**Herding Pseudocode**

|  |
| --- |
| : Classes that was trained during task .  For in do  # Get all training instance of class  # Extract feature using feature extractor |

# Chapter 4: Experimental Evaluation

## 4.1. Benchmark Datasets

## 4.3. Implementation Details

Initial epoch: 300

Next epoch: 300

Exemplar size: 2000 instances

Learning rate: 0.001

Variable

Number of classes in datasets: num\_classes

Number of classses in each task: classes\_per\_task. In my experiments, I set classes\_per\_task = 2

Number of of tasks: num\_tasks = [num\_classes / classes\_per\_task] + 1

Pseudo code

### 4.3.1 Data Preprocessing

### 4.3.2. Exemplar setting

We use the same exemplar setting as mentioned. The exemplar size I use is 2000 instances.

Task 1 have 2 class in exemplar and 1000 instances each.

Task 2 have 4 class in exemplar and 500 instances each.

A graph of a bar

Description automatically generated with medium confidence

### 4.3.3. Model Architecture

In my experiment, with feature extractor I use a simple neural network with 4 layers. The neural net include nn.Linear(128) -> nn.Relu() -> nn.Linear -> nn.Relu()

**Feature extractor**

Target

Input

### 4.3.4. Loss Implementation

Setup

KDD99 dataset

Initial epoch: 300

Next epoch: 300

Exemplar size: 2000 instances

Learning rate: 0.001

KDD99 data setup

Finetune setup

Number of tasks: 6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| normal. | 77931 / 19347 | 0/ 19347 | 0/ 19347 | 0/ 19347 | 0 / 19347 | 0 / 19347 |
| neptune. | 85937 / 21264 | 0 / 21264 | 0 / 21264 | 0 / 21264 | 0 / 21264 | 0 / 21264 |
| satan. | 0 / 0 | 1265 / 324 | 0 / 324 | 0 / 324 | 0 / 324 | 0 / 324 |
| portsweep. | 0 / 0 | 846 / 194 | 0 / 194 | 0 / 194 | 0 / 194 | 0 / 194 |
| back. | 0 / 0 | 0 / 0 | 1773 / 430 | 0 / 430 | 0 / 430 | 0 / 430 |
| nmap. | 0 / 0 | 0 / 0 | 192 / 39 | 0 / 39 | 0 / 39 | 0 / 39 |
| pod. | 0 / 0 | 0 / 0 | 0 / 0 | 211 / 53 | 0 / 53 | 0 / 53 |
| smurf. | 0 / 0 | 0 / 0 | 0 / 0 | 224309 / 56481 | 0 / 56481 | 0 / 56481 |
| warezclient. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 819 / 201 | 0 / 201 |
| teardrop. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 799 / 180 | 0 / 180 |
| ipsweep. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 991 / 256 |

Backbone expansion setup

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| normal. | 77931 / 19347 | 1000 / 19347 | 500 / 19347 | 333 / 19347 | 250 / 19347 | 200 / 19347 |
| neptune. | 85937 / 21264 | 1000 / 21264 | 500 / 21264 | 333 / 21264 | 250 / 21264 | 200 / 21264 |
| satan. | 0 / 0 | 1265 / 324 | 500 / 324 | 333 / 324 | 250 / 324 | 200 / 324 |
| portsweep. | 0 / 0 | 846 / 194 | 500 / 194 | 333 / 194 | 250 / 194 | 200 / 194 |
| back. | 0 / 0 | 0 / 0 | 1773 / 430 | 333 / 430 | 250 / 430 | 200 / 430 |
| nmap. | 0 / 0 | 0 / 0 | 192 / 39 | 192 / 39 | 192 / 39 | 192 / 39 |
| pod. | 0 / 0 | 0 / 0 | 0 / 0 | 211 / 53 | 211 / 53 | 200 / 53 |
| smurf. | 0 / 0 | 0 / 0 | 0 / 0 | 224309 / 56481 | 250 / 56481 | 200 / 56481 |
| warezclient. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 819 / 201 | 200 / 201 |
| teardrop. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 799 / 180 | 200 / 180 |
| ipsweep. | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 991 / 256 |

