水处理系统网络攻击的检测和定位：基于熵的方法

刘可[1]，汪慕峰[2]，麻荣宽[1]，张镇勇[2]，魏强[1]
[1]数学工程与先进计算国家重点实验室，中国郑州市，450001
[2]浙江大学控制科学与工程学院，中国杭州市，310027

摘要：随着工业4.0的发展，水处理系统作为一种典型工业信息物理系统逐渐接入互联网。先进的信息技术使水处理系统在可靠性、效率和经济性方面受益。然而，网络和基础设施中潜在的漏洞使水处理系统很容易遭受网络攻击。由于水处理系统对于实时性和可用性的严苛要求，传统的面向信息系统的防御机制无法直接应用于水处理系统。本文提出一种基于熵的入侵检测方法来抵御针对系统中控制器（如可编程逻辑控制器）的攻击。由于水处理系统运行条件的变化，在模型采用静态阈值进行检测时会产生较高误报率。因此本文提出一种动态阈值调整机制来提高所提方法的检测性能。为验证所提方法，我们建立了一个包含超过50个测量点的高保真水处理系统测试平台。在两种攻击场景下进行实验，共涵盖了36次攻击。结果表明，所提方法能够实现97.22%的检测率和1.67%的误报率。

关键词：工业信息物理系统；水处理系统；入侵检测；异常状态；检测和定位；信息论
https://doi.org/10.1631/FITEE.2000546