Detecting DDoS attack using Logistic Regression

Supervised By
Mr. Jagdish Bhatta
CDCSIT

Submitted By
Brihat Ratna Bajracharya
19/075

Submitted To
Central Department of Computer Science and Information Technology

INTRODUCTION

- DoS Attack
  - denial of service attack
  - continuous attack packets overloads the victim's computer resources making the service unavailable to other devices and users throughout the network
- DDoS attack
  - distributed denial of service attack
  - multiple systems target a single system with a DoS attack
  - Two types
    - Direct
      - Targeting victim's machine in its weakness
    - Indirect
      - Attack performed on elements associated with the victim's machine

INTRODUCTION

- Logistic Regression
  - statistical method for analysing a dataset in which there are one or more independent variables that determine an categorical outcome
  - Three types of logistic regression
    - Binomial logistic regression
      - For two possible outcome
      - Uses sigmoid function
    - Multinomial logistic regression
      - For three or more outcome
      - Uses softmax function (turns logits to probabilities that sums to one)
    - Ordinal logistic regression
      - For ordered outcome

LITERATURE REVIEW

- Classification Based
  - Sahi et al. [1] proposed new classifier system for detecting and preventing DDoS TCP flood attacks
  - Classifies incoming packets and makes decision based on classification result in detection phase
  - Also maintains backlist table of source IP of detected attacks for prevention phase and related packet is terminated

LITERATURE REVIEW

- Entropy Based
  - Gera et al. [6] proposed a system to differentiate DDoS attack from flash events based on the anomaly pattern (time interval and source entropy)
    - *Time interval* – In DDoS, network traffic spikes abruptly whereas in flash event, the traffic increase gradually
    - *Source entropy* – number of source IP addresses from which attack is launched
    - *Traffic cluster* – traffic coming from the same network
  - Classification
    - Flash event – more source IPs but less traffic cluster
    - DDoS (spoofed) – more source IPs and more traffic cluster
    - DDoS (non-spoofed) – the source IP is same and the traffic cluster is more

