研究与开发

基于动态权重分配的智能汽车网络安全评估模型

秘蓉新[1]，林志强[2]，齐佳豪[3]，姚文文[1]，左金鑫[4]，陆月明[4]
（1. 国家计算机网络应急技术处理协调中心，北京 100029；
2. 国家网信办数据与技术保障中心，北京 100080；
3. 中国电信股份有限公司江苏分公司，江苏 南京 210007；
4. 北京邮电大学网络空间安全学院，北京 100876）

摘　要：评估指标权重的确定是影响智能汽车网络安全性评估的重要因素之一。针对传统确权方法忽略指标属性状态变化对评估指标权重影响的问题，提出了一种基于动态权重分配的网络安全评估模型。该模型首先对车辆自组织网络（vehicular Ad Hoc network，VANET）进行安全目标分解与分析，构建其安全性评估指标体系。针对构建出的安全性评估指标体系，利用基于排序的确权算法对安全指标进行指标关联性分析，随后采用所提出的动态权重分配算法，计算指标体系中各个指标的动态权重，进而实现智能汽车VANET的安全性评估，得到安全等级评估结果。实验结果表明，该模型可以提升智能汽车VANET评估的合理性。

关键词：智能网联汽车；安全评估指标体系；动态权重分配；安全评估
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024239

Intelligent automotive network security evaluation model based on dynamic weight allocation

MI Rongxin [1], LIN Zhiqiang [2], QI Jiahao [3], YAO Wenwen [1], ZUO Jinxin [4], LU Yueming [4]
1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
2. Data and Technical Support Center of the Cyberspace Administration of China, Beijing 100080, China
3. Jingsu Branch of China Telecom Co., Ltd., Nanjing 210007, China
4. School of Cyberspace Security Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: The determination of the weight of evaluation indicators is one of the important factors affecting the security evaluation of intelligent vehicle networks. A network security evaluation model based on dynamic weight allocation was proposesd to address the problem of traditional property rights confirmation methods ignoring the impact of changes in indicator attribute states on the weight of evaluation indicators. The model first decomposed and analyzed the security objectives of the vehicle Ad Hoc network (VANET), and constructed its security evaluation index system. Based on the constructed security evaluation index system, the correlation analysis of security indicators was carried

收稿日期：2024−07−19；修回日期：2024−10−14
通信作者：林志强，linzhiqiang@cac.gov.cn；姚文文，yww@cert.org.cn

out using a sorting and confirmation algorithm. Then, the proposed dynamic weight allocation algorithm was used to calculate the dynamic weights of each indicator in the index system, thereby achieving the security evaluation of the intelligent vehicle VANET and obtaining the security level evaluation results. The experimental results indicate that the model can improve the rationality of intelligent vehicle VANET evaluation.

Key words: intelligent automotive vehicle, security assessment index system, dynamic weight allocation, security assessment

0 引言

确定指标权重的目的在于准确反映各指标在智能汽车网络安全评估中的重要性和对整体安全性的贡献，以便更全面、客观地衡量不同方面的影响，并为决策提供有针对性的信息。

目前现有的智能汽车网络安全评估模型，普遍采用静态均分权重，在评估前就给每个评估指标赋予了固定的权重。传统评估方法中权重的确定可以解决大多数场景中的评估问题，但是其存在一定的局限性，忽略了评估指标数据对最终评估结果的影响，导致对智能汽车网络安全评估的区分度不高，并且评估存在严重的滞后性，不能按时反馈智能汽车网络在各个阶段、环节、运行过程中存在的问题，导致在不同评估场景下的评估结果不够准确。智能汽车网络在整个系统运行期间随着各个因素的影响其状态发生了变化，对网络安全状态及相关因素进行实时动态权重调整，可以筛选出当前影响智能汽车网络安全最重要的因素，并将当前的评估结果反馈给管理者，一旦从评估中看出存在影响智能汽车网络安全的问题，就可以快速制订相关的安全措施，及时调整响应的部分，以确保智能汽车网络的安全。

在智能汽车网络安全方面，文献[1]对当前车辆网络易受攻击的原因进行了深入分析，总结了网络安全威胁的3种主要实现方法，对车辆网络安全研究与部署的必要性进行了全面探讨，从数据加密、消息认证和异常入侵检测3个方面介绍了车辆网络的安全增强技术。文献[2]聚焦于汽车关键部件中的汽车网关，对其网络安全威胁和风险进行了深入分析和评估，提出了一种风险分级方法，提高了风险分析的完整性和合理性。深度学习和机器学习技术也在智能汽车网络安全性评估中得到了广泛应用，文献[3]深入研究了10种具有先进代表性的基于深度学习的入侵检测方法，并详细说明了每种方法的特点和优势，并在此基础上，通过设立定量和公平的实验，进行了横向性能比较分析，为相关研究者提供了更全面、客观的评估依据。文献[4]开发了一种基于深度卷积神经网络（deep convolutional neural network，DCNN）的入侵检测系统（intrusion detection system，IDS），DCNN通过学习网络流量特征来识别恶意流量。此外，有研究者通过对大规模实时数据进行训练和分析，致力于建立智能汽车系统的异常检测模型，以实时监测潜在的网络攻击和漏洞[5]。这种数据驱动的方法不仅能够识别已知威胁，还具备一定的自适应性，能够应对新型网络安全挑战[6-7]。

在智能汽车通信网络的安全性研究方面，特别是在车对车通信（vehicle to vehicle，V2V）和车对基础设施通信（vehicle to infrastructure，V2I）方面，国外学者倾向于采用先进的加密技术和身份验证机制，以防范恶意入侵和信息篡改[8-9]。文献[10]通过汇总与黑客攻击车载网络相关的个体风险，采用基于风险的模型来进行面向漏洞的定性风险评估，利用影响可能性矩阵，借助基于风险的方法来确定黑客攻击车载网络的后果。文献[11]建立了车辆网络安全漏洞数据库，提供数据支撑，利用源代码分析、固件逆向、参透测试、仿真等检测技术，对车载终端、数据通信、

