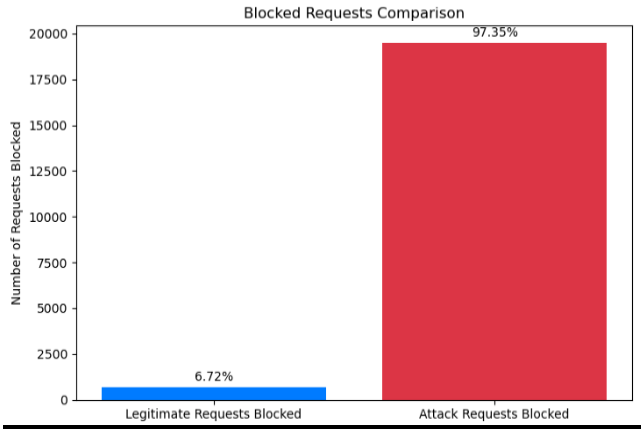
Results

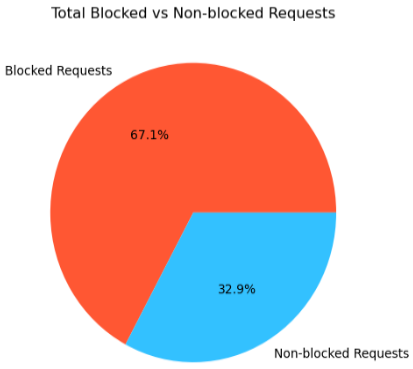
We have run our simulation on various arguments, and here we will display the results. We have a total of 100K packets in our original data, and the user can choose the amount of packets he wants to use every run. The attack packets had been distributed almost equally per timestamp using uniform distribution.

Example 1

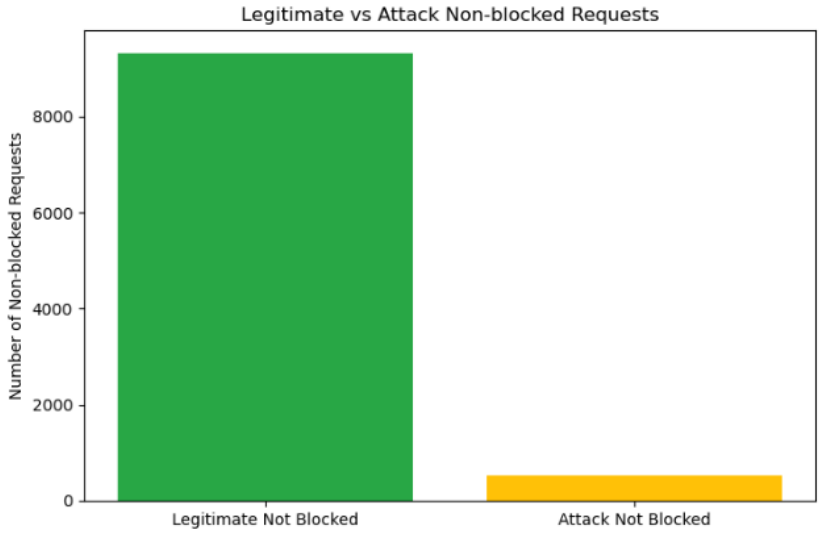
- The amount of data chosen is **10K** traces of the original traces.
- The volume of the attack is **20K** packets.
- The attack started at **5%** of the simulation time.
- The prefix size chosen is 3 means /24.
- The subnets that participated in the attack are: **173.194.90.0, 74.125.47.0, 74.125.181.0**.

- Total Requests: 30K, Attack requests: 20K , Legitimate 10K
- Blocked Requests: 20142 , Attack Blocked 19,470 , Legitimate Blocked:672
- Percentage of Attack Traffic Blocked: 97.35%
- Percentage of Legitimate Traffic Blocked: 6.72%

