

人工智能在计算机网络技术中的应用分析

南海信息技术学校：潘宇

注：此论文曾于 2018 年 8 月发表在《电脑迷》第 10 期 CN50-1163/TP

摘要：计算机网络技术与人们生产生活联系密切，人工智能的应用是计算机网络技术的重要革命，能够显著提高计算机网络技术的质量与效率。本文通过对人工智能在计算机网络技术中的应用分析，以期增强人们对人工智能技术的认识，提高人工智能技术的应用水平，为实现人工智能技术的全面应用创造研究基础与实践条件。

关键词：人工智能；计算机网络技术；移动代理；应用

一、人工智能概述

新型技术人工智能于 20 世纪 60 年代第一次被美国科学家提出，纵观人工智能的发展历史，我们可以发现人工智能与计算机网络技术之间有很大联系，人工智能技术多应用到计算机网络技术中，二者相辅相成，相互影响。人工智能作为计算机网络技术的一个重要分支，具有智能性与应激性，能够通过运用计算机学、语言学、心理学等多个学科知识，对人的行为进行模仿，使得机器具有人的思维，并对人们的生产生活产生有利影响，帮助人们解决实际问题。经过 50 余年的发展，人工智能技术已逐渐发展成熟，并不断应用到人们生活中。

二、人工智能在计算机网络技术中应用的必要性

现今，计算机网络技术在人们工作与生活中的应用范围越发广泛，人们的工作与生活与计算机网络技术紧密的联系在一起。不可置否，计算机网络技术给人们的生活带来了极大的便利，但是随着计算机网络技术的不断应用，其固有弊端也随着显现。

随着信息化的发展，网络犯罪也随之产生，一些不法分子借助计算机网络技术作为犯罪工具，通过网络篡改信息，利用黑客技术攻击一些网站等，给人们带来巨大的损失。为了源头上遏制这类犯罪行为的发生，我们就需要将人工智能技术引入到现代计算机网络技术中去，利用人工智能建立互联网智能管理系统，利

用其庞大的信息收集与数据处理能力，对于计算机网络上出现的安全问题，能够第一时间反应过来，并做到及时处理，从源头上防止网络犯罪的发生，做到对计算机网络的有效监管，为人们的工作与生活提供良好的网络环境。

三. 人工智能在计算机网络技术中的应用分析

随着人们对计算机网络技术的不断应用，人们开始不断的关注计算机网络安全问题，为了保障计算机网络安全，人们开始利用人工智能技术进行网络的安全管理，现今，经过研发人员的不断努力，人工智能技术在入侵检测，智能反垃圾邮件和智能防火墙方面都发挥着重要的作用。

当前我们已经建立了完善智能入侵检测系统，该系统通过对计算机内已有的信息进行全面检测，检测信息是否属于入侵信息，会对电脑造成危害。如果存在入侵信息，入侵检测系统就会发出警告，并且制定出有效地解决方案。当前该技术多用于会计师事务所与图书馆的信息管理中。

通过上面的介绍我们对入侵检测系统已有了初步的了解，下面我们将通过表 1 对分布式入侵检测系统作出形式化的描述，以便于加深我们对它的认识。

表 1 入侵检测形式化描述

检测环境	集合 U 指的是网络系统和主机中的所有模式 $S(\text{self 集合}) \cup N(\text{non-self 集合}) = U \cup N$
问题描述	通过 $\forall s \in U$ ，对 $s \in S?$ or $s \in N$ 进行判断
系统描述	入侵检测系统 $D = (f, M)$ ， $M \in U$ 是 D 的检测规则集。 f 是判定函数 $f: U \times U \rightarrow \{ \text{normal}, \text{anomalous} \}$
误报问题描述	1 是弃真错误：2 是存伪错误。 U_{test} 是试验集合， $U_{\text{test}} \subseteq U$ 。当 $N_{\text{test}} = N \cap U_{\text{test}}$ ， $S_{\text{test}} = S \cap U_{\text{test}}$ ，则 $S \cup N = N$ 。 $S \cap N = \phi$ 时 $N_{\text{test}} \cap S_{\text{test}} = U_{\text{test}}$ 并且 $N_{\text{test}} \cap S_{\text{test}} = \phi$ 。如果 $S \in N_{\text{test}}$ ，并且 $f(M, s) = \text{anomalous}$ ，则为 1。如果 $N \in N_{\text{test}}$ ，并且 $f(M, s) = \text{normal}$ ，则为 2。
检测事件	当 $f(M, s) = \text{anomalous}$ ，即发生检测事件
全局判断函数	当 $\forall i \in L$ ， D_i 中的判定函数 $f_i(M_i, s) = \{ \text{anomalous, if } s \cup j \in L_j M, \text{normal, otherwise} \}$

