(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 117375893 B
(45)授权公告日 2024.05.24

(21)申请号 202311230700.5
(22)申请日 2023.09.22
(65)同一申请的已公布的文献号
申请公布号 CN 117375893 A
(43)申请公布日 2024.01.09
(73)专利权人 南京中新赛克科技有限责任公司
地址 210012 江苏省南京市雨花台区宁双路19号2幢1501室
专利权人 南京理工大学
(72)发明人 顾欢欢 刘瀚文 李千目 王明意
(74)专利代理机构 南京苏高专利商标事务所(普通合伙) 32204
专利代理师 王安琪
(51)Int.Cl.
H04L 9/40(2022.01)
G06N 3/0442(2023.01)
G06N 3/08(2023.01)
(56)对比文件
WO 2023000413 A1,2023.01.26
CN 115002030 A,2022.09.02
CN 116647391 A,2023.08.25
US 2018219895 A1,2018.08.02
WO 2022011977 A1,2022.01.20
审查员 于瑞甫

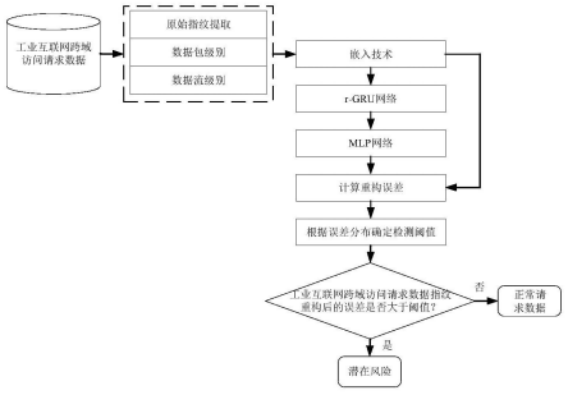
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法及判别系统

(57)摘要

本发明公开了一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法及判别系统,采用嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为低维密集连续指纹向量,利用重新定义的门控循环单元(r-GRU)网络和多层感知器(MLP)网络提取每个网络设备上的工业互联网跨域访问请求的整体时序指纹;根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹可计算出重构误差,并根据误差分布设定检测阈值实现对测试工业互联网跨域访问请求数据集的检测,从而减少了误报率和漏报率高的问题,提高工业互联网跨域访问请求潜在风险判别的精准识别。



CN 117375893 B

1.一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法,其特征在于,包括如下步骤:

步骤1、采集网络设备上实际工业互联网跨域访问请求,通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹;

步骤2、利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量;工业互联网跨域访问请求nf_i在t时间片的指纹表示如下:

$$e_{nf_i}(t)=I_{nf_i}(t)\circ P_{nf_i}(t)\circ PT_{nf_i}(t)\circ F_{nf_i}(t)$$

其中,∘是连接算子,$I_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的IP地址信息,$P_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的端口号信息,$PT_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的协议类型信息,$F_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的标志位信息,在t时间片,$e_{nf_i}(t)$无缝集成了每个网络设备上的工业互联网跨域访问请求nf_i所有信息指纹;

步骤3、利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹;在r-GRU网络中,重置门、候选知识、更新门和隐藏状态分别设置为:

$$r_t^{nf_i}=I$$

$$\tilde{h}_t^{nf_i}=\sigma\left(We_{nf_i}(t)+Vh_{t-1}^{nf_i}\right)$$

$$z_t^{nf_i}=\sigma\left(W_z e_{nf_i}(t)+V_z h_{t-1}^{nf_i}\right)$$

$$h_t^{nf_i}=\left(1-z_t^{nf_i}\right)\odot\tilde{h}_t^{nf_i}+z_t^{nf_i}\odot h_{t-1}^{nf_i}$$

其中,符号“⊙”表示逐元素乘法,$e_{nf_{tar}}(t)\in\mathbb{R}^{4*d*d}$,σ是ReLu、sigmoid、tanh的非线性激活函数,W,V,W_Z和V_Z分别表示对应的权重矩阵,I表示单位矩阵;

工业互联网跨域访问请求nf_i在T个时间片的嵌入信息如下所示:

$$G_{nf_i}=\left(h^{nf_i}{}_1,h^{nf_i}{}_2,\ldots,h^{nf_i}{}_t,\ldots,h^{nf_i}{}_T\right)\quad 1\le T$$

$$G_{ave-nf_i}=\frac{G_{nf_i}}{T}\quad 1\le T;$$

步骤4、使用多层感知机MLP技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;

$$G_{nf_i}^{MLP}=\left(\ldots\left(W_{nf_i}^2\left(W_{nf_i}^1 G_{ave-nf_i}+b_{nf_i}^1\right)+b_{nf_i}^2\right)\right)$$

