工业互联网边缘终端初始接入可信度量方法研究

于亚[1,2]，伏玉笋[2,3,4]
（1. 上海交通大学宁波人工智能研究院，浙江 宁波 315000；2. 上海交通大学电子信息与电气工程学院，上海 200240；
3. 系统控制与信息处理教育部重点实验室，上海 200240；4. 上海工业智能管控工程技术研究中心，上海 200240）

摘 要：离散制造业的发展呈现智能、开放和协同的趋势，大量异构设备接入工业互联网，给安全带来了严重挑战，因此，引入信任管理和对设备进行可信度量的初始接入显得尤为重要。为了更加及时准确地评估初始接入系统的边缘终端的可信程度，创新性地提出了一种基于设备漏洞数据库的可信度量方法。该方法采用云边协同的架构，在中央云端建立设备信息库和漏洞数据库，然后在边缘端计算终端风险因子，最后完成对接入终端的信任初始化。仿真结果表明，该方法很好地兼顾了系统的性能和安全。

关键词：工业互联网；设备接入；安全；信任管理；可信度量；漏洞评估
中图分类号：TN915.08
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2022.00292

Research on trust measurement method for initial access of industrial internet edge terminals

YU Ya[1,2]，FU Yusun[2,3,4]
1. Ningbo Artificial Intelligence Institute of Shanghai Jiao Tong University, Ningbo 315000, China
2. School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
3. Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China
4. Shanghai Engineering Research Center of Intelligent Control and Management, Shanghai 200240, China

Abstract: The development of the discrete manufacturing shows a trend of intelligence, openness and collaboration. As a result, many heterogeneous devices are connected to the industrial internet, which brings serious challenges to the security. Therefore, it is particularly important to introduce trust management and trusted access to devices for trusted measurement. In order to more timely and accurately evaluate the trustworthiness of the edge terminal initially accessing the system, a trustworthiness measurement method based on the device vulnerability database was innovatively proposed. This method adopted the architecture of cloud-edge collaboration, established a device information database and a vulnerability database in the central cloud, and then calculated the terminal risk factor at the edge. Finally, the trust initialization of the access terminal was completed. The simulation results show that the method can well balance the efficiency and security of the system.

Key words: industrial internet, device access, security, trust management, trust measurement, vulnerability assessment

0 引言

随着德国工业 4.0、美国工业互联网和中国“制造强国”等国家层面战略的陆续提出，网络物理系统与云计算、物联网和大数据等技术深度融合，离散制造业呈现智能、开放和协同的发展趋势。大量传感器、

收稿日期：2022−06−07 ；**修回日期：**2022−08−04
通信作者：伏玉笋，fu_yusun@sina.com
基金项目：国家重点研发计划（No.2019YFB1705703）；宁波市重大科技任务攻关项目（No.2021Z022）
Foundation Item: The National Key Research and Development Program of China (No.2019YFB1705703), The Major Scientific and Technological Research Program of Ningbo (No.2021Z022)

控制器等基础设施通过网络互连互通，成为物理世界与信息世界的桥梁[1]。物理资源和能力数字化，离散工业领域支持位置分布与功能异构的设备按需动态共享与协同，融合工业互联网平台的智能分析和决策，从而实现由过去的单一化定制到柔性生产、满足个性化需求的大规模定制的生产模式的转变[2-3]。

安全保障、网络和云平台建设并列为工业互联网三大体系之一[4]。其中工业互联网云平台一方面承载着异构工业设备接入、海量数据接收的任务，另一方面执行着数据处理、分析、决策和监控的任务，从而科学地整合更多生产要素，实现设备的管理和控制、现场数据的监控和生产过程的优化等[5]。但是这也意味着将原来封闭的工业设备与数据充分暴露在互联网之下，给安全保障带来了极大的挑战。

早期的工业控制系统与互联网物理隔离，无须过多地考虑网络信息安全，因此工控领域中的设备甚至系统在设计之初更加关注功能和效率。目前，工业中的大量存量设备存在硬件缺陷[6-7]和软件漏洞[8]，缺乏认证机制[9-11]，缺乏数据保护机制[6-7,12-13]，在异构性[8]等方面具有一定的脆弱性。在开放的趋势下，越来越多的黑客瞄向工业场景，而边缘终端也成为被重点攻击的对象[8]。

目前云平台应用于接入终端的安全防护措施，多采用设备鉴权的方式验证终端身份的合法性，无法监控终端成功接入后的行为。例如，腾讯云物联网平台基于安全传输层（TLS, transport layer security）协议采用预共享密钥（PSK, pre-shared key）和证书的鉴权方式；阿里云物联网平台采用 X.509 证书、CA 证书和物联网设备标识（ID2, internet device ID）的鉴权方式；百度智能云天工物联网平台采用密钥和证书的鉴权方式；华为云物联网平台采用密钥和证书的鉴权方式，不同物联网平台的设备接入鉴权见表 1。

表 1　不同物联网平台的设备接入鉴权

物联网平台	支持协议	设备接入鉴权方式
腾讯云物联网平台	MQTT、HTTP	证书，密钥
	CoAP	DTLS 协议+密钥
阿里云物联网平台	MQTT	X.509 证书、CA 证书、ID2 证书
百度智能云天工物联网平台	MQTT	密钥，证书
华为云物联网平台	LwM2M、CoAP	DTLS 协议+密钥
	MQTT	X.509 证书、CA 证书，密钥
	HTTPS	证书