CIC-IDS-2017 data setup

Finetune

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| Dos Hulk | 184808 / 46265 | 1000 / 46265 | 500 / 46265 | 333 / 46265 | 250 / 46265 | 200 / 46265 |
| BENIGN | 159865 / 40135 | 1000 / 40135 | 500 / 40135 | 333 / 40135 | 250 / 40135 | 200 / 40135 |
| PortScan | 0 / 0 | 127006 / 31924 | 500 / 31924 | 333 / 31924 | 250 / 31924 | 200 / 31924 |
| DDoS | 0 / 0 | 102606 / 25421 | 500 / 25421 | 333 / 25421 | 250 / 25421 | 200 / 25421 |
| DoS GoldenEye | 0 / 0 | 0 / 0 | 8245 / 2048 | 333 / 2048 | 250 / 2048 | 200 / 2048 |
| FTP-Patator | 0 / 0 | 0 / 0 | 6432 / 1506 | 333 / 1506 | 250 / 1506 | 200 / 1506 |
| SSH-Patator | 0 / 0 | 0 / 0 | 0 / 0 | 4755 / 1142 | 250 / 1142 | 200 / 1142 |
| DoS slowloris | 0 / 0 | 0 / 0 | 0 / 0 | 4591 / 1205 | 250 / 1205 | 200 / 1205 |
| DoS Slowhttptest | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 4431 / 1068 | 200 / 1068 |
| Bot | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 1594 / 372 | 200 / 372 |
| Web Attack � Brute Force | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 1224 / 256 |
| Web Attack � XSS | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 0 / 0 | 505 / 147 |

ToN\_IoT

## 4.4. Comparison

Base\_5\_Inc\_5

|  |  |  |  |
| --- | --- | --- | --- |
|  | KDD99 | CIC-IDS-2017 | TON\_IOT\_Network |
| Baseline | 0.76 | 98.82 | 73.74 |
| DER | 94.03 | 97.35 | 65.04 |
| MEMO | 98.0 | 99.21 | 24.61 |

Base\_2\_Inc\_2

|  |  |  |  |
| --- | --- | --- | --- |
|  | KDD99 (after remove class with number of instances < 200) | CIC-IDS-2017 | TON\_IOT\_Network |
| Baseline | 0.39 | 1.85 | 25.99 |
| DER | 90.0 | 67.54 | 68.96 |
| MEMO | 97.55 | 63.25 | 99.84 |

KDD99 dataset accuracy

Setting:

Initial Learning rate

Exemplar: 2000

First epoch: 200

Next epochs: 150

Accuracy curve [100.0, 1.25, 1.12, 57.61, 0.39, 0.39]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| normal. | 1.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| neptune. | 1.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| satan. |  | 0.19 | 0.0 | 0.0 | 0.0 | 0.0 |
| portsweep. |  | 0.02 | 0.0 | 0.0 | 0.0 | 0.0 |
| back. |  |  | 0.92 | 0.0 | 0.0 | 0.0 |
| nmap. |  |  | 0.0 | 0.0 | 0.0 | 0.0 |
| pod. |  |  |  | 0.0 | 0.07 | 0.07 |
| smurf. |  |  |  | 0.87 | 0.0 | 0.0 |
| warezclient. |  |  |  |  | 0.0 | 0.0 |
| teardrop. |  |  |  |  | 0.88 | 0.88 |
| ipsweep. |  |  |  |  |  | 0.0 |

Der

Accuracy curve: [100.0, 99.09, 96.92, 99.45, 99.24, 98.91]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| normal. | 1.0 | 1.0 | 0.98 | 0.99 | 0.98 | 0.98 |
| neptune. | 1.0 | 1.0 | 0.98 | 1.0 | 1.0 | 1.0 |
| satan. |  | 0.22 | 0.84 | 0.96 | 0.97 | 0.97 |
| portsweep. |  | 0.54 | 0.82 | 0.83 | 0.83 | 0.85 |
| back. |  |  | 1.0 | 0.95 | 0.95 | 0.99 |
| nmap. |  |  | 0.07 | 0.35 | 0.21 | 0.14 |
| pod. |  |  |  | 0.4 | 0.32 | 0.47 |
| smurf. |  |  |  | 1.0 | 1.0 | 1.0 |
| warezclient. |  |  |  |  | 0.79 | 0.55 |
| teardrop. |  |  |  |  | 1 | 1 |
| ipsweep. |  |  |  |  |  | 0.05 |

