A network intrusion detection system based on DBN

Weizhi CHEN, Yuyan WANG, Zehao LI

Tsinghua-Berkeley Shenzhen Institute, Tsinghua University

Abstract

- Security threats for computer networks have increased, raising a great need for an effective Intrusion Detection System (IDS) to interpret the intrusion attempts in incoming network traffic.
- Propose a system based on deep belief network to detect these attacks.
- The network is trained upon the CICIDS2017 dataset, and several class balancing techniques is applied and evaluated.

Introduction

- The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators.
- In this project, we design a new intrusion detection system with Deep Belief Network that will addresses such challenges.
- Our model improve the detection performance against infrequent attack samples whilst retaining a high performance against the rest of the attacks.

Method

The dataset is highly imbalanced, with most of its samples labelled as benign. So network trained on it will inevitably bias in favor of the majority class (benign).

For data pre-processing, we implement Synthetic Minority Over-sampling Technique (SMOTE)[1] and Class Weight Strategy[2] to address the minority class issue.

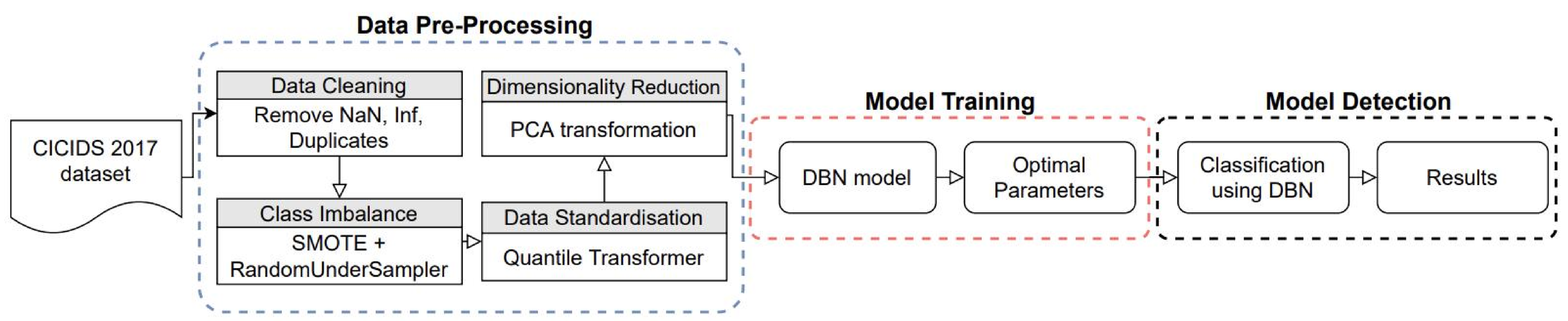

Fig 1. Architecture of our NIDS

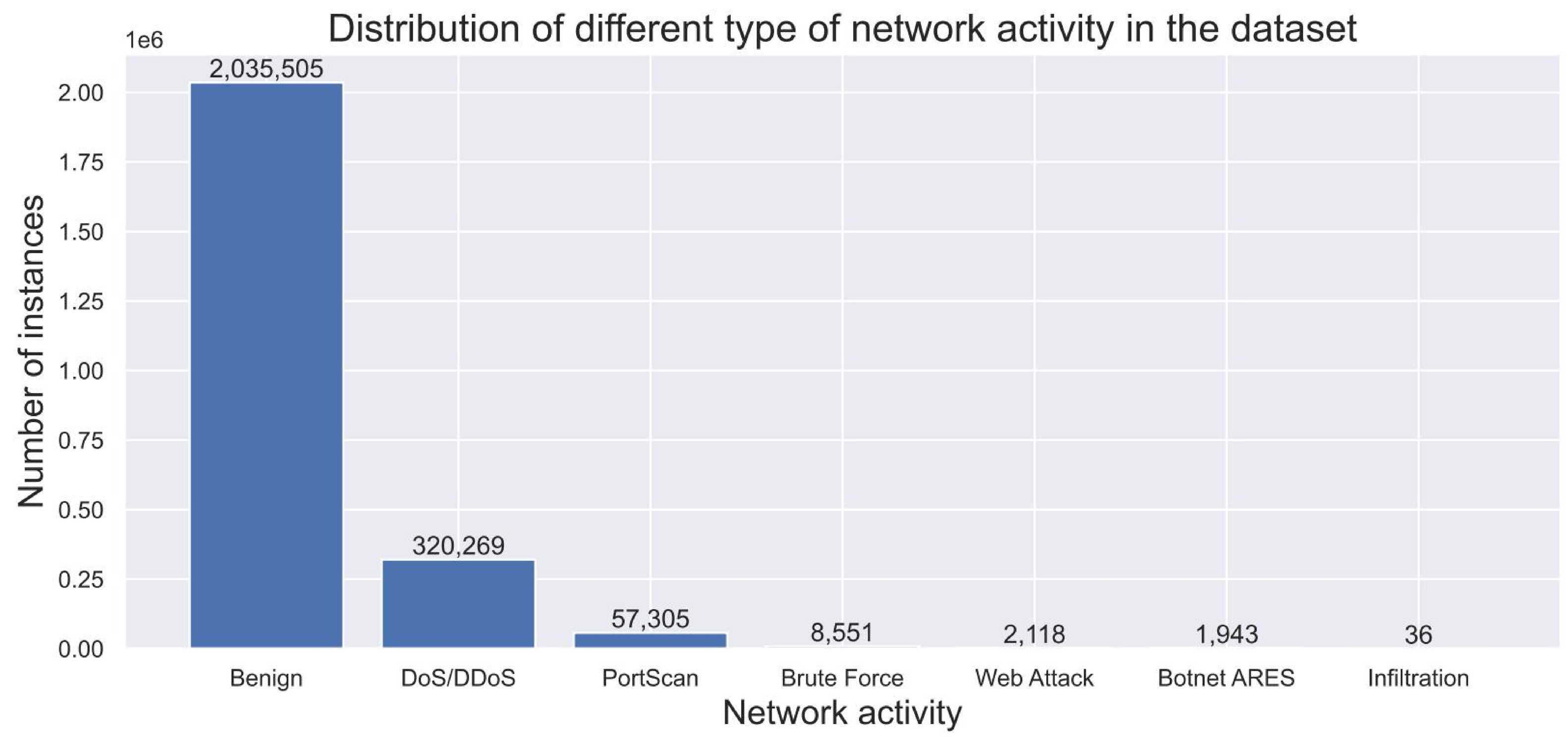

Fig 2. Distribution of network activity in the dataset

- A Deep Belief Network composed of stacks of RBMs is employed.

