(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115580472 B
(45)授权公告日 2024.04.19

(21)申请号 202211240203.9
(22)申请日 2022.10.11
(65)同一申请的已公布的文献号
申请公布号 CN 115580472 A
(43)申请公布日 2023.01.06
(73)专利权人 东北大学
地址 110819 辽宁省沈阳市和平区文化路三巷11号
专利权人 国网辽宁省电力有限公司
(72)发明人 盛川 姚羽 胡博 申益嘉 杨巍 周小明 刘莹 杨道青 李文轩 林小李 单垚 周金磊
(74)专利代理机构 大连理工大学专利中心 21200
专利代理师 梅洪玉
(51)Int.Cl.
H04L 9/40(2022.01)
G06F 18/241(2023.01)
G06F 18/2321(2023.01)
(56)对比文件
CN 113298186 A,2021.08.24
CN 113850346 A,2021.12.28
CN 111953665 A,2020.11.17
US 2012284793 A1,2012.11.08
汪洁;杨力立;杨珉.基于集成分类器的恶意网络流量检测.通信学报.2018,(10),全文.
王娜;胡超芳;师五喜.基于客观满意聚类的pH中和过程建模方法.计算机工程.2018,(02),全文.
许勐;李兴华;刘海;钟成;马建峰.基于半监督学习和信息增益率的入侵检测方案.计算机研究与发展.2017,(10),全文.
审查员 付苗

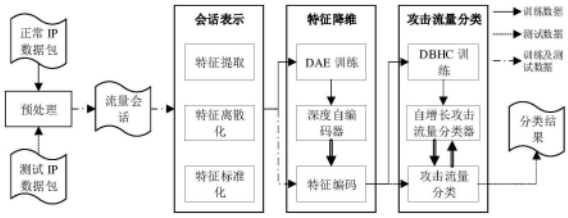
权利要求书3页 说明书8页 附图2页

(54)发明名称

一种基于启发式聚类算法的工业控制网络攻击流量分类方法

(57)摘要

本发明属于网络安全领域,提出了一种基于启发式聚类算法的工业控制网络攻击流量分类方法。该方法通过对工控网络攻击流量提取特征并格式化处理,输入至深度自编码器后进行降维处理,获得低维流量特征表示,基于密度的启发式聚类算法从中获取基础攻击流量分类器,并基于基础攻击流量分类器,采用测试数据构造自增长攻击流量分类器,持续检测和分类未知的攻击流量。本发明的主要目的在于解决仅基于正常工控网络流量对未知攻击流量进行实时分类的难题。针对缺乏足够的训练攻击样本、缺乏工业控制网络流量分布相关知识以及攻击流量的种类是不确定的,且是逐渐出现的特点,本方法实现对攻击流量进行持续性的、实时的检测和分类。



CN 115580472 B

1.一种基于启发式聚类算法的工业控制网络攻击流量分类方法,其特征在于,工控网络攻击流量分为训练数据和测试数据,包括以下步骤:

步骤一:从工控网络攻击流量中提取出工控网络攻击流量特征;使用流量会话作为基本单元分割工控网络攻击流量,流量会话进一步由活跃时间阈值分割;

步骤二:将步骤一获得的工控网络攻击流量特征进行特征离散化和标准化处理,获得格式化后的工控网络攻击流量特征输入至深度自编码器,深度自编码器的解码器部分对工控网络攻击流量特征进行降维,获得低维流量特征表示形式;

步骤三:通过基于密度的启发式聚类算法,从低维流量特征表示形式中获取基础攻击流量分类器;

基于密度的启发式聚类算法获取基础攻击流量分类器的具体步骤为:

3.1将步骤二的低维流量特征表示形式视为数据点,计算每个数据点p_i的局部密度ρ_i;

$$\rho_i = \sum_j \chi(d_{ij} - d_c), \chi(x) = \begin{cases} 1, x < 0 \\ 0, otherwise \end{cases}$$

其中,d_{ij}为数据点p_i和p_j之间的距离,d_c为截断距离;

3.2按局部密度降序排列数据点,形成序列$N=\{p_1, p_2, \ldots, p_n\}$;

3.3计算每个数据点p_i和与其最近且密度更高的数据点间的距离δ_i;

$$\delta_i = \min_{j:\rho_j > \rho_i} (d_{ij})$$

3.4为数据点p_1创建第一个簇C_1,并选择p_1为其质心o_1;

3.5按照序列N的顺序,除p_1外,对每个数据点p_i依次进行检验,当其距离δ_i小于等于截断距离d_c时,p_i被分配到与其最近且密度更高的数据点所属的簇C_x中;通过直接平均法,用p_i来更新簇C_x的质心o_x;

3.6当p_i的距离δ_i大于截断距离d_c时,为p_i创建一个新的簇,且p_i被选为对应新簇的质心;

