Intrusion Detection System Using Deep Learning

-Keerthi Kumar S (1811EE06)
-Mandeep Rathee (1811MC07)
-Sandip Kishore (1711CS12)

Outline

- What is IDS?
- Motivation
- Dataset
- Preprocessing
- Our Model
- Results
- Future Work

What's Intrusion ??

- **Precursor** of more complicated attacks – Technical and non-technical – Severe

- **Network attacks** - hog the network resources
  - Bandwidth, memory, CPU resource of the server etc.

- Results in degraded service or denied of the available service – **DoS & DDoS**

- DDoS - Difficult to characterize and eliminate

- **Evolving techniques**
  - Challenging to detect DDoS attack – Needs adaptability

What's IDS

System to forewarn Network Admins about malicious behaviors

– intrusions, attacks, and malware

Mandatory line of defense to protect critical networks against these ever-increasing issues of intrusive activities

IDS – High Level Taxonomy

McAfee Report 2016

- Brute Force Attack
- Heartbleed Attack
- Botnet
- DoS Attack
- DDoS Attack
- Web Attack
- Infiltration Attack

Motivation – Why IDS for this project??

- IIT Patna - Large Campus Network – around 8000 nodes – more than 1000 concurrent users – Data usage in TB per day
- Liberal approach ICT policy
- Firewall and enterprise security device– handle outbound and inbound traffic
- Need to analyze the campus traffic – validate the filtering and security provided by firewalls and security equipments
- Currently signature based not anomaly based
  - Will be obsolete - Evolving attack paradigms

Challenges

- Difficulty in getting reliable training data
- Behavioral dynamics & patterns
- Volume of data
- Diversity, heterogeneous environment and equipment – adaptability
- Low frequency attacks
- Test data preprocessing

The Data Set

- CICIDS2017 - https://www.unb.ca/cic/datasets/ids-2017.html
- Latest available data set – addresses short coming of currently available other IDS data sets like KDD Cup 1999 and NSL KDD 2009
- The generated attack diversity includes the most common attacks based on the 2016 McAfee report
- Around 80 network flow features
- In this project we are using 78 flow features

Story of the Data set

- **Benign Profile agent – B- Profile System**
  - responsible for profiling the abstract behavior of human interactions
    - Generate a naturalistic benign background traffic
  - tries to encapsulate network events produced by users with machine learning and statistical analysis techniques.

  - encapsulated features are distributions of packet sizes of a protocol, the number of packets per flow, certain patterns in the payload, the size of the payload etc

Story of the Data set

Time slot based Attack Profile and scenarios

Days	Labels
Monday	Benign
Tuesday	BForce,SFTP and SSH
Wednes.	DoS and Hearbleed Attacks slowloris, Slowhttptest, Hulk and GoldenEye
Thurs.	Web and Infiltration Attacks Web BForce, XSS and Sql Inject. Infiltration Dropbox Download and Cool disk
Friday	DDoS LOIT, Botnet ARES, PortScans (sS,sT,sF,sX,sN,sP,sV,sU, sO,sA,sW,sR,sL and B)

Story of the Data set

- **RandomForestRegressor**
  - to select the best short feature set for each attack
- **Performance and accuracy**
  - of the selected features verified with seven common machine learning algorithms
- **Evaluate the quality of the generated dataset**
  - based on the 11 criteria from the last proposed dataset evaluation framework by Canadian Institute for Cybersecurity (CIC)(Sharafaldin et al., 2017).

Story of the Data set

Category	Number of Samples
BENIGN	2273097
FTP-Patator	7938
SSH-Patator	5897
DoS-Slowloris	5796
DoS-Hulk	231073
DoS-Slowhttptest	5499
DoS-GoldenEye	10293
Heartbleed	11
Web Attack-XSS	652
Web Attack-Sql Injection	21
Brute Force	1507
Infiltration	36
Bot	1966
DDoS	128027
PortScan	158930

What’s been done in IDS??

N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, ”A Deep Learning Approach to Network Intrusion Detection,” in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018

- Used Non-Symmetric deep auto encoder
- Used old KDD Cup 99 and NSL KDD 2009 data set

What’s been done in IDS??

