

基于证据推理融合的网络数据流识别方法

张 剑^{1,2*}, 曹 萍³, 寿国础²

(1. 上海工程技术大学 航空运输学院, 上海 201620; 2. 北京邮电大学 通信测试技术研究中心, 北京 100876;

3. 福州大学 经济与管理学院, 福州 350116)

(* 通信作者电子邮箱 zhangj9860@sina.com)

摘 要:针对多分类器决策融合研究中利用有限的训练数据对分类器概率参数估计时存在较大偏差的问题,提出一种基于D-S证据推理(ER)的多分类器决策融合算法。利用不确定性描述分类器性能,并针对D-S组合规则在分类器结果高冲突情形下易出现决策融合悖论的问题,提出基于分类器信度加权融合算法实现流量识别决策融合。实验结果表明,多数投票法和Bayes最大后验概率法识别准确率分别为78.3%和81.7%,证据推理决策融合的识别准确率提高到82.2%~91.6%,而拒识率则保持在4.1%~6.2%。

关键词:数据流识别; D-S证据理论; 决策融合; 信度加权

中图分类号: TP393.06 **文献标志码:** A

Identification method of network traffic flow based on evidence theory fusion

ZHANG Jian^{1,2*}, CAO Ping³, SHOU Guochu²

(1. School of Air Transportation, Shanghai University of Engineering Science, Shanghai 201620, China;

2. Comtest Research and Development Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;

3. School of Economics and Management, Fuzhou University, Fuzhou Fujian 350116, China)

Abstract: In multi-classifier decision fusion, there is great warp when using limited training data to estimate the probability parameters of classifier. For dealing with this problem, a multi-classifier decision fusion method based on D-S (Dempster-Shafer) Evidential Reasoning (ER) was presented. The method utilized the advantages of D-S theory to describe uncertainty of classifiers. To solve the paradox problem in high conflict circumstance among multiple classifiers, a reliability weighted fusion algorithm was proposed to realize the traffic identification decision fusion. The experimental results show that the accuracy rate of majority voting and Bayes maximum posteriori probability are 78.3% and 81.7% respectively, while the proposed algorithm can improve the accuracy rate up to 82.2%–91.6%, and remain the reject rate between 4.1% and 6.2%.

Key words: traffic flow identification; D-S (Dempster-Shafer) evidence theory; decision fusion; reliability weighting

0 引言

网络数据流的准确识别对于网络管理、网络安全等具有重要意义,已成为网络安全管理的研究热点。当前主要识别方法有利用数据流的协议特征字段匹配^[1]、协议过程特征匹配^[2]、主机连接特征匹配^[3]等,用无监督聚类算法、监督分类算法^[4]、神经网络^[5]、支持向量机^[6]等识别数据流。这些方法都需要大量的训练数据以获取分类模型参数,当训练数据集较小时,识别准确率将急剧下降,难以满足需求^[7]。从信息理论角度看,各种不同分类器利用了数据流不同特征信息,存在互补的潜能。因此如何将多个分类器识别结果进行融合,以实现比单分类器更好的识别效果具有重要的现实意义。

目前多分类器融合研究较为深入的是基于同类型分类器的集成学习方法,对于异构分类器,一般采用多数投票法、Bayes方法、神经网络方法等,而这些方法都要求获得足够的训练数据以估算分类器概率特性或参数。在网络数据流分类中,数据量极大且持续,而一般情况下获得的训练数据数量很

少,分类器的概率估计面临较大问题;另外基于概率理论难以描述分类器不确定性的特征,实现分类器融合时误差较大。本文提出基于证据推理的异构多分类器网络流量融合算法,利用不确定性处理有限训练数据以精确描述分类器性能。并针对Dempster组合规则在分类器结果高冲突情形下易出现决策融合悖论的问题^[8],提出基于多分类器的信度加权的决策融合算法——RW-DS (Reliability Weighting Dempster-Shafer),利用证据合成规则实现流量识别决策融合。通过与多数投票法、Bayes最大后验概率融合方法比较,该算法保持了各分类器的不确定性特征,在提高融合准确率的同时,能降低由于分类器不确定性造成的错误率,具有更好的异构多分类器识别融合能力。

