基于CRITIC法和熵值法的智能网联汽车信息安全综合评价方法研究

路鹏飞，邹博松，李京泰
（中国软件评测中心智能网联汽车测评工程技术中心，北京 100048）

摘 要：随着网联化逐渐成为当今汽车技术发展的主流趋势之一，车载端信息安全问题也随之日益紧迫。作为加固信息安全风险点、制定安全技术要求的必要条件之一，研究科学合理的车载端信息安全评价方法，对于提升车载端信息安全水平具有重要意义。文章基于熵值法、基于指标相关性的指标权重确定方法（Criteria Importance Through Intercriteria Correlation，CRITIC）和前期工作成果，介绍了一种新型的综合主、客观权重信息的定量评价方法，并基于对车载端信息安全风险点的梳理，给出了智能网联汽车信息安全评价权重具体计算过程。通过对熵值法和CRITIC法的组合运用，全面考虑了原始评价数据的离散型、冲突性以及变异性，使所得综合权重更加合理。

关键词：智能网联汽车；熵值法；CRITIC赋值法；定量评价
中图分类号： O236.2 **文献标识码：** A

A methodology for cyber security quantitative assessment of intelligent connected vehicles based on CRITIC and entropy method

Lu Pengfei, Zou Bosong, Li Jingtai
(*China Software Testing Center, Intelligent Connected Vehicle Testing Technology Center, Beijing 100048*)

Abstract: The cybersecurity issue on the vehicle end is showing the significance, since the vehicles throughout the world become more and more connected over the network. In this context, a rational method for the quantitative evaluation of the vehicle cybersecurity is urgently needed to enable the customers to quickly obtain an accurate recognition of the chosen vehicle products.A quantitative method is proposed in this paper based on the intensive study on CRITIC and the entropy method. By combing the risky points existing parasitically on the network architecture of typical modern vehicles, the scope for the quantitative assessment is divided into four levels, namely the whole vehicle level, the system level, the components level and the security mechanism level. The computing process of the CRITIC and the entropy method is then carried out and elaborated minutely in this article.

Key words: intelligent connected vehicle; entropy method; CRITIC; quantitative evaluation

1 引言

在智能化、网联化趋势的推动下，汽车产品逐步融合信息技术，通过广泛的信息交互和数据共享实现复杂通信场景下的V2X功能，主流汽车厂商纷纷推出网联汽车相关的典型应用产品，抢夺市场发展先机，并提升了用户的使用体验。与此同时，高度网联化的汽车产品也暴

露出更多的信息安全隐患，成为不法分子实施恶意攻击、数据篡改、非法访问控制，危害车辆安全的风险点。

根据调查研究，2010年至今，由CVE（Common Vulnerabilities & Exposures）公共漏洞和暴露数据库收录的与汽车产品相关的信息安全漏洞超过70例。漏洞涉及T-BOX、车载WiFi、车载蓝牙、IVI、钥匙、OBD、网关、V2X等多种汽车设备，攻击形式包括远程和本地攻击，可造成的攻击结果包括信息泄露、数据内容篡改、拒绝服务、恶意代码执行、系统冻结、身份凭证窃取、脚本注入、远程控制等，严重影响车内和车际信息安全。2019年，中国汽车信息安全共享分析中心（C-Auto-ISAC）在天津发布汽车信息安全十大风险，包括不安全的云端接口、未经授权的访问、系统存在的后门、不安全的车载通讯、车载网络未做安全隔离、系统固件可被提取及逆向、不安全的第三方组件、敏感信息泄漏、不安全的加密和不安全的配置。

随着车载信息系统日益复杂，安全漏洞的分布将更加繁杂，潜在的攻击路径交错，安全风险威胁程度各异，给信息安全测试和安全加固工作带来沉重负担。为此，需要全面梳理整车信息交互系统架构，并为之制定科学的评价体系，从而为汽车信息安全保障工作提供逻辑支持。近年来，研究人员也开始关注汽车信息安全，其中2011年Stephen Checkoway等人对汽车外部攻击入口进行了梳理，并对多种远程攻击方式进行了描述[1]；Jonathan Peti等人在2015年首次对网联汽车面临的潜在安全攻击路径进行了较为全面的梳理[2]；2016年，甘杰夫和张洁对网联汽车的安全风险和潜在的传播路径进行了梳理，并提出了一种风险评估方法[3]；2017年，桂丽分析了网联汽车的常用攻击目标和攻击技术，并提出了汽车信息安全防护的关键技术[4]。随着汽车技术的快速发展，车载端信息系统架构更加复杂，攻击手段更加多样。需要基于研究人员的前期成果，对汽车网联汽车的车载端系统进行全面梳理，呈现出清晰的系统架构，为整车信息安全风险评估建立基础。

