Wireshark Capture for Detection of Malicious Traffic v/s Normal Traffic

SUBMITTED BY:-

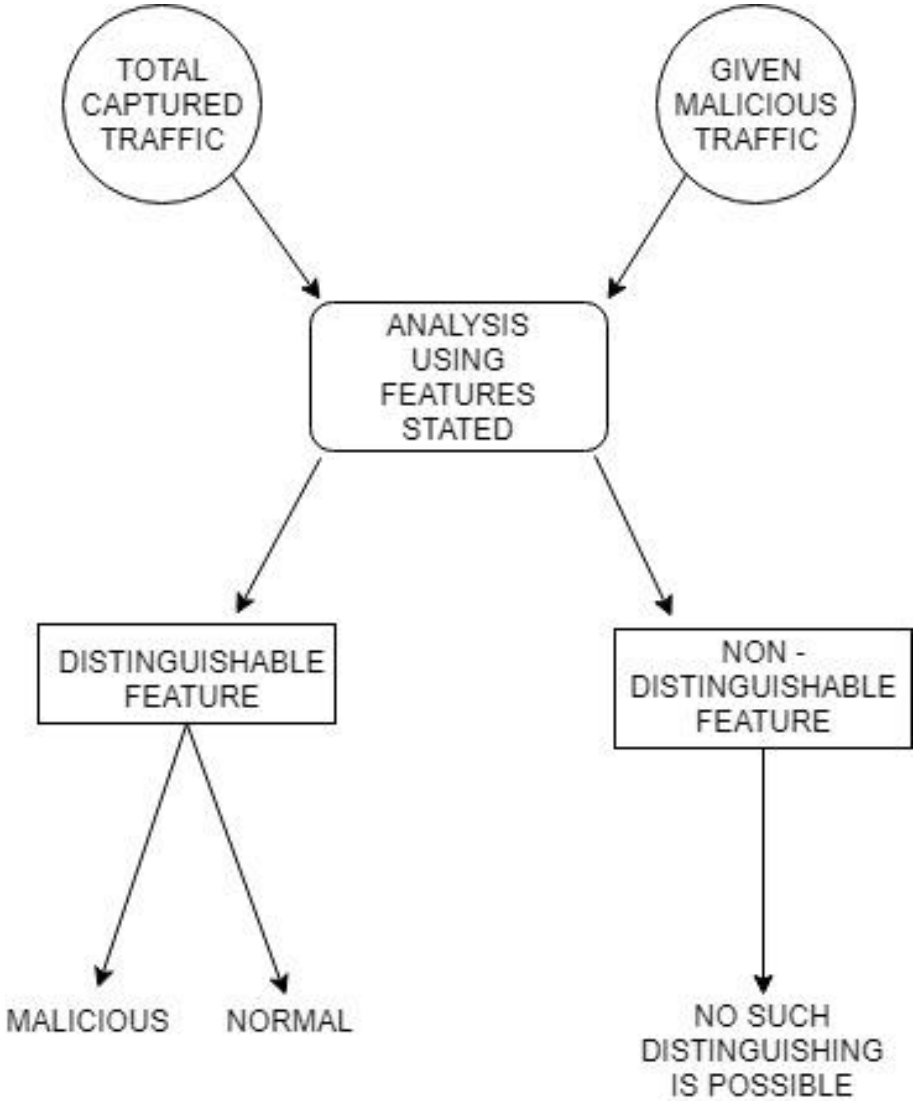
AMBARISH SINGH (18535004)

MOHIT RUSTAGI (18535017)

PATEL DIVYA VASANBHAI (18535021)

TRIPTI GARG (18535026)

Work Done


TOTAL CAPTURED TRAFFIC
GIVEN MALICIOUS TRAFFIC
ANALYSIS USING FEATURES STATED
DISTINGUISHABLE FEATURE
NON - DISTINGUISHABLE FEATURE
MALICIOUS
NORMAL
NO SUCH DISTINGUISHING IS POSSIBLE

Distinguishable v/s Non-Distinguishable Features

Distinguishable Features

1. Average Packet Size
2. Average Flow Duration
3. Average No. of Packets sent per flow
4. Average Amount of Bytes sent per flow
5. Average time interval between Packets sent
6. Average time interval between Packets Received
7. Average ratio of connections to no. of Destination IPs.

Non-Distinguishable Features

1. Average No. of Packets received per flow
2. Average amount of Bytes received per flow
3. Average ratio of incoming to outgoing packets
4. Average ratio of incoming to outgoing Bytes