这些鉴权方式以身份认证为核心，通过密钥、证书等方式验证终端身份的合法性，从而达到保障合法终端接入的目的。然而工业领域具有特殊性，终端往往在一次接入鉴权后长期运作[14]。当终端成功接入云平台后，攻击者再入侵合法终端、获得操作权限，并控制终端在系统内进行恶意行为或者窃取生产数据，此时工业互联网云平台的认证鉴权方式无法保障终端和生产系统的安全。

而信任管理模型和可信度量技术可以对终端的行为建模，实时监控终端的行为，防止合法身份的终端做出不合法行为[15]。信任管理应用于边缘终端安全接入的流程如图 1 所示。

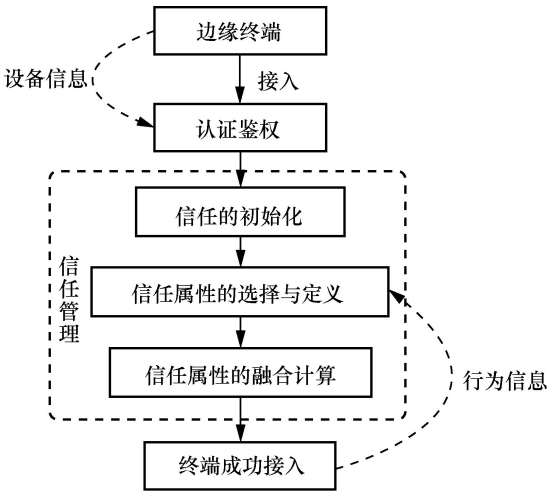


图 1　信任管理应用于边缘终端安全接入的流程

可信度量通常包括信任的初始化、信任属性的选择与定义和信任属性的融合计算 3 个步骤。然而现有的信任管理模型大多聚焦于信任属性的选择[16-20]和信任属性的融合计算[21-24]，对信任的初始化方法关注较少。信任的初始化是赋予接入系统的终端信任初值的过程，也是准确计算信任值的先决条件。如果赋值较高，节点将具有较高的权限，使系统容易受到新加入节点的攻击[25]；赋值较低又会限制接入终端的交互能力，导致整个系统的性能不高[26]。尤其对于安全要求比较高的场景，如工业物联网，初值的设置就显得尤为重要。

目前信任的初始化用于解决两类接入终端的问题：一是初次加入系统、且与系统内其他终端不存在交互行为的终端；二是与系统内终端产生过交互、离开后又重新接入系统的终端。对于后者，目前已经提出了概率统计[27]和数据挖掘等方法[28]，利用系统记录的历史交互信息，完成信任的初始化。然而对于前者，

大多采用统一赋值的方法，即对所有初始接入的终端赋予同一个信任值，常见的有最低值[25]、平均值[29]和最高值。然后设置信任属性和融合算法，通过终端的行为计算信任值。然而，由于信任具有滞后性，统一赋初值的方法通常需要更多的交互数据才能让系统计算出相对准确的信任值。这意味着倘若恶意终端接入工业系统，只有进行更多的恶意操作才能被发现，这显然不符合工业互联网的安全要求。

在此背景下，本文提出了边缘终端初始接入可信度量方法，利用工控设备漏洞数据库评估接入终端可信度。该方法采用云边协同的架构，在中央云端建立设备信息库和漏洞数据库，并基于工控系统的特殊性进行漏洞评估，然后在边缘端计算终端风险因子，最后完成对接入终端更加准确的信任初始化。

1　终端接入可信评估架构与流程

本文提出的方法需要建立设备信息库和对应设备的漏洞数据库，由于两个库对存储资源的要求比较高，也不需要频繁维护，因此选择将库部署在中央云服务器。同时在边缘网关处部署可信通信代理，采用云边协同架构下的应用协同方式，完成对初始接入终端的可信度量。

云边协同架构主要由中央云服务器与边缘网关两部分组成。其中，中央云服务器中部署设备信息库、漏洞数据库、漏洞评估模块和审计数据库；边缘网关中部署可信通信代理，可信通信代理中设置了设备扫描模块、协议转换模块、可信度量模块和信任数据库。当一个边缘终端接入网络后，先由边缘服务器进行扫描，并将扫描的设备信息上传至中央云服务器，经过准确识别并计算后将结果下载至边缘网关，最后由可信通信代理中的可信度量模块完成对接入终端的信任初始化，边缘终端接入可信评估架构和流程如图 2 所示。

- 设备信息库：存储种类、功能、品牌尽可能全面的终端数据，包括设备型号、软件版本、通信协议。
- 漏洞数据库：存储对应终端已被挖掘的漏洞信息集合，包括漏洞编号、危害等级、漏洞公开时间、补丁信息、漏洞评估指标。
- 漏洞评估模块：基于漏洞信息集合计算边缘终端的终端风险因子。
- 审计数据库：存储终端节点的数据和网络的运行状况。
- 设备扫描模块：与边缘终端直连，扫描设备的固件信息和通信报文。
- 协议转换模块：终端使用的协议众多，上传时该模块需要解析并转换为统一协议的数据报文上传至云服务器，下载时该模块将云服务的报文封装为对应终端所使用协议的数据报文并发送。
- 可信度量模块：终端接入后根据云端信息计算其初始信任值，终端运行后实时计算其动态信任度。
- 信任数据库：存储系统内终端的实时信任值。