构建信息安全评价系统的另一项重要内容是制定科学、客观、可量化的评价方法，从而直观体现评价结果，为信息安全技术开发人员提供准确参考。目前，主流的定量评价方法分为主观赋值和客观赋值两种。其中，主观赋值包括模糊综合评价法、层次分析法、主观加权等方法。主观赋值简单易行，充分利用了相关人员的技术背景与经验，但也会因个人主观因素的影响而使赋值结果产生相当程度的偏差。客观分析法包括主成分分析法、熵值法、BP神经网络法、CRITIC法等[5~8]。客观分析法可以有效地避免因主观因素带来的误差，保障评价系统的严谨性，但客观赋值法通常要求评价对象具备一定的样本数量，从而通过数学计算对已有数据进行筛选，进而确定权重。同时，各种客观赋值方法中所关注的因素也不相同，如主成分分析法关注变量间的相关性。熵值法则侧重指标的变异性，各种方法均存在利弊，通过结合不同赋值方法可以得到更加合理的赋值结果。例如，CRITIC算法由于考虑了指标内的相关性和指标间的冲突性，而被认为是相对完善的客观赋权方法，但是由于其没有考虑数据之间的离散性，可以通过与熵权法结合进行改良[9]。

2 方法论

2.1整车网络安全体系

本文提出的智能网联汽车网络安全评价方法，是建立在智能网联汽车整车网络安全研究的基础之上。基于对智能网联汽车整车系统架构和运行环境的分析，将整车网络安全分为车内/车外系统安全和车内/车外网络安全四个方面，每个方面的安全

有相应的关键零部件安全支撑，而各模块的安全又有硬件安全、通信安全、数据安全、访问控制等安全机制予以保障，从而形成清晰的整车网络安全体系。如图1所示，整个体系从整车到系统到关键零部件到安全机制，由上而下分为整车、系统、零部件、安全机制四个层次，

2.2 重要性指数判定

针对图1所示的评价体系，对本文的评价方法

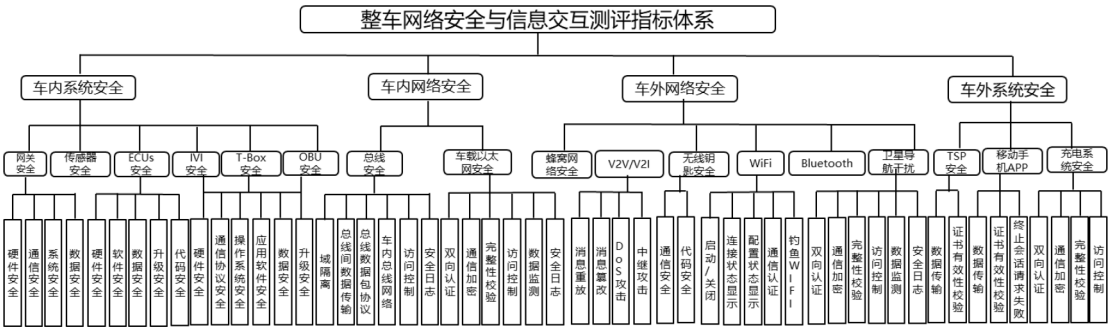

图1 智能网联汽车网络安全（分层）评价体系

有四个主要步骤构成，即重要性指数判定、层次分析法主观权重计算、熵值法与CRITIC法客观权重计算、综合权重计算。

其中，重要性指数判定是从攻击和防御两个方面入手，以攻击/防御成本和攻击/防御收益四个基本要素为出发点，对汽车通信系统第四层中的各个安全机制进行分析。攻击成本考虑了“攻击路径（远程攻击/本地攻击）”“攻击复杂度（是否需要专业人员或专用工具等）”“认证（是否需要获取认证）”三方面的因素；攻击收益由“资产重要度”和“固有致命度”决定，“资产重要度”包括主机类型和操作系统类型两项评价指标；“固有致命度”可依据漏洞编号，在CVSS官网中查询分值。通常在理想状况下，信息安全攻击收益等于防御收益。防御成本则由“漏洞补丁修复等级”“漏洞渗透代码可利用性”“漏洞报告可信度”“漏洞攻击复杂度”“漏洞破坏性（由机密性、完整性、可用性三方面衡量）”“主机类型”六个方面因素组成。依据上述评价指标对各评价对象重要性进行打分的取值区间和最终重要性指数的计算方法可参照参考文献[7]。