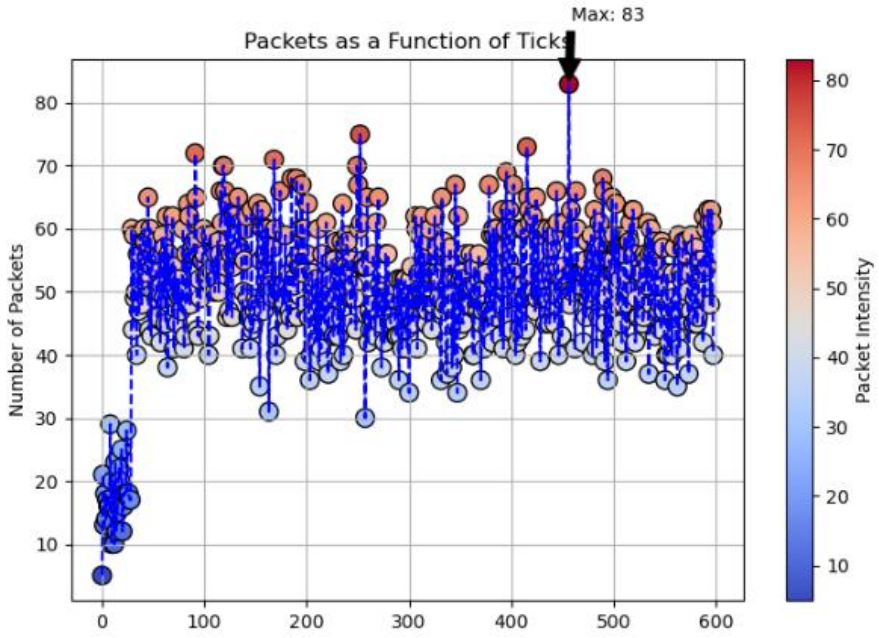




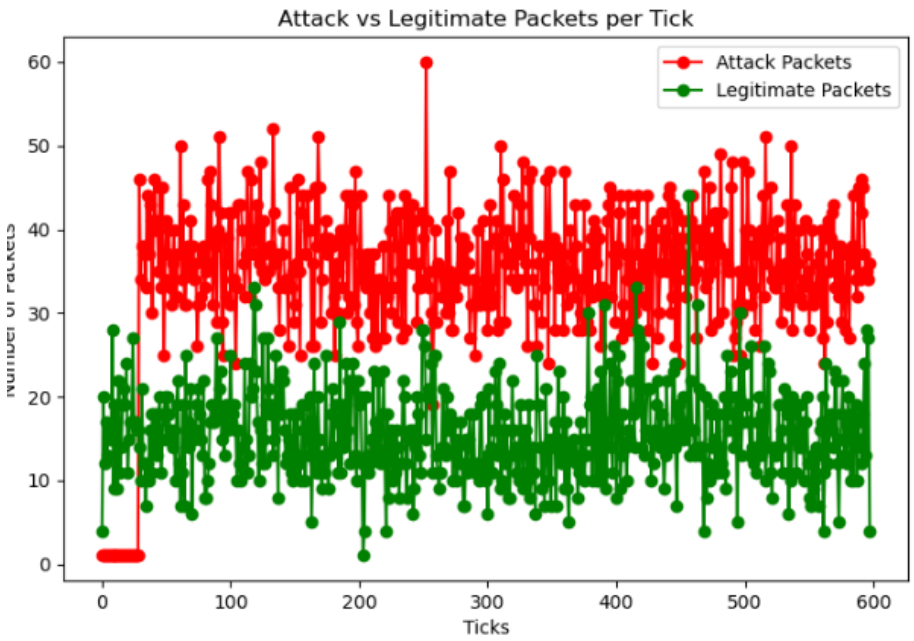
Overall, 67.1% of the total request has been blocked, which are 20130 requests.



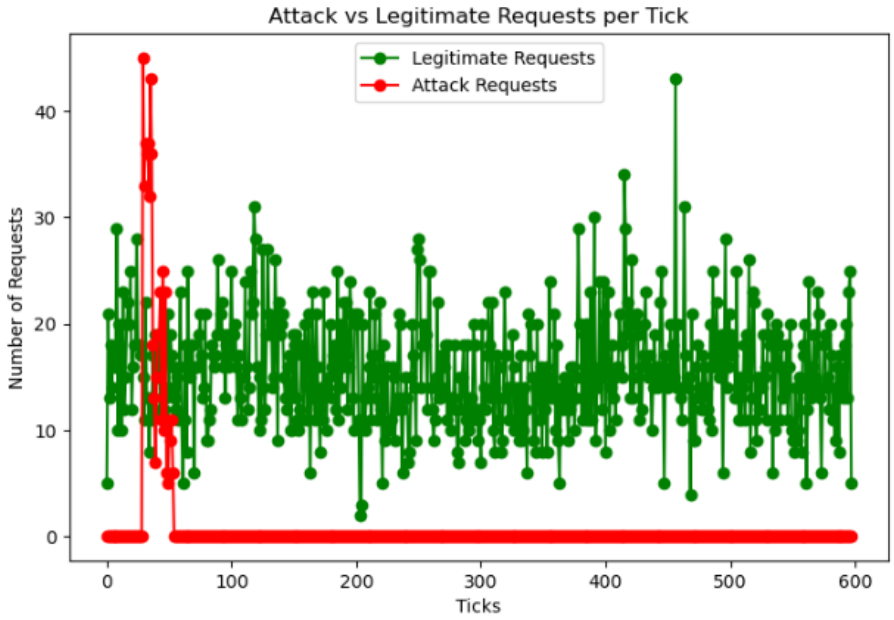
9,328 out of 10,000 Legitimate requests has been passed to the DNS Resolver, while 530 attack requests has passed to it.



Packets has been counted per the timestamp they had been sent, and as we can see , up until 5% of the total ticks, there were at most 30 packets. Afterwards, that attack has been started and we can see that there was at least 30 packets up until to 83 packets at max in the same timestamp.