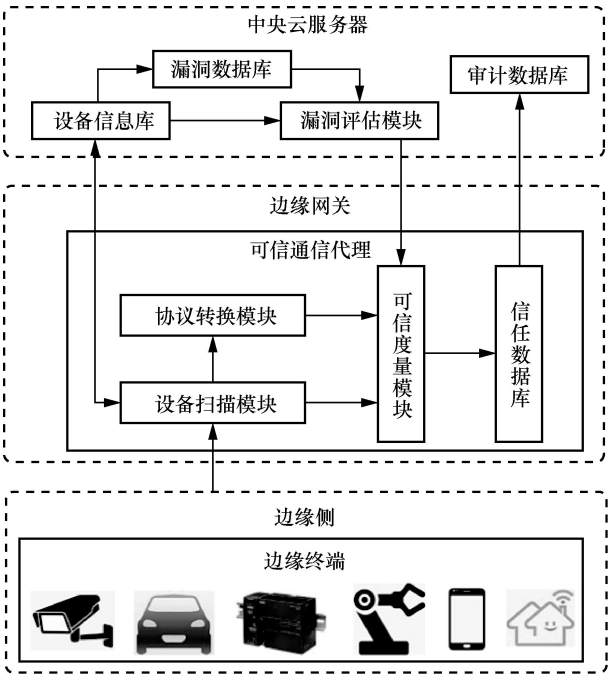


图 2　边缘终端接入可信评估架构和流程

在该评估架构下，具体评估流程如下。

步骤 1　终端接入网络后，可信通信代理中的设备扫描模块扫描终端信息后上传至设备信息库。

步骤 2　设备信息库根据扫描信息准确识别终端设备，并将漏洞数据库中对应终端的漏洞信息集合发送至漏洞评估模块。

步骤 3　漏洞评估模块计算后得到终端风险因子。终端风险因子的计算服从以下规则：漏洞等级越高，风险因子越高；漏洞公开时间越短，风险因子越高；补丁信息越少，风险因子越高；漏洞分数越高，风险因子越高；攻击途径越简单，风险因子越高；攻击复杂性越低，风险因子越高；攻击时所需认证越少，风险因子越高；对机密性（完整性、可用性）的影响越大，风险因子越高。

步骤 4 可信度量模块基于终端功能、终端风险因子和安全等级要求，计算终端的初始信任度。初始信任度的计算服从以下规则：终端功能越强大，初始信任度越高；终端风险因子越低，初始信任度越高；网络安全等级要求越低，初始信任度越高。

步骤 5 边缘终端成功接入，开始工作。

2 基于漏洞数据库的可信接入评估方法

2.1 设备信息库和漏洞数据库的建立

设备接入系统后，代理网关通常仅可获取到设备的品牌和型号信息。基于工控系统对安全的高要求，本文从国家信息安全漏洞共享平台（CNVD, China National Vulnerability Database）、中国国家信息安全漏洞库（CNNVD, China National Vulnerability Database of Information Security）和工业控制系统网络应急小组（ICS-CERT, The Industrial Control Systems Cyber Emergency Response Team）3 个网站搜集工控设备的固件漏洞信息构建知识库，利用先验知识完成对工控接入终端初始信任值的赋值。

本文收集了工业控制系统和物联网智能终端设备等 1 500 余条漏洞的详细信息，包括漏洞名称、漏洞编号、危害等级、公开时间、补丁信息、漏洞描述和通用漏洞评分系统（CVSS, common vulnerability scoring system）[30]具体指标，部分漏洞数据库的漏洞详细信息见表 2。

2.2 工控系统漏洞评估

目前信息，安全领域中对漏洞的量化评估，主要以美国国家漏洞数据库（NVD，National Vulnerability Database）采用的 CVSS 标准为主。CVSS 采用基础（base）、时间（temporal）和环境（environmental）3 组指标描述软件漏洞不同方面的严重性程度。其中，基础指标描述软件漏洞的固有特征反映漏洞的严重性，且这些特征不随时间和应用环境改变；时间指标与漏洞利用技术或代码可用性、是否存在补丁程序或者漏洞描述的可信度有关，且这些特征会随着时间变化；环境指标与受影响的组件的应用场景、对用户的重要性等参数相关。

国内的信息安全漏洞库中也多使用 CVSS 的基础指标对漏洞进行风险评估，基于目前最新的 CVSS v3.1 版本，基础指标共包含以下 8 组参数：攻击向量 AV（attack vector）、攻击复杂性 AC（attack complexity）、特权要求 PR（privileges required）、用户交互 UI（user interaction）、影响范围 S（scope）、机密性影响 CF（confidentiality impact）、完整性影响 I（integrity impact）和可用性影响 A（availability impact）。

然而，陶耀东[31]指出，CVSS 标准更加侧重信息安全，并未充分考虑工业控制系统中安全的特殊性。因此，陶耀东结合工业场景中的安全需求和 CVSS 基础指标，将可见性和可控性等体现工控安全特性的指标纳入评估范围，提出了一种基于 CVSS v3.0 的工控漏洞评分系统 IVSS（industrial vulnerability scoring system）。IVSS 中对可见性和可控性的描述如下：可见性反映工业控制系统的画面功能和监控功能。其中画面功能描述工业过程的当前状态，监控功能表示监视过程的当前状态，包括液位、温度、阀门等；可控性反映工控系统对阀门、控制器等引起现场工艺过程变化的组件的控制能力。