重要性指数的作用在于两个方面。第一，邀请多组行业专家参考国际通用的方法确定各安全机制的重要性指数，为开展客观权重计算提供了数据基础，使得依赖于原始数据的客观评价得以开展。第二，通过将已确定的重要性指数进行两两比较可以方便的得到开展主观评价（层次分析法）所需的重要性判断矩阵，且能够确定判断矩阵满足一致性要求，无需再通过计算判断矩阵的最大特征根和一致性指标进行验证，进一步提升了操作的便利性。

2.3 客观权重计算方法

获取各安全机制的重要性指数后，可参照参考文献中[7]中所描述的AHP层次分析法计算出评测体系中各层的评价对象针对上层相关要素的主观权重。

主观权重确定之后，为了降低层次分析法计算结果的主观随意性，使评价结果更加合理，本文使用熵值法和CRITIC赋值法结合的方式对评价对象进行客观赋权，并将客观赋权的结果与主观赋权结果相结合，从而在参考评价技术人员个人技术经验的同时运用数学方法兼顾评价结果的客观性。

针对客观赋权法的研究是本文的重点。传统的客观赋权方法包括主成分分析法、熵值法、BP神经网络法和CRITIC法等。其中，主成分分析法需要被评价的指标间存在一定的相关关系才能继续下去；而BP神经网络法则需要先验结果；熵值法则侧重某项指标的变异性，但忽视了指标本身的重要程度。相比之下，CRITIC算法考虑了各指标自身的对比强度及指标间的冲突性，能够较全面的衡量各指标重要性，因而被作为一种相对完善赋权算法，被广泛使用。

从对熵值法和CRITIC法的原理进行对比可以发现，二者之间存在完美的互补性，如果将二者结合，则可以在客观赋权过程中既充分考虑各指标数据已有的特性，也可以兼顾数据的变异性。具体而言，CRITIC法是对已有数据本身性质进行分析，考虑了指标内数据的离散性和指标间数据的冲突性，但这种分析是建立在对已有数据充分信任的基础上。换言之，认为现有原始数据是对各评价指标的最合理判定，其他可能出现的判定结果不应被采纳。而这种假设条件显然是与事实

不符的。因为在本文中，智能网联汽车安全机制的原始判定数据来自于主观赋权，由不同专家对于评价指标的原始判定往往是基于不同的专业背景、专业认知和经验积累等因素，因而主观判定结果不能穷举，且任何判定结果都是存在一定可信度的。即任何单纯基于CRITIC法的客观赋权结果，都仅能体现一组特定专家团队的专业认知，专家团队的规模越大，则原始数据所覆盖的情况越丰富，赋权结果理论上越接近于真值，但庞大的专家团队往往是不现实的。而熵值法则考虑了某个指标（安全机制）各原始判定数据发生的概率，即某一数据出现的概率越低，则其发生时所能给出的信息量越大。同时，熵值法也考虑了某个指标所有信息量的期望值，从而衡量了某个指标自身的复杂程度或变异能力，如果指标越复杂，出现不同情况的种类越多，那么它的信息熵是比较大的，反则反之。因而可以认为熵值法从概率的角度考虑了各个评价指标发展变化的可能性，并将其作为客观赋值算法的变量之一，从而对基于确定原始数据的CRITIC算法形成了完美补充。

在基于熵值法和CRITIC法计算出各专家的权重后，将依据各专家判定数据计算出的AHP层次分析法权重与相应的专家权重相乘后求和，即得出各安全机制的主客观综合权重。同理，可得出零部件层和系统层相对于上一层的权重，逐层计算后，可依据对安全机制的信息安全评价，得出智能网联汽车整车的信息安全水平量化指标。

综上所述，智能网联汽车信息安全评价系统的工作流程如图2所示。

3 定量评价实施过程

3.1客观权重确定的熵值法

所有评价指标的重要性指数集合即为重要性指数矩阵M，其中m_{ij}表示第j位专家为第i项指标制定的重要性指数。

$$\mathrm{M}=\begin{bmatrix} m_{11} & m_{12} & m_{1\ldots} \\ m_{21} & m_{22} & m_{2\ldots} \\ m_{\ldots 1} & m_{\ldots 2} & m_{\ldots\ldots} \end{bmatrix}=\left[m_{ij}\right]_{m\times n}$$

