

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 7 月 16 日 (16.07.2020)



(10) 国际公布号
WO 2020/143227 A1

- (51) 国际专利分类号:
G06K 9/62 (2006.01)
- (21) 国际申请号: PCT/CN2019/101247
- (22) 国际申请日: 2019 年 8 月 18 日 (18.08.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910011642.4 2019 年 1 月 7 日 (07.01.2019) CN
- (71) 申请人: 浙江大学(ZHEJIANG UNIVERSITY) [CN/CN]; 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。
- (72) 发明人: 程鹏(CHENG, Peng); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。何阳(HE, Yang); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。陈积明(CHEN, Jiming); 中国浙江省杭州市西湖区余

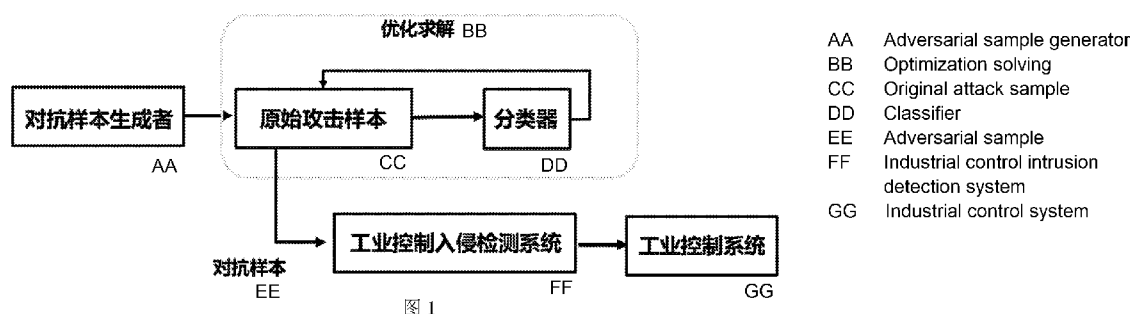
杭塘路 866 号, Zhejiang 310058 (CN)。王文海(WANG, Wenhai); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。孙优贤(SUN, Youxian); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。

(74) 代理人: 杭州求是专利事务所有限公司(HANGZHOU QIUSHI PATENT OFFICE CO., LTD.); 中国浙江省杭州市西湖区玉古路 147 号黄鸿年科技综合大楼 215 室/刘静, Zhejiang 310013 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

(54) Title: METHOD FOR GENERATING MALICIOUS SAMPLE OF INDUSTRIAL CONTROL SYSTEM BASED ON ADVERSARIAL LEARNING

(54) 发明名称: 一种基于对抗学习的工业控制系统恶意样本生成方法



(57) Abstract: Disclosed is a method for generating a malicious sample of an industrial control system based on adversarial learning. In the method, by means of adversarial learning technology, an adversarial sample of an industrial control intrusion detection system based on a machine learning method is calculated by using an optimization solution. A corresponding new adversarial sample can be generated after an attack sample that can originally be found by the intrusion detection system is processed by means of the method. The adversarial sample can bypass an original intrusion detector (recognized to be normal), and still maintains an attack effect. The present invention effectively guarantees the security of an industrial control system by means of actively generating a malicious sample of the industrial control system, thereby taking preventive measures.

(57) 摘要: 本发明公开了一种基于对抗学习的工业控制系统恶意样本生成方法。该方法通过对抗学习技术, 利用优化解法计算出基于机器学习方法的工业控制入侵检测系统的对抗样本。原来能被入侵检测系统发现的攻击样本, 经过该方法处理后能生成对应的新对抗样本。这种对抗样本可以绕过原有的入侵检测器(被识别为正常), 仍保持攻击效果。本发明通过主动生成工业控制系统恶意样本, 有效保障工业控制系统安全, 防患于未然。

