Computer Science and Application 计算机科学与应用, 2020, 10(11), 2141-2146
Published Online November 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.1011225

Hans汉斯

基于深度卷积网络及K均值的工控系统入侵检测研究

徐　峰，张玉贤

衢州职业技术学院，浙江　衢州
Email: qzct99@126.com

收稿日期：2020年11月5日；录用日期：2020年11月20日；发布日期：2020年11月27日

摘　要

随着物联网与智能制造的兴起，工业控制系统的信息安全问题亦日渐受到重视，尤其是公共安全控制要地受到网络攻击后极易导致城市生活网络的瘫痪。为避免严重的网络攻击灾害，本项目对入侵IDS进行深入研究，提出基于深度卷积网络及K均值的工控系统入侵检测方法。实验结果显示，在衢州某水库数据集上，本方法在效能指标上优于其它方法。

关键词

工控系统，卷积网络，网络攻击

Research on Intrusion Detection of Industrial Control System Based on Deep Convolution Network and K-Means

Feng Xu, Yuxian Zhang

Quzhou College of Technology, Quzhou Zhejiang
Email: qzct99@126.com

Received: Nov. 5th, 2020; accepted: Nov. 20th, 2020; published: Nov. 27th, 2020

Abstract

With the rise of the Internet of things and intelligent manufacturing, the information security of industrial control system has been paid more and more attention, especially when the public security control points are attacked by network. It is easy to lead to the paralysis of urban living network. In order to avoid serious network attacks disaster, this project makes an in-depth study on intrusion IDS, and proposes an intrusion detection method of industrial control system based

文章引用: 徐峰, 张玉贤. 基于深度卷积网络及 K 均值的工控系统入侵检测研究[J]. 计算机科学与应用, 2020, 10(11): 2141-2146. DOI: 10.12677/csa.2020.1011225

on deep convolution network and k-means. Experimental results show that this method is superior to other methods in most performance indicators on a data set of a reservoir in Quzhou.

Keywords

Industrial Control Systems, Convolution Network, Network Attack

1. 引言

工业控制系统(ICS)在工业控制领域的监控中起着重要的作用。ICS 是一个通用术语，包含工业生产中使用的几种类型的控制系统，还包括监控和数据采集(SCADA)系统、分布式控制系统(DCS)和其他较小的控制系统配置，如可编程逻辑控制器(PLC)，经常出现在工业部门和重要基础设施中。ICS 普遍存在于许多关键基础设施中，如发电、输配电、水处理及制造业等。在配电网中特别是在住宅区控制效果可以达到最佳[1]。对建筑物内的电热元件进行自动控制已成为 ICS 的一项重要研究内容[2]。现代 ICS 的目标是增强交互式控制策略的功能，从而提高能源效率和更舒适或更友好的环境。近年来 ICS 已经连接到通信网络上，允许远程监视和控制底层进程。虽然这可以带来显著的效率和可用性好处，但它也会增加通过为潜在攻击者提供一个进入点来渗透系统的网络攻击的可能性。近年来发生了一些引人注目的攻击事件，突出表明需要采取适当的安全措施来保护 ICS 基础设施。中国内外相关学者在容错控制方面已经做了许多研究，它们也可以提供工具或攻击弹性控制。然而在攻击检测和隔离方面，容错控制和攻击恢复控制之间存在着很大的差异，这就要求采用特定的方法来解决 ICS 中的安全问题。例如故障是被认为是影响系统行为的物理事件，其中事件不以协调的方式行动，而网络攻击可能以协调的方式在大量攻击点上执行。

工业控制系统(ICS)技术由于具有数据控制稳定，传输效率高等优势，广泛应用于天然气、电网、水利、交通、通讯等民生基础设施中。工业控制系统(ICS)网络中的异常检测是极为重要的一项研究内容，随着工业互联网的高速发展，各系统之间的连通性也越来越高。各制造业者期望通过智慧自动化的生产方式提高生产效率，因此 ICS 由过往的封闭环境逐渐转为网路连接。从信息安全的面向来看，传统 ICS 所依赖的封闭性正逐渐地消失，现有的 ICS 正面临各种潜在的入侵威胁，一旦网络中出现漏洞极容易成为网络黑客的攻击目标，为此我们急需研究网络安全监控设备，旨在改善工业环境中网络安全监控的整体状态。基于深度卷积网络及 K 均值的工控系统入侵检测方法，可以加强控制系统网络的安全，在实际使用过程中主要采用数据训练的方式发现系统中现有的异常。

