网络空间安全系列丛书

证据理论拓展及其在信息安全中的应用研究

◎ 叶 清　秦艳琳　王红霞　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列丛书

证据理论拓展及其在信息安全中的应用研究

叶　清　秦艳琳　王红霞　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书围绕证据理论自身问题和应用展开论述，首先介绍证据理论及应用的研究现状；然后介绍证据理论中识别框架、信任函数、似然函数等基础知识，并详细阐述证据理论在确定基本概率赋值、优化证据合成、近似快速工程应用、与其他理论融合应用、异常证据检测分析等方面的方法和技术；最后针对具体工程尤其是信息安全领域的问题，提出合理、可行的解决方案，并给出具体的案例分析。

本书研究内容兼有理论深度和工程实用性，内容叙述专业性较强，逻辑关系较紧密。本书适合高等院校信息安全、管理工程等专业高年级本科生和研究生作为教材使用，也可供从事信息安全与管理的科研技术人员参考阅读。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

证据理论拓展及其在信息安全中的应用研究 / 叶清，秦艳琳，王红霞编著. —北京：电子工业出版社，2019.5
ISBN 978-7-121-36462-4

I. ①证… II. ①叶… ②秦… ③王… III. ①证据－理论研究 ②信息安全－证据－研究 IV. ①D915.130.1 ②D912.17

中国版本图书馆 CIP 数据核字（2019）第 085483 号

责任编辑：章海涛
文字编辑：张　鑫
印　　刷：北京七彩京通数码快印有限公司
装　　订：北京七彩京通数码快印有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：12.25　　字数：298 千字
版　　次：2019 年 5 月第 1 版
印　　次：2019 年 5 月第 1 次印刷
定　　价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

前　言

随着 Internet 规模的迅速扩大，其复杂性和不确定性随之增加，由此带来的信息安全问题日益严重。一方面是由于互联网的应用范围越来越广泛，规模越来越庞大；另一方面是由于系统脆弱性的不断出现，简单易用的攻击工具越来越普及，使得网络安全事件层出不穷。信息安全中若干关键技术（如入侵检测、WSN 节点信任评估、网络系统方案优选等）已经成为目前信息安全领域的研究热点。

目前，基于不确定性推理的信息安全关键技术已成为该领域重点发展方向之一。作为其中的一种经典方法，DS 证据理论克服了用概率描述不确定性的不足，不需要精确了解概率分布，也不需要显式表示不确定性；通过建立命题和集合之间的对应关系，把命题的不确定性问题转化为集合的不确定性问题，给出信息的信任函数和似然函数。当先验概率很难获得时，DS 证据理论较概率论更为有效。运用 DS 证据理论的另一大优点是形式灵活多变，相关研究将 DS 证据理论和模糊逻辑、神经网络、专家系统相结合，进一步提高推理的准确性。然而 DS 证据理论自身存在若干不足，如客观确定基本概率赋值，证据合成规则需改进优化，证据理论工程近似实用算法难确定等，这些不足必然会直接影响其在信息安全领域中有效应用，进而导致合成结果不够合理，造成较高的错误率。因此，有必要对 DS 证据理论自身存在的若干关键问题进行深入研究，以更有效、更合理地指导其在信息安全领域某些关键问题中的应用。

本书凝结了作者承担的国家自然科学基金“云数据管理相关理论与技术研究”、博士后基金“大规模数据条件下基于 DS 证据理论的网络安全态势评估”、军队预研项目“攻防对抗环境中××系统安全评估技术研究”和“基于 DS 证据理论的融合目标识别研究”、湖北省自然科学基金“入侵检测中高维混合属性的 DS 证据理论处理研究”等科研项目中的部分研究成果。与此同时，本书还参阅了近年来国内外学者相关研究成果，通过系统深入分析 DS 证据理论自身的不足和应用中的难点问题，结合信息安全领域中数据特征与工程应用实际，研究证据基本概率赋值的确定方法、证据合成规则改进与优化、DS 证据理论的近似算法、DS 证据理论和层次分析法融合应用、区间型证据合成方法、异常证据检测分析等共性理论问题，并在此基础上开展 DS 证据理论在入侵检测、信任管理、可生存网络存储系统方案优选、信任路径选择等方面运用研究。本书研究可有效拓展 DS 证据理论内容，并可推广其在信息安全领域中的应用，具有良好的理论意义和应用价值。

