SDN DDOS ATTACK IMAGE DATASET

DESCRIPTION

It is now widely known fact that the Cloud computing and Software defined network paradigms have received a wide acceptance from researchers, academia and the industry. But the wider acceptance of cloud computing and SDN paradigms are hampered by increasing security threats. One of the several facts is that the advancements in processing facilities currently available are implicitly helping the attackers to attack in various directions. For example, it is visible that the conventional DoS attacks are now extended to cloud environments as DDoS attacks. With a huge number of security threats that are continuously occurring in computer networks and environments such as software defined networks (SDN) and Cloud computing, there is a demand to address security solutions that have a better reliability when compared to existing security solutions that are designed by considering datasets that did not meet the assessment and evaluation criterion which must be considered during the design of IDS systems.

In [2], Nisha Ahuja, Gaurav Singal, and Debajyoti Mukhopadhyay have generated DDoS attack dataset for Software Defined Networks. This dataset was generated using mininet emulator. The dataset is available in the form of csv file(.csv) . The original version of dataset consists of 104345 traffic instances defined over 23 features.

For evaluating performance of ML and DL based Intrusion Detection System, we have converted the DDOS attack SDN Dataset [3] in csv format to SDN DDoS attack image dataset consisting of network traffic image instances. Each traffic image instance in SDN DDoS attack image dataset is of 5x5 pixel size.

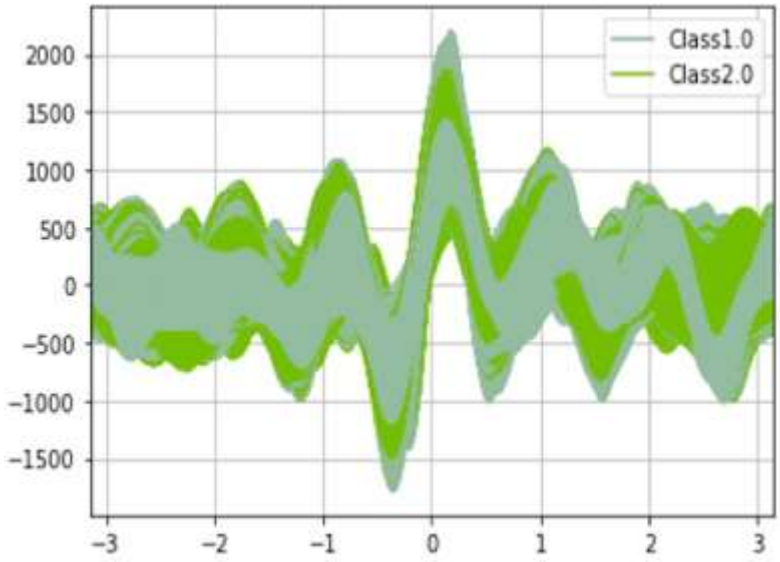

Figure 1: Plot of Andrew Curve showing non-linearity of the feature space for SDN DDoS Dataset.

Andrews curves are plotted for the SDN DDoS attack image dataset as shown in Figure 1. From Figure 1, we can understand that the dataset is highly non-linear in nature. Here, class1.0 represents normal traffic and class2.0 represents the attack.

Figure 2 shows plot of Andrew curve after dimensionality reduction with number of feature dimensions equal to 6 . It can be seen from Figure 2 , that the overlapping is slightly reduced after dimensionality reduction. But still there is high non-linearity.

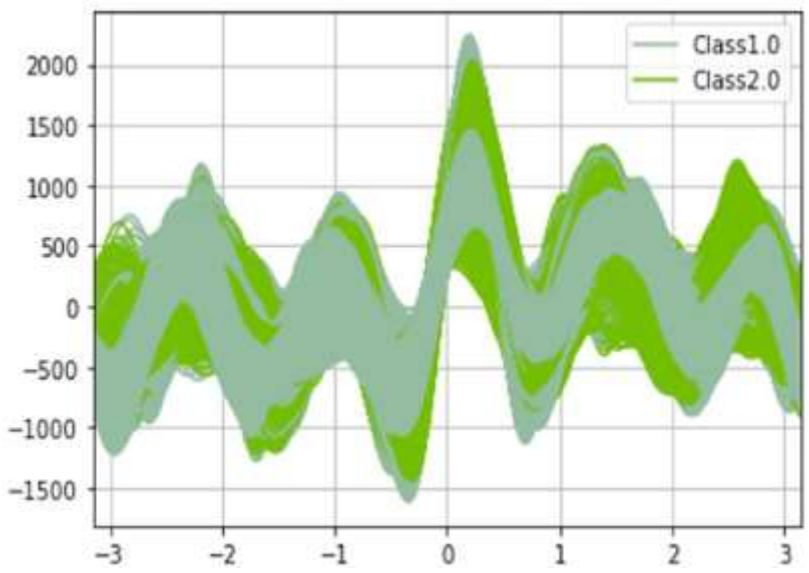

Figure 2: Plot of Andrew Curve showing non-linearity of the feature space for the dimensionality reduced SDN DDoS Dataset.

Acknowledgements

This dataset is created as part of ongoing research study to build better ML and DL models for the design of efficient IDS for SDN, Cloud and IoT. We thank the contributors Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay for making the original version of dataset which also helped in carrying this research.

References

1. Swathi Sambangi and Lakshmeeswari Gondi. 2021. Multiple Linear Regression Prediction Model for DDOS Attack Detection in Cloud ELB. In *The 7th International Conference on Engineering & MIS 2021 (ICEMIS'21), October 11–13, 2021, Almaty, Kazakhstan*. ACM, New York, NY, USA 9 Pages. https://doi.org/10.1145/3492547.3492567
2. Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, Debajyoti (2020), "DDOS attack SDN Dataset", Mendeley Data, V1, doi: 10.17632/jxpfjc64kr.1
3. https://data.mendeley.com/datasets/jxpfjc64kr/1