云平台、App 等进行网络安全评估。文献[12]基于传统的 IT 安全管理指南（guidelines for the management of IT security，GMITS）（ISO 13335）提出了一个针对车辆自组织网络（vehicular Ad Hoc network，VANET）的安全风险评估框架，该框架利用攻击树分析来评估威胁和漏洞。文献[13]针对现有的安全风险监控措施缺乏与攻击行为的联动等问题，提出了一种基于攻击链的智能网联汽车安全评估框架，该框架重点关注攻击产生的机制和步骤，有针对性地评估当前的风险级别和危害程度，并根据危害程度制订相应的安全管理措施。此外，一些研究者在硬件层面提出了创新性的解决方案，如可信计算、硬件安全模块等。这些技术旨在防范物理层面的攻击，并提高整个汽车系统的抗攻击能力。

在面向智能汽车的网络安全评估方面，文献[14]针对智能汽车漏洞评估不合理的问题，综合考虑智能汽车的特点，基于通用的漏洞评分系统漏洞评分原理，提出了面向智能汽车的信息安全漏洞评分模型。文献[15]针对现有的信任评估方案不适用于智能汽车环境的问题，引入社交网络的概念，提出了一种分布式的信任评估方案。文献[16]提出了一种基于信息熵的车载 CAN 总线网络报文异常检测方法，可有效应对车载 CAN 总线网络的攻击。文献[17]利用粗糙集和关联规则技术，改进传统的 Apriori 算法并应用到车载网络入侵检测方面，实现了对车载网络的安全监控。整体而言，一方面，目前针对智能汽车网络安全评估的需求日益迫切，另一方面，相关模型研究较少，细分领域较为分散，缺少统一标准和足够适配并具有针对性的评估模型。

1　基于动态权重分配的网络安全性评估模型

本文提出的基于动态权重分配的网络安全评估模型框架如图 1 所示，该模型主要包括两层共 3 个部分，前置层包括安全目标分解与分析，评估层包括安全性评估指标体系构建、基于状态变权理论的动态权重分配算法。

具体而言，评估模型首先针对待评估对象的典型特点和评估需求，在国家标准的指导下进行安全目标的确定，然后根据其面临的网络安全风险进行分析，进而构建待评估对象的安全性指标

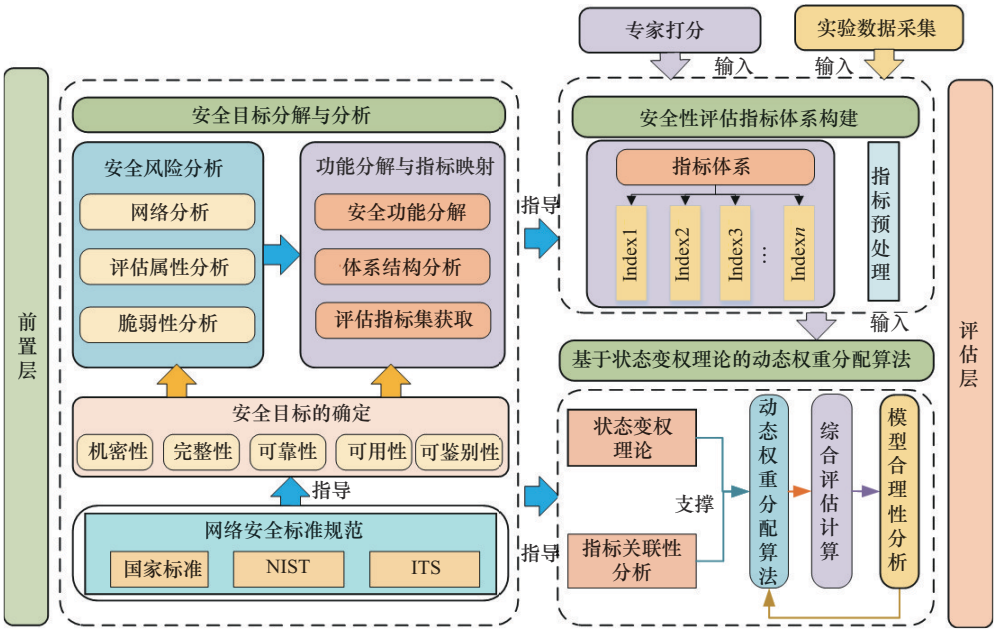


图 1　基于动态权重分配的网络安全评估模型框架

体系。为了计算指标权重时考虑指标关联性的影响，采用基于排序的确权算法计算常权重，随后利用动态权重分配算法计算得到动态权重，再经过综合评估计算，得到待评估对象的安全等级。

1.1 VANET安全性评估指标体系的构建

VANET是由一系列车辆节点以自组织形式组成的网络，旨在通过车辆之间的无线通信和协同工作来提高交通系统的效率和安全性。在VANET安全性评估体系构建过程中，需要考虑其面临的一系列独特之处。首先，由于VANET是动态自组织网络，车辆的位置和连接状态不断变化，因此，安全性评估指标需要考虑这种动态性，确保安全机制能够适应车辆的频繁加入和离开。其次，由于VANET涉及大量车辆和广泛的通信范围，需要考虑大规模、分布式的特点，以确保整个网络范围内的安全性。最后，在多层次的考虑下，综合了物理层、网络层、传输层和应用层的安全指标，以提供全方位的安全性评估。

