Using PU-Learning to Detect Deceptive Opinion Spam

Donato Hernández Fusilier\textsuperscript{1,2}  
Rafael Guzmán Cabrera  
División de Ingenierías  
Campus Irapuato-Salamanca.  
\textsuperscript{1}Universidad de Guanajuato  
Mexico.  
{donato,guzmanc}@ugto.mx

Manuel Montes-y-Gómez  
Laboratorio de Tecnologías del Lenguaje.  
Instituto Nacional de Astrofísica, Óptica y Electrónica.  
Mexico.  
mmontesg@inaoep.mx

Paolo Rosso  
Natural Language Engineering Lab., ELiRF.  
\textsuperscript{2}Universitat Politècnica de València  
Spain.  
prosso@dsic.upv.es

Abstract

Nowadays a large number of opinion reviews are posted on the Web. Such reviews are a very important source of information for customers and companies. The former rely more than ever on online reviews to make their purchase decisions and the latter to respond promptly to their clients’ expectations. Due to the economic importance of these reviews there is a growing trend to incorporate spam on such sites, and, as a consequence, to develop methods for opinion spam detection. In this paper we focus on the detection of \textit{deceptive opinion spam}, which consists of fictitious opinions that have been deliberately written to sound authentic, in order to deceive the consumers. In particular we propose a method based on the PU-learning approach which learns only from a few positive examples and a set of unlabeled data. Evaluation results in a corpus of hotel reviews demonstrate the appropriateness of the proposed method for real applications since it reached a f-measure of 0.84 in the detection of deceptive opinions using only 100 positive examples for training.

1 Introduction

The Web is the greatest repository of digital information and communication platform ever invented. People around the world widely use it to interact with each other as well as to express opinions and feelings on different issues and topics. With the increasing availability of online review sites and blogs, costumers rely more than ever on online reviews to make their purchase decisions and businesses to respond promptly to their clients’ expectations. It is not surprising that opinion mining technologies have been witnessed a great interest in recent years (Zhou et al., 2008; Mihalcea and Strapparava, 2009). Research in this field has been mainly oriented to problems such as opinion extraction (Liu B., 2012) and polarity classification (Reyes and Rosso., 2012). However, because of the current trend about the growing number of online reviews that are fake or paid by companies to promote their products or damage the reputation of competitors, the automatic detection of opinion spam has emerged as a highly relevant research topic (Jindal et al., 2010; Jindal and Liu, 2008; Lau et al., 2011; Wu et al., 2010; Ott et al., 2011; Sihong et al., 2012).

Detecting opinion spam is a very challenging problem since opinions expressed in the Web are typically short texts, written by unknown people using different styles and for different purposes. Opinion spam has many forms, e.g., fake reviews, fake comments, fake blogs, fake social network postings and deceptive texts. Opinion spam reviews may be detected by methods that seek for duplicate reviews (Jindal and Liu, 2008), however, this kind of opinion spam only represents a small percentage of the opinions from review sites. In this paper we focus on a potentially more insidious type of opinion spam, namely, \textit{deceptive opinion spam}, which consists of fictitious opinions that have been deliberately written to sound authentic, in order to deceive the consumers.

The detection of deceptive opinion spam has been traditionally solved by means of supervised text classification techniques (Ott et al., 2011). These
techniques have demonstrated to be very robust if they are trained using large sets of labeled instances from both classes, deceptive opinions (positive instances) and truthful opinions (negative examples). Nevertheless, in real application scenarios it is very difficult to construct such large training sets and, moreover, it is almost impossible to determine the authenticity of the opinions (Mukherjee et al., 2011). In order to meet this restriction we propose a method that learns only from a few positive examples and a set of unlabeled data. In particular, we propose applying the PU-Learning approach (Liu et al., 2002; Liu et al., 2003) to detect deceptive opinion spam.