C. Yin, Y. Zhu, J. Fei and X. He, ”A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks”, in IEEE Access, vol. 5, pp. 21954-21961, 2017

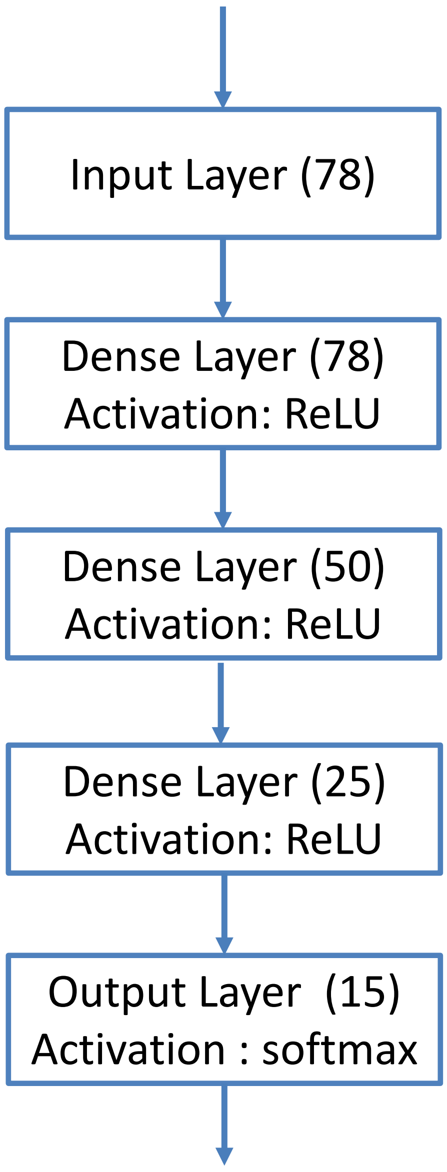
- NSL KDD 2009 data set (41 features, 3, 5 or 13 class)

The recipe - Preprocessing

- Handling NaN – replace with 0
- Handling Infinity – replace by large value
  – 3.4028235e+38
- Dynamic range compression – using log
- Normalize – (x-min)/(max-min)
  – Values between 0 and 1

Our Model

- **Model Summary: DNN**
  - Input Layer : 78 inputs
  - 3 Hidden Layers : 78, 50 and 25 neurons
  - Output Layer : 15 neurons
  - 11,777 trainable parameters



Our Model

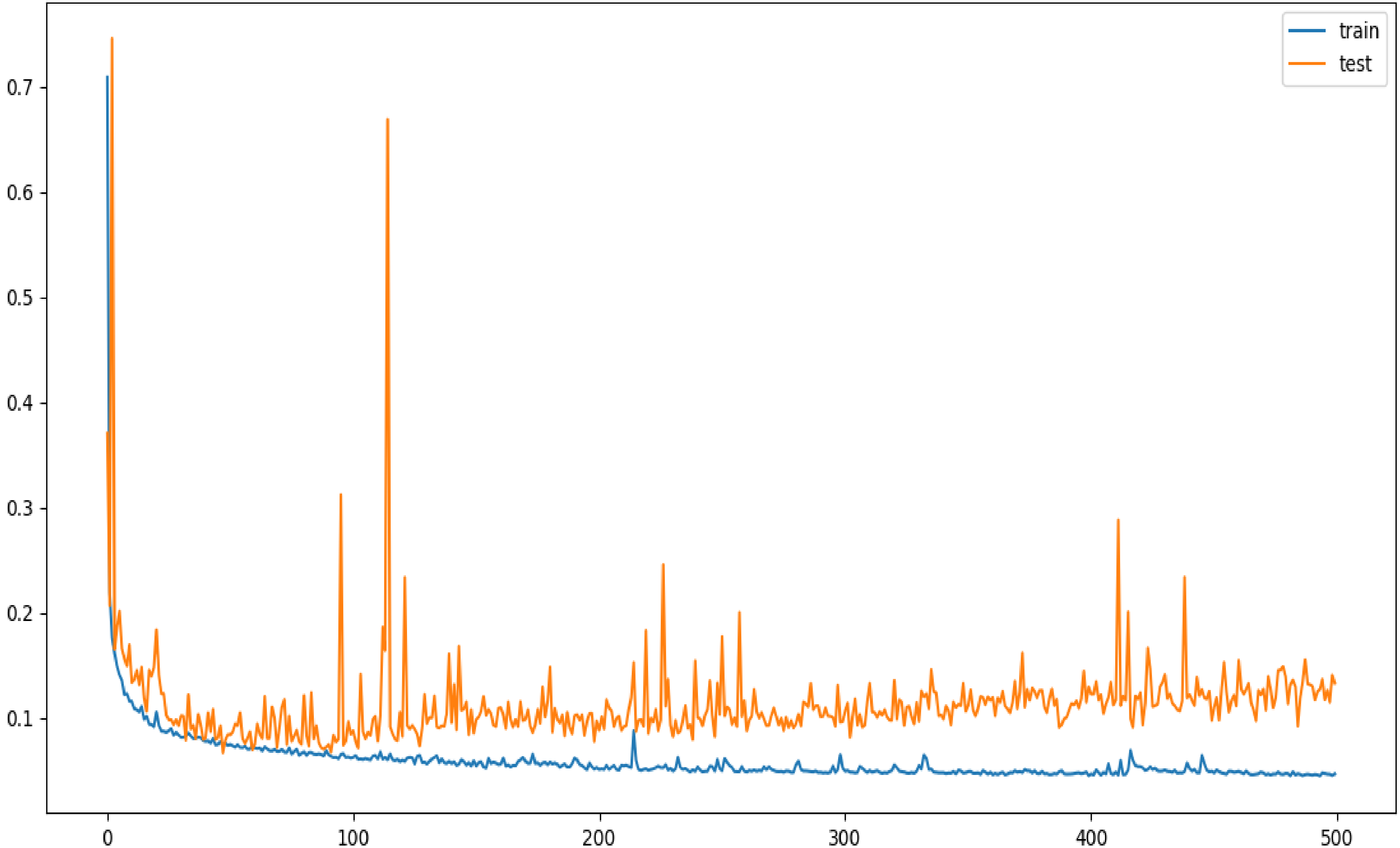
- **Activation Functions**
  - Hidden Layers- ReLU
  - Output Layer – softmax