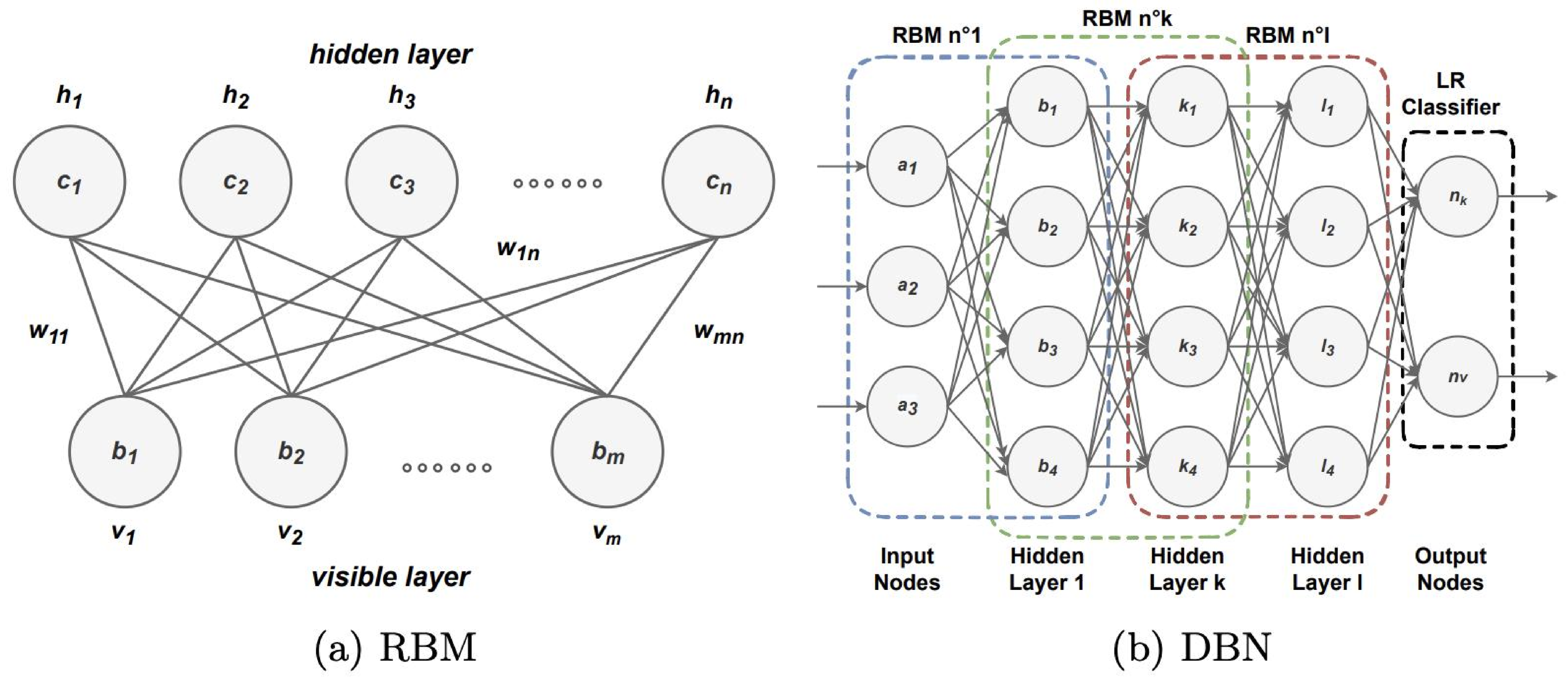

Fig 3. DBN architecture

Results

	precision	recall	f1-score	support
Benign	0.99	1.00	1.00	407115
Botnet ARES	0.00	0.00	0.00	398
Brute Force	1.00	0.16	0.28	1672
DoS/DDoS	1.00	0.99	0.99	64142
PortScan	0.00	0.00	0.00	8
Web Attack	0.96	1.00	0.98	11346
Infiltration	0.00	0.00	0.00	464

