CCF YOCSEF

工业互联网安全技术论坛-人工智能技术如何成为工业互联网安全的“新战力”

人工智能深度加强工业互联网安全

中国科学院沈阳自动化研究所

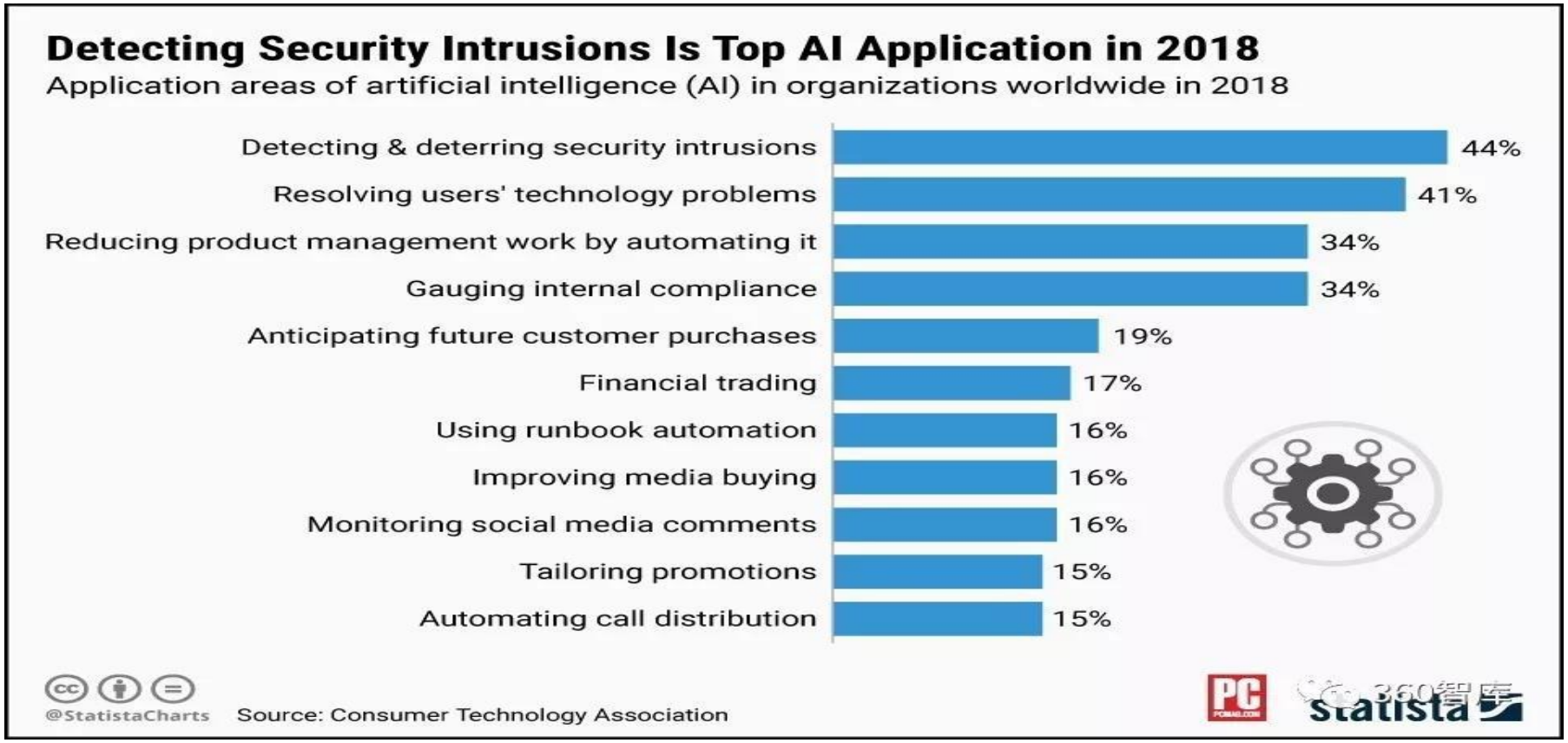
尚文利

2019年09月

提　纲

1. 人工智能与网络安全
2. 人工智能深度加强工业互联网安全
3. 工业互联网安全现状与未来展望

人工智能用于网络安全已经成为主流



2019年4月24日，美国消费者技术协会公布的一组数据显示，2018年，人工智能技术在网络安全领域内的应用频次（44%）远高于其他领域。随着深度学习算法的使用，人工智能正在引领安全互联网的潮流。

人工智能技术适合网络安全任务自动化

- **人工智能特别适合执行网络安全任务，并使其自动化，**比如利用深度学习算法来发现数据中的模式，检测易受攻击的用户行为，以及预测安全趋势。
- **最终的目的**是让人工智能在幕后工作，即在预测、检测和响应恶意威胁方面完全自主，并提供无缝的前端和终端用户体验。