Analysis of Distinguishable Features

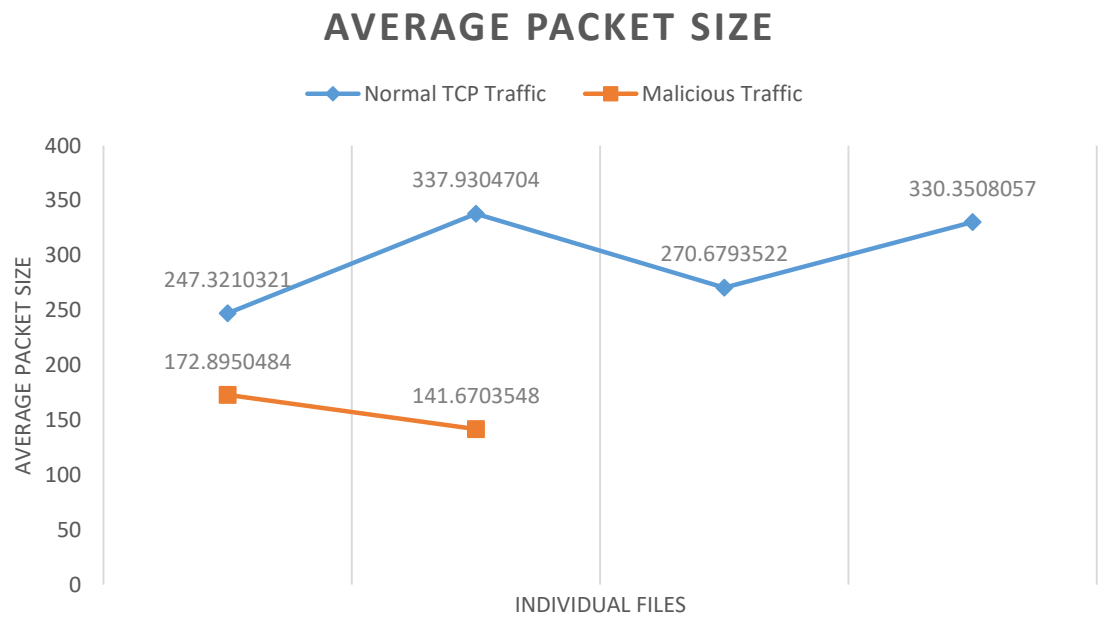
Average Packet Size

- It is calculated as

Average Packet size =

Average (Total No. of Bytes / Total No. of Packets *per flow*).

- For Normal Traffic, it lies in the range of **247 – 338** approx.
- For Malicious Traffic, it lies in the range of **142 – 173** approx.

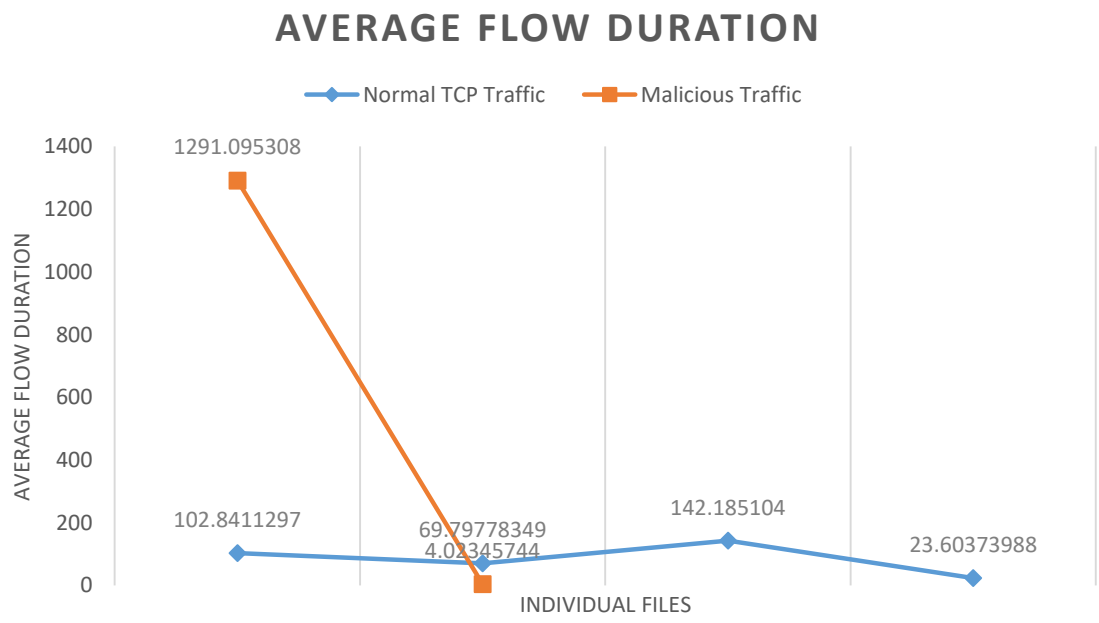


Average Flow Duration

- It is calculated as

  Average Flow Duration = Average (Duration of connection *per flow*).

- For Normal Traffic, the graph is somewhat steady and it lies in the range of **23 – 142** approx.
- For Malicious Traffic, the graph shows an abnormal fluctuation and it lies in the range of **4 – 1291** approx.



