面向信息物理系统的智能攻击感知与协同安全防御策略研究

2024 年 11 月 15 日

目录

1 立项依据与研究现状

1.1 结合国家战略

1.1.1 国家安全与信息物理系统的关系

随着全球数字化和信息化进程的加速，信息物理系统 (Cyber-Physical Systems, CPS) 逐渐成为国家安全与社会稳定的基石。这些系统通过集成信息技术与物理过程，已成为现代工业生产、城市运行和社会管理的核心支撑技术。作为信息技术与物理实体深度融合的产物，这些系统在智能制造、交通管理、能源供应等领域发挥着不可或缺的作用。信息物理系统作为信息化与物理世界交互的核心枢纽，承担着国家安全和社会治理的重要角色，其安全性直接影响国家的稳定与发展。

特别是在当前国际形势中，信息物理系统已成为国家间竞争和对抗的关键技术领域之一。例如，俄乌冲突中的无人机攻击、大规模网络攻击等都显示了信息物理系统作为重要基础设施的战略意义，现代战争中对信息物理系统的网络攻击可以迅速造成物理损害和信息泄露，严重威胁国家的基础设施和公共安全。在此情境下，加强信息物理系统的安全防护不仅关乎经济利益，更关乎国家的安全与稳定。因此，深入研究信息物理系统的安全机制与防护策略，已成为国家层面的迫切需求。

1.1.2 政策导向与研究的必要性

国家在网络安全和信息物理系统安全领域的政策导向日益明显。为应对复杂严峻的网络安全环境，我国出台了多项政策和战略文件，以保障国家关键信息基础设施和信息物理系统的安全。例如，《网络安全法》《数据安全法》和《关键信息基础设施安全保护条例》均明确了对重要信息系统的安全保障措施，要求加强对涉及公共安全、经济运行和国防建设等领域的关键信息基础设施的保护。此外，《“十四五”国家信息化规划》和《数字中国建设总体布局规划》也指出了在信息物理系统中加强网络安全和抗攻击能力建设的必要性，强调利用新兴技术提升网络空间安全。这些政策不仅要求对关键信息基础设施进行全面评估与保护，还倡导在新兴技术应用中加强安全设计。

随着国家对网络空间安全的重视与投入不断增加，信息物理系统在政策导向下逐步成为研究热点。当前，国家在智能制造和智能交通等领域的布局，已将信息物理系统的安全性置于战略高度。国家政策导向不仅表现在基础设施的安全防护方面，还在于要求各部门协同作战，构建全方位的安全防御体系。此外，政策推动了信息物理系统在人工智能和自动化领域的深入应用，但同时也对系统安全提出了更高的要求，尤其是在低空无人机、车联网、电动汽车等新兴应用中，智能攻击的可能性使得安全防护愈发迫切。因此，面向信息物理系统的智能攻击感知和协同安全防御策略的研究，不仅是顺应国家政策导向的需要，更是确保信息物理系统在复杂环境下安全、稳定运行的重要保障。

1.1.3　信息化建设中的安全需求

信息化建设的推进，加速了我国各类信息物理系统在规模和复杂度上不断增加，形成了大规模、分布式、动态变化的系统网络。这种复杂的系统结构使得传统的静态防御手段难以满足安全需求，迫切需要创新性、安全性更强的防御策略。与此同时，智能化攻击技术的迅速发展带来了显著的安全隐患，也增加了信息物理系统的安全防护难度。根据国际电信联盟 (ITU) 的报告，全球信息物理系统的漏洞已成为网络攻击的主要目标。我国的低空无人机、车联网和电动汽车等新兴领域，均展现出极大的发展潜力与安全挑战。特别是在车联网环境中，智能汽车的互联互通一方面提升了出行的安全与便利，另一方面也使得网络攻击成为可能。通过低空无人机进行攻击、利用车联网的漏洞窃取信息、通过电动汽车远程控制等攻击手段，不断挑战现有的安全防御能力。研究表明，针对智能车辆的攻击不仅能够造成经济损失，还可能威胁到乘客的生命安全。因此，面向信息物理系统的安全需求日益显著，尤其是在高风险领域，需要设计具有实时监控和智能防御能力的安全策略，以确保信息物理系统在复杂环境下的稳定与安全运行。

在信息物理系统中，由于其实时性、异构性和高度耦合的特点，任何一个环节出现漏洞，可能会迅速传导到整个系统网络中，造成系统级的安全隐患。因此，针对信息物理系统的安全防护，亟需从传统的单一防御手段转向智能化、协同化、多层次的综合防御体系。未来的防御体系需要具备实时感知、快速响应和协同联动等特点，以有效抵御多样化的攻击手段，从而保障信息物理系统的安全性与稳定性。

1.1.4　国家战略目标对安全防御的影响

我国提出的“制造强国”“网络强国”和“数字中国”等战略目标，明确了信息物理系统在国家发展中的重要地位，旨在推动制造业升级、增强国家科技实力、实现经济高质量发展。根据《数字经济发展战略纲要》(2021)，数字经济的发展与安全相辅相成，必须构建安全可靠的数字基础设施，以支撑国家经济转型与高质量发展。信息物理系统作为国家数字基础设施的重要组成部分，其安全性直接关系到战略目标的实现。在此背景下，信息物理系统作为支撑国家战略的重要基础，必须具备足够的抗攻击能力，以保证国家关键领域的自主可控和安全运行。特别是在智能制造、无人驾驶、电动汽车、智慧城市等领域，信息物理系统已成为实现国家战略目标的核心支撑技术，进一步提升了其安全防护的重要性。

国家战略不仅强调技术创新，还要求强化信息安全。例如，国家在智能制造中的一系列布局，如《智能制造发展规划 (2021-2025)》和《新型基础设施建设行动计划》，均强调了智能化生产过程中的信息安全要求。未来几年，随着车联网、电动汽车等新兴应用领域的迅速发展，信息物理系统的安全需求将不断增加。国家战略目标的实现需要信息物理系统能够应对多种复杂环境和潜在威胁，通过构建全面、智能的安全防护体系，增强抗攻击能力与自我恢复能力，以保障国家在战略层面的长远利益。这不仅是实现国家长远发展的必然要求，也是确保社会安全和公共利益的重要保障。

1.2 现存的问题

1.2.1 攻击感知不全面

在网络安全防御体系中，对潜在威胁和攻击行为的识别与监测存在局限性，导致攻击感知的不全面。当前的攻击感知系统往往依赖于固定的数据源，如网络流量、日志文件和传感器数据。然而，这些数据源可能无法全面捕捉所有的攻击模式，尤其是针对信息物理系统 (CPS) 和物联网 (IoT) 设备的复杂攻击。许多攻击者利用非常规手段进行攻击，这使得传统的数据获取方式难以有效感知。攻击者采用多种技术和策略来发起攻击，如社会工程学、零日漏洞利用等。现有的攻击检测技术主要针对已知威胁，对于新型或混合攻击的识别能力不足。此外，由于攻击模式的不断演化，攻击感知系统需要持续更新和调整，但现实中往往缺乏相应的动态适应能力。许多攻击感知系统依赖于规则或启发式算法进行威胁检测，这可能导致对攻击行为的误判或漏判。例如，某些正常行为可能被误判为攻击，而真正的攻击则可能未被检测到。算法的设计和训练数据的选择直接影响系统的识别能力，存在较大的主观性和不确定性。在信息物理系统中，攻击往往需要实时感知和快速响应。然而，现有的许多攻击感知系统在数据处理和决策制定上存在延迟，这使得在攻击发生时难以及时作出反应。尤其是在高负载或复杂环境下，实时感知能力的不足将导致严重的安全隐患。攻击感知往往是孤立进行的，缺乏跨系统、跨组织的信息共享与协同。不同系统之间的安全信息不对称，使得某些攻击行为难以被全面识别和响应。此外，缺乏统一的标准和协议，导致各个系统的攻击感知能力差异较大，影响了整体安全防护效果。

感知技术的局限性

攻击感知技术是保障网络和信息系统安全的重要手段，但现有技术在多方面存在局限性，影响了对攻击行为的全面识别和响应能力。首先，许多攻击感知技术依赖特定的数据源，例如网络流量监测和系统日志分析，这种单一的数据获取方式难以全面捕捉攻击行为，尤其在复杂网络环境中，攻击者可能通过非常规手段渗透，导致感知系统无法及时识别。此外，当前的检测算法主要基于已知攻击特征和模式（如签名检测和基于规则的检测），难以有效应对新型或变种攻击，尤其是零日攻击通常不在已知签名库中，因此传统检测方法难以识别。攻击感知系统还常面临假阳性（将正常行为误判为攻击）和假阴性（未能识别真正攻击）的困扰，假阳性会导致不必要的警报和资源浪费，而假阴性则可能导致安全漏洞被利用，降低了系统的可信度和实用性。实时处理能力的局限也显著影响了系统的响应速度，现有技术在数据处理和分析上常存在延迟，难以应对攻击的快速和隐蔽特性。同时，许多攻击感知系统缺乏自我学习和适应能力，面对新兴攻击手段无法自动调整参数或更新规则，难以在动态网络环境中有效应对复杂攻击。最后，不同组织和系统之间的信息孤岛现象严重，缺乏跨域的信息共享和协作，许多系统独立运行，未形成有效的情报共享机制，导致对广泛攻击行为的感知不全面，信息不对称使得许多攻击难以被全面识别。

数据获取与处理的挑战

在网络安全领域，攻击感知的有效性依赖于高质量的数据获取与处理。然而，当前的数据获取与处理面临诸多挑战，这些挑战影响了攻击检测的准确性和实时性。首先，数据来源的多样性与复杂性是一个主要挑战。攻击者可以通过多种渠道和手段发起攻击，数据来源不仅限于网络流量、日志记录和传感器数据，还可能包括用户行为数据和设备状态信息。数

据来源的多样性使得数据整合和统一处理变得复杂，不同数据格式、协议和标准的存在增加了数据融合的难度，影响了对系统安全状态的全面掌握。此外，数据的高维度与稀疏性也是问题之一。在网络环境中，数据量庞大且维度高，尤其是在物联网和信息物理系统中，设备数量和数据生成速率急剧增加，这种高维度数据使得计算负担加重，传统数据处理方法难以应对。同时，部分攻击行为可能导致数据稀疏性，进一步增加了有效信息的提取难度，影响攻击检测的准确性。数据质量与完整性问题也不可忽视，数据的丢失、篡改、重复和噪声等问题会导致分析结果不准确，尤其是在信息物理系统中，数据准确性和时效性至关重要，任何数据不完整都可能导致攻击行为的误判。实时性与延迟问题则影响了攻击感知的及时响应能力，现有数据处理系统在性能上常常遇到瓶颈，延迟会导致在攻击发生时未能及时反应，从而给攻击者以可乘之机。此外，隐私与合规性问题同样重要，在数据获取过程中需要遵循隐私法规，如 GDPR，影响了数据采集和使用的范围，限制了攻击感知系统的效果。最后，人工干预与自动化程度的限制也是挑战之一，尽管自动化的数据处理提高了效率，但许多攻击感知系统仍依赖人工干预进行数据分析和决策，这增加了人为错误的风险，限制了系统的响应速度和适应能力。如何实现高度自动化的数据处理过程，是未来研究的重要方向。

