review笔记

动机

- 训练深度学习模型通常需要大量的手工标记数据，即被标记为真实或虚假的新闻文章。创建此类数据既昂贵又耗时。
- 此外，只有当注释者对事件有足够的了解时，才能获得准确标签。
- 此外，新闻文章的动态性导致现有标记样本的质量下降。其中一些样本可能很快就会过时，无法代表新出现事件的新闻报道。为了保持已经标注样本的质量，注释者必须不断标记新出现的新闻文章，这是不可行的。
- 来自用户的此类举报可以被视为假新闻检测任务的“弱”注释。大量的用户报告可以帮助缓解假新闻检测中的标签短缺问题。然而，与专家标记的样本不同，这些弱注释样本不可避免地会产生噪声。

因此，如何获得新鲜、高质量的标记样本是利用深度学习模型进行假新闻检测的主要挑战。为了应对这一挑战，我们提出了一个强化的弱监督假新闻检测框架，即 WeFEND，它可以利用用户的报告作为弱监督来大量训练数据进行假新闻检测。

贡献

- 认识到标签短缺问题，并建议利用用户报告作为对新闻内容中假新闻检测的薄弱监管。为此，我们提出了一个有效的弱监管假新闻检测框架。
- 所提出的 WeFEND 框架可以自动标注新闻文章，这有助于扩大训练集的大小，以确保深度学习模型在假新闻检测中的成功。
- 该框架 WeFEND 采用强化学习技术，具有选择高质量样本的能力，进一步提高了假新闻的检测性能。

  实验证明，所提出的框架 We FEND 可以有效地识别假新闻，并且在从微信公众号收集的大规模数据集上明显优于最先进的假新闻检测模型。

流程图

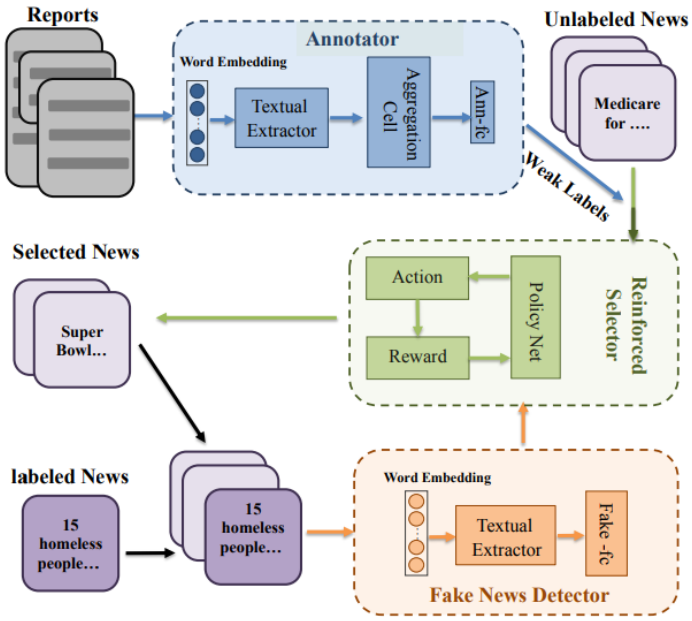


Figure 1: The architecture of proposed framework WeFEND which consists of annotator , reinforced selector and fake news detector.

1. 输入层：举报信息（Reports）与未标注新闻（Unlabeled News）

> - **Reports（举报数据）**：用户标记假新闻时提交的解释文本（如「这则新闻伪造了专家言论」），含关键监督信息。
> - **Unlabeled News（未标注新闻池）**：待检测的原始新闻（如「Medicare for ...」），无明确真假标签，需模型筛选与标注。

2. 标注器（Annotator）：生成弱标签（Weak Labels）

目标：从举报文本中提取信息，为未标注新闻打「弱标签」（非人工精准标注，是辅助监督信号）。
流程：

> 1. **Word Embedding（词嵌入）**：将举报文本、新闻文本转化为向量（如 Word2Vec、BERT 向量），统一语义表示。
> 2. **Textual Extractor（文本抽取）**：从举报文本中提取关键特征（如谣言关键词、矛盾点）。
> 3. **Aggregation Cell（聚合单元）**：融合新闻文本与举报特征，判断新闻是否含「可疑信号」。
> 4. **Ann-fc（标注全连接层）**：输出「弱标签」（如 0.8 表示 80% 概率为假新闻），为未标注新闻初步分类。