全书共 9 章。第 1 章介绍了 DS 证据理论解释、应用领域、若干问题及本书的组织安排。第 2 章介绍了 DS 证据理论的基础知识，对识别框架、基本概率赋值、信任函数、众信度函数、似然函数、证据合成规则及决策规则等进行了系统阐述，同时对 DS 证据理论与其他信息融合方法进行了比较。第 3 章论述了常见基本概率赋值的确定方法，并根据入侵检测中的具体数据的特点和工程应用实践，在对采集数据进行行列压缩的基础上，提出基于 BP 神经网络的基本概率赋值确定模型，并分析了模型运行的效果。第 4 章在分析 DS

证据理论证据合成规则正常应用与失效的基础上，总结归纳了证据合成规则改进与优化方法，并提出了引入优先因子、权重因子的证据合成方法，然后分析了证据权重确定方法，继而给出了基于熵权和基于证据距离的证据合成方法。第 5 章介绍了通过 DS 证据理论进行证据合成时的计算复杂度问题，并分析了当前几种经典的近似算法的具体工作机制，详细阐述了基于基本概率赋值再分配策略的近似算法，并分析了证据冲突较小情况、冲突较大情况的近似算法的效果。第 6 章阐述了 DS 证据理论和层次分析法相结合应用于信息融合工程领域的可能，系统给出了方法运用过程中识别框架建立、证据选择、基本概率赋值计算、证据合成、决策规则等环节的方法，并对两者结合运用的性能进行了分析。第 7 章系统地阐述了区间型证据合成方法的理论基础和运用过程，主要包括广义求和与广义乘积、基于区间数的 DS 证据理论及区间数型证据的合成方法。第 8 章主要阐述了证据聚类与异常证据检测问题的解决方法，涉及聚类分析、证据聚类问题的描述等内容，并在相关理论的基础上，提出了基于证据距离的证据聚类方法、基于互/自冲突量分析的证据聚类方法、基于证据距离和冲突程度的异常证据检测算法、基于投影分解与 KNN 的异常证据检测算法等。第 9 章主要研究了 DS 证据理论在信息安全中的应用情况，分别阐述了基于 DS 证据理论和粗糙集理论的入侵检测方法、基于动态更新证据支持度的节点信任评估方法、不完全信息下可生存网络存储系统方案优选、分布式环境下信任路径选择性搜索及聚合等问题。

本书第 1 章、第 3～6 章由叶清编写，第 2 章由王红霞编写、第 8～9 章由秦艳琳编写，全书由叶清统稿。刘伟、陈渊、黄仁季等提供了部分的研究资料。武汉大学王先甲教授、东南大学李新德教授、杭州电子科技大学文成林教授、徐晓滨副教授、中北大学杨风暴教授、海军工程大学吴晓平教授、宋业新教授等审阅了书稿，并提出了宝贵的修改意见，在此一并表示衷心感谢！

本书在编写过程中参阅了近年来 DS 证据理论领域的一些最新研究成果，在此向相关文献的作者表示诚挚的谢意。

由于学术水平有限，本书难免存在不妥和错误之处，真诚希望各位专家、学者不吝赐教。

作　者

2018 年 8 月于武汉

试读结束，需要全本PDF请购买 www.ertongbook.com

目　录

第1章

绪　论

对不确定性的分析、建模和处理建立在概率论、模糊集理论、粗糙集理论、Dempster-Shafer 证据理论（以下简称 DS 证据理论）四大理论基础之上。概率论以其坚实的数学理论基础为随机不确定性的研究提供了强大的工具支持；模糊集理论为处理客观世界中“亦此亦彼”的模糊现象提供了技术手段；粗糙集理论可以有效地在不确定、不完备信息中发现并揭示隐含的知识和规律；DS 证据理论将概率区间化、一般化，以信任函数的形式处理不完全信息并提供统一的不确定性建模框架。众多学者指出，DS 证据理论与其他不确定性推理理论方法相比较来说，能更加有效地处理不完全、不精确信息，克服概率论对不可知性、信念表达、主观认知等不确知性建模上的不足，提供对各种不确定性的统一建模和有效的信息综合方法。因此，DS 证据理论为不确定性管理决策问题的建模与求解提供了一种可能的基础理论框架。DS 证据理论具有较大的优点，主要表现在以下 4 个方面[1]。

