(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111800421 B
(45)授权公告日 2021.08.24

(21)申请号 202010640942.1

(22)申请日 2020.07.06

(65)同一申请的已公布的文献号
申请公布号 CN 111800421 A

(43)申请公布日 2020.10.20

(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

(72)发明人 毕远国 郝晨阳 李凤云 黄子烜 项天敖

(74)专利代理机构 大连理工大学专利中心 21200
代理人 陈玲玉

(51)Int.Cl.
H04L 29/06(2006.01)
G06Q 10/04(2012.01)
G06N 3/08(2006.01)
G06N 3/04(2006.01)
G06K 9/62(2006.01)

(56)对比文件
CN 107948172 A,2018.04.20
CN 111294341 A,2020.06.16

审查员 黄苏一

权利要求书3页 说明书12页 附图6页

(54)发明名称

一种基于隐马尔科夫模型的车联网入侵检测系统

(57)摘要

本发明属于车联网中入侵检测算法领域，具体涉及一种基于隐马尔科夫模型的车联网入侵检测系统。该系统用于对车联网中的False alert攻击、Sybil攻击、Black hole攻击和DoS攻击的入侵检测。系统设计中主要包括预检测模块，基于DNN的检测中心模块，用于记录车辆状态和生成隐马尔科夫模型的更新模块以及用于产生响应信号的响应中心模块，在车联网正常运行状态下，这几个模块共同保证车联网的高效运行。在攻击检测状态下相辅相成，共同完成一次攻击监测防御过程。在检测精度、开销和检测时间上相比基于DNN的IDS，本发明的检测精度更高，而且平均检测时间远小于基于DNN的IDS，同时具有更少的开销，本发明使用预检测机制相比于使用状态切换的IDS具有更少的开销，更节省计算资源。

CN 111800421 B

1.一种基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,包括预检测模块、更新模块、检测中心模块和响应中心模块;

预检测模块用于过滤邻居车辆的消息;该模块中主要的功能包括获得数据包的目的地址,获得下一跳路径,获得邻居车辆ID,获得邻居车辆起始位置,计算当下位置和起始位置的差值,判断邻居车辆的ID是否在通信范围内,获得邻居车辆消息类型,获得接收的数据包大小,设置数据包大小,添加攻击节点,转发消息;预检测模块从更新模块接收每个邻居车辆的预测链,然后将预测链和该预测链的相关参数存储在预测表中,根据其接收的消息判断ID是否存在于该预测表中,如果存在,判断是否需要更新隐马尔科夫模型,然后根据预测链预测车辆是“正常”节点还是“异常”节点,并将决策结果发送至更新模块和响应中心模块;否则,将邻居车辆的消息转发到检测中心模块;

更新模块用于维护记录表并且根据记录表建立新的隐马尔科夫模型,隐马尔科夫模型生成预测链后会将其发送给预检测模块;而从预检测模块和检测中心模块接收的结果会被记录到更新模块的记录表中,当模型学习时,随机初始化参数值,并根据记录表中车辆的检测结果,利用baum-welch算法学习出模型的最优参数;

检测中心模块中的特征提取模块提取识别攻击的特征,分类器模块用于根据特征对攻击进行分类;无法被预检测模块过滤掉的车辆将由检测中心模块检测,经由检测中心将其标记为“正常”或“异常”,并将结果发送至更新模块和响应中心模块;

响应中心模块从预检测模块和检测中心接收到检测结果,根据检测结果返回相应的信号,使网络管理员做出规避措施,使得车联网损失达到最小;

检测中心模块的特征提取模块,用于提取能够识别False alert攻击的交通流量特征、Sybil攻击的车辆位置特征、Black hole攻击的数据包转发率特征和DoS攻击的数据包转发频率特征;

检测中心模块的特征提取模块,提取能够识别False alert攻击的交通流量特征值Flow;基于Green shield模型,得到交通流量q,根据公式(4)计算出主车所在道路的平均q值$AvgFlow_{own}$,其中q_{ne}代表邻居车辆所在道路的q值,q_{own}代表主车所在道路的q值,n-1代表主车周围邻居车辆的个数;按照同样的方式计算出目标车辆及目标车辆邻居车辆所在道路的平均q值$AvgFlow_{tag}$,如公式(5),q_{tne}代表目标车辆的邻居车辆所在道路的q值,q_{tag}代表目标车辆所在道路q值,m-1代表目标车辆周围邻居车辆的个数;

$$AvgFlow_{own}=\frac{1}{n}\times(\sum_{1}^{n-1}q_{ne}+q_{own}) \quad (4)$$

$$AvgFlow_{tag}=\frac{1}{m}\times(\sum_{1}^{m-1}q_{tne}+q_{tag}) \quad (5)$$

将公式(4)和公式(5)的差值作为特征值Flow,如公式(6)所示,

$Flow=|AvgFlow_{own}-AvgFlow_{tag}|$ (6)。

2.根据权利要求1所述的基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,检测中心模块的特征提取模块,提取能够识别Sybil攻击的车辆位置特征;分两种情形提取车辆位置特征:第一种情形是目标车辆在主车的通信范围内;第二种情形是目标车辆不在主车的通信范围内;

1)目标车辆在通信范围内Pos_{In};

通过公式(9)计算出t-1时刻主车和目标车辆的测量距离d_{tm-1},通过欧式距离计算出t时刻主车和目标车辆的声称距离d_{tm},如公式(10)所示,X_{posown}和Y_{posown}代表主车所在位置,X_{postag}和Y_{postag}代表目标车辆声称位置;两个时刻距离的差值Pos_{In}作为车辆位置特征,如公式(11)所示;

$$d_{tm-1}=\sqrt[4]{\frac{P_tG_tG_rh_t^2h_r^2}{P_r(d)L}} \quad (9)$$

$$d_{tm}=\sqrt{(X_{posown}-X_{postag})^2+(Y_{posown}-Y_{postag})^2} \quad (10)$$

$$Pos_{In}=|d_{tm-1}-d_{tm}| \quad (11)$$

其中,P_t是发送信号的强度,G_t和G_r分别是发射器和接收器的天线增益,h_t和h_r分别是发射天线和接收天线的高度,$p_r(d)$是发送功率,L是系统损失;

2)目标车辆不在通信范围内Pos_{out};

若目标车辆不在通信范围内,则需要邻居车辆转发数据包,此时主车和目标车辆之间的间隔为d_{ot},如公式(12)所示;主车和邻居车辆之间的间隔为d_{on},如公式(13)所示,邻居车辆和目标车辆之间的间隔为d_{nt},如公式(14)所示,X_{postag}和Y_{postag}代表目标车辆声称位置,X_{posn}和Y_{posn}代表邻居车辆所在位置;如公式(15)所示,Pos_{out}越接近0则说明目标车辆携带Sybil攻击的可能性越小;

$$d_{ot}=\sqrt[4]{\frac{P_tG_tG_rh_t^2h_r^2}{P_r(d)L}} \quad (12)$$

$$d_{on}=\sqrt[4]{\frac{P_t'G_t'G_r'h_t'^2h_r'^2}{P_r'(d)L'}} \quad (13)$$

$$d_{nt}=\sqrt{(X_{postag}-X_{posn})^2+(Y_{postag}-Y_{posn})^2} \quad (14)$$

$$Pos_{out}=|d_{ot}-(d_{on}+d_{nt})| \quad (15)。$$

3.根据权利要求1所述的基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,检测中心模块的特征提取模块,提取能够识别Black hole攻击的数据包转发率特征和DoS攻击的数据包转发频率特征;在每一条通信链路上安装一个看门狗,看门狗计算通信链路上每一个节点的数据包转发率,并将该数据包转发率随消息一起发送出去;如公式(16)所示,Pdr代表数据包的转发率,S_{in}代表节点接收数据包的数目,S_{out}代表节点发送数据包的数目;

$$Pdr=\frac{S_{in}-S_{out}}{S_{in}}\times 100\% \quad (16)。$$

4.根据权利要求1所述的基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,检测中心模块中的分类器模块有四层,即输入层、两层隐藏层以及输出层;输入层包括6个神经元,分别是x_1,x_2,x_3,x_4,x_5和一个偏执神经元,其中五个分别代表交通流量特征Flow、位置特征Pos_{In}和Pos_{out}、数据包转发率特征Pdr和数据包转发频率特征F_s;第一层隐藏层由30个神经元组成,第一层隐藏层的每个神经元连接到输入层的所有单元;第二层隐藏层由20个神经元组成,第二层隐藏层的每个神经元连接到第一层隐藏层的所有单元;输出层包括一