3. 强化选择器（Reinforced Selector）：筛选高价值样本

目标：用强化学习选最值得标注的新闻，提升检测模型效率（避免盲目标注低价值样本）。
流程：

> 1. **Policy Net（策略网络）**：基于新闻特征（含弱标签、文本向量等），输出「选择动作」（Action）—— 决定是否选该新闻标注。
> 2. 交互与奖励（Reward）：
>
> - 若选某新闻（Action = 选中），后续会进入标注与检测流程；
> - 检测模型更新后，根据「性能变化」（如准确率提升）给强化学习反馈 **奖励（Reward）**（性能升则奖励高，反之低）。

3. **样本输出**：筛选出的新闻（Selected News，如「Super Bowl...」）进入标注环节，成为模型训练数据。

4. 标注与检测闭环：从标注样本到模型迭代

流程：

1. **标注样本（labeled News）**：筛选出的新闻经人工 / 半自动标注（如「15 homeless people...」），成为「精准标签数据」。
2. 假新闻检测器训练：

- **Textual Extractor（文本抽取）**：再次提取标注新闻的文本特征；
- **Fake-fc（检测全连接层）**：用标注数据训练 / 更新检测模型，输出假新闻判断。

3. **反馈强化学习**：检测模型的**性能变化**（如在验证集的准确率）转化为「奖励信号」，回传给强化选择器，指导下一轮「样本选择策略」优化。

方法

文本特征提取器

我们选择卷积神经网络（Kim，2014）作为文本特征提取器，该网络已被证明在假新闻检测中有效（Wang 等人，2018）。

基于举报信息的自动标注器

用已经标注的报道{R,Y}进行训练，更新参数θ_r，训练完成后可以用来分配弱标签

聚合单元：由一个可交换聚合函数和一个全连接层组成。

i样本聚合后的特征，其中wr是全连接层权重

$$\mathbf{h}^{(i)} = \mathbf{ReLU}(\mathbf{w}_r \cdot \sum_{j=1}^{|R^{(i)}|} \frac{\mathbf{h}_j^{(i)}}{|R^{(i)}|}), \qquad (1)$$

损失函数，其中Dr是样本i经过标注器处理后的预测概率，yi是真实标签

$$L_r(R, Y; \theta_r) = -\frac{1}{|R|} \sum_{i=1}^{|R|} [y^{(i)} \log D_r(R^{(i)}; \theta_r) + (1 - y^{(i)}) \log(1 - D_r(R^{(i)}; \theta_r))]. \qquad (2)$$

基于强化学习的选择器

使用算法1得到选择的高质量样本以及他的弱标签，加入虚假新闻检测器用于训练，验证结果反馈更新参数θ_s

（筛选的标准是添加所选样本后是否能提升虚假新闻检测性能。依据该标准，我们利用强化学习机制设计了一种性能驱动的数据选择方法（称为强化数据选择器）。把整个数据集划分成 K 个小数据样本包，对于第 k 个数据样本包，它包含 B 个样本，这种方法能为选择器提供更多反馈，使强化学习的训练过程更高效。）

状态

样本 $x_i^{(k)}$ 的状态向量记为 $s_i^{(k)}$

当前状态向量包含四个元素：1）标注器的输出概率，2）虚假新闻检测器的输出概率，3）当前样本与已选样本之间余弦相似度的最大值，4）当前样本的弱标签。所有已选样本的表示定义为所有已选样本状态向量的平均值。当前状态向量与之前状态向量平均值的拼接被视为最终的状态 $s_i^{(k)}$

动作

该策略网络包含两个全连接层以及相应的激活函数。保留该样本的概率如下：

$$P(s_i^{(k)};\theta_s) = \delta(\mathbf{w}_{s2} \cdot \mathtt{ReLU}(\mathbf{w}_{s1} \cdot s_i^{(k)})), \qquad (3)$$

根据保留概率p选择动作1,0：

$$\pi_{\theta_s}(s_i^{(k)}, a_i^{(k)}) = \begin{cases} p_i^{(k)} & \text{若 } a_i^{(k)} = 1 \\ 1 - p_i^{(k)} & \text{若 } a_i^{(k)} = 0 \end{cases}$$