Memo [100.0, 99.97, 97.29, 97.75, 95.61, 86.14]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| normal. | 1.0 | 1.0 | 0.97 | 0.94 | 0.88 | 0.46 |
| neptune. | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 |
| satan. |  | 0.99 | 0.95 | 0.98 | 0.97 | 0.98 |
| portsweep. |  | 0.99 | 0.96 | 0.81 | 0.68 | 0.74 |
| back. |  |  | 0.96 | 0.93 | 1.0 | 0.86 |
| nmap. |  |  | 0.07 | 0.04 | 0.07 | 0.15 |
| pod. |  |  |  | 0.99 | 0.03 | 0.04 |
| smurf. |  |  |  | 1.0 | 1.0 | 1.0 |
| warezclient. |  |  |  |  | 0.41 | 0.04 |
| teardrop. |  |  |  |  | 0.01 | 1.0 |
| ipsweep. |  |  |  |  |  | 0.99 |

CIC-IDS-2017 dataset

Finetune [100.0, 39.89, 2.41, 1.57, 1.37, 0.53]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| Dos Hulk | 1.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| BENIGN | 1.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| PortScan |  | 0.85 | 0.0 | 0.0 | 0.0 | 0.0 |
| DDoS |  | 0.40 | 0.0 | 0.0 | 0.0 | 0.0 |
| DoS GoldenEye |  |  | 0.04 | 0.0 | 0.0 | 0.0 |
| FTP-Patator |  |  | 0.07 | 0.0 | 0.0 | 0.0 |
| SSH-Patator |  |  |  | 0.03 | 0.04 | 0.0 |
| DoS slowloris |  |  |  | 0.03 | 0.11 | 0.02 |
| DoS Slowhttptest |  |  |  |  | 0.01 | 0.00 |
| Bot |  |  |  |  | 0.02 | 0.01 |
| Web Attack � Brute Force |  |  |  |  |  | 0.01 |
| Web Attack � XSS |  |  |  |  |  | 0.0 |

Der

Accuracy curve [100.0, 99.94, 80.87, 97.31, 76.59, 57.96]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| Dos Hulk | 1.0 | 1.0 | 0.95 | 1.0 | 0.5 | 0.5 |
| BENIGN | 1.0 | 1.0 | 0.93 | 0.99 | 0.98 | 0.94 |
| PortScan |  | 1.0 | 0.61 | 0.98 | 0.98 | 0.39 |
| DDoS |  | 1.0 | 1.0 | 1.0 | 0.75 | 0.73 |
| DoS GoldenEye |  |  | 0.36 | 0.86 | 0.23 | 0.71 |
| FTP-Patator |  |  | 0.13 | 0.12 | 0.62 | 0.0 |
| SSH-Patator |  |  |  | 0.0 | 0.94 | 0.0 |
| DoS slowloris |  |  |  | 0.76 | 0.49 | 0.47 |
| DoS Slowhttptest |  |  |  |  | 0.17 | 0.14 |
| Bot |  |  |  |  | 0.22 | 0.17 |
| Web Attack � Brute Force |  |  |  |  |  | 0.00 |
| Web Attack � XSS |  |  |  |  |  | 0.01 |

Memo

Accuracy curve

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Training instances / Testing instances | Task 0 | Task 1 | Task 2 | Task 3 | Task 4 | Task 5 |
| Dos Hulk | 1.0 | 0.99 | 0.98 | 0.97 | 0.96 | 0.96 |
| BENIGN | 1.0 | 0.96 | 0.95 | 0.98 | 0.78 | 0.71 |
| PortScan |  | 1.0 | 1.0 | 1.0 | 1.0 | 0.69 |
| DDoS |  | 0.94 | 0.97 | 0.96 | 0.94 | 0.96 |
| DoS GoldenEye |  |  | 0.53 | 0.62 | 0.56 | 0.67 |
| FTP-Patator |  |  | 0.99 | 1.0 | 0.99 | 0.2 |
| SSH-Patator |  |  |  | 0.99 | 0.99 | 0.95 |
| DoS slowloris |  |  |  | 0.93 | 0.82 | 0.42 |
| DoS Slowhttptest |  |  |  |  | 0.79 | 0.39 |
| Bot |  |  |  |  | 0.06 | 0.05 |
| Web Attack � Brute Force |  |  |  |  |  | 0.75 |
| Web Attack � XSS |  |  |  |  |  | 0.84 |