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

一种基于对抗学习的工业控制系统恶意样本生成方法

技术领域

本发明属于工业控制系统安全领域，涉及一种基于对抗学习的工业控制系统恶意样本生成方法。

背景技术

频频发生的工业控制系统安全事件引起世界各国的高度重视。为了积极应对工控安全问题，各种应对措施纷纷展开，如规范标准的制定、入侵检测的部署。在工业控制系统中，基于网络的入侵检测器是非常典型且常见的。通过应用网络(IT)和控制网络(OT)之间部署网络异常检测装置，可以极大地提高工控系统的安全性。目前，基于机器学习的异常检测算法可以在网络异常流量识别中实现较好的性能。这些机器学习技术能够从大量工业控制系统历史数据中找出其内在行为模式以构建异常检测系统。

而另一方面，现有的基于机器学习算法的工业控制系统入侵检测器存在脆弱的地方。机器学习模型在实际应用的时候很容易被攻击者故意生成的对抗样本操纵。攻击者通过对测试示例进行微小的修改，就能让算法模型产生与正常输出完全不同的结果。让模型产生错误预测结果的样本叫做对抗样本。主动对机器学习设计生成对抗性攻击的研究被称为对抗机器学习研究。这种对抗攻击给使用机器学习的系统带来了潜在的安全威胁，尤其是对于诸如工业控制等对安全需求很高的系统。

对于基于机器学习算法的工业控制系统入侵检测系统，如果受到攻击者蓄意的对抗攻击，会无法正常识别出原本能识别的恶意流量。这会给工控系统带来很大的安全隐患。目前现有的工控安全入侵检测研究缺少对于对抗学习部分的研究，而模拟攻击者主动生成针对工控机器学习检测算法的对抗样本是十分有意义的。因此，有必要对工业控制入侵检测系统展开对抗机器学习研究，主动生成能绕过检测器完成隐蔽性攻击的对抗样本，从而保证系统安全，防患于未然。

发明内容

本发明的目的在于针对目前工业控制系统安全的欠缺和不足，提供一种基于对抗学习的工业控制系统恶意样本生成方法。

本发明的目的是通过以下技术方案来实现的：一种基于对抗学习的工业控制系统恶意样本生成方法，包括如下步骤：

(1) 对抗样本生成者对工业控制系统通信数据进行嗅探, 获得与工业控制入侵检测系统所使用的训练数据同分布的通信数据, 并对通信数据标记类别标签, 类别包括异常和正常, 其中的异常通信数据作为原始攻击样本。工业控制入侵检测系统为现有的基于机器学习方法的工业控制入侵检测系统。

(2) 对工业控制系统通信数据进行协议解析工作, 识别、提取其中有效特征, 包括: 通信数据的源 IP 地址(SIP)、源端口号(SP)、目的 IP 地址(DIP)、目的端口号(DP)、包间隔时间(Time delta)、包发送时间(Time)、包功能码(Function code)等。

(3) 根据步骤(2)提取的有效特征建立机器学习分类器, 利用有标签的工业控制系统通信数据对机器学习分类器进行训练, 得到训练好的用于分辨正常或异常通信数据的分类器。

(4) 利用步骤(3)建立的分类器, 将工业控制入侵检测系统的对抗学习问题转化成如下优化问题, 求解优化问题得到最终的对抗样本。

$$\begin{aligned} x^* &= \arg \min g(x) \\ s.t. \quad d(x^*, x^0) &< d_{max} \end{aligned}$$

其中 $g(x)$ 为对抗样本 x^* 被判为异常样本的可能性, 通过分类器计算得到; $d(x^*, x^0)$ 为对抗样本和原始攻击样本的距离, d_{max} 表示工业控制系统允许的最大欧式距离, 即超过此距离对抗样本无恶意效果。

(5) 将步骤(4)生成的对抗样本在实际工业控制系统中进行测试, 若能成功绕过工业控制入侵检测系统并且保留攻击效果则视为有效的对抗样本, 否则舍弃该对抗样本。

进一步地, 所述步骤(1)中, 对抗样本生成者应为黑盒攻击者, 不能直接获得与工业控制入侵检测系统(检测方)完全相同的数据。

进一步地, 所述步骤(2)中, 针对不同的工业控制系统通信协议可以提取出不同的有效特征。常用的工业控制系统通信协议包括 Modbus、PROFIBUS、DNP3、BACnet、Siemens S7 等。其中每种通信协议有对应的格式与应用场景, 根据具体场景可以解析不同的通信协议, 得出有效特征集合。

