工业物联网领域的安全研究

万彬彬，崔登祺，巩　潇*，赵郑斌，李梦玮

（中国软件评测中心（工业和信息化部软件与集成电路促进中心），北京 100084）

摘要：物联网系统已广泛应用于人民生活和工业生产的各个方面。但由于物联网系统具有许多攻击面的性质，不断产生新的攻击方式，物联网系统面临更大的安全性挑战。随着攻击数量和速度的增长，人工智能等新兴技术逐渐作为智能和实时保护物联网系统的手段。本文旨在提供一个研究人员和网络安全专业人员可以在网络安全和人工智能的背景下研究物联网的有用工具，以保护物联网系统。

关键字：工业物联网；网络安全；人工智能；攻击模式

中图分类号：TP393　　**文献标志码：**A

1　引言

自 2008 年左右物联网诞生以来，一直处于蓬勃增长的态势[1]。现在物联网已经成为工业生产和日常生活的一部分。物联网的概念很难定义，因为它自提出以来一直在发展和变化中，但它可以被理解为一个由数字、模拟机器及具有唯一标识符的计算设备组成的网络，这些设备能够在没有人工干预的情况下共享数据[2]。在大多数情况下，这表现为人类与中央中枢设备或应用程序（通常是移动应用程序）的交互，然后 向一个或多个边缘物联网设备发送数据和指令[3]。

物联网在设备连接方面提供了更高水平的可访问性、完整性、可用性、可扩展性、保密性和互操作性[4]。同样，因为物联网本身广泛的连接能力，更容易受到网络攻击，而且受到的网络攻击是多方位的[5]。

随着物联网技术的发展，人工智能技术在物联网安全领域的应用备受关注。如决策树、线性回归、机器学习、支持向量机和神经网络等，已被用于物联网网络安全研究中，已能够识别威胁和潜在的攻击。

2　物联网人工智能应用综述

文献 [6] 中对物联网应用相关的安全风险和可能的应对措施进行了全面的审查，并从完整性、匿名性、保密性、隐私性、访问控制和身份验证等方面对物联网技术进行了比较。授权、弹性和作者使用 CICIDS2017 提出了深度学习模型面向物联网网络安全的 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击检测数据集，准确率达到 97.16%。文献 [7] 评估了网关设备中的人工神经网络，以便能够检测从边缘设备发送的数据中的异常。结果表

* 通信作者：巩潇

明，该方法能够提高物联网系统的安全性。文献 [8] 提出了一种基于人工智能的控制方法，用于检测、估计及补偿工业物联网系统中的网络攻击。文献 [9] 为物联网环境提供了一种强大的普适检测，开发了多种对抗攻击和防御机制，并通过包括 MNIST、CIFAR-10 和 SVHN 在内的数据集验证了他们的方法。文献 [10] 分析了人工智能决策在网络物理系统中的最新发展，并发现由于不断增加的集成，这种发展实际上是自主的物联网设备在网络物理系统中的价值，以及人工智能决策的价值，因为它在处理大量的数据方面的速度和效率可能会使这种演变不可避免。文献 [11] 讨论了使用人工智能和机器学习进行风险分析的新方法，特别是在行业环境中的物联网网络中，并阐述了捕捉和评估物联网设备网络安全风险的方法，目的是标准化此类做法，以便更有效地识别和防范物联网系统中的风险。

3 物联网攻击方式综述

由于许多物联网设备的安全性较低，网络攻击者已经找到了许多方法从不同的方面攻击物联网。攻击面可能因物联网设备本身、硬件和软件、物联网设备所连接的网络及设备所连接的应用程序而异；这是三种最常用的攻击面，它们共同构成了物联网系统的主要部分。

3.1 初步侦察

在物联网攻击者试图对物联网设备进行网络攻击之前，他们通常会对物联网系统进行信息收集，以识别当前资产。然后，攻击者对设备进行逆向工程，创建一个测试攻击，看看可以获得什么输出，以及有什么途径可以攻击设备。这方面的例子包括打开设备并分析内部硬件（如闪存）以了解软件，以及篡改微控制器以识别敏感信息或导致意外行为 [12]。为了对抗逆向工程，物联网设备必须具备基于硬件的安全性。由传感器、执行器、电源和连接组成的应用处理器应放置在防篡改环境中。设备身份验证也可以通过基于硬件的安全性，这样设备可以向它所连接的服务器证明它不是伪造的。