This graph shows both the total legitimate packets and attack packets , and as we can see after 5% of the total ticks, attack packets start to arrive 2 times more than legitimate packet (As we choose 200% as our volume attack).

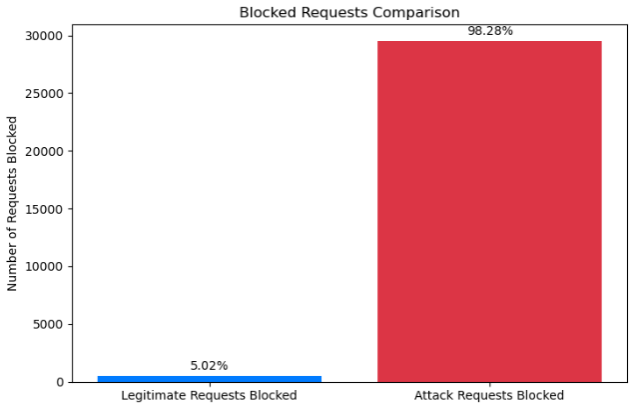


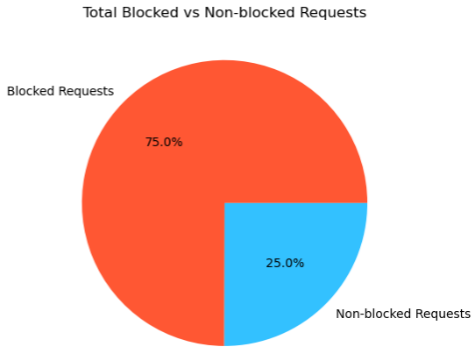
This graph shows both the request passed to the DNS Resolver, both legitimate and attack. As we can see in red, the moment the attack started packets had been sent to the server at high rates, and quickly decreased up until they are totally blocked. In green we can see that legitimate requests are successfully arrive at every timestamp.

Example 2

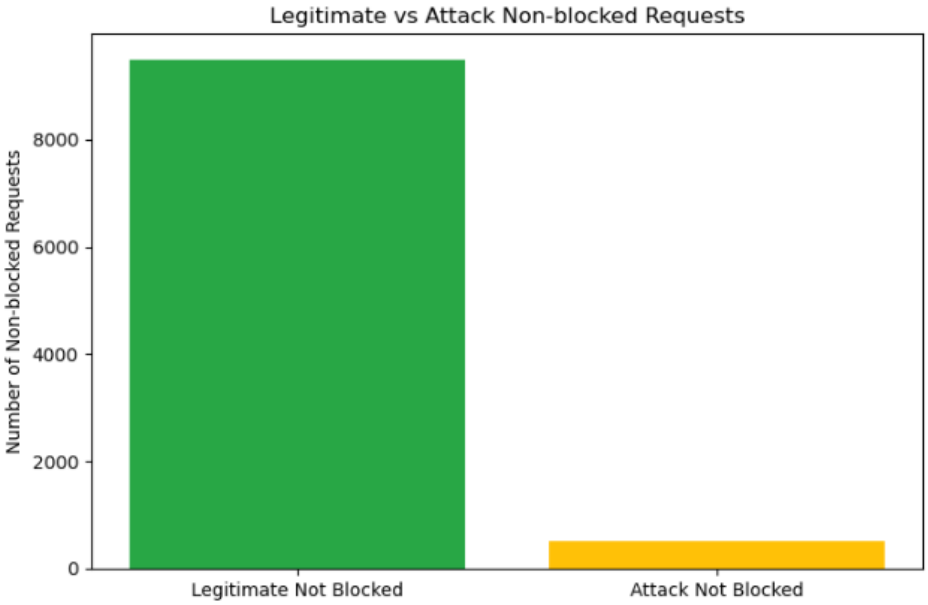
- The amount of data chosen is **10K** traces of the original traces.
- The volume of the attack is **30K** packets.
- The attack started at **30%** of the simulation time.

- Participated in the attack are: **74.125.47.17, 173.194.90.19, 74.125.47.84, 74.125.181.84, 74.125.47.20**.
- Total Requests: 40K, Attack requests: 30K , Legitimate 10K
- Blocked Requests: 29,986 , Attack Blocked 29,484 , Legitimate Blocked:502
- Percentage of Attack Traffic Blocked: 98.28%
- Percentage of Legitimate Traffic Blocked: 5.02%

