DDoS Attack Detection System With Markov Model-RNN integrated Aggregate Based Congestion Control (ACC)

1. Research Background and Objective

【Research Background】

- Cyber Attacks like DDoS attack became an alarming threat in commercial networks.
- Probability based network packet classification by Aggregate based Congestion Control (ACC).

【Challenges】

- Probability calculation does not take current network state and long term pattern in network into account.
- Thresholds for probability is not dynamic.

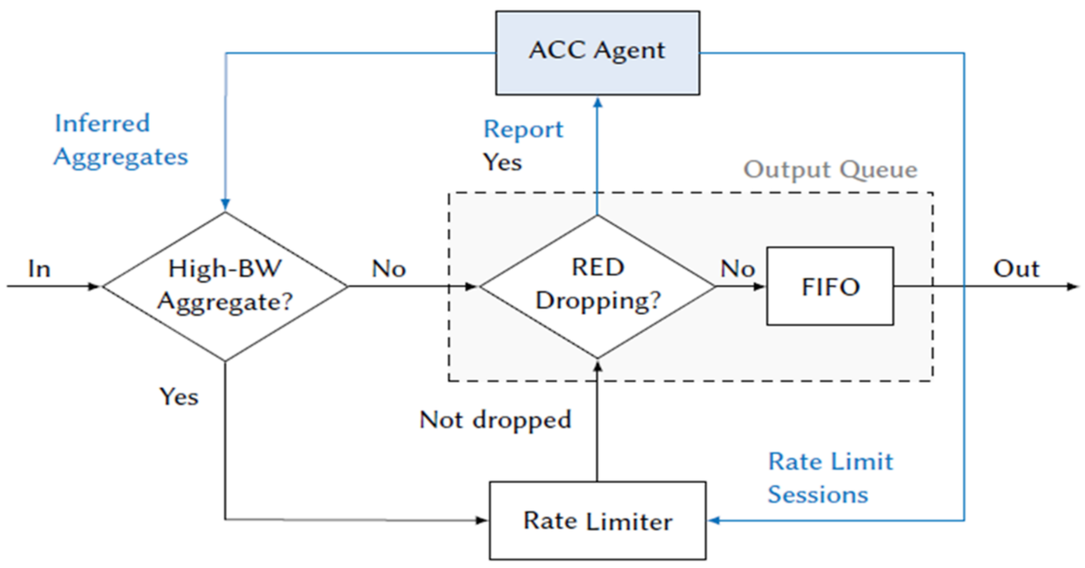
【Research Objective】

Proposing a dynamic probability calculation and threshold update.

2. Aggregate Based Congestion Control (ACC)

【Mechanism of ACC】

- Aggregate network packets according to common features.
- Check whether it is a high bandwidth traffic.
- Push the network traffic to rate limiter and random early detection segment.
- Report ACC agent and drop or keep packets according to probability.



【Usage】

- Can Detect DDoS at the arrival of network packet.
- Can be used different types of protocol dependent DDoS attack.

【Limitation】

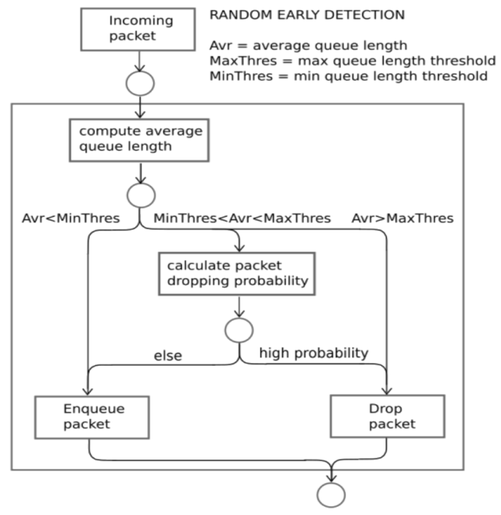
- Detection time is delayed due to packet analysis
  ⇒ Cannot store long term network traffic pattern.
- Static probability and threshold.

【Proposed Approach】

- Dynamic probability update through Markov model approach.
- Threshold update by Recurrent Neural Network (RNN).

3. Random Early Detection (RED)

- RED prevents congestion by randomly dropping packets before the queue is full.
- It uses average queue size to decide when to start dropping packets.
- It avoids global synchronization and promotes fairness among network flows.



4. Markov Model in ACC Agent

- It can model aggregates of network packet that causes traffic and generate probability from one state to another.

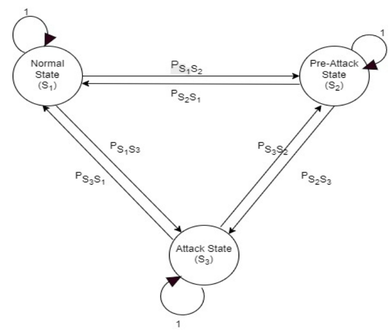
$$P(X_{t+1} = s_j \mid X_t = s_i, X_{t-1}, \ldots, X_0) = P(X_{t+1} = s_j \mid X_t = s_i) \qquad \mathbf{P} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{n1} & P_{n2} & \cdots & P_{nn} \end{bmatrix}$$

- Estimation of the probability that congestion is caused by a particular aggregate, and inform whether to trigger pushback.

$$\pi(a \mid s) = \text{Prob}(\text{action } a \text{ taken in state } s)$$

- Modelling normal congestion and heavy congestion in ACC agent.

$$\boldsymbol{\pi}_{t+1} = \boldsymbol{\pi}_t \cdot \mathbf{P}$$



5. Recurrent Neural Network in ACC Agent

- RNNs predict future network congestion by learning patterns from past traffic data.
- RNNs help in dynamic resource allocation and anomaly detection in aggregate traffic.
- It enable proactive congestion control by adjusting flow rates before congestion occurs.

$$h_t = \sigma(W_{xh}x_t + W_{hh}h_{t-1} + b_h)$$

$$r_t = f(W_{hr}h_t + b_r)$$

- RNN-LSTM (Long Term Short Memory) can store past traffic patterns.