数据源：https://mp.weixin.qq.com/s/R8-ZI4RSMdYhIJv6cC4sWA。

工业互联网已然成为黑客攻击和网络战的重点目标

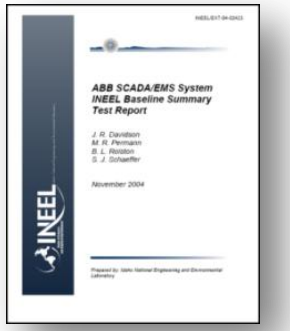
国际、国内政府高度重视工业互联网信息安全

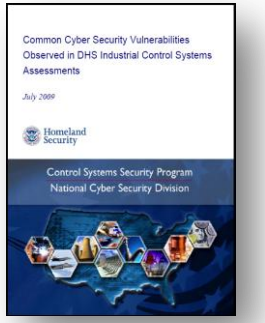
国际

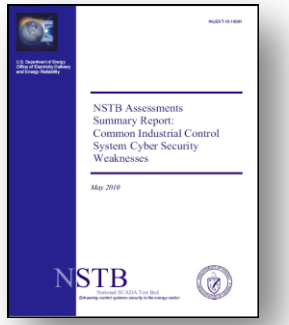
①2017年美国总统签署《增强联邦政府网络与关键性基础设施网络安全》行政令；
②欧盟应急响应组（ICS-CSIRT）承担“欧洲关键基础设施保护项目（EPCIP）”；
③美国国家标准与技术研究院（NIST）制定SP800-82、800-53等工控安全系列标准；
④国际电工委员会（IEC）制定IEC62443工控安全系列标准

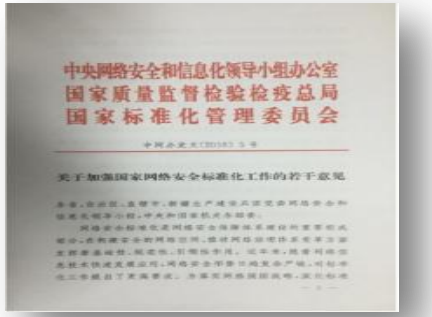
国内

①2017年中国“十九大”报告强调“开展关键信息基础设施保护”；
②中国工信部印发《工业控制系统信息安全行动计划（2018-2020年）》；
③国家工业信息安全产业发展联盟发布《工业信息安全态势白皮书》，指导工业信息安全发展方向；
④《中国制造2025》提出要“加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系”









国际、国内政府高度重视人工智能技术

人工智能已成为国家安全重要影响因素，捍卫网络空间需要人工智能。

- 截至2019年2月，至少有**27个国家**制定了**人工智能**相关的战略或计划，与此同时人工智能的相关投入也在大幅增长。

美国于2019年2月11日签署名为《保持美国在人工智能领域领导地位》的行政令，宣布启动“美国人工智能行动计划”。

欧盟在2018年4月出台人工智能政策文件《欧洲人工智能》，希望联合各成员国和私企加大投资力度，力争使欧盟到2020年总投资达到200亿欧元。

中国于2017年7月推出《新一代人工智能发展规划》，力争到2030年达到世界领先水平。

新加坡、俄罗斯等国家加强对人工智能等产业的投资和支持。

工业互联网的通信网络特点适合人工智能技术

- 工业互联网通信网络特点：“状态有限”和“行为有限”。

“状态有限”是指工业互联网通信具有规律性和稳定性的特点，即规则的通信流。

“行为有限”是指工业互联网具有较固定的行为特征和可预测的行为模式，从而简化模型的描述。就具体通信设备而言，通常重复执行其有限的操作。

人工智能技术能够深度加强工业互联网安全！！！

提　纲

1. 人工智能与网络安全
2. 人工智能深度加强工业互联网安全
3. 工业互联网安全现状与未来展望

示例：基于人工智能的工业控制系统入侵检测技术

- 传统IT安全技术不能直接用于工业控制系统，其采用专有的通信协议或规约（如Modbus、DNP3、IEC61870-5-104、MMS、GOOSE 等），同时协议规约实现具有多样性。
- 工业控制系统协议中的安全问题可分为两类：一类是协议自身的设计和描述引起的，另一类是协议的实现引起的。
- 针对工业控制系统的攻击行为主要以专有的通信协议或规约漏洞为突破口，对系统造成威胁，因此入侵检测技术也应以工控系统的专有协议解析和通信建模分析为基础进行研究。

