 DOI: https://doi.org/10.12349/iser.v5i6.2949

Research on the Automation and Intelligence of Computer Network Security Maintenance

Hua Guo

Shandong Zhaojin Group Co., Ltd., Zhaoyuan, Shandong, 265400, China

Abstract

With the rapid development of information technology, computer network has become an important part of our life and work. However, the network security problem has become the main resistance to affect the popularization of social network applications. In this regard, this study mainly explores how to improve the security of computer network through automation and intelligence. In the process of research, we use machine learning technologies such as deep learning to automatically detect network threats, and also introduce adaptive algorithms and artificial intelligence to realize the automatic protection of network security. The results show that the automation and intelligent maintenance mode of the computer network security can not only find the network threats in real time, but also learn and adapt to themselves, improve the accuracy and response speed of intrusion detection, and effectively improve the security of the computer network. The conclusion of this study has practical significance for improving the automation and intelligent protection ability of the network.

Keywords

computer network security; automatic maintenance; intelligent protection; intrusion detection; deep learning

计算机网络安全维护的自动化与智能化研究

郭华

山东招金集团有限公司，中国 · 山东 招远 265400

摘　要

随着信息技术的快速发展，计算机网络已成为我们生活和工作的重要组成部分。然而，网络安全问题却成为影响社会网络应用普及的主要阻力。对此，本研究主要探索如何通过自动化与智能化的方式来提升计算机网络的安全性。在研究过程中，我们利用深度学习等机器学习技术，自动检测网络威胁，同时也引入了自适应算法和人工智能来实现网络安全的自动防护。结果显示，该计算机网络安全的自动化与智能化维护方式，不仅可以实时发现网络威胁，更可以自我学习和适应，提高了入侵检测的准确率和响应速度，有效地提升了计算机网络的安全性。本研究的结论对于提升网络的自动化和智能化防护能力有着实际意义。

关键词

计算机网络安全；自动化维护；智能化防护；入侵检测；深度学习

1 引言

随着网络在生活中的重要性日益提高，中国网民数量已经达到了 7.78 亿。然而，网络安全问题也越来越严重，如电脑病毒、黑客攻击、个人数据泄露等。为了解决这些问题，我们需要探究一种自动化和智能化的网络保护方式，包括电脑病毒防护、网络漏洞检查、网络入侵检测等。这需要利用深度学习等技术，结合自身适应算法和人工智能，建立一个能自主学习和适应的系统，提高网络入侵检测的速度和准确性，总的来说提高网络的安全性。我们的目标是，通过这项研究可以找到适合中国的网络安全维护策略，并为全球的网络安全防护工作提供理论支持和实践参考，为网络环境的安全稳定作出贡献。

【作者简介】郭华（1973–），男，中国山东招远人，本科，工程师，从事电子信息工程技术研究。

2 计算机网络安全现状及挑战

2.1 计算机网络安全的重要性

计算机网络安全的重要性在当今信息化社会中愈发突出 [1]。随着数字技术的迅猛发展，计算机网络已经深度融入了人们的日常生活和各行各业的运作过程中。无论是个人通信、财务交易，还是企业的业务管理、政府的数据存储，都依赖于计算机网络的高效、安全运行。伴随着网络应用的普及，网络攻击和安全漏洞也呈现出复杂多样的态势，给个人隐私、企业机密以及国家安全构成了严重威胁。

在数字经济时代，信息成为一种重要的资源，而计算机网络作为信息传输和处理的载体，其安全性直接关系到信

息的保密性、完整性和可用性。由于网络环境的开放性和互联性，网络中的任何一个节点受到攻击，都可能导致整个网络的瘫痪。对于个人用户而言，网络安全问题可能会导致个人隐私信息泄露、财务损失等后果。对于企业和组织来说，网络安全漏洞可能引发商业机密泄露、业务中断，甚至是无形的品牌损失和法律责任。而从国家安全的层面看，网络安全威胁对关键基础设施、军事防御、政府数据等构成了潜在的巨大风险。确保计算机网络的安全性已经成为维护国家安全和社会稳定的重要一环。

当前的网络攻击手段日益多样化和复杂化，包括病毒、蠕虫、间谍软件、勒索软件、DDoS 攻击、网络钓鱼以及高级持续威胁（APT）等 [2]。这些攻击手段不仅具有高度隐蔽性，还呈现出定向化、智能化的特点，给传统的安全防护措施带来了巨大挑战。传统的防火墙、杀毒软件、入侵检测系统等手段已经难以应对日益猖獗和复杂的网络威胁，迫切需要更加先进和智能的网络安全防护技术。

