Predicting and visualising ATM attacks

R. Fasel and B. Regnerus
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
7500 AE Enschede, The Netherlands

I. Introduction

ATM attacks and fraud continue to make headlines. The compromise of ATMs is a very lucrative criminal business. ATMs typically exist as physical contact points of the banking infrastructure that are exposed to public sight. This makes ATMs a very accessible target for exploitation, vulnerable to a large variety of attack scenarios. The European ATM Security Team report that the amount of ATM attacks both physical- and logical attacks only increase [1], therefore securing ATMs but also predicting ATM attacks are more important than ever.

This paper describes the process of both visualising ATM attacks and predicting cases where ATM attacks could occur. The main focus of this of this research is the exploration of using tools provided in the DM- and DPV topics provided in the Data Science course. Furthermore other tools such as the Python machine learning library Scikit-learn and JavaScript data visualisation library D3.js will be used.

A. The Dataset

Provided for this project is a dataset from the European TREsPASS project [2] that was developed in collaboration with Spanish banks. The dataset contains information of 723 ATMs, attacks on those ATMs and the information about those attacks. In more detail, the dataset provides: geographical details about ATMs (such as latitude and longitude coordinates, distance to a highway), demographic details (such as per capita income, population density, median population age), logging details of the attacks per ATM, the profile of the involved attacker, the information on how much amount was recovered and when did recovery event took place.

For this research the most important features of the dataset are both the geographical- and demographical features. Those features can be used for both visualising attacks and predicting attacks using a classifier with those features as an input.

B. Research Questions

With the DataScience DM and DPV topics in mind this lead to the following research questions:

> How can a dataset containing geographical- and demographical features of ATM attacks be predicted and visualised?

This question is answered with the support of the following questions:

- How can factors that contribute to attack frequency and attacker success be plotted geographically?
- Which factors contribute most to ATM locations being attacked?
- How can ATM attacks be predicted using a Naive Bayes classifier?

II. Method

To give an accurate answer the above mentioned research questions multiple different tasks have to be conducted. The tasks have been further separated in the application of topic DPV (II-A) and the application of topic DM (II-B).

A. Application of Topic DPV

In this section we try to identify a good method for obtaining visualisation from the raw ATM attack dataset. Raw data was available in an ARFF format and a good description of each data column was also available. The data which was available was already in quite a clear format and did not need many transformations to make it available for visualisation. Therefore Pentaho Kettle was not used, instead basic transformations were performed to transform the ARFF file to a GeoJSON format using the Python language, since the data which is encoded consists of geographic data points this format seemed appropriate. For the visualisation we wanted to also show the contours of the freguesias (municipalities of Lisbon). This data was not available in the ATM attack dataset, however it was available under an Creative Commons licence from the Lisbon Open Data website [4].

Using the two GeoJSON formatted datasets a visualisation was created in Javascript using D3.js. [5] The use of the D3.js library was chosen over other tools such as Tableau since it allows for more flexibility when developing visualisations. D3.js is able to read from the GeoJSON formatted files, using them as the datasource therefore no external database warehouse, such as MySQL, was needed.

B. Application of Topic DM

A Naive Bayes (NB) classifier was created in order to predict ATM attacks. Naive Bayes classifiers provide probabilities for each class, in this case attacked or not attacked. These probabilities can be used to give an accurate prediction of the probability of an ATM attack. The Naive Bayes classifier was created using the Scikit-learn library for the Python programming language. Scikit-learn is a library that provides tools to setup, test and evaluate Machine learning algorithms. The NB classifier was trained using the data available from the European TREsPASS project [2]. The data consisted of

ATM records that described properties of the ATM and most importantly if they were attacked and how many times. The class label was extracted from the variable ”N_FREQ_ATK” which indicates if a ATM was attacked or not. Together with the class labels some features were selected from the ATM properties. These features included: ”MWay_Dist”, ”NUMBER”, ”N_INCOME”, ”N_DENSITY”, ”N_AGE”, ”N_UNP_RATE”, ”N_COM_DENS”, ”Police_Dis”.

III. Results

Following from II (the method) a visualisation was developed in D3.js (III-A) together with a machine learning model created using a Naive Bayes classification method (III-B).

