Support Vector Machine for Network Intrusion and Cyber-Attack Detection

K. Ghanem[1], F. J. Aparicio-Navarro[2], K. G. Kyriakopoulos[1], S. Lambotharan[1], and J. A. Chambers[2]

[1]Loughborough University, [2]Newcastle University

e-mail: {k.ghanem, k.kyriakopoulos, s.lambotharan}@lboro.ac.uk & {francisco.aparicio-navarro, jonathon.chambers}@ncl.ac.uk

Introduction

In cybersecurity, the use of **Support Vector Machine (SVM)** [1] can improve the accuracy of Network **Intrusion Detection Systems (IDSs)**. The classifier that is created by this technique is useful to predict between malicious and benign network traffic.

The study of SVM in tasks of intrusion detection would allow us to identify a technique that could be used as a second line of detection, and to facilitate the creation of a benchmark to compare the performance of our IDS against.

The **aims** of this work are:

- To evaluate which of the SVM techniques produces the best detection results.
- To assess the performance of our unsupervised anomaly-based IDS [2] against one-class and two-class SVMs in intrusion detection tasks.

Support Vector Machine

An SVM finds the optimal separating hyperplane via maximising the margin between classes of data.

- **Linear SVM**

A linear SVM assumes that the different classes in the dataset are clearly distinguishable.

- **Non-Linear SVM**

In data with no possibility for linear separation, an non-linear SVM uses kernel functions to change the non-linear approach into a linear one by projecting the data into a dimensional feature space to allow the separation.

- **One-Class SVM**

Semi-supervised technique that constructs the classification model using only one type of samples. Uses an implicit transformation to project the data into a higher dimensional space:

The SVM-based classifier presented in this work has been developed based on Matlab and *LibSVM* [3].

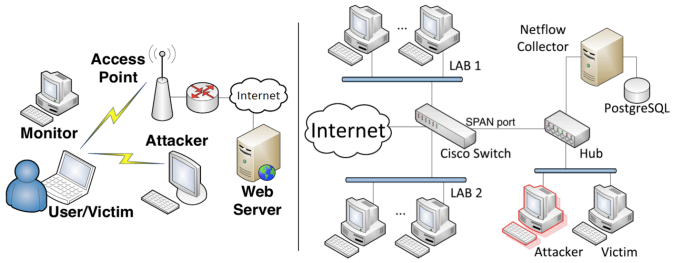
Results

- Two-class SVM trained using 35% of each dataset, and classification conducted using the remaining 65% of the dataset.
- One-class SVM trained using 100% of the dataset *Normal*, and classification conducted using 100% of the remaining datasets.
- Unsupervised anomaly-based IDS [2] based on independent statistical approaches and a cross-layer architecture.

Network Traffic Datasets

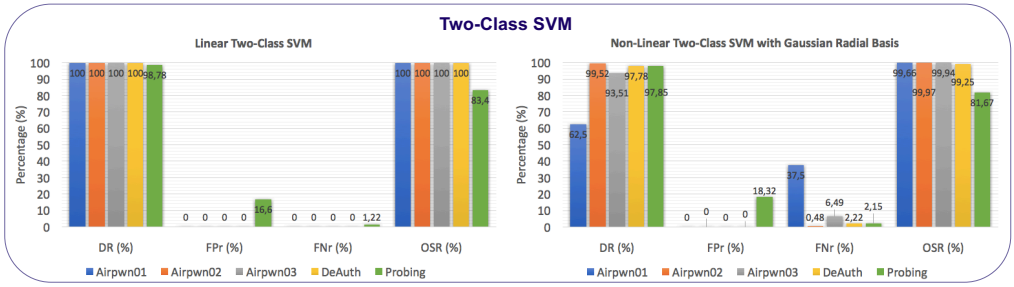
Five datasets gathered from an IEEE 802.11 network testbed comprising different types of **Injection Attacks**: Airpwn & Deauthentication Attacks [4].