在此背景下，自动化与智能化的网络安全技术被认为是应对日益严峻的网络安全挑战的有效途径。通过引入人工智能、机器学习、深度学习等技术，能够实现对网络威胁的实时识别和预测，并对安全事件进行自动化响应和处理。这些智能化技术不仅可以提高威胁检测的准确率，减少误报率，还能够自适应学习和优化，提升应对新型攻击手段的能力。

计算机网络安全的重要性不仅体现在保护信息资源的角度，还涉及网络的高效运行与社会的正常运作 [3]。随着物联网、云计算、5G 等新兴技术的进一步发展，网络安全问题将更加复杂和多样，严峻形势亟需从技术、政策、管理等多个层面加以综合应对。只有通过不断提升网络安全防护技术，才能构筑起信息时代的坚实屏障，保障数字经济和社会的健康发展。

2.2 当前网络安全挑战分析

当前，计算机网络安全面临诸多挑战，这些挑战严重影响了信息技术的发展和应用的普及。网络攻击手段日趋复杂，网络犯罪分子不断利用新技术和新手段进行攻击。例如，复杂的多阶段攻击、分布式拒绝服务（DDoS）攻击、零日漏洞攻击等，给传统的安全防护手段带来了巨大压力。攻击者利用社会工程、恶意软件和高级持续性威胁（APT）等方式隐藏并传播恶意代码，使得安全防护更加困难。

随着物联网（IoT）设备的大规模应用，网络边界逐渐模糊化，大量的物联网设备缺乏足够的安全防护措施，成为攻击者的目标。这些设备通常计算能力有限，易被攻陷，没有足够的资源来应对复杂的安全威胁。云计算和虚拟化技术的广泛应用，使得数据和应用系统从传统的本地环境转移到云端，导致了数据的集中存储和传输过程中安全风险显著增加。

信息化和全球化带来的数据量爆炸式增长，使得数据泄露和隐私保护成为重大挑战。大量敏感信息，如个人隐私、财务数据和企业机密，如果没有得到良好保护，可能被恶意窃取或滥用，导致严重的经济和社会影响。

另外，网络安全人才的匮乏也是一大难题。高级网络安全专家稀缺，许多组织和企业缺乏足够的专业人员来应对复杂的网络安全威胁。网络安全技术的发展速度远超人才培养的进度，使得网络安全防护面临巨大的人员和技能缺口。

面对现今复杂的网络环境，传统的防护措施已经难以应对，迫切需要通过自动化和智能化技术来提升计算机网络的安全性。

2.3 自动化与智能化在网络安全中的应用需求

计算机网络安全威胁的不断演化和复杂化，使得传统的人工安全维护方法难以完全应对。自动化与智能化技术的引入，能够提高网络安全系统的实时响应能力和准确性。深度学习技术能够自动检测和识别潜在威胁，自适应算法则可以根据不同的网络环境动态调整防护措施。这些技术的应用，不仅提升了威胁检测的效率，还增强了整个计算机网络的自我保护和学习能力，显著降低了网络攻击的风险。自动化与智能化成为网络安全领域亟须发展的方向。

3 自动化与智能化网络安全技术

3.1 病毒防护的自动化与智能化方法研究

随着信息技术的发展与普及，计算机病毒的数量和种类也在迅速增加，传统的病毒防护手段已难以应对复杂多变的威胁。通过自动化与智能化技术来提升病毒防护的效果成为当前研究的重点。

自动化病毒防护技术利用预设的算法规则和任务流程，实现病毒的自动检测与处理。此类技术可快速扫描大量文件和数据，识别已知病毒签名，在感染的初期阶段进行隔离与清除操作。通过定时更新病毒库，自动化防护系统能够始终保持最新的病毒特征库，在检测效率和准确性方面表现出色。

智能化病毒防护则更多地依靠机器学习和深度学习技术，能够分析和识别未知病毒。通过对大规模恶意软件样本进行训练，智能化防护系统可以学习和提取病毒特征，并建立行为模型。该模型能够识别异常行为及其潜在威胁，而不依赖于病毒签名的更新，这使得智能化防护在应对零日攻击等未知威胁时更加有效。

深度学习技术在智能化病毒防护中的应用，主要体现在特征提取和分类上。通过卷积神经网络（CNN）等先进算法，对数据进行多层次的特征提取，智能化防护系统能够准确捕捉病毒的隐蔽特征。循环神经网络（RNN）等技术则有助于监测和预测病毒行为，形成动态的防护机制。