首先对各指标的重要性数据进行归一化处理，消除各指标之间含义、度量方式及量级的差别。归一化公式为：

对于正向指标：

$$m_{ij}^{'}=\frac{m_{ij}-Minm_{ij}}{Maxm_{ij}-Minm_{ij}}$$

对于负向指标：

$$m_{ij}^{'}=\frac{Maxm_{ij}-Minm_{ij}}{Maxm_{ij}-Minm_{ij}}$$

其中，正向指标是指取值越大，重要性越高的指标；负向指标是指取值越大，重要性越低的指标。从而得到归一化矩阵为：

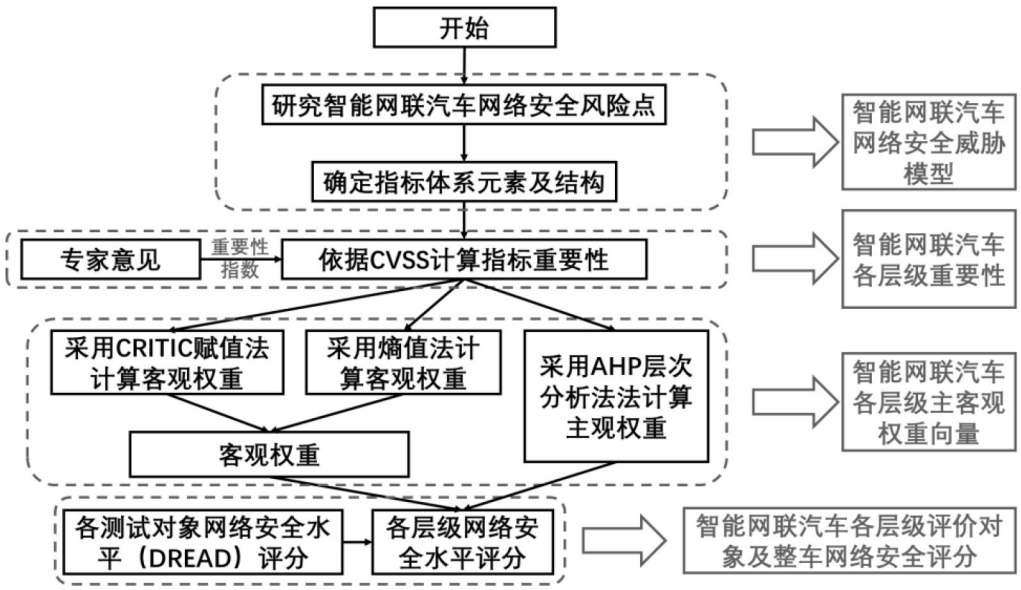

图2 智能网联汽车信息安全评价系统的工作流程

$$\begin{bmatrix} m'_{11} & m'_{12} & m'_{1\ldots} \\ m'_{21} & m'_{22} & m'_{2\ldots} \\ m'_{\ldots 1} & m'_{\ldots 2} & m'_{\ldots\ldots} \end{bmatrix}$$

基于归一化矩阵，计算第j位专家数据的熵值为：

$$E_j = -k\sum_{j=1}^{n} P_{ij}\, In(P_{ij})$$

（i=1、2、3…,m）

其中，$k = 1/In(n)$

n表示样本总数，在本文中为专家数据的组数；P_{ij}为m'_{ij}出现的概率。

根据信息论中对信息熵性质的描述，P_{ij}的值与m'_{ij}取值的大小无关，而是衡量m'_{ij}出现特定取值的概率[10]，因而不能用m'_{ij}的取值与第i项指标所有专家数据之和的比值计算。本文中，为了便于实施，将第i（i=1、2、3…m）项指标的取值范围$Maxm'_{ij} - Minm'_{ij}$平分为n等份，则P_{ij}等于与m'_{ij}处于同一取值区间的专家数据的个数与n的比值，并规定，当$P_{ij} = 0$时，$P_{ij}\, In(P_{ij}) = 0$。

基于第i项指标的熵值，可以计算出第i项指标的权重为：

$$w_j = \frac{1 - E_j}{\sum_{i=1}^{m}(1 - E_j)}$$

3.2 客观权重确定的CRITIC法

在CRITIC客观权重计算过程中，针对归一化矩阵：

$$M=[m'_{ij}]=\begin{bmatrix} m'_{11} & m'_{12} & m'_{1\ldots} \\ m'_{21} & m'_{22} & m'_{2\ldots} \\ m'_{\ldots 1} & m'_{\ldots 2} & m'_{\ldots\ldots} \end{bmatrix}$$

对矩阵M中的每一列分别进行标准差运算：

$$\delta_y = \sqrt{\frac{\left(\sum_{i=1}^{m}\left(m'_{ij} - \frac{\left(\sum_{i=1}^{m} m'_{ij}\right)}{m}\right)^2\right)}{m}}$$