本研究提出了用于工业控制系统的半监督异常侦测方法，使用基于 k-means 分群的方法，以及通过卷积自动编码器学习正常数据的行为模型，分别侦测单一时间点以及连续时间中的异常行为，这类方法具有不需使用带有攻击标记数据训练的优势，也排除了监督式方法需要频繁使用最新带标记的攻击数据重新训练模型的成本。实验结果表明本研究提出的方法在多项效能指标上优于其他方法，且更精确。

2. 国内外研究现状

2.1. 基于误用的入侵检测系统

基于误用的入侵检测系统又称为基于签名的 IDS，由于它的低误报率以及使用上的便捷性一直是一

般商业的首选方案。这种检测方式主要是对已知的攻击建立签名数据库，通过搜寻数据库中是否有符合的签名来侦测攻击。目前被广泛使用的基于签名的 IDS 有 Snort、Suricata 等[3]。这类型 IDS 的一个明显的缺点是难以侦测未知攻击，即使时刻保持攻击数据库是最新的状态，当新型攻击网络工程师发现到分析攻击模式，再到更新签名数据库时可能为时已晚。A. Nisioti 等人认为维护每日出现的新型攻击是不可行的，并且提到已知攻击经过简单变化便可轻易规避这类型基于误用的系统[4]。

2.2. 基于异常的入侵检测系统

近年来，机器学习技术被大量应用在入侵检测系统中，根据带卷标数据的使用程度可分为监督、非监督、半监督，根据 A. Nisioti 等人调查报告中对 IDS 的分类，它们将三种方式归属于基于异常的子类[5]。其中，机器学习中有一类称为新颖检测的半监督异常侦测技术，又称为一类分类，仅使用不带任何异常与攻击的正常数据训练，藉由学习正常行为的特性，以区别出测试数据中偏离正常的数据。相关技术有 One Class SVM、自动编码器等[6]。在优势上，相较于非监督方法这类技术可更好的检测攻击，有着较低的漏报率。但用于训练的正常数据需要足够充分，以避免测试阶段时出现的正常行为与训练数据中的差异太大导致高误报率。在工业控制系统中，往往遵循特定的工业流程，通常有着循环规律以及可预测的通讯特性，因此对于工业控制系统，这类型的 IDS 有着很大的潜力。

3. 测量原理

3.1. 联合 K-Means 异常侦测与卷积自动编码器异常侦测

针对工业控制系统传统单一检测算法模型，对不同攻击类型检测率和检测速度不佳的问题提出一种半监督异常侦测方法。该方法提出一种优化支持向量机和 K-means 结合的深度卷积自动编码器的入侵检测方法[7]。如图 1 所示，于相比其它同类型的方法，能提升对攻击的检测效能，项目的主要内容可以总结为以下三大部分：

