QSNN}_{\mathrm{out}} \in [0,1]$为QSNNs层的原始检测结果,$\alpha$为权重系数,$\alpha$=0.7。

$$\mathrm{Entropy}(X) = -\sum p(x)\log_2 p(x) \quad (2)$$

其中,$\mathrm{Entropy}(X)$为输入数据X的信息熵,用于量化数据复杂性。

应用层实现威胁响应与决策等功能,并为管理层提供安全服务。其威胁响应子模块根据威胁信息自动触发阻断流量、隔离节点、更新安全策略等防御措施[11]。决策支持子模块对历史与实时数据进行分析,以辅助管理员选择最优响应策略。此外,应用层还可

图1　基于量子神经形态计算的实时主动防御系统架构

提供威胁情报共享功能，并和安全设备构成协同防御体系。

管理层实现系统管理与监控功能以保障系统稳定运行与性能优化。管理员通过配置管理子模块调整采集频率、检测阈值等参数，性能监控子模块实时采集CPU利用率、威胁检测率等指标[12]。人机交互界面将指标可视化并在指标异常时进行告警。安全管理子模块实现用户认证、权限管理与日志审计等功能，防止未授权的非法访问。

基于量子神经形态计算的实时主动防御系统架构同时考虑冗余与容错设计，关键节点和模块采用冗余部署方式，结合故障检测与恢复机制，提升系统容错率、可靠性与可用性。光子—量子融合加速架构贯穿处理层，量子计算单元运行量子脉冲神经网络来识别攻击模式，光子计算单元处理大规模线性运算，量子和光子计算单元通过光电接口和控制与同步模块协同工作，共同提升系统处理效率与能效比。

2.2　系统模块

如图2所示，系统包括数据采集与预处理、威胁响应与决策、系统管理与控制、光电接口、控制与同步以及量子神经形态威胁检测引擎6个模块。

数据采集与预处理模块通过部署在网络关键节点的传感器、探针等设备，广泛采集网络流量、系统日志、应用程序日志以及安全设备告警等数据。数据预处理子模块采用数据清洗技术，剔除噪声、重复及错误数据，并从原始数据中提炼出源IP地址、目的IP地址、端口号、协议类型、数据包长度、用户登录信息等关键特征。数据预处理子模块通过霍夫曼编码、LZW编码等压缩算法减少数据量，从而提升传输与处理效率。

威胁响应与决策模块接收威胁检测引擎输出的信息，并判断威胁的紧急程度及可能产生的影响，进而从预设响应策略库中选取合适的应对措施。威胁响应与决策模块面对轻微异常情况可生成安全警报通知管理员；面对严重攻击则采取自动阻断流量、隔离受感染节点等措施。同时，威胁响应与决策模块具备自主学习能力，通过分析历史响应结果持续优化策略，进而提升防御的准确性与有效性。

管理员可通过系统管理与控制模块中的配置管理子模块，调整符合网络环境和安全需求的系统参数，系统管理与控制模块中的性能监控子模块实时采集CPU利用率、内存占用率、威胁检测率等指标，能够及时发现并排除故障。安全审计子模块可记录系统全部操作及安全事件，并形成审计日志，以便于后续分析追溯。

量子神经形态威胁检测引擎包含输入层、QSNNs层和输出层。输入层采用事件驱动编码方式，将预处理后的连续数据流转换为离散脉冲序列，契合神经形态计算特性以提高效率，计算公式为：

$$s(t) = \Theta(x(t) - \theta_{\text{th}}) \tag{3}$$

其中，$\Theta(\cdot)$为阶跃函数，$x(t)$为连续输入信号，θ_{th}为脉冲发放阈值，且可以通过系统配置管理模块动态调整，θ_{th}默认值为0.6。