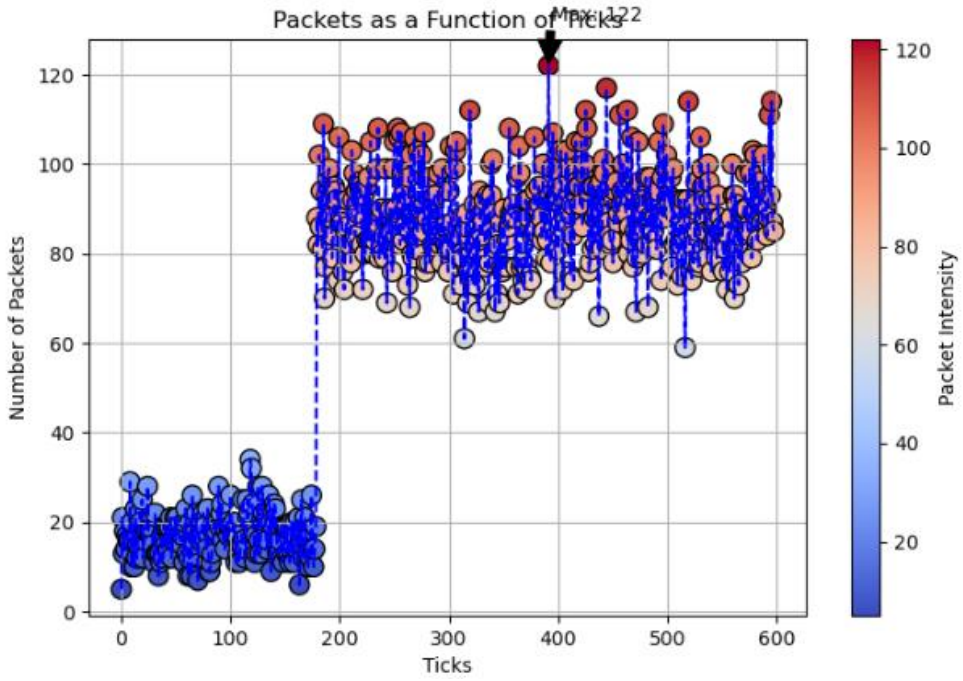




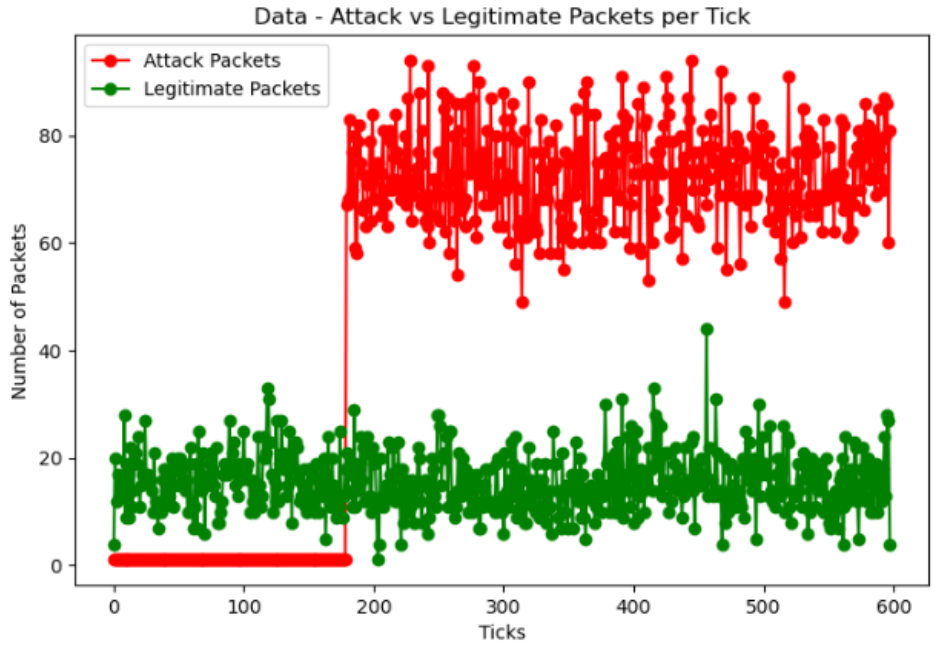
Overall,75% of the total request has been blocked, which are 30K requests.



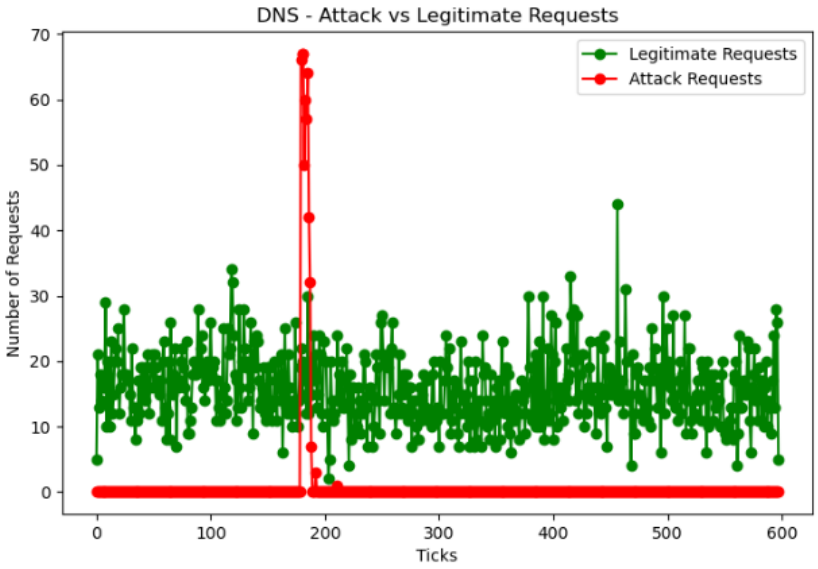
9,498 out of 10,000 Legitimate requests has been passed to the DNS Resolver, while 516 attack requests has passed to it.