（1）具有较强的理论基础，既可处理随机性的不确定性，也可处理模糊性的不确定性。

（2）依靠证据的积累，可不断缩小假设集；而证据积累的过程需要一种方法来计算多个证据对假设的综合影响，即多个证据作用下假设成立的综合信任程度，这就是证据合成方法。

（3）可将“不知道”和“不确定”分开。

（4）不需要先验概率和条件概率密度。

DS 证据理论可视为对概率方法的一种改变。这种改变主要体现在以下 3 个方面。

（1）DS 证据理论对“不知道”的表示更明确、更合理。

（2）DS 证据理论具有综合不同信度函数的 Dempster 规则，而概率论框架不便处理不同概率函数的综合。

（3）DS 证据理论与概率论关于“信任”（Belief）的基本观点是不同的，DS 证据理论把信任视为主体（Agent）基于证据产生的认识；而概率论认为主体的信任是先验的，证据的作用仅仅是修改信任。DS 证据理论对概率方法的这些改变无疑有着广泛的应用价值。

在DS证据理论推理融合模型中，DS证据理论是其核心理论。根据该理论的定义，信息的不确定性包括3个方面：证据的不确定性、推理的不确定性及规则的不确定性。其中，证据是指信息源对某个判断的支持程度，证据的不确定性包括信息的歧义性、不完全性、不精确性、模糊性和随机性等；推理是从一个或多个已有的判断得出新判断的过程；规则是指多个证据进行合成时所采用的规则，推理和规则同样存在不确定性。DS证据理论首先针对每个信息源在证据、推理、规则3方面的确定性进行分析，通过建立问题的识别框架探讨证据的不确定性；通过基本概率赋值来处理推理的不确定性；然后通过一定的证据合成规则对各信息源的证据进行合成，得到综合的决策结果，使得信息互补集成，改善不确定环境中的决策过程，从而减少甚至解决模糊的、不确定的和矛盾的问题。当然，DS证据理论在处理不确定性问题方面的优势非常明显，但是DS证据理论在应用过程中同样存在一些问题，主要表现在：

（1）证据的基本概率赋值（Basic Probability Assignment，BPA）客观获取难，大多数文献中对基本概率赋值获取往往倾向于减轻讨论力度，或者主观给定；

（2）构造证据的数据来源实际情况考虑较少，易带来证据质量下降问题，进而影响证据合成结果；

（3）应用中往往以单值数值型证据为合成对象，而对证据描述形式的多样性缺少研究。

为了解决DS证据理论自身存在的问题，国内外众多学者进行了多方面的研究，并取得了丰硕的研究成果。但也有许多局限，进而影响了DS证据理论的广泛工程化应用，这主要还是由于DS证据理论自身存在的种种缺陷所致，因此笔者针对DS证据理论自身和实际应用中的问题与缺陷，在系统全面的分析研究基础上，对其开展模型建立、理论分析、数值算例和工程模拟计算等研究工作。其目的在于以下两点。

（1）丰富和完善DS证据理论。在综合分析DS证据理论的基础上可知，DS证据理论是信息融合领域中一个重要的理论，该理论有其他理论无法比拟的优势。DS证据理论发展到今天，已经取得了巨大的进步，并在很多领域得到了应用。但是由于理论自身缺陷的限制，其工程应用受到一定的影响。

（2）拓展DS证据理论的应用领域。深入分析现今DS证据理论的众多实用算法和证据支持性的内涵，将证据合成问题进行适当的优化处理，提出切实可行的快速实用的证据推理算法，以供实际工程中应用，进而提高证据合成的准确性、有效性和快速性。