1 多分类器的决策融合模型

多分类器的决策融合按照一定的准则对分类器结果进行综合处理,以获得对象更加准确的识别结果。通过合理的决策融合可以提高系统的准确性,降低分类判断的错误率,提升

收稿日期: 2014-02-13; 修回日期: 2014-03-10。

基金项目: 国家 863 计划项目(2008AA01Z218); 国家社会科学基金资助项目(10CG1005); 校科研基金资助项目(2014-05)。

作者简介: 张剑(1974–),男,甘肃武威人,讲师,博士,主要研究方向: 接入网流量识别与分类; 曹萍(1971–),女,重庆江津人,副教授,博士,主要研究方向: 智能决策算法; 寿国础(1965–),男,浙江诸暨人,教授,博士,主要研究方向: 智能光接入网安全。

系统的鲁棒性和可靠性。

异构多分类器决策融合主要有多数投票法、Bayes 理论^[9]、神经网络^[10]等方法。这些方法存在两个问题:首先,这些方法均需较大训练数据集,通过分析学习使用先验知识和演绎推理以达到一定级别的泛化精度。而实际应用中获得的训练数据集的数量很少,对各种应用类型不足以产生高可信度的覆盖,概率估计面临较大问题。其次,分类器普遍存在拒识问题,概率论描述分类器不确定性方面不足,不能很好描述实际应用中存在的不确定的情形。对于这些问题,这些方法难以实现有效的不确定决策融合。

1.1 D-S 证据推理决策理论

D-S(Dempster-Shafer)的证据推理(Evidential Reasoning, ER)方法引入命题-信任度的概念,对不同的先验概率假设赋予权值的方法,把证据的权值解释为函数,通过函数把假设的先验概率空间映射到后验概率空间。证据推理方法包含了不确定信息,能够避免 Bayes 理论所要求的难以获得的概率估计,实现对有限数据所包含的不确定性进行决策融合。

设辨识框架 H 包含 M 个互斥模式类, $H = \{w_1, w_2, \dots, w_M\}$, 在 H 内的任何命题 A 都是幂集 2^H 的元素,在幂集上定义基本概率赋值函数 $m: 2^H \rightarrow [0, 1]$, 满足以下条件:

$$m(\emptyset) = 0; \sum_{A \subseteq H} m(A) = 1 \quad (1)$$

其中: $m(A)$ 表示已有证据支持 A 的信任度大小,而对 A 的任何真子集不再细分; \emptyset 为空集,无信任度;所有命题的信任度之和为 1。若 $m(A) > 0 (A \subseteq H)$, 则称 A 为焦点。

信任函数 $bel(A)$ 定义为:

$$bel(A) = \sum_{B \subseteq A} m(B); \forall A \subseteq H \quad (2)$$

$bel(A)$ 表示已有证据完全支持命题 A 的程度,还满足以下 3 个关系:

$$\begin{cases} bel(\emptyset) = 0 \\ bel(H) = 1 \\ bel(A_1 \cup A_2 \cup \dots \cup A_n) \geq \sum_{I \subseteq \{1, 2, \dots, n\}, I \neq \emptyset} (-1)^{|I|+1} bel(\bigcap_{i \in I} A_i) \end{cases} \quad (3)$$

似真函数 $pl(A)$ 定义为:

$$pl(A) = \sum_{B \cap A \neq \emptyset} m(B) = 1 - bel(\bar{A}); \forall A \subseteq H \quad (4)$$

其中: $pl(A)$ 表示证据不怀疑命题 A 的程度; $[bel(A), pl(A)]$ 为不确定区间,表示证据对命题 A 的不确定程度。

1.2 Dempster 证据合成公式

在辨识框架 H 上,有 n 个不同来源证据的 m 函数 m_1, m_2, \dots, m_n , 如果这些证据相互独立,且证据之间不完全冲突,则可用证据组合规则得到新的 m 函数: $m_{\oplus} = m_1 \oplus m_2 \oplus \dots \oplus m_n$, m_{\oplus} 称为各 m 函数的直和。Dempster 证据组合规则可表示为:

$$\begin{cases} m_{\oplus}(\emptyset) = 0 \\ m_{\oplus}(A) = \frac{1}{1 - k} \cdot \sum_{A_{i1} \cap A_{i2} \cap \dots \cap A_{in} = A} m_1(A_{i1}) \cdot m_2(A_{i2}) \cdot \dots \cdot m_n(A_{in}); \forall A \subseteq H \end{cases} \quad (5)$$

其中: $k = \sum_{A_{i1} \cap A_{i2} \cap \dots \cap A_{in} = \emptyset} m_1(A_{i1}) \cdot m_2(A_{i2}) \cdot \dots \cdot m_n(A_{in})$ 。