奖励

> **虚假新闻检测器中进行(剩下细节在下一小节)**
>
> 1. 拆分已标注数据集 → 基础训练集（训基础模型） + 验证集（测性能）
> 2. 用基础训练集训基础模型 → 在验证集测基准 acc。
> 3. 数据选择器从样本包选高质量新样本 → 扩充基础训练集 → 重新训模型。
> 4. 重新训的模型在验证集测新acck。

奖励就是他们的差值：

$$R_k = acc_k - acc. \qquad (4)$$

目标是最大化期望总奖励，对每个样本 i，用 “选该样本的概率” 乘以 “选该样本带来的奖励”，再对所有样本求和。

$$J(\theta_s) = \sum_{i=1}^{B} \pi_{\theta_s}(s_i^{(k)}, a_i^{(k)}) R_k. \qquad (5)$$

每次选一个样本（或样本包），计算它对 “奖励总和” 的梯度，梯度公式：

$$\begin{aligned}\nabla_\theta J(\theta_s) &= \sum_{i=1}^{B} R_k \nabla_{\theta_s} \pi_{\theta_s}(s_i^{(k)}, a_i^{(k)}) \\ &= \mathbb{E}_{\pi_{\theta_s}}[\sum_{i=1}^{B} R_k \nabla_{\theta_s} \log \pi_{\theta_s}(s_i^{(k)}, a_i^{(k)})]\end{aligned} \tag{6}$$

随机梯度上升更新更新策略网络的参数，因为只依赖单个（或小批量）样本的反馈，训练速度更快，能处理大规模弱标签数据，最终让策略网络逐渐学会选 “能提升检测模型性能” 的样本，：

$$\theta_s \leftarrow \theta_s + \alpha \sum_{i=1}^{B} R_k \nabla_{\theta_s} \log \pi_{\theta_s}(s_i^{(k)}, a_i^{(k)}), \tag{7}$$

主策略网络更新过快时会导致：模型快速收敛到局部最优策略，不再尝试新样本组合；参数频繁变动，梯度更新不稳定（如奖励波动大时，模型来回调整策略）。

引入**目标策略网络**，其更新速度远慢于主策略网络，用 “慢更新” 的稳定策略辅助训练：

$$\theta'_s = (1-\tau)\theta'_s + \tau\theta_s. \tag{8}$$

- τ：软更新系数（通常是小值，如0.001 ），控制主策略网络参数向目标策略网络传递的速率。

奇数偶数交替：

Algorithm 1 The algorithm of the reinforced selector.

Input: The automatically-annotated news set $\{X^u, \hat{Y}^u\}$, the bag number K, the bag size B and the learning rate α

Sample K bags of data $\{\tilde{X}^{(k)}, \tilde{Y}^{(k)}\}_{k=1}^{K}$ from $\{X^u, \hat{Y}^u\}$ and the size of every bag is B
for k $\in$ K **do**
    if k is even **then**
        Get the actions from policy network $P(\cdot, \theta_s)$
    else
        Get the actions from target policy network $P(\cdot, \theta'_s)$
    end if
    Update the policy network θ_s according to Eq. 7
    Update the target network θ'_s according to Eq. 8
end for

Sample K bags of data $\{\tilde{X}^{(k)}, \tilde{Y}^{(k)}\}_{k=1}^{K}$ from $\{X^u, \hat{Y}^u\}$ and the size of every bag is B
for k $\in K$ **do**
    Based on actions of policy network $P(\cdot; \theta_s)$, the selected samples from data bag $\{\tilde{X}^{(k)}, \tilde{Y}^{(k)}\}$ to form a new data bag $\{X_s^{(k)}, Y_s^{(k)}\}$
end for

Output: The selected data set $\{X_s, Y_s\} = \{X_s^{(k)}, Y_s^{(k)}\}_{k=1}^{K}$

虚假新闻检测器

虚假新闻检测模型是一个神经网络，由文本特征提取器和全连接层（名为 Fake - fc ）组成，配有相应的激活函数。虚假新闻检测器的输入是新闻内容，输出是给定新闻为虚假新闻的概率Dn。

虚假新闻检测器的损失函数两部分组成，在少量人工标记数据和自动标记数据集上的损失。

$$L_n(X, Y, X_s, Y_s; \theta_n) = \lambda_l \cdot L_n^l(X, Y; \theta_n) + \lambda_s \cdot L_n^s(X_s, Y_s; \theta_n), \tag{9}$$

强化弱监督虚假新闻检测框架

Algorithm 2 Reinforced weakly-supervised fake news detection framework.