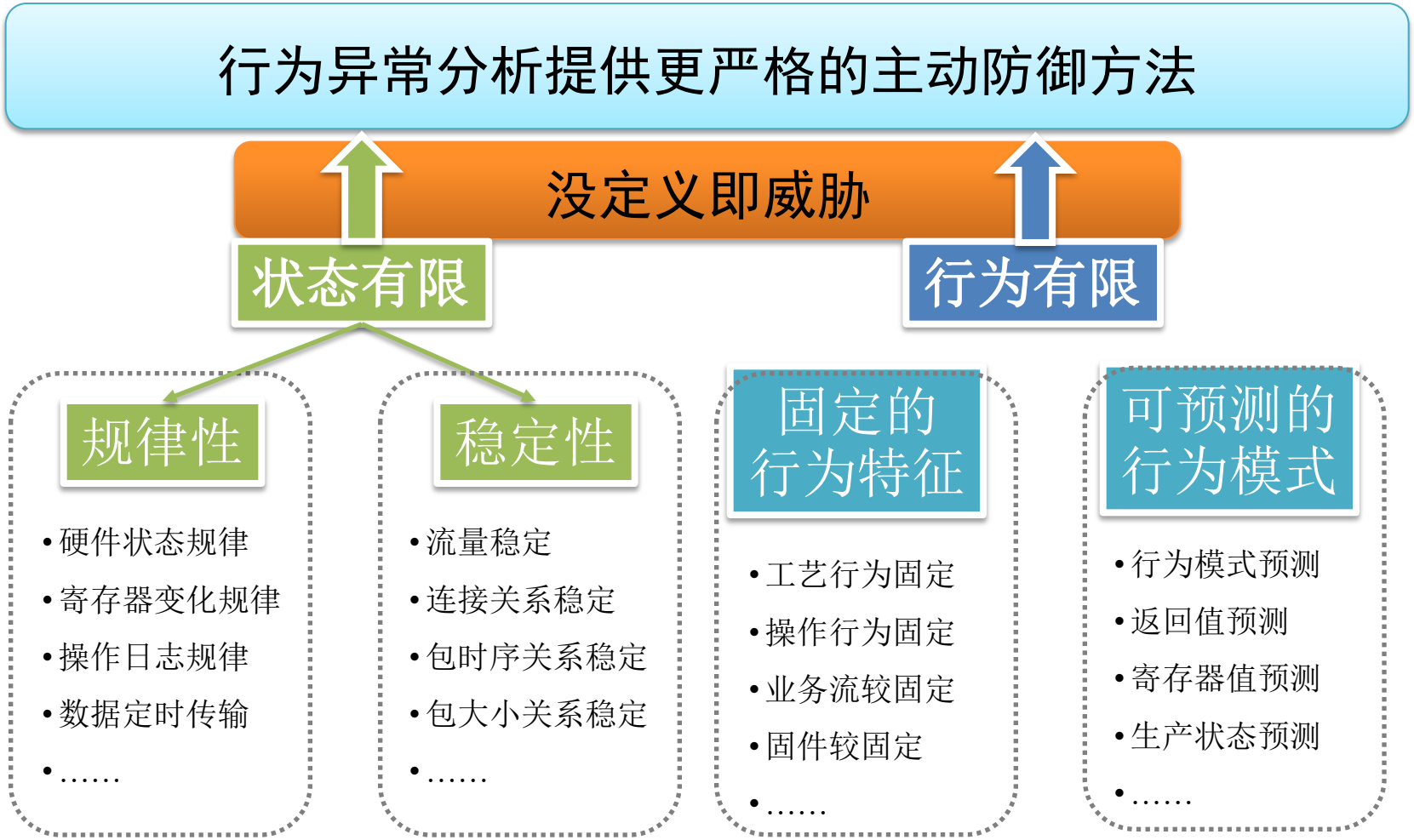
示例：基于人工智能的工业控制系统入侵检测技术

主要检测方法：

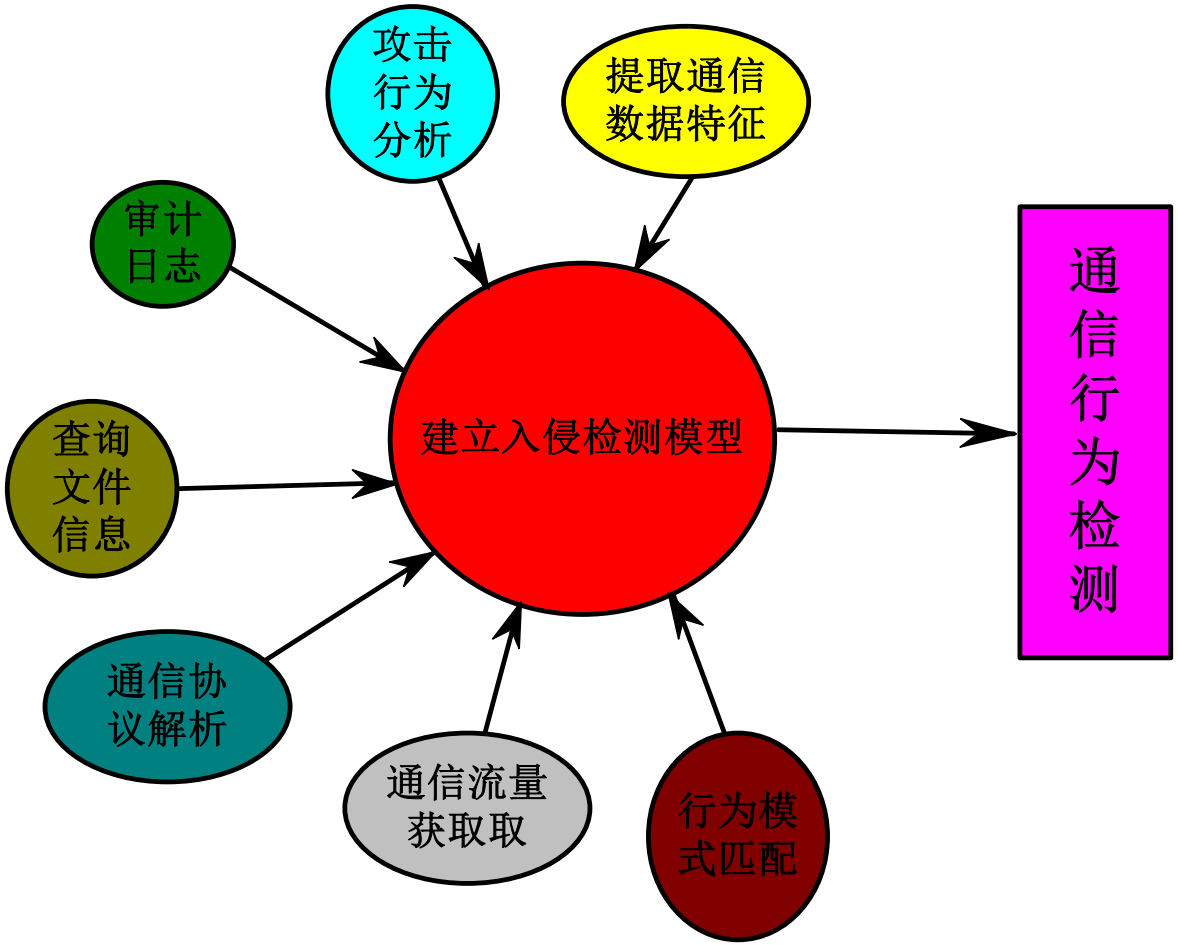
- 基于统计
- 基于知识
- 基于机器学习
  - 人工神经网络
  - 模糊逻辑
  - 贝叶斯网络
  - 遗传算法
  - 聚类算法（模糊C均值聚类，FCM）
  - 支持向量机（SVM）
  - …… …… …… …… …… ……

示例：基于人工智能的工业控制系统入侵检测技术

■ 工业控制系统特点：“状态有限”和“行为有限”