进一步地, 所述步骤(3)中, 对抗样本生成者训练所用的分类器可以是和工业控制入侵检测系统即检测方不一样的分类器, 对抗样本生成者生成的分类器可被称为对抗学习的本地替代模型, 其原理是对抗学习攻击的可迁移性。

进一步地, 所述步骤(4)中, 具体优化问题解法包括梯度下降法、牛顿法、COBYLA (for Constrained Optimization BY Linear Approximations)方法等。

进一步地, 所述步骤(4)中, 距离的表达方法包括一范式距离、二范式距离、无穷范式距离。

进一步地，所述步骤(4)中，机器学习分类器采用神经网络，其概率计算方式如下：

$$p(y = j|x^{(i)}; \theta) = \frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^k e^{\theta_l^T x^{(i)}}}$$

其中 p 为预测概率， $x^{(i)}$ 为样本 x 的第 i 个特征， y 为样本 x 所对应的标签 j ， θ 为神经网络参数， θ_j 为标签 j 对应的神经网络参数， k 为标签的总数；

将工业控制入侵检测系统的对抗学习问题转化成如下优化问题：

$$\begin{aligned} x^* &= -\arg \min[p(x) = 0] \\ s.t. & d(x^*, x^0) < d_{max} \end{aligned}$$

进一步地，所述步骤(4)中，对于特定控制场景，需要在优化问题中加入对变量的特殊约束，如某场景的包功能码是确定的，则对抗样本不能在该维度上做改变。即该方法在应用时，为保证生成的对抗样本能有效的完成恶意攻击效果，生成者需要根据特定的场景对特定维度的变量在做优化问题设计时加上不同的约束条件。

本发明的有益效果是：基于对抗学习的工业控制系统恶意样本生成方法，增加了工业控制系统安全性。将原有的对抗学习研究领域从机器视觉、语音等扩展到了工业控制领域。增强了基于机器学习的工业控制入侵检测系统安全性能，防止恶意样本的攻击。

附图说明

图 1 是本发明方法实现框图。

图 2 是分发明方法仿真结果图。

具体实施方式

下面结合附图和具体实施例对本发明作进一步详细说明。

本发明提供了一种基于对抗学习的工业控制系统恶意样本生成方法，如图 1 所示，包括如下步骤：

(1) 对抗样本生成者对工业控制系统通信数据进行嗅探，获得与工业控制入侵检测系统所使用的训练数据同分布的通信数据，并对通信数据标记类别标签，类别包括异常和正常，其中的异常通信数据作为原始攻击样本。工业控制入侵检测系统为现有的基于机器学习方法的工业控制入侵检测系统。

其中，对抗样本生成者应为黑盒攻击者，不能直接获得与工业控制入侵检测系统（检测方）完全相同的数据。

(2) 对工业控制系统通信数据进行协议解析工作，识别、提取其中有效特征，包括：通信数据的源 IP 地址(SIP)、源端口号(SP)、目的 IP 地址(DIP)、目的端口号(DP)、包间隔时间(Time delta)、包发送时间(Time)、包功能码(Function code)等。

针对不同的工业控制系统通信协议可以提取出不同的有效特征。常用的工业控制系统通信协议包括 Modbus、PROFIBUS、DNP3、BACnet、Siemens S7 等。其中每种通信协议有对应的格式与应用场景，根据具体场景可以解析不同的通信协议，得出有效特征集合。

(3) 根据步骤(2)提取的有效特征建立机器学习分类器，利用有标签的工业控制系统通信数据对机器学习分类器进行训练，得到训练好的用于分辨正常或异常通信数据的分类器。

对抗样本生成者训练所用的分类器可以是和工业控制入侵检测系统即检测方不一样的分类器，对抗样本生成者生成的分类器可被称为对抗学习的本地替代模型，其原理是對抗学习攻击的可迁移性。

(4) 利用步骤(3)建立的分类器，将工业控制入侵检测系统的对抗学习问题转化成如下优化问题，求解优化问题得到最终的对抗样本。

$$\begin{aligned} x^* &= \arg \min g(x) \\ s.t. \quad d(x^*, x^0) &< d_{max} \end{aligned}$$