Input: The labeled input with news content $\{X, Y\}$ and the corresponding report messages $\{R, Y\}$, the unlabeled input with news content X^u and the corresponding report messages R^u and the learning rate α

for number of training epochs **do**
    Update the annotator's parameters θ_r:
        $\theta_r \leftarrow \theta_r - \alpha \bigtriangledown_{\theta_r} L_r(R, Y; \theta_r)$.
end for
Use the trained annotator to assign weak labels $\hat{Y}^u$ to unlabeled news X^u based on report messages R^u.
for number of training epochs **do**
    Select data set $\{X_s, Y_s\}$ from $\{X^u, \hat{Y}^u\}$ according to Algorithm 1;
    Update the fake news detector's parameters θ_n:
        $\theta_n \leftarrow \theta_n - \alpha \bigtriangledown_{\theta_n} L_n(X, Y, X_s, Y_s; \theta_n)$.
end for

实验

数据集描述

训练数据中的新闻发布于 2018 年 3 月至 2018 年 9 月，测试数据集的新闻发布于 2018 年 9 月至 2018 年 10 月。这两个集合中的新闻时间戳没有重叠。这样设计是为了评估对新新闻进行虚假新闻检测的性能。我们还有一个未标记集，包含大量未标注的已收集新闻。未标记集的时间窗口是 2018 年 9 月至 2018 年 10 月。

Table 1: The Statistics of the WeChat Datasets.

		# News	# Report	# Avg. Reports/News
Unlabeled	-	22981	31170	1.36
Labeled Training	Fake	1220	2010	1.65
	Real	1220	1740	1.43
Labeled Testing	Fake	870	1640	1.89
	Real	870	1411	1.62

- **有监督设置**：人工标记 80%（训练）+ 人工标记 20%（验证）

  我们将人工标记好的训练集按 8:2 的比例拆分成两个集合。训练集的 20% 用作验证集，用于选择模型参数，剩余 80% 的数据则用于模型训练。

- **半监督设置**：人工标记 80%（训练）+ 人工标记 20%（验证） + 未标记集（辅助训练）

  我们依旧按照有监督设置的方式拆分数据，同时在半监督设置中引入未标记的数据。训练集的 80% 与未标记集相结合，用于模型训练。我们采用熵最小化的方法来定义未标记数据的损失（依据 Grandvalet 和 Bengio 在 2005 年提出的理论 ）。考虑到数据的相对规模，我们将标记集和未标记集上两种损失的比例设定为 1:0.1。

- **弱监督设置**：弱标记数据内部拆成 90%（训练）+10%（验证）

我们利用训练集中的举报数据对所提出的标注器进行预训练，随后使用预训练好的标注器对未标记集自动标注。基于标注结果，我们把未标记数据分成两个集合：弱虚假数据和弱真实数据。对于每个集合，我们随机选取一部分数据样本，选取的样本数量为整个未标记数据的 10%。这两个子集构成一个新的验证集，用于筛选最佳参数。所有带有弱标签的剩余数据都用于训练模型。

- **自动标注设置**：人工标记 80%（训练） + 弱标记 90%（训练） + 弱标记 10%（验证）

  混合模型的所有设置都与弱监督设置相同，但在最后一步，我们同时采用标记好的训练数据（占比 80%，同有监督和半监督设置中的比例 ）以及带有弱标签的剩余数据来训练模型。

参数细节

使用 200 维的预训练词嵌入权重（Song 等人，2018 年）来初始化嵌入层的参数。检测器的架构与基准 CNN 相同。在标注器中，权重$\boldsymbol{w}_r \in \mathbb{R}^{40\times 20}$ 。在强化选择器中，$\boldsymbol{w}_{s1} \in \mathbb{R}^{88}$ 且 $\boldsymbol{w}_{s2} \in \mathbb{R}^{8\times 1}$ 。我们将包大小B设置为与小批量大小相同，$\tau = 0.001$ ，$K = 200$ 。我们使用 PyTorch 1.2 实现所有深度学习基准方法和所提出的框架。在训练模型时，我们使用 Adam 优化器（Kingma 和 Ba，2014 年）的默认设置。学习率α为 0.0001。我们使用大小为 100 的小批量，训练轮数为 100。

结果

Table 2: The performance comparison of different methods on WeChat dataset.