Packets has been counted per the timestamp they had been sent, and as we can see , up until 30% of the total ticks, there were at most 38 packets. Afterwards, the attack has been started and we can see that there were at least 60 packets up until to 122 packets at max in the same timestamp.



This graph shows both the total legitimate packets and attack packets , and as we can see after 30% of the total ticks, attack packets start to arrive 3 times more than legitimate packet (As we choose 300% as our volume attack).

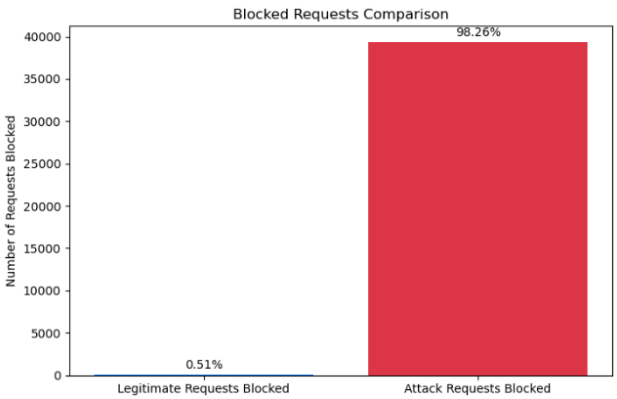


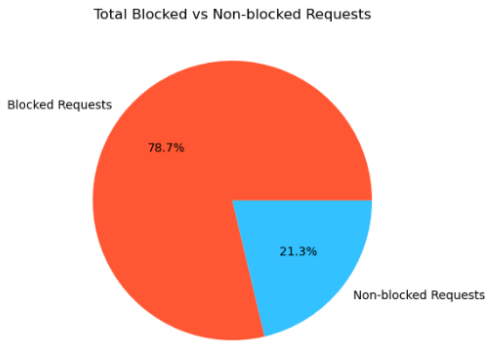
This graph shows both the request passed to the DNS Resolver, legitimate and attack. As we can see in red, the moment the attack started packets had been sent to the server at high rates, and quickly decreased up until they are totally blocked. In green we can see that legitimate requests are successfully arrive at every timestamp.

Example 3

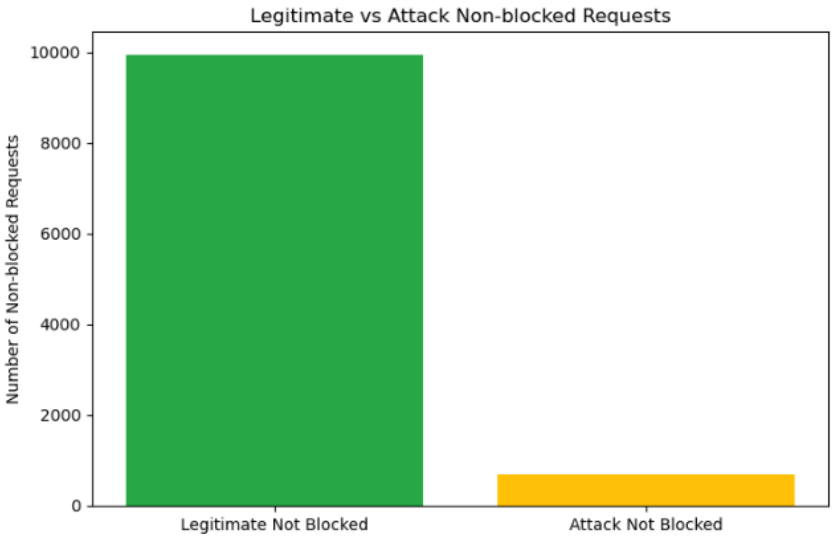
- The amount of data chosen is **10K** traces of the original traces.
- The volume of the attack is **40K** packets.
- The attack started at **5%** of the simulation time.
- The prefix size chosen is 2 means /16.