2 网络流量识别的证据推理融合

流量识别的决策目标为融合多个分类器生成的识别结果,最终确定输入数据最终归属类别,或者拒绝识别结果。设 H 包含 M 个互斥模式类,即数据流的应用类型 $H = \{w_1, w_2, \dots, w_M\}$ 。分类器 e_i 对输入数据流 x 进行分类,得到证据 $e_i(x) = w_k$, 表示把 x 划分到应用类型 w_k 中, $w_k \in H \cup \{M+1\} (k = 1, 2, \dots, R)$, $e_i(x) = M+1$ 表示分类器不能作出分类决策,拒绝识别 x 。

本文基于证据推理进行分类决策融合,首先获取训练数据集,并据此评估各分类器的正确识别率、错误识别率和拒绝识别率以确定各分类器的基本概率赋值(Basic Probability Assignment, BPA) m 函数。通过证据融合算法融合各分类器的识别结果,并按照融合判决规则输出最终识别结果。反馈部分对融合结果进行评估,调整各分类器的基本概率赋值函数。

2.1 BPA 函数分配策略

分类器 e_i 的正确识别率用 $\varepsilon_C^{(i)}$ 表示,错误识别率用 $\varepsilon_E^{(i)}$ 表示,由于识别结果存在不确定性,一般 $\varepsilon_C^{(i)} + \varepsilon_E^{(i)} < 1$, $\varepsilon_U^{(i)}$ 表示分类器识别的不确定率。各分类器的参数 $\varepsilon_C^{(i)}, \varepsilon_E^{(i)}$ 是实现证据推理决策融合的关键因素。根据训练数据及测试数据所生成的混淆矩阵计算分类器的 $\varepsilon_C^{(i)}, \varepsilon_E^{(i)}$, 如式(6)所示:

$$\begin{cases} \varepsilon_C^{(i)} = \frac{\sum_k C_i(w_k)}{\sum_k S_i(w_k) + U_i} \\ \varepsilon_E^{(i)} = \frac{\sum_k E_i(w_k)}{\sum_k S_i(w_k) + U_i} \\ \varepsilon_U^{(i)} = 1 - \varepsilon_C^{(i)} - \varepsilon_E^{(i)} \end{cases} \quad (6)$$

其中: $C_i(w_k)$ 表示分类器 e_i 对 w_k 的正确数据量, $E_i(w_k)$ 表示 e_i 对 w_k 的错误数据量, $S_i(w_k)$ 表示被 e_i 标记为 w_k 的数据量, U_i 表示 e_i 未识别的数据量。

分类器 e_i 对数据流的 x 识别结果 $e_i(x) = w_k$, 定义 $m_i(\{w_k\})$ 的规则如下。

1) 若分类器拒绝识别 x , 即分类器不提供分类信息, e_i 仅支持 H , 令 $e_i(x) = M+1$, 则 m_i 只有一个焦点 H , 且 $m_i(H) = 1$; 即 $e_i(x) = M+1 \Rightarrow m_i(H) = 1$ 。

2) 若 $w_k \in \{1, 2, \dots, M\}$, 即分类器作出判决, 则支持 $x \in w_k$ 成立的信任度为 $\varepsilon_C^{(i)}$; 支持 $x \in w_k$ 不成立的信任度为 $\varepsilon_E^{(i)}$; 支持 H (无法决策) 的信任度为 $1 - \varepsilon_C^{(i)} - \varepsilon_E^{(i)}$ 。则 m_i 可能存在 3 个焦点, 分别为 $w_k, \{w_k\}^C = H \setminus \{w_k\}$ 和 H , 且

$$w_k \in \{1, 2, \dots, M\} \Rightarrow \begin{cases} m_i(\{w_k\}) = \varepsilon_C^{(i)} \\ m_i(\{w_k\}^C) = \varepsilon_E^{(i)} \\ m_i(H) = 1 - \varepsilon_C^{(i)} - \varepsilon_E^{(i)} \end{cases} \quad (7)$$

2.2 基于分类器信度加权的证据融合算法

Dempster 组合规则在多分类器结果高度冲突情形下存在 Zadeh 决策悖论及一票否决等问题^[11], 采用对证据平均或对冲突信息重新分配等办法并未根本解决证据冲突问题。一般认为这些问题是由于组合规则不完备或证据源不可靠造成的。在网络流量识别应用中, 分类的辨识框架是根据具体应用环境而设定的, 因而可以认为是完备的, 可通过修正 m 函