1.1 DS证据理论解释

DS证据理论是一种证据推理的数值推理方法。证据推理通常表示依赖于证据进行推理的一类技术。DS证据理论最初是Dempster在1967年提出的，他用多值映射得出了概率的上下界，后来由其学生Shafer在1976年推广并且形成证据理论[3]，因此称为Dempster-Shafer证据理论。它是一种在不确定条件下进行推理的强有力的方法，可以看成概率论的推广。

DS证据理论已经过了50多年的发展，为此，许多国内外学者、专家付出了努力，取得了国际学术界认可的累累硕果。国外主要研究者除Dempster和Shafer外，长期关注DS证据理论自身与应用，并且其研究成果得到广泛认可的专家有：法国Rouen大学的Lefevre，

试读结束，需要全本PDF请购买 www.ertongbook.com

Compiegne 大学的 Thierry Denoeux，Paul Sabatier 大学的 Didier Dubois，英国 Cardiff 大学 Cardiff 商学院的 Malcolm Beynon，德国人工智能研究中心（DFKI）的 Mathias Bauer，捷克科学院的 Ivan Kramosil，比利时 Bruxelles 大学的 Philippe Smets，美国 Penn 州立大学的 Catherine Kuenz Murphy 博士。2008 年 Roland R Yager，Liping Liu 出版了 *Classic Works of the Dempster-Shafer Theory of Belief Functions*，收录了自 DS 证据理论诞生以来具有代表性的学术论文，总结了概念解释、理论基础和应用研究取得的成就并对其未来发展方向做了展望。

DS 证据理论因算法结构简单，融合精度高，能较好地处理不确定性信息，成为一种重要的推理融合方法。DS 证据理论解释可归纳为 4 种经典模型[2]：上下概率解释模型、广义化贝叶斯理论模型、随机集理论解释模型及可传递信任模型。

1. 上下概率解释模型

在上下概率（Upper and Lower Probability，ULP）解释模型中，信任函数（Belief Function）被认为是命题的概率下界，似然函数（Plausibility Function）则是命题的概率上界，Dempster 正是通过这个概念创立了 DS 证据理论。从信息融合的角度来说，ULP 解释模型适用于先验知识不满足概率可加性的数据进行融合的情况。

给定概率空间 (Θ,R,P)，P 为 (Θ,R) 上的概率测度。这里 R 为 Θ 的一些子集（不必是 Θ 的所有子集）而构成的集合。可以通过将 P 拓展到 2^{Θ} 上来定义 P_* 和 P^*：

$$P_*(A)=\sup\{P(x)\mid x\subseteq A\text{且}x\in R\}$$

$$P^*(A)=\inf\{P(x)\mid x\supseteq A\text{且}x\in R\}$$

一般地有 $P^*(A)\geqslant P_*(A)$，$P^*(A)=1-P_*(\overline{A})$。当 $P^*(A)=P_*(A)=P(A)$ 时，称 A 为可测集。由此可见 DS 证据理论和上下概率函数理论具有相同之处。首先，概念间的关系相似，即 $P^*(A)\geqslant P_*(A)$，$\mathrm{Bel}(A)\geqslant \mathrm{Pl}(A)$；其次，内外测度像信任函数和似然函数一样，都定义在 Θ 的幂集上。很自然地，人们用上下概率函数来解释信任函数和似然函数。

2. 广义化贝叶斯理论模型

广义化贝叶斯（Generalized Bayesian）理论模型认为当基本概率赋值的所有焦元都是单个假设集，且这些焦元满足贝叶斯独立条件时，Dempster 合成公式就退化为贝叶斯公式，因此贝叶斯公式是 Dempster 合成公式的特例，广义化贝叶斯理论模型由此而来。这说明所有应用贝叶斯概率推理方法的信息融合系统都可以用 DS 证据理论来替代，而且能够获得比贝叶斯概率推理方法更好的结果。

