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.



/ww.PosterPresentations.co

A network intrusion detection system based on DBN

Weizhi CHEN, Yuyan WANG, Zehao LI

Tsinghua-Berkeley Shenzhen Institute, Tsinghua University

Model Detection Classification Results using DBN



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

				Conf	fusion M	atrix							Prec	ision M	atrix							Re	call Mat	rix			
	Benign -	406452	0	0	173	0	490	0	- 400000	Benign -	0.998	1.000	0.834	0.013	1.000	0.001	0.996	- 1.0	Benign -	0.992		0.000	0.003		0.041		- 1.0
	Botnet ARES -	398	0	0	0	0	0	0	- 350000	Botnet ARES	- 0.000	0.000	0.000	0.000	0.000	0.000	0.000	- 0.8	Botnet ARES -	0.001		0.000	0.000		0.000		- 0.8
-	Brute Force -	1394	0	268	8	0	2	0	- 250000	Brute Force	- 0.000	0.000	0.160	0.000	0.000	0.000	0.000	- 0.6	Brute Force -	0.003		1.000	0.000		0.000		- 0.6
True labe	DoS/DDoS -	849	0	0	63293	0	0	0	- 200000	True labe DoS/DDoS	- 0.000	0.000	0.005	0.987	0.000	0.001	0.004		ade DoS/DDoS - True labe	0.002		0.000	0.997		0.000		
	PortScan -	8	0	0	0	0	0	0	- 150000	PortScan	0.000	0.000	0.000	0.000	0.000	0.000	0.000	- 0.4	PortScan -	0.000		0.000	0.000		0.000		- 0.4
	Web Attack -	11	0	0	17	0	11318	0	- 100000	Web Attack	- 0.001	0.000	0.001	0.000	0.000	0.998	0.000	- 0.2	Web Attack -	0.000		0.000	0.000		0.958		- 0.2
	Infiltration -	462	0	0	2	0	0	0	- 50000	Infiltration -	0.000	0.000	0.000	0.000	0.000	0.000	0.000		Infiltration -	0.001		0.000	0.000		0.000		
		Benign -	Botnet ARES -	Brute Force -	DoS/DDoS -	PortScan -	Web Attack -	Infiltration -	- 0		Benign -	Botnet ARES -	Brute Force -	DoS/DDoS -	PortScan -	Web Attack -	Infiltration -	- 0.0		Benign -	Botnet ARES -	Brute Force -	- DoS/DDoS -	PortScan -	Web Attack -	Infiltration -	- 0.0
Predicted label											Predicted label								Predicted label								

Fig 5. Test Confusion Matrix

- reaches nearly 1.00.

Conclusions

- attacks are detected.
- distributed approach might be necessary.

[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.

• For major class like benign, DoS/DDoS, F1-score

• 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

• The final F1-score reaches 0.99, indicating that most

• 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

References