3.2 物理攻击

物理攻击通常是一种低技术类型的攻击方式，常见的有：①断电攻击，设备所连接的网络被关闭以中断其功能；②物理损坏，设备或其组件受到损坏，无法正常工作；③恶意代码注入，例如攻击者将包含病毒的 USB 插入目标设备；④对象干扰，信号干扰器用于阻止或操纵设备发出的信号；⑤ PDoS（Permanent Denial of Service，永久拒绝服务）攻击，可以作为物理攻击来执行，例如物联网设备连接到高压电源，它的电力系统可能变得过载，然后需要更换。

3.3 MITM 攻击

MITM（Man-in-the-Middle，中间人）攻击拦截物联网系统中的两个节点之间的通信，并允许攻击者扮演代理的角色。MITM 攻击在物联网安全领域的有两种常见的攻击模式：云轮询和直接连接。在云轮询中，如智能物联中的智能家居设备经常与云通信，通常是为了寻找固件更新。攻击者可以使用地址解析协议破坏或通过改变域名系统设置来重定向网络流量，或通过使用自签名证书或工具来拦截 HTTPS 流量。许多物联网设备不验证证书的真实性或信任级别，这使得自签名证书方法特别有效。在直接连接的情况下，设备与同一网络中的集线器或应用程序通信。移动应用程序可以通过探测本地网络上特定端口的每个 IP 地址来定位新设备。攻击者可以做同样的事情来发现网络上的设备。

此外，针对物联网设备的 MITM 攻击的另一种常见形式是通过蓝牙连接。许多物联网设备运行蓝牙低能耗，其设计理念是物联网设备更小、更便宜、更节能。

一旦攻击者通过 MITM 攻击访问了物联网网络上的部分或全部设备，他们接下来可能实施的攻击就是虚假数据注入攻击，攻击者少量改变物联网传感器的测量值以避免被怀疑，然后输出错误的数据 [13]。

3.4 僵尸网络

物联网设备的另一种常见攻击是挖掘许多设备来创建僵尸网络，并发起 DDoS 攻击。DoS（Denial of Service，拒绝服务）攻击的特征是精心策划的阻止合法使用服务的行为；DDoS 攻击使用来自多个实体的攻击来实现这一目标。DDoS 攻击旨在摧毁目标服务的基础设施，并中断正常的数据流。DDoS 攻击通常经历几个阶段：①攻击者扫描要使用的易受攻击的机器；②利用易受攻击的机器，并注入恶意代码；③攻击者评估受感染的机器，看到哪些是在线的，并决定何时安排攻击或升级机器；④在攻击中，攻击者命令受感染的机器发送恶意的数据包。由于物联网设备的高可用性及普遍较差的安全性和维护性，获得受感染机器和进行 DDoS 攻击的最流行方式之一是通过物联网设备。僵尸网络常见命令结构如图 1 所示，其中攻击者的主计算机向一个或多个受感染的命