3.7计算每个簇之间极限距离d_l,极限距离为两个簇质心间最大距离,

$$d_l(C_a, C_b) = \frac{(|C_a| + |C_b|)}{2} * d_c$$

3.8 C_a,C_b两个簇质心的距离小于d_l时,计算二者之间最小距离d_{min}:

$$d_{min}(C_a, C_b) = \min_{p_i^a \in C_a, p_j^b \in C_b} dist(p_i^a, p_j^b)$$

3.9 d_{min}小于截断距离d_c时,C_a,C_b两个簇被合并成一个新的簇C'_a,并更新簇C'_a的质心o'_a,将C_b标记成已合并;

3.10遍历各个簇,删除所有标记为已合并的簇;

步骤四:基于基础攻击流量分类器,采用测试数据构造自增长攻击流量分类器,用于持续检测和分类未知的攻击流量;

所述自增长攻击流量分类器的具体实现步骤为:

4.1测试数据p^*所属簇C^*设为空,$d_{min}^{p^*}$置为正整数,计算测试数据p^*和基础攻击流量分

类器中所有簇的极限距离d_l',d_l'计算公式如下:

$$d_l'(p^*, C_i) = \frac{(|C_i| + 1)}{2} * d_c$$

4.2 p^*和o_i之间的距离不大于d_l'时,计算对应的最小距离d_{min},

$$d_{min}(p^*, C_i) = \min_{p_i \in C_i} dist(p^*, p_i)$$

4.3 $d_{min}(p^*, C_i)$不大于截断距离d_c且小于$d_{min}^{p^*}$,更新$d_{min}^{p^*}$为$d_{min}(p^*, C_i)$,将C^*置为簇C_i,C^*不为空;否则C^*为空;

4.4当C^*不为空时,$|C^*|$小于更新系数M时,计算更新距离d_u:

$d_u = d_c * |C^*| / M$

$|C^*|$不小于更新系数M时,计算更新距离d_u:

$d_u = d_c$

4.5 $dist(p^*, o^*)$大于d_u时,p^*来更新簇C^*;

4.6计算每个簇C_j的簇C^*之间极限距离d_l;

4.7 C^*,C_j两个簇质心的距离小于等于d_l时,进一步计算它们之间的最小距离$d_{min}(C^*, C_j)$;

4.8 $d_{min}(C^*, C_j)$小于截断距离d_c时,C^*,C_j两个簇将被合并成一个新的簇C_{new}^*,利用分配机制将C_{new}^*映射到一个已有类别;

4.9将簇C_{new}^*赋给簇C^*,将p^*分类为C^*所属类别;

4.10当C^*为空时,为p^*创建一个新的簇C_{new}^*,并选择p^*为其质心,分配一个新的类别给p^*和C_{new}^*。

2.根据权利要求1所述的基于启发式聚类算法的工业控制网络攻击流量分类方法,其特征在于,所述步骤二中的深度自编码器包含三个隐藏层,每层均以ReLU作为激活函数;损失函数反映了格式化后的工控网络攻击流量特征与低维流量特征表示形式之间偏差平方的平均值,其中x_i表示格式化后的工控网络攻击流量特征,x_i^*表示低维流量特征表示形式,N表示数据量,即数据输出个数;

$$E = \frac{1}{N}\sum_i (x_i^* - x_i)^2$$

其中,E为输入数据与输出数据之间偏差平方的平均值。

3.根据权利要求1或2所述的基于启发式聚类算法的工业控制网络攻击流量分类方法,其特征在于,所述训练数据经步骤一、步骤二和步骤三获取基础攻击流量分类器。

4.根据权利要求3所述的基于启发式聚类算法的工业控制网络攻击流量分类方法,其特征在于,所述测试数据经步骤一、步骤二和步骤四构造自增长攻击流量分类器。

5.根据权利要求1、2或4所述的基于启发式聚类算法的工业控制网络攻击流量分类方

法,其特征在于,所述$d_{min}^{p^*}$不小于10^5。

一种基于启发式聚类算法的工业控制网络攻击流量分类方法

技术领域

[0001] 本发明涉及网络安全领域,具体涉及一种基于启发式聚类算法的工业控制网络攻击流量分类方法。

背景技术

[0002] 威胁分析是网络安全态势理解阶段的重要环节,无论从哪个角度对工业控制系统中的网络攻击行为进行分析,对于网络攻击流量的分类都在其中扮演着重要的角色,其打开了对网络攻击行为进行进一步深入探索的大门。

[0003] 网络攻击流量分类已经成为现代网络安全研究中一项重要的基础性技术。近年来对攻击流量分类的研究主要集中在将机器学习及深度学习技术应用于网络流量统计特征的分类方法上,许多有监督的分类方法和无监督的聚类方法已经被应用于攻击流量分类。基于不同的训练样本和防御目标,攻击流量分类方法能够被应用于不同的场景,主要包括检测恶意流量、区分已有类别攻击和发现未知种类攻击等。