Table 1. Detection Precision

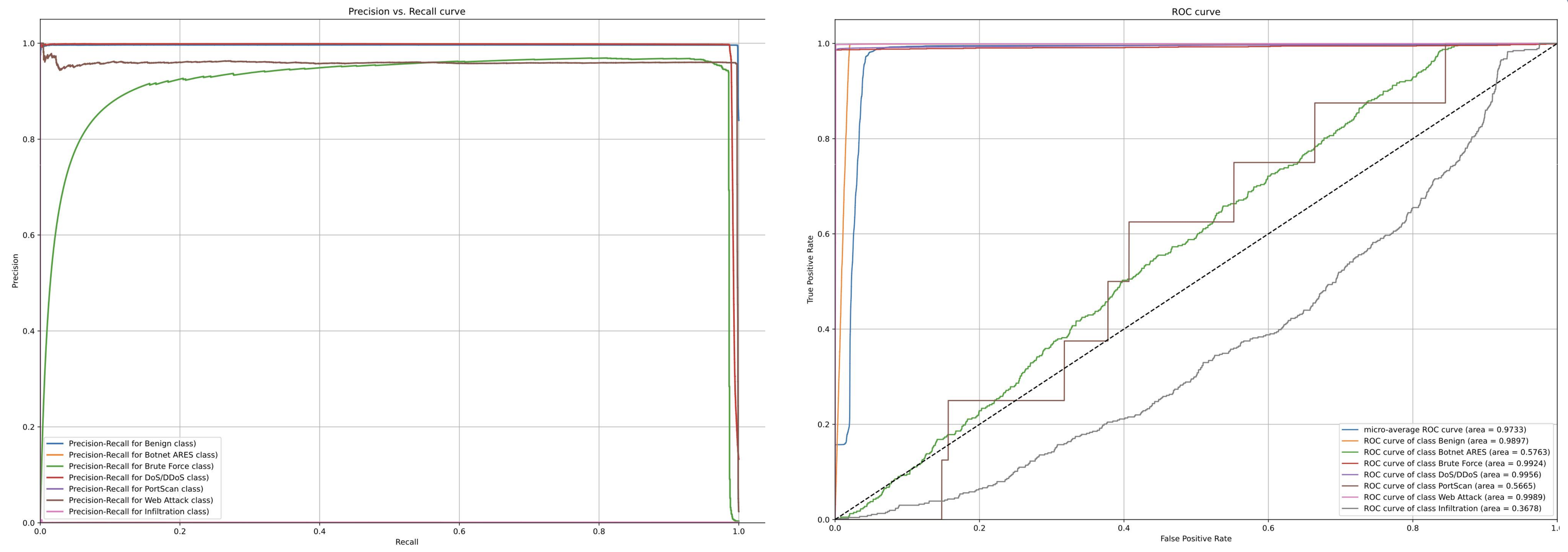

Fig 4. Precision&Recall Curve, ROC curve

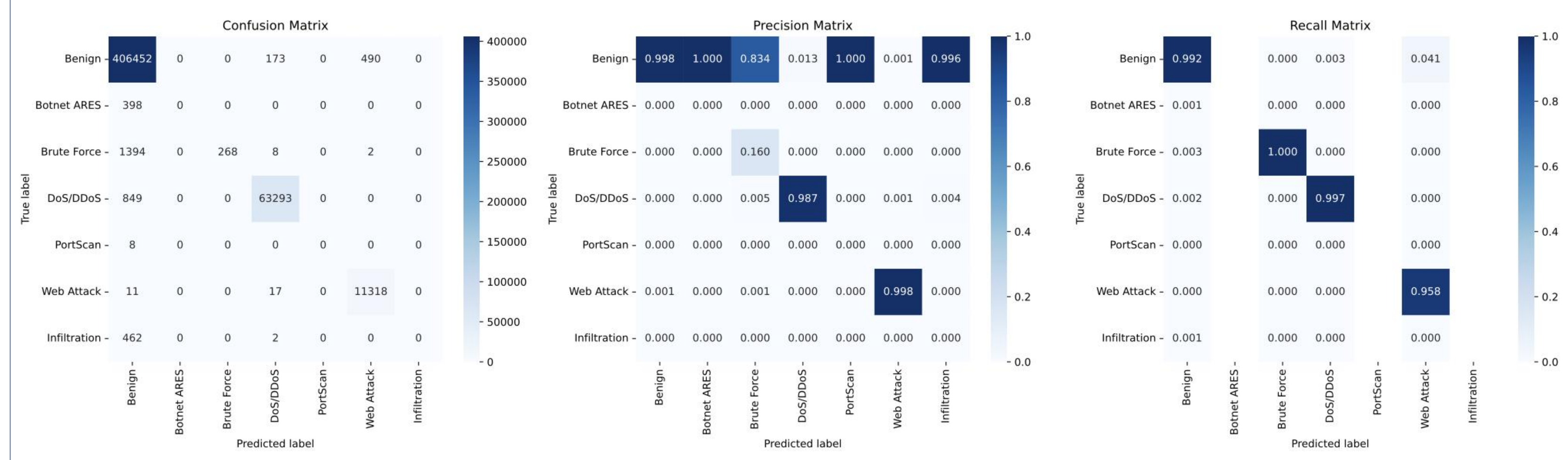

Fig 5. Test Confusion Matrix

- For major class like benign, DoS/DDoS, F1-score reaches nearly 1.00.
- Training only takes 30 minutes on Apple M2 CPU.
- After utilizing SMOTE, class Botnet with only 1672 samples reaches precision of 1 and F1-score of 0.28

Conclusions

- The final F1-score reaches 0.99, indicating that most attacks are detected.
- The technique of SMOTE enables the system to detect certain minor classes. More can be done on improving the system's capability to detect minor classes.
- Our system is based upon a centralized network, a distributed approach might be necessary.

References

[1] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer. SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 16:321–357, June 2002.

[2] Shoujin Wang, Wei Liu, Jia Wu, Longbing Cao, Qinxue Meng, and Paul J. Kennedy. Training deep neural networks on imbalanced data sets. In 2016 International Joint Conference on Neural Networks (IJCNN), pages 4368–4374, July 2016. ISSN: 2161-4407.