LITERATURE REVIEW

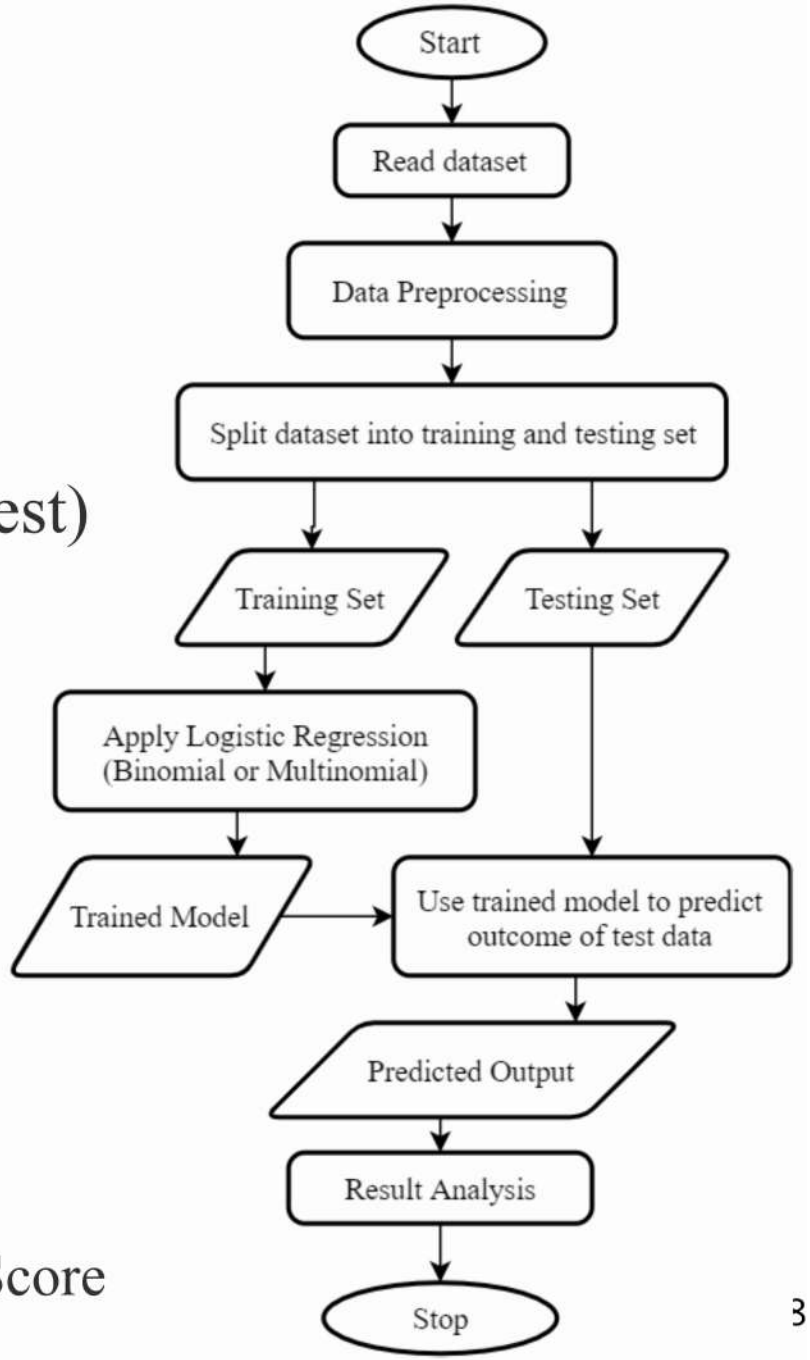
- Regression Based
  - Divakaran et al. [5] proposed a framework of gathering evidences to detect traffic sessions related to attacks and malicious activities
  - Three stages
    - *Modeling and analyzing sessions to detect anomalous patterns* – by analysing the inter-arrival time of flows (set of packets) in the session, randomness is lesser for attack flow than normal flow
    - *Detecting scans and illegitimate TCP state sequences* – using TCP state sequence, anything that does not correspond to normal flow (SYN, SYN_ACK, DATA, FIN) is considered illegitimate
    - *Evidence correlation and decision making* - Spacial correlation (using IP addresses) is performed to correlate the anomalous pattern, regression model used to detect anomalous pattern

LITERATURE REVIEW

- Artificial Neural Network
  - Saied et al. [2] used supervised ANN (feed forward, error back propagation) approach on three different type of packets: TCP, UDP and ICMP
    - ANN ICMP uses three input nodes (*source_ip, icmp_sequence, and icmp_ip*), four hidden nodes and one output node
    - ANN TCP uses five input nodes (*source_ip, tcp_sequence, source_port, destination_port, and tcp_flags*), four hidden nodes and one output node
    - ANN UDP, four input layer nodes (*source_port, destination_port, source_ip, and packet_length*), three hidden nodes and one output node
  - **Basic flow**
    - DDoS detectors are installed in different network, each detector registering the IP of neighboring detectors, communicating via encrypted messages and continuously monitors the number of passing packets
    - If number of packets are greater than certain threshold, then attack is suspected. The packets are sorted and IP of the victim is identified. The ANN retrieves the required patterns and prepares for the ANN engine. The trained ANN engine takes the input and produces the output (attack or normal).
    - Above step is repeated for three times and final outcome is the majority of three outputs.
  - This ANN engine needs to be trained regularly for detecting up-to-date DDoS attacks.