个神经元,输出层输出一个二分类值r,该值如果是“0”代表节点是“正常”节点,如果是“1”代表节点是“异常”节点;在本分类器模型中,输入层不使用激活函数,其它层都使用sigmoid激活函数进行非线性变换。

5.根据权利要求4所述的基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,分类器的训练过程如下:首先利用车辆历史消息训练出一个分类器模型,在真实交通环境中,将训练好的分类器模型加载到车联网入侵检测系统中用来对未知车辆进行预测,然后通过Greenshield模型计算交通流量值,通过Two-ray ground reflection模型计算出车辆的测量距离,每一辆车通过GPS获取车辆的位置坐标,车辆之间发送的消息中包括车辆的ID、车辆密度、车辆位置坐标、速度、车辆作为转发节点时接收数据包个数和实际转发数据包个数,当接收到目标车辆的消息时,主车计算自己的平均交通流量$AvgFlow_{own}$,并和目标车辆平均交通流量$AvgFlow_{tag}$做差值提取出流量特征Flow,接着计算目标车辆的数据包转发率特征Pdr和数据包转发频率特征F_s,然后判断目标车辆是否在通信范围内,根据判断结果提取位置特征,将提取出的这些特征作为一条特征输入到训练好的分类器中,就得到分类结果。

6.根据权利要求1所述的基于隐马尔科夫模型的车联网入侵检测系统,其特征在于,预检测模块中提出的车联网中的隐马尔科夫模型被定义为$\lambda=(A,B,\theta)$,A表示车辆状态转移概率矩阵,B表示车辆输出观测矩阵,θ是车辆初始状态概率,记为$\theta=(\theta_1,\theta_2,...,\theta_n)$,其中$\theta_i=P(y_1=Y_i)$,表示车辆的初始状态为$Y_i$的概率;

预检测模块构建的隐马尔科夫模型中的变量分为两组,第一组是邻居车辆的状态变量,状态空间Y∈{“安全”,“不安全”},划分为n个离散水平Y:$\{y_1,y_2,...,y_n\}$,其中$y_t\in Y$表示第t时刻车辆的状态,车辆的状态是隐藏的、不可被观测的;

在车联网中,车辆的状态在多个状态$\{y_1,y_2,...,y_n\}$间转换,转换的概率用状态转移概率矩阵$A(a_{ij})$表示,如公式(17)所示,P表示车辆的状态i从t-1时刻转变为t时刻状态j的概率,用a_{ij}表示;

$$A(a_{ij})=[a_{ij}],\text{where } i,j\in Y,a_{ij}=P(y_t=j|y_{t-1}=i) \quad (17)$$

第二组是观测变量,车辆的观测空间X表示为{“正常”,“异常”},划分为m个离散水平X:$\{x_1,x_2,...,x_n\}$,其中$x_t\in X$表示第t时刻车辆的观测值;令时刻t的状态值为Y_t,观测值为X_t,则在任意时刻t,若车辆的状态为i,则观测矩阵$B(b_j(x_t))$中$b_j(x_t)$表示观测值x_t被获取的概率,见公式(18);

$$b_j(x_t)=P\{X_t=x_t|Y_t=i\},\text{where } i\in Y,x_t\in X \quad (18)$$

在t时刻,状态Y_t的观测值为X_t的概率序列就可以用观测矩阵$B(b_j(x_t))$表示,如公式(19)所示:

$$B(b_j(y_t))=\text{diag}[b_1(y_t),...,b_N(y_t)] \quad (19)。$$

一种基于隐马尔科夫模型的车联网入侵检测系统

技术领域

[0001] 本发明属于车联网中入侵检测算法领域，具体涉及一种基于隐马尔科夫模型的车联网入侵检测系统。该系统用于对车联网中的False alert攻击、Sybil攻击、Black hole攻击和DoS攻击的入侵检测。

背景技术

[0002] 车联网作为物联网中一个重要的概念，不仅在学术研究中成为热点，而且在工程领域也受到了广泛的应用。无论是物联网还是互联网，其背后的安全问题都是首要关心的问题，而这些安全问题具体表现为严重的交通堵塞、耗油量逐年增加以及交通事故源源不断等。但由于国民经济逐年迅速的增长，汽车的销售量也随之倍增，这些问题是无法避免的。

[0003] 但是将网络应用于具有动态拓扑结构的交通环境中，这项技术带来了很多的安全隐患。如果无法解决，必定会造成严重的后果和不可挽回的损失，因此，这一技术的关键和核心就是解决安全问题。计算机网络中的安全问题早已暴露，并且许多的问题都有效的解决了，但是由于车联网中层出不穷的攻击以及车联网这一领域的特殊性，使得同样的安全问题在车联网中不仅表现不同，而且安全解决方案也无法有效的应用。

[0004] 车联网是一代新型网络，主要是以数据为中心，而一些传统网络是以地址为中心，所以在传统网络中影响不大、破坏也较小的攻击，但是在车联网中会有非常大的危害性。另外，车联网由于其动态拓扑特性，使得车联网中的安全问题变得更加复杂，解决方案的也变得不再容易。

[0005] 对于车联网中的攻击车辆的检测和防御中，除了考虑攻击的检测方法外，也需要对车联网通信链路进行一定的分析和研究。总之，在车联网攻击检测和防御的研究中，除了借鉴计算机网络安全的解决方案，也要考虑车联网固有的特点，然后将二者结合后再进行应用创新，另外，利用当下深受欢迎的深度学习在一定程度上优化检测和防御的研究。

发明内容

[0006] 针对上述问题，本发明的目的是提供一种适用于车联网环境的基于隐马尔可夫模型的深度学习的入侵检测系统，在保证可靠性的同时，能够有效降低传输时延、减轻网络负载。

[0007] 本发明设计的一种基于隐马尔科夫模型的车联网入侵检测系统，即预检测模块，更新模块，检测中心模块和响应中心模块。

[0008] 预检测模块用于过滤邻居车辆的消息。该模块中主要的功能包括获得数据包的目的地址；获得下一跳路径；获得邻居车辆ID；获得邻居车辆起始位置；计算当下位置和起始位置的差值；判断邻居车辆的ID是否在通信范围内；获得邻居车辆消息类型；获得接收的数据包大小；设置数据包大小；添加攻击节点；转发消息。它从更新模块接收每个邻居车辆的预测链，然后将预测链和该预测链的相关参数存储在预测表中，根据其接收的消息判断ID

是否存在于该预测表中，如果存在，判断是否需要更新隐马尔科夫模型，然后根据预测链预测车辆是“正常”节点还是“异常”节点，并将决策结果发送至更新模块和响应中心。否则，将邻居车辆的消息转发到检测中心模块。

[0009] 更新模块负责维护记录表并且根据记录表建立新的隐马尔科夫模型，隐马尔科夫模型生成预测链后会将其发送给预检测模块。而从预检测模块和检测中心模块接收的结果会被记录到更新模块的记录表中，当模型学习时，随机初始化参数值，并根据记录表中车辆的检测结果，利用baum-welch算法(Bilmes,Jeff A.A gentle tutorial of the EM algorithm and its application to parameter estimation for gaussian mixture and hidden markov models[M].CA:International Computer Science Institute,1998,7-13.)学习出模型的最优参数。

[0010] 检测中心模块中的特征提取模块可以提取识别攻击的特征，分类器模块用于根据特征对攻击进行分类。无法被预检测模块过滤掉的车辆将由检测中心模块检测，经由检测中心将其标记为“正常”或“异常”，并将结果发送至更新模块和响应中心模块。