1.1.1 评估指标体系的建立

目前，我国国家标准GB/T 40861—2021《信息安全技术 汽车信息安全通用技术要求》提供了VANET信息安全技术要求和测试方法的参考框架。美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）提出的网络安全框架2.0版本，为VANET系统的安全性提供了指导。此外，与智能交通系统（intelligent transportation system，ITS）相关的标准在车辆与基础设施、车辆间通信的安全性能等方面也提供了参考。在以上标准的指导下，本文进行多级评估指标体系的构建，分为目标层、因素层、指标层。目标层定义为“VANET安全”。因素层（也称为一级指标），对安全评估过程起到指引和支撑的作用。指标层（也称为二级指标），是可以直接进行评估的最小维度。在安全目标上，本文参考业界公认的信息安全CIA属性，结合VANET的客观现实特点，分解为5个方面，分别是机密性、完整性、可靠性、可用性、可鉴别性。通过这一系列的考虑和细致设计，VANET安全性评估指标体系如图2所示。其中，因素层（一级指标）为4个指标，分别是机密性、可用性、完整性、可靠性。每个因素层（一级指标）分别对应制定了指标层（二级指标）元素。指标层是可以直接进行评估的最小单元，通过获取对每个指标所处的安全状态的量化打分评估表，可以进一步汇聚得到一级指标的安全状态，最终得到对应VANET系统的整体安全状态。

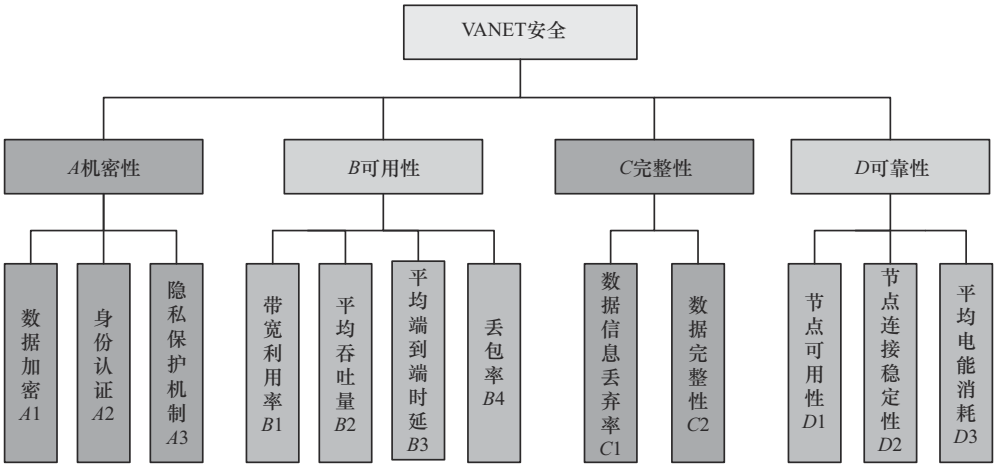


图2 VANET安全性评估指标体系

1.1.2　指标数据的标准化

（1）机密性

机密性给出了保护数据和信息的不被未授权实体访问、获取、泄露的相关指标，具体包括数据加密、身份认证和隐私保护机制。

- 数据加密：评估在VANET中传输的数据的加密程度和安全性，按照数据加密程度将其划分为弱加密级别、中等加密级别和强加密级别。
- 身份认证：评估VANET中节点身份认证机制的安全性，按照身份认证的安全性和可信度将其划分为低级、基础级、中级、高级、最高级。
- 隐私保护机制：评估隐私保护机制的实施和效果，包括匿名性保护、隐私数据脱敏和隐私保护协议的使用等方面，按照隐私保护机制的效果和安全性将其划分为低级、基础级、中级、高级、最高级。

（2）可用性

可用性给出了VANET中节点之间通信稳定性和持续性的相关指标，具体包括带宽利用率、平均吞吐量、平均端到端时延、丢包率。

- 带宽利用率：指已使用的带宽与总可用带宽之比，定义为：

$$\text{带宽利用率}=\frac{\text{实际传输的数据量}}{\text{最大带宽}}\times 100\% \quad (1)$$

- 平均吞吐量：指单位时间内单个节点的网络传输数据量的速率，定义为：

$$\text{平均吞吐量}=\frac{\text{数据包总数}}{\text{时间}\times\text{节点数}}\times 100\% \quad (2)$$

- 平均端到端时延：指数据包从发送到到达目的节点所经历的平均时延，定义为：

$$\text{平均端到端时延}=\frac{\sum\text{数据包时延}}{\text{数据包总数}}\times 100\% \quad (3)$$

- 丢包率：指丢失数据包的总数量与发送数据包的总数量之比，定义为：

$$\text{丢包率}=\frac{\text{丢失的数据包数量}}{\text{发送的数据包数量}}\times 100\% \quad (4)$$

（3）完整性

完整性给出了VANET中数据资源被窃取破坏程度的相关指标，包括数据信息丢弃率和数据完整性。

- 数据信息丢弃率：指数据资源在传输过程中被丢弃或删除的比例，按照数据被窃取的程度将其划分为低级、基础级、中级、高级、最高级。
- 数据完整性：指数据在传输过程中是否受到了篡改或破坏，按照数据完整性保护的程度将其划分为低级、基础级、中级、高级、最高级。

（4）可靠性

可靠性给出了度量网络在规定时间和规定条件下完成工作概率的相关指标，包括节点可用性、节点连接稳定性和平均电能消耗。

- 节点可用性：指目标网络中有效节点变化的个数占总个数的百分比，定义为：

$$\text{节点可用性}=\frac{\text{有效节点变化的个数}}{\text{有效节点的总个数}}\times 100\% \quad (5)$$

- 节点连接稳定性：评估节点之间连接的稳定性和持久性，按照节点连接稳定性程度将其划分为低级、基础级、中级、高级、最高级。
- 平均电能消耗：指单位时间单个节点的平均电能消耗，定义为：

$$\text{平均电能消耗}=\frac{\text{目标网络的总耗能}}{\text{攻击时间}\times\text{节点数}}\times 100\% \quad (6)$$