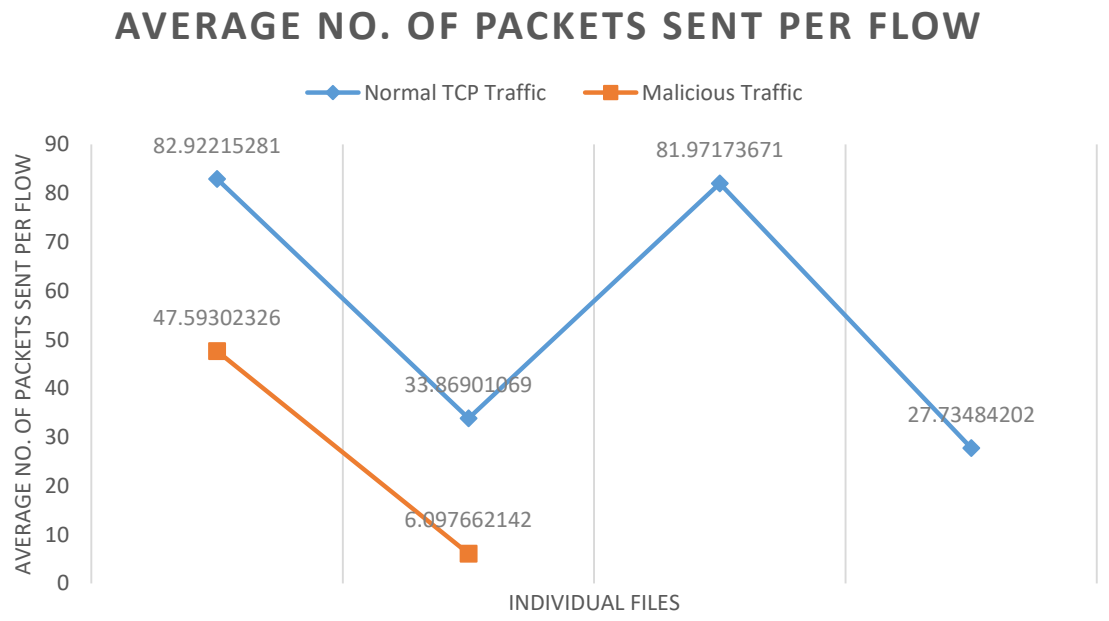
Average No. of Packets Sent Per Flow

- It is calculated as

Average No. of packets sent per flow =

Average (No. of Packets A→B *per flow*).

- For Normal Traffic, it lies in the range of **28 – 83** approx.
- For Malicious Traffic, it lies in the range of **6 – 48** approx.



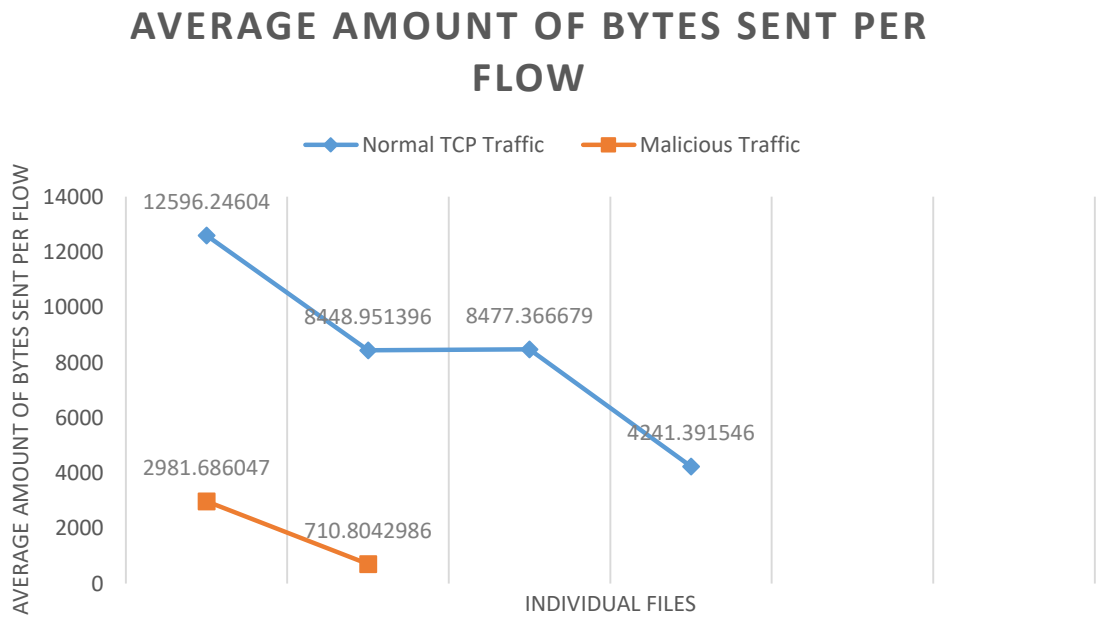
Average Amount of Bytes Sent Per Flow

- It is calculated as

Average amount of bytes sent per flow =

Average (No. of Bytes A→B *per flow*).

- For Normal Traffic, it lies in the range of **4241 – 12596** approx.
- For Malicious Traffic, it lies in the range of **710 – 2981** approx.

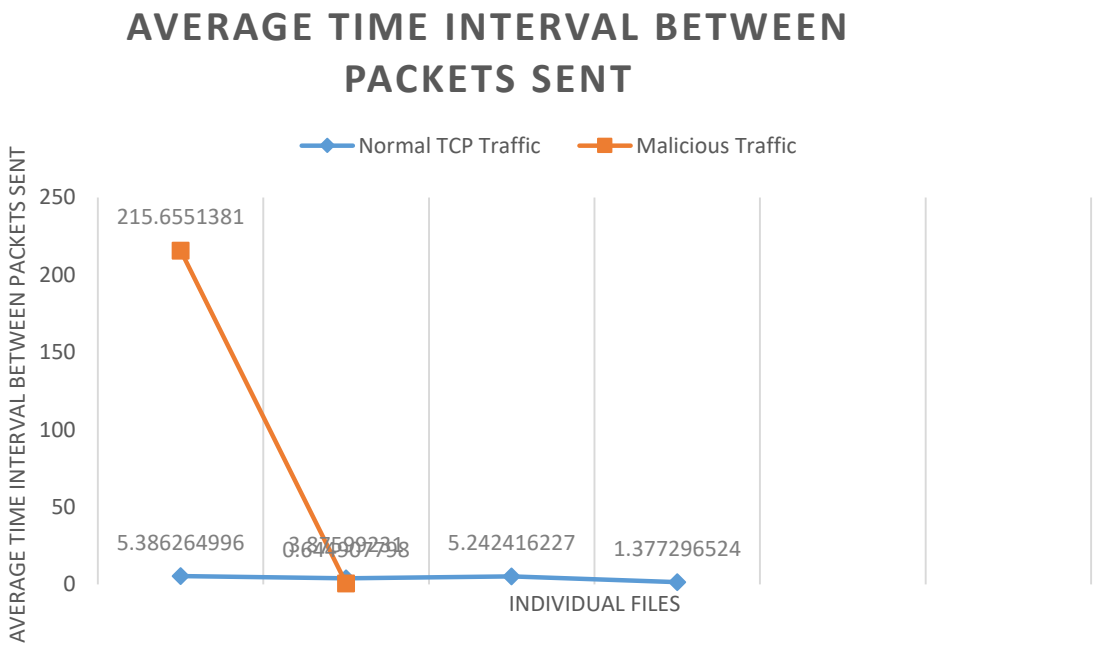


Average Time Interval Between Packets Sent

- It is calculated as

Average Time Interval Between Packets Sent = Average(Duration/Packets A→B *per flow*).