[0004] 论文“Z.Jun,C.Chao,X.Yang,Z.Wanlei,and A.V.Vasilakos,An Effective Network Traffic Classification Method with Unknown Flow Detection[J].IEEE Trans.Netw.Serv.Manage.2019,10(2):133-147.”提出了流量标签传播,从大量的无标签数据集中自动标记相关流量,以解决监督训练集小的问题,并使用半监督的方法来检测未知的网络流量。

[0005] 论文“A.A.Ahmed,W.A.Jabbar,A.S.Sadiq,and H.Patel.Deep learning based classification model for botnet attack detection.J.Ambient Intell.Hum.Comput.,2020.”使用卷积神经网络对SCADA流量的突出时间模式进行建模,并确定网络攻击存在的时间窗口。特别是,这种方法设计了一个重新训练的方案来处理未知的攻击。

[0006] 论文“Z.Jun,C.Chao,X.Yang,Z.Wanlei,and A.V.Vasilakos,An Effective Network Traffic Classification Method with Unknown Flow Detection[J].IEEE Trans.Netw.Serv.Manage.2019,10(2):133-147.”提出了流量标签传播,以解决监督训练集小的问题。虽然这种方法减少了对监督训练数据的依赖,但它没有尝试对未知流量进行进一步分类。

[0007] 论文“A.A.Ahmed,W.A.Jabbar,A.S.Sadiq,and H.Patel.Deep learning based classification model for botnet attack detection.J.Ambient Intell.Hum.Comput.,2020.”提出的方法依赖于SCADA系统操作员检查和标记新发现的攻击,这可能是非常耗时的。其次,重新训练方案需要足够数量的新攻击实例,这可能导致分类模型无法及时适应新出现的攻击。

[0008] 近些年来,虽然已有一些方法被提出用于发现未知种类的网络攻击,然而现阶段这些方法仍然面临3个主要挑战:1)无法直接对侦测到的未知攻击流量进行进一步的分类;2)主要依赖安全分析人员对未知攻击流量进行种类划分和打标签;3)需要足够多的未知种

类攻击流量样本进行分类模型的训练。

[0009] 本发明提出了一种能够在仅有正常工控网络攻击流量作为参考的情况下对目标工业控制网络中的未知攻击流量进行实时检测和分类的方法。从有监督学习的角度来看，该方法摆脱了对训练攻击样本的依赖。与已有无监督聚类方法相比，该方法的分类过程是实时的，且被发现的新的攻击流量类别将被直接保留在分类模型中，而不是每次都重新训练和生成新的簇。况且对原有攻击流量和新的攻击流量的重新聚类很难保证与前一次聚类结果的一致性，即原属于相同簇的攻击流量可能被新的聚类过程分配到不同的簇中，从而导致生成的簇无法始终代表某一类攻击流量，进而导致整个聚类结果失去代表性。

发明内容

[0010] 本发明提出了一种基于启发式聚类算法的工业控制网络攻击流量分类方法，这是一种具有自增长能力的无监督分类方法，以解决仅基于正常工控网络攻击流量对未知攻击流量进行实时分类的难题。首先，由于缺乏足够的训练攻击样本，无监督聚类方法更适合解决该问题。其次，由于缺乏工业控制网络流量分布相关知识，自动化的聚类过程比预定义聚类结果更加符合实际需求。最后，由于攻击流量的种类是不确定的，且是逐渐出现的，因此对于攻击流量的持续性的、实时的检测和分类能力是非常重要的。

[0011] 本发明的技术方案如下：一种基于启发式聚类算法的工控网络攻击流量分类方法，工控网络攻击流量分为训练数据和测试数据，包括以下步骤：

[0012] 步骤一：从工控网络攻击流量中提取出工控网络攻击流量特征；使用流量会话作为基本单元分割工控网络攻击流量，流量会话进一步由活跃时间阈值$T_{activation}$分割；

[0013] 步骤二：将步骤一获得的工控网络攻击流量特征进行特征离散化和标准化处理，获得格式化后的工控网络攻击流量特征输入至深度自编码器，深度自编码器的解码器部分对工控网络攻击流量特征进行降维，获得低维流量特征表示形式；

[0014] 步骤三：通过基于密度的启发式聚类算法(Density-Based Heuristic Clustering，DBHC)，从低维流量特征表示形式中获取基础攻击流量分类器；

[0015] 步骤四：基于基础攻击流量分类器，采用测试数据构造自增长攻击流量分类器(Self-Growing Attack Traffic Classifier，SGATC)，用于持续检测和分类未知的攻击流量。

[0016] 所述步骤二中的深度自编码器包含三个隐藏层，每层均以ReLU作为激活函数；损失函数反映了格式化后的工控网络攻击流量特征与低维流量特征表示形式之间偏差平方的平均值，其中x_i表示格式化后的工控网络攻击流量特征，x_i^*表示低维流量特征表示形式，N表示数据量，即数据输出个数；