其中 $g(x)$ 为对抗样本 x^* 被判为异常样本的可能性，通过分类器计算得到； $d(x^*, x^0)$ 为对抗样本和原始攻击样本的距离， d_{max} 表示工业控制系统允许的最大欧式距离，即超过此距离对抗样本无恶意效果。

具体优化问题解法可以采用梯度下降法、牛顿法、COBYLA (for Constrained Optimization BY Linear Approximations) 方法等。距离的表达方法可以采用一范式距离、二范式距离、无穷范式距离等。

对于特定控制场景，需要在优化问题中加入对变量的特殊约束，如某场景的包功能码是确定的，则对抗样本不能在该维度上做改变。即该方法在应用时，为保证生成的对抗样本能有效的完成恶意攻击效果，生成者需要根据特定的场景对特定维度的变量在做优化问题设计时加上不同的约束条件。

机器学习分类器可以采用神经网络，采用神经网络时，其概率计算方式如下：

$$p(y = j | x^{(i)}; \theta) = \frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^k e^{\theta_l^T x^{(i)}}}$$

其中 p 为预测概率， $x^{(i)}$ 为样本 x 的第 i 个特征， y 为样本 x 所对应的标签 j ， θ 为神经网络参数， θ_j 为标签 j 对应的神经网络参数， k 为标签的总数；此时，将工业控制入侵检测系统的对抗学习问题转化成如下优化问题：

$$\begin{aligned} x^* &= - \arg \min [p(x) = 0] \\ s.t. \quad d(x^*, x^0) &< d_{max} \end{aligned}$$

(5) 将步骤(4)生成的对抗样本在实际工业控制系统中进行测试,若能成功绕过工业控制入侵检测系统并且保留攻击效果则视为有效的对抗样本,否则舍弃该对抗样本。

以下以一个具体的应用场景为例,产生工业控制入侵检测系统对抗样本过程如下:

1. 嗅探得到现有的基于机器学习算法的工业控制系统入侵检测器所使用的通信数据;初始攻击样本包括注入攻击、功能码攻击、窃听攻击。
2. 进行协议解析,如西门子 S7comm 协议,解析得到源 IP,目的 IP,端口号,功能码,子功能码,包间隔时间等特征;
3. 在本地生成替代分类器,如用多层感知机生成基本的神经网络算法;
4. 根据该神经网络设计成优化求解问题,并加入该具体应用场景的使用约束,如功能码的固定选值,其他网络特征为离散正整数值等;
5. 利用 COBYLA 方法计算得到对抗样本,并在工业控制系统安全测试平台中测试其对抗效果,三种初始攻击样本的攻击成功率见图 2。通过图 2 可以看出,本发明方法对窃听攻击的攻击成功率达到 100%,对功能码攻击的攻击成功率达到 80%,注入攻击由于实际攻击复杂,较难完成原始攻击样本与对抗样本的转化,其攻击成功率仍然能够达到 20%。

上述实施例用来解释说明本发明,而不是对本发明进行限制,在本发明的精神和权利要求的保护范围内,对本发明作出的任何修改和改变,都落入本发明的保护范围。

权 利 要 求 书

1、一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，包含以下步骤：

(1) 对抗样本生成者对工业控制系统通信数据进行嗅探，获得与工业控制入侵检测系统所使用的训练数据同分布的通信数据，并对通信数据标记类别标签，其中的异常通信数据作为原始攻击样本。

(2) 对工业控制系统通信数据进行协议解析工作，识别、提取其中有效特征，包括：通信数据的源 IP 地址(SIP)、源端口号(SP)、目的 IP 地址(DIP)、目的端口号(DP)、包间隔时间(Time delta)、包发送时间(Time)、包功能码(Function code)等。

(3) 根据步骤(2)提取的有效特征建立机器学习分类器，利用有标签的工业控制系统通信数据对机器学习分类器进行训练，得到训练好的用于分辨正常或异常通信数据的分类器。