全局误报描述	<p>1 全局弃真错误, 则 $\forall s \in S, \exists l \in L, s. t. s \in U l \wedge f l(M, s) = \text{anomalous}$</p> <p>2 全局存伪错误, 则 $\forall s \in N, \exists l \in L, s. t. s \in U l \wedge f l(M, s) = \text{normal}$</p>
--------	--

移动代理是是人工智能的重要分支之一，是实现分布式系统的有效手段，其主要功能主要体现在以下方面：

一是在网络入侵检测方面。利用各种手段方式，对异常网络流量等数据进行收集、筛选、处理，自动生成安全报告提供给用户，如 DDos 检测、僵尸网络检测。

二是在预测性恶意软件防御方面。通过使用机器学习和统计模型，寻找恶意软件家族特征，预测进化方向，提前进行防御。

三是在网络安全动态感知方面。利用数据融合、数据挖掘、智能分析和可视化等技术，直观显示、预测网络安全态势，为网络安全预警防护提供保障，可在不断的自学习过程中提高系统的防御水平。例如，如果遇到突发大流量的情况，则人工智能系统可以推测网络中存在分布式拒绝服务（DDoS）攻击，并立即分析软件包特性，协调探针协作任务，将具有同类特征的所有软件包丢弃，从而最大限度地避免对其他网络业务造成损失。

下面我们将对基于移动代理的入侵检测系统作出测试。

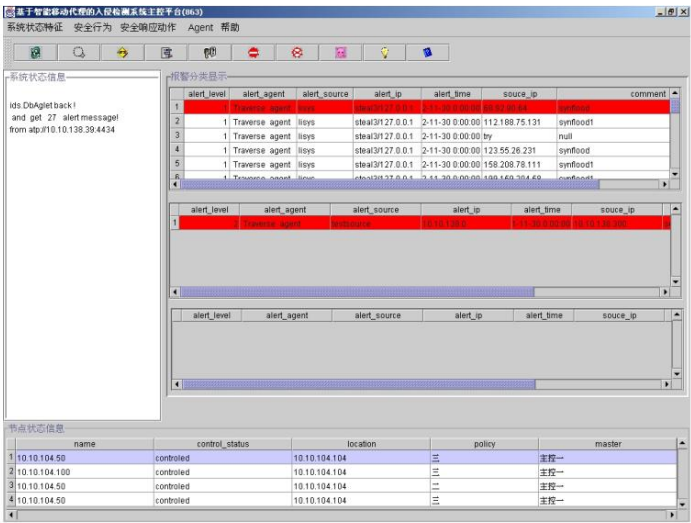


图 1 分布式入侵检测系统的控制台

图一所示的是入侵检测系统的系统控制台界面，图一左上角的系统状态信息

包括报警和各种的移动代理信息。右上角条框中指的是三级报警信息。最下面的区域显示的是传感器的状态信息和各个移动代理的派发情况。

下面我们针对移动代理（分布式入侵检测系统的关键技术之一）作出测试，以证明移动代理可成为分布式入侵检测系统的基础平台。

首先，我们对移动代理作出守护进程测试。我们在网络链接断断续续的情况下，使用 aglet 开发的移动代理守护进程，通过对移动代理进行编程设置，最终证实其能够实现移动代理安全的接受和传送。在测试中，我们发现，移动代理的主控制节点能够实现移动代理技术全面地控制，而分控制节点只能实现部分功能。最后我们对移动代理的节点主动报警功能作出测试，经过测试发现在遇到突发情况是，移动代理的多个节点能够同时向主控制台发出报警。

经过测试我们移动代理平台是入侵检测系统重要的基础平台，在入侵检测系统中发挥着重要的作用。

四. 总结

通过上面的分析我们发现，在当今这个信息化大环境下，人工智能技术以其特有优势受到人们的关注，人们将人工智能技术越来越多的应用到计算机网络技术中，该技术的应用，不仅能够提高计算机工作效率，还可以保证计算机网络管理系统的安全与稳定。故希望我国的研究人员能够更加深入的对人工智能技术进行研究，让人工智能技术更好的应用到计算机网络技术中去，为人们的工作与生活带来更多的便利。

参考文献

- [1] 颜红限. 人工智能在计算机网络技术中的运用分析[J], 无限互联科技, 2017, 20:43-44.
- [2] 孙晓霞. 人工智能在计算机网络技术中的应用探究[J], 网络安全技术与应用, 2016, 03:99-101.
- [3] 吴振宇. 试析人工智能在计算机网络技术中的运用问题[J], 网络安全技术与应用, 2015, 01: 70-74.
- [4] 马越. 探讨人工智能在计算机网络技术中的应用[J], 计算机光盘软件与应用, 2014, 22: 43-44.