示例：基于人工智能的工业控制系统入侵检测技术

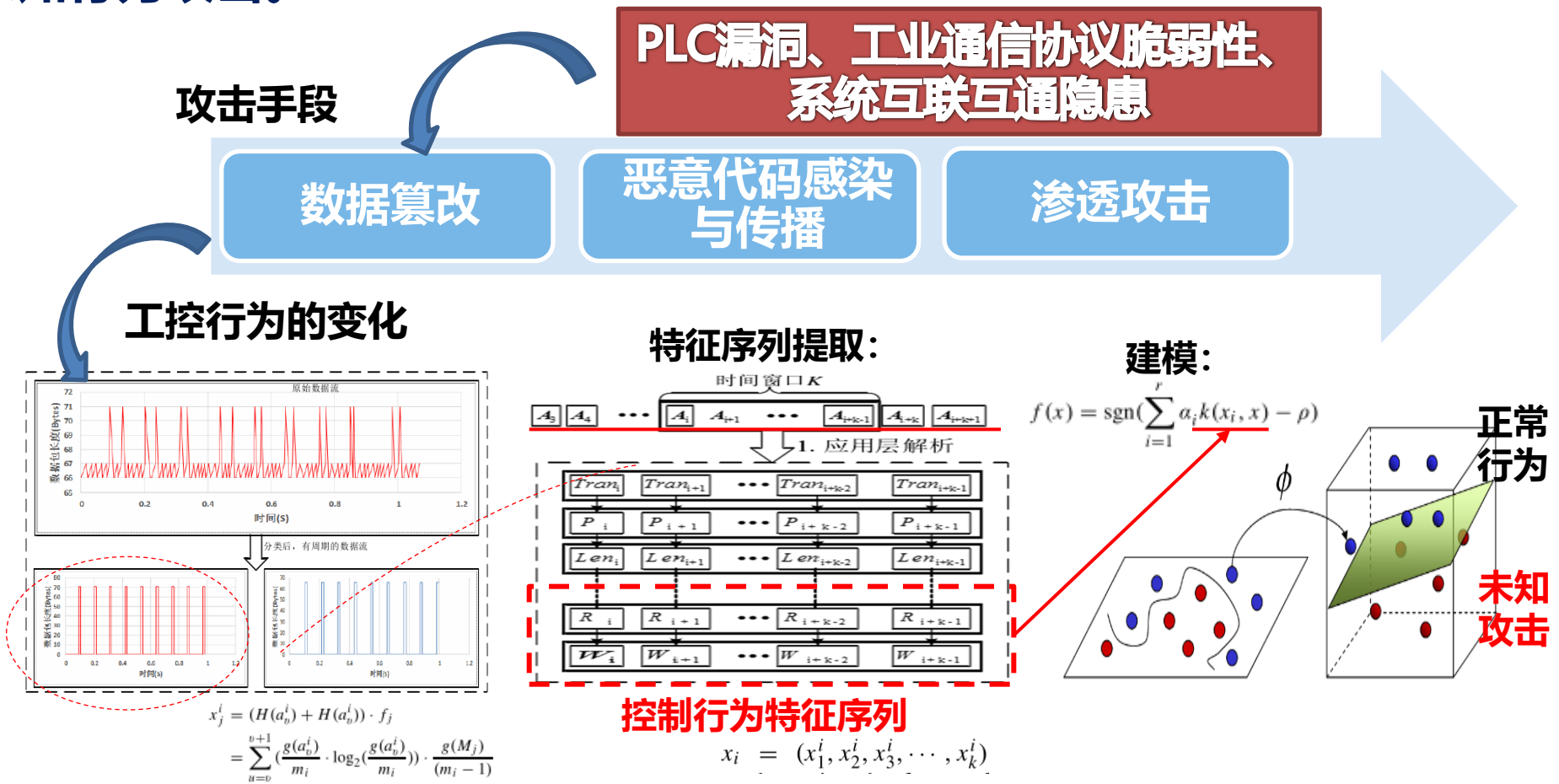


主要检测特征对象：

- 工控通信协议的数据特征
- 异常行为模式的数据特征
- 工控系统模型参数特征
- 通信流量大小特征
- 通信时间间隔模式特征

示例：基于人工智能的工业控制系统入侵检测技术

- **一种研究思路**：根据工控系统**控制行为特征**，对通信进行深度行为分析，判别是否存在未知行为攻击。



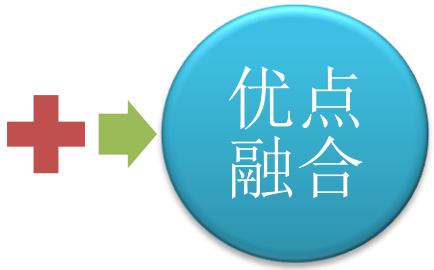
示例：基于人工智能的工业控制系统入侵检测技术

状态有限——基于“白名单”规则的异常检测方法

通过对工控系统通信网络数据进行规律学习，生成匹配规则，为入侵检测系统基于规则匹配检测异常提供理论和技术支撑。

能够有效检测单条通信协议的异常行为。

能够检测同时存在于多个数据包中的通信异常行为。



警报融合机制

行为有限——基于通信行为模式的异常检测方法

通过对工控系统通信网络数据进行正常模型训练分析，凡是不符合训练模型的，认为是异常行为，进行报警。

示例：基于人工智能的工业控制系统入侵检测技术

（1）基于“白名单”规则的异常检测方法：现有工控入侵检测“白名单”机制的缺点：人工配置规则，缺少自学习功能。

国内外相关理论研究

序号	研究机构	学者	年份	提出方法
1	英国贝尔法斯特女王大学	Yang等	2013	设计了一种基于规则的入侵检测系统，包括基于签名和基于模型两种方法。
2	荷兰屯特大学	Barbosa等	2013	提出一种面向工业SCADA系统安全的流白名单检测方法。
3	韩国电子通信研究所	Yun等	2013	通过分析SCADA系统主站和从站之间的DNP3协议通信行为，建立了基于分帧模式的白名单规则集。
4	美国橡树岭国家实验室	Linda等	2011	提出一种构建模糊逻辑规则库的学习方法，基于模糊规则进行系统行为建模，以检测通信的异常行为。

示例：基于人工智能的工业控制系统入侵检测技术

➢ 理论研究难点集中在如何设计适合工业控制系统的规则自学习算法，具体表现为：

1. **自学习方法特征属性选择**
   - 合理选择通信行为特征属性，并实现深度协议行为解析。如协议中功能码取值合法性。
2. **自学习规则集优化**
   - 对规则的遍历和搜索效率将直接影响到实时入侵检测算法性能。因此，需要研究控制规则集规模的方法。
3. **新的学习算法**
   - 合理确定检测粒度，再生成规则。