METHODOLOGY

- Read Dataset
- Data Pre-processing
  - Encoding non numeric values
  - Feature Selection (correlation test)
  - Train Test Split
- Model classifier using train set
- Predict output using test set
- Analysis
  - Confusion Matrix
  - Performance Metrics
    - Accuracy, Precision, Recall, F1 Score
- Conclusion



IMPLEMENTATION DETAILS

- Dataset Details
  - Used CICDDoS2019 dataset from University of New Brunswick [9]
  - Result of abstract behaviour of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols
  - Analysed Portmap and LDAP and NetBIOS variant of DDoS attack
  - Consist of 88 columns (87 features and one outcome column)
  - Portmap dataset contains 191694 records and LDAP dataset contains 2113234 records

IMPLEMENTATION DETAILS

	Unnamed_0	Flow_ID	Source_IP	Source_Port	Destination_IP	Destination_Port	Protocol	Timestamp	Flow_Duration
0	24	192.168.50.254-224.0.0.5-0-0-0	192.168.50.254	0	224.0.0.5	0	0	2018-11-03 09:18:16.964447	114456999
1	26	192.168.50.253-224.0.0.5-0-0-0	192.168.50.253	0	224.0.0.5	0	0	2018-11-03 09:18:18.506537	114347504
2	176563	172.217.10.98-192.168.50.6-443-54799-6	192.168.50.6	54799	172.217.10.98	443	6	2018-11-03 09:18:18.610576	36435473
3	50762	172.217.7.2-192.168.50.6-443-54800-6	192.168.50.6	54800	172.217.7.2	443	6	2018-11-03 09:18:18.610579	36434705
4	87149	172.217.10.98-192.168.50.6-443-54801-6	192.168.50.6	54801	172.217.10.98	443	6	2018-11-03 09:18:18.610581	36434626
5	0	172.217.9.238-192.168.50.6-80-54805-6	192.168.50.6	54805	172.217.9.238	80	6	2018-11-03 09:18:18.626325	3
6	1	172.217.9.238-192.168.50.6-80-54805-6	172.217.9.238	80	192.168.50.6	54805	6	2018-11-03 09:18:18.667379	2
7	144429	172.217.9.238-192.168.50.6-80-54805-6	192.168.50.6	54805	172.217.9.238	80	6	2018-11-03 09:18:18.667575	2
8	224	255.255.255.255-0.0.0.0-67-68-17	0.0.0.0	68	255.255.255.255	67	17	2018-11-03 09:18:18.758942	28870362
9	25	172.16.0.5-192.168.50.4-0-0-0	172.16.0.5	0	192.168.50.4	0	0	2018-11-03 09:18:19.155867	118365715

10 rows × 88 columns

Portmap Dataset (1/2)

IMPLEMENTATION DETAILS

Total_Fwd_Packets	...	Active_Std	Active_Max	Active_Min	Idle_Mean	Idle_Std	Idle_Max	Idle_Min	SimillarHTTP	Inbound	Label
45	...	2.833711e+04	98168.0	3.0	9529897.25	3.515826e+05	10001143.0	9048097.0	0	0	BENIGN
56	...	1.213149e+05	420255.0	4.0	9493929.75	3.515411e+05	9978130.0	8820294.0	0	0	BENIGN
6	...	0.000000e+00	62416.0	62416.0	36373056.00	0.000000e+00	36373056.0	36373056.0	0	0	BENIGN
6	...	0.000000e+00	62413.0	62413.0	36372291.00	0.000000e+00	36372291.0	36372291.0	0	0	BENIGN
6	...	0.000000e+00	62409.0	62409.0	36372216.00	0.000000e+00	36372216.0	36372216.0	0	0	BENIGN
2	...	0.000000e+00	0.0	0.0	0.00	0.000000e+00	0.0	0.0	0	0	BENIGN
2	...	0.000000e+00	0.0	0.0	0.00	0.000000e+00	0.0	0.0	0	1	BENIGN
2	...	0.000000e+00	0.0	0.0	0.00	0.000000e+00	0.0	0.0	0	0	BENIGN
5	...	0.000000e+00	2501634.0	2501634.0	8789576.00	2.955921e+06	10912366.0	5413491.0	0	0	BENIGN
40	...	3.462641e+06	7515650.0	103.0	9687762.70	5.445120e+06	18391321.0	5118819.0	0	1	Portmap