The evaluation of the proposed method was carried out using a corpus of hotel reviews under different training conditions. The results are encouraging; they show the appropriateness of the proposed method for being used in real opinion spam detection applications. It reached a f-measure of 0.84 in the detection of deceptive opinions using only 100 positive examples, greatly outperforming the effectiveness of the traditional supervised approach and the one-class SVM model.

The rest of the paper is organized as follows. Section 2 presents some related works in the field of opinion spam detection. Section 3 describes our adaptation of the PU-Learning approach to the task of opinion spam detection. Section 4 presents the experimental results and discusses its advantages and disadvantages. Finally, Section 5 indicates the contributions of the paper and provides some future work directions.

2 Related Work

The detection of spam in the Web has been mainly approached as a binary classification problem (spam vs. non-spam). It has been traditionally studied in the context of e-mail (Drucker et al., 2002), and web pages (Gyongyi et al., 2004; Ntoulas et al., 2006). The detection of opinion spam, i.e., the identification of fake reviews that try to deliberately mislead human readers, is just another face of the same problem (Lau et al., 2011). Nevertheless, the construction of automatic detection methods for this task is more complex than for the others since manually gathering labeled reviews –particularly truthful opinions– is very hard, if not impossible (Mukherjee et al., 2011).

One of the first works regarding the detection of opinion spam reviews was proposed by (Jindal and Liu, 2008). He proposed detecting opinion spam by identifying duplicate content. Although this method showed good precision in a review data set from Amazon\(^1\), it has the disadvantage of underdetecting original fake reviews. It is well known that spammers modify or paraphrase their own reviews to avoid being detected by automatic tools.

In (Wu et al., 2010), the authors present a method to detect hotels which are more likely to be involved in spamming. They proposed a number of criteria that might be indicative of suspicious reviews and evaluated alternative methods for integrating these criteria to produce a suspiciousness ranking. Their criteria mainly derive from characteristics of the network of reviewers and also from the impact and ratings of reviews. It is worth mentioning that they did not take advantage of reviews’ content for their analysis.

Ott et al. (2011) constructed a classifier to distinguish between deceptive and truthful reviews. In order to train their classifier they considered certain types of near duplicates reviews as positive (deceptive) training data and the rest as the negative (truthful) training data. The review spam detection was done using different stylistic, syntactical and lexical features as well as using SVM as base classifier.

In a recent work, Sihong et al. (2012) demonstrated that a high correlation between the increase in the volume of (singleton) reviews and a sharp increase or decrease in the ratings is a clear signal that the rating is manipulated by possible spam reviews. Supported by this observation they proposed a spam detection method based on time series pattern discovery.

The method proposed in this paper is similar to Ott’s et al. method in the sense that it also aims to automatically identify deceptive and truthful reviews. However, theirs shows a key problem: it depends on the availability of labeled negative instances which are difficult to obtain, and that causes traditional text classification techniques to be ineffective for real application scenarios. In contrast,
our method is specially suited for this application since it builds accurate two-class classifiers with only positive and unlabeled examples, but not negative examples. In particular we propose using the PU-Learning approach (Liu et al., 2002; Liu et al., 2003) for opinion spam detection. To the best of our knowledge this is the first time that this technique, or any one-class classification approach, has been applied to this task. In (Ferretti et al., 2012) PU-learning was successfully used in the task of Wikipedia flaw detection.

3 PU-Learning for opinion spam detection

PU-learning is a partially supervised classification technique. It is described as a two-step strategy which addresses the problem of building a two-class classifier with only positive and unlabeled examples (Liu et al., 2002; Liu et al., 2003; Zhang and Zuo, 2009). Broadly speaking this strategy consists of two main steps: i) to identify a set of reliable negative instances from the unlabeled set, and ii) to apply a learning algorithm on the refined training set to build a two-class classifier.