3. 随机集理论解释模型

随机集（Random Sets）理论解释模型把证据的合成看成随机事件的并（或交）。按照这种解释模型的观点，信息融合过程相当于随机集的集合运算过程。

至此，以上 3 种解释模型都是以概率理论为基础的。

4. 可传递信任模型

Smets 发现许多 DS 证据理论的研究者只看到基本概率赋值在识别框架 Θ 的幂集上的

静态概率分布，他们都没有研究 DS 证据理论模型的动态部分，即信任函数是如何更新的。因此，他提出了可传递信任模型（Transferable Belief Model，TBM）。TBM 是一个双层模型：一个是 Credal 层，在这层获取信任并对其进行量化、赋值和更新处理；另一个是 Pignistic 层，它将 Credal 层上的信任转换成 Pignistic 概率，并由此做出决策。Credal 层先于 Pignistic 层，在 Credal 层上随时可对信任进行赋值和更新，而只有在必须做出决策时，Pignistic 层才出现。因此，TBM 包括了两部分：一个是静态的，即基本概率赋值确定；另一个是动态的，即信任的传递过程。Smets 指出 TBM 区别于其他的 DS 证据理论模型是因为它不依赖于任何概率理论，TBM 可以看成一种“纯粹”的 DS 证据理论模型，即它已经完全从任何概率内涵中“提纯”出来。Smets 的 TBM 模仿了人类的思维和行动的区别，或者说模仿了“推理”（表明信任是如何受证据影响的）和“行为”（从多个可行的行为方案中选择一个似乎是最好的）的差别。从信息融合角度来看，TBM 在理论和实际应用上都很有价值，它是一种层次化的递进模型，体现了信息融合系统的层次化描述特征，尤其适用于需要逐层进行数据层、特征层或决策层融合的系统。

除上述 4 种经典模型外，模糊数学的创立者 Zadeh 也积极地进行 DS 证据理论的模型解释和模糊 DS 证据理论模型的算法实现。专家系统 MYCIN 的主要开发者 Gordon 和 Shortliffe 对可以表示成树状层次空间的异类证据推理问题，提出了 GS 算法模型解释。Dubois 等人指出 DS 证据理论中的基本概率赋值是一个模糊测度，以集合的观点解释了证据的并、交、补和包含等问题。

1.2 DS 证据理论的应用领域

DS 证据理论为不确定信息的表达和合成提供了自然而强有力的方法，这使得它在民用和军用等众多领域得到了广泛的应用，如表 1-1 所示。下面仅列举 DS 证据理论在目标识别、故障诊断、入侵检测、多属性决策等领域的应用现状，其他领域的情况读者可查阅相关文献。

表 1-1 DS 证据理论应用一览表

应用方向	应用领域
民用	网络信任评估、风险综合评价、视觉词典、系统安全评估、故障诊断、路由算法、数字图像处理、服务质量可信度、网络入侵检测、程序恶意性判定
军用	作战效能评估、目标识别跟踪、装备备件确定、态势评估、决策分析

1.2.1 目标识别

在目标识别领域，单一的传感器难以实现对空中目标的准确识别判断，利用多源传感器的信息融合可以提高目标识别的精确度和准确度。在异类源信息的目标识别系统中，由于存在传感器元器件故障、环境噪声等原因，所以系统存在一些不确定性。目前，对目标识别的理论和应用研究已进行了较长时间，主要有基于不确定性信息融合技术的两种方法：贝叶斯网络和 DS 证据理论。

张燕君等[3]提出一种基于证据理论的目标识别方法，该方法先定义了冲突系数，并在

此基础上设计了目标识别方法。该方法根据传感器信息间冲突情况的不同进行不同目标识别方法的设计，不仅保证了传感器数据正常情况下识别的速度和效率，而且保证了传感器高度冲突情况下识别结果的合理性，提高了抗干扰能力。

为了有效利用目标的宽窄带识别信息提高系统的目标识别性能，孙俊等[4]利用 DS 证据理论实现了宽窄带信息相结合的目标融合识别，将基本概率赋值的获得与宽窄带识别系统的特点相结合，利用证据组合，实现了宽窄带信息的融合，得到样本的融合识别结果。该方法可以有效提高系统的识别性能，增强系统识别方法的推广能力，而且在不同信噪比条件下具有很好的稳定性。

王杨等[5]提出一种基于权重的证据调整方法，为证据分配不同的权重，重新修正基本概率赋值，利用 Dempster 组合规则实现信息融合，通过数值验证并与其他的改进算法对比，结果更为理想，能有效减小冲突证据的不良影响，同时具有较高的收敛速度，降低了决策风险。