数来解决证据冲突等问题。

本文提出基于证据推理的异构多分类器网络流量融合算法——RW-DS,采用信度动态加权预处理各分类器的 m 函数,并利用 Dempster 组合规则进行决策融合。设分类器 e_i 在训练集和测试数据集上得到混淆矩阵 B_i ,定义分类器 e_i 关于 w_k 的信度为 $R_i(w_k)$:

$$R_i(w_k) = \frac{C_i(w_k) - E_i(w_k)}{S_i(w_k)} \quad (8)$$

信度 $R_i(w_k)$ 包含了分类器 e_i 对应用类型 w_k 识别准确率、错误率等信息,较全面地描述了分类器的识别性能。通过 $R_i(w_k)$ 对 $m_i(\{w_k\})$ 加权处理如式(9)所示,BPA 函数能更好地体现分类器识别准确率、错误率和拒识率的特性,在 Dempster 证据组合过程中区分各分类器的不同的信度水平,有效避免证据高度冲突时所产生的决策悖论的问题。

$$\begin{cases} m'_i(\{w_k\}) = \frac{\sum_k R_i(w_k) C_i(w_k)}{\sum_k S_i(w_k) + U_i} \\ m'_i(\{w_k\}^c) = \frac{\sum_k R_i(w_k) E_i(w_k)}{\sum_k S_i(w_k) + U_i} \\ m'_i(H) = 1 - m'_i(\{w_k\}) - m'_i(\{w_k\}^c) \end{cases} \quad (9)$$

RW-DS 算法描述如下:

- 步骤1 生成训练数据集。
- 步骤2 计算单分类器各焦元 m 函数。
- 步骤3 生成单分类器信度矩阵 D 。
- 步骤4 单分类器对网络数据流识别。
- 步骤5 提取信度向量,确定各分类器权值,对各分类器 m 加权处理。
- 步骤6 使用 Dempster 证据合成规则生成融合的 m 函数。
- 步骤7 基于融合判决准则输出识别结果。
- 步骤8 更新训练数据集。
- 步骤9 评估各分类器性能,是否重新估算单分类器 m 函数?是则转步骤2;否则转步骤4。

采用 Dempster 公式计算综合的 m 函数,进一步求得信任函数、似真函数等,决策将依据这些函数的按一定规则来确定最终输出结果。

2.3 融合判决准则

证据合成后得到合成后的 m 函数,并可得到相应的最终信任函数和似真函数,本文中最终融合判决输出类型判决准则采用设定阈值的最大化支持信任函数 $bel(w_j)$,即:

$$e(x) = \begin{cases} w_j, & bel(\{w_j\}) = \max_{1 \leq k \leq M} bel(\{w_k\}), bel(\{w_j\}) \geq \alpha \\ M+1, & \text{其他} \end{cases} \quad (10)$$

其中 $0 < \alpha < 1$ 为信任函数阈值,选择具有最大信任函数值的类型并设定了信任函数最低门限值。

3 分类决策融合实验与分析

3.1 实验数据集

网络数据流分类的公开数据集主要有 CAIDA 研究机构、

MAWI 研究组和 Moore 等数据集,这些数据集仅提供数据包头的简单匿名信息或数据流统计信息,难以判断产生数据流的真实应用类型,进而难以评估分类器性能。为能获取更准确产生数据流的应用类型,以评估各单分类器及多分类器决策融合算法的性能,实验的数据集采用文献[12]的 Comtest 数据集,该数据集采用被动测量和主动测量结合的方法得到完整的数据包集,包含基本的网络应用类型,并应用深度包检测等离线技术获得数据流真实的应用类型,以评估各单分类器和融合算法的性能。同时数据集包含不同时间段的数据流,因此该数据集有利于比较和验证新算法的有效性。

本文在原有数据集的基础上生成新的测试数据子集,数据子集约为 1.5 GB,共提取了1 600 000个数据流样本,分别为 Web 类型、P2P 类型、IM 类型各 500 000 个及 Attack 类型 100 000 个数据流, $H = \{w_1, w_2, w_3, w_4\} = \{\text{Web, P2P, IM, Attack}\}$ 。