A. Results of Topic DPV

The visualisation which was developed contains the outlines of the freguesias as a grey shape, on top of those shapes the ATMs are plotted geographically as black dots. ATMs which have been attacked have a red circle around them. The visualisation can be further explored by turning on- and off other visualisation layers. There can be chosen from a list of nine different features that will be visualised as circles on the map. Most prominently, the predicted attack probability can be visualised, this probability is the outcome of II-B (the Application of Topic DM) and will be further discussed in III-B (Results of Topic DM). Other features that can be displayed are, inter alia, motorway distance, or police distance. These features were all present in the ATM attacks dataset. The scale of the circles is explained by a circle legend giving the values of the corresponding circle size. The source code and full visualisation can be found on Github [3][6].

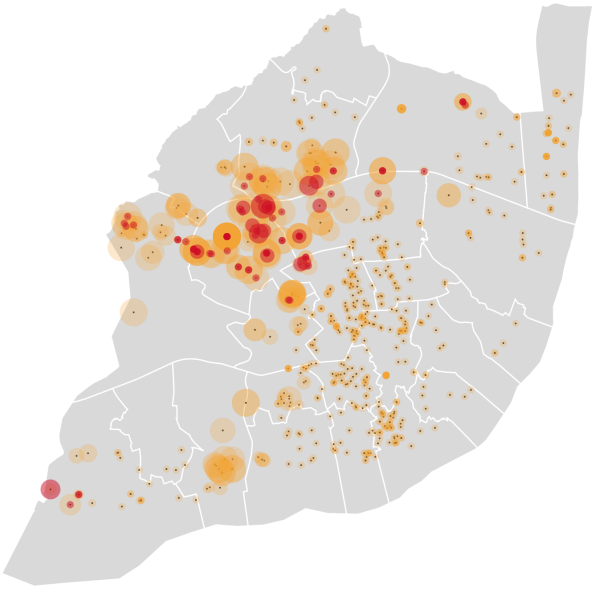

Fig. 1: Visualisation of ATM attacks (red circles), Predicted ATM attacks (orange circles) and ATM locations (black dots) on the map of Lisbon. [3]

B. Results of Topic DM

TABLE I: Performance results

	Precision	Recall	F1-score	Support
Not Attacked	1.00%	0.92%	0.96%	162
Attacked	0.59%	1.00%	0.75%	19
avg / total	0.96%	0.93%	0.94%	181

The final model described in the previous chapter was evaluated using a test set of 181 ATM locations. Table I shows the performance metric of the model on the test set. The overall accuracy was 92.82%.

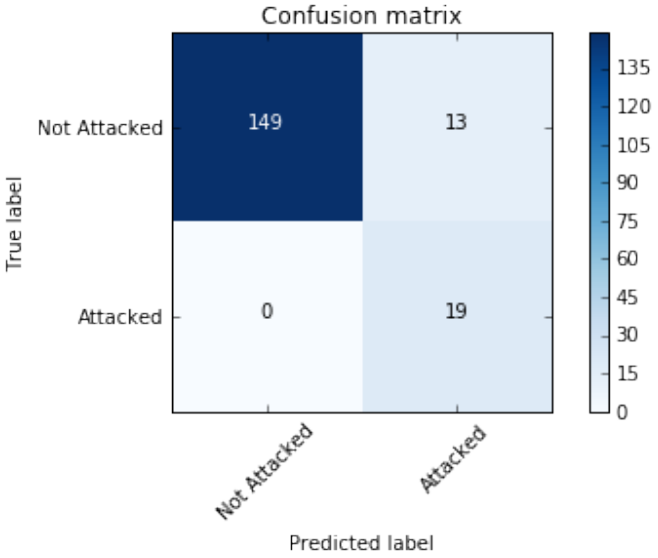

Fig. 2: Confusion matrix of the results. [3]
fig:confusion

The confusion matrix of the model on the test set can be seen in Figure **??**. It shows that the model never classified a attacked ATM as not attacked. It did however classify some ATMs that were not attacked as attacked.