其中,$W_{nf_i}^1$和$b_{nf_i}^1$分别为工业互联网跨域访问请求nf_i的第一层权重矩阵和偏置项,$W_{nf_i}^2$和$b_{nf_i}^2$分别为第二层权重矩阵和偏置项,以此类推;

步骤5、根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹计算出重构误差,通过统计重构误差的分布确定检测阈值τ,阈值τ计算过程如下:

$$\tau = \frac{1}{N}\sum_{i=1}^{N}\left\| G_{nf_i}^{MLP} - e_{nf_i}(t) \right\|^2$$

其中,N表示工业互联网跨域访问请求数据的数量;当新输入工业互联网跨域访问请求数据的重构误差大于该阈值时则可认为该数据为异常工业互联网跨域访问请求数据。

2.如权利要求1所述的基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法,其特征在于,步骤1中,请求数据指纹包括IP地址信息、端口号信息、协议类型信息、标志位信息。

3.一种如权利要求1所述的基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法的判别系统,其特征在于,包括:数据采集模块、数据转换模块、数据提取模块和数据计算模块;数据采集模块采集网络设备上实际工业互联网跨域访问请求,通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹;数据转换模块利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量;数据提取模块通过两次提取更高维度的基于时间的工业互联网跨域访问请求数据指纹,第一次利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹,第二次使用多层感知机MLP技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;数据计算模块根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹计算出重构误差,数据计算模块计算出重构误差,通过统计重构误差的分布确定检测阈值τ,当新输入工业互联网跨域访问请求数据的重构误差大于该阈值时则认为该数据为异常工业互联网跨域访问请求数据。

4.如权利要求3所述的基于r-GRU网络的工业互联网跨域访问请求潜在风险判别系统,其特征在于,数据采集模块采集网络设备上实际工业互联网跨域访问请求,请求的相关数据指纹包括IP地址信息、端口号信息、协议类型信息、标志位信息。

一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法及判别系统

技术领域

[0001] 本发明涉及网络异常检测技术领域,尤其是一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法及判别系统。

背景技术

[0002] 网络流量的异常检测对于识别网络攻击起着关键作用。然而,由于流量特征维度和噪音数据的增加,传统的机器学习方法在处理流量异常检测时,会出现特征提取精度低和鲁棒性弱的问题,这在一定程度上削弱了对流量攻击的检测效能。因此,目前基于深度学习的网络流量异常检测方法已经成为了研究焦点。

[0003] 基于深度学习的异常检测方法主要有以下3种:一种是利用深度玻尔兹曼机进行异常检测方法:这种方法能通过学习高维流量数据来识别其核心特征,以此提升对流量攻击的侦查效率;然而,这种方法在提取特征时的鲁棒性较差,若输入数据含有噪声,其侦测攻击的性能可能会下降。另一种是采用堆叠自编码器(Stacked Auto Encoders,SAE)进行异常检测方法:这种方式可以逐层学习流量数据以获取较高准确性的流量特征,但同样面临鲁棒性较差的问题,当测试数据被破坏时,其侦测精确度可能会降低。最后一种是基于卷积神经网络进行异常检测方法:这种方法所提取的流量特征具有较强的鲁棒性,侦测攻击的性能相对较高;但是,它需要先将网络流量转换为图片,增加了数据处理的负担,并且没有充分考虑网络结构信息对特征提取准确性的影响。

[0004] 在文献Session-based network intrusion detection using a deep learning architecture中,作者引入了一种基于堆叠降噪自编码器(Stacked Denoising Autoencoders,简称SDA)进行异常检测的技术。尽管它可以在大数据环境下有效地提升流量特征获取的准确性和鲁棒性,并且不需要将流量转换为图像,从而减轻了额外的处理负荷。然而,其采用的SDA仅有3个隐藏层并且每一层的节点数量相同,这未能最大限度地发挥出SDA的特征提取和降维功能。当训练数据较少时,这可能会影响到特征提取的精确度,进一步削弱其对流量攻击检测的能力。