示例：基于人工智能的工业控制系统入侵检测技术

挑战：协议深度解析、高实时性。

- 基于“白名单”策略进行过滤，设计多比特Trie树匹配机制，提高访问控制效率。

研究进展：能够有效拦截Modbus/TCP非法访问。吞吐量＞线速20%，最大并发连接数＞1000个，基于加/解密的基本访问控制处理时间＜10ms。

（已在可信控制器中实现，进一步工作内置无线变送器/执行器中，提高性能）

相关研究成果发表在电子学报、信息与控制、Telecommunication Systems、ICCCS2018、ICMIR 2017、IEEE-CYBER 2015、InfoSec2015、ICINS 2015等期刊。

示例：基于人工智能的工业控制系统入侵检测技术

（2）基于通信行为模式的工业控制系统入侵检测方法：SCADA、DCS等工控系统数据具有异常样本少、维度高、关联性强等特点，**支持向量机**已被证明是一种有效的控制系统通信网络入侵检测的机器学习方法。

国内外相关理论研究

序号	研究机构	学者	年份	提出方法
1	英国萨里大学	J. M. Jiang等	2013	设计了单类支持向量机分类模型，通过自适应控制松弛变量和参数权衡检测输入的异常模式。仅针对TCP/IP协议。
2	开罗德国大学	M. Amer等	2013	设计了两类增强的单类支持向量机方法用于无监督异常检测，以降低奇异点对正常数据边界决策的影响。
3	日本中央电力研究所	T. Onoda等	2012	设计了单类支持向量机和支持向量数据描述学习算法OSVM SVDD，用于控制系统网络的入侵检测。
4	爱荷华州立大学	Y. X. Wang等	2004	扩展了适于入侵检测的内核方法，并与无监督学习单类支持向量机方法相结合。

示例：基于人工智能的工业控制系统入侵检测技术

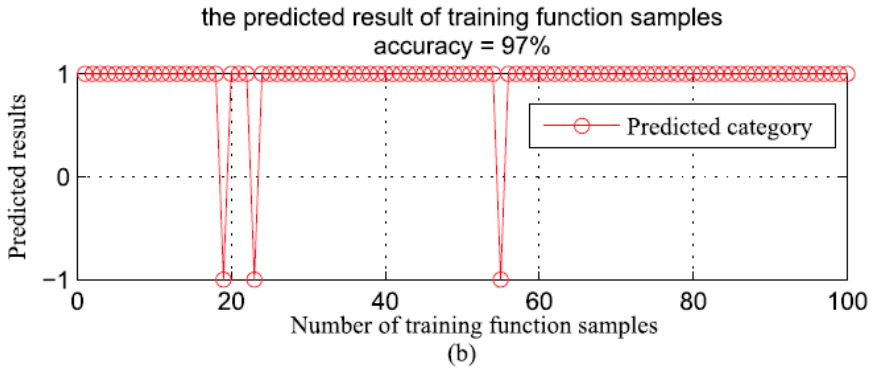
➢ 理论研究的难点集中在以下几个方面：

1. **异常通信行为模型建立**
   - 如何建立工业控制系统工业通信协议（如Modbus TCP、DNP3等）的通信行为模型，以及如何通过自学习逐步提高分类模型的准确度和泛化能力。
2. **降低分类器训练和测试时间**
   - 如何通过数据预处理、特征选择、参数寻优等方法，有效降低分类器训练时间和测试时间，满足工业现场在线实时性要求。
3. **如何降低误报率**
   - 采用单类支持向量分类器进行入侵检测，有效降低其误报率。

示例：基于人工智能的工业控制系统入侵检测技术

挑战：高实时性、低误报率。

$$\min \ \frac{1}{2}\|\omega\|^2 + \frac{1}{\nu r}\sum_{i=1}^{r}\xi_i - \rho$$
$$s.t.\ (\omega \cdot \Phi(x_i)) \geq \rho - \xi_i, \quad \xi$$



研究进展：实现针对Modbus/TCP、PowerLink工艺数据通信行为异常检测。目前准确率97%。

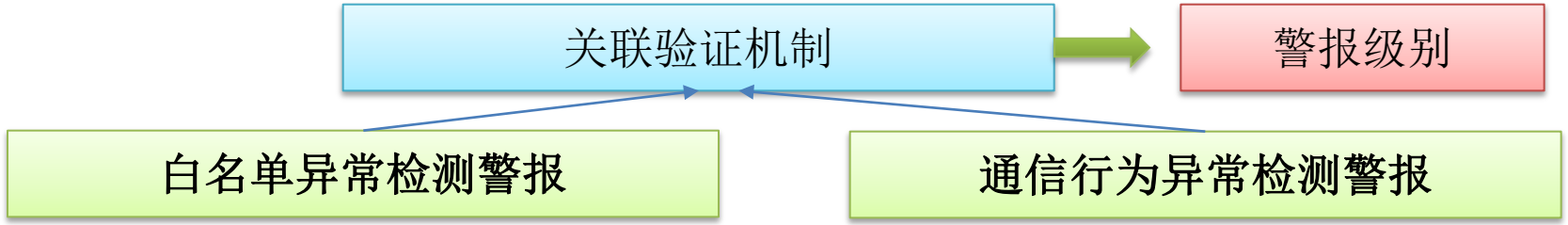
企业难题：绿盟科技基金项目“基于行业知识向量机集的工控系统异常行为检测方法研究”（电力、石化行业现场行为库）

