基于AI的电子通信工程信息安全防护技术

曹 琦
江西诚科建设咨询监理有限公司 江西 南昌 330025

摘 要：随着5G普及，AI赋能通信安全新篇。本文聚焦基于AI的电子通信工程信息安全防护技术。首先概述该技术，涵盖数据采集层、模型训练层与决策执行层。接着阐述其关键技术，包括多模态威胁感知、分布式智能决策等六项技术。最后探讨发展趋势，如量子计算与AI融合、边缘智能与5G/6G协同等。该技术借助AI提升电子通信工程信息安全防护能力，有效应对复杂安全威胁，为行业发展提供有力支撑，保障通信系统的稳定与安全运行。

关键词：AI；电子通信工程；信息安全防护技术；关键技术；发展趋势

引言：在电子通信工程迅猛发展的当下，信息安全问题日益凸显。网络攻击手段不断翻新，传统安全防护技术已难以满足需求。AI凭借强大的数据处理与分析能力，为信息安全防护带来新契机。基于AI的电子通信工程信息安全防护技术应运而生，它通过智能算法和模型，实现威胁的精准感知、快速决策与有效应对。研究这一技术，不仅能提升电子通信工程的安全防护水平，还能推动整个行业向智能化、安全化方向发展，具有重要的现实意义和战略价值。

1 AI 电子通信工程信息安全防护技术的概述

1.1 数据采集层

数据采集层是基于AI的电子通信工程信息安全防护技术的基石。它负责从电子通信工程的各类设备和系统中广泛收集信息，涵盖网络流量数据、设备运行日志、用户操作记录等。通过多种传感器、监控工具和数据接口，实现多源数据的实时、全面采集。这些原始数据是后续分析的素材，其完整性和准确性直接影响整个防护体系的效果。同时，数据采集层还需对采集到的数据进行初步筛选和预处理，去除噪声和无效信息，为模型训练层提供高质量的数据输入，确保AI模型能够基于可靠数据进行学习和分析。

1.2 模型训练层

模型训练层是该技术的核心处理环节。它接收来自数据采集层的预处理数据，运用机器学习、深度学习等AI算法构建安全模型。通过对大量正常和异常数据样本的学习，模型能够识别出电子通信工程中的潜在安全威胁模式。在训练过程中，不断调整模型参数，优化其性能，提高对各类攻击的检测准确率和召回率。模型训练层的质量决定了整个防护系统对安全威胁的感知和判断能力，是保障信息安全的关键所在。

1.3 决策执行层

决策执行层是基于AI的电子通信工程信息安全防护技术的最终行动环节。它依据模型训练层输出的分析结果，做出相应的安全决策并执行。当检测到安全威胁时，决策执行层会迅速判断威胁的类型、严重程度和影响范围，然后选择合适的应对策略，如阻断网络连接、隔离受感染设备、启动备份系统等。同时，它还能将决策结果反馈给相关管理人员，以便及时了解安全状况并采取进一步措施。决策执行层的高效性和准确性对于及时遏制安全威胁、减少损失至关重要，是保障电子通信工程信息安全运行的最后一道防线[1]。

2 AI 在电子通信工程安全防护的关键技术

2.1 多模态威胁感知技术

在电子通信工程安全防护领域，多模态威胁感知技术发挥着至关重要的作用。（1）该技术能够整合多种数据来源。电子通信工程中，安全威胁往往隐藏在复杂多样的数据里，单一数据源难以全面捕捉。多模态威胁感知技术可综合网络流量数据、设备日志、用户行为信息以及物理环境数据等。例如，通过分析网络流量特征能发现异常连接，结合设备日志可定位故障或受攻击的设备，参考用户行为信息能识别内部人员的违规操作，利用物理环境数据能感知外界对通信设施的破坏风险，多源数据融合提升了威胁发现的全面性。（2）它具备强大的模式识别能力。借助先进的AI算法，如深度学习中的卷积神经网络、循环神经网络等，对多模态数据进行深度挖掘。能自动学习正常通信模式和各类威胁模式的特征，精准识别出新型、复杂的攻击手段，像零日漏洞攻击、高级持续性威胁（APT）等，有效弥补传统基于规则检测的不足。（3）多模态威胁感知技术可实现实时监测与预警。能够实时处理海量数据，快速分析并判断是否存在安全威胁。一旦检测到潜在风险，立即发出预警，为安全人员争取宝贵的应对时间，及时采取措施阻止攻