[0011] 响应中心模块从预检测模块和检测中心接收到检测结果，根据检测结果返回相应的信号，使网络管理员做出一些规避措施，使得车联网损失达到最小。

[0012] 检测中心模块主要是检测预检测模块无法过滤的车辆，该模块包括特征提取模块和分类器模块。

[0013] 特征提取模块主要用来提取能够识别False alert攻击的交通流量特征、Sybil攻击的车辆位置特征、Black hole攻击的数据包转发率特征和DoS攻击的数据包转发频率特征。

[0014] 这部分主要是提取交通流量特征Flow，因为在相同的交通条件下，每个车辆的交通流量应当与其邻居车辆的交通流量非常接近。如果攻击车辆为了创造不存在的事故，从而为自己开辟一条道路，攻击车辆可以降低自己的流量，这个流量与正常情况下不同。因此，提取交通流量特征Flow能够检测False alert攻击。

[0015] 如图2所示，为了能提取出特征Flow，使用了Green shield模型(Greenshield's model.https://www.webpages.uidaho.edu/niatt_labmanual/chapters/trafficflowtheory/theoryandconcepts/greenshieldsmodel.htm.last access 2019.)，该模型主要用来描述速度v，密度k和交通流量q这三者之间的关系。

[0016] 表1 Green shield模型中各个变量的说明

[0017]

变量名	定义	单位	描述
v	速度	公里/小时	每小时车辆行驶的路程
k	密度	车辆/公里	每公里车辆数
q	交通流量	车辆/小时	每小时车辆数
v_j	自由流量车速	公里/小时	当密度最小时车辆的速度
k_j	拥塞密度	车辆/公里	密度能够达到的最大值，此时速度为0
k_m	最优道路车辆速度	车辆/公里	-
v_m	最优道路车辆密度	公里/小时	-
q_j	最优道路交通流量	车辆/小时	最优道路车辆密度和车辆速度下的交通流量值

[0018] 图2中各个变量的物理意义描述如上表所示。在图2左侧中是车辆速度和车辆密度的关系图，可以看出，随着道路车辆密度的上升，车辆速度就会下降，直到达到拥塞密度，v和k之间的关系如公式(1)所示。在图2右侧中是车辆速度与密度和交通流量之间的关系图，q与v/k的关系如公式(2)所示。

[0019] $$v_j = v_j - \frac{k}{k_j} \times v_j \quad (1)$$

[0020] $$q = k \times v \quad (2)$$

[0021] 由公式(1)和(2)可以获得q和k的关系式(3)：

[0022] $$q = v_j \times k - \frac{k^2}{k_j} \times v_j \quad (3)$$

[0023] 基于Green shield模型，以及公式(1)，(2)和(3)，能够得到交通流量q，根据公式(4)计算出主车所在道路的平均q值$AvgFlow_{own}$，其中q_{ne}代表邻居车辆所在道路的q值，q_{own}代表主车所在道路的q值，n-1代表主车周围邻居车辆的个数。接着按照同样的方式计算出目标车辆及目标车辆邻居车辆所在道路的平均q值$AvgFlow_{tag}$，如公式(5)所示，q_{tne}代表目标车辆的邻居车辆所在道路的q值，q_{tag}代表目标车辆所在道路q值，m-1代表目标车辆周围邻居车辆的个数。

[0024] $$AvgFlow_{own} = \frac{1}{n} \times (\sum_1^{n-1} q_{ne} + q_{own}) \quad (4)$$

[0025] $$AvgFlow_{tag} = \frac{1}{m} \times (\sum_1^{m-1} q_{tne} + q_{tag}) \quad (5)$$

[0026] 接着将公式(4)和公式(5)的差值作为特征值Flow，如公式(6)所示，求差值的物理意义是在相同的道路环境下，两个车的交通流量非常相似，所以这个差值越大说明目标车

辆是攻击车辆的可能性也越大。

[0027] $Flow=|AvgFlow_{own}-AvgFlow_{tag}|$ (6)

[0028] 为了能够提取出反映Sybil攻击的位置信息的特征，使用在NS3中实现的无线电传播模型Two-ray ground reflection model。该模型考虑了直接和地面反射路径，并在接收数据包时评估每个数据的信号强度，公式如(7)所示。公式中$p_r(d)$是发送功率，d是发送方和接受方之间的距离，P_t是发送信号的强度，L(L＞＝1)是系统损失，G_t和G_r分别是发射器和接收器的天线增益，h_t和h_r分别是发射天线和接收天线的高度。

[0029] $$P_r(d)=\frac{P_tG_tG_rh_t^2h_r^2}{d^4L} \quad (7)$$

[0030] 因而，主车和目标车辆测量距离的公式如公式(8)。

[0031] $$d=\sqrt[4]{\frac{P_tG_tG_rh_t^2h_r^2}{P_r(d)L}} \quad (8)$$

[0032] 接下来分两种情形提取车辆位置特征：第一种情形是目标车辆在主车的通信范围内；第二种情形是目标车辆不在主车的通信范围内，此时需要邻居车辆转发数据包，所以要分别检查目标车辆和邻居车辆，由于邻居车辆在主车的通信范围内，所以检查的方式和第一种情况检查方式相同。下面分别讨论这两种情形。

[0033] (1)目标车辆在通信范围内

[0034] 通过公式(9)计算出t-1时刻主车和目标车辆的测量距离d_{tm-1}，通过欧式距离计算出t时刻主车和目标车辆的声称距离d_{tm}，如公式(10)所示，X_{posown}和Y_{posown}代表主车所在位置，X_{postag}和Y_{postag}代表目标车辆声称位置。两个时刻距离的差值Pos_{In}作为车辆位置特征，如公式(11)所示。计算两者差值Pos_{In}的物理意义是，主车和目标车之间的距离在t-1时刻和t时刻应该非常接近，差值越大则目标车辆携带Sybil攻击的可能性越大。

[0035] $$d_{tm-1}=\sqrt[4]{\frac{P_tG_tG_rh_t^2h_r^2}{P_r(d)L}} \quad (9)$$

[0036] $$d_{tm}=\sqrt{(X_{posown}-X_{postag})^2+(Y_{posown}-Y_{postag})^2} \quad (10)$$

$$Pos_{In}=|d_{tm-1}-d_{tm}| \quad (11)$$

[0037] (2)目标车辆不在通信范围内

[0038] 若目标车辆不在通信范围内，则需要邻居车辆转发数据包，此时主车和目标车辆之间的间隔为d_{ot}，如公式(12)所示。主车和邻居车辆之间的间隔为d_{on}，如公式(13)所示，邻居车辆和目标车辆之间的间隔为d_{nt}，如公式(14)所示，X_{postag}和Y_{postag}代表目标车辆声称位置，X_{posn}和Y_{posn}代表邻居车辆所在位置。如公式(15)所示，Pos_{out}越接近0则说明目标车辆携带Sybil攻击的可能性越小。

[0039] $$d_{ot}=\sqrt[4]{\frac{P_tG_tG_rh_t^2h_r^2}{P_r(d)L}} \quad (12)$$

[0040] $$d_{on}=\sqrt[4]{\frac{P_t'G_t'G_r'h_t'^2h_r'^2}{P_r'(d)L'}} \quad (13)$$

[0041] $$d_{nt}=\sqrt{(X_{postag}-X_{posn})^2+(Y_{postag}-Y_{posn})^2} \quad (14)$$

[0042] $Pos_{out}=|d_{ot}-(d_{on}+d_{nt})|$ (15)

[0043] 如图3,A车和C车不在同一通信范围内,如果要发送数据包,则需要B车转发,B车如果不是攻击车辆,那么在不考虑数据包冲突的情况下,B车将全部转发,如果B车携带攻击,那么数据包将会被B车全部丢弃或者重定向。

[0044] 携带黑洞攻击的车辆会将接收到的数据包全部丢弃,那么可以通过检测一条通信链路上节点的转发率来检测该节点是否携带Black hole攻击。具体的操作如下,在每一条通信链路上都安装一个看门狗,看门狗计算通信链路上每一个节点的数据包转发率,并将该数据包转发率随消息一起发送出去。如公式(16)所示,Pdr代表数据包的转发率,S_{in}代表节点接收数据包的数目,S_{out}代表节点发送数据包的数目。