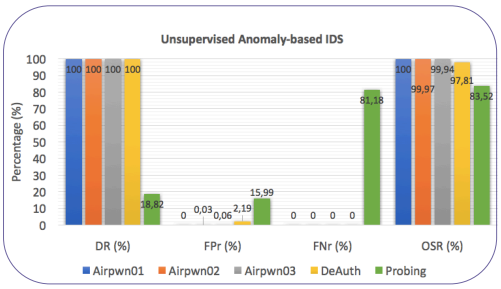
One dataset gathered from an Ethernet Local Area Network (LAN) comprising different modes of **Port Scanning Attacks** [5].

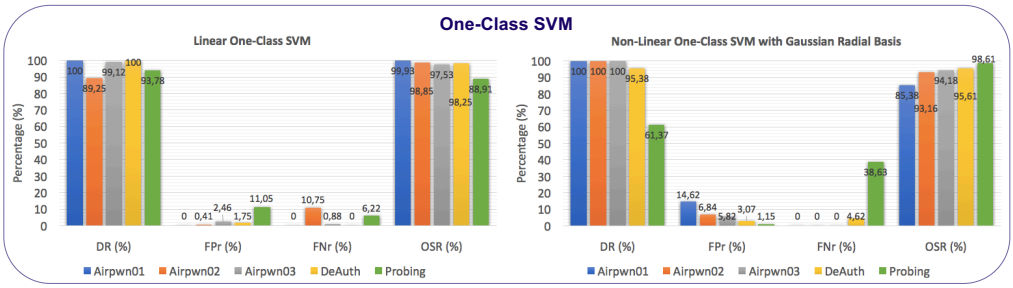


- *Normal*: Comprises non-malicious network traffic only.
- *Airpwn01*: Attacker injects crafted HTML code and replaces the HTTP headers fields of a requested website.
- *Airpwn02*: Attacker injects crafted HTML code and replaces the images in a requested website.
- *Airpwn03*: Comprises the two modes of the Airpwn attack.
- *DeAuth*: Attacker injects deauthentication frames using the MAC address of the legitimate wireless Access Point.
- *Probing*: Comprises traces of a Port Scanning Attack.

Dataset	Total Instances	Normal Instances	Normal Instances (%)	Malicious Instances	Malicious Instances (%)
Normal	3631	3631	100	n/a	n/a
Airpwn01	1361	1350	99.2	11	0.8
Airpwn02	14493	13498	93.1	995	6.9
Airpwn03	12130	12016	99.1	114	0.9
DeAuth	228	164	71.93	64	28.07
Probing	700484	696638	99.4	4220	0.6







Conclusions

- Linear two-class SVM is the most accurate technique. However, linear one-class SVM performs comparably well without labelled training datasets.
- The accuracy of the unsupervised anomaly-based IDS [2] is comparable to the detection results generated by the two linear SVM techniques. This is due to the benefits of the cross-layer architecture.
- In cases where a non-homogeneous dataset (i.e. metric values are very variable) is analysed (e.g. *Probing*), our anomaly-based IDS could benefit from the use of SVM techniques to increase its detection accuracy.

References

[1] C. J. Burges, "A tutorial on support vector machines for pattern recognition," in *Data mining and knowledge discovery*, vol. 2, no. 2, 1998, pp. 121-167.

[2] K. G. Kyriakopoulos, F. J. Aparicio-Navarro, D. J. Parish, "Manual and automatic assigned thresholds in multi-layer data fusion intrusion detection system for 802.11 attacks," in *IET Information Security*, vol. 8, no. 1, 2014, pp.42-50.

[3] C.-C. Chang, and C.-J. Lin, "LibSVM: A library for support vector machines," 2001. Available: http://www.csie.ntu.edu.tw/~cjlin /libsvm.

[4] K. G. Kyriakopoulos, and F. J. Aparicio-Navarro, "Man-In-the-Middle, De-authentication and Rogue AP Attacks in 802.11 networks," 2017, Available: https://figshare.com/s/4bd0fe2dab7e09ce61dc.

[5] K. G. Kyriakopoulos, and F. J. Aparicio-Navarro, "Network Traffic with Port Scanning Attack," 2017, Available: https://figshare.com/s/4bd0fe2dab7e09ce61dc

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) Grant number EP/K014307/2 and the MOD University Defence Research Collaboration in Signal Processing, and the British Council.