为了更好地解决高冲突证据的融合问题，周莉等[6]提出一种 3 条证据直接融合的改进算法，该算法先根据证据支持贴近度函数给出识别框架下各焦元支持度的计算方法，再根据三维证据直接融合产生的冲突因子的性质及各焦元的支持度，提出一种基于 DS 证据合成规则的冲突信息加权分配算法，该算法具有较强的抗干扰性能，能有效融合各种冲突信息，提高目标识别概率。

涂世杰等[7]通过建立各类特征的模糊隶属度函数，完成相应不同证据体的基本概率赋值；再利用重新定义的证据理论冲突系数，对冲突或较低可信度证据进行修正；最后，尝试将模糊函数与改进证据理论相结合的算法应用于弹道中段的目标识别，该方法在利用有限个稳健特征的条件下，可以无监督识别模式的方法从目标群中成功识别出真实弹头。

Dong 等[8]提出一种基于 DS 证据理论的目标融合分类模型，该模型采用单演信号分析法捕获 SAR 图像的特征，为提升目标识别性能，基于 SRC 产生证据基本概率赋值，使得证据融合更客观，效果更优。

1.2.2 故障诊断

在线故障监测与诊断是提高设备运行安全性和可靠性的有效途径，其依赖各种传感器采集的故障特征（征兆）信号监测设备的运行状况。通常，同一故障可由多种不同的故障特征表示；反之，同一故障特征的变化可由不同故障引起。因此，单一传感器一般不能提供充足的故障信息用于诊断，往往需要将多传感器提供的故障特征信息进行融合来实现精确诊断。此外，由于传感器误差、环境噪声干扰及设备运行状况的变化等内因和外因的影响，从传感器获取的故障特征往往是不确定、非精确甚至是不完整的。面对此类多源不确定性信息融合问题，基于 DS 证据理论的信息融合方法，通过信度分布（诊断证据）来描述故障特征对各种故障模式（命题）的支持程度，利用证据合成规则融合多源诊断证据，从而获得更为精确的融合结果，并进行故障决策。

徐晓滨等[9]针对不确定性故障特征信息的融合决策问题，给出基于证据推理规则的故

障诊断方法。首先基于故障特征样本似然函数归一化的方法求取各传感器（信息源）提供的诊断证据；再从传感器误差及故障特征对各故障类型辨别能力的差异出发，给出获取诊断证据可靠性因子的方法；给出双目标优化模型训练得到诊断证据的重要性权重，最后利用 ER 规则融合经可靠性因子和重要性权重修正后的诊断证据，利用融合结果进行故障决策。该方法继承了 DS 证据理论处理不确定性信息融合问题的优点，同时克服了它在实际应用中无法区分证据可靠性和重要性的不足，使得所获诊断证据更为客观、可信。2016 年，他们又提出一种将诊断证据静态融合与动态更新相结合的故障诊断方法[10]。在静态融合阶段，利用证据合成规则融合每个时刻的多条局部诊断证据获取静态融合证据，并给出基于证据距离的故障信度静态收敛指标；在动态更新阶段，基于条件化的线性组合更新规则，利用当前时刻静态融合证据更新历史证据，获取更新后的全局性诊断证据，并给出基于 S 函数的故障信度动态收敛指标。在两个阶段中，基于静态和动态信度收敛性指标函数，分别给出相应的优化学习方法，获取静态融合中局部诊断证据的静态折扣系数、动态更新中历史与当前证据的更新权重系数等参数的最优值，在最大信度原则下，利用更新后获取的诊断证据做出诊断决策。

孙伟超等[11]基于粗糙集与证据理论在处理不确定问题时的优势，提出了一种融合粗糙集与证据理论的故障诊断方法，该方法利用粗糙集将信息源给出的诊断数据转化为证据理论中的 mass 函数，并进行结果融合；同时，该方法给出边界粗糙熵的定义，并基于边界粗糙熵获得反映各信息源在诊断融合过程中重要度的动态权重参数，提出一种新的证据理论的冲突合成规则，该方法可以有效地提升诊断信息融合结果的准确性。