相较 CVSS v3.0，CVSS v3.1 版本虽然没有引入新的度量标准，也未对现有计算式进行重大修改，但是对攻击复杂性、特权要求、攻击范围等提供了更为合理的指南和计算规则。因此本文基于最新的 CVSS v3.1，更新了 IVSS 评估算法，并使用更新后的算法对漏洞数据库中的漏洞进行风险评估，IVSS 基础指标量化标准见表 3。

表 2 部分漏洞数据库的漏洞详细信息

设备名称	漏洞编号	危害等级	CVSS 评分	漏洞描述
ABB 工业机器人示教器	CNVD-2020-49104	中	5	存在加密算法漏洞，攻击者可利用漏洞破解出 ABB 工业机器人的用户密码
ACSSpiiPlusEC-08 运动控制器	CNVD-2020-75690	高	7.8	存在拒绝服务漏洞，攻击者可利用该漏洞发起拒绝服务攻击
CC-PCNT02 控制器	CNVD-2020-62870	中	6.1	存在拒绝服务漏洞，攻击者可利用该漏洞造成拒绝服务
Siemens S7-200 控制器	CNVD-2019-40162	中	6.6	攻击者可以通过伪造数据绕过身份认证从而任意篡改 PLC 寄存器的值
Bit defender BOX 智能家居安全控制设备	CNVD-2020-15145	高	7.6	存在安全漏洞，源于网络系统或产品的代码开发过程中存在设计或实现不当的问题
Cisco 809 Industrial ISRs 工业路由器	CNVD-2020-31825	高	10	存在缓冲区溢出漏洞，源于错误的边界检查。远程攻击者可通过发送恶意的数据包利用该漏洞造成系统崩溃并重新加载

表 3　　IVSS 基础指标量化标准

指标	指标值	数值
攻击向量 AV	网络	0.85
	局域	0.62
	本地	0.55
	物理	0.2
攻击复杂性 AC	低	0.77
	高	0.44
未超出影响范围的所需权限 PR（privileges required/unchanged scope）	无	0.85
	低	0.62
	高	0.27
超出影响范围时的所需权限 PR（privileges required/changed scope）	无	0.85
	低	0.68
	高	0.5
用户交互 UI（user interaction）	无要求	0.85
	有要求	0.62
机密性影响 CF、完整性影响 I、可用性影响 A、可见性影响 V、可控性影响 CT	无	0
	中	0.22
	高	0.56

输入漏洞信息后将各个分值带入式(1)～式(7)。其中，ISS 表示影响子分数，IMPACT 表示影响因子，EXPLOIT 表示可利用性因子，BS 表示 IVSS 的基础指标得分。

$$\mathrm{ISS}=1-((1-\mathrm{CF})\times(1-I)\times(1-A)\times(1-V)\times(1-\mathrm{CT})) \tag{1}$$

若 ISS≥0，且影响范围 Scope 为 Unchanged，则

$$\mathrm{IMPACT}=6.42\times\mathrm{ISS} \tag{2}$$

若 ISS≥0 且影响范围 Scope 为 Changed，则

$$\mathrm{IMPACT}=7.52\times(\mathrm{ISS}-0.029)-3.25\times(\mathrm{ISS}-0.02)^{15} \tag{3}$$

$$\mathrm{EXPLOIT}=8.22\times\mathrm{AV}\times\mathrm{AC}\times\mathrm{PR}\times\mathrm{UI} \tag{4}$$

若 $\mathrm{ISS}<0$，则

$$\mathrm{BS}=0 \tag{5}$$

若 $\mathrm{ISS}<0$ 且影响范围 Scope 为 Unchanged，则

$$\mathrm{BS}=\mathrm{Roundup}(\mathrm{Min}((\mathrm{ISC}+\mathrm{ESC}),10)) \tag{6}$$

若 $\mathrm{ISS}<0$ 且影响范围 Scope 为 Changed，则

$$\mathrm{BS}=\mathrm{Roundup}(\mathrm{Min}(1.08\times(\mathrm{ISC}+\mathrm{ESC}),10)) \tag{7}$$

其中，Roundup 函数，保留一位小数，并向上取整；Min 函数，取最小值。

基于工控系统漏洞评估的结果，将漏洞风险等级划分为低危、中危、高危和极危，漏洞风险划分依据见表 4。

表 4　　漏洞风险划分依据

等级	IVSS 评分
低危	0.1～3.9
中危	4.0～6.9
高危	7.0～8.9
极危	9.0～10.0

2.3　基于终端风险因子的信任值初始化方法

本文建立信任值初始化的规则为：终端的能力越强，其信任初值越高；终端的风险越高，其信任初值越低；接入系统的安全要求越高，终端的信任初值越低。因此，本文引入了终端功能系数 fun，终端风险因子 Risk 和接入系统的安全等级要求 Req，提出了基于终端风险因子的信任值初始化方法。其中，本文将漏洞数据库和工控系统漏洞评估结果作为先验信息，用于计算终端风险因子 Risk。

$$\mathrm{Risk}=\sum_{i\in C}\frac{w_{\mathrm{level}}\times\mathrm{BS}_i}{N} \tag{8}$$

$$w_{\mathrm{level}}=\frac{n_{\mathrm{level}}}{N} \tag{9}$$

其中，Risk 反映终端的受信任程度；C 表示漏洞数据库中对应终端的漏洞集合；N 表示集合 C 中的漏洞数量；BS_i 表示第 i 条漏洞的评估结果；W_{level} 表示第 i 条漏洞的权重，其计算方法如式(9)所示；n_{level} 表示漏洞等级为 level 的漏洞数量，level 的取值有低危、中危、高危和极危。