# Chapter 7: Appendix

## Features set of each dataset.

Target:

|  |  |
| --- | --- |
| BENIGN | 440031 |
| DoS Hulk | 231073 |
| DoS GoldenEye | 10293 |
| DoS slowloris | 5796 |
| DoS Slowhttptest | 5499 |
| Heartbleed | 11 |

Missing data 1008 / 692703

### ToN IoT Network Dataset.

|  |  |  |
| --- | --- | --- |
| ts | dst\_ip\_bytes | http\_trans\_depth |
| src\_ip | dns\_query | http\_method |
| src\_port | dns\_qclass | http\_uri |
| dst\_ip | dns\_qtype | http\_version |
| dst\_port | dns\_rcode | http\_request\_body\_len |
| proto | dns\_AA | http\_response\_body\_len |
| service | dns\_RD | http\_status\_code |
| duration | dns\_RA | http\_user\_agent |
| src\_bytes | dns\_rejected | http\_orig\_mime\_types |
| dst\_bytes | ssl\_version | http\_resp\_mime\_types |
| conn\_state | ssl\_cipher | weird\_name |
| missed\_bytes | ssl\_resumed | weird\_addl |
| src\_pkts | ssl\_established | weird\_notice |
| src\_ip\_bytes | ssl\_subject | label |
| dst\_pkts | ssl\_issuer | type |

|  |  |
| --- | --- |
| normal | 300000 |
| scanning | 20000 |
| dos | 20000 |
| injection | 20000 |
| ddos | 20000 |
| password | 20000 |
| xss | 20000 |
| ransomware | 20000 |
| backdoor | 20000 |
| mitm | 1043 |

Missing data: 0/461043

|  |  |
| --- | --- |
| smurf | 280790 |
| neptune | 107201 |
| normal | 97278 |
| back | 2203 |
| satan | 1589 |
| ipsweep | 1247 |
| portsweep | 1040 |
| warezclient | 1020 |
| teardrop | 979 |
| pod | 264 |
| nmap | 231 |
| guess\_passwd | 53 |
| buffer\_overflow | 30 |
| land | 21 |
| warezmaster | 20 |
| imap | 12 |
| rootkit | 10 |
| loadmodule | 9 |
| ftp\_write | 8 |
| multihop | 7 |
| phf | 4 |
| perl | 3 |
| spy | 2 |

Missing data: 0/494021

# Chapter 8: List of Figures

Accuracy of CIC-IDS-2017 Wednesday DoS (with Base 2 and Increment 2)

A graph of different colored bars

Description automatically generated

CIC-IDS-2017 Data Distribution

A graph with green bars

Description automatically generated

There are a total of 2.2 million records of BENIGN data. I only use 200.000 records because of memory related problem when running on server. I also drop classes has number of instances < 200.

Most instances: Dos Hulk – 231073 Least instances: Web attack XSS 652

A green bar graph with white text

Description automatically generated

I drop all class that has < 200 instances.

Most instances: Smurf attack: 280790 Least instances: nmap 231

KDD99 accuracy curve (Base 2 Increment 2)

A graph of a curve

Description automatically generated with medium confidence

CIC-IDS-2017 Full accuracy curve (Base 2 Increment 2)

A graph of a line

Description automatically generated with medium confidence

KDD F1 Score Curve

Finetune – Der - Memo

A graph with colored lines

Description automatically generatedA graph with colored lines and white text

Description automatically generatedA graph of lines and numbers

Description automatically generated with medium confidence

CIC-IDS-2017 F1 Score Curve

Finetune – Der - Memo

A graph with lines and numbers

Description automatically generated A graph with lines and text

Description automatically generated with medium confidence A graph with colorful lines and text

Description automatically generated