**模式识别和机器学习在农业领域应用的国内外研究现状**

**摘要：**……………………………………………………………………………………………

…………………………………………………………………………………………………….

关键词：二语动机自我系统；研究现状；述评

## 引言

…………………………………………………………………………………………………………

……………………………………………………………………………………………（宋体，小四）

## 正文部分

四 农业工控设备安全

4.1 工控设备安全

工业控制系统（Industrial Control System，ICS）[1]是一种表示用于工业控制的几种类型的控制仪器和相关仪器的通用总成。工业控制系统（ICS）通过整合信息技术（IT）来提高效率和可控性，但是也因此引入了对ICS的网络威胁[2]。ICS开始面临像IT同样的漏洞环境，经受IT一样的安全考验。而且越来越多的攻击开始针对性的选择ICS进行攻击。如Stuxnet和乌克兰电网的网络攻击，导致大规模的电力瘫痪，对社会造成巨大影响[3]。但是由于这些系统的重要性和独特性，很难找到通用的方式去防御攻击。目前重要的是设计新颖的防御机制，包括对底层物理结构的防御，并能在早期阶段检测到攻击[2]。

4.1 农业工控设备安全

随着生产力的提升，智慧农业在农业生产中的应用越来越广泛。大量的传感器和无线通信技术应用于农业生产，广泛用于环境监测，精确农业。通讯协议有基于ZigBee的WSN和无源，半无源和有源RFID[4]。还有基于M2M的机器和过程控制，建筑和设施自动化以及基于RFID的可追溯系统[5]。农业工控设备的安全性至关重要，由于农业设备的脆弱性，设备被劫持后被应用于DDOS攻击的影响十分巨大。

4.1 传统的工控设备防御方法

由于工控设备的的脆弱性和重要性，研究者对工控设备安全性的防御进行了很多研究。包括如下方面（1）提升工控设备软硬件的稳健性，在生产阶段对软件的源代码进行静态分析[6-8]，对设备进行动态分析[9,10]（2）在生产阶段对网络的流量，控制反馈进行实时的监控。

4.1 基于机器学习的工控设备防御方法

传统的工控设备防御方法难以应对大规模的工控设备的安全问题。随着机器学习技术的广泛应用，研究者开始使用训练机器学习模型以解决工控设备的安全问题。基于机器学习进行流量分析是其中一种实现方式。Li等[3]通过基于遥测分析的入侵检测，优化系统模型，捕获系统中不同节点之间的通信包，然后使用机器学习算法对数据集进行训练，实现恶意流量检测，进一步区分攻击类型。其优势在于遥测意味着它不需要进入工业控制系统网络，而是通过远程捕获数据包来实现入侵检测。Keliris等[2]针对底层集成电路进行了攻击模拟，重点研究可编程逻辑控制器（PLC）的控制系统实现。攻击分为三类，传感器攻击、执行器攻击和控制器攻击，并将攻击将用于训练基于机器学习的攻击检测模块。为了检测和对抗ICS上的恶意活动，Keliris利用基于模型和经验的动态过程中的典型时间信号模式及其动态特性的知识来确定攻击的状态，并训练了一个主SVM来检测正在进行的攻击的存在，以及一组辅助的、独立的SVM来检测特定类型和类型的攻击。SVM除了提供简单的基于范围的分类器外，还具有显著的鲁棒性。通过对多个信息流之间运行的相关性，支持向量机支持高检测精度。相比之下，简单的基于范围的攻击检测器在设置足够窄的范围以可靠地检测攻击时会遇到大量的误报，或者在扩大范围以减少误报时会遇到大量的误报。

3.结论

………………………………………………………………………………………………………………………………………………………………………………………………………(宋体，小四)

**注释和参考文献**：

[1] Wikipedia. Industrial control system[EB/OL]. [20190328]. <https://en.wikipedia.org/wiki/Industrial_control_system>.

[2] Keliris A, Salehghaffari H, Cairl B, et al. Machine learning-based defense against process-Aware attacks on Industrial Control Systems[C]. 47th IEEE International Test Conference, ITC 2016, November 15, 2016 - November 17, 2016, 2017: IEEE Philadelphia Section; Institute of Electrical and Electronic Engineers, Inc. (IEEE).

[3] Li H, Qin S. Optimization and implementation of industrial control system network intrusion detection by telemetry analysis[C]. 3rd IEEE International Conference on Computer and Communications, ICCC 2017, December 13, 2017 - December 16, 2017, 2018: 1251-1254.

[4] Ruiz-Garcia L, Lunadei L, Barreiro P, et al. A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends[J]. Sensors, 2009, (9): 4728-4750.

[5] Wang N, Zhang N, Wang M. Wireless sensors in agriculture and food industry—Recent development and future perspective[J]. Computers and Electronics in Agriculture, 2006, 50(1): 1-14.

[6] 张健, 张超, 玄跻峰, et al. 程序分析研究进展[J]. 软件学报, 2019, 30(1): 1-31.

[7] Feng Q, Zhou R, Xu C, et al. Scalable Graph-based Bug Search for Firmware Images[C]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016: 480-491.

[8] Dewey D, Giffin J T. Static detection of C++ vtable escape vulnerabilities in binary code[C]. NDSS, 2012.

[9] Chen J, Diao W, Zhao Q, et al. IOTFUZZER: Discovering Memory Corruptions in IoT Through App-based Fuzzing[C]. Proceedings of the 2018 Network and Distributed System Security Symposium, 2018.

[10] 邹权臣, 张涛, 吴润浦, et al. 从自动化到智能化:软件漏洞挖掘技术进展[J]. 清华大学学报(自然科学版), 2018: 1-16.