[0005] 文献Network Traffic Anomaly Detection Method Based on Deep Features Learning提出一种基于深度特征学习的网络流量异常检测方法,这是借助于堆叠降噪自编码器(SDA)和softmax实现的,这种方法可以提取出具有较高鲁棒性的流量特征。不过,该研究并未充分考虑网络流量的时序性特征信息,因此,对网络流量特征的全面分析可能尚存在不足。

[0006] 文献A Novel Two-Stage Deep Learning Structure for Network Flow Anomaly Detection结合Denoising Auto-Encoder(GRU)和Denoising Auto-Encoder(DAE)模型,提出了一种新型的两阶段深度学习结构,用于网络流量异常检测。通过使用监督异常检测和选择机制来辅助半监督异常检测,提高了异常检测系统的精度和准确性。但是这种方法不能充分的利用现有网络设备上网络流量的数据指纹,这就会出现网络流量特征提取

精度低和误报率和漏报率高的问题。

发明内容

[0007] 本发明所要解决的技术问题在于,提供一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法及判别系统,能够减少误报率和漏报率,提高工业互联网跨域访问请求潜在风险判别的精准识别。

[0008] 为解决上述技术问题,本发明提供一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法,包括如下步骤:

[0009] 步骤1、采集网络设备上实际工业互联网跨域访问请求,通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹;

[0010] 步骤2、利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量;

[0011] 步骤3、利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹;

[0012] 步骤4、使用多层感知机MLP技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;

[0013] 步骤5、根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹计算出重构误差,通过统计重构误差的分布确定检测阈值τ,当新输入工业互联网跨域访问请求数据的重构误差大于该阈值时则可认为该数据为异常工业互联网跨域访问请求数据。

[0014] 优选的,步骤1中,请求数据指纹包括IP地址信息、端口号信息、协议类型信息、标志位信息。

[0015] 优选的,步骤2中,利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量,工业互联网跨域访问请求nf_i在t时间片的指纹表示如下:

[0016] $$e_{nf_i}(t)=I_{nf_i}(t)\circ P_{nf_i}(t)\circ PT_{nf_i}(t)\circ F_{nf_i}(t)$$

[0017] 其中,o是连接算子,$I_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的IP地址信息,$P_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的端口号信息,$PT_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的协议类型信息,$F_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的标志位信息,在t时间片,$e_{nf_i}(t)$无缝集成了每个网络设备上的工业互联网跨域访问请求nf_i所有信息指纹。

[0018] 优选的,步骤3中,利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹,在r-GRU网络中,重置门、候选知识、更新门和隐藏状态分别设置为:

[0019] $$r_t^{nf_i}=I$$

[0020] $$\tilde{h}_i^{nf_i}=\sigma\left(We_{nf_i}(t)+Vh_{t-1}^{nf_i}\right)$$

[0021] $$z_t^{nf_i}=\sigma\left(W_z e_{nf_i}(t)+V_z h_{t-1}^{nf_i}\right)$$

[0022] $$h_t^{nf_i}=\left(1-z_t^{nf_i}\right)\odot\tilde{h}_t^{nf_i}+z_t^{nf_i}\odot h_{t-1}^{nf_i}$$

[0023] 其中,符号“⊙”表示逐元素乘法,$e_{nf_{tar}}(t)\in\mathbb{R}^{4*d*d}$,σ是ReLu、sigmoid、tanh的非线性激活函数,W,V,W_Z和V_Z分别表示对应的权重矩阵,I表示单位矩阵;

[0024] 工业互联网跨域访问请求nf_i在T时间片的嵌入信息如下所示:

[0025] $$G_{nf_i}=\left(h^{nf_i}{}_1,h^{nf_i}{}_2,\ldots,h^{nf_i}{}_t,\ldots,h^{nf_i}{}_T\right)\quad 1\le T$$

[0026] $$G_{ave-nf_i}=\frac{G_{nf_i}}{T}\quad 1\le T\circ$$

[0027] 优选的,步骤4中,使用多层感知机MLP技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹:

[0028] $$G_{nf_i}^{MLP}=\left(\ldots\left(W_{nf_i}^{2}\left(W_{nf_i}^{1}G_{ave-nf_i}+b_{nf_i}^{1}\right)+b_{nf_i}^{2}\right)\right)$$

[0029] 其中,$W_{nf_i}^{1}$和$b_{nf_i}^{1}$分别为工业互联网跨域访问请求nf_i的第一层权重矩阵和偏置项,$W_{nf_i}^{2}$和$b_{nf_i}^{2}$分别为第二层权重矩阵和偏置项,以此类推。