Figure 1 shows our adaptation of the PU-learning approach for the task of opinion spam detection. The proposed method is an iterative process with two steps. In the first step the whole unlabeled set is considered as the negative class. Then, we train a classifier using this set in conjunction with the set of positive examples. In the second step, this classifier is used to classify (automatically label) the unlabeled set. The instances from the unlabeled set classified as positive are eliminated; the rest of them are considered as the reliable negative instances for the next iteration. This iterative process is repeated until a stop criterion is reached. Finally, the latest built classifier is returned as the final classifier.

In order to clarify the construction of the opinion spam classifier, Algorithm 1 presents the formal description of the proposed method. In this algorithm $P$ is the set of positive instances and $U_i$ represents the unlabeled set at iteration $i$; $U_1$ is the original unlabeled set. $C_i$ is used to represent the classifier that was built at iteration $i$, and $W_i$ indicates the set of unlabeled instances classified as positive by the classifier $C_i$. These instances have to be removed from the training set for the next iteration. Therefore, the negative class for next iteration is defined as $U_i - W_i$. Line 4 of the algorithm shows the stop criterion that we used in our experiments, $|W_i| < |W_{i-1}|$. The idea of this criterion is to allow a continue but gradual reduction of the negative instances.

```
1: $i \leftarrow 1$
2: $|W_0| \leftarrow |U_1|$
3: $|W_1| \leftarrow |U_1|$
4: while $|W_i| < |W_{i-1}|$ do
5:  $C_i \leftarrow \text{Generate Classifier}(P, U_i)$
6:  $U_i^L \leftarrow C_i(U_i)$
7:  $W_i \leftarrow \text{Extract Positives}(U_i^L)$
8:  $U_{i+1} \leftarrow U_i - W_i$
9:  $i \leftarrow i + 1$
10: Return Classifier $C_i$
```

Algorithm 1: PU-Learning for opinion spam detection

4 Evaluation

4.1 Datasets

The evaluation of the proposed method was carried out using a dataset of reviews assembled by Ott et al. (2011). This corpus contains 800 opinions, 400 deceptive and 400 truthful opinions. These opinions are about the 20 most popular Chicago hotels; deceptive opinions were generated using the Amazon Mechanical Turk (AMT)\(^3\), whereas –possible– truthful opinions were mined from a total of 6,977 reviews on TripAdvisor\(^4\). The following paragraphs show two opinions taken from (Ott et al., 2011). These examples are very interesting since they show the great complexity of the automatically –and even manually– detection of deceptive opinions. Both opinions are very similar and just minor details can help distinguishing one from the other. For example, in his research Ott et al. (2011) found that deceptive reviews used the words “experience”, “my husband”, “I”, “feel”, “business”, and “vacation” more than genuine ones.

\(^3\)http://www.mturk.com
\(^4\)http://www.tripadvisor.com
Example of a truthful opinion

We stay at Hilton for 4 nights last march. It was a pleasant stay. We got a large room with 2 double beds and 2 bathrooms. The TV was Ok, a 27’ CRT Flat Screen. The concierge was very friendly when we need. The room was very cleaned when we arrived, we ordered some pizzas from room service and the pizza was ok also. The main Hall is beautiful. The breakfast is charged, 20 dollars, kinda expensive. The internet access (WiFi) is charged, 13 dollars/day. Pros: Low rate price, huge rooms, close to attractions at Loop, close to metro station. Cons: Expensive breakfast, Internet access charged. Tip: When leaving the building, always use the Michigan Ave exit. It’s a great view.

Example of a deceptive opinion

My husband and I stayed for two nights at the Hilton Chicago, and enjoyed every minute of it! The bedrooms are immaculate, and the linens are very soft. We also appreciated the free WiFi, as we could stay in touch with friends while staying in Chicago. The bathroom was quite spacious, and I loved the smell of the shampoo they provided—not like most hotel shampoos. Their service was amazing, and we absolutely loved the beautiful indoor pool. I would recommend staying here to anyone.