决策融合模型采用了 3 个不同类型的分类器 $e = \{e_1, e_2, e_3\} = \{\text{AGSW-DT, OL-DBSCAN, TCTP}\}$,分别为基于自适应滑动窗的 AGSW-DT 决策树分类器、基于聚类的 OL-DBSCAN 分类器和基于传输层拓扑信息的 TCTP 分类器。从数据子集随机选取 $x = \{1\%, 2\%, \dots, 10\%\}$ 的数据作为各分类器的预处理样本。该预处理样本作为 3 个分类器的训练集,产生各自相应的分类决策机制;从数据子集另外随机选取 $(50 - x)\%$ 的数据作为评估分类器性能指标的测试数据,计算各分类器的 BPA 函数;剩余 50% 的数据测试各单分类器、多数投票法、最大 Bayes 后验概率方法及证据推理方法的分类识别性能。

3.2 实验结果与分析

实验结果在不同的训练集比例下,各分类器的特征估计与决策融合结果具有相似性,限于篇幅,仅列出在 3% 的训练数据集上得到相应的分类器参数如表 1 所示。根据各分类器参数,计算得到初始 BPA 函数如表 2 所示。从表 2 中可以看出,由于 e_1 为决策树分类器,分类器 e_1 的初始 BPA 函数 $\varepsilon_U^{(1)} = 0$,测试数据将在决策树上得到分类结果,不存在拒识,在决策融合时就会产生证据冲突问题,无法应用 Dempster 证据组合规则。经过分类器信度加权处理后,其修正 BPA 函数如表 2 所示。

表 1 3 种网络流量分类器参数

分类器	应用类型	$C_i(w_k)$	$E_i(w_k)$	$S_i(w_k)$	$R_i(w_k)$
e_1	w_1	122	22	144	0.69
	w_2	110	43	153	0.44
	w_3	115	35	150	0.53
	w_4	21	12	33	0.27
e_2	w_1	128	16	144	0.78
	w_2	96	23	119	0.61
	w_3	121	28	149	0.62
	w_4	17	8	25	0.36
e_3	w_1	89	8	97	0.84
	w_2	86	6	92	0.87
	w_3	107	23	130	0.65
	w_4	5	1	6	0.67

3 个分类器对 50% 的测试数据处理,得到相应的识别结果,以及各分类器对数据流的识别结果按照证据合成规则和

判决准则(10)完成信息融合的结果如表3所示。

表2 3种网络流量分类器BPA函数

分类器	识别参数	BPA函数	
		初始BPA	信度加权BPA
e_1	$\varepsilon_C^{(1)}$	0.77	0.42
	$\varepsilon_E^{(1)}$	0.23	0.12
	$\varepsilon_U^{(1)}$	0.00	0.47
e_2	$\varepsilon_C^{(2)}$	0.66	0.44
	$\varepsilon_E^{(2)}$	0.14	0.08
	$\varepsilon_U^{(2)}$	0.20	0.48
e_3	$\varepsilon_C^{(3)}$	0.60	0.46
	$\varepsilon_E^{(3)}$	0.08	0.06
	$\varepsilon_U^{(3)}$	0.32	0.48

通过表3可知,3个单分类器的识别准确率分别为74%、64%、58%,在3%训练数据下分类器的性能都较低; e_1 的错误率较高,达26%,但不存在拒识率; e_2 、 e_3 的错误率相对较

低,分别为17%和12%,但拒识率较高,分别为19%和30%。

基于多数投票融合可获得78.3%的准确率,高于各单分类器;融合后的错误率、拒识率分别为18.6%、3.1%,均低于单个分类器。基于Bayes最大后验概率方法融合的准确率为81.7%,高于多数投票方法结果,其错误率低于多数投票方法3.7%,拒识率则持平。

3个分类器的识别结果经过证据推理融合,识别准确率在[82.3%,91.6%]区间,在低门限值下,远高于单个分类器的识别准确率及另外两种融合方法;同时,决策融合后的错误率也显著低于单个分类器及另外两种融合方法,拒识率低于单个分类器,但高于另外两种融合方法。随着门限值 α 的提高,融合决策的准确率逐渐下降,决策错误率逐渐上升;同时融合系统的拒识率也在下降,表明要减小系统的拒识率,则融合系统的识别准确率将会下降。在实际应用时,需要对系统的不确定性和识别准确率均衡考虑。