- For Normal Traffic, it lies in the range of **1.38-5.38** approx.
- For Malicious Traffic, it lies in the range of **0.65-215** approx.

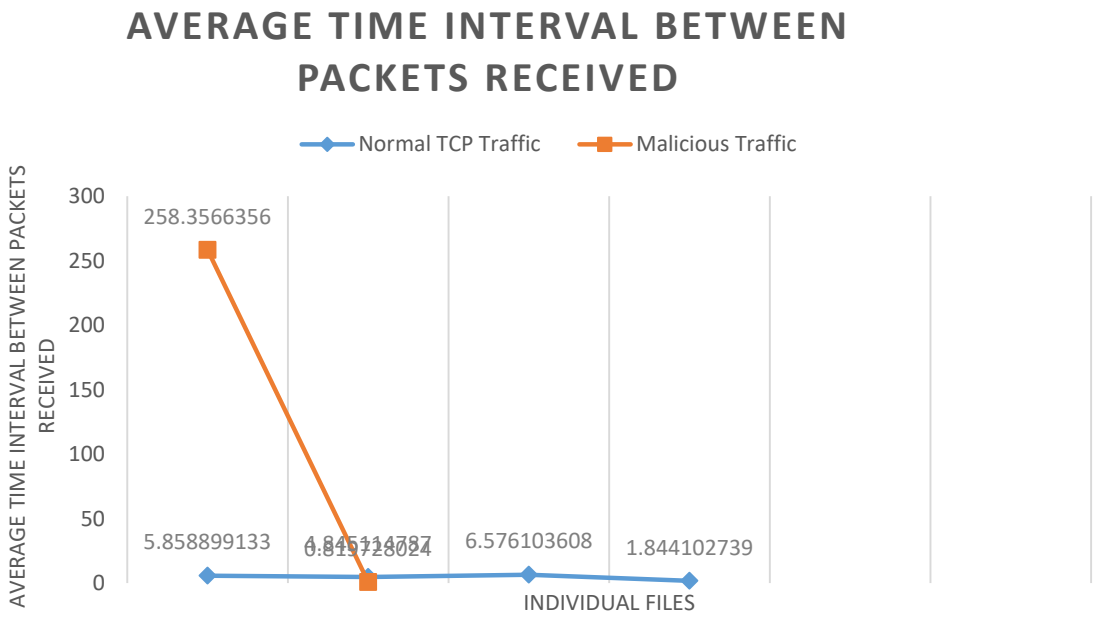


Average Time Interval Between Packets Received

- It is calculated as

Average Time Interval Between Packets Received = Average(Duration/Packets B→A *per flow*).

- For Normal Traffic, it lies in the range of **1.85-6.58** approx.
- For Malicious Traffic, it lies in the range of **0.82-258.36** approx.



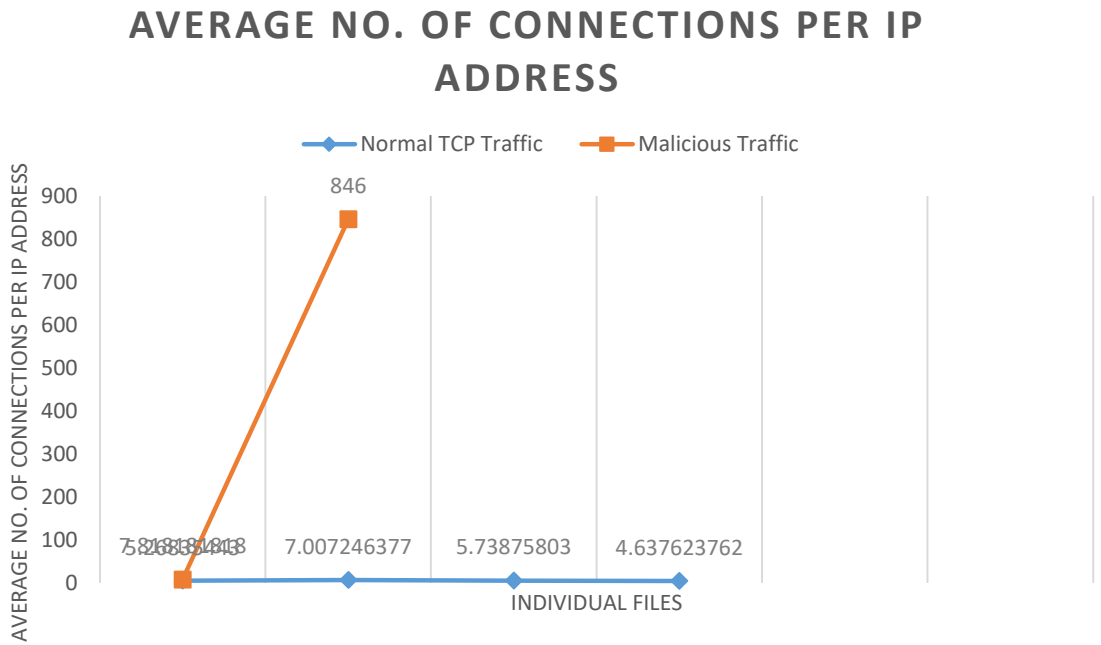
Average Ratio of Connections to Number of Destination IPs

- It is calculated as

Average Time Interval Between Packets Received =

count_unique(concat(Source IP, Source Port, Destination IP, Destination Port)) / No. of Destination IPs.