多样化攻击手段的识别困难

随着攻击技术的发展，攻击者不断采用更加复杂、多样化的手段，导致传统的感知方法难以有效识别这些新型攻击行为。主要难点包括零日攻击与高级持续性威胁（APT），隐蔽性攻击手段以及异构攻击与组合攻击。零日攻击利用未公开的漏洞进行攻击，而高级持续性威胁通常具有高度隐蔽性并持续时间较长，这些攻击手段超出了传统检测系统的应对范围，难以通过签名或规则进行识别。尤其是零日攻击因缺乏已知特征而识别难度极大。隐蔽性攻击手段则使得攻击者通过加密流量、混淆代码或分布式攻击等方式隐藏攻击行为，使得感知系统难以检测，此类攻击流量往往与正常流量难以区分，传统特征匹配方法难以有效应对，导致漏报。此外，信息物理系统中存在多种设备和网络，攻击者可能利用这些设备的差异性，发起多维度、组合型攻击。在异构环境中，单一维度的监测难以全面感知这些攻击行为，识别此类组合攻击需要更复杂的数据分析和模型匹配。

实时监测能力不足

在信息物理系统中，实时监测是保障系统安全的关键。然而，当前的感知系统往往缺乏足够的实时监测能力，存在数据处理延迟、资源受限、大规模网络环境的负载，以及监测与响应协调等多方面的挑战。实时监测要求快速处理大量数据，而现有系统在数据处理速度上难以满足高频监测的需求，特别是在多源数据融合和复杂计算任务下，处理延迟显著，影响了对攻击的即时响应。此外，边缘设备在信息物理系统中广泛应用，但由于计算能力、内存和带宽的限制，边缘设备上的实时监测受到瓶颈，如何在资源受限的环境下实现高效实时监测仍是技术难点。在大型信息物理系统中，传感器、节点和网络设备数量庞大，数据量巨大，实时处理这些数据要求系统具备极高的吞吐量，现有架构难以应对大规模网络环境下的高频攻击感知需求。同时，实时监测不仅需要发现威胁，还需要及时做出响应，但监测与响应的协调存在时滞，尤其在复杂系统中，难以实现高效的自动化联动响应。这些因素共同影响了攻击感知的实时性，削弱了整体防御效果。

1.2.2 态势评估不精确

当前的态势评估模型通常依赖于预定义的规则或简单的统计方法，但在复杂环境下，这些模型存在一定的局限性。许多模型为了降低计算复杂度，对环境因素进行了简化处理，忽略了攻击者的动态行为和环境变化的影响，从而导致评估结果无法准确反映真实的安全态势。此外，信息物理系统涉及多种类型的数据源，如传感器数据、网络流量、系统日志等，数据模型的缺乏使得无法全面整合这些不同的数据，影响了态势评估的准确性。

态势评估的准确性还受到主观判断和算法偏差的影响。许多安全系统依赖安全专家的经验判断，虽然经验可以提供有效参考，但主观判断往往受个人认知和知识局限的影响，容易造成评估偏差。评估算法在设计时可能带有某种偏好或先验假设，这导致在实际应用中对异常情况的处理不够灵活，尤其是在面对非典型攻击时，容易出现漏报或误报。

信息物理系统的环境复杂且动态，态势评估在此环境下面临更大的挑战。动态环境要求态势评估能够快速响应环境变化，但由于复杂的数据处理过程，实时性常常难以保证，从而影响对突发性威胁的响应。此外，在动态环境中，传感器和网络数据往往包含大量噪声，这些噪声可能掩盖真实威胁信息，增加了评估的难度。如何有效过滤噪声并提取有用信息，成为态势评估的一大挑战。

态势评估的有效性还依赖于多方协同和信息共享。然而，当前在信息共享和协同方面仍存在不足。不同部门和系统之间的信息流动性差，导致在进行态势评估时，难以获取全面数据，从而影响系统的整体感知能力。信息共享的障碍还在于数据格式和接口的非标准化，不同系统之间的数据难以互通，阻碍了跨部门的协同分析。更进一步，态势评估中的协同需求不仅仅是数据共享，还涉及跨组织的合作机制，如联合威胁分析和共享防御策略。然而，缺乏完善的合作机制往往导致评估信息不对称，影响态势感知的全面性和精确性。

1.2.3 安全防御不彻底

现有的防御体系通常存在脆弱性，无法在攻击发生时充分发挥保护作用，主要体现在防御架构单一、应对攻击链条的能力不足等方面。许多系统依赖单一的防御手段，如防火墙或入侵检测系统，缺乏纵深防御的结构，因此容易被攻击者突破。一旦核心防御被攻破，后续防护措施往往无法有效应对。此外，攻击通常是分阶段实施的，涉及多种方式和路径，但现有防御体系在识别和切断攻击链方面能力不足，容易出现防御缺口，使得攻击得以逐步深入。

资源配置的不均衡性直接影响了防御体系的完整性和持续性。许多系统在资源分配上存在严重倾斜，往往将更多的资源投入到核心设备或关键区域，而外围设备或次要区域的防御则较为薄弱，攻击者可以通过这些薄弱点进入系统。同时，缺乏足够的专业安全人员或技术支持，使得系统在发现和响应安全威胁时存在滞后性。资源的限制也影响了新型防御技术的引入，导致系统的防护手段相对滞后。

有效的安全防御需要完善的应对策略，但许多系统在此方面存在缺失。面对突发攻击，许多系统缺乏明确的应急响应方案，导致在攻击发生时无法及时采取有效措施，这种缺失往往会导致攻击影响范围扩大，甚至可能造成系统瘫痪。此外，攻击手段快速演变，防御策略需要定期更新以适应新的威胁。然而，部分系统的策略更新不及时，仍然依赖过时的防御

规则，无法应对最新的攻击技术。

安全防御不仅依赖于技术手段，还需要全体人员的安全意识来增强防御效果。在信息物理系统中，安全意识的不足尤为突出。许多系统的运营和维护人员未接受足够的安全培训，缺乏对常见攻击手段和防御措施的基本了解，可能在无意中放大系统的安全漏洞。同时，用户行为往往是系统安全的薄弱环节，但当前对用户行为的监控和引导措施不足，容易因不当操作导致安全风险。例如，未及时安装安全补丁或随意共享敏感信息等行为，都会影响系统整体的安全性。

1.3　研究意义

1.3.1　提升国家安全保障能力

国家安全方面的优势体现

CAN 总线技术具有多项优势，能够在保障国家安全方面发挥重要作用。首先，其高可靠性源于差分传输和错误检测纠正机制，这不仅有效降低了数据传输过程中的错误率，还能够自动纠正错误，确保数据的准确性和稳定性。在国家安全领域，任何数据错误或传输延迟都可能带来不可估量的影响。例如，在智能网联汽车领域，CAN 总线技术确保车辆控制指令准确传输，防止因数据错误引发交通事故或系统瘫痪，从而保障国家交通系统的安全稳定运行。

此外，CAN 总线技术具备较低的传输延迟和快速的数据传输速率，满足了实时性要求较高的应用需求。在国家安全领域，这种实时性优势至关重要。例如，在军事通信系统中，CAN 总线技术能够确保指挥信息的实时传输，使指挥员能够迅速做出决策并下达指令，从而提升应急响应速度和作战效能。同时，在智能交通系统中，CAN 总线技术实现了车辆与交通管理中心的实时通信，提升了交通系统的整体效率和安全性。

CAN 总线技术还支持分布式控制和多主机通信，节点可以根据需求灵活配置和扩展。这一特性在国家安全领域同样具有显著优势。以智能电网为例，CAN 总线技术可以实现各个电力节点的分布式控制，从而提升电力系统的灵活性和可靠性。在军事通信系统中，CAN 总线技术的分布式通信和控制功能增强了作战系统的整体效能和协同作战能力。

在安全性方面，CAN 总线技术通过引入加密技术和访问控制机制，有效防范网络攻击和数据泄露风险。例如，在智能网联汽车领域，通过加密通信和身份验证机制，可以防止攻击者通过逆向总线通信协议或伪造控制指令来攻击车辆系统。类似地，在军事通信系统中，加密通信和身份验证机制可以防止敌方通过窃取或篡改通信内容来获取敏感信息或干扰指挥系统。

最后，CAN 总线技术的标准化进程促进了国际合作与交流，推动了其在国家安全领域的广泛应用。作为国际标准之一，CAN 总线技术的普及不仅推动了技术共享，也增强了各国在国家安全领域的技术防御能力。通过与国际伙伴的合作，能够共享最新的技术成果和经验，进一步提升国家安全领域的整体技术水平和防御能力。

强化国家关键基础设施的网络安全韧性

信息物理系统 (CPS) 作为新一代信息技术与物理世界深度融合的产物，已深度嵌入国家关键基础设施之中，包括但不限于智能交通、智能电网、智能制造等关键领域。CAN 总

线作为智能网联汽车内部通信的核心协议，其安全性直接关系到整个交通系统的稳定与安全，乃至国家关键基础设施的整体安全。通过深入研究基于 CAN 总线入侵检测的智能攻击感知技术，可以实现对车辆网络异常行为的实时监测与精准识别，有效抵御外部势力的网络攻击和物理破坏，从而显著提升国家关键基础设施的网络安全韧性，确保国家经济命脉、社会稳定和人民生命财产安全不受侵害。

推动网络安全防御体系向智能化、自主化转型随着网络攻击手段的不断演进，传统的网络安全防御手段已难以满足当前复杂多变的网络安全需求。基于 CAN 总线入侵检测的面向 CPS 的智能攻击感知与协同安全防御策略，通过引入先进的智能算法、机器学习技术和大数据分析手段，实现了对网络攻击行为的智能感知、预警与响应，推动了网络安全防御体系向智能化、自主化转型。这种转型不仅提高了网络安全防御的效率和准确性，降低了误报率和漏报率，还增强了网络安全防御体系的自适应性和灵活性，使其能够更有效地应对新型网络攻击威胁。

提升国家应对复杂安全挑战的能力与水平在全球化背景下，国家面临着来自多方面的安全挑战，如网络犯罪、恐怖主义、跨国犯罪等。这些安全挑战往往具有跨国性、隐蔽性和复杂性等特点，给国家安全带来了前所未有的压力。基于 CAN 总线入侵检测的面向 CPS 的智能攻击感知与协同安全防御策略，通过实时监测和分析车辆网络中的异常行为，可以及时发现并处置潜在的安全威胁，为国家安全决策提供科学依据和参考。这种能力不仅有助于提升国家应对复杂安全挑战的整体效能，还可以促进国家间在安全领域的交流与合作，共同应对全球性的安全挑战。

推动国际交流与合作基于 CAN 总线入侵检测的面向 CPS 的智能攻击感知与协同安全防御策略的研究，不仅对于单个国家具有重要意义，而且对于全球信息物理系统安全领域的标准制定与技术交流也具有积极的推动作用。通过分享研究成果、交流经验和技术，可以促进国际间的合作与交流，共同推动全球信息物理系统安全领域的技术创新和标准制定。这种合作不仅可以提升全球信息物理系统安全领域的整体水平，还可以促进国际间的经济、科技和文化交流，增进各国之间的友谊与互信。同时，这种合作还可以为全球安全治理体系的完善与发展提供有益的借鉴和参考，推动全球信息物理系统安全领域的可持续发展。

1.3.2 促进信息物理系统的安全发展

深度提升信息物理系统的安全防护能力

通过智能攻击感知技术，研究能够精准识别针对 CAN 总线的各种攻击模式，包括但不限于伪装攻击、中间人攻击、拒绝服务攻击等。通过实时监测和异常检测，系统能够迅速响应并采取措施，有效阻止攻击行为，保障系统的稳定运行。