(4) 利用步骤(3)建立的分类器，将工业控制入侵检测系统的对抗学习问题转化成如下优化问题，求解优化问题得到最终的对抗样本。

$$\begin{aligned} x^* &= \arg \min g(x) \\ s.t. \quad d(x^*, x^0) &< d_{max} \end{aligned}$$

其中 $g(x)$ 为对抗样本 x^* 被判为异常样本的可能性，通过分类器计算得到； $d(x^*, x^0)$ 为对抗样本和原始攻击样本的距离， d_{max} 表示工业控制系统允许的最大欧式距离，即超过此距离对抗样本无恶意效果。

(5) 将步骤(4)生成的对抗样本在实际工业控制系统中进行测试，若能成功绕过工业控制入侵检测系统并且保留攻击效果则视为有效的对抗样本，否则舍弃该对抗样本。

2、根据权利要求 1 所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(1)中，对抗样本生成者应为黑盒攻击者，不能直接获得与工业控制入侵检测系统（检测方）完全相同的数据。

3、根据权利要求 1 所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(2)中，针对不同的工业控制系统通信协议可以提取出不同的有效特征。常用的工业控制系统通信协议包括 Modbus、PROFIBUS、DNP3、BACnet、Siemens S7 等。其中每种通信协议有对应的格式与应用场景，根据具体场景可以解析不同的通信协议，得出有效特征集合。

4、根据权利要求 1 所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(3)中，对抗样本生成者训练所用的分类器可以是和工业控制入侵检测系统不

一样的分类器，对抗样本生成者生成的分类器可被称为对抗学习的本地替代模型，其原理是對抗学习攻击的可迁移性。

5、根据权利要求1所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(4)中，具体优化问题解法包括梯度下降法、牛顿法、COBYLA (for Constrained Optimization BY Linear Approximations)方法等。

6、根据权利要求1所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(4)中，距离的表达方法包括一范式距离、二范式距离、无穷范式距离。

7、根据权利要求1所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(4)中，机器学习分类器采用神经网络，其概率计算方式如下：

$$p(y = j | x^{(i)}; \theta) = \frac{e^{\theta_j^T x^{(i)}}}{\sum_{l=1}^k e^{\theta_l^T x^{(i)}}}$$

其中 p 为预测概率， $x^{(i)}$ 为样本 x 的第 i 个特征， y 为样本 x 所对应的标签 j ， θ 为神经网络参数， θ_j 为标签 j 对应的神经网络参数， k 为标签的总数；

将工业控制入侵检测系统的对抗学习问题转化成如下优化问题：

$$\begin{aligned} x^* &= -\arg \min [p(x) = 0] \\ \text{s.t. } d(x^*, x^0) &< d_{\max} \end{aligned}$$

8、根据权利要求1所述的一种基于对抗学习的工业控制系统恶意样本生成方法，其特征在于，所述步骤(4)中，对于特定控制场景，需要在优化问题中加入对变量的特殊约束，即该方法在应用时，为保证生成的对抗样本能有效的完成恶意攻击效果，生成者需要根据特定的场景对特定维度的变量在做优化问题设计时加上不同的约束条件。