- The subnets that Participated in the attack are: **173.194.0.0, 74.125.0.0**
- Total Requests: 50K, Attack requests: 40K , Legitimate 10K
- Blocked Requests: 39353 , Attack Blocked 39302 , Legitimate Blocked:51
- Percentage of Attack Traffic Blocked: 98.26%
- Percentage of Legitimate Traffic Blocked: 0.51%

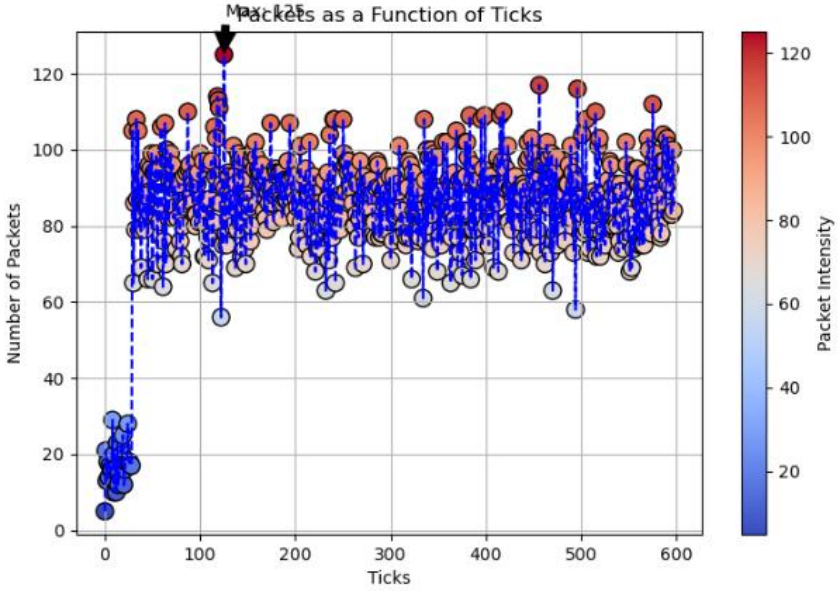




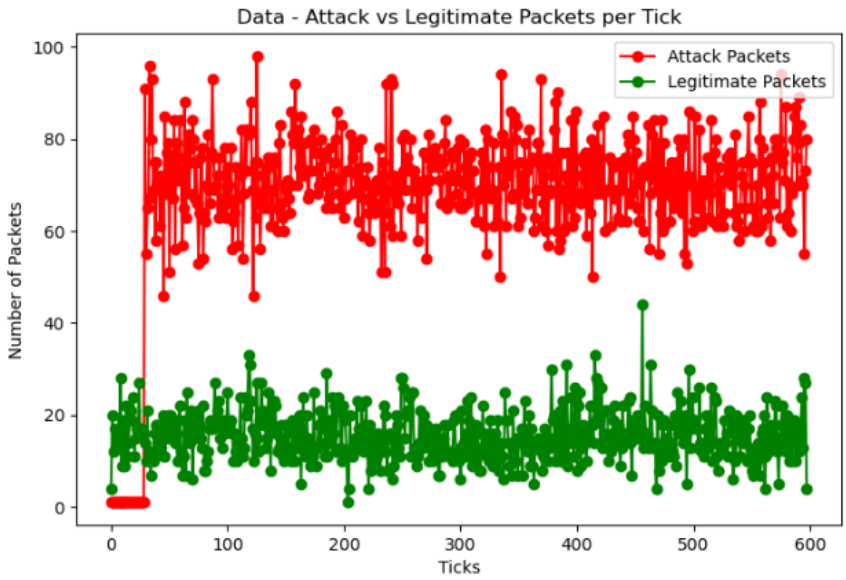
Overall,78.7% of the total request has been blocked, which are 39,353 requests.



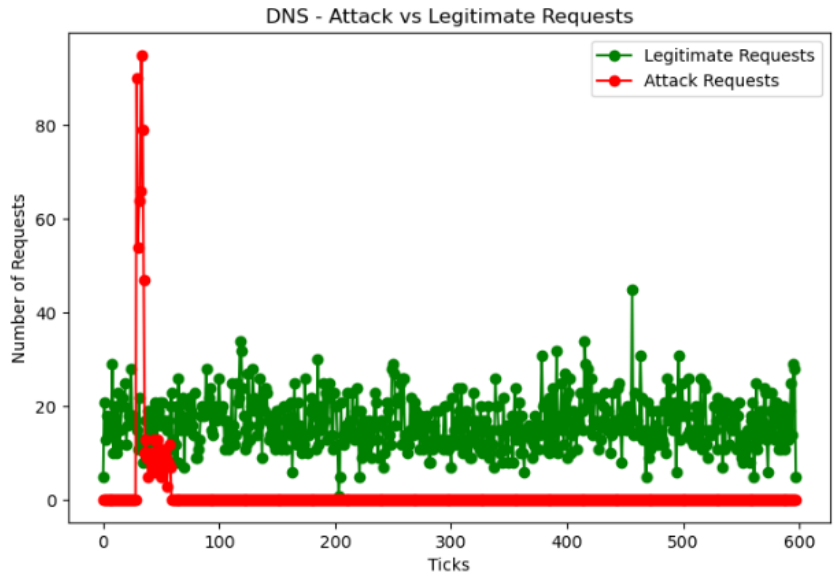
9,949 out of 10,000 Legitimate requests has been passed to the DNS Resolver, while 798 attack requests has passed to it.