研究不仅关注即时防御，还致力于提升系统的韧性。通过模拟和分析各种攻击场景，系统能够学习并适应不同的攻击模式，增强自身的恢复能力和自我修复能力。即使遭受攻击，系统也能在短时间内恢复并继续运行，从而减少损失。

CAN 总线作为信息物理系统中数据交换的桥梁，其安全性直接关系到数据的隐私和完整性。研究通过加密传输、数据完整性校验等技术手段，确保数据在传输过程中的隐私性和完整性，防止数据被篡改或泄露。

推动信息物理系统安全技术的持续创新与发展

研究将促进计算机科学、网络安全、自动化控制、人工智能等多个领域的技术融合与突破。通过结合机器学习、深度学习等先进技术，开发出更加高效、智能的安全防御系统，提升系统的自适应性和智能化水平。

随着研究的深入，信息物理系统安全技术的标准化和规范化建设也将得到推动。通过制定统一的安全标准和规范，可以提高系统的互操作性和安全性，降低系统建设和运维的成本与风险。

此外，研究还将促进相关学科的发展和人才培养。通过培养具备跨学科知识和技能的复合型人才，为信息物理系统的安全发展提供有力的人才支持。同时，推动相关学科的交叉融合，形成更加完善的知识体系。

1.3.3　促进技术创新与应用

技术创新层面的深度推进

研究将推动针对 CAN 总线入侵检测的算法与模型的创新。这包括但不限于深度学习、强化学习、异常检测等先进技术在 CAN 总线安全领域的应用与优化。通过引入先进的机器学习算法，研究将实现对 CAN 总线通信数据的实时分析、模式识别与异常检测，从而实现对潜在攻击行为的快速响应与防御。研究将探索信息物理系统中智能攻击感知与协同安全防御的系统架构与协同机制。这包括分布式协同防御、多层级协同防御等策略的设计与实施。通过优化系统架构与协同机制，研究将实现不同安全组件之间的高效协同与信息共享，提升整个系统的安全防御能力。研究将推动硬件与软件在安全防御领域的融合创新。例如，开发专门的安全芯片或安全模块，将安全功能嵌入到 CAN 总线通信的硬件层面，实现硬件级别的安全防护。同时，研究还将探索软件层面的安全防护策略，如开发专门的安全协议、加密技术等，以提高 CAN 总线通信的安全性。

应用实践层面的广泛拓展

研究将直接应用于智能网联汽车的安全防护领域。通过实时监测 CAN 总线通信数据，及时发现并阻止潜在的恶意攻击，保障车辆的正常运行和乘客的安全。同时，研究还将为智能网联汽车的安全认证、数据保护等提供有效的技术支持和解决方案。除了智能网联汽车领域，研究还将拓展到工业物联网 (IIoT) 的安全保障领域。通过借鉴和移植相关技术，为工业设备、生产线等提供全面的安全防护方案。这将有助于降低工业物联网领域的安全风险，提高整个工业生态系统的安全性和稳定性。研究还将为智慧城市和智能家居的安全管理提供技术支持。通过实时监测和分析城市基础设施和家居设备的通信数据，及时发现并处理潜在的安全威胁。这将有助于提升智慧城市和智能家居的安全性和用户体验。

行业标准与规范层面的积极贡献

研究将推动 CAN 总线安全标准的制定与完善。通过深入分析 CAN 总线的安全需求和挑战，为相关标准的制定提供科学依据和技术支持。这将有助于形成统一的安全标准和规范，提高不同厂商、不同设备之间的安全兼容性和互操作性。研究将促进 CAN 总线安全评估与认证体系的发展。通过开发专门的安全评估工具和方法，对 CAN 总线通信的安全性进行定量和定性的评估。同时，研究还将推动安全认证体系的建立与完善，为相关设备和系统

的安全认证提供技术支持和解决方案。

未来技术发展趋势的深远影响

研究将激发信息安全技术的持续创新动力。通过不断探索新的安全技术和方法，为 CAN 总线安全领域的发展注入新的活力和动力。这将有助于推动整个信息安全技术的不断进步和发展，提高整个信息物理系统的安全性和稳定性。研究将促进跨领域技术的融合与发展。通过借鉴和移植相关技术，推动计算机科学、电子工程、自动化控制、通信等多个学科领域的交叉融合与技术创新。这将有助于形成更加全面和深入的技术创新生态，推动整个信息物理系统向更加智能化、网联化的方向发展。

1.3.4 加强跨部门协同防御机制

强化信息共享的深度与广度

在跨部门协同防御机制中，信息共享是核心环节。基于 CAN 总线入侵检测的 CPS 智能攻击感知与协同安全防御策略研究，能够推动信息共享机制向更深、更广的方向发展。研究不仅要求共享基本的安全事件信息，还强调对安全事件背后的攻击手法、攻击源、攻击路径等深度信息的共享。这种深度共享有助于各部门更全面地理解安全威胁，从而制定更精准的防御策略。除了传统的安全部门外，研究还鼓励与技术研发、运营管理、法律法规等部门进行信息共享。这种跨领域的广度共享有助于形成更全面的安全防御体系，从多个角度共同应对安全威胁。

促进技术标准与流程的协同

跨部门协同防御机制的高效运作依赖于统一的技术标准和流程。研究通过深入分析 CAN 总线通信协议和入侵检测技术，提出了一套适用于跨部门协同的技术标准和规范。这些标准有助于确保各部门在信息共享、安全检测、应急响应等方面能够无缝对接，提高协同效率。研究还关注跨部门协同防御流程的优化。通过模拟演练、案例分析等方式，研究能够发现现有流程中的瓶颈和冗余环节，并提出优化建议。这种流程优化有助于减少协同过程中的摩擦和延误，提高整体响应速度。

提升跨部门沟通与协作能力

跨部门协同防御机制的成功实施还依赖于各部门之间的沟通与协作能力。研究通过组织跨部门会议、建立信息共享平台等方式，促进各部门之间的定期沟通和交流。这种沟通机制有助于各部门及时了解彼此的工作进展和面临的困难，从而共同寻找解决方案。研究还强调跨部门协作的重要性，通过培训、演练等方式提升各部门的协作意识和能力。这种协作精神的培养有助于形成更加紧密的安全防御网络，共同应对各种安全威胁。

推动法律法规与政策的完善

跨部门协同防御机制的发展还需要法律法规和政策的支持。研究通过深入分析跨部门协同防御过程中的责任划分问题，提出了一套明确的责任体系。这有助于确保各部门在协同防御过程中能够各司其职、各尽其责。研究还关注相关政策法规的完善情况，通过调研、分析等方式提出改进建议。这些建议有助于为跨部门协同防御机制的发展提供更有力的法律保障和政策支持。

1.4　研究现状

1.4.1　攻击感知方面

当前主流攻击感知技术

该技术通过计算 CAN 总线消息的信息熵来监测网络状态。在正常情况下，CAN 总线中各 ID 段消息的比例和信息熵应处于一定范围内。当攻击者发动 DoS（拒绝服务）攻击时，他们会在总线上短周期内注入高优先级消息，导致信息熵的异常变化。通过设定决策条件区间，可以检测并预测 DoS 攻击的发生。这种技术不仅适用于 DoS 攻击，还可以用于检测其他可能导致信息熵异常变化的攻击类型。

与基于信息熵的检测技术类似，基于样本熵的检测技术也是通过实时采样汽车的总线数据构建样本熵测试集，并利用样本熵的计算方法统计样本熵值。通过观察熵值的突变情况，可以确定该时刻是否有攻击发生。这种技术已经在实际汽车 ECU（电子控制单元）上进行了硬件在环测试，并验证了其对 DoS 攻击、模糊攻击和 bus-off 攻击的检测能力。

基于侧信道分析的检测技术主要监控 CAN 总线的侧信道信息，如总线的流量、ECU 的时钟和消息的电压等。这种技术不需要修改现有总线的协议，且不会增加 CAN 总线的流量。其中，基于电压的 IDS 可以检测所有 ID 的恶意帧并定位被攻击者控制的 ECU 和外部节点。这种技术通过为每个 ECU 和每个 ID 建立电压指纹，实现对恶意帧的准确检测和攻击源的定位。

态势感知（Cyber Situational Awareness, CSA）是一种前沿的网络安全技术，它通过收集、分析和解释来自不同来源的数据，实时监控和评估网络的安全状态。在 CAN 总线入侵检测中，态势感知技术可以综合运用大数据分析、机器学习和威胁情报等手段，提供实时的安全状态评估和威胁预测。通过与其他安全工具和系统的联动，如防火墙、入侵检测系统 (IDS) 和入侵防御系统 (IPS)，态势感知技术可以实现实时的威胁检测和响应，有效应对各种复杂和隐蔽的攻击手段。

攻击模式与行为分析

攻击模式分析中，典型的攻击类型包括物理攻击、逻辑攻击和社会工程学攻击。物理攻击直接针对物理设备或系统进行破坏或篡改，逻辑攻击则通过网络或信息系统对设备进行远程攻击，如病毒攻击、木马攻击和蠕虫攻击等。社会工程学攻击利用人的心理和行为特点进行攻击，例如钓鱼邮件、诈骗电话等。此外，信息物理协同攻击采用双层协同攻击策略，将蠕虫传播模型引入电力通信网络，通过分析病毒传播机理和错误数据注入攻击 (FDI) 来量化攻击行为对电力系统物理层的破坏。马尔科夫决策过程建模则用于模拟攻击者发动协同攻击与电力 CPS 系统的交互过程，以寻求最佳协同攻击策略。

攻击行为的分析揭示了攻击手段的多样化和攻击目标的广泛性。随着网络技术的发展，攻击手段愈加多样，涵盖病毒、木马、蠕虫、钓鱼、拒绝服务攻击等。攻击目标不仅限于传统的服务器和数据库，还包括物联网设备、移动设备等。在信息物理系统中，攻击者可能同时针对信息层和物理层进行攻击。随着网络普及，攻击的频率不断增加，攻击强度也逐步提升，旨在突破日益增强的安全防护措施。与此同时，攻击技术的复杂化使得攻击手段更加隐蔽，人工智能和机器学习的应用使攻击手段更具挑战性，防范难度加大。

此外，网络攻击的影响范围和程度也在不断扩大，不仅影响个人隐私，还可能波及国家

安全和社会稳定。在信息物理系统中，攻击可能导致物理设备的损坏、系统瘫痪和服务中断等严重后果。攻击手段的隐蔽性也日益增强，攻击者往往利用各种方式进行隐蔽攻击，规避检测和追踪。综上所述，面向信息物理系统的智能攻击感知与协同安全防御策略研究需要全面考虑各种攻击类型、手段、目标、频率、强度、影响范围、隐蔽性等因素，以便制定更为有效的防御策略并提升系统的安全防护能力。

感知系统的应用实例

在电力系统中，信息物理系统（CPS）的深度融合使得电力系统的通信、计算和控制能力得到了极大的发展，但同时也引入了网络攻击的风险。感知系统在这一领域的应用主要体现在对电力网络状态的实时监控和异常检测上。例如，通过部署传感器和监控设备，感知系统可以实时监测电力系统的运行状态，包括电流、电压、频率等关键参数。当这些参数出现异常波动或超出预设范围时，系统能够迅速发出警报，并触发相应的安全防御机制。此外，感知系统还可以与智能电表、配电自动化系统等相结合，实现对电力需求的精准预测和智能调度，从而提高电力系统的安全性和稳定性。