- For Normal Traffic, it lies in the range of **4.64 – 7** approx.
- For Malicious Traffic, it lies in the range of **7.8 – 846** approx.



Analysis of Non–Distinguishable Features

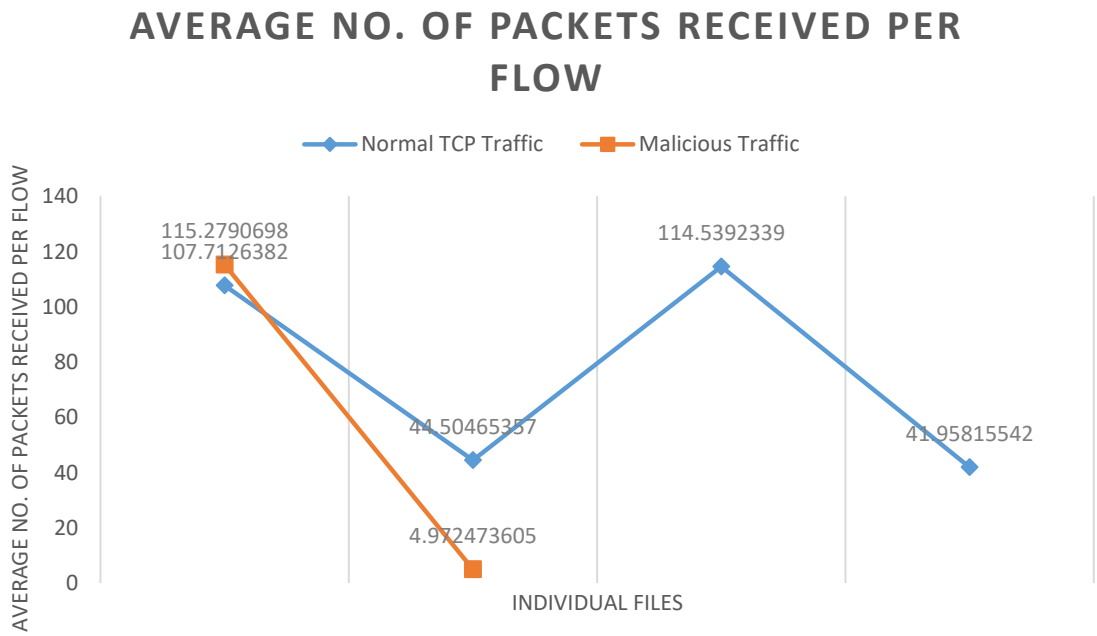
Average No. of Packets Received Per Flow

- It is calculated as

Average No. of Packets received per flow =

Average (No. of Packets B→A *per flow*).

- For Normal Traffic, it lies in the range of **42 – 115** approx.
- For Malicious Traffic, it lies in the range of **5 – 115** approx.



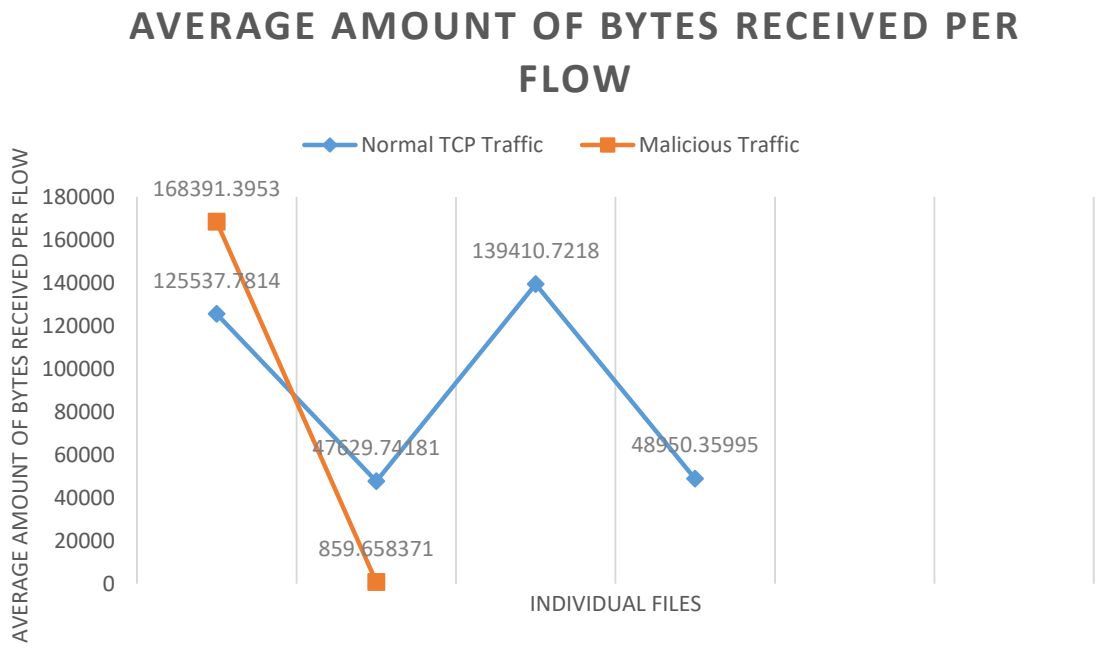
Average Amount of Bytes Received Per Flow

- It is calculated as

  Average amount of Bytes received per flow =

  Average (No. of Bytes B→A *per flow*).