TABLE II: Most Informative Features

Coef	Feature Name
-0.4678	Police_Dis
-1.0099	MWay_Dist
-5.8621	N_INCOME
-6.3765	N_UNP_RATE
-6.5414	N_DENSITY
-6.6055	N_COM_DENS
-6.6429	N_AGE
-7.2555	NUMBER

Table II show the features orderd on how informative they are. The top feature is the most informative feature. According to this table the features ”Police_Dis” and ”MWay_Dist” contribute significantly more to the prediction than the other features.

TABLE III: Example features

Feature	Example 1	Example 2	Example 3
MWay_Dist	1000	730	1480
Police_Dis	685	500	1020
N_UNP_RATE	2	2	2
N_AGE	2	2	2
N_INCOME	2	2	2
N_DENSITY	2	2	2
N_COM_DENS	2	2	2
NUMBER	2	2	2

TABLE IV: Example results

	Example 1	Example 2	Example 3
Attacked	0.0916	0.2251	0.9364
Not Attacked	0.9084	0.7749	0.0636

Some example ATMs were made to test the ability of the classifier to generate attack probabilities the results can be seen in table IV. The values for the properties of the example ATMs can be found in table III.

IV. Conclusion and Discussion

According to the results from both the data visualisation and machine learning prediction, it is possible to accurately predict locations for ATM attacks and visualise the attacks with the geographical- and demographical features provided by the ATM attacks dataset.

Since the data was labeled with latitude and longitude coordinates the visualisation created in D3.js proves that it is possible to plot attack frequency and attacker success geographically. There are however a few drawbacks from the visualisation. Since some locations, for example a bank, have multiple ATMs at the same location, the circles overlap and therefore can distort the visualisation. In addition all features are labeled to a specific ATM location, therefore some locations have a lot of demographical data available while other places have little data available.

The classifier showed to be accurate in predicting ATM attacks. The classifier had some problems with falsely classfiyng not attacked ATMs as attacked. This is however not necessarily a flaw of the classification. The Naive Bayes classifier gives a probability if the ATM was attacked or not. This probability can be very high due to the properties of the ATM but it does not mean that it was attacked just that the probability is very high but probably was not attacked due to chance. This means that police departments can still use the classifier but not to predict where ATM attacks are going to happen. Instead they can use it to identify areas that have a high attack risk in order to improve them.

The properties that contribute the most to the prediction are ”Police_Dis” and ”MWay_Dist. These results are also quite intuitive. One can easily understand why a criminal does not attack a ATM very near to a police station or why a criminal prefers to attack a ATM close to a motorway in order to escape quickly. Police departments can use these insights in order to decrease the probability of an attack by changing these important properties.

Further research should be done to optimise the machine learning model even further. More datasources could be sourced as input features for the model. Furthermore there could be experimented with other types of classifiers to further improve the classification.

References

[1] European ATM Crime Report Archives — European ATM Security Team, European ATM Security Team. [Online]. Available: https://www.european-atm-security.eu/tag/european-atm-crime-report/. [Accessed: 13-Apr-2017]

[2] The TREsPASS Project. [Online]. Available: https://www.trespass-project.eu. [Accessed: 13-Apr-2017]

[3] ATM Attacks. [Online]. Available: https://regnerus.github.io/atm-attack-data-visualisation/. [Accessed: 13-Apr-2017]

[4] Cmara Municipal de Lisboa - Organisationer - Portal Dados Abertos. [Online]. Available: http://dados.cm-lisboa.pt/sv/organization/camara-municipal-de-lisboa. [Accessed: 14-Apr-2017]

[5] M. Bostock, D3.js - Data-Driven Documents. [Online]. Available: https://d3js.org/. [Accessed: 14-Apr-2017]

[6] regnerus, regnerus/atm-attack-data-visualisation, GitHub. [Online]. Available: https://github.com/regnerus/atm-attack-data-visualisation. [Accessed: 14-Apr-2017]

V. Appendix

Both the visualisation and data mining projects are available on Github.

The data mining approach and can be viewed as a Python Jupyter Notebook file: https://github.com/regnerus/atm-attack-data-visualisation/blob/master/datamining/DM.ipynb.

The visualisation created in D3 can be viewed as source code or as live visualisation: https://regnerus.github.io/atm-attack-data-visualisation/.