QSNNs层包含多个专用网络，用于识别网络扫

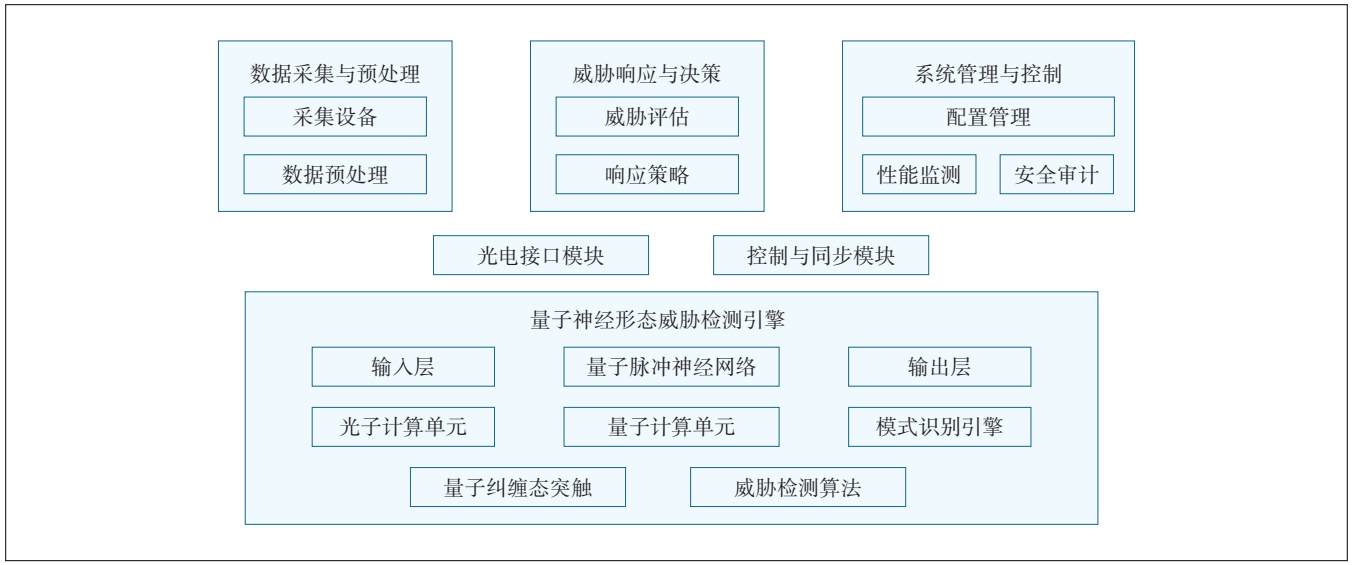

图2 系统模块

描、恶意软件传播、DDoS攻击等特定攻击模式[13]。网络中神经元通过量子纠缠态突触连接,其连接强度更新规则为:

$$\Delta\omega_{ij} = \eta \cdot \exp\left(-\frac{|t_i - t_j|}{\tau}\right) \cdot \xi \tag{4}$$

其中,η为学习率,取值范围为[0.01,0.1],τ为时间衰减常数,默认值为5 ms,ξ为量子纠缠度,$\xi \in [0,1]$。

利用量子纠缠特性能够实现高效信息传递,突破传统架构的能效瓶颈。输出层则将QSNNs的输出结果转换为威胁类型、概率、严重程度等系统可解读的信息,为后续响应决策提供依据。同时,该引擎依托光子—量子融合加速架构,让光子计算负责处理大规模线性运算,量子计算实现复杂非线性变换,充分发挥两者的优势。

光电接口模块是光子—量子融合加速架构的关键连接部分,用于实现光子计算与量子计算之间的信息交互[14]。该模块可实现光信号与电信号的低损耗、高保真转换,确保光子计算处理的光信号能准确转换为量子计算可处理的电信号。同时,该模块具备高速数据传输能力,能够匹配2种计算方式的高速特性,保障系统高效运行。

控制与同步模块在混合架构中可实现协调调度功能,确保光子计算与量子计算的协同工作,该模块通过精确的时钟同步机制,使光子计算与量子计算在时间上保持一致,避免因时间偏差导致的数据处理错误。控制与同步模块还可根据任务类型和负载情况动态分配计算资源,任务分配公式为:

$$\text{Processing Unit}(T) = \begin{cases} \text{Photonic Computing} & \alpha \geqslant 0.7 \\ \text{Quantum Computing} & \alpha < 0.7 \end{cases} \tag{5}$$

其中,α为任务中线性运算占比。

将任务分配给对应计算部分,以最大化系统整体性能,同时监测2个部分运行状态,在出现异常时及时调整恢复,保障系统稳定。

2.3 业务流程

基于量子神经形态计算的实时主动防御系统业务流程主要包含数据采集与预处理、威胁检测、威胁响应与决策3个紧密衔接的防御闭环。业务流程如图3所示。

数据采集与预处理是流程起点,系统通过网络中部署的采集设备持续收集网络流量、系统日志、安全事件等数据,并按照预设策略发送至预处理模块。预处理模块首先进行过滤格式错误的日志、删除重复数据包等操作来清洗数据,其次再提取网络流量的IP地址、端口号,以及系统日志的用户操作信息等安全相关特征,最后压缩特征数据以提升后续处理效率,压缩后的数据将传输至威胁检测引擎。系统最大吞吐量反映了处理海量数据的能力。