1.2　基于状态变权理论的动态权重分配算法

为了衡量各评估指标在安全评估中的重要性，需要对智能汽车VANET安全性指标体系中的各个指标进行赋权。安全评估指标的权重是表征各指标对评估结果影响重要程度的量化，只有

合理、准确地对各个安全指标赋权，才能保证评估结果的可信度。因此，本文在使用PageRank算法（基于排序的确权算法）计算指标常权的基础上，引入状态变权理论，提出基于激励与惩罚的变权设计，最终形成基于状态变权理论的动态权重分配算法。

1.2.1 状态变权理论

变权综合与常权综合的不同之处在于，变权综合不仅考虑了基本因素的相对重要性，而且考虑了目标值关于决策变量的水平组态。引入状态变权理论计算动态权重，本质上是在将常权重作为常权向量的基础上，结合安全评估指标的状态变权向量（即归一化后的指标数据），形成变权向量，得到动态权重，可以说，动态权重就是在常权重基础上，结合状态向量而得到的权重，从而达到动、静态结合的效果。李洪兴教授[18-19]基于因素空间理论分别给出了常权向量、变权向量和状态变权向量的公理化定义。

（1）常权向量定义

$$\begin{cases} \boldsymbol{W}=(w_1,w_2,\cdots,w_m) \\ \boldsymbol{w}_j\in[0,1](j=1,2,\cdots,m) \\ w_1+w_2+\cdots+w_m=1 \end{cases} \tag{7}$$

（2）变权向量定义

一组 m 维变权是指下述 m 个映射 $\boldsymbol{w}_j(j=1,2,\cdots,m)$：

$$\boldsymbol{w}_j:[0,1]^m\to[0,1],(x_1,\cdots,x_m)\mapsto\boldsymbol{w}_j(x_1,\cdots,x_m) \tag{8}$$

满足下面3条公理。

- 归一性：$\sum_{j=1}^{m}\boldsymbol{w}_j(x_1,\cdots,x_m)=1$。
- 连续性：$\boldsymbol{w}_j(x_1,\cdots,x_m)(j=1,2,\cdots,m)$ 关于每个变元 x_1 连续。
- 单调性：$\boldsymbol{w}_j(x_1,\cdots,x_m)(j=1,2,\cdots,m)$ 关于每个变元 x_j 单调递减或增大。

如果变权向量 $\boldsymbol{w}_j(x)$ 满足上述3条公理，就称向量 $\boldsymbol{w}_j(x)=(w_1(x),w_2(x),\cdots,w_m(x))$ 为一个 m 维变权向量。

（3）状态变权向量定义

给定映射：

$$\boldsymbol{S}_x:[0,1]^m\to[0,1],(x_1,x_2,\cdots,x_m)\mapsto \boldsymbol{S}_x(X)(x_1,x_2,\cdots,x_m) \tag{9}$$

$x_i\geqslant x_j\Rightarrow\boldsymbol{S}_i(X)\leqslant\boldsymbol{S}_j(X)$ 或 $\boldsymbol{S}_i(X)\geqslant\boldsymbol{S}_j(X)$；

$\boldsymbol{S}_j(X)(x_1,x_2,\cdots,x_m)$ 关于每个变元 x_j 连续；

$\boldsymbol{S}_j(X)(x_1,x_2,\cdots,x_m)$ 关于每个变元 x_j 严格单调递减或单调递增，对于任意的组合 $\sum_{k\neq i}w_kS_k(X)$ 关于 x_i 非减或非增。

当矢量 $\boldsymbol{S}_x$ 满足上述3个条件时，就称该矢量 $\boldsymbol{S}_x=(S_1(X),S_x(X),\cdots,S_m(X))$ 是一个 m 维局部状态的变权向量。

状态变权向量 $\boldsymbol{S}_x$ 与状态向量 $\boldsymbol{X}$ 计算Hardarmard乘积，并将结果执行归一化。采用式（10）方法对状态向量 $\boldsymbol{X}$ 进行加权：

$$\begin{aligned} &\boldsymbol{X}\mapsto\boldsymbol{S}_1(X)=\boldsymbol{S}_x\cdot\boldsymbol{X} \\ &=\big(S_1(X),S_2(X),\cdots,S_m(X)\big)\cdot(x_1,x_2,\cdots,x_m) \\ &=\big(S_1(X)\cdot x_1,S_2(X)\cdot x_2,\cdots,S_m(X)\cdot x_m\big) \end{aligned} \tag{10}$$

可得变权向量 $\boldsymbol{W}_j(X)$ 是常权向量 W 与状态变权向量 $\boldsymbol{S}_x$ 的归一化乘积，如下所示。

$$\begin{aligned} \boldsymbol{W}_j(X)&=\frac{\big(w_1S_1(X),w_2S_2(X),\cdots,w_mS_m(X)\big)}{\sum_{j=1}^{m}\big(w_jS_j(X)\big)} \\ &=\frac{\boldsymbol{W}\cdot\boldsymbol{S}_i(X)}{\sum_{j=1}^{m}\big(w_jS_j(X)\big)} \end{aligned} \tag{11}$$

文献[19]中论述了惩罚型变权、激励型变权、混合型变权的公理化定义。

1.2.2 基于激励与惩罚的变权设计

由上述的理论表达式定义可知，基于激励与惩罚机制的变权算法的实质是通过评估指标数值的波动从而明确影响指标权重的分配变化。变权思想强调，评估的目的在于掌握待评估系统的安全状态，是否对系统进行漏洞加固和安全组件的