In order to simulated real scenarios to test our method we assembled several different sub-corpora from Ott’s et al. (2011) dataset. First we randomly selected 80 deceptive opinions and 80 truthful opinions to build a fixed test set. The remaining 640 opinions were used to build six training sets of different sizes and distributions. They contain 20, 40, 60, 80, 100 and 120 positive instances (deceptive opinions) respectively. In all cases we used a set of 520 unlabeled instances containing a distribution of 320 truthful opinions and 200 deceptive opinions.

4.2 Evaluation Measure

The evaluation of the effectiveness of the proposed method was carried out by means of the f-measure. This measure is a linear combination of the precision and recall values. We computed this measure for both classes, deceptive and –possible– truthful opinions, nevertheless, the performance on the deceptive opinions is the only measure of real relevance. The f-measure for each opinion category $O_i$ is defined as follows:

$$f\text{-measure}(O_i) = \frac{2 \times \text{recall}(O_i) \times \text{precision}(O_i)}{\text{recall}(O_i) + \text{precision}(O_i)} \quad (1)$$

$$\text{recall}(O_i) = \frac{\text{number of correct predictions of } O_i}{\text{number of opinions of } O_i} \quad (2)$$
precision(O_i) = \frac{\text{number of correct predictions of } O_i}{\text{number of predictions as } O_i} \tag{3}

4.3 Results

Tables 1 and 2 show the results from all the experiments we carried out. It is important to notice that we used Naïve Bayes and SVM classifiers as learning algorithms in our PU-learning method. These learning algorithms as well as the one-class implementation of SVM were also used to generated baseline results. In all the experiments we used the default implementations of these algorithms in the Weka experimental platform (Hall et al., 2009).

In order to make easy the analysis and discussion of the results we divided them in three groups: baseline results, one-class classification results, and PU-learning results. The following paragraphs describe these results.

**Baseline results**: The baseline results were obtained by training the NB and SVM classifiers using the unlabeled dataset as the negative class. This is a common approach to build binary classifiers in lack of negative instances. It also corresponds to the results of the first iteration of the proposed PU-learning based method. The rows named as "BASE NB" and "BASE SVM" show these results. They results clearly indicate the complexity of the task and the inadequacy of the traditional classification approach. The best f-measure in the deceptive opinion class (0.68) was obtained by the NB classifier when using 120 positive opinions for training. For the cases considering less number of training instances this approach generated very poor results. In addition we can also noticed that NB outperformed SVM in all cases.

**One-class classification results**: These results correspond to the application of the one-class SVM learning algorithm (Manevitz et al., 2002), which is a very robust approach for this kind of problems. This algorithm only uses the positive examples to build the classifier and does not take advantage of the available unlabeled instances. Its results are shown in the rows named as "ONE CLASS"; these results are very interesting since clearly show that this approach is very robust when there are only some examples of deceptive opinions (please refer to Table 1). On the contrary, it is also clear that this approach was outperformed by others, especially by our PU-learning based method, when more training data was available.

**PU-Learning results**: Rows labeled as "PU-LEA NB" and "PU-LEA SVM" show the results of the proposed method when the NB and SVM classifiers were used as base classifiers respectively. These results indicate that: i) the application of PU-learning improved baseline results in most of the cases, except when using 20 and 40 positive training instances; ii) PU-Learning results clearly outperformed the results from the one-class classifier when there were used more than 60 deceptive opinions for training; iii) results from "PU-LEA NB" were usually better than results from "PU-LEA SVM". It is also important to notice that both methods quickly converged, requiring less than seven iterations for all cases. In particular, "PU-LEA NB" took more iterations than "PU-LEA SVM", leading to greater reductions of the unlabeled sets, and, consequently, to a better identification of the subsets of reliable negative instances.

