1. Qual o ambiente em que esta estratégia está sendo aplicada? ISP, data plane…

A implantação de DDoS no domínio do provedor de serviços de Internet distribuído (ISP). propuseram sistemas de detecção de DDoS baseados em estruturas de processamento distribuído. Este tipo de implantação

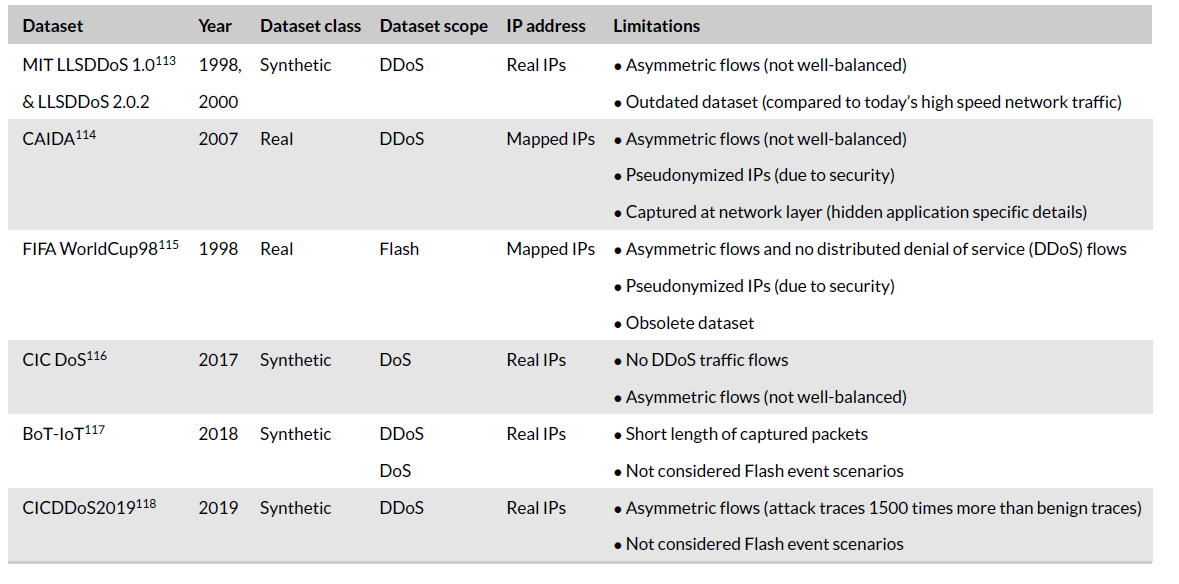
implantação de defesa em dois grupos com suas estruturas de design: defesa DDoS baseada em estruturas de processamento tradicional e distribuído



1. Qual o tipo de observação e interação existe no ambiente?

Ele recebe fluxos de tráfego de rede agregados para análise, o que ajuda a minimizar as taxas de falsos positivos. Analisa e armazena com eficiência uma grande quantidade de dados (fluxos de tráfego de rede) usando um cluster de nós.

1. Caso eles usem um dataset:



* Que técnicas de ML são usadas?
* Precision (*PR*): *PR*
* Detection rate/Recall (*DR*): *DR*
* False Positive Rate (FP*R*): *FPR*
* False Negative Rate (FN*R*): *FNR*
* True Positive Rate (TP*R*): *TPR*
* Confusion matrix
* True Negative Rate (TN*R*): *TNR*
* F-Measure (*FM*): *FM*
* Negative Predictive Value (NP*V*)
* F-Measure Complement (*FMC*):
* Classification rate/detection accuracy (*CR*)
* Balance accuracy (*Bacc*): *Bacc*
* Misclassification rate (*MR*):*MR*

1. Qual o tipo de dado? pcap, flow?

Pcap e Flow.

1. Como este dado será abordado em relação ao seu tipo? São dados categóricos? São dados numéricos ? São dados textuais?

Nao e citado no artigo a tipagem dos dados recolhidos.

1. Qual algoritmo de ML está sendo utilizado? Como este algoritmo está sendo aplicado (é possível utilizar mais de uma estratégia ao mesmo tempo)?

O artigo Não cita as tecnicas utilizadas pelos framework para a sua analise, ele apenas da uma introdução das ferramentas e uma conseituada do funcionamento da ferramenta implemetadas no DDoS