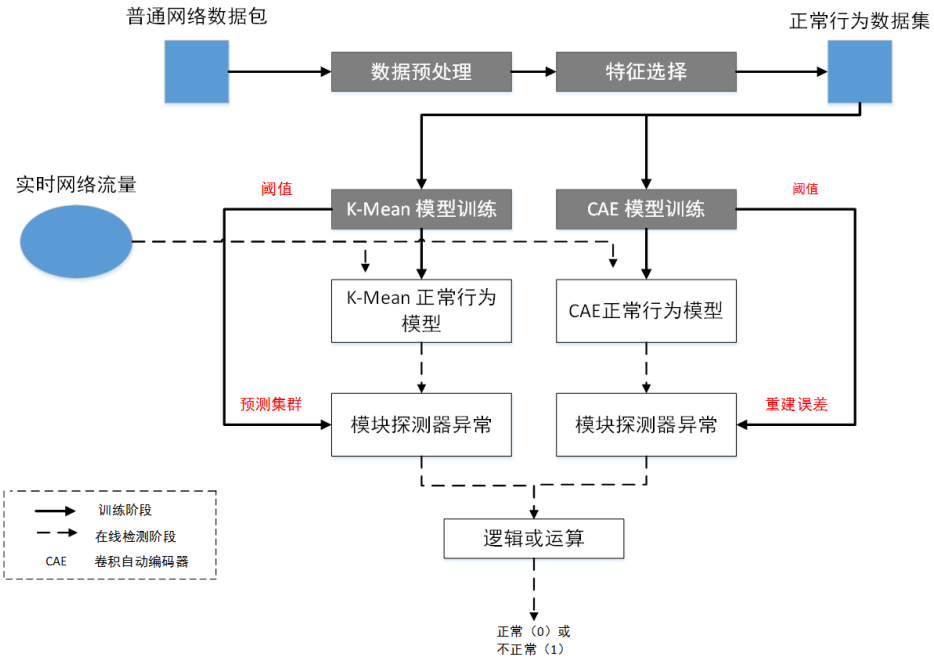

Figure 1. System architecture
图 1. 系统架构

1) 采用半监督的方式训练异常侦测器，在实际使用过程中只用正常数据训练，学习正常行为的特性，即可区分偏离正常的异常行为。

2) 选择 k-means 学习各属性值的正常区间，以此找测试数据中出不在这些范围的异常值。

3) 利用深度学习卷积自动编码器学习数据正常变化模式，用以检测的异常行为。

该方法采用半监督的异常侦测技术，仅取用工业控制系统在正常运作状态下的数据建立正常行为模型。没有因需要人工标记攻击数据而带来的成本，亦没有训练用的攻击数据难以取得以及无法涵盖所有可能攻击行为的隐忧，并有着检测未知攻击的能力。

在实际使用过程中在本方法的框架中有 k-means 异常侦测模块与 CAE 异常侦测模块，每一笔数据会同时进入两个模块进行检测，只有同时被两个模块判定为正常的数据会在最后输出为正常，一旦有一个或以上的模块认为这笔数据异常，则对这笔数据的异常判定结果即是异常。

在建立 CAE 正常行为模型后，模型已具备了提取正常行为特征以及重建正常行为数据的能力。为了能分类数据的正常与否，通过观察 CAE 输入与输出的重建误差(Reconstruction Error)是一种常被使用的判断方式。在训练完成 CAE 正常行为模型后，需要订定一个合适的重建误差门坎值，以期望在测试阶段中数据可以被正确的分类为正常或异常。在重建误差门坎值的订定上，本方法将训练用的正常行为的数据集分成五份，使用五折交叉验证的方式，每次取四份作为训练数据训练 CAE，剩余一份作测试数据并记录其中最大的重建误差，最后将五次的最大重建误差取其平均，作为判断正常与不正常的门坎值。假设门坎值为 θ，CAE 的输入与输出数据为 x_T 与 $\hat{x}_T$，则对于原始数据 x_T 的异常判断式为：

$$F_{CAD}\left(x_t\right)=\begin{cases}1 & \text{if } \mathrm{MSE}\left(x_T,\hat{x}_T\right)\succ 0\\ 0 & \text{otherwise}\end{cases} \tag{1}$$

当 $F_{CAD}\left(x_t\right)$ 输出为 1 时表示 CAE 异常侦测方法将 x 判断为异常，反之则是正常。其中 $MSE\left(x_T,\hat{x}_T\right)$ 为均方误差(Mean Square Error, MSE)。

在本方法的框架中有 k-means 异常侦测模块与 CAE 异常侦测模块。每一笔数据会同时进入两个模块进行检测，只有同时被两个模块判定为正常的数据会在最后输出为正常，一旦有一个或以上的模块认为这笔数据异常，则对这笔资料的异常判定结果即是异常，如图 2 所示。

$$F_{CAD}\left(x_t\right)=\begin{cases}1 & \text{if } F_{KAD}\left(x_t\right)\succ 0 \text{ and } F_{CAD}\left(x_t\right)=0\\ 0 & \text{otherwise}\end{cases} \tag{2}$$

后判定测试资 x 是否异常的函式为：

$$F_{KAD}\left(x_t\right)=\begin{cases}1 & \text{if } \exists d_{ti}\succ g\left(l_{ti},i\right), \text{for } i=0,1,2\cdots\\ 0 & \text{otherwise}\end{cases} \tag{3}$$

函式 $g\left(l_{ti},i\right)$ 会利用所属群的标记 l_{ti} 找到并回传该群的半径 $r_{tij}\in radii\in \mathrm{Radii}$ 当函式 $F_{KAD}\left(x_t\right)$ 的输出为 1 时表示此的基于分群的异常侦测方法将 x_t 判断为异常；0 表示正常。

式(2)中的函式 $F_{KAD}\left(x_t\right)$ 即为式(3)。

3.2. 结果分析

衢州某水库数据集共有 274,620 份资料，其中攻击占 60,040 份，其余 214,580 为正常封包数据，共含 17 个属性与 3 个类标记属性。标签属性中 binary|result 属性为二元标记，表示正常与攻击；categorized result 标签属性使用 8 个类别分别表示正常与 7 种攻击，而 specific result 则是再将攻击在细分成 35 种不同攻击，水库资料集效能比较如表 1 所示。