相关研究成果发表在IEEE Transaction on Information Forensics and Security、Security and Communication Networks、Computers Materials & Continua、IEEE TrustCom 2018等期刊。

示例：基于人工智能的工业控制系统入侵检测技术

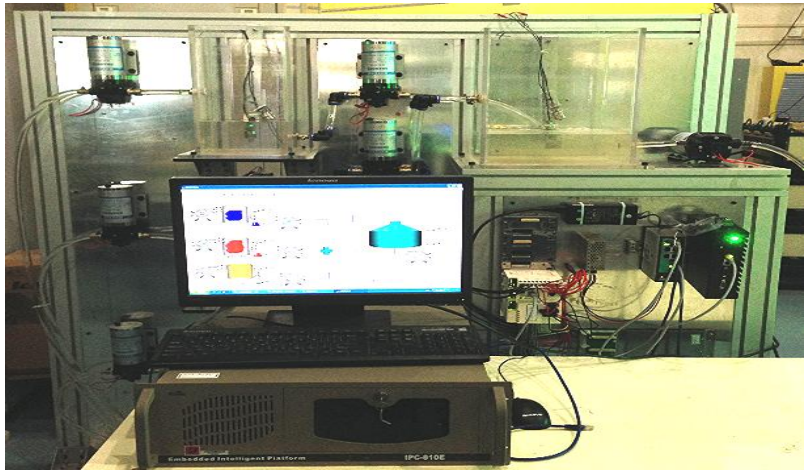
- **警报关联机制**

通过警报关联机制确认、容忍机制等，降低误报率、漏报率，确认警报级别。



- **评估方法**

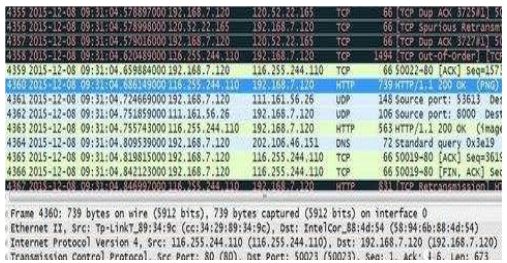
研究性能指标（检测率、True Ppositive（TP）、False Ppositive（FP）、True Nnegative（TN）、False Nnegative（FN）），以及参数对性能指标的影响。