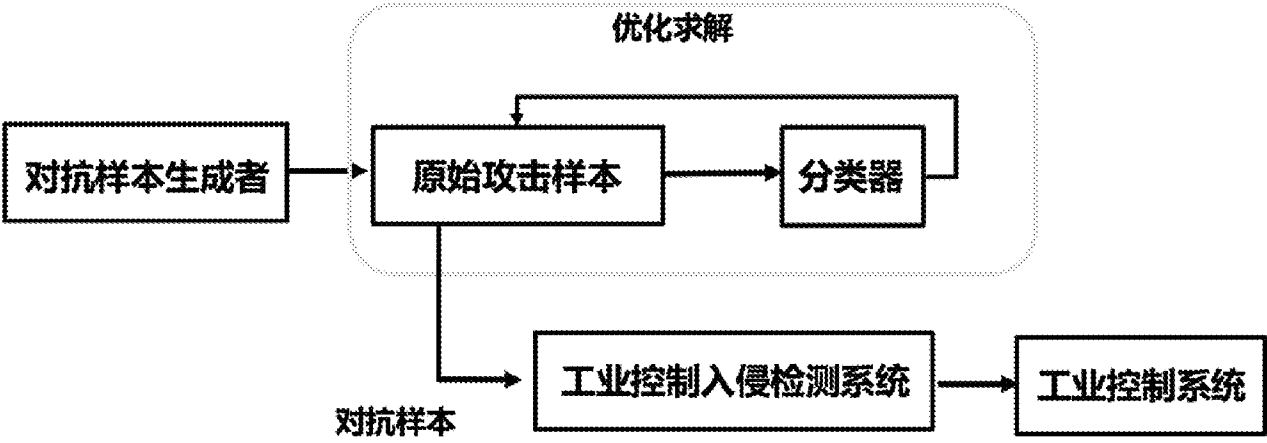


图 1

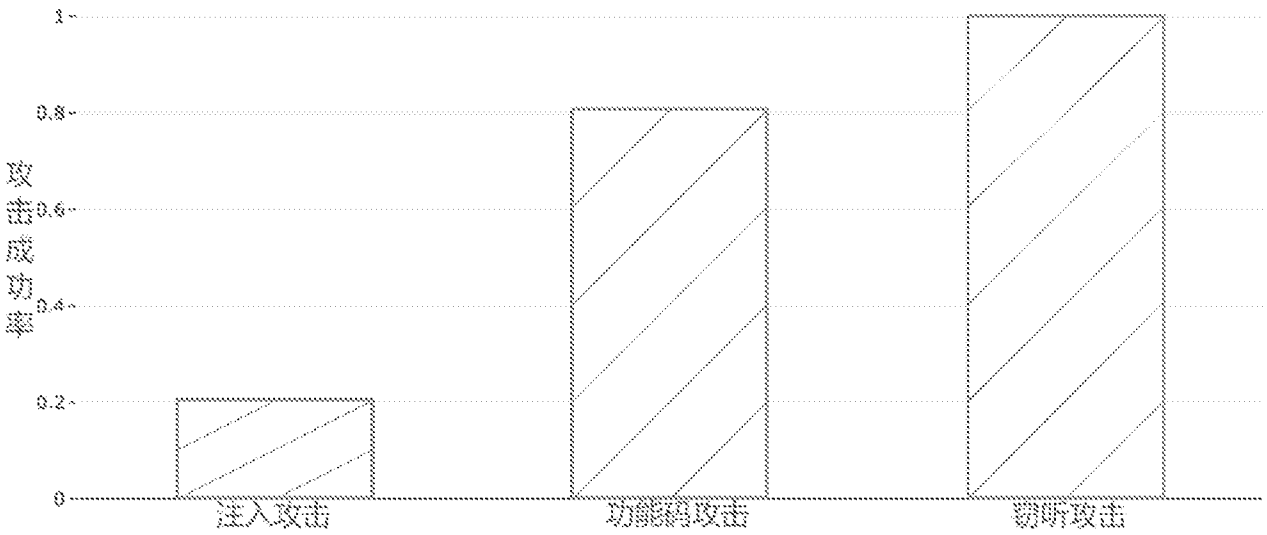


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/101247

A. CLASSIFICATION OF SUBJECT MATTER G06K 9/62(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC																	
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06K Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) CNABS, CNTXT, VEN, USTXT, WOTXT, EPTXT, CNKI: 对抗学习, 恶意, 工业控制, 距离, 分类器, 样本, anti-learning, malicious, industrial control, distance, classifier, sample																	
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 109902709 A (ZHEJIANG UNIVERSITY) 18 June 2019 (2019-06-18) entire document</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 108509966 A (GU, Zecang) 07 September 2018 (2018-09-07) description, paragraphs 60-74</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 108171266 A (CHINA UNIVERSITY OF MINING AND TECHNOLOGY) 15 June 2018 (2018-06-15) description, paragraphs 11-29, and figure 1</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 26 January 2006 (2006-01-26) entire document</td> <td>1-8</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	PX	CN 109902709 A (ZHEJIANG UNIVERSITY) 18 June 2019 (2019-06-18) entire document	1-8	A	CN 108509966 A (GU, Zecang) 07 September 2018 (2018-09-07) description, paragraphs 60-74	1-8	A	CN 108171266 A (CHINA UNIVERSITY OF MINING AND TECHNOLOGY) 15 June 2018 (2018-06-15) description, paragraphs 11-29, and figure 1	1-8	A	WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 26 January 2006 (2006-01-26) entire document	1-8
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.															
PX	CN 109902709 A (ZHEJIANG UNIVERSITY) 18 June 2019 (2019-06-18) entire document	1-8															
A	CN 108509966 A (GU, Zecang) 07 September 2018 (2018-09-07) description, paragraphs 60-74	1-8															
A	CN 108171266 A (CHINA UNIVERSITY OF MINING AND TECHNOLOGY) 15 June 2018 (2018-06-15) description, paragraphs 11-29, and figure 1	1-8															
A	WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 26 January 2006 (2006-01-26) entire document	1-8															
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.																	
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “E” earlier application or patent but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family																	
Date of the actual completion of the international search 08 November 2019		Date of mailing of the international search report 20 November 2019															
Name and mailing address of the ISA/CN China National Intellectual Property Administration No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088 China Facsimile No. (86-10)62019451		Authorized officer Telephone No.															

