一种基于"交并集"和 Pignistic 概率的证据冲突的改进方法*)

潘 巍[1] 李晋川[2] 王阳生[3] 杨宏戟[4]

(首都师范大学信息工程学院 北京 100037)[1] (四川大学 成都 610065)[2]

(中国科学院自动化研究所模式识别国家重点实验室 北京 100080)[3]

(Software Technology Research Laboratory, De Montfort University, Leicester, LE1 9BH, England)[4]

摘 要 针对D-S证据理论无法解决高冲突证据的缺陷,通过对现有几种证据冲突的改进方法进行分析,提出了基于"交并集"和Pignistic概率的改进方法。本文放宽D-S组合规则的假设,只要求证据在组合时至少有一条是真实的,如果证据A和B相互支持,说明它们都是真实的,可以用"交集"运算将证据的信度聚焦在它们的交集上;如果证据A和B相互冲突,表明不知道哪一条证据是真实的,则用"并集"运算将信度聚焦在它们的并集上,即证据支持A或B中的一个,这种思路更符合人类的直觉。由于在目标识别系统中,最终决策是单个待识目标,因此以还要用Pignistic概率转换法将多元素命题的BPA再分配给它的各个组合元素,最后,信度最高的元素作为结果进行输出。实验表明,本文方法在解决证据冲突方面较其他方法拥有明显的优势。使用本文方法时,证据的融合顺序对融合结果没有影响,因此可以很方便地编程实现。

关键词 证据理论,证据组合规则,证据冲突,Pignistic概率

A New Solution Based on "Conjunctive & Disjunctive Pooling" and Pignistic Probability Transforms According to the Evidence Conflict Problems in D-S Theory of Evidence

PAN Wei[1] LI Jin-Chuan[2] WANG Yang-Sheng[3] YAGN Hong-Ji[4]

(Institute of Information Engineering, Capital Normal University, Beijing 100037)[1] (Sichuan University, Chengdu 610065)[2]

(Institute of Automation, Chinese Science Academies, Beijing 100080)[3]

(Software Technology Research Laboratory, De Montfort University, Leicester, LE1 9BH, England)[4]

Abstract According to the defect that in the D-S Theory of Evidence, the evidence combination rules can't work correctly facing high conflicting evidences, a new solution based on "conjunctive & disjunctive pooling" and Pignistic probability transforms is introduced. The solution supposes that at least one evidence is true among all the given evidences. When evidence A and B are consistent which means both the evidences are true, the beliefs of evidences will focus on their conjunctive pooling. On the other hand, when evidence A and B are inconsistent which means can't judge which evidence is true, the beliefs of evidences will focus on their disjunctive pooling. In object recognition systems, owing to the request of single final output, a pignistic probability transform is used to reassign the basic probability assignments of multi-element propositions to each element thus the final output is the one with the highest belief. The experiment results show that the solution can get best performance evaluation. Finally, the sequence of evidence fusion has no effect on fusion results so the solution can be programmed easily.

Keywords Theory of evidence, Evidence combination rules, Evidence conflict, Pignistic probability

1 引言

Dempster-Shafer证据理论,简称D-S理论或证据理论,源于1967年Dempster提出的根据多值映射确定概率上下界的原理[1],Shafer随即将其推广并形成D-S证据理论。D-S证据理论属于不确定推理算法,其主要优点是:不需要先验信息,对不确定信息的描述采用"区间"的方法,解决了关于不确定性信息的表示方法,在区分"不知道"与"不确定"方面以及精确反映证据收集方面显示出很大的灵活性。在D-S证据理论中,证据与子集相关,而不是与单个元素相关,并且随着证据的积累,可以不断地缩小假设集的范围,减轻处理的复杂度。因此,在目标识别领域的各种推理算法中,D-S证据理论具有独特的优势。遗憾的是,证据组合规则不能很好地处理具有高冲突性的证据,有时甚至会得到有悖常理的结论。本文将针对这一问题进行分析并提出相应的改进方法。