[0045] $$Pdr=\frac{S_{in}-S_{out}}{S_{in}}\times 100\% \quad (16)$$

[0046] 车联网中的DoS攻击主要是通过频繁的请求连接而导致服务器崩溃,因此通过计算节点发送数据包的频率可以检测出车联网中的DoS攻击。节点单位时间发送数据包数目的公式如(17)所示,公式中S_{out}代表节点发送数据包的数量,T代表发送周期,单位为秒,F_s代表节点每秒发送的数据包数目,即发送频率。

[0047] $$F_s=\frac{S_{out}}{T} \quad (17)$$

[0048] 提取出能够识别出车联网中的False alert攻击,Sybil攻击,Black hole攻击和DoS攻击的特征后,分类器模块选择了具有高检测精度和高表达能力的DNN作为分类器。

[0049] 有监督的DNN模型常常用于检测网络中的异常,如图4所示,的分类器模块有四层,即输入层Layer1,两层隐藏层Layer2和Layer3以及输出层Layer4。这些层由许多神经元组成,也称为单位。

[0050] 图4的输入层包括6个神经元,分别是x_1,x_2,x_3,x_4,x_5和一个偏执神经元,分别代表交通流量特征Flow、位置特征Pos_{In}和Pos_{out}、数据包转发率特征Pdr和数据包转发频率特征F_s。第一层隐藏层由30个神经元组成,第一层隐藏层的每个神经元连接到输入层的所有单元。第二层隐藏层由20个神经元组成,第二层隐藏层的每个神经元连接到第一层隐藏层的所有单元。输出层包括一个神经元,输出层输出一个二分类值r,该值如果是“0”代表节点是“正常”节点,如果是“1”代表节点是“异常”节点。在本分类器模型中,输入层不使用激活函数,其它层都使用sigmoid激活函数进行非线性变换。尽管sigmoid激活函数在模型训练的时候容易引起梯度弥散的问题,然而提出的分类器模型只有四层,不会出现梯度弥散的问题。

[0051] 模型采用有监督训练方式,在训练阶段,将样本标签设置为0或1,其中将“正常”节点的标签值设置为0,“异常”节点的标签值设置为1,“正常”节点不携带任何攻击,“异常”节点包括携带False alert攻击,Sybil攻击,Black hole攻击和DoS攻击的样本。

[0052] DNN训练分为两个阶段:正向传播阶段和反向传播阶段。第一阶段是前向传播阶

段。神经网络的各层是完全连接的，即第i层的任意一个神经元一定与第i+1层的任意一个神经元相连。从输入层到隐藏层到最终输出层，每个层节点仅接受上一层的输入，并影响下一层的输出。第二阶段是反向传播阶段。如果未达到最大迭代次数或未获得预期输出，则将计算实际输出与预期输出之间的误差，并从最后一层到第一层逐层更新。更新每一层的连接权重是为了使输出值无限接近预期值。

[0053] 分类器的训练过程如下：首先利用车辆历史消息训练出一个分类器模型，在真实交通环境中，将训练好的分类器模型加载到IDS中用来对未知车辆进行预测，然后可以通过Greenshield模型计算交通流量值，通过Two-ray ground reflection模型计算出车辆的测量距离，每一辆车通过GPS获取车辆的位置坐标，车辆之间发送的消息中包括车辆的ID，车辆密度，车辆位置坐标，速度，车辆作为转发节点时接收数据包个数和实际转发数据包个数，当接收到目标车辆的消息时，主车计算自己的平均交通流量$AvgFlow_{own}$，并和目标车辆平均交通流量$AvgFlow_{tag}$做差值提取出流量特征Flow，接着计算目标车辆的数据包转发率特征Pdr和数据包转发频率特征F_s，然后判断目标车辆是否在通信范围内，根据判断结果提取位置特征，将提取出的这些特征作为一条特征输入到训练好的分类器中，就可以得到分类结果。

[0054] 更新模块一方面维护记录表，另一方面要根据记录表生成A、B并初始化θ，从而生成上述的隐马尔科夫模型。

[0055] 预检测模块中提出的车联网中的隐马尔科夫模型如图8所示，该模型被定义为$\lambda=(A,B,\theta)$，A表示车辆状态转移概率矩阵，B表示车辆输出观测矩阵，θ是车辆初始状态概率，记为$\theta=(\theta_1,\theta_2,\ldots,\theta_n)$，其中$\theta_i=P(y_1=Y_i)$，表示车辆的初始状态为$Y_i$的概率。

[0056] 预检测模块构建的隐马尔科夫模型中的变量可以分为两组，第一组是邻居车辆的状态变量，状态空间Y∈{“安全”，“不安全”}，可以划分为n个离散水平$Y:\{y_1,y_2,\ldots,y_n\}$，其中$y_t\in Y$表示第t时刻车辆的状态，车辆的状态是隐藏的、不可被观测的。

[0057] 在车联网中，车辆的状态在多个状态$\{y_1,y_2,\ldots,y_n\}$间转换，转换的概率用状态转移概率矩阵$A(a_{ij})$表示，如公式(17)所示，P表示车辆的状态i从t-1时刻转变为t时刻状态j的概率，用a_{ij}表示。

[0058] $$A(a_{ij})=[a_{ij}],\text{where } i,j\in Y,a_{ij}=P(y_t=j|y_{t-1}=i) \quad (17)$$

[0059] 第二组是观测变量，车辆的观测空间X表示为{“正常”，“异常”}，可以划分为m个离散水平$X:\{x_1,x_2,\ldots,x_n\}$，其中$x_t\in X$表示第t时刻车辆的观测值。令时刻t的状态值为Y_t，观测值为X_t，则在任意时刻t，若车辆的状态为i，则观测矩阵$B(b_j(x_t))$中$b_j(x_t)$表示观测值x_t被获取的概率，见公式(18)。

[0060] $$b_j(x_t)=P\{X_t=x_t|Y_t=i\},\text{where } i\in Y,x_t\in X \quad (18)$$

[0061] 那么在t时刻，状态Y_t的观测值为X_t的概率序列就可以用观测矩阵$B(b_j(x_t))$表示，如公式(19)所示。

[0062] $$B(b_j(y_t))=\text{diag}[b_1(y_t),\ldots,b_N(y_t)] \quad (19)$$

[0063] 上述隐马尔科夫模型可以预测邻居车辆未来时刻的行为，然后将检测结果直接反馈。

[0064] 响应中心主要从预检测模块和检测中心接收到检测结果，根据检测结果标记为“正常”节点或者“异常”节点来返回相应的信号。

[0065] 本发明的有益效果为:在检测精度、开销和检测时间上相比基于DNN的IDS,本发明提出的基于隐马尔科夫模型的IDS的检测有更高的精度,而且平均检测时间远小于基于DNN的IDS,同时具有更少的开销,本发明使用预检测机制相比于使用状态切换的IDS具有更少的开销,更节省计算资源。

附图说明

[0066] 图1是入侵检测算法框架。

[0067] 图2是Green shield模型,(a)密度k&速度v,(b)速度v/密度k&交通流量q。

[0068] 图3是攻击车辆示意图。

[0069] 图4是DNN分类器模型。

[0070] 图5是IDS框架。

[0071] 图6是隐马尔科夫模型的图结构。

[0072] 图7是车辆状态的转移示意图。

[0073] 图8是车联网中的隐马尔科夫模型。

[0074] 图9是预检测模块工作流程图。

[0075] 图10是更新模块流程图。

[0076] 图11是检测中心训练阶段流程图。

[0077] 图12是检测中心预测阶段流程图。

[0078] 图13是路基设施范围图。

[0079] 图14是IDS在线学习阶段。

[0080] 图15是IDS预测流程图。

具体实施方式

[0081] 图2展示了Green shield模型中车辆速度与密度和交通流量之间的关系

[0082] 图3为黑洞攻击车辆的示意图

[0083] 图4展示了DNN的结构

[0084] 图5显示了本发明设计的简单易操作的系统。

[0085] 隐马尔科夫模型的图结构如图6所示。

[0086] 本发明提出的车联网中的隐马尔科夫模型如图8所示,

[0087] 图9中的流程图,预检测模块会实时的从更新模块获取预测链更新到自己的预测表中,当接收到消息时,预检测模块判断消息的ID是否存在于预测表中,如果存在,判断是否更新隐马尔科夫模型,然后根据预测链判断该ID是“正常”节点还是“异常”节点,并将检测结果和相应参数发送至更新模块和响应中心模块。该模块必须定义的属性有:标准包的大小;正常消息报文标记;转发消息报文标记;目标消息报文标记;车辆唯一ID;转发、源、目标消息的标记;数据包大小;目的路径和转发路径的标记。