自适应算法在智能化病毒防护中也发挥着重要作用。这些算法不仅能够根据检测到的威胁实时调整防护策略，还可以在运行过程中不断优化和学习，大幅提升了病毒防护的

反应速度和精准性。利用人工智能技术，自适应防护系统可以在检测出新型病毒后，迅速应用学到的知识进行自动防护，从而避免病毒的进一步传播和破坏。

面向未来的病毒防护技术，自动化和智能化手段的结合是一个重要趋势。自动化技术提供了高效的检测与处理能力，并辅以智能化技术实现未知威胁的识别与防护，这一组合在提升计算机网络整体安全性也有效减轻了人工干预的负担。随着技术的不断发展与完善，病毒防护的自动化与智能化将为网络安全的建设与维护带来新的契机。

3.2 漏洞扫描的自动化与智能化方法研究

漏洞扫描是维护计算机网络安全的重要环节，其主要目的是发现系统和应用软件中的安全漏洞，防止潜在的攻击者利用这些漏洞进行非法操作。传统的漏洞扫描主要依赖于人工操作，存在效率低、误报率高以及及时性不足等问题。在信息技术飞速发展的今天，传统方法已无法满足现代网络环境中对安全性的高要求。将自动化和智能化技术引入漏洞扫描领域具有重要意义。

自动化漏洞扫描通过预先设定的扫描规则和脚本，可以在较短时间内完成广域的系统检查，大幅提升了漏洞检测的效率。在自动化技术的支持下，日常的漏洞扫描工作得以简化，大幅减少了人工干预的需求，减轻了运维人员的负担。智能化漏洞扫描则借助机器学习和深度学习等先进的信息技术，进一步提升了漏洞检测的准确性和及时性。

运用机器学习算法，可以分析大量的网络行为和历史数据，自动更新扫描规则和策略，提高了对新型漏洞的识别能力。深度学习技术则通过建立复杂的神经网络模型，对海量的网络数据进行自动分析和模式识别，显著增强了对未知威胁的察觉能力。应用自适应算法，可以使漏洞扫描工具根据实际网络状况进行调整和优化，保证扫描结果的有效性和针对性。

智能化技术除了能提高漏洞扫描的准确性，还能实现对扫描结果的高级分析与处理。通过引入自然语言处理技术，能够从大量扫描报告中提取关键威胁信息，自动生成简明的安全评估报告，为网络安全防护决策提供有力支持。在实施过程中，需要结合大数据分析技术，对历史漏洞数据进行深入挖掘和分析，为构建更加智能化的漏洞扫描系统提供基础数据支持。

总体来看，自动化与智能化技术在漏洞扫描中的应用，不仅提高了漏洞检测的效率和准确性，也增强了对未知威胁的防范能力，为保障计算机网络的安全性提供了强大技术支持。通过这些技术的有机结合，可以实现对复杂网络环境的全面高效防护，切实提升网络安全维护的自动化与智能化水平。

3.3 网络入侵检测的自动化与智能化方法研究

在网络入侵检测中，自动化与智能化技术通过深度学习、神经网络等方法，实现了对异常流量和行为的实时监测。基于大数据分析，系统能够快速识别潜在威胁并自动响应。自适应算法使得系统能够动态调整检测策略，提高检测的准确率和速度。机器学习模型通过不断迭代和自我优化，增强了检测系统的灵活性和鲁棒性，降低了误报率和漏报率，有效提升了计算机网络的整体安全性。

4 结语

本研究对计算机网络安全的自动化与智能化维护机制进行了深入探讨，利用深度学习等机器学习技术自动检测网络威胁，引入自适应算法和人工智能实现网络安全的自动防护。通过这种方式，我们可以实时发现网络威胁，并且能够自我学习和适应，从而提高了网络入侵检测的准确率和响应速度，有效提升了计算机网络的安全性。然而，虽然本研究取得了一些初步的成果，但网络安全仍然面临众多挑战。例如，对一些先进的、隐蔽的攻击手段，现有的检测和防护技术可能还无法完全应对。此外，深度学习和人工智能技术的应用仍然需要更大的计算和存储资源，这也是需要进一步解决的问题。未来的研究，我们打算进一步优化自动化与智能化的网络安全防护技术，降低其对计算和存储资源的需求，使之更易于在各种环境下部署。同时，我们也将研究更先进的、针对新的网络攻击类型的防护方案，以应对网络安全的快速发展。本研究的成果，不仅对于理论界有启示意义，对于当前网络安全威胁频繁的现实环境也具有一定的指导和参考作用。希望能为网络安全防护技术的发展提供一定的研究基础与实践参考。

参考文献

[1] 汪升华.智能化计算机网络安全技术的应用[J].电子技术与软件工程,2021(19).

[2] 谭江汇,周亮,罗小刚.智能化计算机网络安全技术的应用研究[J].中国新通信,2023,25(16).

[3] 张海英.医院计算机网络安全维护[J].电子乐园,2019(16).