- **Loss Function : Categorical crossentropy**

$$-\frac{1}{N}\sum_{i=1}^{N}\log(p_i)$$

- **Optimizer : SGD**
  - Learning rate : 0.1

Loss v/s Epoch curve



**L
o
s
s**

No. of Epochs

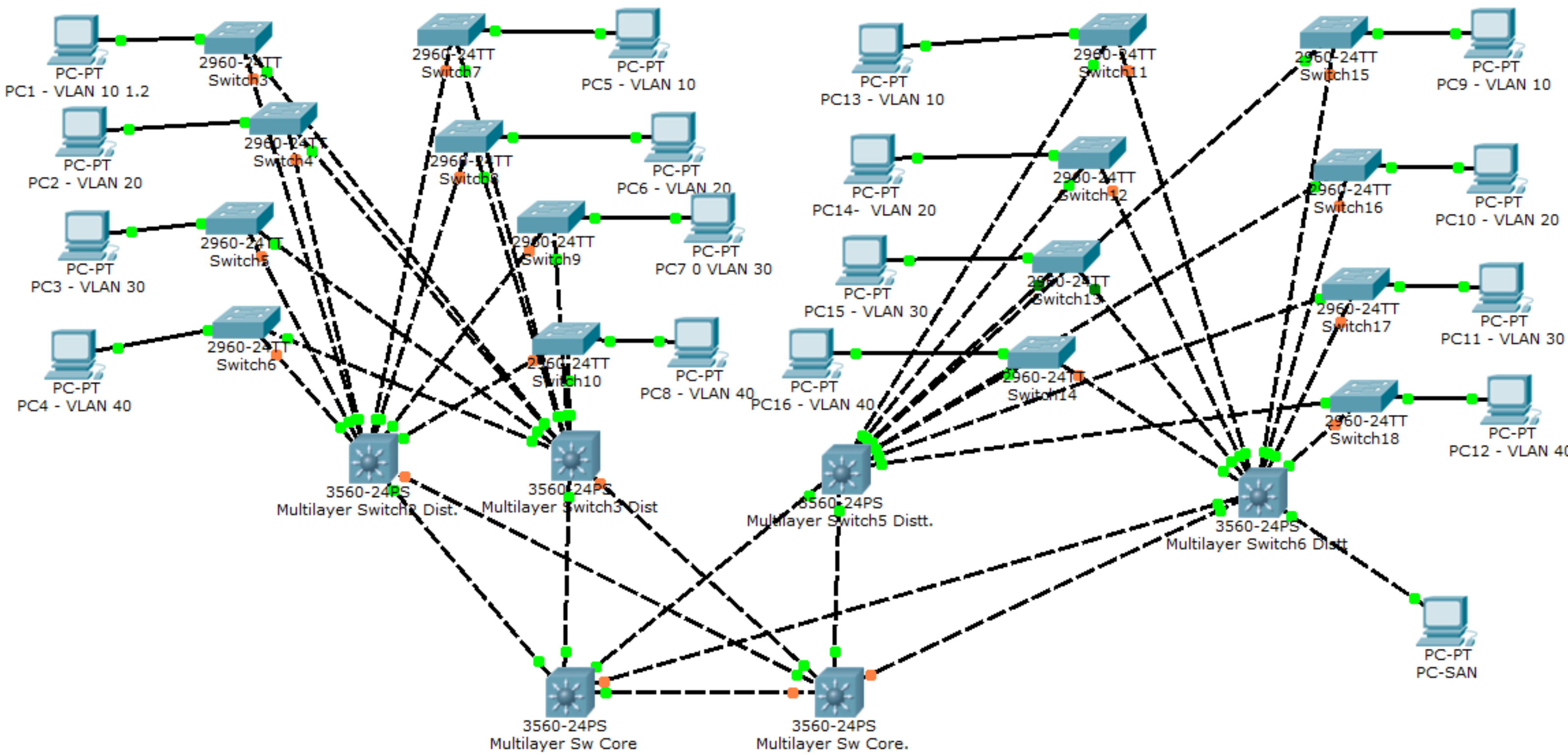
Our Model – Train and Test data

- Oversampling the classes with less samples
  - Affects the accuracy of BENIGN class
- **Train-Test Split**
  - From each of the negative classes with N samples, the number of test samples (N_test) were chosen using: N_test = min(1000,(0.5*N))
  - Rest of the samples were used for the training data along with 528911 BENIGN samples
  - Combined the negative test samples with the live BENIGN traffic to obtain the test samples

Train Test samples

Category	Training samples	Test Samples
BENIGN	528911	22501
FTP-Patator	6938	1000
SSH-Patator	4897	1000
DoS slowloris	4796	1000
DoS Slowhttptest	230073	1000
DoS GoldenEye	4499	1000
DoS Hulk	9293	1000
Heartbleed	6	5
Web Attack XSS	352	300
Web Attack Sql Injection	11	10
Web Attack Brute Force	1007	500
Infiltration	21	15
Bot	966	1000
PortScan	127027	1000
DDoS	157930	1000
Total	1076727	32331

Live Topology



Results

- **Confusion matrix**

22501	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	993	6	0	0	0	0	0	0	0	1	0	0	0	0
1	2	997	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	988	1	2	0	0	0	0	5	0	0	0	0
1	0	0	71	928	0	0	0	0	0	0	0	0	0	0
23	0	32	0	2	943	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	998	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	4	0	0	0	0	0	0	0
1	0	0	0	0	3	0	0	16	0	280	0	0	0	0
1	0	1	0	0	4	0	0	0	0	4	0	0	0	0
5	0	0	0	0	3	1	0	1	0	490	0	0	0	0
11	0	0	0	0	0	0	0	0	0	3	1	0	0	0
335	0	0	0	0	0	0	0	0	0	0	0	665	0	0
3	0	0	0	0	3	1	0	6	0	73	0	0	906	8
3	0	0	0	1	7	0	0	0	0	0	0	0	6	983

Average accuracy : 97.16%

Classification Report