[0017] $$E = \frac{1}{N}\sum_{i}(x_i^* - x_i)^2$$

[0018] 其中，E为输入数据与输出数据之间偏差平方的平均值。

[0019] 所述步骤三的具体步骤为：

[0020] 3.1将步骤二的低维流量特征表示形式视为数据点，计算每个数据点p_i的局部密度ρ_i；

[0021] $$\rho_i = \sum_j \chi(d_{ij} - d_c), \chi(x) = \begin{cases} 1, x < 0 \\ 0, otherwise \end{cases}$$

[0022] 其中，d_{ij}为数据点p_i和p_j之间的距离，d_c为截断距离；

[0023] 3.2按局部密度降序排列数据点，形成序列N＝{p_1，p_2，…，p_n|；

[0024] 3.3计算每个数据点p_i和与其最近且密度更高的数据点q_i间的距离δ_i，

[0025] $$\delta_i = \min_{j:\rho_j > \rho_i} (d_{ij})$$

[0026] 3.4为数据点p_1创建第一个簇C_1，并选择p_1为其质心o_1；

[0027] 3.5按照序列N的顺序，除p_1外，对每个数据点p_i依次进行检验，当其距离δ_i小于等于截断距离d_c时，p_i被分配到与其最近且密度更高的数据点所属的簇C_x中；通过直接平均法，用p_i来更新簇C_x的质心o_x；

[0028] 3.6当p_i的距离δ_i大于截断距离d_c时，为p_i创建一个新的簇，且p_i被选为对应新簇的质心；

[0029] 3.7计算每个簇之间极限距离d_l，极限距离为两个簇质心间最大距离，

[0030] $$d_l(C_a, C_b) = \frac{(|C_a| + |C_b|)}{2} * d_c$$

[0031] 3.8C_a，C_b两个簇质心的距离小于d_l时，计算二者之间最小距离d_{min}：

[0032] $$d_{min}(C_a, C_b) = \min_{p_i^a \in C_a, p_j^b \in C_b} dist(p_i^a, p_j^b)$$

[0033] 3.9d_{min}小于截断距离d_c时，C_a，C_b两个簇被合并成一个新的簇C'_a，并更新簇C'_a的质心o'_a，将C_b标记成已合并；

[0034] 3.10遍历各个簇，删除所有标记为已合并的簇。

[0035] 所述步骤四的具体步骤为：

[0036] 4.1测试数据p^*所属簇C^*设为空，$d_{min}^{p^*}$置为正整数，计算测试数据p^*和基础攻击流量分类器中所有簇的极限距离d_l'，d_l'计算公式如下：

[0037] $$d_l'(p^*, C_i) = \frac{(|C_i| + 1)}{2} * d_c$$

[0038] 4.2p^*和o_i之间的距离不大于d_l'时，计算对应的最小距离d_{min}，

[0039] $$d_{min}(p^*, C_i) = \min_{p_i \in C_i} dist(p^*, p_i)$$

[0040] 4.3d_{min}(p^*，C_i)不大于截断距离d_c且小于$d_{min}^{p^*}$，更新$d_{min}^{p^*}$为d_{min}(p^*，C_i)，将C^*置为簇C_i，C^*不为空；否则C^*为空；

[0041] 4.4当C^*不为空时，|C^*|小于更新系数M时，计算更新距离d_u：

[0042] $d_u = d_c * |C^*| / M$

[0043] |C^*|不小于更新系数M时，计算更新距离d_u：

[0044] $d_u = d_c$

[0045] 4.5dist(p^*，o^*)大于d_u时，p^*来更新簇C^*；

[0046] 4.6计算每个簇C_j的簇C^*之间极限距离d_1；

[0047] 4.7C^*,C_j两个簇质心的距离小于等于d_1时,进一步计算它们之间的最小距离$d_{min}(C^*,C_j)$；

[0048] 4.8$d_{min}(C^*,C_j)$小于截断距离d_c时,C^*,C_j两个簇将被合并成一个新的簇C^*_{new},利用分配机制将C^*_{new}映射到一个已有类别；