在智能制造领域，信息物理系统同样发挥着重要作用。感知系统通过集成各种传感器和执行器，可以实时监测生产线的运行状态、产品质量以及设备故障等信息。这些信息被实时传输到数据处理中心进行分析和处理，从而实现对生产过程的智能监控和优化。例如，当生产线上的某个设备出现故障时，感知系统能够迅速检测到故障信号并触发报警机制，同时提供故障定位和维修建议。这不仅可以减少生产中断时间，提高生产效率，还可以降低维修成本和安全风险。

智慧城市是信息物理系统应用的另一个重要领域。在智慧城市中，感知系统通过部署在城市各个角落的传感器和监控设备，可以实时监测城市的交通流量、空气质量、环境监测等关键信息。这些信息被用于城市管理和决策支持，帮助城市管理者更好地了解城市的运行状态和居民需求。例如，在交通管理方面，感知系统可以实时监测交通流量和拥堵情况，并提供交通疏导和路线优化建议；在环境监测方面，感知系统可以实时监测空气质量、水质等环境参数，并提供环境污染预警和治理建议。

除了上述领域，感知系统还可以应用于多个其他场景。例如，在农业领域，感知系统可以通过监测土壤湿度、温度等参数来指导灌溉和施肥等农业生产活动；在医疗领域，感知系统可以通过监测患者的生理参数来提供及时的医疗救助和健康管理建议；在航空航天领域，感知系统则可以监测飞行器的运行状态，以确保其安全性和可靠性。综上所述，感知系统在面向信息物理系统的智能攻击感知与协同安全防御策略研究中扮演着重要角色。通过实时监测和异常检测等功能，感知系统能够及时发现并应对各种网络攻击和安全威胁，为信息物理系统的安全性和稳定性提供有力保障。

现有技术的局限与挑战

当前，智能攻击行为的深度研究尚存在不足。尽管对智能攻击行为的研究已经取得了一定进展，但许多模型仍无法涵盖真实环境中的复杂场景。例如，针对拒绝服务（DoS）攻击造成的数据包丢失的模型，大多仍选用基本的 Bernoulli 模型，这在实际应用中存在较大难度。攻击者可能会采用更加隐蔽和复杂的攻击策略，这使得现有的攻击检测与防御技术难以有效应对。

系统防御措施的理论建立仍显不足。在设计有效且高效的防御措施之前，需要对智能攻击的行为模式有一定认知。然而，目前基于最优攻击行为设计的防御策略相对较少，相关的防御措施研究仍处于匮乏状态。这导致在实际应用中，防御者往往难以制定出针对性的防御策略，从而无法有效地抵御智能攻击。

此外，信息物理系统中应用的各种通信技术、网络协议和系统软件存在设计上的缺陷和无法避免的技术漏洞。这些漏洞可能被攻击者利用，从而发动针对信息物理系统的智能攻击。信息物理系统的网络架构和安全协议也并不统一，这使得网络之间的信息交换成为安全性的脆弱点，存在跨网攻击的风险。

智能攻击行为的动态演化是面临的一个挑战。攻击者会根据防御者的策略不断调整自己的攻击方式，这使得防御者需要不断更新和完善自己的防御策略，以适应攻击行为的变化。在信息物理系统中，攻击者和防御者之间的博弈过程往往非常复杂，攻击者可能采用多种攻击手段，而防御者则需要综合考虑多种防御措施，这使得攻防博弈的建模和求解变得非常困难。

制定防御策略时，还需要平衡系统的安全性和稳定性。过于严格的防御措施可能会导致系统稳定性下降，而过于宽松的防御措施则可能无法有效抵御攻击，这使得防御策略的制定变得非常棘手。

随着信息技术的不断发展，新的攻击手段和防御技术不断涌现，这给防御者带来了更新和升级的压力。防御者需要不断更新和升级技术体系，以适应新的安全威胁，但技术更新和升级往往需要投入大量的资源，这对一些资源有限的组织来说是一项巨大的挑战。

综上所述，面向信息物理系统的智能攻击感知与协同安全防御策略研究面临着诸多局限和挑战。为了应对这些挑战，需要不断加强技术研究、完善防御策略、提高系统的安全性和稳定性，并注重技术更新和升级。

1.4.2　态势评估方面

态势评估是对网络环境中引起网络态势变化的安全要素信息进行获取、理解，并评估网络安全状况，预测其发展趋势的过程。在信息物理系统中，态势评估是智能攻击感知与协同安全防御策略的重要组成部分，能够帮助及时发现潜在的安全威胁，为制定有效的防御措施提供科学依据。态势评估包括态势认知、态势理解和态势预测三个核心环节。首先，通过各类检测工具，收集多层次、多维度的系统安全性数据，包括网络安全防护系统的数据（如防火墙、WAF、IDS/IPS 等安全设备日志或告警等）、重要服务器和主机的数据（如服务器安全日志、进程调用和文件访问等）以及网络骨干节点数据。然后，对收集到的数据进行整合、分析和处理，以形成对网络当前安全态势的全面理解，利用大数据关联分析和机器学习等技术，从海量数据中提取有价值的信息，并识别潜在的安全威胁。最后，根据网络安全态势的历史信息和当前状态，对未来安全状况进行预测，态势预测是评估的基本目标，也是制定协同安全防御策略的重要依据。在信息物理系统中，态势评估的方法与技术可以包括基于数学模型的评估方法（如网络安全态势值的算法，通过数学计算得到反映某个时间段内网络安全状态的数值），基于机器学习的评估方法（利用机器学习算法识别潜在的安全威胁和攻击模式），以及基于信息物理融合的评估方法（将信息侧与物理侧的数据进行融合和分

析，以全面评估系统的安全态势)。态势评估在网络安全监测与预警、安全策略优化与调整以及应急响应与处置等方面具有广泛应用，通过综合运用多种评估方法和技术，可以实现对网络安全态势的全面、准确和实时评估，为制定有效的防御措施提供科学依据。

现有评估模型与方法

智能攻击感知方法包括基于信息物理关联状态挖掘的动态权值集成孤立森林模型和基于观测器方法的攻击检测。基于信息物理关联状态挖掘的动态权值集成孤立森林模型通过挖掘电力 CPS 在稳态运行阶段信息侧状态与物理侧状态的关联关系，应用无监督学习和集成学习方法，构建孤立森林子树模型和集成森林模型，并通过遗传算法优化集成孤立森林权重组合，最终构建稳定的攻击事前感知模型，以感知潜伏的信息侧攻击活动。基于观测器方法的攻击检测则是针对信息物理系统中潜在攻击的特点和策略，采用观测器方法进行攻击检测。这类方法通常基于系统状态估计，通过比较观测到的系统输出与预期输出之间的差异来检测攻击。

协同安全防御策略方面，提出了信息物理协同的电力系统网络攻击纵深防御体系架构，基于电力 CPS 信息物理深度耦合的特性，提出信息物理协同的主动防御方法。通过分析电力 CPS 典型网络攻击事件，剖析防御难点和关键问题，构建了纵深防御体系。基于信息物理双侧信息的网络攻击协同辨识方法提出了电力 CPS 事件的完整状态表达序列建模方法，并提出特征序列挖掘方法，用于构建电力系统故障事件辨识模型。在此基础上，结合机器学习方法，提出了信息物理融合序列-数据联合驱动的网络攻击事中在线辨识方法，为电力 CPS 提供针对性的控制措施。信息物理协同应对网络攻击造成工程故障的紧急控制措施调整方案，则基于关联矩阵的电力 CPS 通用化建模方法分析网络攻击的影响，提出了考虑网络攻击的电力 CPS 预想故障集生成方法，并针对预想故障提出包含信息物理双层优化的策略调整方法，提供了可扩展的策略判断函数分析以评估策略的可行性，进而实现紧急状态下的网络攻击应对。

评估模型与方法方面，建立了业务重要性评价体系及量化规则，通过评估电力物联网节点的重要性，帮助确定关键节点和薄弱环节，从而制定针对性的防御策略。基于观测器方法的安全状态估计则通过比较系统实际状态与估计状态之间的差异，评估系统的安全状态，并采取相应的防御措施。此外，仿真模拟和实验验证用于评估智能攻击感知与协同安全防御策略的有效性，包括构建仿真模型、设置攻击场景、观察系统响应等步骤，以验证策略在实际应用中的可行性和效果。

综上所述，面向信息物理系统的智能攻击感知与协同安全防御策略研究涵盖了多种方法和模型，为信息物理系统的安全防护提供了有力的支持，提升了系统的安全性和可靠性。

评估指标的选择与应用

评估指标的选择包括多个方面。首先，攻击感知能力指标包括准确率、漏报率和误报率。准确率评估智能攻击感知系统正确识别攻击事件的能力，较高的准确率表明系统能够准确区分正常状态和攻击状态。漏报率衡量系统未能识别出实际攻击事件的比例，较低的漏报率能够确保系统捕捉到所有潜在的攻击。误报率评估系统错误地将正常状态识别为攻击状态的比例，较低的误报率有助于减少不必要的警报和响应成本。协同安全防御能力指标则包括防御成功率、响应时间和资源利用率。防御成功率衡量系统在受到攻击时能够成功阻

止或减轻攻击影响的能力，高防御成功率表明系统具有强大的防御能力。响应时间评估系统从检测到攻击到采取防御措施所需的时间，较短的响应时间有助于减少攻击造成的损害。资源利用率衡量系统在防御过程中使用的资源效率，高效的资源利用率意味着系统能够以较低的成本提供强大的防御能力。系统性能与可靠性指标包括可用性、稳定性和可扩展性。可用性评估系统在正常运行和受到攻击时保持可用性的能力，高可用性意味着系统能够持续提供稳定的服务。稳定性衡量系统在受到外部干扰（如攻击）时保持性能稳定的能力，稳定性是确保系统长期稳定运行的关键因素。可扩展性评估系统在面对新攻击或新威胁时能否容易地进行扩展和升级，良好的可扩展性有助于保持系统的长期有效性。

在评估指标的应用方面，首先需要根据所选的评估指标构建适用于信息物理系统的评估模型。这个模型应综合考虑各个指标的影响，并给出综合评估结果。随后，可以利用仿真软件或实验平台对智能攻击感知与协同安全防御策略进行模拟测试。通过调整参数和场景，观察不同评估指标的变化情况，并验证策略的有效性。根据评估结果，可以对智能攻击感知与协同安全防御策略进行性能优化和改进。针对评估中发现的弱点或不足，提出改进措施，以提高系统的整体安全性和可靠性。最终，将优化后的策略应用于实际的信息物理系统中，并收集运行数据和用户反馈。通过持续监测和评估系统的性能，不断调整和优化策略，以适应不断变化的威胁环境。