升级，相关算法的调整取决于综合评估等级的优劣，还需要考虑评估结果由于受个别指标的影响而呈现出偏大或偏小的情况。因此，当评估指标数值存在极端情况时，指标的权重不仅要反映指标的相对重要程度，同时也要反映个别指标的影响。变权算法的核心思想在于对评估结果进行灵活的权衡，确保在综合考虑评估结果和个别指标的影响时，更有针对性地进行方案的选择。

对于惩罚型变权来说，当评估指标中的个别指标数值远小于其他指标值时，指标权重会随着指标数值的减少而增大，从而惩罚指标值过低的属性。因为指标体系中某项指标过小，可能会严重影响整个系统的安全状态，十分严重时可能会导致整个系统不可用，此时就需要对指标的权重进行重新分配调整，以适度地突出评估指标值较低的因素，进而引起相关人员对其重要性的高度关注。对于激励型变权来说，指标的权重会随着指标数值增大而增大，激励指标数值高的属性。

考虑VANET安全性评估中的实际情况，只有构建适当的状态变权向量，才能客观、真实地反映系统网络安全情况。由于VANET安全具有类似“木桶原理”的性质，系统中一个指标出现较低的分数时，可能会影响整个网络的安全性能，而一个指标的数值非常好时，对整个系统的安全性影响却不是十分明显，因此，构建的向量选择惩罚性大于激励性。此外，VANET安全状态还取决于常权比较大的指标。对于常权比较大的指标，惩罚与激励的幅度较大，对于常权较小的指标，惩罚与激励的幅度较小。综合考虑以上分析，本文决定采用下面的状态变权函数来评估VANET的安全性：

$$\boldsymbol{S}_j(X)=\begin{cases}1, & x_j\in[0,a]\\ \dfrac{\boldsymbol{w}_j}{b-a}(x_j-a), & x_j\in(a,b]\\ \boldsymbol{w}_j, & x_j\in(b,c]\\ d\cdot\left(1-\dfrac{\boldsymbol{w}_j(1-x_j)}{1-c}\right), & x_j\in(c,1]\end{cases}\tag{12}$$

其中，$a,b,c\in[0,1]$，a表示否定水平，b表示及格水平，c表示激励水平，$d\in(0,1)$表示激励调节水平，$\boldsymbol{w}_j$为常权权重。由式（12）确定的状态变权向量的函数曲线如图3所示。

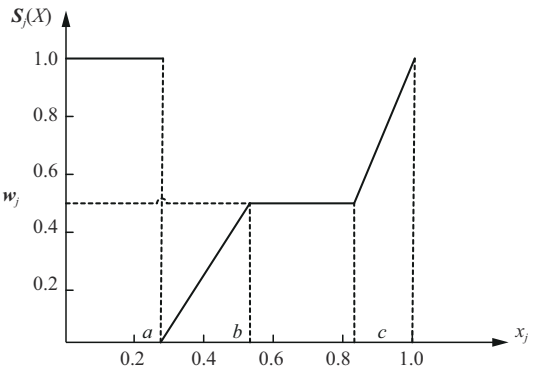


图3　状态变权向量的函数曲线

由图3可知，当$x_j\in[0,a]$时，惩罚幅度最大；当$x_j\in(a,b]$时，惩罚幅度随着x_j的变大而减小；当$x_j\in(b,c]$时，对该指标主观上既不惩罚，也不激励；当$x_j\in(c,1]$时，对该指标进行激励，且激励幅度随着x_j的变大而增大。

1.3　综合评估计算

将上述提及的n个指标的m组标准化后的样本数据x_{ij}，根据最终确定的指标$\{w_1,w_2,\cdots,w_n\}$，通过加权累加的方式，得到最后目标系统的量化得分$\text{Score}=\sum_{j=1}^{n}\boldsymbol{w}_j\times x_{ij},i\in(1,m)$。

将上述量化得分映射到对应的等级表中可得到相应的安全等级。评分与安全等级映射关系见表1。

表1　评分与安全等级映射关系

得分数值	安全等级
[0.85, 1)	优秀
[0.7, 0.85)	良好
[0.6, 0.7)	中等
[0.4, 0.6)	一般
[0, 0.4)	差

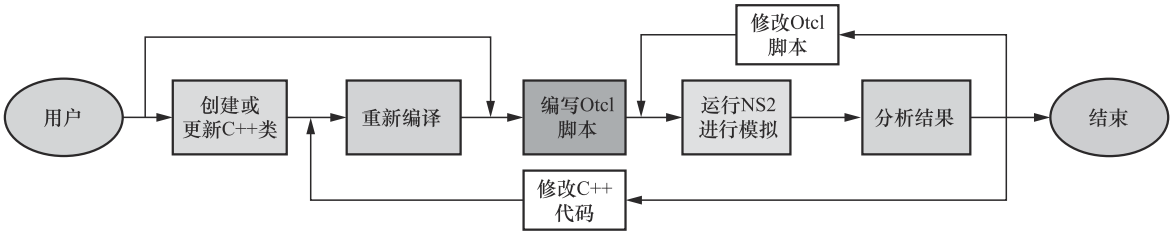


图4　VANET安全性评估流程

2　实验与结果分析

2.1　实验环境描述

本文通过NS2仿真实现VANET的安全状态评估。NS2是一款基于Linux系统的免费、开源的网络模拟器，经常被用于VANET的仿真研究。NS2以离散事件调度为核心功能，使用Otcl脚本语言配置节点和链路，具有灵活性和易用性。NS2通过C++语言定义和扩展网络协议。NS2充当了Otcl脚本语言解释器，可以通过可视化工具NAM观察节点移动和数据传输情况。基于NS2网络仿真工具实现VANET安全性评估流程如图4所示。NS2通过分离编译调试和场景布置工作，提高了网络模拟的效率。