威胁检测是流程的核心环节,量子神经形态威胁检测引擎接收预处理数据,并将其转换为QSNN可处理的脉冲序列。输入层初步处理后传递给QSNN层,多个QSNN并行工作,神经元通过量子纠缠态突触连接,利用量子特性快速分析脉冲序列,识别特定攻击

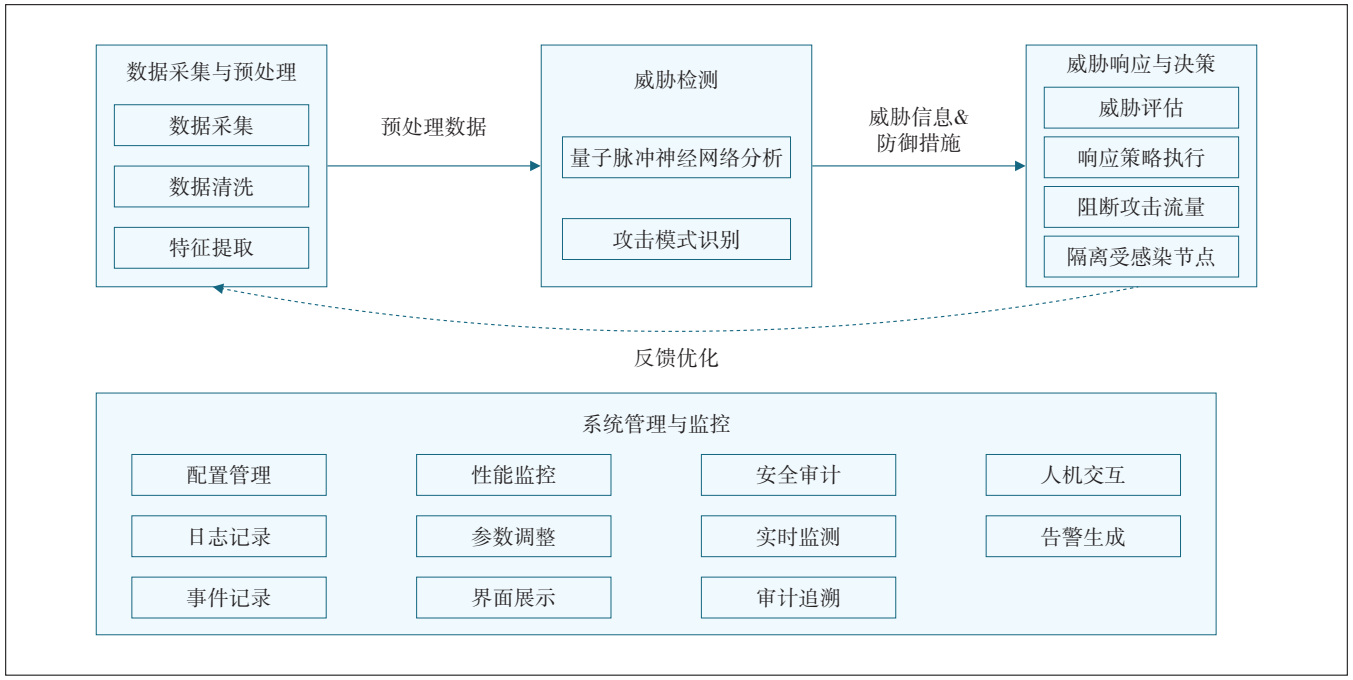

图3　业务流程

模式。输出层整合处理网络输出结果，生成威胁类型、等级、来源等信息，传递至响应与决策模块。

威胁响应与决策中的威胁评估子模块评估威胁紧急程度、影响范围及可能损失，并选择响应措施。响应策略执行子模块执行响应策略，具体包含：低等级威胁对应的生成警报并通知管理员，中等级别威胁对应的暂时阻断访问和加强监控等措施，高等级攻击对应的立即阻断流量和隔离受感染节点。威胁响应与决策阶段在执行后将持续监测执行结果，若威胁未消除则重新评估并调整策略。