[0088] 该模块中主要的功能是:获得数据包的目的地址;获得下一跳路径;获得邻居车辆ID;获得邻居车辆起始位置;计算当下位置和起始位置的差值;判断邻居车辆的ID是否在通信范围内;获得邻居车辆消息类型;获得接收的数据包大小;设置数据包大小;添加攻击节点;转发消息。

[0089] 该模块的流程图如图10,不管邻居车辆的ID是否存在于预检测模块的预测表,都应该将检测结果更新并记录到更新模块的记录表中,该记录表中存储每一时刻该车辆的检测结果。经过多次试验证明,当记录表中记录的检测结果达到100个时,隐马尔科夫模型会学习到最优的参数,因此本发明将该值设置为100。

[0090] 该模块必须定义的属性有:车辆唯一ID;预测链存储变量;检测时刻。该模块主要的功能有:实现baum-welch算法。

[0091] 首先,在训练阶段,将所有训练样本通过特征提取模块计算并提取出这些样本的流量特征Flow,位置特征Pos_{In}和Pos_{out},消息的转发率Pdr,消息的转发频率F_s,将这些特征作为特征向量记录到特征记录表中,当特征记录表的数量足够多时,将这些特征输入到四层的神经网络模型中,每一次迭代中都进行前向传播和反向传播,在经过多次迭代之后模型的参数变化值都小于停止迭代阈值,此时模型的损失函数达到最优解,最后将训练好的模型保存起来。经过多次试验证明,当特征记录表中数量越多,模型学习的越好,但是训练时间也越长,因此为了同时保证学习效果和效率,本系统将记录数值设置为10000。训练阶段的流程图如图11所示。

[0092] 在预测阶段,将邻居车辆的消息经过特征提取后直接输入模型,经过DNN模型后将节点分为“正常”节点或“异常”节点,最后将检测结果发送至更新模块和响应中心。将模型输出概率值以0.5为界限分为“正常”节点或“异常”节点是因为本发明使用的是sigmoid激活函数。预测阶段的流程图如图12所示。

[0093] 为了计算提取这些特征,该模块必须定义的属性有:标识一个车辆唯一的ID;车辆类型;车辆的位置;标识车辆的速度;车辆起始位置;车辆目的位置。这些值都是String类型的,除了ID不能是空值,其他值可以出现空值。该模块的主要功能有:设置车辆的属性;计算交通流量;判断目标车辆是否在通信范围内;计算交通位置;计算数据包转发率;计算数据包转发频率。

[0094] 系统会对每一个车辆一个信誉分,根据不同攻击类型对车联网的破坏,车辆每一次被判定为攻击车辆时,系统将扣掉相应的信誉分,直到该信誉分降到0或者负值时,系统将对该车辆进行惩罚措施。采用这样的方式,就避免了因为误判而直接将车辆节点排除在外造成的损失,只有同一车辆多次被测量为攻击车辆时才会被惩罚,同时本系统不会出现一个合法车辆被多次判定为攻击车辆的情况。

[0095] 为了让系统的相应模块具有更高的效率,避免响应过程中车辆之间频繁交换信息占用资源,本系统使用RSU来辅助响应。具体的,RSU中存储着据它距离较近的所有车辆的信誉得分,每一次检测出一个车辆可能携带攻击时,该车辆都会被上报到距他最近的RSU,而RSU会检查并扣除该车辆的信誉值。

[0096] 假设系统中每隔距离L_R处部署一个RSU,车辆的通信范围为$2L_C$,那么通信半径就是L_C,则为了减小RSU与车辆之间的通讯时间并且提高RSU处理消息的时间,同时,为了提高资源的利用率,应该使得$L_R >> L_C$。

[0097] 如图13所示,位置A处的车辆和距离其最近的路边单元1交换信息,位置B和位置C的车辆会与路边单元2交换信息,当位置B处的车辆行驶到位置A时,该车辆会得知路边单元1的信息。

[0098] 综合以上分析,每个RSU都向其通信范围内的车辆提供服务,同时协同响应模块对

每个车辆进行信誉计分，以此来完成整个IDS的安全工作。在本发明的IDS中要求每个RSU具有如下功能：

[0099] (1)记录其通信范围内所有车辆的信息，包括车辆ID，车辆位置坐标，信誉得分等。一方面记录的信息过多会导致RSU的负载过大，另一方面，一定程度上可以检测出车辆信息不一致现象。

[0100] (2)协助IDS进行车辆检测，协助相邻RSU以及车辆对被举报车辆进行监测，同时计算每个车辆的信誉得分。

[0101] (3)对每个信誉得分为0或负值的车辆直接进行拒绝服务的操作，同时断掉其所有正在进行的服务。

[0102] 在开始时，记录表是空的，所以用于生成隐马尔科夫模型的参数A、B和θ是未知的，因此系统包括在线学习阶段和预测阶段。在线学习阶段用来记录足够多的参数，以生成隐马尔科夫模型，之后将模型保存起来，在预测阶段，加载这个模型，对接收到的消息进行预测。

[0103] 在接收到目标车辆的消息时，如果隐马尔科夫模型未生成，则无法使用预测链进行决策，因此将消息转发至检测中心进行检测，只有当IDS经过在线学习得到了隐马尔科夫模型，预检测模块才能够对消息进行过滤。下面本发明结合图5的IDS框架分别阐述IDS在线学习阶段和预测阶段。

[0104] (1)IDS在线学习阶段，图14是IDS在线学习阶段工作流程图，其具体工作流程如下：

[0105] 1)系统在正式工作之前，需要通过历史数据集在线下训练一个分类器模型，一开始就将该分类模型加载到IDS中。当主车收到目标车辆的消息时，将消息发送至预检测模块。

[0106] 2)预检测模块接收到消息后，更新其维护的预测表，预测表中存储着邻居车辆的ID以及对应的预测链和相关参数，更新过程是从更新模块中读取最新的观测链，并写入预测表中。

[0107] 3)预检测模块判断该消息的ID是否存在于其所维护的预测表中，如果存在，在做出决策之前，判断更新模块中维护的记录表中记录的该ID的记录序列是否达到N个。

[0108] 4)如果记录表的记录序列达到100个，则随机初始化A、B和θ，结合记录序列，学习出具有最优参数的隐马尔科夫模型。接着生成新的预测链，最后将该ID的预测链和相关参数发送至预测表中。

[0109] 5)如果记录表的记录序列未达到100个，则说明此时无法通过隐马尔科夫模型过滤此消息，那么就将该消息转发至检测中心检测。

[0110] 6)检测中心收到该消息后，则对该消息进行特征处理，提取出能够识别攻击的特征：流量特征$Flow_{own}$、位置信息特征Pos_{In}和Pos_{out}、数据包转发率特征Pdr和数据包转发频率特征F_s。然后将这些特征作为一条特征记录输入到训练好的分类器模型中，分类器模型将该消息分类为正常节点或异常节点。

[0111] 7)将从预检测模块或检测中心得到的结果分别发送至记录表和响应中心。记录表记录该ID的检测结果，接着响应中心根据该检测结果做出响应。

[0112] 8)全部流程结束。

[0113] (2)IDS预测阶段,图15是IDS预测阶段工作流程图,其具体工作流程如下:

[0114] 1)系统在正式工作之前,需要通过历史数据集在线下训练一个分类器模型,一开始就将该分类模型加载到IDS中。当主车收到目标车辆的消息时,将消息发送至预检测模块。

[0115] 2)预检测模块接收到消息后,更新其维护的预测表,预测表中存储着邻居车辆的ID以及对应的预测链和相关参数,更新过程是从更新模块中读取最新的预测链,并写入预测表中。

[0116] 3)预检测模块判断该消息的ID是否存在于其所维护的预测表中,如果存在,则判断步长是否大于预测链长度,如果大于,则更新隐马尔科夫模型,生成新的预测链,并得出决策结果r,并将r发送至记录和响应中心。否则,读取该步长的预测值,并发送至记录表和响应中心。

[0117] 4)响应中心根据r返回响应信号。记录表记录r,然后根据该记录表生成该ID的A、B和θ。然后根据A,B,θ生成隐马尔科夫模型λ=(A,B,θ),接着生成预测链,最后将该ID的预测链和相关参数发送至预测表中。

[0118] 5)如果该消息的ID不存在于其所维护的预测表中,则预检测模块不对该消息做任何处理,直接将该消息转发至检测中心。

[0119] 6)检测中心收到该消息后,则对该消息进行特征处理,提取出能够识别攻击的特征:流量特征$Flow_{own}$、位置信息特征Pos_{In}和Pos_{out}、数据包转发率特征Pdr和数据包转发频率特征F_s。然后将这些特征作为一条特征记录输入到训练好的分类器模型中,分类器模型将该消息分类为正常节点或异常节点,即检测结果r。

[0120] 7)记录表记录r,接着根据该记录表生成该ID的A、B并初始化θ。然后根据A,B,θ生成隐马尔科夫模型λ=(A,B,θ),接着生成预测链,最后将该ID的预测链和相关参数发送至预测表中。响应中心根据r返回响应信号。

[0121] 8)全部流程结束。

[0122] 本系统生成正常以及异常数据的工作环境是Ubuntu18.04,编程语言是C++,需要在Ubuntu18.04环境下安装配置相应的SUMO和NS3的相关模块和依赖;IDS工作环境是Windows10,IDS中分类器模块使用Python3语言实现,其他模块是基于Java语言实现的,所以在进行相应模块的设计开发之前,需要在Windows环境下安装配置相应的Java环境。

[0123] 实验的参数如表2所示。交通场景是一个具有2车道的高速公路,公路长度为5米,通信协议是802.11p协议。为了避免在模拟中产生过多的数据,本发明将模拟时间设置为165s,车辆到达间隔为1s,传输间隔为0.1s,根据若干实验,将最大错误阈值设置为3,观测链长度设置为100。

[0124] 表2实验参数

[0125]

参数名称	参数值
实验场景	2 车道公路
高速公路长度	5km
最大车辆速度	100km/h
无线通信协议	802.11p
传输范围	500m

[0126]

模拟时间	165s
车辆到达间隔	1s
传输间隔	0.1s
最大错误阈值	3
观测链长度	100

[0127] 通过计算检测精度,开销和平均检测时间来评价所提出的IDS,计算方法如下:

[0128] (1)检测精度:即在模拟时间内不携带攻击的车辆被分类为正常节点的车辆,以及携带攻击的车辆被分类为异常节点的车辆,所占总检测车辆的百分比,假设车辆的总数为n,其中分类正确车辆的个数为m,检测精度用acc表示,则检测精度的计算公式如(20)所示。

[0129] $$acc=\frac{m}{n} \quad (20)$$

[0130] (2)开销:表示单位时间内IDS处理消息的规模,单位为Kbytes/s,用ov表示开销,t表示处理时间,k表示时间t内处理的消息的总数量,b表示每个消息的字节数,则ov的计算公式如(21)所示。

[0131] $$ov=\frac{k\times b}{t\times 1000} \quad (21)$$

[0132] (3)平均检测时间:即IDS处理消息的平均花费时间,单位为秒,假设车辆的检测时间用t表示,平均检测时间用dt表示,则计算公式如(22)所示。

[0133] $$dt=\frac{\sum_{i=1}^{n} t_i}{n} \quad (22)$$

[0134] 为了能清楚的显示检测出的攻击车辆,本发明将系统运行结果进行可视化,在界面中通过按钮来对车辆注册IDS,系统默认是基于隐马尔科夫模型的IDS,由于将同一条比较长的道路模拟在屏幕中不易于用户的直观感受,因此在系统中,当距离较远的情况下,将这条道路反映到屏幕中的其他地方。

[0135] 一旦车辆进入道路系统,每个车辆节点要向其距离最近的路基设施发送请求服务消息。区域I是菜单栏,作为控制程序运行状态的空间,可以通过菜单栏的按钮对道路中的车辆进行开始、暂停和重置的操作,用户选择注册基于DNN的IDS或基于隐马尔科夫模型的

IDS，系统默认是注册基于隐马尔科夫模型的IDS；区域II为文本提示框，在程序运行过程中显示对道路中车辆的检测结果，并实时的统计道路上车辆的总数、已经检测出的攻击车辆的数量以及车辆的平均检测时间，通过区域II，用户可以直观看到程序的运行过程。区域III对检测进度实时提示，会显示出当前检测车辆的ID、对当前车辆的检测结果，即是“正常”或“异常”，以及对当前车辆的检测时间。

[0136] 表3两种IDS性能对比

[0137]

攻击车辆比例	基于 DNN 的 IDS			基于隐马尔科夫模型的 IDS		
	检测精度	开销	平均检测时间(秒)	检测精度	开销	平均检测时间(秒)
10%	99	9	7.01	99.4	0.9	3.01
20%	98.7	4.5	7.56	99.2	1.0	4.56
30%	98.1	4.66	8.22	98.4	1.55	212
40%	98	4.78	8.35	97.6	1.79	6.35

[0138] 表3展示了在攻击车辆分别是10％、20％、30％和40％的场景中，基于DNN的IDS和基于隐马尔科夫模型的IDS之间在检测精度、开销和检测时间上的比较。由此看出，相比基于DNN的IDS，基于隐马尔科夫模型的IDS的检测精度更高，而且平均检测时间远小于基于DNN的IDS，同时，基于隐马尔科夫模型的IDS具有更少的开销。

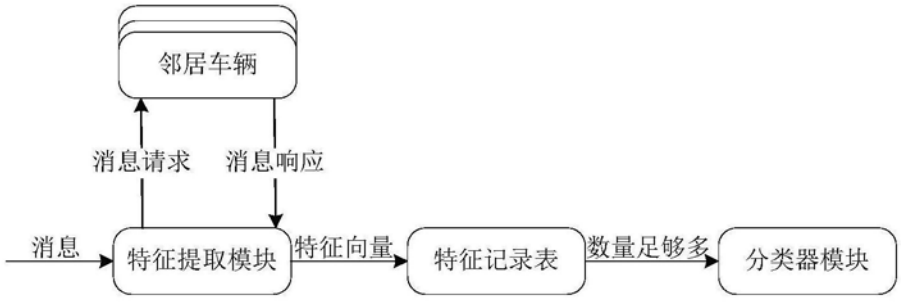
邻居车辆
消息请求
消息响应
消息
特征提取模块
特征向量
特征记录表
数量足够多
分类器模块

图1

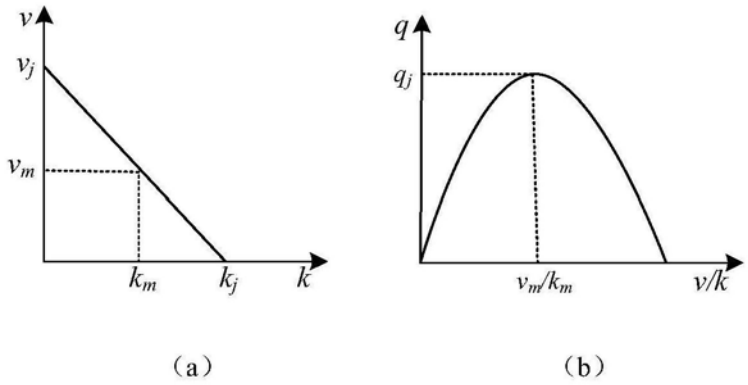
v
v_j
v_m
k_m
k_j
k
q
q_j
v_m/k_m
v/k
(a)
(b)