Category	Precision	Recall	F1 Score	Support
BENIGN	0.98	1.00	0.99	22501
FTP-Patator	1.00	0.99	1.00	1000
SSH-Patator	0.96	1.00	0.98	1000
DoS slowloris	0.93	0.99	0.96	1000
DoS Slowhttptest	1.00	0.93	0.96	1000
DoS GoldenEye	0.98	0.94	0.96	1000
DoS Hulk	1.00	1.00	1.00	1000
Heartbleed	1.00	0.80	0.89	5
Web Attack XSS	0.70	0.05	0.10	300
Web Attack Sql Injection	0.00	0.00	0.00	10
Web Attack Brute Force	0.57	0.98	0.72	500
Infiltration	1.00	0.07	0.12	15
Bot	1.00	0.67	0.80	1000
PortScan	0.99	0.91	0.95	1000
DDoS	0.99	0.98	0.99	1000

Binary Classification-Results

- Confusion matrix

	BENIGN	Attack
BENIGN	22501	0
Attack	391	9439

Average accuracy : 98.79%

- Classification Report

	Precision	Recall	F1-Score
BENIGN	0.98	1.00	0.99
Attack	1.00	0.96	0.98

Future Extension

- CNN
- RNN
- SMOTE
- LIVE data generation with attacks

USP

- Real world DL based problem modelling
- Use of latest dataset;
  - no standard reference of its use for DL.
- Identification of novel, advanced and near real-world simulator based architecture
  - generate realistic and comprehensive dataset.
- Potential to evaluate existing signature based methods for efficiency and performance.
- Potential to become foundation for more advanced game theoretic approach based IDS.

References

- Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

- N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, ”A Deep Learning Approach to Network Intrusion Detection,” in IEEE Transactionson Emerging Topics in Computational Intelligence, vol.2, no.1, pp.41-50, Feb.2018.

- C. Yin, Y. Zhu, J. Fei and X. He, ”A Deep Learning Approach for Intrusion Detection Using RecurrentNeural Networks”, in IEEE Access, vol. 5, pp. 21954-21961, 2017

- https://www.unb.ca/cic/datasets/ids-2017.html

Thank You…