2 D-S证据理论相关概念介绍

2.1 辨识框架

设Ω为一个有穷而完备的论域集合,且Ω中的各元素相互独立,如果我们所关心的任一命题均对应于Ω的一个子

*)国家863高技术研究发展计划项目(编号:2003AA114020)。潘 巍 博士,讲师,研究方向为模式识别、信息融合;李晋川 博士,副教授,研究方向为软件仿真;王阳生 研究员,博士生导师,研究方向为模式识别;杨宏戟 博士生导师,英国De Montfort大学软件技术研究室主任,研究方向为软件工程。

集，则称 Ω 为样本空间或辨识框架(frame of discernment)。如果 Ω 中元素的个数为 N，则 Ω 的幂集合 2Ω 的元素个数为 $2N$，并构成该域中所有命题的集合。

2.2 焦元

对于辨识框架 Ω 的任意一个子集 A，如果 $m(A)>0$，则称 A 为焦元元素(focal element)，所有焦元的并称为核(core)。

2.3 基本概率分配函数 BPA

对任何一个属于辨识框架 Ω 的命题 A，如果有函数 m：$2\Omega\to[0,1]$，且满足

$$\begin{cases}\sum\limits_{A\subseteq\Omega}m(A)=1\\ m(\Phi)=0\end{cases}\tag{1}$$

则称 m 是基本概率分配函数，$m(A)$ 是 A 的基本概率分配(Basic Probability Assignment，简称 BPA)，表示证据支持命题 A 发生的程度，而不支持任何 A 的子集。对于 A 的不知道信息可用 $\overline{A}$ 的基本概率分配来度量，$\overline{A}=\Omega-A$，$m(A)+m(\overline{A})\leqslant 1$，说明 $m(A)$ 不是概率。

2.4 证据组合规则

假设 $m_1,m_2,\cdots,m_n$ 为辨识框架 Ω 上的相互独立的基本概率分配函数，则组合这 n 个证据所得到的新证据的基本概率分配为：

$$m(A)=m_1\oplus m_2\oplus\cdots\oplus m_n=\begin{cases}0 & A=\Phi\\ \dfrac{\sum\limits_{\cap X_1=A i=1}\prod\limits^{n}m_i(X_i)}{1-k}, & k=\sum\limits_{\cap X_1=\Phi i=1}\prod\limits^{n}m_i(X_i),A\neq\Phi,k\neq 1\end{cases}\tag{2}$$

其中“$\oplus$”表示直和，k 是证据冲突度。

由于 D-S 组合规则满足结合律，融合的顺序对最终的融合结果没有影响，因此在实际使用时，往往先对两个证据进行融合，然后把融合后的结果再与第三个证据融合，以此类推。

3 D-S 证据理论中证据冲突的改进方法

在 D-S 证据组合规则中，k 是证据冲突度，反映了证据之间的冲突程度，k 越大表明冲突越大。当 $k=1$ 时，分母为 0，组合规则无法使用；当 $k\to 1$，即证据高度冲突时，组合规则可能会产生有悖常理的结论。

例 1 设 a,b,c 是焦元，有 2 组证据，$m_1(a)=\alpha,m_1(b)=\beta,m_1(c)=1-\alpha-\beta;m_2(a)=1-\alpha-\beta,\ m_2(b)=\beta,\ m_2(c)=\alpha,0\leqslant\alpha,\beta\leqslant 1$。由组合规则得：

$$k=1-\beta^2+2\alpha^2-2\alpha+2\alpha\beta$$

$$m(a)=m(c)=\alpha(1-\alpha-\beta)/(1-k)=\alpha(1-\alpha-\beta)/(\beta^2+2\alpha(1-\alpha-\beta))$$

$$m(b)=\beta^2/(\beta^2+2\alpha(1-\alpha-\beta))$$

若 $\alpha=0,\beta=0.1$，则 $k=0.99,m(a)=m(c)=0,m(b)=1$。尽管 m_1,m_2 对 b 的支持度都非常低，但组合结果却认为 b 为真，这显然是不合理的。

若 $\alpha=0.01,\beta=0.1$，则 $k=0.9722,\ m(a)=m(c)=0.32,\ m(b)=0.36$。

若 $\alpha=0.1,\beta=0.1$，则 $k=0.83,m(a)=m(c)=0.47,m(b)=0.06$。

可见，由于证据冲突度 k 的存在，D-S 组合规则对 α 是很敏感的。图 1 描述了例 1 中证据冲突度 k 与归一化因子 $1/(1-k)$ 的关系。可以看到，当证据冲突度 $k\to 1$ 时，归一化因子发生陡变，导致融合结果随之陡变。