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/101247

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109902709	A	18 June 2019	None			
CN	108509966	A	07 September 2018	None			
CN	108171266	A	15 June 2018	None			
WO	2006007633	A1	26 January 2006	US	2008027886	A1	31 January 2008
				AU	2005263171	B	17 November 2011
				AU	2005263171	A1	26 January 2006

国际检索报告

国际申请号

PCT/CN2019/101247

A. 主题的分类 G06K 9/62 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																	
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) G06K 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS, CNTXT, VEN, USTXT, WOTXT, EPTXT, CNKI: 对抗学习, 恶意, 工业控制, 距离, 分类器, 样本, anti-learning, malicious, industrial control, distance, classifier, sample																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 109902709 A (浙江大学) 2019年 6月 18日 (2019 - 06 - 18) 全文</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 108509966 A (顾泽苍) 2018年 9月 7日 (2018 - 09 - 07) 说明书第60-74段</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>CN 108171266 A (中国矿业大学) 2018年 6月 15日 (2018 - 06 - 15) 说明书第11-29段, 图1</td> <td>1-8</td> </tr> <tr> <td>A</td> <td>WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 2006年 1月 26日 (2006 - 01 - 26) 全文</td> <td>1-8</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 109902709 A (浙江大学) 2019年 6月 18日 (2019 - 06 - 18) 全文	1-8	A	CN 108509966 A (顾泽苍) 2018年 9月 7日 (2018 - 09 - 07) 说明书第60-74段	1-8	A	CN 108171266 A (中国矿业大学) 2018年 6月 15日 (2018 - 06 - 15) 说明书第11-29段, 图1	1-8	A	WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 2006年 1月 26日 (2006 - 01 - 26) 全文	1-8
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
PX	CN 109902709 A (浙江大学) 2019年 6月 18日 (2019 - 06 - 18) 全文	1-8															
A	CN 108509966 A (顾泽苍) 2018年 9月 7日 (2018 - 09 - 07) 说明书第60-74段	1-8															
A	CN 108171266 A (中国矿业大学) 2018年 6月 15日 (2018 - 06 - 15) 说明书第11-29段, 图1	1-8															
A	WO 2006007633 A1 (NATIONAL ICT AUSTRALIA LIMITED) 2006年 1月 26日 (2006 - 01 - 26) 全文	1-8															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																	
国际检索实际完成的日期 2019年 11月 8日		国际检索报告邮寄日期 2019年 11月 20日															
ISA/CN的名称和邮寄地址 中国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 古志春 电话号码 86-(20)-28950386															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/101247

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	109902709	A	2019年 6月 18日	无			
CN	108509966	A	2018年 9月 7日	无			
CN	108171266	A	2018年 6月 15日	无			
WO	2006007633	A1	2006年 1月 26日	US	2008027886	A1	2008年 1月 31日
				AU	2005263171	B	2011年 11月 17日
				AU	2005263171	A1	2006年 1月 26日