本文搭建的实验环境仿真参数设置见表2。

表2　实验环境仿真参数设置

网络参数	数值
仿真区域大小	1 000 m×1 000 m
网络中的节点数	60
信道类型	Channel/Wireless
信道带宽	2 Mbit/s
最大运动速率	30 m/s
发射距离	250 m
数据分组大小	512 byte

2.2　实验评估结果

基于搭建的VANET实验场景，运用基于动态权重分配的网络安全评估模型对VANET进行网络安全评估，本文对3个同类评估对象*M*001、*M*002、*M*003进行评估。

（1）计算评估指标体系中各个指标的常权

本文中评估对象的指标常权是根据基于排序的确权算法计算得到的，具体的指标在指标体系构建部分已做了详细的介绍。实验根据10位专家的评分，构建算法所需要的专家评分表。由于指标体系中的指标较多，此处以一级指标可用性下的5个二级指标作为计算示例，分别计算带宽利用率（*B*1）、平均吞吐量（*B*2）、平均端到端时延（*B*3）、丢包率（*B*4）、规范化路由开销（*B*5）等指标的权重。专家对二级指标间的影响关系打分情况见表3。

表3　专家对二级指标间的影响关系打分情况

二级指标	*B*1	*B*2	*B*3	*B*4	*B*5
*B*1	0	6	6	2	2
*B*2	7	0	7	2	1
*B*3	8	6	0	7	3
*B*4	6	8	7	0	6
*B*5	6	8	5	5	0

根据表3的数据，构造的邻接矩阵$\boldsymbol{Q}$为：

$$\boldsymbol{Q}=\begin{bmatrix}0 & 6 & \cdots & 4\\ 7 & 0 & \cdots & 2\\ \vdots & \vdots & \ddots & \vdots\\ 3 & 4 & \cdots & 0\end{bmatrix}_{6\times 6}。$$

概率转移矩阵$\boldsymbol{H}$为：

$$\boldsymbol{H}=\begin{bmatrix}0 & 0.365\,5 & \cdots & 0.368\,1\\ 0.296\,1 & 0 & \cdots & 0.345\,1\\ \vdots & \vdots & \ddots & \vdots\\ 0.370\,2 & 0.414\,3 & \cdots & 0\end{bmatrix}_{6\times 6}。$$

最终的概率转移矩阵$\boldsymbol{G}$计算式如下。

$$\boldsymbol{G}=\alpha\cdot\boldsymbol{S}+\frac{1-\alpha}{N}\cdot\boldsymbol{U} \tag{13}$$

其中，$\boldsymbol{U}$是$n\times n$阶的全1矩阵，N代表指标节点

的数量。

根据最终的转移矩阵 $\boldsymbol{G}$，在重复迭代后计算权重向量 $\boldsymbol{P}_n$，最终 $\boldsymbol{P}_n$ 值构成每个二级指标的权重向量 $\boldsymbol{W}$。代入计算后，指标体系常权为 $\boldsymbol{W}^0$=[0.31, 0.28, 0.19, 0.22]，$\boldsymbol{W}_1^0$=[0.38, 0.33, 0.29]，$\boldsymbol{W}_2^0$=[0.27, 0.26, 0.29, 0.18]，$\boldsymbol{W}_3^0$=[0.49, 0.51]，$\boldsymbol{W}_4^0$=[0.35, 0.31, 0.34]。

（2）数据标准化

本文通过实验环境采集相关的指标数据，将采集到的数据进行标准化，一类是可以从程序中采集的定量指标，按照标准化表达式对其进行标准化处理，处理为[0, 1]的无量纲数值，另一类是定性指标，采取专家打分法确定。安全指标初始值见表4。

（3）确定惩罚和激励参数

考虑 VANET 的特点，状态变权激励和惩罚函数需要进行对应的调整。本文取否定水平 a=0.6，及格水平 b=0.7，激励水平 c=0.9，激励调节水平 d=0.8。这表明，当某个指标属性 $x_j \in [0, 0.6]$时，对其惩罚幅度最大；当 $x_j \in (0.6, 0.7]$时，惩罚幅度随着 x_j 的变大而减小；当 $x_j \in (0.7, 0.9]$时，对该指标不惩罚，也不激励；当 $x_j \in (0.9, 1]$时，对该指标进行激励，因为激励的区间较小，所以达到了降低激励力度的目的。

（4）计算各评估对象的权重和综合值

将计算出的常权和处理后的数据带入变权函数，计算评估指标的状态变权和变权值。*M*001、*M*002、*M*003 的评估计算分别见表5、表6和表7，变权评估法与常权评估法的计算结果比较见表8。

2.3　实验比较分析

在实验环境设置方面，本文针对 *M*001 对象进行了虫洞攻击，虫洞攻击会导致数据包经过虫洞时产生较大的时延，也会导致丢包率上升。由表5可知，*M*001 实验对象评估指标体系中的指标 *B*3 和 *B*4 状态值很低，这是因为实施攻击之后，网络受到了影响。在这种情况下，如果使用常权综合评估法计算出的综合评估值为0.73分，此时 *M*001 对象的网络安全评估等级为良好，意味着

表4　安全指标初始值

指标体系	*M*001	*M*002	*M*003
(*A*1, *A*2, *A*3)	(0.78.0.82.0.85)	(0.69,0.81,0.15)	(0.95,0.91,0.92)
(*B*1, *B*2, *B*3, *B*4)	(0.81,0.85,0.16,0.18)	(0.82,0.80,0.75,0.78)	(0.82,0.80,0.75,0.78)
(*C*1, *C*2)	(0.80,0.85)	(0.75,0.13)	(0.75,0.72)
(*D*1, *D*2, *D*3)	(0.90,0.75,0.80)	(0.88,0.73,0.85)	(0.88,0.73,0.85)