Portmap Dataset (2/2)

IMPLEMENTATION DETAILS

	Unnamed_0	Flow_ID	Source_IP	Source_Port	Destination_IP	Destination_Port	Protocol	Timestamp	Flow_Duration
0	24	94238	161	0	33	0	0	80260	114456999
1	26	39286	137	0	33	0	0	25731	114347504
2	176563	177204	67	54799	179	443	6	132519	36435473
3	50762	156514	67	54800	10	443	6	150107	36434705
4	87149	132848	67	54801	179	443	6	23012	36434626
5	0	187888	67	54805	163	80	6	82928	3
6	1	187888	141	80	78	54805	6	185496	2
7	144429	187888	67	54805	163	80	6	113771	2
8	224	146542	154	68	176	67	17	134822	28870362
9	25	42694	202	0	68	0	0	23065	118365715

10 rows × 88 columns

Portmap Dataset after encoding

IMPLEMENTATION DETAILS

- Feature Selection using correlation test
  - Selected features for Portmap dataset

```
Protocol:              0.705635574606102
Fwd_Packet_Length_Min: 0.7291026803636192
Min_Packet_Length:     0.7291679201346289
Source_Port:           0.8189050406122815
Inbound:               0.8600933612454168
Source_IP:             0.8660476930033244
Label:                 1.0
```

  - Some of discarded features for Portmap dataset

```
Down_Up_Ratio':           0.6485234774068003
URG_Flag_Count':          0.6150806663811492
Bwd_Packet_Length_Min':   0.5505265792832202
Destination_IP':          0.5434405331523054
CWE_Flag_Count':          0.4208864290747812
Avg_Bwd_Segment_Size':    0.41915492520184805
Bwd_Packet_Length_Mean':  0.41915492520184805
Fwd_IAT_Total':           0.3345362968706236
Unnamed_0':               0.11675730059144739
```

IMPLEMENTATION DETAILS

- Feature Selection using correlation test
  - Selected features for LDAP dataset

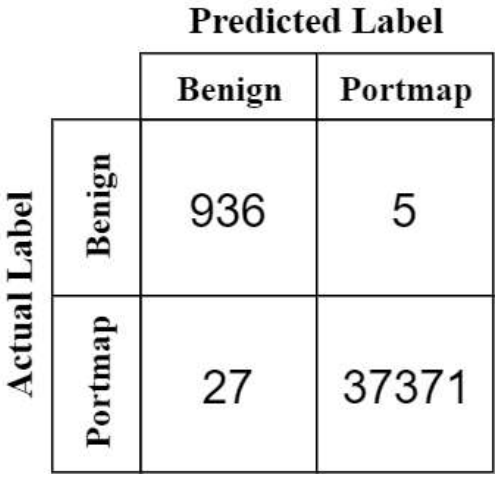
```
Min Packet Length:          0.9276131094369818
Fwd Packet Length Min:      0.9277359022458002
Avg Fwd Segment Size:       0.9291694741755031
Fwd Packet Length Mean:     0.9291694741755031
Average Packet Size:        0.9292312255418383
Packet Length Mean:         0.9302060576330425
Fwd Packet Length Max:      0.9327888918318388
Max Packet Length:          0.9359158567754134
Label:                      1.0
```