Finally, Figure 2 presents a summary of the best results obtained by each of the methods in all datasets. From this figure it is clear the advantage of the one-class SVM classifier when having only some examples of deceptive opinions for training, but also it is evident the advantage of the proposed method over the rest when having a considerable quantity of deceptive opinions for training. It is important to emphasize that the best result obtained by the proposed method (a F-measure of 0.837 in the deceptive opinion class) is a very important results since it is comparable to the best result (0.89) reported for this collection/task, but when using 400 positive and 400 negative instances for training. Moreover, this result is also far better than the best human result obtained in this dataset, which, according to (Ott et al., 2011) it is around 60% of accuracy.

5 Conclusions and future work

In this paper we proposed a novel method for detecting deceptive opinion spam. This method adapts the PU-learning approach to this task. In contrast to traditional approaches that require large sets of labeled instances from both classes, deceptive and truthful
<table>
<thead>
<tr>
<th>Original Training Set</th>
<th>Approach</th>
<th>Truthful</th>
<th>Deceptive</th>
<th>Iteration</th>
<th>Final Training Set</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>P</td>
<td>R</td>
<td>F</td>
<td>P</td>
</tr>
<tr>
<td>20-D</td>
<td>ONE CLASS</td>
<td>0.500</td>
<td>0.688</td>
<td>0.579</td>
<td>0.500</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.506</td>
<td>1.000</td>
<td>0.672</td>
<td>1.000</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.506</td>
<td>1.000</td>
<td>0.672</td>
<td>1.000</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.500</td>
<td>1.000</td>
<td>0.667</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.500</td>
<td>1.000</td>
<td>0.667</td>
<td>0.000</td>
</tr>
<tr>
<td>80-D</td>
<td>ONE CLASS</td>
<td>0.500</td>
<td>0.500</td>
<td>0.500</td>
<td>0.500</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.569</td>
<td>0.975</td>
<td>0.719</td>
<td>0.913</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.574</td>
<td>0.975</td>
<td>0.722</td>
<td>0.917</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.510</td>
<td>0.938</td>
<td>0.661</td>
<td>0.615</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.517</td>
<td>0.950</td>
<td>0.670</td>
<td>0.692</td>
</tr>
<tr>
<td>100-D</td>
<td>ONE CLASS</td>
<td>0.494</td>
<td>0.525</td>
<td>0.509</td>
<td>0.493</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.623</td>
<td>0.950</td>
<td>0.752</td>
<td>0.895</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.615</td>
<td>0.938</td>
<td>0.688</td>
<td>0.773</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.561</td>
<td>0.925</td>
<td>0.698</td>
<td>0.786</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.608</td>
<td>0.913</td>
<td>0.730</td>
<td>0.825</td>
</tr>
<tr>
<td>120-D</td>
<td>ONE CLASS</td>
<td>0.494</td>
<td>0.525</td>
<td>0.509</td>
<td>0.493</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.679</td>
<td>0.950</td>
<td>0.792</td>
<td>0.917</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.708</td>
<td>0.850</td>
<td>0.773</td>
<td>0.789</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.581</td>
<td>0.938</td>
<td>0.718</td>
<td>0.839</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.615</td>
<td>0.738</td>
<td>0.670</td>
<td>0.672</td>
</tr>
</tbody>
</table>

Table 1: Comparison of the performance of different classifiers when using 20, 40 and 60 examples of deceptive opinions for training; in this table D refers to deceptive opinions and U to unlabeled opinions.