动态态势评估的挑战

评估指标的选择涉及多个方面。首先，攻击感知能力指标包括准确率、漏报率和误报率。准确率评估智能攻击感知系统正确识别攻击事件的能力，较高的准确率表明系统能够准确区分正常状态和攻击状态。漏报率衡量系统未能识别出实际攻击事件的比例，较低的漏报率能够确保系统捕捉到所有潜在的攻击。误报率评估系统错误地将正常状态识别为攻击状态的比例，较低的误报率有助于减少不必要的警报和响应成本。协同安全防御能力指标则包括防御成功率、响应时间和资源利用率。防御成功率衡量系统在受到攻击时能够成功阻止或减轻攻击影响的能力，高防御成功率表明系统具有强大的防御能力。响应时间评估系统从检测到攻击到采取防御措施所需的时间，较短的响应时间有助于减少攻击造成的损害。资源利用率衡量系统在防御过程中使用的资源效率，高效的资源利用率意味着系统能够以较低的成本提供强大的防御能力。系统性能与可靠性指标包括可用性、稳定性和可扩展性。可用性评估系统在正常运行和受到攻击时保持可用性的能力，高可用性意味着系统能够持续提供稳定的服务。稳定性衡量系统在受到外部干扰（如攻击）时保持性能稳定的能力，稳定性是确保系统长期稳定运行的关键因素。可扩展性评估系统在面对新攻击或新威胁时能否容易地进行扩展和升级，良好的可扩展性有助于保持系统的长期有效性。

在评估指标的应用方面，首先需要根据所选评估指标构建适用于信息物理系统的评估模型。该模型应综合考虑各个指标的影响，并给出综合评估结果。随后，可以利用仿真软件或实验平台对智能攻击感知与协同安全防御策略进行模拟测试。通过调整参数和场景，观察不同评估指标的变化情况，并验证策略的有效性。根据评估结果，可以对策略进行性能优化和改进。针对评估中发现的弱点或不足，提出改进措施，以提高系统的整体安全性和可靠性。最终，将优化后的策略应用于实际的信息物理系统中，并收集运行数据和用户反馈。通过持续监测和评估系统的性能，不断调整和优化策略，以适应不断变化的威胁环境。

1.4.3 安全防御方面

主要安全防御技术与手段

感知层的安全防御技术包括加密与认证技术和入侵检测与防御系统。在感知层，由于传感器等物理设备通常部署在无人监管的环境中，容易受到攻击。因此，采用加密技术对传感器采集的数据进行加密，可以确保数据在传输过程中的安全性。同时，通过身份认证技术，确保只有合法的设备或用户才能访问或修改数据，从而防止未经授权的访问。入侵检测与防御系统在感知层的部署，能够实时监测和识别潜在的攻击行为，如数据篡改、信息窃听等，并采取相应的防御措施，例如阻断攻击源或报警。

在数据传输层，安全路由机制是确保数据完整性和机密性的重要手段。采用安全路由机制，可以避免数据在传输过程中被恶意篡改或泄露。安全路由机制可以包括路径选择、数据加密、数据完整性校验等措施。此外，数据加密技术可以确保传输过程中的机密性，而通过完整性验证技术，则能够确保数据在传输过程中没有被篡改，从而保证数据的可靠性。

在应用控制层，访问控制与权限管理技术能够限制用户对系统资源的访问权限，防止未经授权的访问和操作。常见的控制策略包括基于角色的访问控制和基于属性的访问控制等。同时，通过安全审计与日志管理技术，可以记录并分析用户对系统的操作行为，及时发现和响应潜在的安全威胁。这些措施有助于追踪和定位攻击行为，为后续的防御措施提供依据。

协同安全防御策略则包括跨层协同防御、主动防御与弹性恢复，以及智能安全分析与预警。信息物理系统是一个复杂的系统，各个层次之间紧密相关。因此，采用跨层协同防御策略，将感知层、数据传输层和应用控制层的安全防御措施相互结合，形成一个完整的防御体系，这包括信息共享、协同检测和协同响应等措施。除了被动地防御攻击外，主动防御策略也同样重要，如定期更新安全策略、进行安全漏洞扫描等，以发现并修复潜在的安全隐患。在攻击发生时，还需要采取弹性恢复策略，如备份恢复和故障切换等，确保系统的连续性和可用性。最后，利用人工智能和大数据技术，对系统的安全状态进行智能分析和预警，通过建立安全模型、挖掘安全规律、预测安全趋势等方式，能够及时发现潜在的安全威胁，并采取相应的防御措施。

防御体系的构建与优化

在构建防御体系时，首先需要制定主动防御策略。这包括对网络攻击行为的实时弹性防御，通过避免、转移或降低信息系统面临的风险，确保电力物联网的安全稳定运行。网络安全风险评估是防御体系建设的基础，通过评估资产威胁和发生危险事件的概率，可以对网络安全环境和现状有充分的认知，为制定有效的网络安全措施提供技术支撑。此外，针对信息物理系统的特点，需要构建信息物理协同的纵深防御体系，该体系包括多个层次的防御措施，如网络层的安全防护、系统层的安全监测、数据层的安全加密等，以确保系统的全面安全。智能攻击感知方法也应被引入，通过基于信息物理关联状态挖掘的动态权值集成孤立森林模型等方法，实现对潜在攻击活动的实时监测和预警。

在防御体系的优化方面，首先要加强信息物理系统之间的协同防御机制。通过信息侧与物理侧的紧密配合，可以实现对攻击行为的快速响应和有效防御。同时，不断推动安全防御技术的创新与升级，适应不断变化的网络攻击手段，例如引入更先进的入侵检测系统、防火墙技术、数据加密技术等，以提升系统的安全防护能力。建立并完善应急响应机制也是

至关重要的。这包括制定详细的应急预案、建立应急响应团队以及进行应急演练等，确保在网络攻击发生时能够迅速做出反应并恢复系统的正常运行。此外，防御体系的有效性和稳定性需要通过持续的安全监测与评估来保证。通过定期的安全检查、漏洞扫描和风险评估等手段，及时发现并修复系统中的安全隐患，确保防御体系始终处于最佳状态。最后，人员培训和意识提升也不可忽视。通过提高相关人员的安全操作技能、风险识别能力和应急处理能力，可以确保他们在日常工作中严格遵守安全规范，共同维护系统的安全稳定。

多层次防御策略的应用

多层次防御策略是指在信息物理系统中，通过构建多个层次的防御措施，形成互补和协同的安全防护体系。这些层次包括网络层、系统层、数据层和应用层等，每个层次都有其特定的防御目标和手段。通过不同层次的防护措施，可以有效提升系统的安全性，防止不同类型的攻击。

在具体应用中，网络层的防御主要包括防火墙和入侵检测系统。在网络入口处部署防火墙可以有效阻止未经授权的访问和数据传输。同时，通过入侵检测系统，实时监测网络流量中的异常行为，及时发现潜在的网络攻击。为了确保数据的机密性和完整性，网络层还采用安全协议（如 SSL/TLS）进行数据加密，并通过身份认证技术验证用户或设备身份，防止假冒攻击。

在系统层的防御中，定期对系统进行加固是非常重要的。这包括更新系统补丁、关闭不必要的端口和服务等，以减少系统漏洞的存在。同时，建立漏洞管理机制，及时发现并修复已知漏洞。在访问控制与权限管理方面，严格的访问控制策略能够限制用户或设备的访问权限，确保只有授权的用户或设备才能访问系统资源。

数据层的防御则侧重于数据加密和备份。对敏感数据进行加密存储，有助于防止数据泄露。同时，建立数据备份机制，确保在数据丢失或损坏时能够迅速恢复。通过数据审计与监控，记录数据的访问和操作日志，可以监控数据的流动和变化，及时发现异常行为并采取必要的措施。

在应用层的防御中，安全测试与加固是关键。在应用上线前进行安全测试，有助于发现潜在的安全漏洞并修复。同时，通过对应用的加固处理，可以提高应用的抗攻击能力。智能攻击感知技术，如基于机器学习的异常检测模型，可以实时监测应用中的异常行为，一旦检测到攻击行为，立即触发响应机制，采取相应措施进行防御。

为了确保多层次防御策略的有效性，所有层次之间需要相互协同与整合。信息共享机制能够确保各个层次之间的安全信息能够实时传递，增强整体防御能力。通过联动机制，当某一层次检测到攻击行为时，能够迅速触发其他层次的防御措施。此外，根据实际应用场景和安全需求，对多层次防御策略进行优化和调整，以确保防御体系在不断变化的威胁环境中始终保持有效。

通过多层次防御策略的应用，能够显著提高信息物理系统的安全防护能力。构建互补和协同的防御体系，可以有效抵御来自不同层面的网络攻击。同时，通过持续的安全监测和评估，及时发现并修复系统中的安全隐患，确保系统的长期安全与稳定运行。

1.4.4 单智能体态势感知技术的使用

在单智能体态势感知技术中，整个系统由一个智能体负责数据的收集、分析、评估和响应。这种方式适用于规模较小、结构相对简单的信息物理系统。智能体通过传感器、设备和信息系统收集与领域相关的数据，包括但不限于声音、图像、视频、地理位置等。随后，利用数据分析算法和模型，对收集到的数据进行处理与分析，提取出有用的信息和知识。基于处理后的数据，智能体进行态势评估，判断当前系统的安全状态，并预测潜在的安全威胁。最后，根据评估结果，智能体制定相应的安全策略，并触发安全响应机制，如报警、隔离等，以应对可能的威胁。

1.4.5 多智能体态势感知技术的使用

对于规模较大、结构复杂的信息物理系统，多智能体态势感知技术可能更为合适。在这种方式中，多个智能体协同工作，共同完成数据的收集、分析、评估和响应。根据系统的结构和功能，多个智能体进行分工，每个智能体负责特定区域或特定功能的数据收集和分析。各智能体分别收集各自负责区域的数据，并通过信息共享平台进行数据的共享和交流。多个智能体协同工作，对收集到的数据进行综合分析和评估，以更准确地判断系统的安全状态。基于评估结果，多个智能体共同制定安全策略，并触发相应的安全响应机制。由于多个智能体可以相互协作，因此能够更快速地应对安全威胁。

1.4.6 单智能体与多智能体的比较

单智能体态势感知技术相对简单，适用于规模较小的系统；而多智能体态势感知技术则更为复杂，但能够处理更大规模、更复杂的系统。多智能体态势感知技术具有更好的可扩展性，可以随着系统的扩展而增加智能体的数量，从而保持系统的性能和安全性。在多智能体系统中，即使某个智能体出现故障或受到攻击，其他智能体仍然可以继续工作，从而提高系统的容错性和鲁棒性。

1.5 技术发展趋势

1.5.1 人工智能在安全中的应用

人工智能 (AI) 作为一种变革性技术，正展现出其在安全领域的巨大潜力和价值。通过快速处理数据并进行预测分析，AI 能够完成从自动化系统到保护信息的多项任务，显著提升安全防护能力。

在安全风险的预警与分析中，AI 技术发挥着重要作用。利用机器学习和深度学习等算法，AI 系统可以对大量安全事件的数据进行挖掘和分析，识别并预测潜在的安全风险。例如，通过机器学习算法对网络流量进行分类和识别，AI 能够发现潜在的网络攻击行为；深度学习算法则能对网络日志进行分析，揭示潜在的安全漏洞。这些技术不仅提高了安全预警的准确性，还能显著提升响应的速度。

人工智能技术在安全策略的规划与优化方面也显示出了明显优势。通过优化算法和决策树等方法，AI 能够对现有的安全策略进行评估与优化，找出其中的弱点和优化空间，帮

助企业和政府机构更好地制定和实施安全策略。这不仅提高了安全防护水平，还降低了安全运营成本。

在安全事件的处理与响应中，AI 同样扮演着重要角色。借助自然语言处理和图像处理等方法，AI 能够快速分析和处理安全事件。例如，通过自然语言处理技术，AI 可以迅速分析安全事件报告；利用图像处理技术，AI 能够及时发现安全监控视频中的异常行为并发出预警。这些技术提高了安全事件响应的速度，也增强了安全防护的智能化水平。