由于异构性，不同边缘终端的 Risk 存在差异较大的情况，考虑激励机制[32]（给风险因子低的终端相对高的信任初值）和惩罚机制（给风险因子高的终端相对低的信任初值），本文引入了速率调节因子 $\alpha(\alpha\geqslant 1)$。计算终端风险因子后，终端初始信任值 T_0 为

$$T_0=\mathrm{fun}\times\mathrm{e}^{-\left(\frac{\mathrm{risk}}{\alpha}+\mathrm{Req}\right)},\mathrm{Req}\in[0,0.5],\mathrm{fun}\in[0.5,1] \tag{10}$$

初始信任值与参数 Risk 和 α 的关系如图 3 所示，可以看出，Req 决定了曲线的起点高度，α 决定了曲线的下落速度。

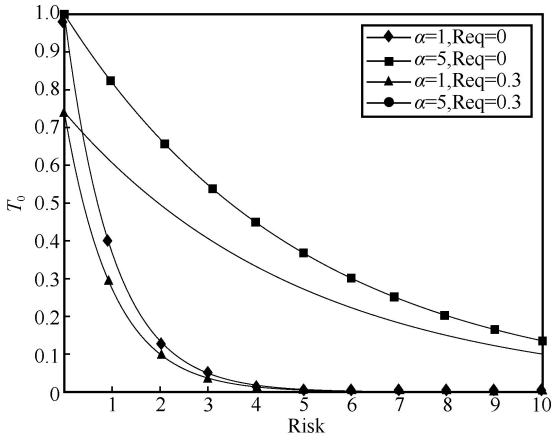


图 3 初始信任值与 Risk 和 α 的关系

3 仿真测试

目前主要的信任值初始化方法有最小值，平均值和最大值 3 种。为了证明本文提出的初始化方法的有效性，设计了仿真测试，从交互成功率和恶意终端参与率这两个角度对方法进行评估。交互成功率代表系统的效率，计算方法为

$$\text{交互成功率}=\frac{\text{交互成功次数}}{\text{交互总次数}}\times 100\% \tag{11}$$

恶意终端参与率代表系统的安全性，计算方法为

$$\text{恶意终端参与率}=\frac{\text{参与交互的恶意终端数量}}{\text{恶意终端总数}}\times 100\% \tag{12}$$

仿真采用的设备性能如下：CPU 型号为 i7-8700，机带 RAM 容量为 16 GB，硬盘容量为 512 GB，显卡型号为 GTX1060。仿真采用 NetLogo 事件模拟器，接入终端总数为 1 000 台，其中包括 20%的高性能终端和 80%的低性能终端。仿真详细参数设置见表 5。

表 5 仿真详细参数设置

参数	参数设置	
终端	总数	1 000
	高性能终端占比	20%
	低性能终端占比	80%
恶意终端占比	10%	
	20%	
	40%	
交互任务设置	复杂任务比例	10%
	中等任务比例	30%
	简单任务比例	60%
信任度要求	复杂任务	[0.7,1.0]
	中等任务	[0.4,0.7]
	简单任务	[0,0.4]

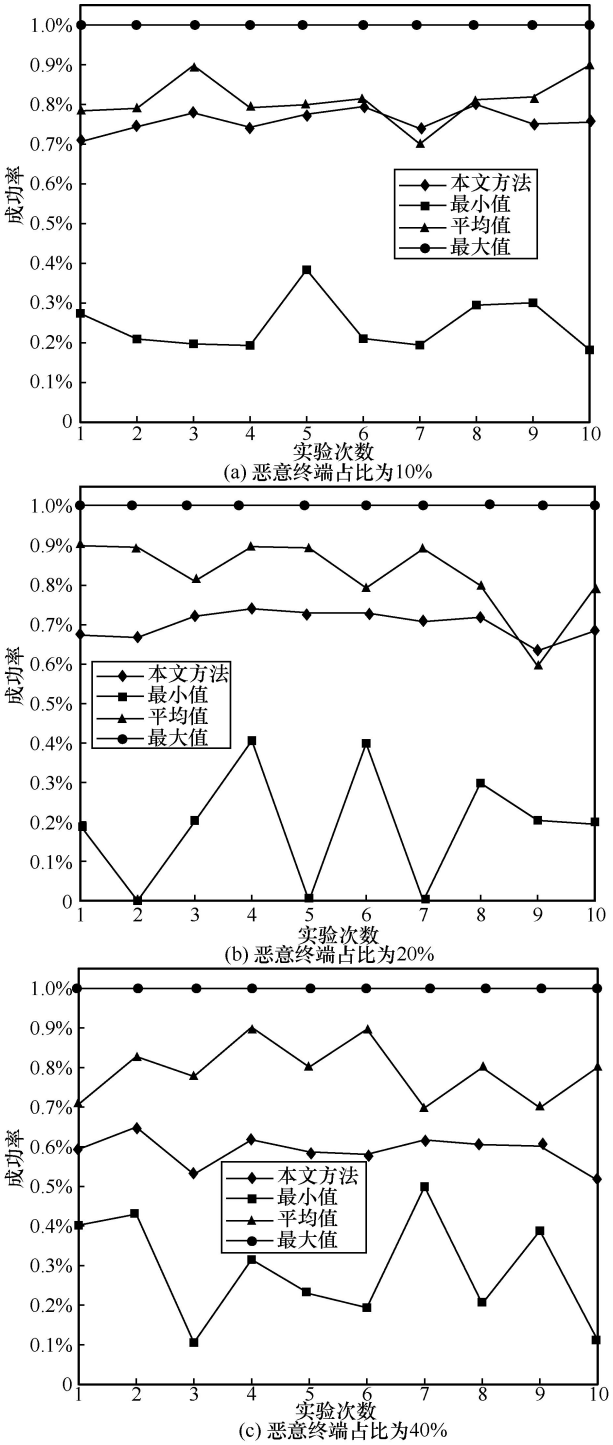
为了贴合实际场景，仿真设置了 10%的复杂性任务、30%的中等任务和 60%的简单任务。其中，简单任务对资源和信任度的要求低，复杂任务对资源和信任度的要求高，中等任务介于两者之间。为了验证本文方法面对攻击的防护能力，在仿真中分别随机设置了 10%、20%和 40%的恶意终端（离散系统中恶意终端占比超过 40%具有一定的特殊性，实际意义不大，因此本文暂不考虑更高的占比情况），并与目前主要的最小值法、平均值法和最大值法对比。