[0049] 4.9将簇C^*_{new}赋给簇C^*,将p^*分类为C^*所属类别；

[0050] 4.10当C^*为空时,为p^*创建一个新的簇C^*_{new},并选择p^*为其质心,分配一个新的类别给p^*和C^*_{new}。

[0051] 所述训练数据经步骤一、步骤二和步骤三获取基础攻击流量分类器。

[0052] 所述测试数据经步骤一、步骤二和步骤四构造自增长攻击流量分类器。

[0053] 所述$d^{p^*}_{min}$不小于10^5。

[0054] 本发明的有益效果:本发明解决了仅基于正常工控网络流量对未知攻击流量进行实时分类的难题。从有监督学习的角度来看,本发明提出的方法摆脱了对训练攻击样本的依赖。与已有无监督聚类方法相比,本发明提出的方法的分类过程是实时的,且被发现的新的攻击流量类别将被直接保留在分类模型中,而不是每次都重新训练和生成新的簇。况且对原有攻击流量和新的攻击流量的重新聚类很难保证与前一次聚类结果的一致性,即原属于相同簇的攻击流量可能被新的聚类过程分配到不同的簇中,从而导致生成的簇无法始终代表某一类攻击流量,进而导致整个聚类结果失去代表性。针对缺乏足够的训练攻击样本、缺乏工业控制网络流量分布相关知识以及攻击流量的种类是不确定的,且是逐渐出现的特点,本方法实现对攻击流量进行持续性的、实时的检测和分类。

附图说明

[0055] 图1为未知攻击流量分类系统模型；

[0056] 图2为基于启发式聚类算法的工业控制网络攻击流量分类方法过程流程图；

[0057] 图3为本发明与四种比较算法的性能对比图。

具体实施方式

[0058] 下面结合附图和实施例,对本发明的具体实施方式做进一步详细描述。

[0059] 一种基于启发式聚类算法的工业控制网络攻击流量分类方法,算法步骤如下：

[0060] 步骤一:用流量会话的形式表示工控网络攻击流量,作为IT特征的补充,用工控网络攻击流量特征来表示数据单元。

[0061] 步骤二:采用特征离散化和标准化的数据处理方法,格式化被提取的工控网络攻击流量特征以适应接下来的深度学习方法。

[0062] 步骤三:使用一个包含三个隐藏层的深度自编码器来对工控网络攻击流量特征进行降维,该深度自编码器的所有层均采用ReLU作为激活函数,其为一个简单的非线性函数,如果输入值为正值,则返回输入值,否返回0。其次,选择MSE作为损失函数,其反映了输入与输出之间偏差平方的平均值。MSE计算式如下：

[0063] $$E = \frac{1}{N}\sum_{i}(x_i^* - x_i)^2$$

[0064] 步骤四:通过DBHC对由正常工控网络攻击流量组成的训练数据集进行建模,具体包括:

[0065] ①计算每个数据点p_i的局部密度ρ_i,其中,d_c为截断距离,设置为0.03;

[0066] $$\rho_i = \sum_{j}\chi(d_{ij} - d_c), \chi(x) = \begin{cases} 1, x < 0 \\ 0, otherwise \end{cases}$$

[0067] ②按局部密度降序排列数据点,形成序列N=$\{p_1, p_2, \cdots, p_n\}$;

[0068] ③计算每个数据点p_i和与具有更高密度的且与其最近的数据点q_i间的距离δ_i,生成二元组<q_i,δ_i>,δ_i计算公式如下:

[0069] $$\delta_i = \min_{j:\rho_j > \rho_i}(d_{ij})$$

[0070] ④为数据点p_1创建第一个簇C_1,并选择p_1为其质心o_1;

[0071] ⑤按照序列N的顺序,除p_1外,每个数据点p_i依次进行检验,当其距离δ_i小于等于截断距离d_c时,p_i被分配到具有更高密度的且与其最近的数据点所属的簇C_x中。同时,通过直接平均法,用p_i来更新簇C_x的质心o_x;

[0072] ⑥当p_i的距离δ_i大于截断距离d_c时,为p_i创建一个新的簇,且p_i被选为对应新簇的质心;

[0073] ⑦经过上述步骤,共创建了k个簇,对每个簇进行簇之间极限距离d_l的计算,极限距离被定义为两个簇质心间最大可能距离,计算公式如下:

[0074] $$d_l(C_a, C_b) = \frac{(|C_a| + |C_b|)}{2} * d_c$$

[0075] ⑧如果C_a,C_b两个簇质心的距离小于d_l时,进一步计算它们之间的最小距离d_{min}:

[0076] $$d_{min}(C_a, C_b) = \min_{p_i^a \in C_a, p_j^b \in C_b} dist(p_i^a, p_j^b)$$

[0077] ⑨当d_{min}小于截断距离d_c时,C_a,C_b两个簇将被合并成一个新的簇C'_a,并更新其质心o'_a,同时将C_b标记成已合并;

[0078] ⑩遍历一遍k个簇,将所有标记为已合并的簇删除。

[0079] 步骤五:构造SGATC,用于持续检测和分类未知的攻击流量,具体步骤为:

[0080] ①p^*所属簇C^*置为空,$d_{min}^{p^*}$置为较大正整数,计算测试数据p^*和原始簇集合中所有簇的质心o_i的距离,同时计算极限距离d_l',d_l'计算公式如下:

[0081] $$d_l'(p^*, C_i) = \frac{(|C_i| + 1)}{2} * d_c$$

[0082] ②如果p^*和o_i之间的距离小于等于d_l',那么计算它们对应的最小距离d_{min},公式如下:

[0083] $$d_{min}(p^*, C_i) = \min_{p_i \in C_i} dist(p^*, p_i)$$

[0084] ③当$d_{min}(p^*,C_i)$小于等于截断距离d_c且小于$d_{min}^{p^*}$,更新$d_{min}^{p^*}$为$d_{min}(p^*,C_i)$,将C^*置为簇C_i;

[0085] ④当C^*不为空时,如果$|C^*|$小于更新系数M,M设置为50,计算更新距离d_u:

[0086] $d_u=d_c*|C^*|/M$

[0087] 如果$|C^*|$不小于更新系数M,计算更新距离d_u:

[0088] $d_u=d_c$

[0089] ⑤当$dist(p^*,o^*)$大于d_u时,用p^*来更新簇C^*;

[0090] ⑥经过上述步骤,当前模型中有m个簇,对每个簇C_j计算其与簇C^*之间的极限距离d_l;

[0091] ⑦如果C^*,C_j两个簇质心的距离小于等于d_l时,进一步计算它们之间的最小距离$d_{min}(C^*,C_j)$;

[0092] ⑧当$d_{min}(C^*,C_j)$小于截断距离d_c时,C^*,C_j两个簇将被合并成一个新的簇C_{new}^*,利用分配机制将C_{new}^*映射到一个已有类别;

[0093] ⑨将簇C_{new}^*赋给簇C^*,将p^*分类为C^*所属类别;

[0094] ⑩当C^*为空时,为p^*创建一个新的簇C_{new}^*,并选择p^*为其质心,分配一个新的类别给p^*和C_{new}^*。

[0095] 本实施例使用SCADA系统及相应的网络流量数据集作为实验数据,以正常网络流量“Run1_6RTU”作为训练数据,以其余所有种类的攻击流量作为测试数据。主要目的在于检测攻击流量的同时对其种类进行区分,以便于与来自其他工控网络的攻击流量以及来自分布式工控蜜网的攻击流量进行比对分析。此外,为丰富实验数据中攻击流量的种类,本实施例使用7个攻击工具对5个暴露在互联网上的基于Modbus的工控设备进行了10次独立的扫描,进而形成攻击工具数据。进一步,为增加攻击工具数据的识别和分类难度,将5个被扫描的工控设备映射到SCADA系统中的前5个RTU,即将相应的IP地址替换成RTU的IP地址。具体的数据分布情况如表1所示。

[0096] 表1攻击流量数据集详细表

[0097]

攻击	数据名称	描述	数据总数	恶意数据
Normal	Run1_6RTU	一小时常规 Modbus 流量，包含轮询流量和人工操作流量。	134690	0
Attack 1	6RTU_with_operate	使用 Metasploit 利用一个漏洞（ms08_netapi）通过一个被俘获的 RTU 去入侵另一个 RTU。	1856	1200
Attack 2	CnC_uploading_exe	通过 Metasploit 的 Meterpreter 通道从一个被俘获的 RTU 向另一个被俘获的 RTU 发送 EXE 文件。	1426	121
Attack 3	Moving_two_files	从一个被俘获的 RTU 向另一个被俘获的 RTU 发送两个文件。	3319	75
Attack 4	Characterization	发送一系列 Modbus 读命令来刻画一个被俘获 RTU 的可用寄存器特征。	12296	6719
Attack 5	Send_a_fake_command	使用 Metasploit 代理功能和代理链工具从一个被俘获的 RTU 发送一个 Modbus 写操作命令。	11166	10
Attack 6	Channel_4d_12s	使用 RTU 的 12 个存储寄存器的 4 个最低有效位作为 Modbus 隐蔽通道实现隐匿通信。	44977	44977
Attack 7	Modbus-Discover	使用 Modbus-Discover 对 5 个基于 Modbus 的工控设备扫描 10 次。	110247	110247
Attack 8	Modbus-Fuzzer	使用 Modbus-Fuzzer 对 5 个基于 Modbus 的工控设备扫描 10 次。	1396	1396
Attack 9	Modicon-Info	使用 Modicon-Info 对 5 个基于 Modbus 的工控设备扫描 10 次。	602	602
Attack 10	Modscan	使用 Modscan 对 5 个基于 Modbus 的工控设备扫描 10 次。	902	902
Attack 11	MRCT	使用 MRCT 对 5 个基于 Modbus 的工控设备扫描 10 次。	452	452
Attack 12	Plcscan	使用 Plcscan 对 5 个基于 Modbus 的工控设备扫描 10 次。	1254	1254
Attack 13	Scadascan-Master	使用 Scadascan-Master 对 5 个基于 Modbus 的工控设备扫描 10 次。	457	457