为了综合合理利用设备多个方面的特征信息来提高故障诊断的准确性，向阳辉等[12]提出一种结合支持向量机（Support Vector Machine，SVM）和改进证据理论的多信息融合故障诊断方法。该方法通过混淆矩阵获取各支持向量机局部诊断证据对各故障模式的可靠度，赋予不同的权重系数，并对由各支持向量机局部诊断硬输出判决矩阵构造出的基本概率赋值进行加权处理，从而实现支持向量机与改进证据理论在多信息融合故障诊断中的有效结合。

1.2.3 入侵检测

随着网络安全的重要性日益提升，入侵检测技术作为信息安全技术的一个重要方面得到了迅速的发展，分布式和智能化是入侵检测发展的方向。入侵检测系统的发展依赖于入侵检测技术的研究。入侵检测技术的发展在一定程度上取决于理论和方法的研究进展。真正将多传感器数据融合技术应用于入侵检测以提高入侵检测能力的研究还较少，且取得的具有实质性的研究成果更少。

王勇等[13]首次将 DS 证据理论应用于入侵检测领域中，给出了一个分布式入侵检测系统的体系结构模型，该模型不但综合了 HIDS（基于主机的入侵检测系统）和 NIDS（基于网络的入侵检测系统）、滥用检测和异常检测的优点，而且将可疑事件的可疑性进行量化，通过融合形成了全局的决策信息，仿真实验表明通过多传感器数据融合后得到的结果优于单传感器得到的结果。

邱科宁[14]将 DS 证据推理应用于 DoS 入侵检测领域中，给出了一个基于 DS 证据理论的 DoS 入侵检测引擎，该引擎优势在于不但综合了基于主机的入侵检测技术和基于网络的

入侵检测技术、滥用检测和异常检测的优点，而且将可疑事件的可疑性进行量化，通过融合形成了全局的检测结论。然而入侵检测系统在实际的运行环境中也暴露出一些问题，如过高的误报率、告警洪流、告警之间的关联性差、系统本身的扩展性差等。产生这些问题的一个关键因素是入侵检测系统在采集数据时的信息量不足及在进行数据分析时的相对简单化的分析。

龚琼瑶等[15]针对这一问题，将数据融合技术引入到入侵检测技术中，提出了一种分层的基于 DS 证据理论的入侵检测模型。该模型在检测过程中引入数据融合思想，实现了多信息源报警的融合处理，在一定程度上降低了报警数量、漏报率和误报率，提高了分布式入侵检测系统的检测性能。

Oliviero F 等[16]将 DS 证据理论应用到分布式异常检测系统中以改善检测效率，重点分析并解决了运用过程中需处理的独立证据不确定性的优先级排序问题，提高了异常检测性能。

Ciza Thomas 等[17]在对 DS 证据理论进行改进的基础上，提出了基于改进 DS 证据理论的入侵检测模型，该模型整合了访问事件检测传感器的局部结果，通过 DARPA 数据集测试，证明了模型的有效性。

陈烨等[18]提出将基于改进的加权 DS 证据组合方法应用到网络异常行为检测中，并融合多个支持向量机，建立新的入侵检测模型。该方法通过引入平均证据得到权重系数，以此区分各证据在 DS 证据理论融合中的影响程度，因此能有效解决证据的高度冲突，与传统的基于 DS 证据理论的异常检测相比，该模型能够有效提高融合效率，进而提高检测性能。

为了提高检测率，李永忠等[19]采用 DS 证据理论合成技术融合多个 ELM，能够提高整个检测系统的精确性。但是传统的 DS 证据理论技术在处理冲突信息源时并不理想。因此，通过引入证据之间的冲突强度，将信息源划分为可接受冲突和不可接受冲突，给出了新的证据理论，同时针对 ELM 随机产生的隐层神经元对算法性能造成影响的缺陷做出改进。

1.2.4 多属性决策

多属性决策是决策理论和方法研究的重要内容，多属性决策问题涉及社会、经济和管理中的诸多问题。在决策过程中，由于决策信息的不确定性和决策者认知能力的局限性，大部分多属性决策属于不确定性多属性决策。目前，不确定性多属性决策包括 3 方面的不确定性：决策信息本身的不确定性；在对定性属性进行量化时，决策者主观判断的不确定性；存在两种或两种以上可能的自然状态，而任何自然状态终将产生不确定性。除上述由问题本身和外部环境引起的不确定性外，决策者的行为也会对决策结果产生影响，因此，将 DS 证据理论推广应用到多属性决策问题中已成为研究热点。