为了模拟真实交互的情况，仿真并没有固定终端之间的交互顺序，而是设置了一定的随机性。终端随机移动，相遇时代表产生一次交互，每次交互随机分配任务，当服务提供方节点满足任务要求时，则交互成功。由于交互的随机性，每次仿真的结果不完全一致。因此对于每种场景，本文都进行了多次独立的仿真测试，并随抽取 10 次测试结果，最后计算平均值和方差等统计特征。

不同恶意终端占比下的系统交互成功率如图 4 所示。不同恶意终端占比下的交互成功率统计结果见表 6。通过仿真结果可得，最大值的信任初始化方法使得系统内所有参与交互的终端都满足信任值的阈值，因此交互成功率最高，始终保持在 100%；反之，最小值的信任初始化方法使得交互成功率保持在一个最低的水平；平均值的信任初始化方法使得交互成功率保持较高的水平，在不同恶意终端占比下始终保持 80%左右的平均成功率，但是具有较高的方差；相对而言，本文提出的信任初始化方法，在恶意终端占比为 10%、20%和 40%的情况下，平均交互成功率分别保持在 75%、70%和 60%，而且具有较小的方差，可以更好地应用于存在恶意终端攻击的离散制造系统中。

不同恶意终端占比下的恶意终端参与率如图 5 所示。通过仿真结果可得，在不同的恶意终端占比下，恶意终端参与率的仿真结果具有较高的一致性。具体地，最大值和平均值的信任初始化方法，其恶意终端参与率相对较高；而最小值和本文提出的方法，恶意终端参与率操持在一个较低的水平，且这种结果相对比较稳定，与恶意终端占比的相关性不高。