[0030] 优选的,步骤5中,阈值τ计算过程如下:

[0031] $$\tau=\frac{1}{N}\sum_{i=1}^{N}\left\|G_{nf_i}^{MLP}-e_{nf_i}(t)\right\|^2$$

[0032] 其中,N表示工业互联网跨域访问请求数据的数量。

[0033] 相应的,一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别系统,包括:数据采集模块、数据转换模块、数据提取模块和数据计算模块;数据采集模块采集网络设备上实际工业互联网跨域访问请求,通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹;数据转换模块利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量;数据提取模块通过两次提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;数据计算模块根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹计算出重构误差。

[0034] 优选的,数据采集模块采集网络设备上实际工业互联网跨域访问请求,请求的相关数据指纹包括IP地址信息、端口号信息、协议类型信息、标志位信息。

[0035] 优选的,数据提取模块通过两次提取更高维度的基于时间的工业互联网跨域访问请求数据指纹,第一次利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹,第二次使用多层感知机MLP技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹。

[0036] 优选的,数据计算模块计算出重构误差,通过统计重构误差的分布确定检测阈值τ,当新输入工业互联网跨域访问请求数据的重构误差大于该阈值时则认为该数据为异常工业互联网跨域访问请求数据。

[0037] 本发明的有益效果为:本发明采用嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为低维密集连续指纹向量,利用重新定义的门控循环单元

(r-GRU)网络和多层感知器(MLP)网络提取每个网络设备上的工业互联网跨域访问请求的整体时序指纹;根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹可计算出重构误差,并根据误差分布设定检测阈值实现对测试工业互联网跨域访问请求数据集的检测,从而减少了误报率和漏报率高的问题,提高工业互联网跨域访问请求潜在风险判别的精准识别。

附图说明

[0038] 图1为本发明的方法流程示意图。

具体实施方式

[0039] 如图1所示,一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别方法,包括如下步骤:

[0040] S1,采集网络设备上实际工业互联网跨域访问请求,主要是通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹,即IP地址信息、端口号信息、协议类型信息、标志位信息;

[0041] S2,利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹(即IP地址、端口号、协议类型、标志位)转换为密集且连续的向量;工业互联网跨域访问请求nf_i在t时间片的指纹表示如下:

[0042] $$e_{nf_i}(t)=I_{nf_i}(t)\circ P_{nf_i}(t)\circ PT_{nf_i}(t)\circ F_{nf_i}(t)$$

[0043] 其中,o是连接算子,$I_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的IP地址信息,$P_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的端口号信息,$PT_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的协议类型信息,$F_{nf_i}(t)\in\mathbb{R}^{d*d}$表示工业互联网跨域访问请求在t时间片的标志位信息。此外,在t时间片,$e_{nf_i}(t)$无缝集成了每个网络设备上的工业互联网跨域访问请求nf_i所有信息指纹。

[0044] S3,为了更全面表征工业互联网跨域访问请求数据指纹,利用r-GRU网络训练和提取每个网络设备上基于时间的工业互联网跨域访问请求数据指纹;在r-GRU网络中,重置门、候选知识、更新门和隐藏状态分别设置为:

[0045] $$r_t^{nf_i}=I$$

[0046] $$\tilde{h}_t^{nf_i}=\sigma\left(We_{nf_i}(t)+Vh_{t-1}^{nf_i}\right)$$

[0047] $$z_t^{nf_i}=\sigma\left(W_z e_{nf_i}(t)+V_z h_{t-1}^{nf_i}\right)$$

[0048] $$h_t^{nf_i}=\left(1-z_t^{nf_i}\right)\odot\tilde{h}_t^{nf_i}+z_t^{nf_i}\odot h_{t-1}^{nf_i}$$

[0049] 其中,符号“⊙”表示逐元素乘法,$e_{nf_{tar}}(t)\in\mathbb{R}^{4*d*d}$。σ是ReLu、sigmoid、tanh等的非线性激活函数。W,V,W_Z,和V_Z分别表示对应的权重矩阵。I表示单位矩阵。

[0050] 工业互联网跨域访问请求nf_i在T时间片的嵌入信息如下所示:

[0051] $$G_{nf_i}=\left(h^{nf_i}{}_1,h^{nf_i}{}_2,\ldots,h^{nf_i}{}_t,\ldots,h^{nf_i}{}_T\right)\quad 1\le T$$