Packets has been counted per the timestamp they had been sent, and as we can see , up until 5% of the total ticks, there were at most 30 packets. Afterwards, the attack has been started and we can see that there were at least 55 packets up until to 125 packets at max in the same timestamp.



This graph shows both the total legitimate packets and attack packets , and as we can see after 5% of the total ticks, attack packets start to arrive 4 times more than legitimate packet (As we choose 400% as our volume attack).



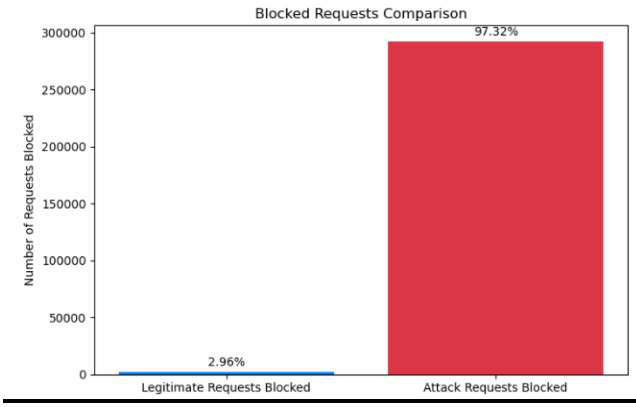
This graph shows both the request passed to the DNS Resolver, legitimate and attack. As we can see in red, the moment the attack started packets had been sent to the server at high rates, and quickly decreased up until they are totally blocked. In green we can see that legitimate requests are successfully arrive at every timestamp.

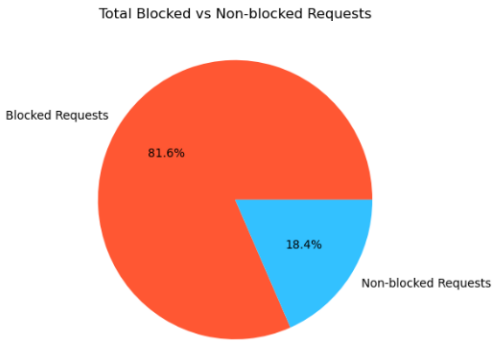
Example 4 – Larger data

We have used larger amount of data, and as results more we've got more timestamps to send packets in.

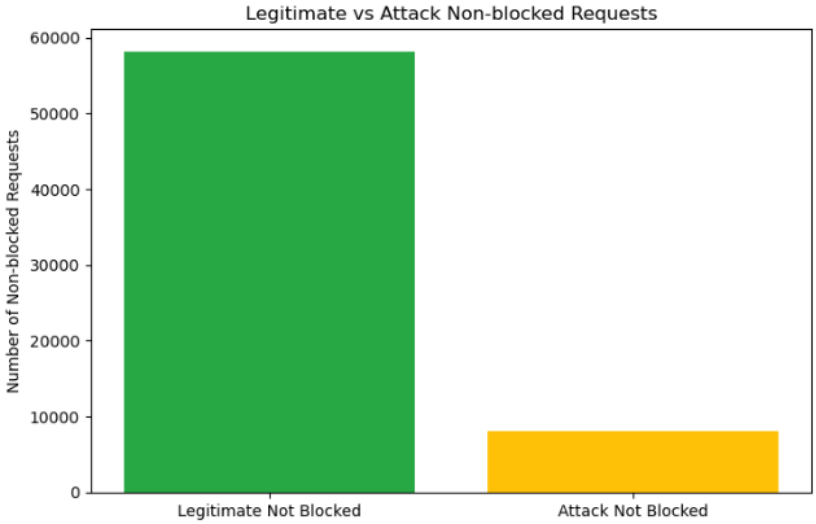
- The amount of data chosen is **60K** traces of the original traces.
- The volume of the attack is **300K** packets.
- The attack started at **10%** of the simulation time.
- The total number of legitimate source IP packets is **193**.
- The prefix size chosen is 2 means /16.

- The subnets that Participated in the attack are: **173.194.0.0, 74.125.0.0**.
- Total Requests: 360K, Attack requests: 300K , Legitimate 60K
- Blocked Requests: 293,752 , Attack Blocked 291,974 , Legitimate Blocked:1778
- Percentage of Attack Traffic Blocked: 97.32%
- Percentage of Legitimate Traffic Blocked: 2.96%