击的进一步扩散，保障电子通信工程的安全稳定运行。

2.2 分布式智能决策技术

在电子通信工程安全防护中，分布式智能决策技术是保障系统安全高效运行的关键支撑。（1）它实现了决策的分散化与协同化。电子通信工程网络规模庞大、结构复杂，单一节点的决策能力有限。分布式智能决策技术将决策任务分配到多个网络节点，每个节点依据自身采集的局部信息和预设规则进行初步判断。同时，各节点通过高效通信机制共享信息、协同工作，综合全局情况做出更准确、全面的决策。（2）该技术具备快速响应能力。电子通信工程中的安全威胁往往瞬息万变，需要迅速做出反应。分布式智能决策技术通过并行处理和就近决策，减少了决策延迟。各节点能在本地快速处理紧急安全事件，无需将所有信息传输到中心节点等待指令，大大提高了对安全威胁的应对速度，有效降低损失。（3）它增强了系统的可靠性和容错性。即使部分节点出现故障或受到攻击，其他正常节点仍能继续工作，保证决策过程的连续性。这种分布式架构使得系统不会因单点故障而瘫痪，提高了电子通信工程安全防护的稳定性和韧性。

2.3 隐私增强型协同防御技术

在电子通信工程安全防护领域，隐私增强型协同防御技术正发挥着日益关键的作用。（1）它有效解决了协同防御中的隐私泄露难题。电子通信工程涉及众多参与方，如不同企业、机构，在协同防御过程中，各方需共享安全信息以共同应对威胁。然而，直接共享可能暴露敏感数据，如用户隐私信息、企业核心业务数据等。隐私增强型协同防御技术通过加密、匿名化等手段，对共享信息进行预处理，使各方在无法获取对方原始敏感信息的情况下，仍能基于处理后的数据进行协同分析和决策，保障了数据隐私安全。（2）该技术提升了协同防御的效率与效果。借助先进的隐私计算技术，如安全多方计算、联邦学习等，各参与方可以在不泄露隐私的前提下，联合训练安全模型、分析威胁模式。不同方的数据和知识得以融合，从而更全面、准确地识别和应对各类安全威胁，尤其是那些跨区域、跨系统的复杂攻击，增强了整体防御能力。（3）它促进了电子通信工程领域的广泛合作。由于隐私得到保障，各参与方更愿意积极参与协同防御，打破了数据孤岛，形成了更强大的安全防护合力，共同营造安全可靠的电子通信环境，推动整个行业健康稳定发展。

2.4 自进化安全验证技术

在电子通信工程安全防护体系里，自进化安全验证技术是保障系统长期安全稳定运行的关键创新。（1）它具备动态适应能力。电子通信工程所处环境复杂多变，新的安全威胁和攻击手段不断涌现。传统安全验证技术往往基于固定的规则和模式，难以应对这些动态变化。而自进化安全验证技术能够实时感知环境变化和新的攻击特征，通过机器学习、深度学习等算法，自动调整验证策略和参数，如同拥有“自我学习”的大脑，始终保持对最新安全威胁的有效识别和验证，确保安全防护的时效性。（2）该技术提高了验证的准确性和全面性。它可以从海量的安全数据中不断学习和总结经验，挖掘潜在的安全风险模式。不仅能对已知的安全问题进行精准验证，还能预测和发现未知的安全漏洞，大大扩展了安全验证的范围和深度，为电子通信工程构建起更严密的安全防线。（3）自进化安全验证技术降低了人工干预成本。传统安全验证需要大量专业人员进行规则设定、更新和维护，而自进化技术实现了自动化和智能化，减少了人力投入，提高了安全验证的效率，使电子通信工程能够以更低的成本获得更高水平的安全保障。

2.5 动态策略生成技术

在电子通信工程安全防护中，动态策略生成技术是应对复杂多变安全威胁的核心手段。（1）它能实时感知安全态势。电子通信工程面临的安全威胁瞬息万变，网络攻击手段不断升级。动态策略生成技术借助先进的监测工具和算法，实时收集网络流量、设备状态、用户行为等多维度数据，精准分析当前安全状况。（2）该技术可快速生成针对性策略。基于实时感知的安全态势，动态策略生成技术能运用智能算法，结合预设的安全规则和历史经验，快速生成与之匹配的安全防护策略。这些策略涵盖了访问控制、流量过滤、加密处理等多个方面，能够精准应对不同类型的攻击，有效阻止安全威胁的扩散，将损失降到最低。（3）它具备策略的动态调整能力。随着安全态势的持续变化，已生成的策略可能不再适用。动态策略生成技术能够实时评估策略的执行效果，根据新的安全信息自动调整策略参数或生成全新的策略，确保安全防护始终与当前的安全威胁相匹配，为电子通信工程提供持续、有效的安全保障。