图2

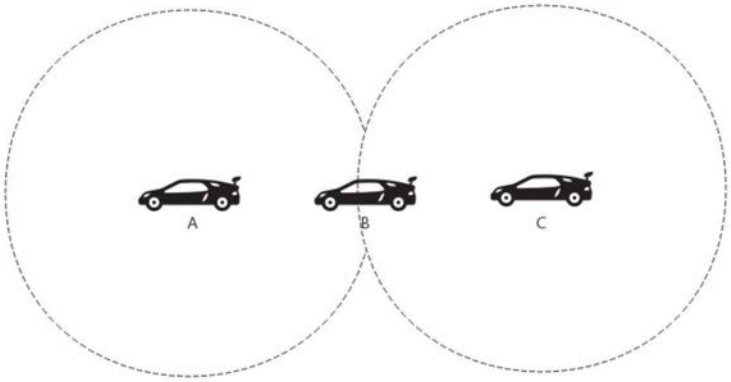
A
B
C

图3

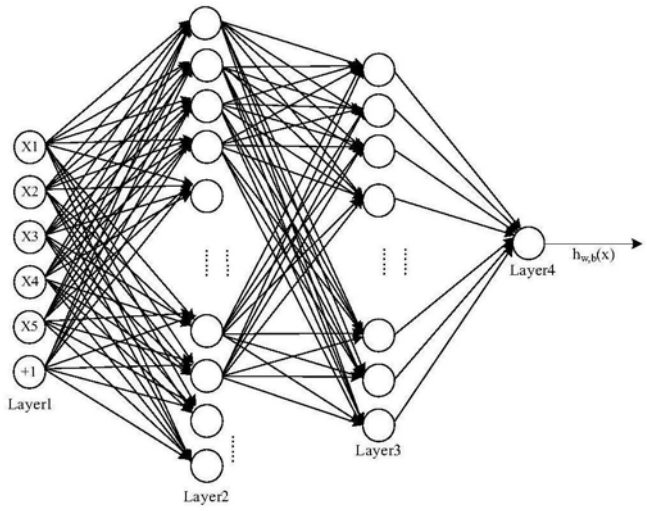
X1
X2
X3
X4
X5
+1
Layer1
Layer2
Layer3
Layer4
$h_{w,b}(x)$

图4

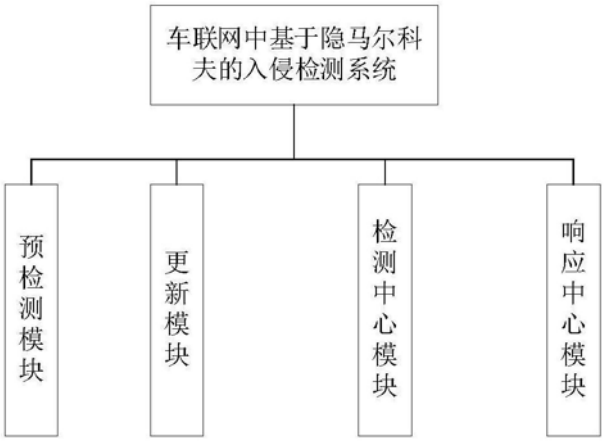
车联网中基于隐马尔科夫的入侵检测系统
预检测模块
更新模块
检测中心模块
响应中心模块

图5

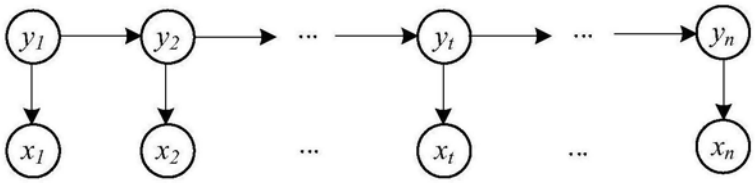
y_1
y_2
y_t
y_n
x_1
x_2
x_t
x_n

图6

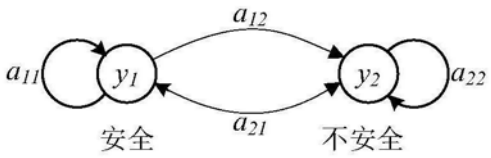
a_{12}
a_{11}
y_1
y_2
a_{22}
a_{21}
安全
不安全

图7

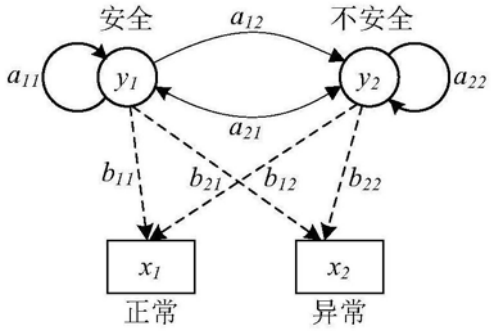
安全
a_{12}
不安全
a_{11}
y_1
y_2
a_{22}
a_{21}
b_{11}
b_{21}
b_{12}
b_{22}
x_1
x_2
正常
异常

图8

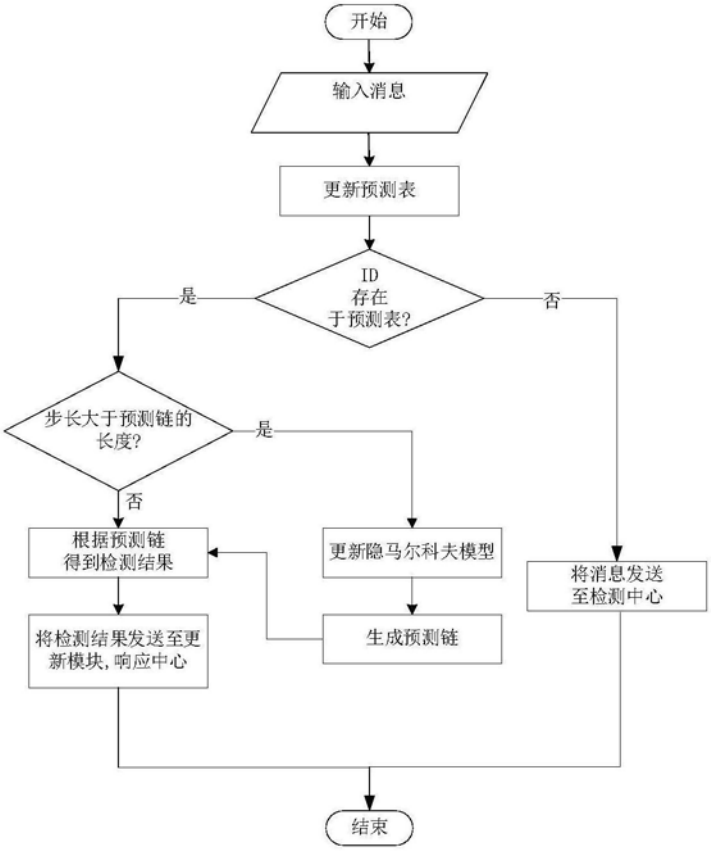
开始
输入消息
更新预测表
ID
存在
于预测表?
是
否
步长大于预测链的
长度?
是
否
根据预测链
得到检测结果
更新隐马尔科夫模型
将消息发送
至检测中心
将检测结果发送至更
新模块,响应中心
生成预测链
结束

图9

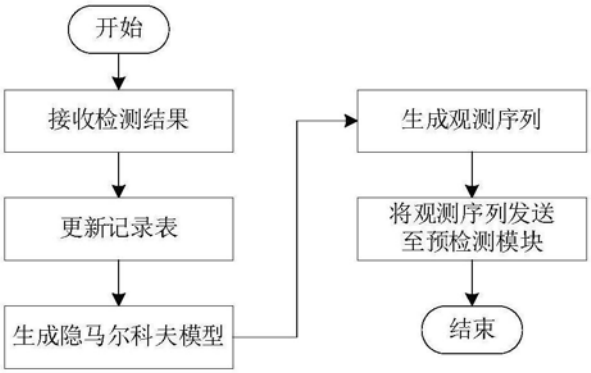
开始
接收检测结果
更新记录表
生成隐马尔科夫模型
生成观测序列
将观测序列发送至预检测模块
结束