（j=1,2⋯，n）

δ_y是第y组重要性指数的标准差，其代表了各个评价指标重要性指数取值差距的大小。

接下来计算第i组和第j组重要性指数数据之间的相关系数σ_{ij}：

$$\sigma_{ij} = \frac{\sum_{x=1}^{m}\left(\left(m'_{xi} - \frac{(\sum_{x=1}^{m} m'_{xi})}{n}\right)\left(m'_{xj} - \frac{(\sum_{x=1}^{m} m'_{xj})}{n}\right)\right)}{\sqrt{\sum_{x=1}^{m}\left(m'_{xi} - \frac{(\sum_{x=1}^{m} m'_{xi})}{n}\right)^2 \sum_{x=1}^{m}\left(m'_{xj} - \frac{(\sum_{x=1}^{m} m'_{xj})}{n}\right)^2}},$$

(i,j=1,2⋯,n)

则各权重向量所包含的信息量可由公式表示：

$$C_j = \delta_j \sum_{i=1}^{n}(1 - \sigma_{ij}),\ (\mathrm{i,j} = 1,2\ldots,\mathrm{n})$$

第j个权重向量K_j所对应的CRITIC权重为：

$$T_j = \frac{C_j}{\sum_{j=1}^{y} C_j}$$

各专家数据的客观权重为：$W_j = w_j \times T_j$，（j=1、2、3…,n）

将W_j进行归一化处理即可得到个专家数据的客观权重向量W_0。

参考文献[7]中所面熟的方法，将客观权重向量 与基于AHP层次分析法计算得出的主管权重向量结合，得出智能网联汽车网络安全水平综合权重架构。

4 结束语

本文提出的智能网联汽车网络安全水平综合权重计算方法，结合了AHP层次分析法、熵值法和CRITIC客观赋权法，综合考虑了原始数据的变异性、冲突性和离散度，并充分运用了专业技术人员的背景经验，能够在充分运用业内专家的专业经验的基础上，有效地规避了因人为赋值造成的主观随意性，从而为重要性赋权提供了可靠依据。

本文中介绍的评价方法尚未经过实际测试评价工作的检验。未来将在实地的智能网联汽车信息安全评价过程中对本方法进行实施和验证，及时发现问题并加以改进，使其成为可行、可靠、并具备较高公信力的评价方法。

基金项目：

国家自动驾驶电动汽车集成与示范项目（项

目编号：2018YFB0105204）。

参考文献

[1] Stephen Checkoway, Damon Mccoy, Brian Kantor, et al.Comprehensive Experimental Analyses of Automotive Attack Surfaces [A].Venue: USENIX SECURITY.

[2] Jonathan Petit, Steven E. Shladover. Potential Cyberattacks on Automated Vehicle [J].IEEE Trans on Intelligent Transportation Systems,2015,16 (2): 546-556.

[3] 甘杰夫,张洁.网联汽车系统信息安全及其风险评估方法[A].2016中国汽车工程学会年会论文集，2011.

[4] 桂丽.移动互联汽车信息安全风险研[J].Telecommunication Network Technology，NO.6，2017.

[5] 陈伟,夏建华.综合主、客观权重信息的最有组合赋权方法[J].数学的时间与认识，2007,37(1).

[6] 陈秀真,吴越,李建华.车载信息系统的安全测评体系及方法[J].信息安全学报, 2017,2(02):15-23.

[7] 路鹏飞,薛晓卿,丁文龙,朱科屹.智能网联汽车网络安全水平定量评价方法研究[J].中国科技纵横，2019(1).

[8] 黄加增.基于模糊数学的网络安全评价模型研究[J].网络空间安全,2020,11(4):1-.

[9] 刘志惠,黄志刚.P2P网络借贷平台风险识别及度量研究[J].合肥工业大学学报，2019,33(02).

[10] 李航.统计学习方法[A].北京：清华大学出版社，2012-3.

作者简介：

路鹏飞（1986-），男，汉族，河南商丘人，英国巴斯大学，博士，中国软件评测中心智能网联汽车测评工程技术中心，工程师；主要研究方向和关注领域：智能网联汽车信息安全、功能安全测试与评价技术。

邹博松（1986-），男，汉族，北京人，英国牛津布鲁克斯大学，硕士，中国软件评测中心智能网联汽车测评工程技术中心，工程师；主要研究方向和关注领域：智能交通、车联网、智能网联汽车、自动驾驶。

李京泰（1994-），男，汉族，四川营山人，香港科技大学，硕士，中国软件评测中心智能网联汽车测评工程技术中心，工程师；主要研究方向和关注领域：车载智能计算平台、信息安全，关注领域自动驾驶、智能网联汽车、汽车电子。