令和控制中心发送命令，每个控制中心控制一系列僵尸设备，然后这些设备可以攻击目标。

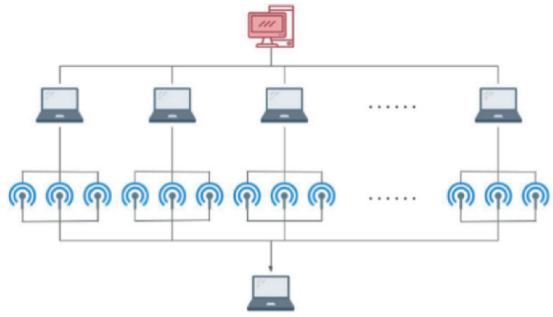

图 1　僵尸网络常见命令结构

3.5　DoS 攻击

物联网设备可能经常受到 DoS 攻击。物联网设备特别容易受到 PDoS 攻击，导致设备或系统完全无法运行。这可以通过电池或电源系统过载，或者更普遍的固件攻击来实现。在固件攻击中，攻击者可能利用漏洞将设备的基本软件（通常是其操作系统）替换为有缺陷或者已损坏的版本，使其无法使用。当设备被清空时，设备的所有者别无选择，只能用操作系统的干净副本和可能放在设备上的任何内容来刷新设备。在特别强大的攻击中，被破坏的软件可能使设备的硬件超负荷工作，使得在不更换设备部件的情况下恢复是不可能的。对该设备电源系统的攻击虽然不太受欢迎，但可能更具破坏性。例如当加载了恶意软件的 USB 设备插入计算机时，会过度使用设备功率达到设备硬件完全损坏并需要更换的程度。

由于物联网系统的结构，存在多种攻击面，但攻击物联网系统最常见的方式是通过连接，因为这些连接往往是最薄弱的环节。在未来，物联网开发商最好确保他们的产品能够抵御此类攻击，物联网安全标准的引入将防止用户在不知不觉中购买不安全的产品。保持物联网系统所在网络的安全将有助于防止许多常见的攻击，保持该系统与其他关键系统基本隔离或采取备份措施将有助于减轻万一发生的损害。

4　结论

本文探讨了试图破坏或危及物联网的流行技术，并从表面上解释了这些攻击是如何进行的。首先介绍了一些研究人员人工智能算法在网络安全中的应用。在许多情况下，这些模型在商业应用中还不常见，而是仍在研究和开发中，或者仍难以实现，因此很少出现。尽管如此，所讨论的模型是有前途的，并且可能在几年内成为常见的攻击检测系统。同时结合物联网系统的框架，介绍了多种常见的物联网攻击模式，其中最为核心的是 MITM 攻击方式。此外，本文旨在强调新兴技术的含义及这些领域对其他领域的影响。重要的是要考虑技术发展在公开之前和之后的所有潜在后果，因为网络攻击者不断寻求利用新技术为自己谋利，可能改变技术的原始用途，也可能将技术用作延续其他攻击的工具。

参考文献

[1]　赵汉卿，段京丰，罗嘉伦．人工智能技术在大数据网络安全防御中的运用研究 [J]．网络安全技术与应用，2023，267 (3)：19-20．

[2]　牛文．人工智能技术在网络空间安全防御中的实践探究 [J]．无线互联科技，2021，18 (8)：72-73．

[3]　姜顺荣．物联网中信息共享的安全和隐私保护的研究 [D]．西安：西安电子科技大学，2016．

[4]　苏玉燕．基于人工智能技术的网络安全防御系统设计分析 [J]．信息记录材料，2021，22 (9)：151-152．

[5]　丁爱萍．大数据时代网络信息安全及对应策略研究 [J]．电子技术与软件工程，2021，210 (16)：253-254．

[6]　梁广俊，辛建芳，王群，等．物联网取证综述 [J]．计算机工程与应用，2022，58 (8)：12-32．

[7]　田春平，张晋源，武靖莹．云计算网络信息安全防护思路探究 [J]．通信技术，2019，52 (4)：939-945．

[8]　MARCO D R，ALESSIO Z，MEROUANE D，et al．Smart radio environments empowered by reconfigurable intelligent surfaces：how it works，state of research，and road ahead[J]．IEEE Journal on Selected Areas in Communications，2020，38 (11)：2450-2525．

[9]　邹聪．基于人工智能技术的网络安全防护探究 [J]．办公自动化，2022，27 (24)：10-12，40．

[10]　苗耀锋．基于人工智能技术的网络安全防护探索 [J]．中国管理信息化，2021，24 (4)：197-198．

[11]　吴彤．无线网络物理层安全传输策略研究 [D]．北京：北京交通大学，2016．

[12]　郎风华．基于人工智能理论的网络安全管理关键技术的研究 [D]．北京：北京邮电大学，2008．

[13]　牛颉．基于人工智能的网络入侵检测技术研究 [D]．北京：北京邮电大学，2021．

收稿日期：2023-08-29