综上所述，通过交互成功率和恶意终端参与率

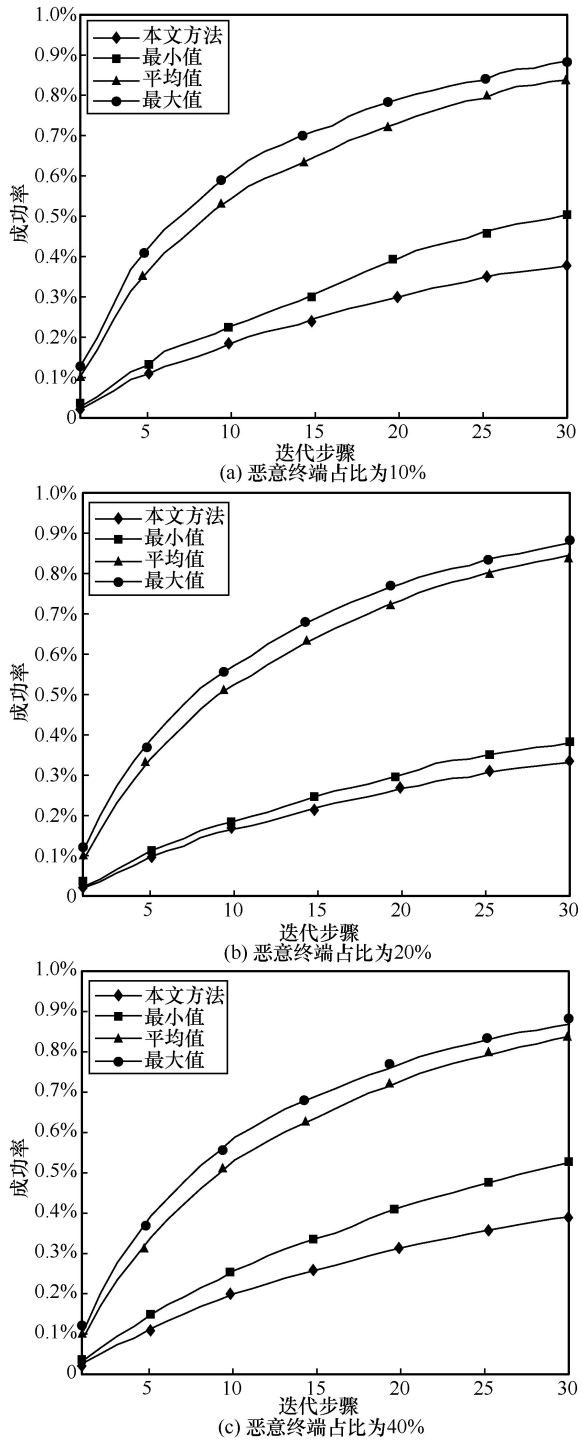


(a) 恶意终端占比为10%

(b) 恶意终端占比为20%

(c) 恶意终端占比为40%

图 4　不同恶意终端占比下的系统交互成功率



(a) 恶意终端占比为10%

(b) 恶意终端占比为20%

(c) 恶意终端占比为40%

图 5　不同恶意终端占比下的恶意终端参与率

表 6　　**不同恶意终端占比下的交互成功率统计结果**

对比项	恶意终端占比为 10%的交互成功率		恶意终端占比为 20%的交互成功率		恶意终端占比为 40%的交互成功率	
	平均值	方差($\times10^{-3}$)	平均值	方差($\times10^{-3}$)	平均值	方差($\times10^{-3}$)
本文方法	75.9%	8.2	70.1%	1.19	59.0%	1.63
最小值	24.4%	44	18.9%	23.42	28.8%	19.15
平均值	81.1%	325	82.8%	9.03	79.1%	55
最大值	100%	0	100%	0	100%	0

的曲线图可以看出，与目前主流的信任初始化方法相比，本文提出的方法可以在保证较高交互成功率的基础上，使得恶意终端参与率保持较低的水平，即在保证系统效率的同时，兼顾了系统的安全性。

4　结束语

鉴于目前主流的信任初始化方法无法满足安全要求高的场景的问题，本文提出了工业互联网边缘终端初始接入的可信度量方法。首先介绍了终端接入可信评估架构和流程，给出了基于漏洞数据库的终端可信接入评估方法；然后构建了设备信息库和漏洞数据库，采用工控系统漏洞评估结果引入了终端风险因子；最后基于终端信息和风险因子完成更加精确的信任值初始化，并且基于仿真测试证明了本文提出的方法的有效性。需要说明的是，可信度量包括初始度量和过程度量，未来可在过程度量方面开展进一步研究。

参考文献：

[1] 陶永, 蒋昕昊, 刘默, 等. 智能制造和工业互联网融合发展初探[J]. 中国工程科学, 2020, 22(4): 24-33.
TAO Y, JIANG X H, LIU M, et al. A preliminary study on the integration of intelligent manufacturing and industrial internet[J]. Strategic Study of CAE, 2020, 22(4): 24-33.

[2] 陶利民. 开放网络环境下基于不确定性理论的主观信任管理研究[D]. 杭州: 浙江工业大学, 2013.
TAO L M. Research on subjective trust management based on uncertainty theory under open network environment[D]. Hangzhou: Zhejiang University of Technology, 2013.

[3] 冯玉翔. 大规模分布式环境下动态信任管理机制的研究[D]. 广州: 华南理工大学, 2013.
FENG Y X. Research on dynamic trust management for large scale distributed environment[D]. Guangzhou: South China University of Technology, 2013.

[4] 边缘计算产业联盟, 工业互联网产业联盟. 边缘计算与云计算协同白皮书 2.0[R]. 2020.
Edge Computing Consortium (ECC), Alliance of Industrial Internet (AII). Edge computing and cloud computing collaboration white paper 2.0[R]. 2020.

[5] 董悦, 王志勤, 田慧蓉, 等. 工业互联网安全技术发展研究[J]. 中国工程科学, 2021, 23(2): 65-73.
DONG Y, WANG Z Q, TIAN H R, et al. Development of industrial internet security technology in China[J]. Strategic Study of CAE, 2021, 23(2): 65-73.

[6] CLEMENS J, PAL R, PHILIP P. Poster abstract: extending trust and attestation to the edge[C]//Proceedings of 2016 IEEE/ACM Symposium on Edge Computing (SEC). Piscataway: IEEE Press, 2016: 101-102.

[7] SHAPSOUGH S, ALOUL F, ZUALKERNAN I A. Securing low-resource edge devices for IoT systems[C]//Proceedings of 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI). Piscataway: IEEE Press, 2018: 1-4.

[8] 张鑫, 杨晓元, 朱率率, 等. 物联网环境下移动节点可信接入认证协议[J]. 计算机应用, 2016, 36(11): 3108-3112.
ZHANG X, YANG X Y, ZHU S S, et al. Trusted access authentication protocol for mobile nodes in Internet of Things[J]. Journal of Computer Applications, 2016, 36(11): 3108-3112.

[9] 张玉婷, 严承华, 魏玉人. 基于节点认证的物联网感知层安全性问题研究[J]. 信息网络安全, 2015(11): 27-32.
ZHANG Y T, YAN C H, WEI Y R. Research on security of IoT perception layer based on node authentication[J]. Netinfo Security, 2015(11): 27-32.

[10] 钱明茹. 物联网中基于属性的安全访问控制研究[D]. 沈阳: 辽宁大学, 2013.
QIAN M R. Research on security attribute-based access control in the Internet of Things[D]. Shenyang: Liaoning University, 2013.

[11] GUIN U, CUI P C, SKJELLUM A. Ensuring proof-of-authenticity of IoT edge devices using blockchain technology[C]//Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Piscataway: IEEE Press, 2018: 1042-1049.

[12] 向宏, 夏晓峰. 轻量级密码在资源受限设备安全中的应用简析[J]. 自动化博览, 2018, 35(S2): 72-75.
XIANG H, XIA X F. Overview on the application of lightweight cryptography in resource-constrained system security[J]. Automation Panorama, 2018, 35(S2): 72-75.

[13] LOU X, TELLABI A. Cybersecurity threats, vulnerability and analysis in safety critical industrial control system (ICS)[C]//Recent Developments on Industrial Control Systems Resilience. Cham: Springer, 2020: 75-97.