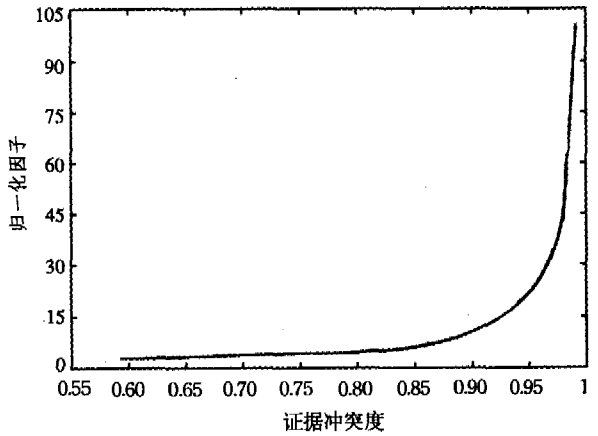

图 1 例 1 中证据冲突度 k 与归一化因子 $1/(1-k)$ 的关系

3.1 现有改进证据冲突的方法

由于 Dempster 认为信度不应该分配在空集上，因此 D-S 组合规则将证据冲突度 k 舍去并且对信度进行了归一化过程。而对高度冲突的证据使用 D-S 组合规则的归一化过程可能会导致某种与直觉相悖的融合结果，其根本原因在于 D-S 证据理论要求分配在空集上的信度为 0。目前主要存在 3 种基于这一观点的改进方法。

1)把冲突证据赋予 $m(\Omega)$

Yager[2] 认为，既然人们并不真正知道冲突部分的情况，那么就让它分配在所有的元素中而不像原来那样仅仅分配在焦元集合上，因此取消了归一化过程：

$$m(A)=m_1\oplus\cdots\oplus m_n=\begin{cases}0 & A=\Phi\\ \sum\limits_{\cap X_1=A i=1}\prod\limits^{n}m_i(X_i), & A\neq\Phi,A\neq\Omega\\ \sum\limits_{\cap X_1=\Omega i=1}\prod\limits^{n}m_i(X_i)+k, & k=\sum\limits_{\cap X_1=\Phi i=1}\prod\limits^{n}m_i(X_i),A=\Omega\end{cases}\tag{3}$$

Yager 的组合规则中去掉了归一化因子 $1/(1-k)$，而把 k 完全赋给 $m(\Omega)$。对于例 1，如果 $\alpha=0,\beta=0.1$，Yager 改进规则的组合结果为：$m(a)=m(c)=0,m(b)=0.01,m(\Omega)=0.99$。可以看出，原来冲突的证据在组合后仍然被否定，原来支持度低的证据在组合后支持度仍然比较低，但不确定度 $m(\Omega)$ 却大大增加了。Yager 提出的组合规则虽然能组合高度冲突的证据，但对于冲突的证据是完全否定的，因此在证据源多于 2 个时组合结果并不理想。

孙全[3] 认为冲突证据是部分可用的，并用证据可信度 ε 衡量冲突证据之间的可信程度。孙全提出的改进组合规则如式(4)所示。

$$m(A)=m_1\oplus m_2\oplus\cdots\oplus m_n=\begin{cases}0 & A=\Phi\\ \sum\limits_{\cap X_1=A i=1}\prod\limits^{n}m_i(X_i)+k\cdot\varepsilon\cdot q(A), & A\neq\Phi,A\neq\Omega\\ \sum\limits_{\cap X_1=\Omega i=1}\prod\limits^{n}m_i(X_i)+k\cdot\varepsilon\cdot q(A)+k(1-\varepsilon), & A=\Omega\end{cases}$$

$$q(A)=\frac{1}{n}\sum_{i=1}^{n}m_i(A),k=\sum_{\cap X_1=\Phi i=1}\prod^{n}m_i(X_i)$$

$$\varepsilon=e^{-\bar{k}},\bar{k}=\frac{1}{n(n-1)/2}\sum_{i<j}k_{ij}\tag{4}$$

k_{ij} 为两两证据间的冲突，其计算方式与 k 相同。事实上，孙全的改进组合规则是 D-S 组合规则的加权和形式，当 $k=0$ 时，与 D-S 组合规则相同；当 $k\neq 0$ 时，组合结果由 $\varepsilon\cdot q(A)$ 决