[0098] 为了验证本发明提出方法的有效性,通过一组实验将该系统模型与4种较为先进的无监督聚类算法,包括k-means、EM、Hierarchical Agglomerative Clustering(HAC)及DBSCAN,在检测和分类未知攻击流量方面进行了比较。注意,4种比较算法皆在无监督模式下同时以训练和测试数据作为它们的输入。为使上述4种比较算法适用于攻击流量的检测和分类,本发明中的两条规则也被应用于它们。一方面,一旦测试流量会话被分配到训练流量会话所在的簇中,则被判定为正常。另一方面,不包含任何训练流量会话的簇被判定为异常,其类别通过概率分配机制来决定。

[0099] 图3展示了该系统模型与4种比较算法的性能。显然,该系统模型在各个评价指标上都优于其他比较算法。例如,该系统模型的分类准确率比次优算法,DBSCAN,高出0.04以上。尽管HAC算法在检测率和总体准确率方面与该系统模型相当,但其在分类准确率上出现

了急剧的下降,这暗示着其在分类工控网络攻击流量的过程中可能出现了过拟合现象。这是因为参数“簇的总数量”能够迫使HAC算法产生足够多的簇从而将攻击流量从正常流量中分离出来,但是其没有考虑攻击流量的分布情况,这并不利于区分不同种类的攻击流量。而且,攻击流量的数量远少于正常流量的数量,这也使得其难以为不同种类的攻击流量形成具有代表性的簇。这也是基于原型的聚类算法(k-means和EM)能够获得比基于密度的聚类算法(DBSCAN)更高的检测率和总体准确率的原因。但是基于密度的聚类算法试图探索数据点的分布情况,并将相似的数据点分配到相同的簇中,因此其更善于分类攻击流量。

[0100] 鉴于上述观察,该系统模型采用了更加严格的聚类条件来划分数据点,并利用更新操作来合并相似的簇以减小分类模型的规模。通过这种方式,该系统模型能够充分利用工控网络攻击流量的分布特征,并获得比4种比较算法更好的检测和分类性能。而且,该系统模型无需再训练便能够实时持续地发现新类别的攻击流量。

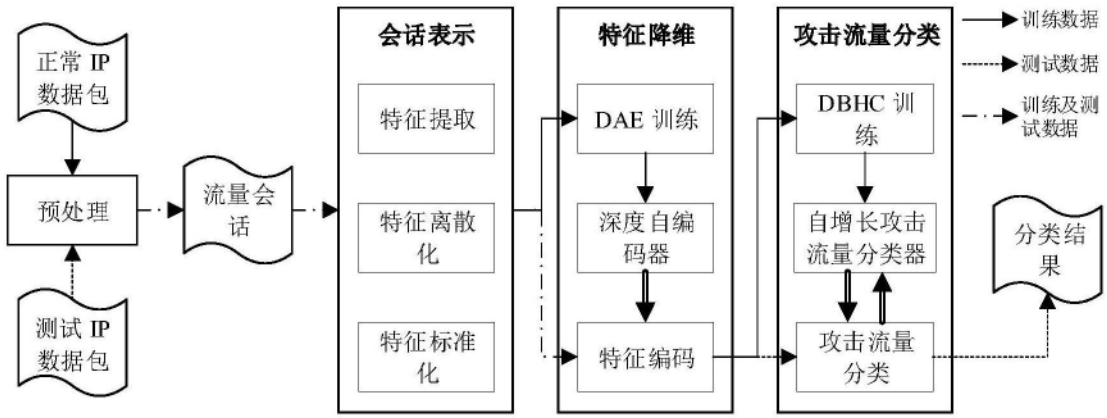

正常 IP 数据包
预处理
测试 IP 数据包
流量会话
会话表示
特征提取
特征离散化
特征标准化
特征降维
DAE 训练
深度自编码器
特征编码
攻击流量分类
DBHC 训练
自增长攻击流量分类器
攻击流量分类
分类结果
训练数据
测试数据
训练及测试数据