靳留乾等[20]建立了基于证据推理和第 3 代前景理论的决策方法，以解决动态参考点的不确定性多属性决策问题。该方法采用确定因子结构表示不确定性信息，能够处理效益型、成本型和非效益非成本型属性，先根据第 3 代前景理论得到各方案在各属性下的前景价值，再根据证据推理方法将前景价值进行融合得到各方案的前景价值，并根据前景价值对方案进行排序。

在考虑决策者主观偏好的基础上，龚本刚等[21]将 DS 证据理论与 DEA 交叉评价效率相结合，提出了一种新的混合型多属性决策方法。该方法通过模糊评价等级对评价指标的模

糊性进行量化，采用证据理论完成评价指标信息的融合，从而克服了评价指标难以量化及不满足可加性与独立性等缺陷。

针对以往匹配决策方法不适用于某一方因地位不对等、信息不对称等因素而造成偏好失效的情形，林杨等[22]提出一种基于证据推理和最优指派策略的单边匹配决策模型，以实际单边匹配问题为背景，考虑参与匹配的一方主体采用不同类型信息，包括精确值、区间值和三角模糊数，表示由另一方指定的属性信息；另一方给出对各属性的权重并指定属性的评价等级；根据双方提供的信息，利用证据推理组合规则计算一方给出的所有属性在给定评价等级下的可信度，再通过集结得到双方任意主体匹配度，并构成匹配度矩阵。在匹配度矩阵基础上，运用求解指派问题的思想，建立匹配模型并求解得到匹配结果。

针对多属性群决策中可解释性证据融合推理的实体异构性问题，沈江等[23]给出了一个实体异构性下证据链融合推理的多属性群决策方法，基于证据推理理论，引入证据链关联的概念，从多数据表提供的数据矩阵中获取可区分的近邻证据集，推导了各数据表的相似度矩阵，并构建半正定矩阵的二次优化模型，共享群决策专家的经验知识，使用 Dempster 正交规则，论证了异构实体之间可解释性推理中可信度融合的合理性，并使用证据合成规则集成在各个数据表的近邻证据中获得的可信度，验证了调和多源异构数据中不一致信息的有效性。

1.3 DS 证据理论的若干问题

DS 证据理论能融合不同层次上的属性信息，能区分不确定性信息与未知性信息，还能较好地解决证据冲突，容错能力强。在受到各领域广泛青睐的同时，人们也发现了它自身存在的一些缺陷[34~37]，为了解决 DS 证据理论的缺陷，国内外许多学者对其理论研究和应用方法做出了大量的工作。

1.3.1 证据合成方法

证据合成方法是 DS 证据理论的核心，它将来自不同信息源的独立证据信息组合，产生更可靠的证据信息。但由于自身存在种种不足，使得 DS 证据理论在实际应用过程中受到了不同程度的限制，所以国内外该领域的研究者从各自不同的角度出发，提出了多种改进措施。

文献[24]提出一种新的区间直觉模糊集决策模型。首先采用区间直觉模糊集表示属性值，将区间直觉模糊数转换为区间基本概率赋值，然后利用基于区间数的合成规则进行融合，最后将融合后的区间基本概率赋值转换为经典基本概率赋值用于决策，可直接方便地实现多属性数据的融合。为更好地对证据质量进行管理，Johan Schubert 提出了一种新的证据折扣方法[25]，该方法依据每个证据对冲突值影响的大小按比例进行折扣处理。证据之间相似度评估是 DS 证据理论中的一个核心问题，到目前为止，还没有一种证据相似度测度可以全面衡量证据之间的相关性，为此，Atiye Sarabi-Jamab 等提出了一种可选择、可分辨的相似度测度算法[26]，并在此基础上提出了一种合适的 DS 证据合成方法。文献[27]提出了一种证据加权的合成算法，较之以往的加权合成算法而言，该算法具有客观、简捷等优

试读结束，需要全本PDF请购买 www.ertongbook.com