<table>
<thead>
<tr>
<th>Original Training Set</th>
<th>Approach</th>
<th>Truthful</th>
<th>Deceptive</th>
<th>Iteration</th>
<th>Final Training Set</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>P</td>
<td>R</td>
<td>F</td>
<td>P</td>
</tr>
<tr>
<td>80-D</td>
<td>ONE CLASS</td>
<td>0.494</td>
<td>0.525</td>
<td>0.509</td>
<td>0.493</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.611</td>
<td>0.963</td>
<td>0.748</td>
<td>0.912</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.615</td>
<td>0.938</td>
<td>0.743</td>
<td>0.868</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.543</td>
<td>0.938</td>
<td>0.688</td>
<td>0.773</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.561</td>
<td>0.925</td>
<td>0.698</td>
<td>0.786</td>
</tr>
<tr>
<td>100-D</td>
<td>ONE CLASS</td>
<td>0.482</td>
<td>0.513</td>
<td>0.497</td>
<td>0.480</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.623</td>
<td>0.950</td>
<td>0.752</td>
<td>0.895</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.882</td>
<td>0.750</td>
<td>0.811</td>
<td><strong>0.783</strong></td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.540</td>
<td>0.938</td>
<td>0.685</td>
<td>0.762</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.608</td>
<td>0.913</td>
<td>0.730</td>
<td>0.825</td>
</tr>
<tr>
<td>120-D</td>
<td>ONE CLASS</td>
<td>0.494</td>
<td>0.525</td>
<td>0.509</td>
<td>0.493</td>
</tr>
<tr>
<td></td>
<td>BASE NB</td>
<td>0.679</td>
<td>0.950</td>
<td>0.792</td>
<td>0.917</td>
</tr>
<tr>
<td></td>
<td>PU-LEA NB</td>
<td>0.708</td>
<td>0.850</td>
<td>0.773</td>
<td>0.789</td>
</tr>
<tr>
<td></td>
<td>BASE SVM</td>
<td>0.581</td>
<td>0.938</td>
<td>0.718</td>
<td>0.839</td>
</tr>
<tr>
<td></td>
<td>PU-LEA SVM</td>
<td>0.615</td>
<td>0.738</td>
<td>0.670</td>
<td>0.672</td>
</tr>
</tbody>
</table>

Table 2: Comparison of the performance of different classifiers when using 80, 100 and 120 examples of deceptive opinions for training; in this table D refers to deceptive opinions and U to unlabeled opinions.
opinions, to build accurate classifiers, the proposed method only uses a small set of deceptive opinion examples and a set of unlabeled opinions. This characteristic represents a great advantage of our method over previous approaches since in real application scenarios it is very difficult to construct such large training sets and, moreover, it is almost impossible to determine the authenticity or truthfulness of the opinions.

The evaluation of the method in a set of hotel reviews indicated that the proposed method is very appropriate for the task of opinion spam detection. It achieved a F-measure of 0.837 in the classification of deceptive opinions using only 100 positive examples and a bunch of unlabeled instances for training. This result is very relevant since it is comparable to previous results obtained by highly supervised methods in similar evaluation conditions.

Another important contribution of this work was the evaluation of a one-class classifier in this task. For the experimental results we can conclude that the usage of a one-class SVM classifier is very adequate for cases when there are only very few examples of deceptive opinions for training. In addition we could observe that this approach and the proposed method based on PU-learning are complementary. The one-class SVM classifier obtained the best results using less than 50 positive training examples, whereas the proposed method achieved the best results for the cases having more training examples.

As future work we plan to integrate the PU-learning and self-training approaches. Our idea is that iteratively adding some of the unlabeled instances into the original positive set may further improve the classification accuracy. We also plan to define and evaluate different stop criteria, and to apply this method in other related tasks such as email spam detection or phishing url detection.

Acknowledgments

This work is the result of the collaboration in the framework of the WIQEI IRSES project (Grant No. 269180) within the FP 7 Marie Curie. The work of the last author was in the framework the DIANA-APPLICATIONS-Finding Hidden Knowledge in Texts: Applications (TIN2012-38603-C02-01) project, and the VLC/CAMPUS Microcluster on Multimodal Interaction in Intelligent Systems.

References


conference on Web search and web data mining, Volume 2 Issue 4, Article 25. pages 1-30. ACM.


G. Wu, D. Greene and P. Cunningham. 2010. Merging multiple criteria to identify suspicious reviews. Rec-Sys10, pages 241-244. ACM.