系统管理与监控中的配置管理子模块可根据网络环境调整采集策略、检测阈值等参数，性能监控子模块可实时监测 CPU 利用率、数据处理速度等指标，并在指标异常时告警。安全审计子模块可记录全部操作与事件，并形成审计日志用于分析追溯。管理员可通过人机交互界面查看系统状态，并进行手动干预。

3　系统部署方案

基于量子神经形态计算的实时主动防御系统部署方案如图 4 所示，该方案的整体架构分为 3 个主要部署环境和 1 个统一的网络拓扑结构。在网络部署环境中，系统采用三层架构设计，核心层承载威胁检测引擎和数据存储节点 2 个关键模块，威胁检测引擎负责运行量子脉冲神经网络算法进行实时威胁分析，数据存储节点采用分布式架构存储海量安全数据和威胁情报。汇聚层部署数据采集设备和预处理节点，数据采集设备通过高速网络接口从各个网络节点收集流量数据、日志信息和安全事件，预处理节点对收集到的原始数据进行清洗、格式化和特征提取处理，为上层威胁检测提供标准化的数据输入。接入层部署轻量级探针和终端设备，轻量级探针以最小的系统资源占用监控终端行为和网络通信，终端设备包括各类工作站、服务器和网络设备，通过探针实现全面的安全监控覆盖。

云计算环境部署展现了系统在现代云基础设施中的适配能力，云平台层面部署虚拟机集群和容器服务 2 种计算资源形式，虚拟机集群提供传统的虚拟化计算环境，支持大规模并行处理任务，容器服务则提供轻量级、快速部署的微服务架构支持。云服务层包含弹性扩展和 API 接口 2 个核心功能模块，弹性扩展模块根据威胁检测负载和数据处理需求自动调整计算资源分配，API 接口模块提供标准化的服务接口供外部系统集成和调用。云端管理层由中心管理节点和协同防御模块构成，中心管理节点负责整个云环境中各个模块的统一调度和管理，协同防御模块实现多