Category	Method	Accuracy	AUC-ROC	Fake News			Real News		
				Precision	Recall	F_1	Precision	Recall	F_1
Supervised	LIWC-LR	0.528	0.558	0.604	0.160	0.253	0.517	0.896	0.655
	LIWC-SVM	0.568	0.598	0.574	0.521	0.546	0.563	0.614	0.587
	LIWC-RF	0.590	0.616	0.613	0.483	0.541	0.574	0.696	0.629
	LSTM	0.733	0.799	0.876	0.543	0.670	0.669	**0.923**	0.775
	CNN	0.747	0.834	0.869	0.580	0.696	0.685	0.913	0.783
	EANN	0.767	0.803	0.863	0.634	0.731	0.711	0.899	0.794
Semi-supervised	LSTM_{semi}	0.753	0.841	0.854	0.611	0.713	0.697	0.895	0.784
	CNN_{semi}	0.759	0.848	0.850	0.630	0.723	0.706	0.889	0.787
Weakly supervised	LSTM_{weak}	0.762	0.813	0.804	0.692	0.744	0.730	0.831	0.777
	CNN_{weak}	0.759	0.823	0.754	0.769	0.762	0.766	0.749	0.757
Automatically annotated	WeFEND−	0.807	0.858	0.846	**0.751**	0.795	0.776	0.863	0.817
	WeFEND	**0.824**	**0.873**	**0.880**	**0.751**	**0.810**	**0.783**	0.898	**0.836**

在监督学习设置中，LIWC-LR 达到了最差的性能。原因在于 LIWC-LR 是一个线性模型，难以区分虚假新闻和真实新闻内容的复杂分布。与 LIWC-LR 相比，LIWC-SVM 和 LIWC-RF 在大多数测量指标上提升了性能。

然而，与传统机器学习模型相比，基于深度学习的模型，包括 LSTM、CNN 和 EANN，显著提高了性能。这确认了深度学习模型在提取有用特征以进行检测方面的优越能力。特别是，与最好的传统机器学习基准 LIWC-RF 相比，CNN 在准确率和 AUC-ROC 上分别提高了约 27% 和 35%。

EANN 模型能够通过学习事件不变的特征表示来捕捉新闻的动态特性，这导致了性能的提升和相比普通 LSTM 和 CNN 更好的泛化能力。

由于数据量大幅增加，我们可以观察到两个模型的性能提升。以 LSTM 为例，LSTMsemi 的准确率和 AUC-ROC 分别提高了 3% 和 5%，相比于监督学习下的 LSTM。这表明，使用未标记数据扩大了训练集的规模并提高了性能。

弱监督的 CNNweak 和 LSTMweak 与其监督版本相比，表现更好。这验证了来自报告的弱监督在虚假新闻检测中的重要性。

WeFEND− 的性能优于监督学习和半监督学习设置中的模型。

虽然将自动标注作为弱监督的引入在某些方面有助于虚假新闻检测，但弱监督不可避免地是有噪声的。随着覆盖率的增加，WeFEND− 的召回值提高，但虚假新闻检测的精度下降。这表明，加入弱监督可能会增加更多的假阳性例子。对于真实新闻，由于大多数未标记的数据报告仍然是真实新闻，精度仍然有所提高。

所提出的 WeFEND 在所有基准模型中取得了最佳的性能。加入数据选择器后，虚假新闻和真实新闻的精度相比于同一混合设置中的简化版本得到了改善。

两个问题：

1.新闻分布是否随时间变化?