定。

类似地，Fabio 和 Sergio[4] 用证据冲突函数 $1+\log(1/k)$ 按比例将 k 赋予 $m(\Omega)$，以使冲突证据部分可用。

2)把证据冲突赋予 $m(\Phi)$

Smets[5] 认为导致冲突证据组合结果不合理的主要原因是由于在未知环境中不可能得到一个有穷且完备的识别框架，因此必然存在着一些人们无法判断其真假的未知命题，而冲突部分正是由这些未知命题造成的。所以空集 $m(\Phi)>0$，对 $m(\Phi)$ 的信任值可以理解为赋给未知命题的。Smets 因此提出可传递置信模型：

$$m(A)=m_1\oplus\cdots\oplus m_n=\begin{cases}\sum\limits_{\cap X_i=\Phi}\prod\limits_{i=1}^{n}m_i(X_i) & A=\Phi\\ \sum\limits_{\cap X_i=A}\prod\limits_{i=1}^{n}m_i(X_i) & A\neq\Phi\end{cases}\tag{5}$$

与 Yager 组合规则类似，Smets 的可传递置信模型也完全否定了冲突的证据，相互冲突的证据将不会参与下一次的融合。

类似地，吴根秀[6] 使用权重因子法对 m(Φ) 进行再分配。

3)证据冲突在命题集合上的再分配

Dubois 和 Prade[7] 提出“并集”多数规则（Disjunctive Consensus Rule），即

$$m\bigcup(C)=\sum_{A\cup B=C}m_1(A)m_2(B)\tag{6}$$

“并集”运算的最大特点是没有冲突产生，也不会否定任何证据，但这也同时扩大了命题的不确定性，同时降低了决策的精确性。

Ferson 和 Dreinovich[8] 提出平均分配法（Averaging Rule）：

$$m_{1\cdots n}(A)=\frac{1}{n}\sum_{i=1}^{n}w_im_i(A)\tag{7}$$

w_i 是分配给证据的权值

向阳等人[9] 提出，当相互支持的证据组合在一起时，证据聚焦的权重应该由更大基数的集合指向更小基数的集合；而当相互冲突的证据组合在一起时，则结果正好相反，所以根据证据携带的信息量决定聚焦的权重并同时根据证据冲突度 k 决定聚焦的方向。不过，在使用该法时，证据的融合顺序会对融合结果产生影响。

3.2 基于“交并集”和 Pignistic 概率的改进证据冲突的方法

D-S 组合规则是建立在每个证据所提供的信息都是真实的这一假设之上的，因此会把证据的信度向它们的共同支持部分（交集）聚焦；而当证据相互冲突时，D-S 组合规则无法判断证据信度的聚焦方向，所以只能将其进行归一化。因此，本文放宽 D-S 组合规则的假设，只要求证据在组合时至少有一条是真实的，如果证据 A 和 B 相互支持，说明它们都是真实的，可以用“交集”运算将证据的信度聚焦在它们的交集 $A\cap B=C$ 上；如果证据 A 和 B 相互冲突，表明不知道哪一条证据是真实的，那么，就可以用“并集”运算将信度聚焦在它们的并集 $A\cup B=D$ 上，即证据支持 A 或 B 中的一个，这种思路更符合人类的直觉。

$$m\bigcap(C)=\sum_{A\cap B=C}m_1(A)m_2(B),\text{if}(A\cap B\neq\Phi)$$
$$m\bigcup(D)=\sum_{A\cup B=D}m_1(A)m_2(B),\text{if}(A\cap B=\Phi)\tag{8}$$