表5　*M*001 的评估计算

评估项	一级指标											
	A(0.31)			*B*(0.28)				*C*(0.19)		*D*(0.22)		
二级指标	*A*1	*A*2	*A*3	*B*1	*B*2	*B*3	*B*4	*C*1	*C*2	*D*1	*D*2	*D*3
二级指标权重	0.38	0.33	0.29	0.27	0.26	0.29	0.18	0.49	0.51	0.35	0.31	0.34
二级指标状态值	0.78	0.82	0.85	0.81	0.85	0.16	0.15	0.80	0.85	0.90	0.75	0.80
一级指标状态值		0.81			0.51			0.83			0.82	
常权综合值					0.73							
$\boldsymbol{S}_j(X)$状态变权		0.31			1.00			0.19			0.22	
$\boldsymbol{W}_j(X)$变权		0.21			0.61			0.08			0.10	
一级指标状态值		0.81			0.31			0.83			0.82	
变权综合值					0.508 1							

表6 *M*002的评估计算

评估项	一级指标											
	A(0.31)			*B*(0.28)				*C*(0.19)		*D*(0.22)		
二级指标	*A*1	*A*2	*A*3	*B*1	*B*2	*B*3	*B*4	*C*1	*C*2	*D*1	*D*2	*D*3
二级指标权重	0.38	0.33	0.29	0.27	0.26	0.29	0.18	0.49	0.51	0.35	0.31	0.34
二级指标状态值	0.69	0.81	0.15	0.82	0.80	0.75	0.78	0.75	0.13	0.88	0.73	0.85
一级指标状态值	0.57			0.79				0.43		0.82		
常权综合值	0.66											
$S_j(X)$状态变权	0.31			0.08				0.19		0.05		
$W_j(X)$变权	0.49			0.13				0.30		0.08		
一级指标状态值	0.42			0.79				0.33		0.83		
变权综合值	0.47											

表7 *M*003的评估计算

评分项	一级指标											
	A(0.31)			*B*(0.28)				*C*(0.19)		*D*(0.22)		
二级指标	*A*1	*A*2	*A*3	*B*1	*B*2	*B*3	*B*4	*C*1	*C*2	*D*1	*D*2	*D*3
二级指标权重	0.38	0.33	0.29	0.27	0.26	0.29	0.18	0.49	0.51	0.35	0.31	0.34
二级指标状态值	0.95	0.91	0.92	0.82	0.80	0.75	0.78	0.75	0.72	0.88	0.73	0.85
一级指标状态值	0.93			0.79				0.73		0.82		
常权综合值	0.83											
$S_j(X)$状态变权	0.37			0.28				0.19		0.22		
$W_j(X)$变权	0.58			0.20				0.09		0.13		
一级指标状态值	0.93			0.79				0.73		0.83		
变权综合值	0.87											

表8 变权评估法与常权评估法的计算结果比较

比较项	*M*001	*M*002	*M*003
指标常权	（0.31,0.28,0.19,0.22）	(0.31,0.28.0.19,0.22)	(0.31,0.28.0.19,0.22)
指标常权状态值	(0.81.0.51.0.83)	(0.57,0.79,0.43,0.82)	(0.93,0.79,0.74,0.82)
常权综合值	0.73	0.66	0.83
常权评估等级	良好	中等	良好
指标变权	(0.21,0.61,0.08,0.10)	(0.49,0.13,0.30,0.08)	(0.58,0.20,0.09,0.13)
指标变权状态值	(0.81,0.31,0.83,0.82)	(0.42,0.79,0.33,0.83)	(0.93,0.79,0.73,0.83)
变权综合值	0.51	0.47	0.87
变权评估等级	一般	差	优秀

此时系统处于正常的工作状态。但是从实验对象*M*001实际网络状态进行考虑，此时网络的可用性已经发生了显著的变化。使用常权综合评估法评估出的安全等级与网络真实状况出现了不一致，其原因是常权评估法中的权重不受指标取值的影响，指标状态不会影响权重的计算。因此，当评估指标体系中出现非常差的指标时，运用传统的常权评估方法计算出的安全状态等级是不合理的。但是，使用

本模型提出的动态权重分配算法可以较好地解决该问题，使用该算法计算出的变权综合值为0.51，此时评估出的安全等级为一般，评估结果更能反映系统的实际情况，更具有参考价值。

针对*M*002对象，本文对其施加中间人攻击，并且修改其隐私保护机制，由表6可知，评估指标体系中指标*A*3隐私保护机制和指标*C*2数据完整性等状态很差时，运用常权综合评估法计算其综合评估值为0.66，对应的安全等级为中等，并且偏向于良好，使用新算法计算出的变权综合值为0.47，对应的安全等级为一般，且偏向于差。

针对*M*003对象，本文重点加强VANET的机密性指标，由表7可知，评估指标体系中指标*A*1数据加密、指标*A*2身份认证、指标*A*3隐私保护机制等状态较好时，运用常权综合评估法计算其综合评估值为0.83，对应的安全等级为良好，并且偏向于优秀，使用新算法计算出的变权综合值为0.87，对应的安全等级为优秀。经比较可知，由于*M*003对象机密性非常好，其他方面也基本良好，此时采用新算法计算的变权综合达到了对该系统激励的目的。

3　结束语

本文重点研究了基于动态权重分配的网络安全评估模型，在安全评估过程中，引入了状态变权算法，采用变权算法计算其安全值。首先，根据智能汽车VANET的特点，构建了智能汽车VANET的安全性评估指标体系。然后，设计了激励与惩罚的状态变权算法，提出了基于动态权重分配的网络安全评估模型，用以提高智能汽车网络安全评估的合理性。最后通过仿真实验进行了验证。

参考文献：

[1] GUAN T, HAN Y, KANG N, et al. An overview of vehicular cybersecurity for intelligent connected vehicles[J]. Sustainability, 2022, 14(9): 5211.