生物特征识别与身份认证是 AI 技术应用最成功的信息安全领域之一。通过深度学习技术，AI 能够显著提高人脸、语音和指纹等生物特征的识别率。目前，人脸识别的准确率已达到 99

在漏洞检测和恶意代码分析方面，AI 技术同样具有显著优势。AI 系统能够模拟大量的攻击技术模式，通过学习人类已有经验或全新的样本空间，提高漏洞检测的全面性、准确性和时效性。在恶意代码分析中，AI 通过数据挖掘和机器学习，可以检测并预警恶意代码，从而有效防止其传播和危害。

自动化渗透测试和安全运营是 AI 技术在安全领域的另一重要应用。AI 通过模拟黑客攻击行为，进行自动化渗透测试，发现系统中的漏洞和弱点，并提供有效的修复建议。在安全运营方面，AI 能够辅助安全分析人员分析数据，快速发现安全事件，并自动完成分析和响应，降低安全运营成本，提高效率和准确性。

此外，AI 技术还可用于数据分类分级和隐私保护。通过对数据进行分类和分级，AI 可以根据数据的敏感性制定相应的安全策略和控制措施，保护重要数据免受攻击和泄露，确保系统的安全性和稳定性。在提升网络安全的同时，AI 技术的应用必须严格遵守数据隐私法规，开发隐私保护技术以防止隐私泄露或数据滥用。

1.5.2　区块链技术的潜力

区块链技术，作为一种新兴的具有特殊数据结构的信息基础设施，自诞生以来便展现出巨大的潜力和广泛的应用前景。其核心特性之一是去中心化的结构，这种结构使得数据不再依赖于单一的中央机构进行验证和存储，而是由网络中的多个节点共同维护。这不仅提高了数据的安全性和可靠性，还极大地降低了数据被篡改或删除的风险。通过区块链技术，人们可以建立全新的信任机制，无需依赖传统的信任中介，从而降低交易成本，提高交易效率。

区块链上的数据一旦写入，便无法被篡改或删除，这一特性为数据的真实性和完整性提供了强有力的保障。与此同时，区块链的透明度也得到提升，所有交易记录都是公开可查的，极大地防止了欺诈和腐败行为的发生。在金融、供应链管理等领域，区块链技术的这一特性尤为重要，它能够确保交易的合法性和真实性，提高整个行业的透明度和公信力。

智能合约是区块链技术的另一项重要创新。它以计算机代码形式存在，可以在满足特定条件时自动执行。通过智能合约，可以建立更加高效、自动化且可信的交易系统，交易过程无需人工干预即可完成。这不仅降低了交易成本和时间，还提高了交易的准确性和安全性。未来，智能合约有望在金融、法律、医疗等多个领域发挥重要作用。

区块链技术的应用前景并不仅限于金融领域，它在供应链管理、知识产权保护、医疗健

康等多个领域也展现出广泛的潜力。在供应链管理中，区块链能够实时追踪商品的来源和流向，确保产品的质量与安全；在知识产权保护方面，区块链为创作者提供去中心化的版权注册与追踪机制，保护其权益；在医疗健康领域，区块链有助于确保患者数据的安全性与隐私性，提高医疗服务的效率和质量。

作为数字化转型的重要推动力量，区块链技术正在加速各行各业的产业升级。通过区块链，企业能够实现数据的共享与协同，从而提高生产效率与运营效率；同时，区块链还可以降低企业的运营成本与风险，提升企业的竞争力和可持续发展能力。随着区块链技术的不断成熟和普及，它将为更多行业带来革命性的变革。

1.5.3 自动化防御系统的发展

自动化防御系统，作为网络安全领域的重要组成部分，近年来得到了快速发展。这些系统利用先进的技术手段，实现了对网络攻击的快速响应和有效防御。其起源可以追溯到网络安全威胁日益严峻的背景下。随着网络技术的不断发展，网络攻击的手段和方式变得越来越复杂和多样化，传统的人工防御方式已经无法满足日益增长的网络安全需求，因此，自动化防御系统应运而生。

自动化防御系统的发展经历了多个技术阶段，从最初的基于规则的防御系统，到后来基于统计学和机器学习的智能防御系统。这些系统利用了多种技术方法，其中包括传感器技术，通过部署在网络中的传感器实时监测网络流量和行为模式，为防御系统提供数据支持；规则匹配与过滤技术，通过预设规则库对网络流量进行匹配和过滤，识别和阻止潜在的恶意活动；统计学方法，利用统计学原理对网络流量进行分析和建模，发现异常行为和潜在威胁；以及机器学习与人工智能技术，通过训练机器学习模型，对网络流量进行智能分析和预测，提高防御系统的准确性和效率。

自动化防御系统广泛应用于企业网络、数据中心、云计算平台等多个领域。它们能够实时监测和响应网络攻击，有效降低攻击的成功率和影响范围。同时，自动化防御系统还能提供详细的日志记录和审计信息，为安全团队提供有力的证据支持和调查手段。然而，尽管这些系统取得了显著成效，但仍面临一些挑战。例如，误报率和漏报率较高，增加了企业在处理安全问题上的成本；缺乏自适应能力，难以应对不断变化的新型攻击手法；以及有限的审计记录功能，限制了安全团队对潜在安全隐患的深入调查。

未来，自动化防御系统将继续朝着智能化、高效化和集成化的方向发展。随着人工智能和大数据技术的不断发展，自动化防御系统将具备更强的自学习和自适应能力，能够根据环境和任务的变化进行智能调整和优化。同时，这些系统将与互联网、云计算等技术相结合，实现对系统的远程监控和管理，进一步提高系统的灵活性和可扩展性。

在学术研究领域，自动化防御系统的发展也得到了广泛关注。许多学者和研究机构致力于研究新的算法和技术，以提高防御系统的性能和准确性。例如，利用深度学习技术进行网络流量分析和预测，利用强化学习技术进行策略优化和自适应调整等。这些研究不仅推动了自动化防御系统的发展，也为网络安全领域的学术研究提供了新的思路和方法。

2 参考文献

[24, 4, 3, 22, 11, 27, 26, 2, 9, 20, 14, 21, 28, 25, 23, 15, 16, 12]

[17, 8, 10, 7, 6, 1, 19, 13, 18, 5, ?, ?, ?, ?, ?, ?, ?, ?, ?]

3 研究目标

3.1 攻击感知能力的提升

信息物理系统的安全性在国家关键基础设施和经济活动中扮演着核心角色。然而，随着攻击技术的不断升级，传统的安全防护手段已难以有效应对智能化、多样化的新型攻击。这些攻击通常具有隐蔽性强、持续性高和适应性强等特征，使得及时、准确地感知攻击变得异常困难。基于此，本研究针对当前攻击感知中的不足，提出一系列具体目标，以期构建一个更全面、精准、自适应的攻击感知系统，从而增强信息物理系统的整体安全性。研究内容主要包括以下几个方面：

针对攻击手段的多样性，本研究将从网络流量、系统日志、设备状态、环境数据等多维度建立综合感知模型。该模型将结合深度学习与统计分析技术，全面分析各类数据特征，以识别已知和未知的攻击行为。同时，应用数据增强与对抗训练，提升模型在复杂攻击场景下的鲁棒性，确保其在异常环境中仍能有效识别潜在威胁。

威胁情报作为攻击感知中的关键数据来源，可帮助系统及时更新攻击模式和规则。本研究将探索动态威胁情报的实时获取和处理方法，利用流数据处理与分布式计算，增强系统面对新兴威胁时的响应速度。通过人工智能技术的引入，使系统能够自主分析和提取威胁情报中的关键特征，动态适应新的攻击模式，从而提高攻击感知的准确性和时效性。

在实际应用中，误报与漏报不仅浪费大量资源，还可能忽视重要攻击。为应对这一问题，本研究拟采用智能化的误报过滤算法与分层告警机制，对感知模型的初步结果进行进一步优化。算法优化将基于聚类、分类和异常检测等技术的集成方法，以筛选高风险告警，降低误报与漏报，提升系统的防护效率与准确性。

针对不断变化的攻击技术，本研究提出一种自适应的攻击感知策略，使系统能够根据外部威胁环境的变化动态调整策略。具体而言，通过数据反馈机制不断更新模型参数，以确保系统在新威胁出现时具备快速响应和调整能力。此外，引入强化学习算法，基于历史攻击数据的学习，逐步优化系统的决策路径，提升威胁识别效率。

在实际部署中，攻击感知系统需要具备一定的容错性和集成性，以确保其在复杂环境下的稳定性与可靠性。因此，本研究将设计一种具备容错能力的系统架构，使系统在部分节点失效或数据缺失的情况下仍能正常运行。同时，探索将攻击感知模块与现有安全防护系统无缝集成的方法，构建一体化的安全防御体系，以确保在威胁发生时实现高效检测与响应。

3.2 态势评估精度的提升

在复杂网络环境下，提升态势评估精度是网络安全的关键任务之一。随着网络攻击手段的不断升级和攻击频次的增加，仅依靠传统防护机制难以有效应对各种新型威胁。数据融合和态势推理技术的引入，为提升态势评估的准确性提供了新的解决方案。这两种技术的结合，可以在动态、复杂的网络环境中实现对安全态势的实时监控与精确评估，帮助安全管理者及时识别潜在风险，进行有效防御决策。

首先，数据融合技术在态势评估中起到了至关重要的作用。不同数据源提供的信息存在异构性和不完整性，通过多源数据融合，能够去除冗余数据并填补信息缺口，进而形成更为全面、清晰的网络态势。多层次的数据融合可以结合传感器数据、网络流量、日志信息等多维数据，生成实时、准确的网络全貌图。此外，基于历史数据的时序分析也能提供未来态势的预测，为防御策略制定提供依据。

其次，态势推理技术是提升评估精度的另一关键技术。态势推理通过分析和解读融合后的数据，进一步挖掘出隐含的威胁模式和行为特征。尤其是基于机器学习和深度学习的态势推理方法，能够在海量数据中自动学习并识别复杂威胁模式，从而快速适应新的攻击手段。这一过程包括异常检测、行为分析以及威胁相关性分析等，通过这些环节的有机结合，可以从更高层次上识别出潜在的网络攻击路径和威胁传播模式。

通过将数据融合和态势推理技术相结合，态势评估系统可以实现动态、实时的安全风险评估，并具备较强的自适应能力。在复杂的网络环境中，态势评估的精准性和实时性显著提升，从而有效支撑安全防御决策的及时性和科学性。这一评估能力的提升不仅提高了对已知威胁的应对效率，更增强了应对未知攻击的敏捷性，为网络安全防御体系的构建提供了坚实的技术基础。

3.3 安全防御能力的增强

在当前信息物理系统（CPS）逐渐融入各行各业的背景下，提升其安全防御能力已成为迫切的需求。信息物理系统不仅承载着关键信息的传输与处理任务，同时与现实物理世界的互动也使其成为潜在攻击的高价值目标。为了应对多样化、复杂化的安全威胁，必须采用更加全面、深度的防御体系。这一防御体系不仅涵盖了传统的网络安全防护技术，还结合了人工智能、机器学习、大数据分析等新兴技术，以实现对攻击的智能识别、实时响应和动态防御。