[14] 徐震, 周晓军, 王利明, 等. PLC 攻防关键技术研究进展[J]. 信息安全学报, 2019, 4(3): 48-69.
XU Z, ZHOU X J, WANG L M, et al. Recent advances in PLC attack and protection technology[J]. Journal of Cyber Security, 2019, 4(3): 48-69.

[15] 荆琦, 唐礼勇, 陈钟. 无线传感器网络中的信任管理[J]. 软件学报, 2008, 19(7): 1716-1730.
JING Q, TANG L Y, CHEN Z. Trust management in wireless sensor networks[J]. Journal of Software, 2008, 19(7): 1716-1730.

[16] 夏辉, 张三顺, 孙运传, 等. 车载自组网中基于信任管理的安全组播协议设计[J]. 计算机学报, 2019, 42(5): 961-979.
XIA H, ZHANG S S, SUN Y C, et al. Design of trust-based secure multicast routing protocol in VANETs[J]. Chinese Journal of Computers, 2019, 42(5): 961-979.

[17] JAYASINGHE U. Trust evaluation in the IoT environment[D]. Liverpool John Moores University. 2018.

[18] 梁洪泉, 吴巍. 基于动态贝叶斯网络的可信度量模型研究[J]. 通信学报, 2013, 34(9): 68-76.
LIANG H Q, WU W. Research of trust evaluation model based on dynamic Bayesian network[J]. Journal on Communications, 2013, 34(9): 68-76.

[19] JAYASINGHE U, LEE G M, UM T W, et al. Machine learning based trust computational model for IoT services[J]. IEEE Transactions on Sustainable Computing, 2019, 4(1): 39-52.

[20] WANG Y B, WEN J H, ZHOU W, et al. A novel dynamic cloud ser-

vice trust evaluation model in cloud computing[C]//Proceedings of 2018 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). Piscataway: IEEE Press, 2018 : 10-15.

[21] WU D X, SHEN G H, HUANG Z Q, et al. A trust-aware task offloading framework in mobile edge computing[J]. IEEE Access, 2019, 7: 150105-150119.

[22] WANG T, LUO H, JIA W J, et al. MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2054-2062.

[23] LI W J, MENG W Z, KWOK L F, et al. Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model[J]. Journal of Network and Computer Applications, 2017, 77: 135-145.

[24] JIA C H, LIN K, DENG J. A multi-property method to evaluate trust of edge computing based on data driven capsule network[C]//Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops. Piscataway: IEEE Press, 2020: 616-621.

[25] 蒋伟进, 许宇胜, 郭宏, 等. 网络在线交易动态信任计算模型与信誉管理机制[J]. 中国科学: 信息科学, 2014, 44(9): 1084-1101.
JIANG W J, XU Y S, GUO H, et al. Dynamic trust calculation model and credit management mechanism of online trading[J]. Scientia Sinica (Informationis), 2014, 44(9): 1084-1101.

[26] FRIEDMAN| E J, RESNICK P. The social cost of cheap pseudonyms[J]. Journal of Economics & Management Strategy, 2001, 10(2): 173-199.

[27] 胡建理, 周斌, 吴泉源, 等. P2P 网络环境下基于信誉的分布式抗攻击信任管理模型[J]. 计算机研究与发展, 2011, 48(12): 2235-2241.
HU J L, ZHOU B, WU Q Y, et al. A reputation-based attack-resistant distributed trust management model for P2P networks[J]. Journal of Computer Research and Development, 2011, 48(12): 2235-2241.

[28] 付才, 洪帆, 洪亮, 等. 基于信任保留的移动 Ad Hoc 网络安全路由协议 TPSRP[J]. 计算机学报, 2007, 30(10): 1853-1864.
FU C, HONG F, HONG L, et al. Mobile ad hoc secure routing protocol based on trust preserving[J]. Chinese Journal of Computers, 2007, 30(10): 1853-1864.

[29] GAO Z P, ZHAO W S, XIA C X, et al. A credible and lightweight multidimensional trust evaluation mechanism for service-oriented IoT edge computing environment[C]//Proceedings of 2019 IEEE International Congress on Internet of Things. Piscataway: IEEE Press, 2019: 156-164.

[30] FIGUEROA L S, AÑORGA J, ARRIZABALAGA S. A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS[J]. ACM Computing Surveys, 2021, 53(2): 44.

[31] 陶耀东, 贾新桐, 吴云坤. 一种工业控制系统漏洞风险评估方法[J]. 小型微型计算机系统, 2020, 41(3): 603-609.
TAO Y D, JIA X T, WU Y K. Industry control system vulnerability risk assessment method[J]. Journal of Chinese Computer Systems, 2020, 41(3): 603-609.

[32] 魏志强, 周炜, 任相军, 等. 普适计算环境中防护策略的信任决策机制研究[J]. 计算机学报, 2012, 35(5): 871-882.
WEI Z Q, ZHOU W, REN X J, et al. A strategy-proof trust based decision mechanism for pervasive computing environments[J]. Chinese Journal of Computers, 2012, 35(5): 871-882.

[作者简介]

于亚（1996− ），男，上海交通大学硕士生，主要研究方向为工业通信系统与安全、可信计算、物联网安全等。

伏玉笋（1972− ），男，博士，上海交通大学助理研究员，主要研究方向为无线通信与系统、无线网联智能系统、工业互联网与安全可信、智能制造等。