[2] ZHAO H, GUO J, WU Z, et al. Cyber security risk analysis and evaluation for intelligent vehicle gateway[C]// Proceedings of the International Conference on Smart Transportation and City Engineering 2021. SPIE, 2021, 12050: 662-670.

[3] WANG K, ZHANG A, SUN H, et al. Analysis of recent deep-learning-based intrusion detection methods for in-vehicle network[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(2): 1843-1854.

[4] KALKAN S C, SAHINGOZ O K. In-vehicle intrusion detection system on controller area network with machine learning models[C]//Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Piscataway: IEEE Press, 2020: 1-6.

[5] ALFARDUS A, RAWAT D B. Intrusion detection system for CAN bus in-vehicle network based on machine learning algorithms[C]//Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). Piscataway: IEEE Press, 2021: 944-949.

[6] LOKMAN S F, OTHMAN A T, ABU-BAKAR M H. Intrusion detection system for automotive controller Area Network (CAN) bus system: a review[J]. EURASIP Journal on Wireless Communications and Networking, 2019(1): 184.

[7] BANAFSHEHVARAGH S T, RAHMANI A M. Intrusion, anomaly, and attack detection in smart vehicles[J]. Microprocessors and Microsystems, 2023(96): 104726.

[8] MALIK R Q, ALSATTAR H A, RAMLI K N, et al. Mapping and deep analysis of vehicle-to-infrastructure communication systems: coherent taxonomy, datasets, evaluation and performance measurements, motivations, open challenges, recommendations, and methodological aspects[J]. IEEE Access, 2019 (7): 126753-126772.

[9] ALI AMEEN H, MAHAMAD A K, ZAIDAN B B, et al. A deep review and analysis of data exchange in vehicle-to-vehicle communications systems: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions[J]. IEEE Access, 2019(7): 158349-158378.

[10] KELARESTAGHI K B, FORUHANDEH M, HEASLIP K, et al. Intelligent transportation system security: impact-oriented risk assessment of in-vehicle networks[J]. IEEE Intelligent Transportation Systems Magazine, 2019, 13(2): 91-104.

[11] SHAO X, DONG C, DONG L. Research on detection and evaluation technology of cybersecurity in intelligent and connected vehicle[C]//Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM). Piscataway: IEEE Press, 2019: 413-416.

[12] KONG H K, HONG M K, KIM T S. Security risk assessment framework for smart car using the attack tree analysis[J]. Journal of Ambient Intelligence and Humanized Computing, 2018(9): 531-551.

[13] LI Q, ZUO J X, CAO R H, et al. A security evaluation framework for intelligent connected vehicles based on attack chains[J]. IEEE Network, 2023, 38(2): 148-155.

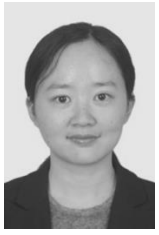
[14] 于海洋, 陈秀真, 马进, 等. 面向智能汽车的信息安全漏洞评分模型[J]. 网络与信息安全学报, 2022, 8(1): 167-179.
YU H Y, CHEN X Z, MA J, et al. Information security vulnerability scoring model for intelligent vehicles[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 167-179.
[15] 杨雪婷, 李重. 车联网中基于车辆行为预测的身份认证方案[J]. 计算机工程, 2021, 47(1): 129-138.
YANG X T, LI Z. Identity authentication scheme based on vehicle behavior prediction for IoV[J]. Computer Engineering, 2021, 47(1): 129-138.
[16] 于赫. 网联汽车信息安全问题及CAN总线异常检测技术研究[D]. 长春: 吉林大学, 2016.
YU H. Research on information security of networked automobile and CAN bus anomaly detection technology[D]. Changchun: Jilin University, 2016.
[17] 李飞, 王超. 基于关联规则挖掘的车载网络入侵检测技术研究[J]. 数据挖掘, 2017, 7(3): 65-69.
LI F, WANG C. Research on intrusion detection technology based on association rules mining in vehicular networks[J]. Hans Journal of Data Mining, 2017, 7(3): 65-69.
[18] 李洪兴. 因素空间理论与知识表示的数学框架(VIII): 变权综合原理[J]. 模糊系统与数学, 1995, 9(3): 1-9.
LI H X. Factor spaces and mathematical frame of knowledge representation(VIII) —— Variable weights analysis[J]. Fuzzy Systems and Mathematics, 1995, 9(3): 1-9.
[19] 李洪兴. 因素空间理论与知识表示的数学框架(IX): 均衡函数的构造与Weber-Fechner特性[J]. 模糊系统与数学, 1996, 10(3): 12-17, 19.
LI H X. Factor space theory and mathematical framework of knowledge representation (IX) —— construction of equilibrium function and Weber—Fechner characteristics[J]. Fuzzy Systems and Mathematics, 1996, 10(3): 12-17, 19.

[作者简介]

秘蓉新（1984– ），女，国家计算机网络应急技术处理协调中心副研究员，主要研究方向为人工智能多模态识别、网络安全、信息安全。

林志强（1984– ），男，现就职于国家网信办数据与技术保障中心，主要研究方向为网络数据安全、个人信息保护。

齐佳豪（1999– ），男，现就职于中国电信股份有限公司江苏分公司，主要研究方向为信息安全认证评估、网络安全态势感知。



姚文文（1984– ），女，国家计算机网络应急技术处理协调中心助理研究员，主要研究方向为网络信息安全战略、信息科技发展态势。

左金鑫（1992– ），女，北京邮电大学网络空间安全学院在站博士后，主要研究方向为车联网安全、网络安全风险评估。

陆月明（1969– ），男，博士，北京邮电大学网络空间安全学院教授，主要研究方向为车联网安全、网络安全风险评估。