当前的防御策略通常分为三个层次：感知层、传输层和应用层。感知层主要侧重于对物理设备和网络通信的监测，通过部署传感器、监控设备以及利用数据加密、身份认证等技术，保障数据的传输安全和设备的完整性。在这一层次，入侵检测系统（IDS）和入侵防御系统（IPS）扮演着重要角色，它们能够实时监测网络活动，并对可疑行为做出快速反应。然而，传统的基于规则或签名的检测方法在面对复杂且多变的攻击时存在明显局限。因此，近年来，越来越多的研究开始采用基于深度学习和强化学习的智能化检测方法，能够有效应对零日攻击、先进持续性威胁（APT）等复杂攻击。

在数据传输层，安全路由技术和数据完整性验证技术被广泛应用。通过加密传输、数据

哈希等手段，可以确保信息在传输过程中不会被篡改或泄露。此外，采用动态路由协议和容错机制，能够有效避免中间人攻击（Man-in-the-Middle, MITM）和拒绝服务攻击（DoS）。这一层次的安全防护不仅保证了数据的隐私性，还提高了系统在恶劣环境中的韧性，确保信息物理系统在遭遇攻击时能够保持基本的功能和服务。

在应用控制层，防御策略着重于权限管理、访问控制和审计跟踪等技术，以确保信息系统的资源不被未授权用户滥用。这一层面的防御措施不仅对防止内部威胁至关重要，还能有效识别和阻止恶意软件和内部攻击者对系统的破坏。通过结合人工智能算法和行为分析，系统可以实现对用户行为的实时监控和异常检测，及时发现潜在的攻击者。

总的来说，提升信息物理系统的安全防御能力是一个综合性的任务，需要从感知、传输和应用各个层次加强安全防护，并结合现代信息技术进行优化升级。近年来，许多学者提出了多层次安全防御框架，并验证了其在实际应用中的有效性。研究表明，通过多种技术的协同作用，可以显著增强信息物理系统在面对复杂攻击时的防护能力，同时提高系统的抗攻击能力、恢复能力和自适应能力。此外，智能化的防御策略通过机器学习和深度学习模型，实现了对潜在攻击的实时识别与预警。这类技术不仅能够提高系统对复杂攻击行为的检测准确率，还能够通过实时更新和自动学习提升系统的适应能力。防御系统的核心在于快速响应和协调联动，通过跨层次的信息共享和动态防护机制，确保在遭受攻击时能够迅速应对、限制攻击影响，并恢复系统的正常运行。

这些防御策略的实施旨在通过纵深防御结构来提升系统的整体安全性。感知层采用加密和身份认证技术以保护数据的机密性与完整性，数据传输层通过路径加密和安全路由技术防止数据泄露，应用控制层则通过严格的权限管理和审计机制限制未经授权的访问和操作。通过多层次、全方位的防护体系，信息物理系统的抗攻击能力得以显著增强，保障了系统在复杂和高风险环境中的稳定运行。

信息物理系统的安全防御能力建设需要采用多层次、全方位的策略，不仅依赖传统的网络安全措施，还需整合人工智能和智能化技术的创新应用。现代技术，如机器学习和深度学习，已在提高对复杂威胁的实时监测与快速响应方面展现出显著优势。这些技术的引入能够增强系统的检测准确性和适应性，确保其在威胁演化过程中具备动态调整与更新的能力。通过多种技术的协同作用，系统实现了从感知层到传输层，再到应用控制层的全面防护，增强了抵御攻击的能力以及恢复与自适应的性能。在复杂的网络环境中，这种多维度的防御体系有效提升了系统的稳定性和安全性，成为应对未来多样化安全挑战的重要技术支撑和战略基础。

3.4 协同防御机制的构建

在信息物理系统（CPS）的背景下，提升其安全防御能力已成为一个迫切的需求。CPS不仅承载着关键信息的传输与处理任务，而且与现实物理世界的互动使其成为潜在攻击的高价值目标。为了应对多样化、复杂化的安全威胁，必须采用更加全面、深度的防御体系。这一防御体系不仅涵盖了传统的网络安全防护技术，还结合了人工智能、机器学习、大数据分析等新兴技术，以实现对攻击的智能识别、实时响应和动态防御。

当前的防御策略通常分为三个层次：感知层、传输层和应用层。感知层主要侧重于对物

理设备和网络通信的监测，通过部署传感器、监控设备以及利用数据加密、身份认证等技术保障数据的传输安全和设备的完整性。在这一层次，入侵检测系统（IDS）和入侵防御系统(IPS）扮演着重要角色，它们能够实时监测网络活动，并对可疑行为做出快速反应。然而，传统的基于规则或签名的检测方法在面对复杂且多变的攻击时存在明显局限，因此，近年来越来越多的研究开始采用基于深度学习和强化学习的智能化检测方法，能够有效应对零日攻击、先进持续性威胁（APT）等复杂攻击。

在数据传输层，安全路由技术和数据完整性验证技术被广泛应用。通过加密传输、数据哈希等手段，可以确保信息在传输过程中不会被篡改或泄露。此外，采用动态路由协议和容错机制，能够有效避免中间人攻击（Man-in-the-Middle, MITM）和拒绝服务攻击（DoS)。

在应用控制层，防御策略侧重于权限管理、访问控制和审计跟踪等技术，以确保信息系统的资源不被未授权用户滥用。这一层面的防御措施不仅对防止内部威胁至关重要，还能有效识别和阻止恶意软件和内部攻击者对系统的破坏。通过结合人工智能算法和行为分析，系统可以实现对用户行为的实时监控和异常检测，及时发现潜在的攻击者。

总的来说，提升信息物理系统的安全防御能力是一个综合性的任务，需要从感知、传输和应用各个层次加强安全防护，并结合现代信息技术进行优化升级。近年来，许多学者提出了多层次安全防御框架，并验证了其在实际应用中的有效性。研究表明，通过多种技术的协同作用，可以显著增强信息物理系统在面对复杂攻击时的防护能力，同时提高系统的抗攻击能力、恢复能力和自适应能力。

此外，智能化的防御策略通过机器学习和深度学习模型，实现了对潜在攻击的实时识别与预警。这类技术不仅能够提高系统对复杂攻击行为的检测准确率，还能够通过实时更新和自动学习提升系统的适应能力。防御系统的核心在于快速响应和协调联动，通过跨层次的信息共享和动态防护机制，确保在遭受攻击时能够迅速应对、限制攻击影响，并恢复系统的正常运行。

这些防御策略的实施旨在通过纵深防御结构来提升系统的整体安全性，感知层采用加密和身份认证技术以保护数据的机密性与完整性，数据传输层通过路径加密和安全路由技术防止数据泄露，应用控制层则通过严格的权限管理和审计机制限制未经授权的访问和操作。通过多层次、全方位的防护体系，信息物理系统的抗攻击能力得以显著增强，保障了系统在复杂和高风险环境中的稳定运行。信息物理系统的安全防御能力建设需要采用多层次、全方位的策略，不仅依赖传统的网络安全措施，还需整合人工智能和智能化技术的创新应用。现代技术，如机器学习和深度学习，已在提高对复杂威胁的实时监测与快速响应方面展现出显著优势。

3.5 模型与算法的创新

在信息物理系统（CPS）的安全防御领域，模型与算法的创新是推动技术进步的核心。随着信息科学与技术的快速发展，CPS 已成为支撑新一轮产业变革的核心技术，其安全防御能力的提升显得尤为重要。在此背景下，创新的算法和模型的开发对于增强 CPS 的攻击感知和安全防御策略至关重要。

Zonouz 等人提出了安全导向的信息物理关联状态估计（SCPSE)，该方法通过构建攻

击图并移除可疑节点的量测值，以检测系统中存在的不良数据，并提供对系统真实状态的可靠估计。此外，信息物理安全评估技术（SOCCA）提供了信息元素与物理元素统一的形式化描述方法，根据信息物理意外事故的威胁程度来评估意外事件可能产生的影响。

Rahman 等人提出的协调变参防御（CPVD）方法，通过随机改变传输线阻抗和用于状态估计的传输线集合，增加系统的不确定性，从而阻碍攻击的执行。这种方法源自网络安全技术中的移动目标防御（MTD），通过不断改变系统配置来减少攻击面和增加攻击者探测系统漏洞的成本。基于系统模型融合的 CPS 综合安全防御方法将网络安全防御的思想和技术应用于物理系统的安全监控，构建出新的 CPS 综合安全防御方法，这包括协调变参防御和物理系统水印等技术。

随着深度学习和强化学习等技术的出现，CPS 能够处理更复杂的任务和问题，提高对复杂攻击行为的检测准确率，并能够通过实时更新和自动学习提升系统的适应能力。算法模型的创新和改进提高了 AI 系统的泛化能力，使得经过训练的模型能够更好地应对新的、未曾见过的数据和场景，从而在实际应用中取得更好的效果。

在 AI 领域的历史中，很多重要的技术突破都源于算法模型的创新，例如卷积神经网络(CNN)、循环神经网络（RNN）等模型的出现引领了一系列技术革新，大大提升了 AI 系统的性能。通过这些算法和模型的创新，CPS 在面对复杂攻击时的防护能力得到了显著增强，同时提高了系统的抗攻击能力、恢复能力和自适应能力。

最后，基于攻防博弈的网络防御决策方法和融合攻击图与博弈模型的网络防御策略生成方法也是本研究的重点。构建网络攻防微分博弈模型，设计攻防决策控制函数和收益积分函数，在求解鞍点控制策略的基础上给出最优防御策略。同时，将攻击图与博弈模型结合，引入强化学习算法 Minimax-Q Learning 设计网络主动防御策略生成方法，通过模拟实验验证算法的有效性和先进性。

3.6 系统实时性与可扩展性的提升

在信息物理系统（CPS）日益复杂的背景下，基于 CAN 总线的入侵检测成为保障车辆及工业物联网安全的关键环节。面对日益多样化的网络攻击手段，如何提升系统的实时性与可扩展性，确保在复杂多变的网络环境中既能迅速响应潜在威胁，又能随着系统规模的扩大和功能的增加而保持高效运行，成为当前研究的重点。

3.6.1 系统实时性提升的迫切性与挑战

实时性是入侵检测系统（IDS）的核心性能指标之一，它直接关系到系统能否在攻击发生的第一时间作出响应，从而有效阻止攻击的进一步扩散。在基于 CAN 总线的 CPS 中，由于车辆和工业设备的实时性要求极高，任何延迟都可能导致严重后果，如车辆失控、生产线停工等。因此，提升系统实时性不仅是技术上的需求，更是安全性的保障。然而，提升实时性面临着诸多挑战。首先，CAN 总线作为一种低速、低带宽的通信协议，其数据吞吐量有限，如何在有限的带宽内实现高效的数据处理和入侵检测是一个难题。其次，随着车辆和工业设备的智能化程度不断提高，CAN 总线上的数据量呈爆炸式增长，如何快速处理和分

析这些数据，准确识别出异常行为，对系统的计算能力提出了更高要求。最后，实时性还受到系统架构、算法效率、资源分配等多重因素的影响，需要综合考虑和优化。

3.6.2 系统可扩展性提升的必要性

可扩展性是确保系统能够随着需求变化而持续发展的关键因素。在基于 CAN 总线的 CPS 中，随着车辆和工业设备的智能化程度不断提高，新的功能和组件不断涌现，对系统的可扩展性提出了更高要求。可扩展性的提升意味着系统需要能够灵活地适应新的安全需求和技术发展。这要求系统具备模块化设计、插件化接口以及标准化协议等特性，以便方便地添加新的检测算法、安全策略以及硬件设备。同时，系统还需要具备弹性伸缩能力，能够根据系统负载和检测需求，动态调整计算资源和存储资源，以确保在高峰期能够高效运行，同时避免资源浪费。