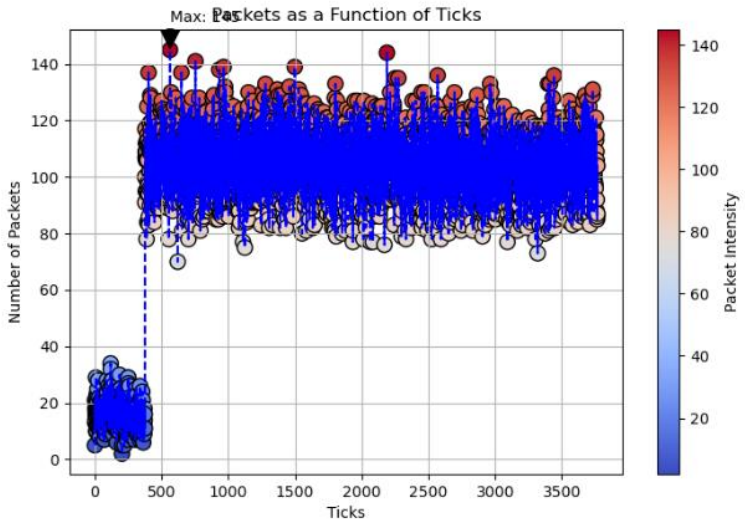




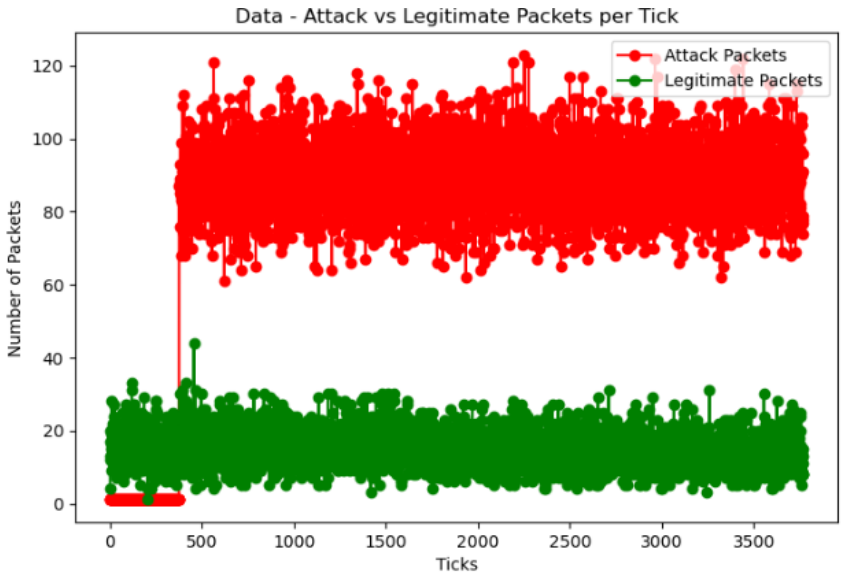
Overall,81.6% of the total request has been blocked, which are 293,760 requests.



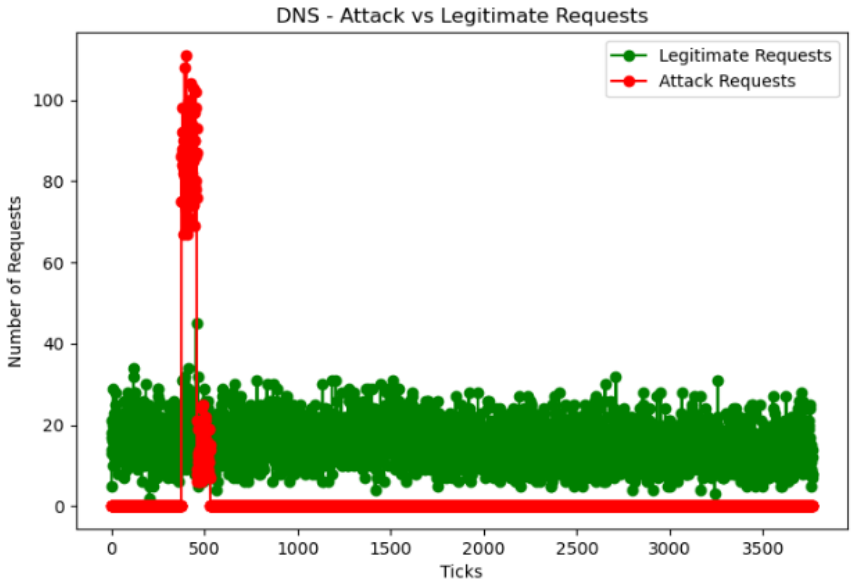
58,222 out of 60,000 Legitimate requests has been passed to the DNS Resolver, while 8026 attack requests has passed to it.



Packets has been counted per the timestamp they had been sent, and as we can see , up until 10% of the total ticks, there were a small vast of packets . Afterwards, the attack has been started and we can see that volume of the total packets has been dramatically increased.



This graph shows both the total legitimate packets and attack packets , and as we can see after 5% of the total ticks, attack packets start to arrive at much higher rates.



This graph shows both the request passed to the DNS Resolver, legitimate and attack. As we can see in red, the moment the attack started packets had been sent to the server at high rates, and quickly decreased up until they are totally blocked. In green we can see that legitimate requests are successfully arrive at every timestamp.