需要指出的是，如果证据冲突度 $k=0$，“交并集”规则与 D-S 组合规则是一样的；如果 $k\neq0$，采用“交并集”运算后，多元素命题的信度会高于用 D-S 组合规则组合后相应的多元素命题的信度，而单元素命题的信任度却会低于用 D-S 规则组合后相应的单元素命题的信度。由于在目标识别系统中，人们要根据单元素命题（即待识目标）的最终信度进行决策，为了保证识别精度，在决策时需要将多元素命题的信度按某种原则重新分配给它所包含的各个元素。在这里，本文使用比例因子法[10] 来分配多元素命题的 BPA。

对 D-S 组合规则进行改进时，还应考虑到融合顺序对融合结果的影响。由于 D-S 组合规则满足结合律，融合顺序不影响融合结果，因此为编程方便，总是两个证据先进行融合，融合后的结果再与第三个证据融合，以此类推。本文也遵循了这个原则，具体算法步骤如下：

TempPro[$n(n-1)/2$][m] 用于存放临时计算结果，n 是证据个数，$n(n-1)/2$ 为实际融合次数，m 是目标类别数，count 是计数器。

1)取前两个证据根据式(8)做第一次融合，并对融合结果按比例因子法求取 Pignistic 概率，存入 TempPro[0][x]，($x=0,\cdots,m-1$)。设 count 为计数器，count=1。

2)for $i=2$ to $n-1$

　　$j=0$ to $i-1$

把证据 i,j 按照式(8)融合，并求相应的 Pignistic 概率；

存入 TempPro[count][x]，count=count+1；

　　endfor

　endfor

3)$\text{Pro}[i]=\dfrac{\sum\limits_{j=0}^{n-1}\text{Temp Pro}[j][i]}{\text{count}}$，$i=0,1,\cdots,m-1$

Pro[i]即为最后融合结果。如果需要将数据送入下一层融合，则可将 Pro[i]直接赋予 $m[i]$。

4 仿真实验

4.1 实验 1

本文取文[3]中的数据，共有 3 个目标类别 a,b,c，4 组证据，并分别采用 D-S 组合规则、Yager 改进规则、孙全的改进规则、平均分配法与本文方法进行比较，结果如表 1 所示。

从表 1 可以看出，对于高度冲突的证据，D-S 组合规则和 Yager 组合规则都不能很好地处理。以目标类别 a 为例，尽管绝大多数的证据高度支持 a，$m_1(a)=0.98$，$m_3(a)=0.9$，$m_4(a)=0.8$，但由于某一个证据 $m_2(a)$ 否定了 a，组合后的结果也否定 a。因此，对于多模态系统，会由于某一个或少数几个模态的出错而导致整个系统无法正常工作。孙全的改进规则用证据可信度 ϵ 判断冲突证据的部分可用性，但其对于证据变化的敏感度偏低，即使 4 个证据中有 3 个高度支持目标类别 a，仍然分配给 $m(\Omega)$ 将近 50% 的不确定性，表示根据现有证据，系统还是不能确定地得出结论。平均分配法仅是对所有证据的信度进行平均，以平均后的信度作为融合结果，完全没有考虑证据冲突。因此，在证据冲突度 k 较小时，平均分配法得到的融合结果要远低于其它方法，总体融合效果并不突出。本文建议，可将平均分配法与比例因子法结合使用，可以适当地提高决策性能。本文方法模仿人类认识事物时的推理思维，对证据进行两两比较，对一致性好的证据给予更高的信任，对冲突性大的证据给予较低的信任，综合所有证据后即可得到最后的结论。随着高度支持目标类别 a 的证据的增加，系统对 a 的确定度明显提高，这是符合人类的认识过程的。

证据 1：$m_1(a)=0.98, m_1(b)=0.01, m_1(c)=0.01$

证据 2：$m_2(a)=0.0, m_2(b)=0.01, m_2(c)=0.99$

证据 3：$m_3(a)=0.9, m_3(b)=0.0, m_3(c)=0.1$

证据 4：$m_4(a)=0.8, m_4(b)=0.1, m_4(c)=0.1$

4.2 实验 2

本文针对 D-S 证据理论中的证据冲突问题提出了基于“交并集”和 Pignistic 概率相结合的方法，其中的 Pignistic 概率转换方法选用了比例因子法。在实验 2 中，随着证据冲突度 k 的变化，本文将考查“交并集”搭配不同的 Pignistic 概率转换方法时，证据组合规则的融合性能。