- For Normal Traffic, it lies in the range of **48950 – 125537** approx.
- For Malicious Traffic, it lies in the range of **859 – 168391** approx.



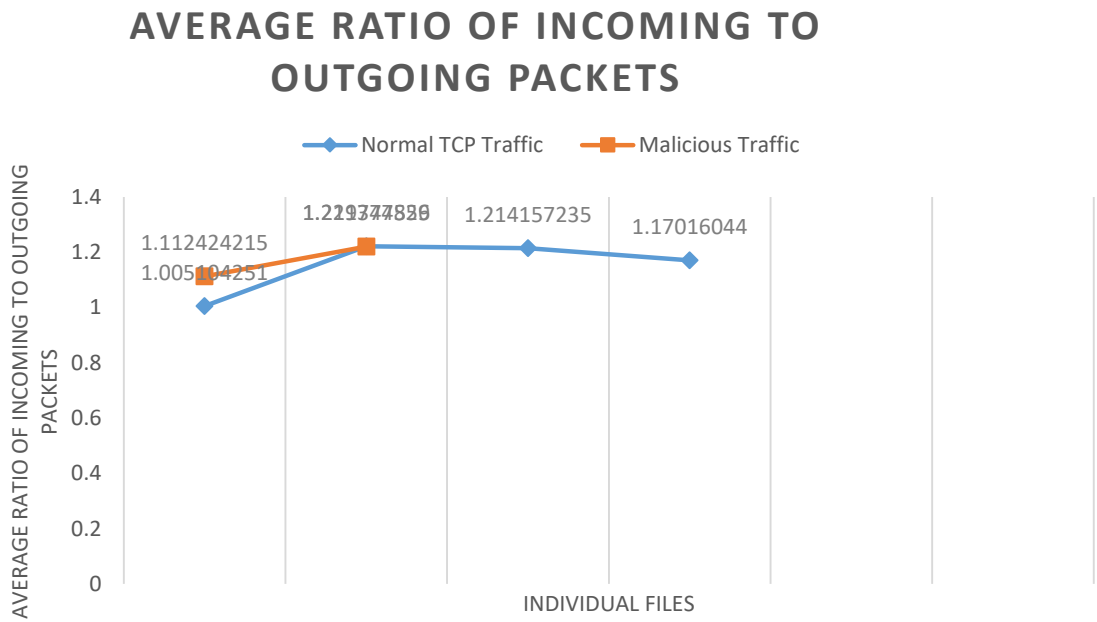
Average Ratio of Incoming to Outgoing Packets

- It is calculated as

Average ratio of incoming to outgoing packets =

Average((No. of Packets B→A)/ (No. of Packets A→B))(*per flow*).

- For Normal Traffic, it lies in the range of **1.00– 1.22** approx.
- For Malicious Traffic, it lies in the range of **1.11 – 1.21** approx.



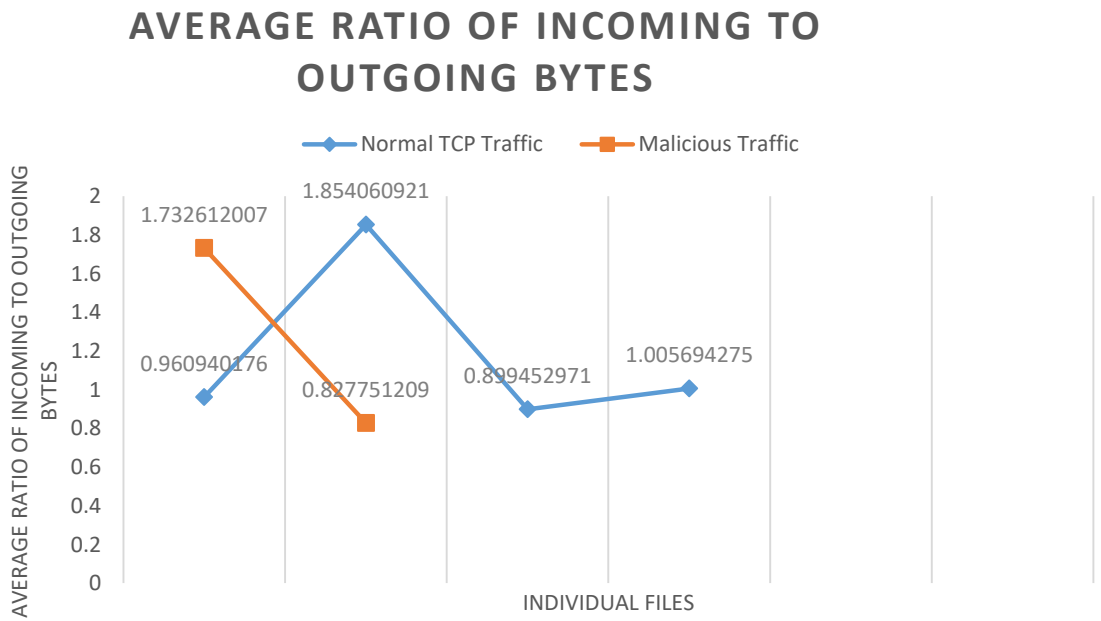
Average Ratio of Incoming to Outgoing Bytes

- It is calculated as

Average ratio of incoming to outgoing Bytes =

Average((No. of Bytes B→A)/ (No. of Bytes A→B))(*per flow*).

