École Polytechnique Fédérale de Lausanne

EE-558: A Network Tour of Data Science

Fall 2018

Predicting the nature of terrorist attacks

Team 34:
Charles-Théophile Coen, Valentin Morel, Cédric Schumacher, Xavier Sieber

Professors: Pierre Vandergheynst and Pascal Frossard
Assistants: Michael Defferrard, Effrosyni Simou, Hermina Petric Maretic, Eda Bayram,Benjamin Ricaud, Rodrigo Pena

January 18, 2019

1 Introduction

The past few years have seen a growth in terrorist attack around the world. In 2014, the Global Terrorism Database[1] listed over 12'900 incidents for a total of more than 44'490 casualties. With the emergence of new and more radicalized terrorist groups, the necessity of analyzing, classifying and understanding these attacks is urgent for most of the nations worldwide.

Bearing this in mind, the goal of this project is to classify and cluster real-world data in an attempt to respond to this global demand. The data-set we chose is provided by the UCSC for free (*https://linqs-data.soe.ucsc.edu/public/lbc/TerrorAttack.tgz*). It consists of 1293 different attacks, each of which is described by 106 binary features. The nature of these features are not known, but each feature vector comes assigned with two labels. The first label describes the type of the attack while the second specifies the location. The type of attack is always labeled as one of the following: arson, bombing, kidnapping, NBCR attack, weapon attack or 'other'. One the other hand, the labels of location is created from the list of edges provided in addition to the data-set. They link attacks that are perpetrated in the same location, and thanks to them, a vector assigning each node to a specific location is computed.

In this project we will focus on trying to predict the labels of an attack only using the feature vector. We will present different approaches for predicting each label, where every proposed solution is tailored to the problem at hand in an attempt to increase its performance.

2 Data pre-analysis

As a first step into the project, we performed a statistical analysis on our data. This allowed us to get an idea about distributions and correlation within our feature matrix $y \in \mathbb{R}^{1293\times 106}$. Each row of the feature matrix corresponds to an attack or node while each column corresponds to a binary feature.

The first statistical test performed was computing a pairwise correlation of the columns in the feature matrix. This allowed us to discriminate features expressing the same behaviour making them redundant. Luckily only 6 features displayed a correlation greater than 85% with some other features. This means that of the total 106 features, 100 actually contribute to distinct observations.

The second statistical test was performed on the label of the different attacks, namely the type of the perpetrated attack. As we are interested in classifying the features into the labels, it is important to know if the labels are equally distributed or if certain labels dominate the majority of the data. The test was run twice, once only using the attacks occurring at single location and a second time only using locations where multiple attacks were perpetrated. Both runs actually displayed the same trend in terms of attack type which indicates that this label is independent of the number of attacks that already happened in a given location. The results nevertheless show that three attack types account for almost 97% of the total attacks as can be observed in pie charts below. A special care will need to be taken while choosing the metric for the classification as certain labels only display few data-points.

[1] `https://ourworldindata.org/terrorism`

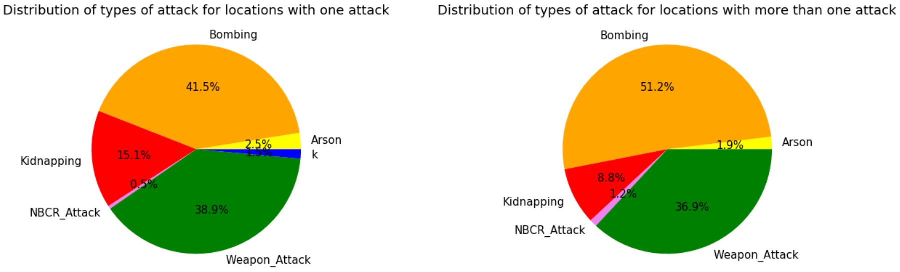


Figure 1: Distriubtions of attack types

3 Collocation prediction

The objective of this section is to predict if an attack is collocated with another one by looking at the 106 features given in the dataset. The location of terrorist attack is a trivial information that may seem pointless to predict. However, by studying the prediction model, several conclusion could be drawn. The prediction model uses the features and, by knowing which features play important role in which location, underlying pattern in the data could emerge.

As the data-set contains locations where only a single attack occurred, trying to generalize the behaviour of the features on such locations using a single data point makes little sense. Therefore, the dataset is confined to locations where more than one attack was perpetrated.

The dataset is classified using four clustering techniques namely Birch, HDBscan, Kmeans and spectral clustering. The wide panel of algorithm allows to exclude that failure is due to a non-adapted algorithm. The metric used to compare the result of each clustering technique is the Adjusted Mutual Information indice (AMI)[2].