本文设计了两组实验，每组实验数据分别包含两个证据，其中目标类别数为 3。随着证据冲突度 k 的变化，通过计算融合后的目标类别 a 的 BPA 值来考查“交并集”搭配不同的 Pignistic 概率转换方法时的组合规则性能。

第一组实验数据：

证据 1：$m_1(a)=0.85, m_1(b)=0.1, m_1(c)=0.05$

证据 2：$m_2(a)=\alpha, m_2(b)=0.1, m_2(c)=0.9-\alpha$

第二组实验数据：

证据 1：$m_1(a)=\alpha, m_1(b)=0.1, m_1(c)=0.9-\alpha$

证据 2：$m_2(a)=0.9-\alpha, m_2(b)=0.1, m_2(c)=\alpha$

随着 α 的变化，证据冲突度 k 也会发生相应的改变，实验结果如图 2 所示。第一组实验数据中，k 的变化范围较大，其目的是考查“交并集”搭配不同的 Pignistic 概率转换方法时，组合规则的总体性能；第二组实验数据中，k 的变化范围较小，其目的是考查组合规则在证据冲突较大时的组合性能。

可以发现，在证据冲突度 k 较小的情况下，采用比例因子法的组合规则与 D-S 组合规则的融合结果极为相似。而当 $k\to1$ 时，D-S 组合规则的性能急剧下降，而采用比例因子法的组合规则仍然能够保持较好的融合性能。

在几组采用不同 Pignistic 概率的组合规则中，比例因子法能很好地把各个证据的信度向具有一致性的目标类别聚焦，因而具有更高的融合性能。相比之下，Smets 的 BetP 概率转换法和 Sunado 的 PrPl 概率转换法对证据冲突度 k 的变化不是非常敏感，因而不能有效地扩大各命题之间的信度差异。

表 1 几种改进证据冲突方法的比较结果

	$m_1\oplus m_2$	$m_1\oplus m_2\oplus m_3$	$m_1\oplus m_2\oplus m_3\oplus m_4$
D-S 组合规则	$k=0.99$, $m(a)=0$, $m(b)=0.01$, $m(c)=0.99$, $m(\Omega)=0$	$k=0.99901$, $m(a)=0$, $m(b)=0$, $m(c)=1$, $m(\Omega)=0$	$k=0.999901$, $m(a)=0$, $m(b)=0$, $m(c)=1$, $m(\Omega)=0$
Yager 组合规则	$k=0.99$, $m(a)=0$, $m(b)=0.0001$, $m(c)=0.0099$, $m(\Omega)=0.99$	$k=0.99901$, $m(a)=0$, $m(b)=0$, $m(c)=0.00099$, $m(\Omega)=0.99901$	$k=0.999901$, $m(a)=0$, $m(b)=0$, $m(c)=0.000099$, $m(\Omega)=0.999001$
孙全 组合规则	$\varepsilon=0.3716$ $m(a)=0.18$, $m(b)=0.004$ $m(c)=0.194$, $m(\Omega)=0.622$	$\varepsilon=0.512$ $m(a)=0.321$, $m(b)=0.003$ $m(c)=0.188$, $m(\Omega)=0.4882$	$\varepsilon=0.568$ $m(a)=0.381$, $m(b)=0.017$ $m(c)=0.17$, $m(\Omega)=0.432$
平均 分配法	$m(a)=0.49$, $m(b)=0.01$ $m(c)=0.5$	$m(a)=0.627$, $m(b)=0.007$ $m(c)=0.367$	$m(a)=0.67$, $m(b)=0.03$ $m(c)=0.3$
本文方法	$m(a)=0.4898$, $(b)=0.0005$ $m(c)=0.5097$	$m(a)=0.6324$, $(b)=0.0002$ $m(c)=0.3674$	$m(a)=0.7008$, $m(b)=0.003$ $m(c)=0.2962$