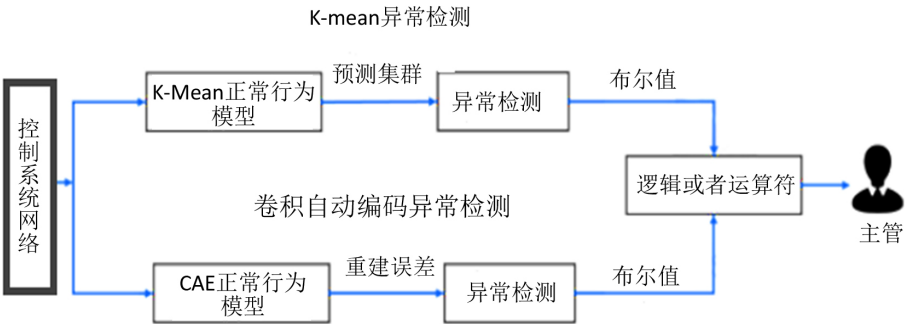

Figure 2. Combined k-means and convolution encoder automatically
图 2. 联合 k-means 与卷积自动编码器

Table 1. Comparison of the effectiveness of a reservoir data set
表 1. 某水库资料集效能数据分析

模型	精度	Recall	F1-score 比较
Proposed 算法	0.9553	0.9543	0.8352
Proposed 算法 + Whitelist	0.8908	0.8862	0.8985
LSTM (Long Short Term Memory network)	0.9245	0.7898	0.8589
K-means 算法	0.5680	0.5728	0.6751

4. 结论

本论文提出了应用于工业控制系统的半监督异常侦测方法，使用 k-means 与卷积自动编码器分别针对正常数据在单一时间点的特性与在时间序列中的变化模式建立正常行为模型。接着以分群后各群的最大半径以及数据重构前后的误差建立异常侦测机制。实验结果显示，在衢州某水库数据集上，本方法在大多数效能指标上优于其他方法，其中 F1-socre 在两个数据集上分别高于其它方法。

致　谢

诚挚感谢衢州职业技术学院院级科研项目(“基于深度卷积网络及 K 均值的工控系统入侵检测应用研究”，No：QZYY2013 及“成果导向视角下课程体系的构建与探索”，No：VER201901)项目的资助。感谢国家自然科学基金资助项目(项目编号：50902110)。

参考文献

[1] Zheng, Z. and Reddy, A.L.N. (2017) Safeguarding Building Automation Networks: THE-Driven Anomaly Detector Based on Traffic Analysis. 2017 26*th International Conference on Computer Communication and Networks* (*ICCCN*), Vancouver, BC, 31 July-3 August 2017, 1-11. https://doi.org/10.1109/ICCCN.2017.8038393

[2] Chalapathy, R., Menon, A.K. and Chawla, S. (2020) Anomaly Detection Using One Class Neural Networks. arXiv preprint arXiv,2020.1802.06360

[3] White, J.S., Fitsimmons, T. and Matthews, J.N. (2013) Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata. *SPIE Defense Security & Sensing Cyber Security Conference*, Baltimore, 875704. https://doi.org/10.1117/12.2015616

[4] Nisioti, A., Mylonas, A., Katos, V., *et al.* (2017) You Can Run But You Cannot Hide from Memory: Extracting IM Evidence of Android Apps. 2017 *IEEE Symposium on Computers and Communications* (*ISCC*), Heraklion, 3-6 July 2017, 457-464. https://doi.org/10.1109/ISCC.2017.8024571

[5] Wan, M., Shang, W. and Zeng, P. (2017) Double Behavior Characteristics for One Class Classification Anomaly Detection in Networked Control Systems. *IEEE Transactions on Information Forensics and Security*, **12**, 3011-3023. https://doi.org/10.1109/TIFS.2017.2730581

[6] Mantere, M., Sailio, M. and Noponen, S. (2014) A Module for Anomaly Detection in ICS Networks. *The Proceedings of the* 3*rd International Conference on High Confidence Networked Systems*, Berlin, April 2014, 49-56. https://doi.org/10.1145/2566468.2566478

[7] 张文安，洪榛，朱俊威. 工业控制系统网络入侵检测方法综述[J]. 控制与决策, 2021(11): 2277-2288.