图1

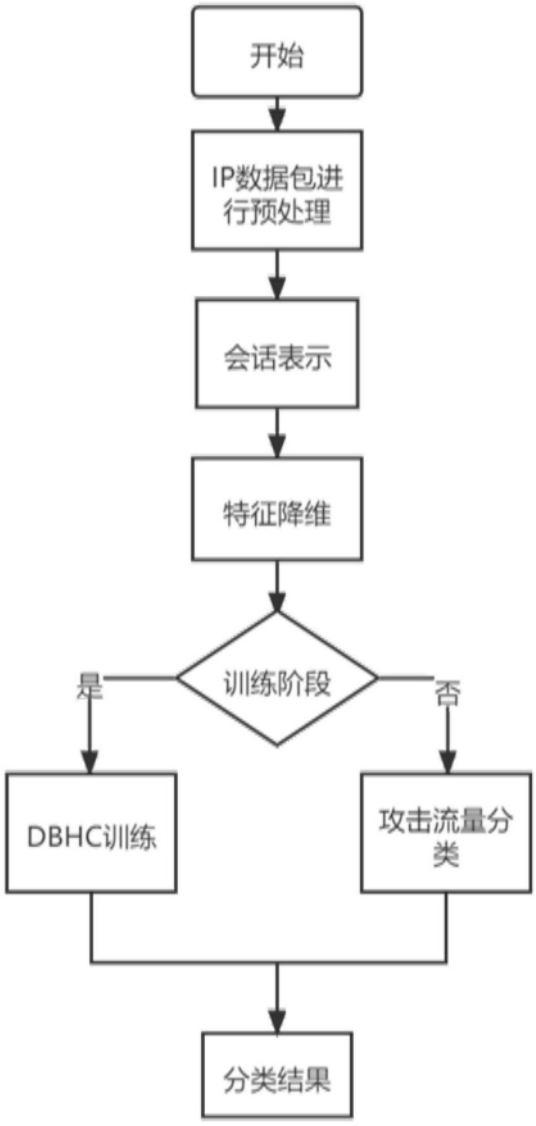

开始
IP数据包进行预处理
会话表示
特征降维
训练阶段
是
否
DBHC训练
攻击流量分类
分类结果

图2

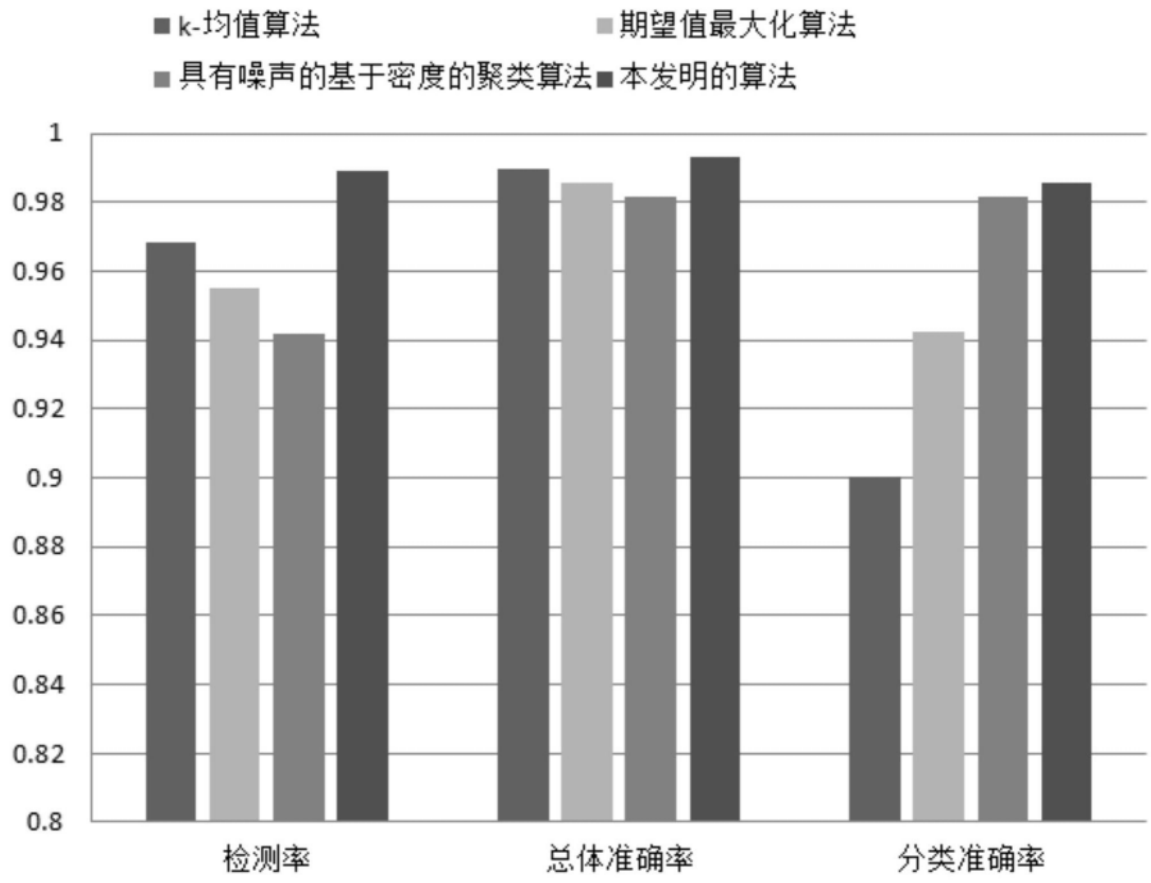

k-均值算法
期望值最大化算法
具有噪声的基于密度的聚类算法
本发明的算法
1
0.98
0.96
0.94
0.92
0.9
0.88
0.86
0.84
0.82
0.8
检测率
总体准确率
分类准确率

图3