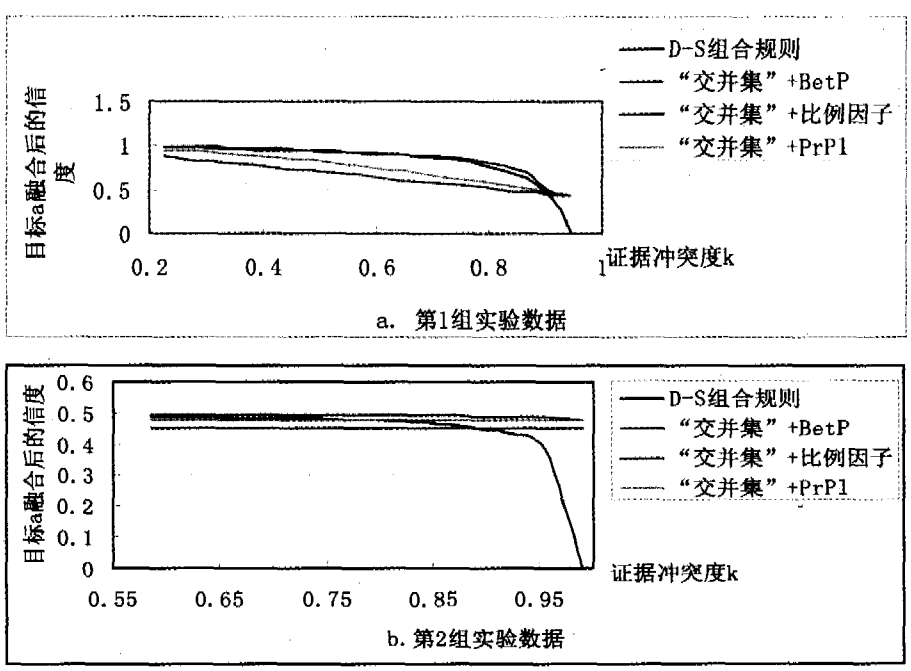

图 2 不同 Pignistic 概率转换方法对证据冲突的敏感度

小结 本文针对 D-S 证据理论无法解决高冲突证据的缺陷，提出了基于“交并集”和 Pignistic 概率的改进方法，如果证

据A和B相互支持，说明它们都是真实的，可以用“交集”运算将证据的信度聚焦在它们的交集上；如果证据A和B相互冲突，表明不知道哪一条证据是真实的，那么，就可以用“并集”运算将信度聚焦在它们的并集上，即证据支持A或B中的一个，这种思路更符合人类的直觉。由于在目标识别系统中，最终决策是单元素，因此要用Pignistic概率转换法将多元素命题的BPA再分配给它的各个组合元素。使用本文方法时，证据的融合顺序对融合结果没有影响，因此可以很方便地编程实现。

参考文献

1 Dempster A. Upper and lower probabilities induced by a multivalued mapping. Annals of Mathematical Statistics, 1967,38:325～339

2 Yager R R. On the Dempster-Shafer framework and new combination rule. Information Science, 1987,41:93～137

3 孙全，叶秀清，顾伟康. 一种新的基于证据理论的合成公式. 电子学报，2000,28(8):1～3

4 Campos F, Cavalcante S. An extended approach for Dempster-Shafer theory. IEEE, 2003. 338～344

5 Smets P. The combination of evidence in the transferable belief model. IEEE Trans on Pattern Analysis and Machine Intelligence, 1990,12(5):447～458

6 吴根秀. 冲突证据组合方法. 计算机工程，2005,31(9):151～154

7 Prade D D H. On the combiniation of evidence in various mathematical frameworks. Reliability Data Collection and Analysis, 1992, EAFC: 213～241

8 Ferson S, Kreinovich V. Representation, propagation, and aggregation of uncertainty:[SAND Report]. [in progress],2002

9 向阳，史习智. 证据理论合成规则的一点修正. 上海交通大学学报，1999,33(3):357～360

10 潘巍，王阳生，杨宏戟. Pignistic概率算法设计. 计算机工程，2005,31(4):20～23

(上接第41页)