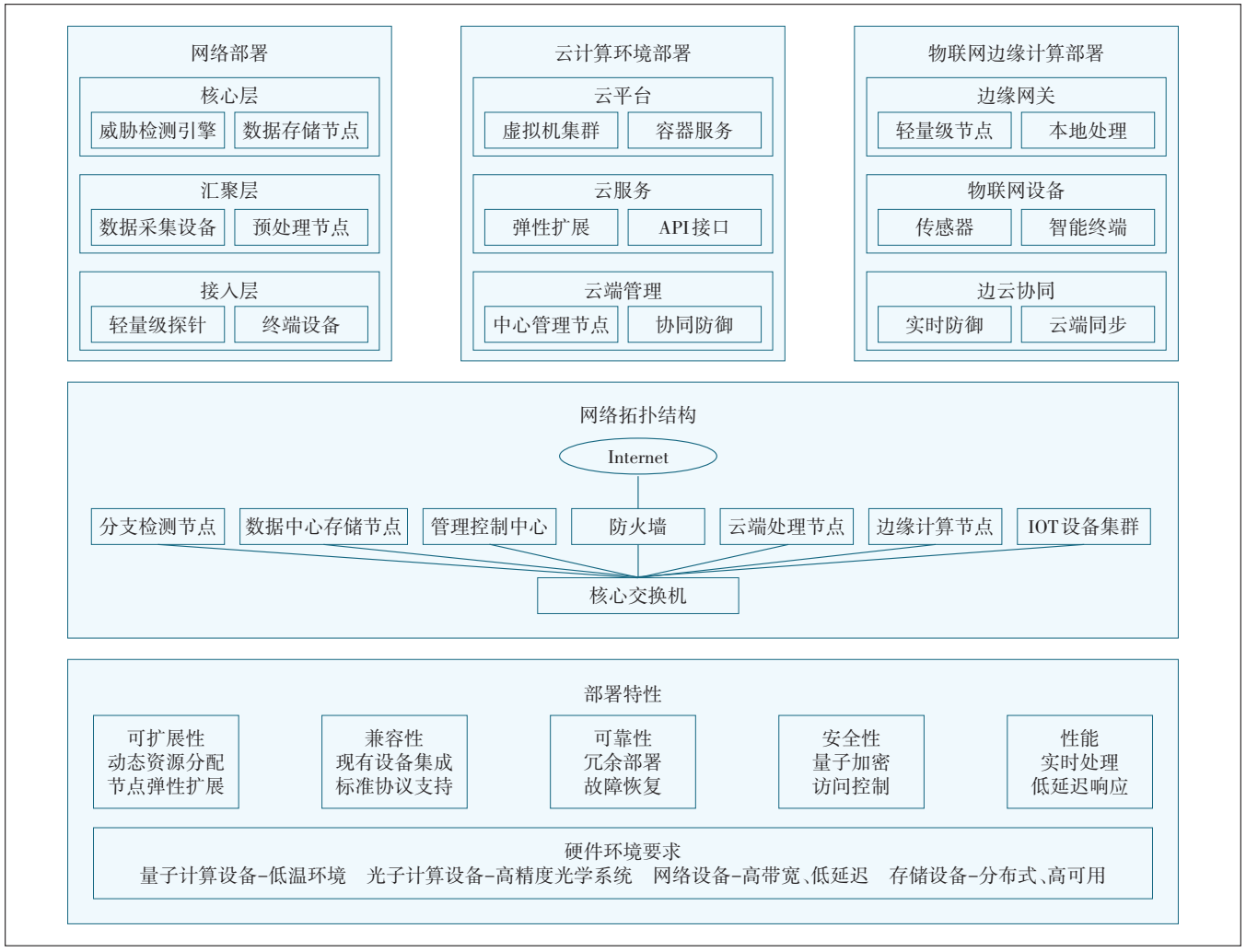

图4　部署方案

云环境下的威胁情报共享和联动响应机制。

物联网边缘计算部署针对大规模IoT设备场景进行了专门优化,边缘网关层部署轻量级节点和本地处理模块,轻量级节点运行精简版的量子神经网络模型,在边缘侧实现基础的威胁检测功能,本地处理模块对IoT设备产生的数据进行就近处理,减少数据传输延迟和带宽占用。物联网设备层包含传感器和智能终端2类设备,传感器负责采集环境数据、设备状态信息和安全相关的监控数据,智能终端包括各类IoT网关、智能摄像头、工业控制设备等具备一定计算能力的边缘设备。边云协同层通过实时防御和云端同步2个机制实现边缘与云端的有机结合,实时防御机制确保边缘节点能够独立处理常见的安全威胁,云端同步机制将复杂威胁和分析结果上传至云端进行深度处理和全局协调。

网络拓扑结构具体说明了系统各组成部分之间的连接关系和数据流向,其中,Internet是系统与外部网络的唯一接入方式,并通过防火墙进行安全过滤和访问控制。核心交换机是网络的汇聚中心,负责连接各个分布式节点并进行数据的路由和转发。分支检测节点实时监控数据流,并进行威胁识别。数据中心存储节点采用分布式存储架构,以确保数据的可靠性和可用性,并提供集中化的数据存储和管理服务。管理控制中心是系统的指挥调度中枢,用于策略配置、威胁响应决策和系统运维管理。云端处理节点基于云计算的强大算力处理复杂的威胁分析任务,边缘计算节点部署在网络边缘,就近提供威胁检测和快速响应能力。IoT设备集群采用统一的管理接口,以实现大规模物联网设备的安全防护。

在部署特性方面,系统具备5个核心特征。可扩

展性体现为系统通过动态资源分配和节点弹性扩展来实现，能够根据业务需求和威胁态势灵活调整系统规模。兼容性体现为系统通过现有设备集成和标准协议支持来实现，确保与传统网络安全设备的无缝对接。系统通过部署标准化数据转换接口，与传统的冯·诺依曼架构系统实现对接，支持 TCP/IP、SNMP 等通用协议，可将传统系统产生的结构化与非结构化数据实时转换为量子神经形态计算可处理的格式，确保在异构环境下数据交互的兼容性。可靠性体现为系统通过冗余部署和故障恢复机制来保证，确保系统在各种异常情况下持续运行。安全性体现为系统通过量子加密和访问控制，保护系统自身免受攻击。同时，系统通过实时处理和低延迟响应实现性能要求。硬件环境要求涵盖量子计算设备的低温环境控制需求、光子计算设备的高精度光学系统要求、网络设备的高带宽低延迟特性以及存储设备的分布式高可用架构，这些硬件要求共同构成了系统稳定运行的基础保障。