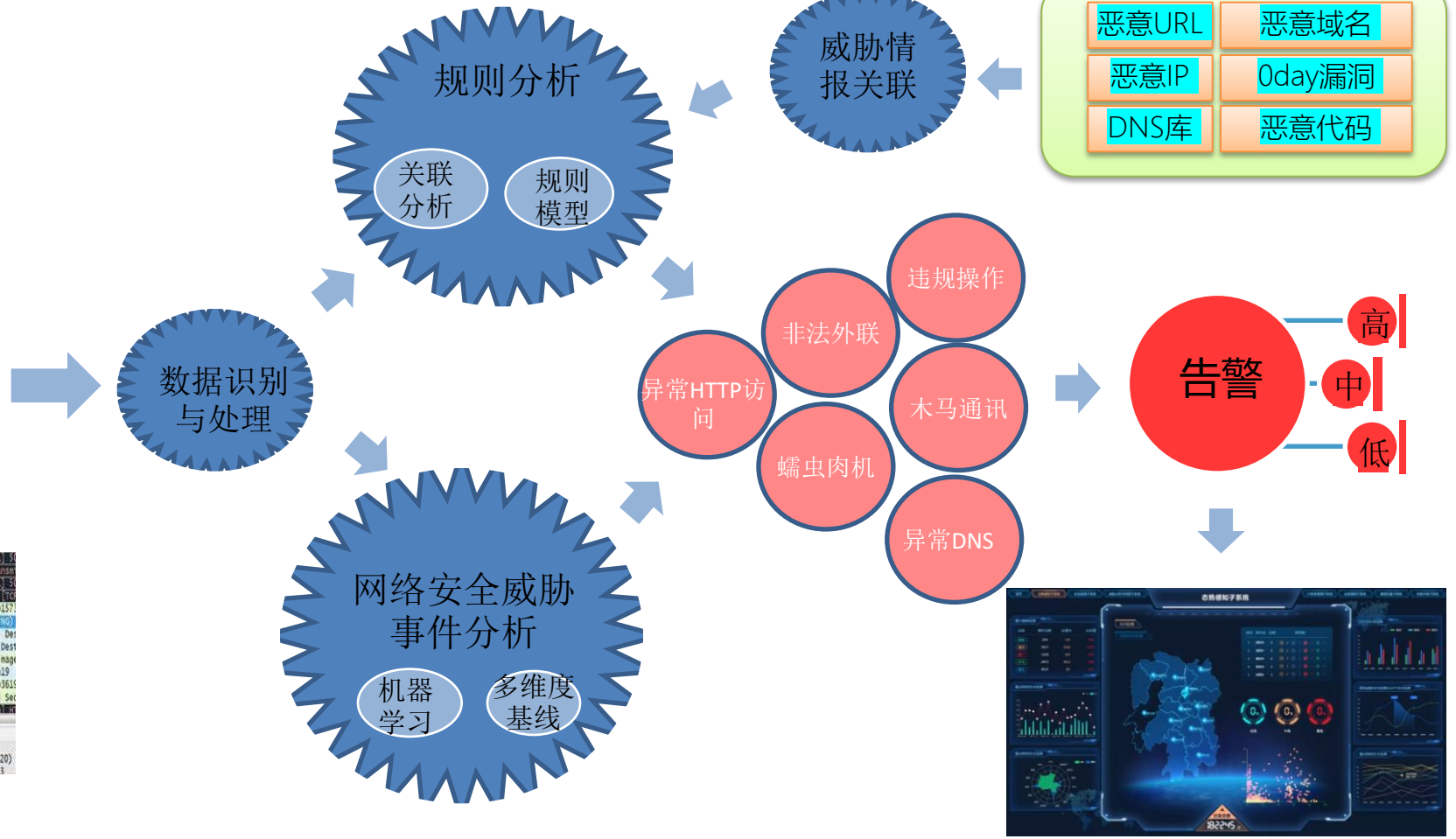


工业网络仿真实验环境

示例：基于人工智能的工业控制系统入侵检测技术

网络设备端口镜像





承担入侵检测技术方面的相关科研项目情况

1. 2018年度国家自然科学基金项目“面向工业通信行为的异常检测及安全感知方法研究”。
2. 2016年度国家自然科学基金项目“面向工控通信协议的自学习式异常检测方法及评估研究”。
3. 2019年度国家电网公司科学技术项目课题“电力系统边缘计算的安全防护技术”。
4. 2018年度国家电网公司科学技术项目课题“边缘计算在智能电网的应用和安全防护技术研究”。
5. 2018年度CCF-绿盟科技“鲲鹏”基金项目“基于行业知识向量机集的工控系统异常行为检测方法研究”
6. 2015年度工信部智能制造专项项目课题“工业控制网络监测安全技术要求和测试评价方法”。
7. 2015年度中国科学院网络化控制系统重点实验室开放课题“工业控制网络异常行为建模、在线入侵检测及自学习方法研究”。

提　纲

1. 人工智能与网络安全
2. 人工智能深度加强工业互联网安全
3. 工业互联网安全现状与未来展望

工业互联网安全现状与未来展望

国内外工业互联网信息安全产品：

产品种类多、覆盖面广，包括内生安全工控设备类、工控检测防御类、工控安全监管类、工控安全平台类、工控安全评估类、工控安全实训类、工控攻防演练类等。

行业应用现状和存在的主要问题：

（1）各家产品功能相近，区分度不大；（2）通用类产品多，行业专用类产品少；（3）OPC、Modbus等以太网协议层工控产品应用多，总线控制、实时控制环节工控产品应用少；（4）与工艺数据结合工控产品更少；（5）深度检测与防护能力和技术指标急需提升。

应用现状总结与未来技术展望：

（1）工业互联网安全与人工智能技术相结合是必然趋势之一；（2）也要重视人工智能技术自身存在的各种安全问题。

工业互联网安全现状与未来展望

工业互联网安全当前面临的10大难题	当前主流的解决方案
1.未知威胁检测	拟态、多态、诱骗、机器学习
2.已知威胁检测的准确率不高、实时性不够	特征库更新、深度解析、基于流检测、机器学习
3.安全事件漏报、误报、错报、重复上报	事件上报聚合、人工筛选、机器学习（聚类）
4.APT攻击检测（定向、有组织的攻击）	UEBA、基于规则的交叉关联分析、机器学习
5.DDoS攻击检测与防御	检测：阈值、代理、反向探测 防御：近目标清洗、近源压制
6.加密内容威胁检测	解密后检测、机器学习（识别+基线建模）
7.攻击溯源	威胁情报、人工分析、线下跟踪、设备指纹、黑客画像
8.攻防对抗博弈的智能化	人工智能（机器学习、知识图谱...）
9.威胁预测（时间、威胁类型、威胁来源、攻击目标、攻击意图、攻击手段等）	人工智能（机器学习、知识图谱...）
10.网络欺诈检测	阈值、UEBA、交叉关联分析、机器学习

敬请批评指正！