6 实现与性能测试

本文基于VSB-SSL VPN[9]设计实现了CCM机制。VSB-SSL VPN在实现标准SSL VPN的基础上提出了两项关键性技术：虚拟服务和基于VPN流的访问控制模型。CCM以VPN流的访问控制模型为信息交换中心；通过在虚拟服务中植入终端关联模块，从而能够动态检测客户终端信息实现终端认证；以IDS关联插件的形式在IDS设备实现了IDS关联的通信模块，从而到达与控制模型通信的能力；通过流分析实现应用服务关联。

由于在VBS-SSL VPN中添加了CCM功能，使得隧道建立过程开销有所增加。针对有CCM机制和无CCM机制两种情况，VBS-SSL VPN在不同并发隧道数目下的性能测试如表1和图6所示。

表1 VBS-SSL VPN通道建立平均时间

通道数	VSB-SSL VPN(无CCM)通道建立时间/s	VSB-SSL VPN(有CCM)通道建立时间/s
1	10.03	10.58
5	10.72	10.93
10	11.13	11.22
15	11.36	11.45
20	11.52	11.63
25	11.77	11.82

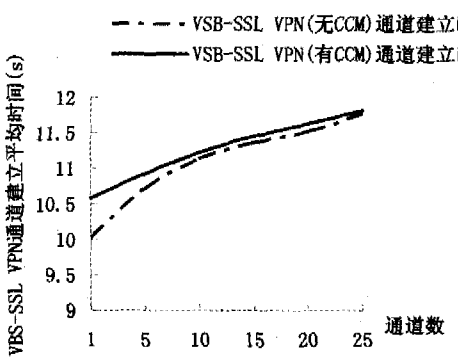

图6 CCM对VBS-SSL VPN性能影响的测试

由于CCM机制的加入，使得VSB-SSL VPN通道建立平均时间比无CCM时稍长，但是通道建立时间增加百分比的平均值$r<3\%$(r如下计算：先求出$d=$(有CCM时隧道建立时间－无CCM时隧道建立时间)/无CCM时隧道建立时间；$r=d$的平均值，即$r=((10.58-10.03)/10.03+(10.93-10.72)/10.72+(11.22-11.13)/11.13+(11.45-11.36)/11.36+(11.63-11.52)/11.52+(11.82-11.77)/11.77)/6))=1.74\%$)。而且随着连接通道数增多，每条隧道建立平均时间越来越接近无CCM时的值。这是因为随着隧道数的增加，CCM机制对隧道建立平均时间的影响越来越小，而SSL握手和加密解密耗时对隧道建立时间的影响占了主要。由此可见，虽然有CCM机制的VBS-SSL VPN系统会导致隧道建立时间稍微增加，但是CCM机制提高和完善了VBS-SSL VPN体系的安全性。

小结 本文针对VPN网络结构特点，从终端安全延伸、IDS关联延伸、应用引擎技术三个方面论述了VPN网络拓扑的关联技术——关联控制机制CCM。通过终端安全延伸将VPN客户终端状态纳入VPN网络安全策略中；通过IDS关联延伸将IDS与CCM系统关联，形成有机控制体；通过应用引擎技术实现上层协议的深度解析；从而实现高安全性的VPN网络结构。

参考文献

1 Cohen R. On the Establishment of an Access VPN in Broadband Access Networks. Communications Magazine, IEEE, February 2003,41(2): 156～163

2 Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401, November 1998

3 Dierks T, Allen C. The TLS Protocol Version 1.0. RFC2246, January 1999

4 欧阳凯，周敬利，夏涛，等. 基于SSL VPN接入机制的研究. 计算机科学，2005,32(5):59～64

5 卿斯汉，蒋建春，马恒太，等. 入侵检测技术综述. 通信学报，2004,25(7):19～28

6 Denning D E. An intrusion-detection model. IEEE Transactions on Software Engineering,1987,13(2):222～232

7 Dillis C D. IDS event correlation with SEC-the simple event correlator:[White paper]. Available at: http://www.giac.org. 2005

8 Zhang Xinyou, Li Chengzhong, Zheng Wenbin. Intrusion Prevention System Design. In: Proceedings of the Fourth International Conference on Computer and Information Technology. September 2004. 386～390

9 欧阳凯，周敬利，夏涛，等. 基于虚拟服务的SSL VPN研究. 小型微型计算机，2006,27(2):229～232