- For Normal Traffic, it lies in the range of **0.89–1.85** approx.
- For Malicious Traffic, it lies in the range of **0.83 – 1.73** approx.



New Proposed Features For Distinguishing

Distinguishable Vs Non-Distinguishable Features

Distinguishable Features

1. Average No. of Packets sent per second.
2. Average amount of Bytes sent per second.
3. Average amount of Bytes received per second.

Non-Distinguishable Features

1. Average Amount of Packets received per second.

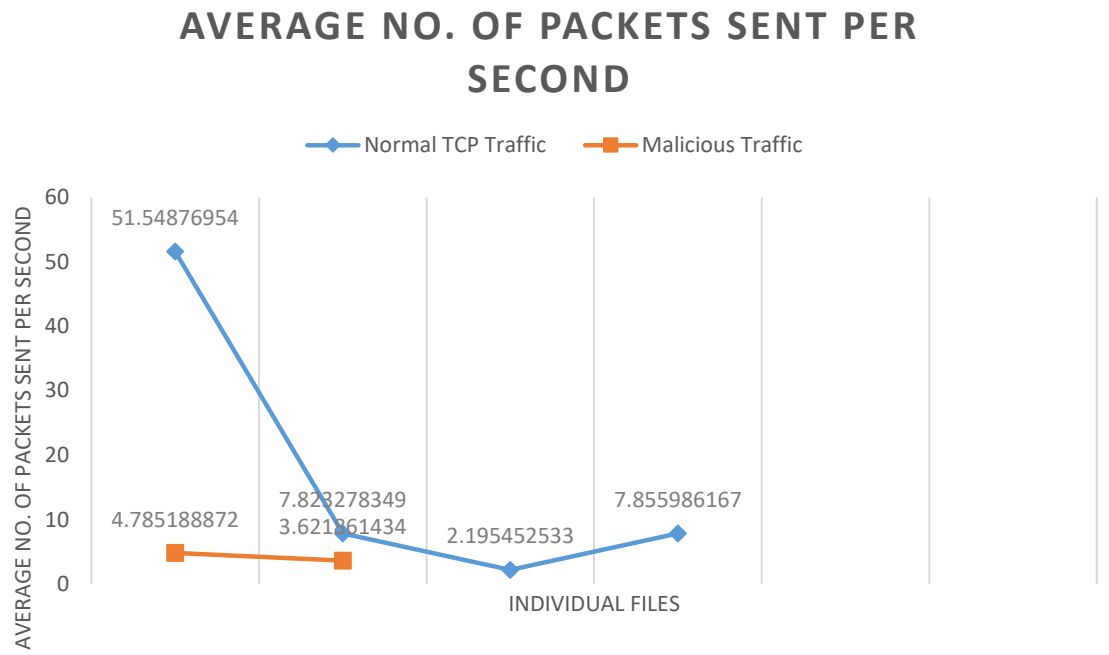
Average No. of Packets Sent Per Second

- It is calculated as

Average No. of packets sent per Second =

Average (No. of Packets A→B / Duration *per flow*).

- For Normal Traffic, it lies in the range of **2.19 – 51.55** approx.
- For Malicious Traffic, it lies in the range of **3.62 – 4.79** approx.



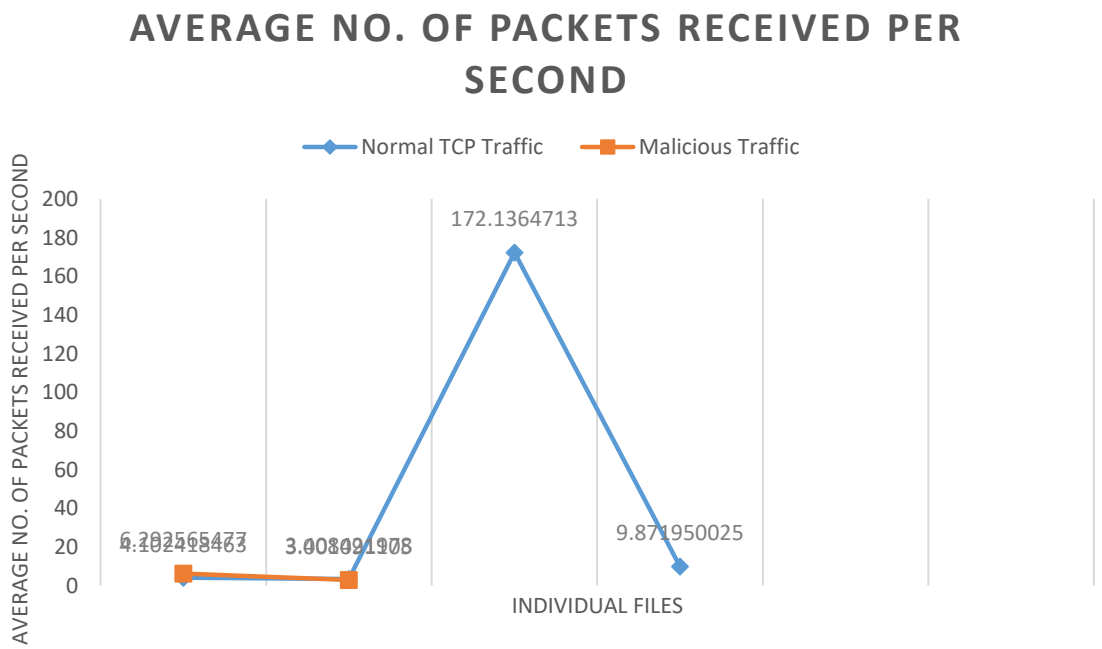
Average No. of Packets Received Per Second

- It is calculated as

Average No. of Packets received per Second =

Average (No. of Packets B→A / Duration *per flow*).