[0052] $$G_{ave-nf_i}=\frac{G_{nf_i}}{T} \quad 1\le T$$

[0053] S4,使用多层感知机(MLP)技术对r-GRU网络生成的隐式表达向量进一步提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;

[0054] $$G_{nf_i}^{MLP}=\left(\ldots\left(W_{nf_i}^{2}\left(W_{nf_i}^{1}G_{ave-nf_i}+b_{nf_i}^{1}\right)+b_{nf_i}^{2}\right)\right)$$

[0055] 其中,$W_{nf_i}^{1}$和$b_{nf_i}^{1}$分别为工业互联网跨域访问请求nf_i的第一层权重矩阵和偏置项,$W_{nf_i}^{2}$和$b_{nf_i}^{2}$分别为第二层权重矩阵和偏置项,以此类推。

[0056] S5,根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹可计算出重构误差。通过统计重构误差的分布确定检测阈值τ,当新输入工业互联网跨域访问请求数据的重构误差大于该阈值时则可认为该数据为异常工业互联网跨域访问请求数据。阈值τ计算过程如下:

[0057] $$\tau=\frac{1}{N}\sum_{i=1}^{N}\left\|G_{nf_i}^{MLP}-e_{nf_i}(t)\right\|^2$$

[0058] 其中,N表示工业互联网跨域访问请求数据的数量。

[0059] 相应的,一种基于r-GRU网络的工业互联网跨域访问请求潜在风险判别系统,包括:数据采集模块、数据转换模块、数据提取模块和数据计算模块;数据采集模块采集网络设备上实际工业互联网跨域访问请求,通过数据包级别和会话流级别提取基于时间信息的多维工业互联网跨域访问请求数据指纹;数据转换模块利用相应的嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为密集且连续的向量;数据提取模块通过两次提取更高维度的基于时间的工业互联网跨域访问请求数据指纹;数据计算模块根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹计算出重构误差。

[0060] 本发明采用嵌入技术将每个网络设备上的工业互联网跨域访问请求的相关数据指纹转换为低维密集连续指纹向量;利用重新定义的门控循环单元r-GRU网络和多层感知器MLP网络提取每个网络设备上的工业互联网跨域访问请求的整体时序指纹;根据工业互联网跨域访问请求数据的嵌入信息和利用深度学习网络获得的基于时间的工业互联网跨域访问请求数据指纹可计算出重构误差;并根据误差分布设定检测阈值实现对测试工业互联网跨域访问请求数据集的检测,从而减少了误报率和漏报率高的问题,提高工业互联网跨域访问请求潜在风险判别的精准识别。

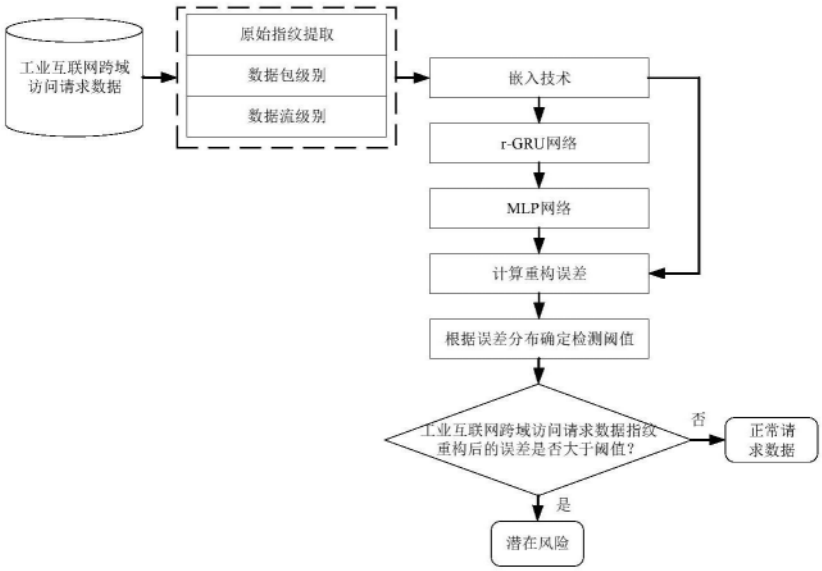

工业互联网跨域
访问请求数据
原始指纹提取
数据包级别
数据流级别
嵌入技术
r-GRU网络
MLP网络
计算重构误差
根据误差分布确定检测阈值
工业互联网跨域访问请求数据指纹
重构后的误差是否大于阈值?
否
正常请
求数据
是
潜在风险

图1