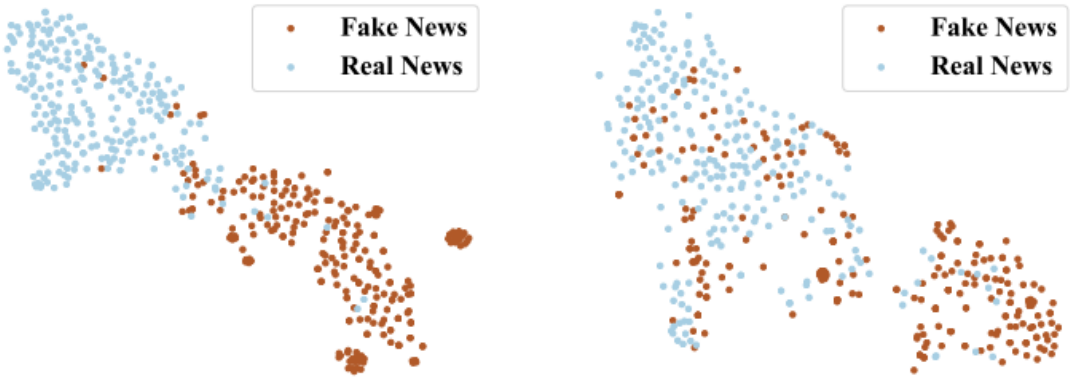
实验设置

- 同时间窗口（D_t 和 D_s ）：
  - 原始训练集（含新闻内容 + 举报） → 拆成 80%（D_t，新训练集 ）和 20%（D_s，同时间测试集 ）。
- 不同时间窗口（D_d ）：
  - 从原始测试集随机选子集 → 构造不同时间窗口的测试集 D_d ，保证 D_s 和 D_d 样本量相近。

t - SNE 是一种降维可视化方法，把高维特征压缩到 2D/3D，方便观察数据分布。

- D_s（图 2a ）：假新闻和真实新闻的特征表示**区分度高**（分隔区域清晰 ）；
- D_d（图 2b ）：假新闻和真实新闻的特征表示**缠绕在一起**（区分度低 ）。

这种对比表明，不同时间窗口内新闻的特征表示存在显著差异。



(a) Same Time (b) Different Time

我们还对比了虚假新闻检测器在同一时间集 (D_s) 上的性能与其在不同时间集 (D_d) 上的性能。

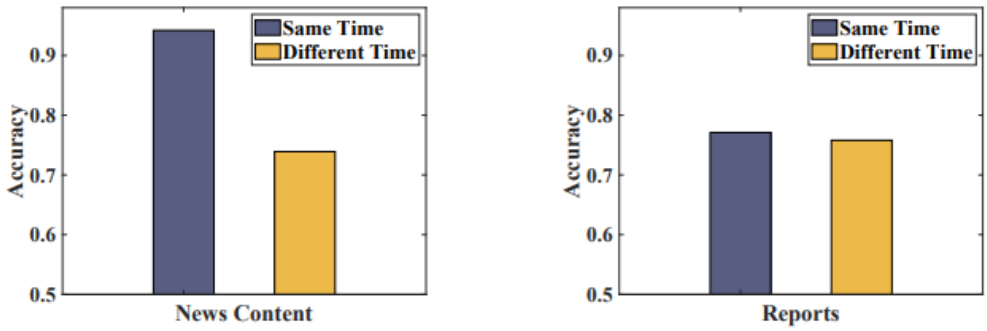
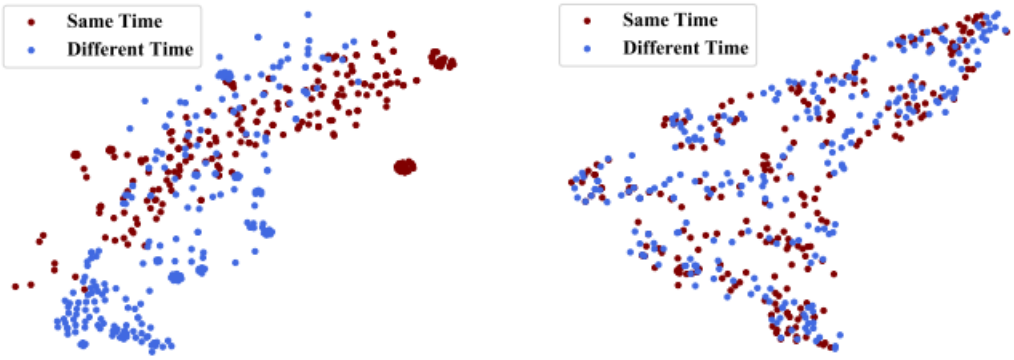


Figure 3: The performance comparison of fake news detection on news content and reports in the two sets (D_s and D_d).

可以看到，检测器在同一时间集上的准确率约为 90% 。然而，在不同时间集上，准确率仅约为 70% 。两个集合间显著的性能差异证实了新闻的分布是在变化的。

2.为何用举报标注假新闻?

基于集合 D_t 中的举报来训练标注器，并在集合 D_s 和 D_d 上测试性能。借助举报信息，标注器在同一时间集和不同时间集上能取得相近的性能。(还是图3)



(a) News Content (b) Reports

Figure 4: The Visualization of latent representations for news content and reports of fake news.