- For Normal Traffic, it lies in the range of **3.41 – 172.14** approx.
- For Malicious Traffic, it lies in the range of **3 – 6.29** approx.



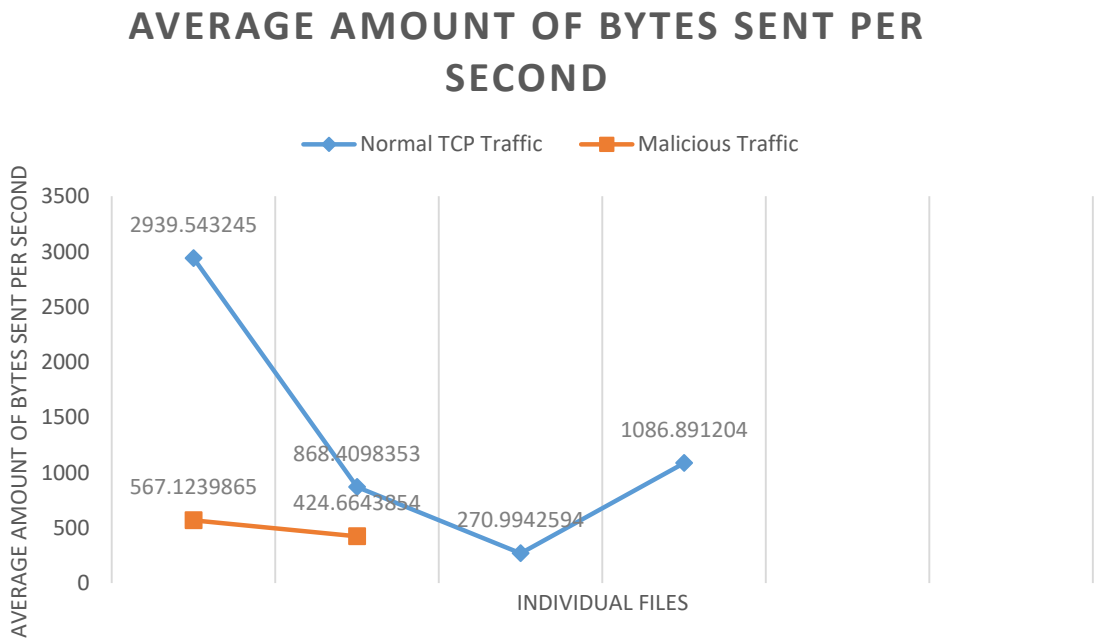
Average Amount of Bytes Sent Per Second

- It is calculated as

Average amount of bytes sent per flow =

Average (No. of Bytes A→B / Duration *per flow*).

- For Normal Traffic, it lies in the range of **271 – 2940** approx.
- For Malicious Traffic, it lies in the range of **425 – 567** approx.



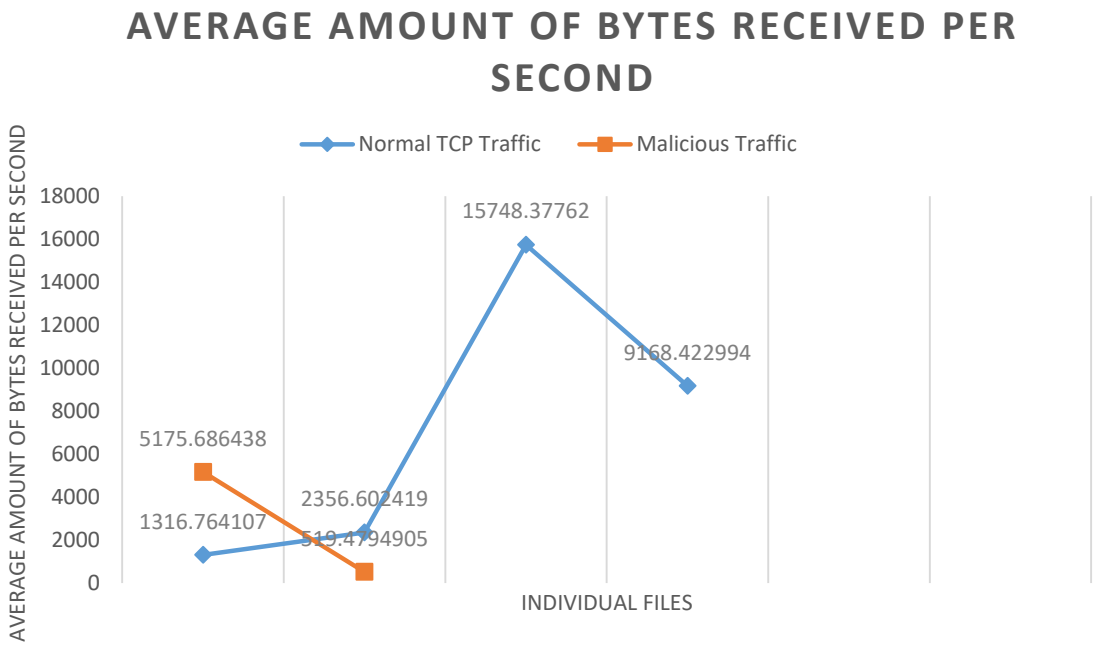
Average Amount of Bytes Received Per Second

- It is calculated as

  Average amount of Bytes received per Second =

  Average (No. of Bytes B→A / Duration *per flow*).

- For Normal Traffic, it lies in the range of **1317 – 15748.4** approx.
- For Malicious Traffic, it lies in the range of **519.48 – 5175.7** approx.



Thank You.