4 结束语

基于量子神经形态计算的实时主动防御系统的光子—量子融合架构、量子脉冲神经网络算法及量子纠缠态突触，能高度适配物联网边缘计算、多云协同等复杂场景，解决能效、延迟和动态适应性等方面的难题，为网络安全提供更高效的技术保障。随着量子技术与神经形态计算的快速发展，基于量子神经形态计算的实时主动防御系统通过融合硬件迭代、神经形态算法创新及强化学习等技术，将成为应对复杂网络威胁的核心技术保障[15]，并推动网络安全防御进入量子神经形态驱动的智能时代。

参考文献：

[1] STUIJT J, SIFALAKIS M, YOUSEFZADEH A, et al. μBrain: an event-driven and fully synthesizable architecture for spiking neural networks[J]. Frontiers in neuroscience, 2021, 15: 664208.

[2] YIK J, FRENKEL C, REDDI V J. Advancing neuromorphic computing algorithms and systems with NeuroBench [C]//NeurIPS 2024 Workshop Machine Learning with new Compute Paradigms. Vancouver, BC: MLNCP Poster, 2024: 1-8.

[3] YIK J, VAN DEN BERGHE K, DEN BLANKEN D, et al. The neurobench framework for benchmarking neuromorphic computing algorithms and systems[J]. Nature Communications, 2025, 16(1): 1545.

[4] BRAND D, PETRUCCIONE F. A quantum leaky integrate-and-fire spiking neuron and network[J]. npj Quantum Information, 2024, 10(1): 125.

[5] MARKOVIĆ D, GROLLIER J. Quantum neuromorphic computing [J]. Applied Physics Letters, 2020, 117(15): 150501.

[6] TAGHAVI M, FARNOOSH R. Quantum computing and neuromorphic computing for safe, reliable, and explainable multi-agent reinforcement learning: optimal control in autonomous robotics [J/OL]. Iran Journal of Computer Science, 2025 (2025-07-03) [2025-07-17]. https://doi.org/10.1007/s42044-025-00306-z.

[7] CHENG R, GOTETI U S, WALKER H, et al. Toward learning in neuromorphic circuits based on quantum phase slip junctions[J]. Frontiers in neuroscience, 2021, 15: 765883.

[8] ASHAR V, BANSAL S, V P. Quantum-enhanced spiking neural networks for closed-loop neuromodulation systems: a theoretically advanced framework[C]//2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). Chennai: IEEE, 2024: 1-9.

[9] ASSI D S, HUANG H, KARTHIKEYAN V, et al. Quantum topological neuristors for advanced neuromorphic intelligent systems[J]. Advanced Science, 2023, 10(24): 2300791.

[10] ALI B. Neuromorphic quantum adversarial learning (NQAL): a bio-inspired paradigm for DNS over HTTPS threat detection [EB/OL]. (2025-04-09) [2025-07-17]. https://www.researchsquare.com/article/rs-6414048/v1.

[11] GANDOTRA V, SINGHAL A, BEDI P. Threat-oriented security framework: a proactive approach in threat management[J]. Procedia Technology, 2012, 4: 487-494.

[12] MISHRA A K, DAS A, KANDASAMY N. Online performance monitoring of neuromorphic computing systems[C]//2023 IEEE European Test Symposium (ETS). Venezia: IEEE, 2023: 1-4.

[13] REN C, TANG Y P, GAO Y L, et al. QFEVAL: quantum federated ensembled variational adaptive learning for dynamic security assessment in cyber-physical systems[J]. IEEE Journal on Selected Areas in Communications, 2025, 43(9): 3200-3213.

[14] EL S L, KRISHNAN A, RAVICHANDRAN R, et al. Photonic and optoelectronic neuromorphic computing [J]. APL Photonics, 2022, 7(5): 051101.

[15] SINGH S, KUMAR D. Enhancing cyber security using quantum computing and artificial intelligence: a review[J]. International Journal of Advanced Research in Science Communication and Technology, 2024, 4(3): 2581-9429.

作者简介：
王智明，毕业于北京邮电大学，教授级高级工程师，博士，主要从事网络安全、黑灰产治理、物联网安全研发工作；丁莹，毕业于浙江大学，高级工程师，硕士，杭州市科技专家，主要从事AI安全、网络安全、车联网安全、物联网安全研究工作；于城，毕业于北京邮电大学，高级工程师，硕士，主要从事网络安全、黑灰产治理、物联网安全研发及相关管理工作。