3.6.3 持续优化与跨领域协作提升系统的实时性和可扩展性

为了持续提升基于 CAN 总线入侵检测的面向信息物理系统（CPS）的智能攻击感知与协同安全防御策略的实时性和可扩展性，建立持续监控和评估机制具有至关重要的意义。在高度互联且快速变化的 CPS 环境中，系统面临着来自内外部的多样化威胁。这些威胁可能源自恶意攻击、系统故障、数据泄露等多种原因，且其形态和手法不断演进。因此，持续监控和评估机制能够实时捕捉系统的运行状态和安全态势，及时发现并预警潜在的安全隐患和性能瓶颈。通过对系统关键指标如响应时间、吞吐量、资源利用率等的持续监测，可以确保系统在复杂多变的网络环境中保持高效稳定的运行，从而有效应对各种安全挑战。同时，持续监控和评估机制还为系统的持续优化提供了数据支持和决策依据。通过对历史数据的分析和挖掘，可以揭示系统性能变化的规律和趋势，发现潜在的性能瓶颈和安全隐患。这些分析结果可以为系统优化提供科学依据，指导开发者对系统进行针对性的改进和升级。例如，根据监控数据调整检测算法的参数、优化系统架构、增加新的安全策略等，以提升系统的实时性和可扩展性。此外，持续监控和评估机制还有助于提升系统的可维护性和可靠性。通过实时监控系统的运行状态和健康状况，可以及时发现并处理系统故障和异常，避免系统崩溃或数据丢失等严重后果。同时，定期的评估和审计可以确保系统的安全性和合规性，降低因系统漏洞或违规操作而引发的安全风险。

在基于 CAN 总线入侵检测的面向信息物理系统的智能攻击感知与协同安全防御策略的研究中，提升系统实时性与可扩展性具有深远的意义。这不仅是应对当前网络安全挑战的必要举措，更是推动 CPS 系统智能化、互联化发展的重要保障。通过提升系统实时性，可以确保系统在面临网络攻击时能够迅速作出响应，有效阻止攻击的进一步扩散，从而保护车辆和工业设备的安全运行。同时，通过提升系统可扩展性，可以确保系统能够灵活适应新的安全需求和技术发展，为未来的智能化、互联化发展奠定坚实基础。

3.7 跨领域应用推广

信息物理系统的安全防护技术并非局限于某一特定行业或领域，其技术成果具有广泛的适用性和推广潜力。当前，信息物理系统在智能制造、智能电网、智能交通、智慧城市等领域的应用已经取得了显著进展，并对社会的各个层面产生了深远影响。因此，将安全防护技术推广至这些领域，不仅能够提升各行业的安全性，还能推动跨行业的协同创新和安全防护体系的建设。通过在不同领域中的应用，研究成果能够实现知识和技术的迁移与共享，促进相关领域的协同防御能力和整体安全性。

以智能电网为例，智能电网作为现代能源管理和分配系统的核心，其运行依赖于信息物理系统的支持。随着电力需求和分配的日益智能化，电网面临的安全威胁也日益复杂。针对这一挑战，基于多层次防御的安全框架可以有效地监测电网中各个环节的异常，实时识别和隔离恶意攻击。利用智能攻击感知技术，能够动态调整电网的运行状态，确保在遭受攻击时，电网能够迅速切换到备用路径或自动恢复。类似的防御措施也可以应用于智能交通系统，通过实时监控交通流量、交通信号控制系统等，确保交通系统在面对网络攻击时的稳定运行。

在智慧城市建设中，信息物理系统被广泛应用于城市基础设施管理、环境监控和公共安全等多个领域。跨领域的安全防护技术，尤其是基于人工智能和大数据分析的智能攻击感知与防御策略，能够提高城市的综合安全管理能力。例如，在智慧城市的应急响应系统中，基于多源数据融合的态势感知系统可以在突发事件发生时，迅速评估城市安全态势并作出响应，确保公共安全。

此外，跨领域的安全防护技术还能够通过标准化和模块化的方式，推动不同领域之间的技术共享与协同。在智能电网和智慧城市等领域，虽然面临不同的应用场景和技术要求，但通过制定统一的安全标准和技术规范，不同系统之间可以实现信息共享和协同防御。通过推动技术标准化，能够有效降低各类信息物理系统的建设和维护成本，并增强系统的互操作性和安全性。

信息物理系统的安全防护技术能够在不同领域中提升整体安全水平，通过跨领域应用和技术推广，这些成果在更大范围内实现了知识与技术的共享，进一步增强了系统的协同防御能力和互操作性。通过推动技术标准化、政策引导和跨部门合作，这些技术不仅被有效应用于多个关键领域，还助力实现社会在信息安全方面的协同应对。这种技术的推广和应用契合了现代信息技术的发展趋势，为打造更安全、智能的社会环境提供了坚实基础和有力保障。

参考文献

[1] A. Ayodeji, Y.-k. Liu, N. Chao, and L.-q. Yang. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear Engineering and Technology*, 52(12):2687–2698, 2020.

[2] Bowen Hu, Chunjie Zhou, Yu-Chu Tian, Xiaoya Hu, and Xinjue Junping. Decentralized consensus decision-making for cybersecurity protection in multimicrogrid systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(4):2187–2198, 2021.

[3] Kaixing Huang, Chunjie Zhou, Yuanqing Qin, and Weixun Tu. A game-theoretic approach to cross-layer security decision-making in industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 67(3):2371–2379, 2020.

[4] Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuanghua Yang, and Yuanqing Qin. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(10):8153–8162, 2018.

[5] Xianting Huang, Jing Liu, Yingxu Lai, Beifeng Mao, and Hongshuo Lyu. Eefed: Personalized federated learning of execution & evaluation dual network for cps intrusion detection. *IEEE Transactions on Information Forensics and Security*, 18:41–56, 2023.

[6] Feng Jiang, Yunsheng Fu, B. B. Gupta, Yongsheng Liang, Seungmin Rho, Fang Lou, Fanzhi Meng, and Zhihong Tian. Deep learning based multi-channel intelligent attack detection for data security. *IEEE Transactions on Sustainable Computing*, 5(2):204–211, April–June 2020.

[7] Zizhi Jin, Qinhong Jiang, Xuancun Lu, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Phantomlidar: Cross-modality signal injection attacks against lidar. In *Network and Distributed System Security (NDSS) Symposium 2024*, pages 173–198, San Diego, CA, USA, February 2024.

[8] Soheil Khodayari, Thomas Barber, and Giancarlo Pellegrino. The great request robbery: An empirical study of client-side request hijacking vulnerabilities on the web. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 166–184, San Francisco, USA, May 2024.

[9] Xinge Li, Xiaoya Hu, Rongqing Zhang, Chunjie Zhou, Quan Yin, and Liuqing Yang. A model-driven security analysis approach for 5g communications in industrial systems. *IEEE Transactions on Wireless Communications*, 22(2):889–902, 2023.

[10] Xiulai Li, Jieren Cheng, Zhaoxin Shi, Jingxin Liu, Bin Zhang, Xinbing Xu, Xiangyan Tang, and Victor S. Sheng. Blockchain security threats and collaborative defense: A literature review. *Computers, Materials & Continua*, 76(3):2597–2629, 2023.

[11] Xuan Li, Chunjie Zhou, Yu-Chu Tian, and Yuanqing Qin. A dynamic decision-making approach for intrusion response in industrial control systems. *IEEE Transactions on Industrial Informatics*, 15(5):2544–2554, 2019.

[12] M. Ma, L. Han, and C. Zhou. Research and application of artificial intelligence based webshell detection model: A literature review, 2024.

[13] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz. Multi-source multi-domain data fusion for cyberattack detection in power systems. *IEEE Access*, 9:1–12, 2021.

[14] H. Sun, Y. Huang, L. Han, and C. Zhou. Few-shot detection of anomalies in industrial cyber-physical system via prototypical network and contrastive learning. *arXiv:2302.10601 [cs.CR]*, 2023.

[15] Jun Yang, Chunjie Zhou, Yu-Chu Tian, and Chao An. A zoning-based secure control approach against actuator attacks in industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 68(3):2637–2647, 2021.

[16] Jun Yang, Chunjie Zhou, Shuanghua Yang, Haizhou Xu, and Bowen Hu. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(5):4257–4267, 2018.

[17] Zhen Yin, Wei Wang, Xiaozhen Lu, and Zhisheng Yin. Multi-level collaborative defense strategies against malicious traffic in wireless edge networks. In *2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 185–190, Nanjing, China, January–June 2024.

[18] Bin Yuan, Maogen Yang, Zhen Xu, Qunjinming Chen, Zhanxiang Song, Zhen Li, Deqing Zou, and Hai Jin. Leakage of authorization-data in iot device sharing: New attacks and countermeasure. *IEEE Transactions on Dependable and Secure Computing*, 21(4):3196–3210, July–August 2024.

[19] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7):4362–4369, 2019.

[20] Qi Zhang, Chunjie Zhou, Naixue Xiong, Yuanqing Qin, Xuan Li, and Shuang Huang. Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46(10):1429–1444, 2016.

[21] Yue Zhao, Xin Du, Chunjie Zhou, and Yu-Chu Tian. Anti-saturation resilient control of cyber-physical systems under actuator attacks. *Information Sciences*, 608:1245–1260, 2022.

[22] Yue Zhao, Xin Du, Chunjie Zhou, Yu-Chu Tian, Xiaoya Hu, and Daniel E. Quevedo. Adaptive resilient control of cyber-physical systems under actuator and sensor attacks. *IEEE Transactions on Industrial Informatics*, 18(5):3203–3212, 2022.

[23] Yue Zhao, Chunjie Zhou, Yu-Chu Tian, and Yuanqing Qin. Composite finite-time resilient control for cyber-physical systems subject to actuator attacks. *IEEE Transactions on Cybernetics*, 53(2):1063–1077, 2023.

[24] Yue Zhao, Chunjie Zhou, Yu-Chu Tian, Yuanqing Qin, and Xiaoya Hu. l_2 gain secure control of cyber-physical systems under fast time-varying cyber attacks. *IEEE Transactions on Network Science and Engineering*, 9(2):648–659, 2022.

[25] Yue Zhao, Chunjie Zhou, Yu-Chu Tian, Jianhui Yang, and Xiaoya Hu. Cloud-based underactuated resilient control for cyber-physical systems under actuator attacks. *IEEE Transactions on Industrial Informatics*, 19(5):6317–6325, 2023.

[26] Chunjie Zhou, Bowen Hu, Yang Shi, Yu-Chu Tian, Xuan Li, and Yue Zhao. A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE*, 109(4):517–541, 2021.

[27] Chunjie Zhou, Shuang Huang, Naixue Xiong, Shuang-Hua Yang, Huiyun Li, Yuanqing Qin, and Xuan Li. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(10):1345–1360, 2015.

[28] Chunjie Zhou, Xuan Li, Shuanghua Yang, and Yu-Chu Tian. Risk-based scheduling of security tasks in industrial control systems with consideration of safety. *IEEE Transactions on Industrial Informatics*, 16(5):3112–3123, 2020.