2.6 跨模态关联分析技术

在电子通信工程安全防护领域，跨模态关联分析技术正成为应对复杂安全挑战的关键利器。（1）它打破了数据模态的壁垒。电子通信工程中存在着多种不同模态的数据，如文本形式的日志记录、图像形态的网络拓扑图、数值类型的流量统计数据等。这些数据各自蕴含着关于安全状况的重要信息，但传统分析方法往往局限于

单一模态。跨模态关联分析技术能够将这些分散在不同模态的数据进行有机整合，挖掘出它们之间隐藏的关联关系，从而更全面、深入地理解系统的安全态势。（2）该技术提升了安全威胁检测的准确性。通过跨模态关联分析，可以从多个角度对安全事件进行综合判断。例如，当网络流量出现异常时，结合设备日志中的操作记录和系统运行状态图像，能够更准确地判断是正常业务波动还是恶意攻击行为，有效减少误判和漏判，提高安全防护的可靠性。（3）跨模态关联分析技术有助于预测潜在安全风险。通过对历史跨模态数据的深度分析，能够发现安全威胁发生的规律和趋势，提前预测可能出现的攻击类型和攻击路径，为安全人员制定预防策略提供有力依据，实现从被动防御到主动预防的转变，保障电子通信工程的安全稳定运行[2]。

3 AI 电子通信工程信息安全防护技术的发展趋势

3.1 量子计算与AI的融合

量子计算与AI的融合将为电子通信工程信息安全防护带来革命性突破。量子计算强大的并行计算能力，可大幅提升AI算法处理海量安全数据的效率，加速对复杂安全威胁模式的学习与识别。AI则能借助量子计算的特性，开发出更精准的安全模型，实现对高级持续性威胁、量子密钥分发攻击等新型威胁的有效防范。同时，二者融合有助于优化加密算法，提升通信数据的安全性，构建起更坚固、高效的信息安全防护体系，推动电子通信工程安全防护迈向新高度。

3.2 边缘智能与5G/6G的协同

边缘智能与5G/6G的协同是电子通信工程信息安全防护的重要发展方向。5G/6G网络的高速率、低时延特性，为边缘智能设备间的实时数据传输提供了保障。边缘智能设备可在本地进行初步的安全数据处理与分析，快速响应局部安全事件，减少数据传输到中心服务器的延迟。同时，借助5G/6G网络，边缘智能设备能与云端安全中心高效协同，共享安全策略与威胁情报。这种协同模式能提升安全防护的实时性和精准性，有效应对电子通信工程中快速多变的安全威胁。

3.3 人机协同的安全运营

人机协同的安全运营将成为电子通信工程信息安全防护的主流模式。AI凭借强大的数据处理和分析能力，可快速检测安全威胁、分析攻击路径，并提供初步的应对建议。而安全人员则能运用专业知识和经验，对AI的输出进行审核和决策，处理复杂、模糊的安全情况。人机协同能充分发挥双方的优势，AI提高安全运营的效率和准确性，安全人员保障决策的合理性和灵活性。通过紧密配合，可实现对电子通信工程安全威胁的及时、有效应对，提升整体安全防护水平。

3.4 自主可控的技术生态

构建自主可控的技术生态是电子通信工程信息安全防护的必然要求。在全球化背景下，依赖外部技术和产品存在安全风险。自主可控的技术生态能够确保从芯片、操作系统到安全软件等关键环节都掌握在自己手中，避免受制于人。通过自主研发和创新，可针对电子通信工程的特殊需求，开发出更贴合实际、安全可靠的信息安全防护技术和产品。同时，自主可控的技术生态有助于培养本土技术人才，提升产业竞争力，为电子通信工程的信息安全提供坚实保障[3]。

结束语

基于AI的电子通信工程信息安全防护技术，正以磅礴之势重塑安全格局。它凭借多模态威胁感知、分布式智能决策等前沿技术，构建起全方位、多层次的安全防线，有效抵御日益复杂多变的网络攻击。量子计算与AI的融合、边缘智能和5G/6G的协同等发展趋势，更为其注入源源不断的创新动力。展望未来，我们应持续加大研发投入，推动技术自主可控，深化人机协同。

参考文献

[1]张建岳,王增刚.智能化通信中的电子信息工程技术应用[J].信息与电脑,2025,37(12):96-98.

[2]肖兰.电子通信工程信息安全防护探讨[J].中国信息界,2024,12(04):220-222.

[3]杨宣有.基于AI的电子通信工程信息安全防护技术[J].通信电源技术,2025,42(2):143-145.