表3 单分类器及多分类器融合识别结果

识别参数	e_1	e_2	e_3	多数投票融合	最大后验概率融合	证据推理融合 α					
						0.1	0.2	0.4	0.6	0.8	0.9
$\varepsilon_C^{(-)}$	0.74	0.64	0.58	0.783	0.817	0.916	0.903	0.875	0.856	0.841	0.822
$\varepsilon_E^{(-)}$	0.26	0.17	0.12	0.186	0.149	0.022	0.043	0.073	0.096	0.116	0.137
$\varepsilon_U^{(-)}$	0.00	0.19	0.30	0.031	0.034	0.062	0.054	0.052	0.048	0.043	0.041

从以上实验可以得出结论:基于证据推理融合结果在各指标上都要优于单个分类器的结果,识别准确率优于多数投票方法和Bayes最大后验概率方法,错误率也显著低于单个分类器及另外两种融合方法,拒识率低于单个分类器,但高于另外两种融合方法,说明该方法保持了各单分类器的不确定性。

4 结语

证据推理理论在表述、处理未知性和不确定性问题时比传统的多数投票机制和Bayes理论具有明显的优势。本文提出基于证据推理的异构多分类器网络流量融合算法——RWDS,采用信度动态加权预处理各分类器的 m 函数,并利用Dempster组合规则进行决策融合。从网络数据流分类决策融合实验中可以看出,在少量训练数据条件下,融合结果在各性能指标上都优于单分类器的测试结果,表明信息融合充分发挥了各分类器的优势,有效利用了各分类器的互补信息,保留了各分类器的不确定性,并全面提高了分类识别性能。

参考文献:

- [1] ANTONELLO R, FERNANDES S, KAMIENSKI C, *et al.* Deep packet inspection tools and techniques in commodity platforms: challenges and trends [J]. *Journal of Network and Computer Applications*, 2012, 35(6): 1863–1878.
- [2] XU K, ZHANG M, YE M, *et al.* Identify P2P traffic by inspecting data transfer behavior [J]. *Computer Communications*, 2010, 33(10): 1141–1150.
- [3] DEWAELE G, HIMURA Y, BORGNET P, *et al.* Unsupervised host behavior classification from connection patterns [J]. *International Journal of Network Management*, 2010, 20(5): 317–337.
- [4] ZHANG J, XIANG Y, ZHOU W, *et al.* Unsupervised traffic classification using flow statistical properties and IP packet payload [J]. *Journal of Computer and System Sciences*, 2013, 79(1): 573–

- 585.
- [5] AULD T, MOORE A W, GULL S F. Bayesian neural networks for Internet traffic classification [J]. *IEEE Transactions on Neural Networks*, 2007, 18(1): 223–239.
- [6] GU C, ZHANG S. Network traffic classification based on improved support vector machine [J]. *Chinese Journal of Science Instrument*, 2011, 32(7): 1507–1513. (顾成杰, 张顺颐. 基于改进SVM的网络流量分类方法研究[J]. *仪器仪表学报*, 2011, 32(7): 1507–1513.)
- [7] CALLADO A, KAMIENSKI C, SZABO G, *et al.* A survey on Internet traffic identification [J]. *IEEE Communications Survey and Tutorials*, 2009, 11(3): 37–52.
- [8] GUAN X, YI X, SUN X, *et al.* Efficient fusion approach for conflicting evidence [J]. *Journal of Tsinghua University: Science and Technology*, 2009, 49(1): 138–141. (关欣, 衣晓, 孙晓明, 等. 有效处理冲突证据的融合方法[J]. *清华大学学报: 自然科学版*, 2009, 49(1): 138–141.)
- [9] KRISHNAPURAM B, HARTENINK A J, CARIN L, *et al.* A Bayesian approach to joint feature selection and classifier design [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2004, 26(9): 1105–1111.
- [10] FISCH D, HOFMANN A, SICK B. On the versatility of radial basis function neural networks: a case study in the field of intrusion detection [J]. *Information Sciences*, 2010, 180(12): 2421–2439.
- [11] JIANG W, PENG J, DENG Y. New representation method of evidential conflict [J]. *Systems Engineering and Electronics*, 2010, 32(3): 562–565. (蒋雯, 彭进业, 邓勇. 一种新的证据冲突表示方法[J]. *系统工程与电子技术*, 2010, 32(3): 562–565.)
- [12] ZHANG J, QIAN Z, SHOU G, *et al.* Network traffic identification based on online clustering [J]. *Journal of Beijing University of Posts and Telecommunications*, 2011, 34(3): 103–106. (张剑, 钱宗珏, 寿国础, 等. 在线聚类的网络流量识别[J]. *北京邮电大学学报*, 2011, 34(3): 103–106.)