Techniques	**AMI score**
Birch,	0.32
HDBscan,	0.0
Kmeans	0.31
Spectral clustering	0.25

The result are globally poor for every method. The best algorithm seems to be the Birch clustering with an AMI value of 0.32. With this low value, the clustering cannot be trusted. Thus, other method and subject will be tested in the following sections.

4 Type of attack prediction

We have seen in the previous section that the feature vectors do not allow to create a network where edges reflect a collocation probability of two attacks. This might be because the similarity of two feature vectors in reality reflect another label, for example the attack type.

In this section we will try to rerun spectral clustering algorithm, this time searching for

[2] `https://en.wikipedia.org/wiki/Adjusted_mutual_information`

6 clusters, where each cluster is expected to correspond to an attack type. The results are displayed below.

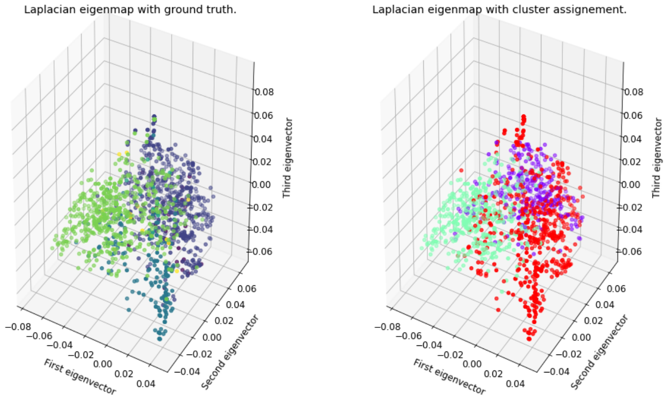


Figure 2: *Left*: Ground truth *Right*: Birch clustering result

	Euclidean		Cosine	
Cluster number	3	6	3	6
Birch	0.24	0.26	0.24	0.26
HDBScan	0.14	0.13	0.14	0.13
KMeans	0.24	0.23	0.23	0.23
Spectral Clustering	0.27	0.21	0.25	0.16

Table 1: AMI metric score for different clustering techniques

These results seem to indicate that the similarity of two feature vectors does not reflect similarity of the attached labels, it being the location or the attack type.

5 Hybrid approach to clustering

As we are determined to make the clustering work, we decided to take a different approach to the problem. The issue up to this point seemed to be that the similarity between the feature vectors failed to reflect the similarity of their labels. In this section we will try to project the data from the feature space into a lower dimensional space such that the similarity in this new space optimally reflects the similarity of the attack type.
Let $y \in \mathbb{R}^{1293\times 106}$ be the features in original space and $p : \mathbb{R}^{106} \to \mathbb{R}^{6}$ a projection onto a lower dimension. The features in the lower dimensional space $\tilde{y}$ can therefore be expressed by

$$\tilde{y} = yP \quad P \in \mathbb{R}^{106\times 6} \tag{1}$$

We want to tweak this projection matrix P such that the projection optimally reproduces similarity between two feature vectors of $\tilde{y}$ if they are of the same label.
This was done by creating a target matrix $y_t \in \mathbb{R}^{1293\times 6}$ using the label ground truth, where each row of y_t is a unit vector pointing in a direction assigned by the labels, forming a orthnormal basis. This matrix can then be used to find the optimal projection by solving

$$\underset{P}{\arg\min} \quad \|yP - y_t\|_2^2 \tag{2}$$

Equation 2 was solved using a gradient descent algorithm. The projection result $\tilde{y}$ was then fed to the spectral clustering algorithm.

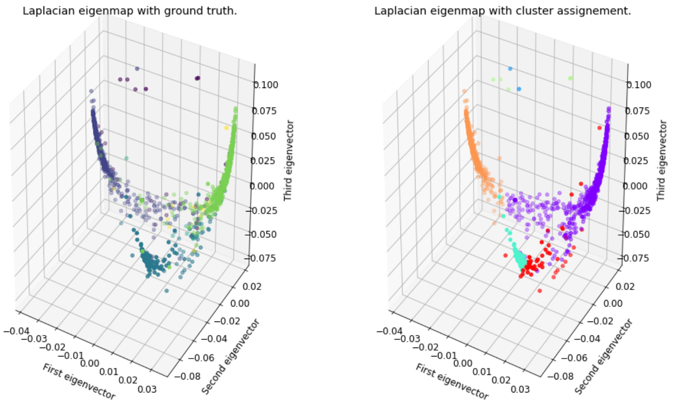


Figure 3: *Left*: Ground truth *Right*: Spectral Clustering result

	Euclidean		Cosine	
Cluster number	3	6	3	6
Birch	0	0	0	0
HDBScan	0.20	0.34	0.20	0.34
KMeans	0.53	0.43	0.53	0.43
Spectral Clustering	0.53	0.46	0.55	0.58

Table 2: AMI metric score for different clustering techniques

The scores are better compared to before. By optimizing the similarities between the features and the labels, better clustering is achieved.