为进一步解释并证实基于举报的标注能够实现一致的质量，我们展示举报在两个时间集上的分布情况。

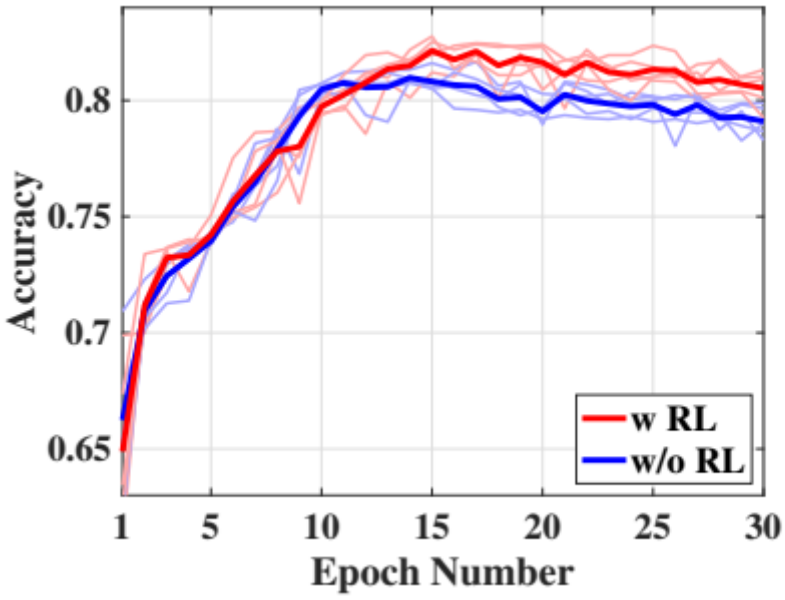
举报在同一时间集和不同时间集上的分布如图 4 所示。为清晰对比举报和新闻内容的分布，虚假新闻的新闻内容的特征表示也展示在图 4a 中。由于真实新闻易于收集，标注流程的目标是扩充虚假新闻样本的规模。因此，为分析举报的分布，我们主要聚焦于虚假新闻样本。

我们可以观察到，尽管同一时间集和不同时间集内新闻内容的分布存在重叠，但来自两个集合的样本分别聚集在右上角和左下角。这表明新闻内容的分布会随时间发生变化。

相比之下，如图 4b 所示，来自两个集合的举报信息的特征表示相互缠绕，无法区分。

这证明举报的分布不随时间变化，进一步解释了为何基于举报信息训练的模型能取得一致的性能。因此，即使对于最新的新闻文章，基于举报的标注也能保证一致的质量。

强化选择器重要性



为了验证强化选择器的重要性，我们将 WeFEND−(“w/o RL”，蓝) 和 WeFEND (“w RL”，红）分别运行 5 次，并将前 30 个轮次（epochs）的性能对比结果展示在图 5 中。实线代表 5 次运行的平均准确率，浅色线条代表单次运行的准确率数值。

需要注意的是，这两个模型之间唯一的区别在于是否包含强化选择器这一组件。

由于虚假新闻检测模型输出的概率能为强化选择器提供更多信息，从图 5 中我们可以看到，在 12 个轮次之后，带有强化选择器的模型的平均准确率稳定高于不带有强化选择器的模型。消融实验（ablation study ）表明，所设计的强化选择器能有效提升虚假新闻检测的性能 。

总结

新闻的动态特性使得获取持续标注的高质量样本以训练有效模型变得不可行，尤其是用于训练强大的基于深度学习的模型时。因此，我们提出了一个新颖的框架，该框架可将用户举报作为弱监督用于虚假新闻检测。

所提出的框架通过集成三个组件来工作，包括标注器、强化选择器和虚假新闻检测器。

标注器基于用户举报将未标记的新闻文章自动标注为真实或虚假。基于强化学习技术的强化选择器从标注器标注的样本中选择高质量样本。然后，虚假新闻检测器通过在由标注器和强化选择器生成的增强训练集上训练的模型来预测所有新闻文章的标签。

通过提高训练集的质量和规模，所提出的框架在虚假新闻检测中表现出显著提升的性能。这一点在对由新闻文章和用户反馈组成的微信数据集进行的一系列实验中得到了验证。