图10

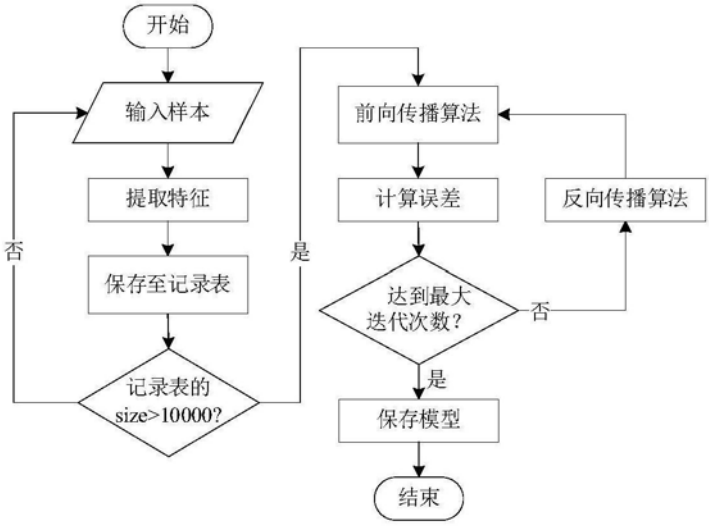
开始
输入样本
提取特征
保存至记录表
记录表的size>10000?
否
是
前向传播算法
计算误差
达到最大迭代次数?
否
是
反向传播算法
保存模型
结束

图11

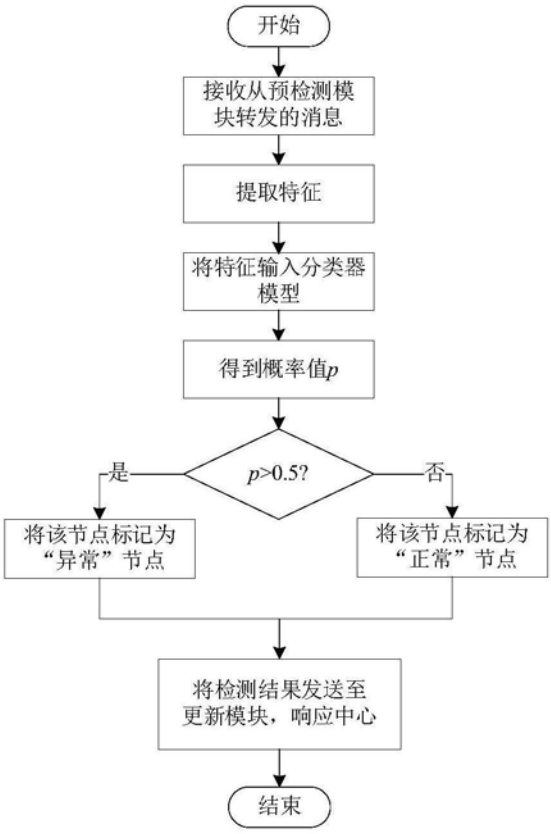
开始
接收从预检测模块转发的消息
提取特征
将特征输入分类器模型
得到概率值p
p>0.5?
是
否
将该节点标记为“异常”节点
将该节点标记为“正常”节点
将检测结果发送至更新模块，响应中心
结束

图12

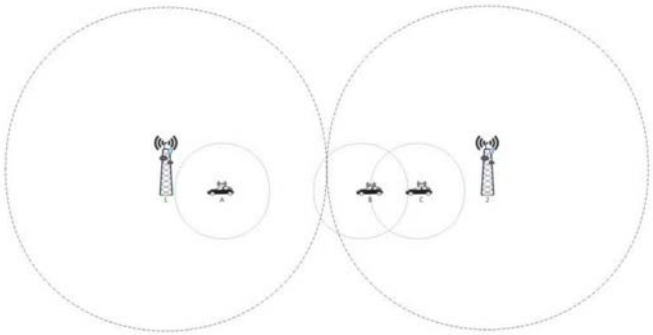

图13

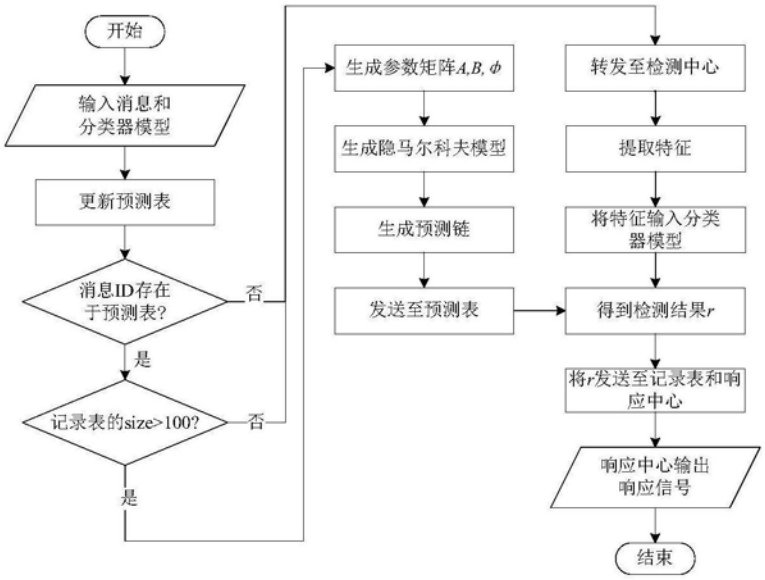
开始
输入消息和分类器模型
更新预测表
消息ID存在于预测表?
否
是
记录表的size>100?
否
是
生成参数矩阵A,B,ϕ
生成隐马尔科夫模型
生成预测链
发送至预测表
转发至检测中心
提取特征
将特征输入分类器模型
得到检测结果r
将r发送至记录表和响应中心
响应中心输出响应信号
结束

图14

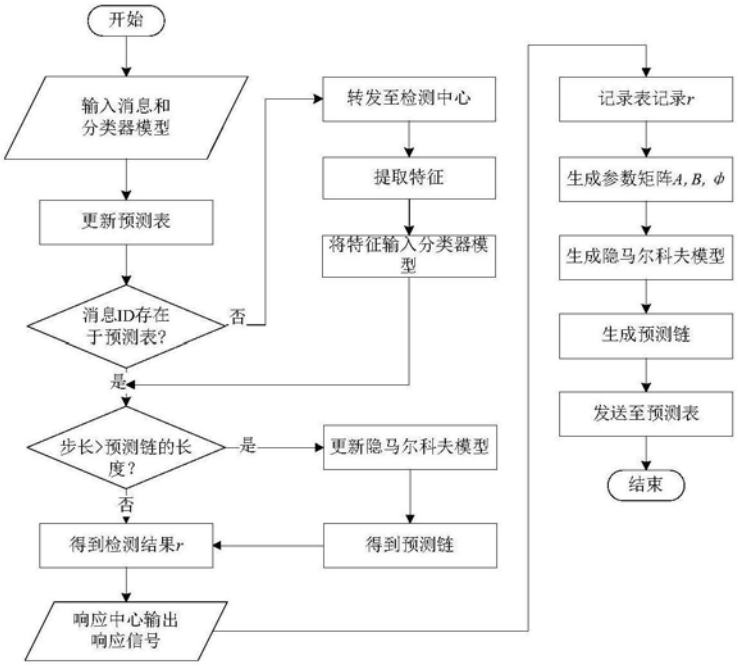
开始
输入消息和分类器模型
更新预测表
消息ID存在于预测表?
否
是
步长>预测链的长度?
是
否
得到检测结果r
响应中心输出响应信号
转发至检测中心
提取特征
将特征输入分类器模型
更新隐马尔科夫模型
得到预测链
记录表记录r
生成参数矩阵A,B,ϕ
生成隐马尔科夫模型
生成预测链
发送至预测表
结束

图15