6 Classification

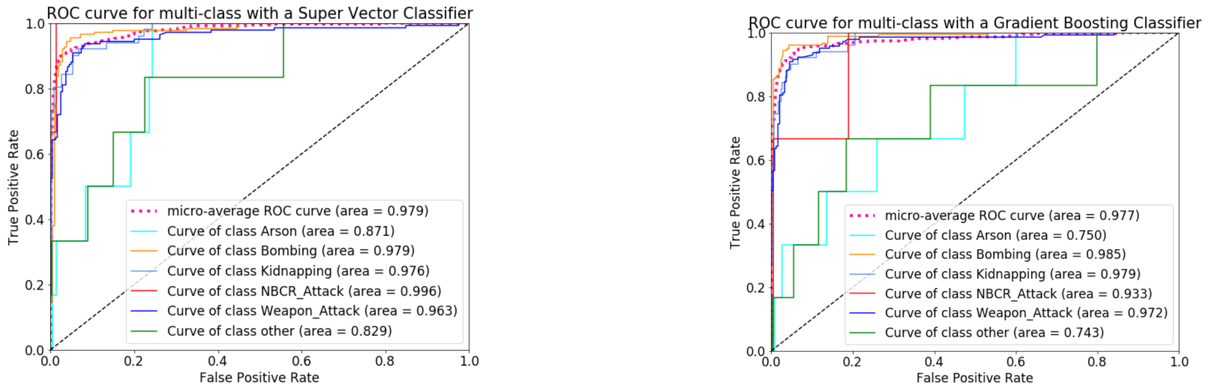
Finally, different classifiers are trained to see if the 106 features can express the 6 different types of attack. For this purpose, 70% of the 1293 attacks are used to train and 30% are used to test the different algorithms. The splitting is stratified[3]. For each algorithm, 3-folds cross-validation are done to avoid overfitting. A grid search is performed on selected hyperparameters. One-vs-the-rest (OvR) multiclass/multilabel strategy is chosen. This strategy consists in fitting one classifier per class. For each classifier, the class is fitted against all the other classes. The metric "F1 score"[4] is chosen to optimize each algorithm because predicting positive cases is important.

To compare the different algorithms, the ROC (receiver operating characteristic) curve is traced and the AUC (area under curve) is calculated. The advantage of the ROC[5] curve is that it synthesizes all the confusion matrix depending on the threshold chosen to classify an attack. As our dataset is unbalanced, the micro-average ROC curve is also traced. It considers each element of the label indicator matrix as a binary prediction.

[3] For more details: `https://en.wikipedia.org/wiki/Stratified_sampling`

[4] For more details: `https://en.wikipedia.org/wiki/F1_score`

[5] For more details: `https://en.wikipedia.org/wiki/Receiver_operating_characteristic`



(a) SVC ROC curves

(b) Gradient Boosting ROC curves

Figure 4: ROC curves for both approaches

In figure 4 and in table 3, the two classifiers give satisfying results. The features express well the type of attacks which means that the type of the attack is strongly linked to the features. These classifiers could be used to predict the type of future attacks or, as mentioned above, they could be analyzed to detect underlying pattern between the labels and the attack type. However, the *Arson* and *other* attack type are more difficult to classify than the others type of attacks and for these type precaution on the result is advised.

Classifier	**F1-score**	**weighted AUC**
Super Vector Machine Classification	0.875	0.969
Gradient Boosting Tree Classification	0.872	0.973

Table 3: Results for different classifier

7 Conclusion

During this project we have seen that terrorist attacks can be described by a set of features which can be used to create a network connecting attacks sharing similarities. Even by knowing the nature of each attack, it was difficult to link the set of feature to the correct label of the attacks, should it be the type of the attack or the location of the attack. The fact that a pure network approach failed at first, indicates a complex interaction between the features and their labels. The steps taken show the importance that for a network approach to succeed, the data used needs to reflect the similarities of the labels. If this condition is met, the network approach actually yields among the best results.

With our solutions, future attacks could be classified and clustered by their type using the features without other prior knowledge. If an attack is tracked before its perpetuation and intelligence agencies or police services have access to the features, assumption could be made on how the attack will be performed. A more focused study on the labels could even allow intelligence agency to detect the underlying patterns that could help understand how terrorists act.