  - Some of discarded features for LDAP dataset

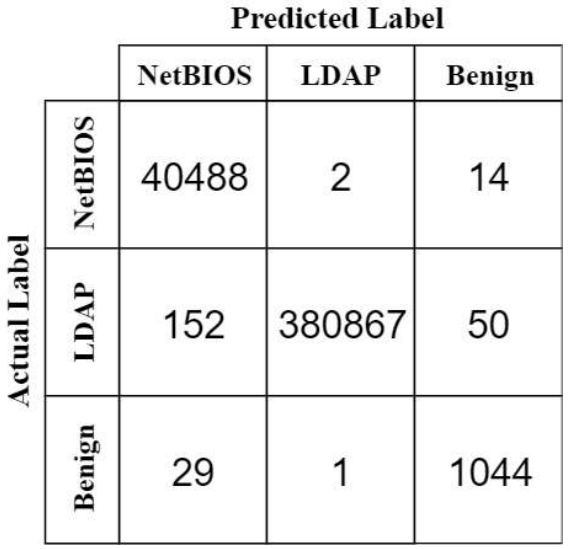
```
Protocol:              0.15101837887241756
Inbound:               0.14945687840206262
min_seg_size_forward: 0.05637313458482986
Fwd Header Length:     0.05629353491866543
Destination_Port:      0.012102190951823352
Bwd Header Length:     0.00633967032746798
Timestamp:             0.00018127588100869682
Flow ID:               0.0014231120955229765
SimillarHTTP:          0.014568932109410395
Active Std:            0.01713683548092619
```

RESULT

Confusion Matrix for Portmap dataset and LDAP dataset



Actual Label \ Predicted Label	Benign	Portmap
Benign	936	5
Portmap	27	37371



Actual Label \ Predicted Label	NetBIOS	LDAP	Benign
NetBIOS	40488	2	14
LDAP	152	380867	50
Benign	29	1	1044

Performance Metrics for Portmap dataset

```
Accuracy  = 99.91 %
Precision = 98.59 %
Recall    = 99.69 %
F1 Score  = 0.9913
```

Performance Metrics for LDAP dataset

```
Accuracy  = 99.94 %
Precision = 97.92 %
Recall    = 99.03 %
F1 Score  = 0.9847
```

CONCLUSION

- Out of 87 features, considering only few features that are highly correlated with the attack class is sufficient for detecting DDoS attack variants
- We used six features for detecting portmap attack and eight features for detecting LDAP and NetBIOS variant of DDoS attack
- From the result analysis, we see that performance metrics (accuracy and f1 score) of our classifier is high for both datasets
- We have modeled a good classifier for detecting Portmap, LDAP and NetBIOS variant of DDoS attack

REFERENCES

1. A. Sahi, D. Lal, Y. Li, and M. Diykh, “An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment”, in *IEEE Access*, vol. 5, pp. 6036-6048, 2017.

2. A. Saied, R. E. Overhill, T. Radzik, “Detection of known and unknown DDoS attacks using Artificial Neural Networks”, in *Neurocomputing* 172, pp. 385-393, 2016.

3. B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, The Economic Impact of Cyber-Attacks, document CRS RL32331, *Congressional Research Service Documents*, Washington, DC, USA, 2004.

4. C. Bedon, A. Saied, Snort-AI (Version 2.4.3), “Open Source Project”, 2009. Available from: http://snort-ai.sourceforge.net/index.php/

5. D. M. Divakaran, K. W. Fok, I. Nevat, and V. L. L. Thing, “Evidence gathering for network security and forensics”, in *Digital Investigation 20*, pp. S56-S65, 2017.

6. J. Gera, and B. P. Battula, “Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds”, in *EURASIP Journal on Information Security*, doi:10.1186/s13635-018-0079-6, 2018.

7. M. Roesch, Snort (Version 2.9), “Open Source Project”, 1998. Available from: http://www.snort.org/.

8. R. Russell, Iptables (Version 1.4.21), “Open Source Project”, 1998. Available from: http://ipset.netfilter,org/iptables.man.html/.

9. *DDoS Evaluation Dataset ”CICDDoS2019” Dataset*, [online] Available: http://205.174.165.80/CICDataset/CICDDoS2019/Dataset/CSVs/CSV-03-11.zip

10. “*Logistic Regression For Dummies: A Detailed Explanation*”. Accessed on: Dec. 9, 2019. [Online]. Available: https://towardsdatascience.com/logistic-regression-for-dummies-a-detailed-explanation-9597f76edf46

Thank You