Classificação de tráfego DRDoS usando Aprendizado de Máquina

Mestrando: Rafael Tenfen
Orientador: Rafael Obelheiro
Joinville, 2020

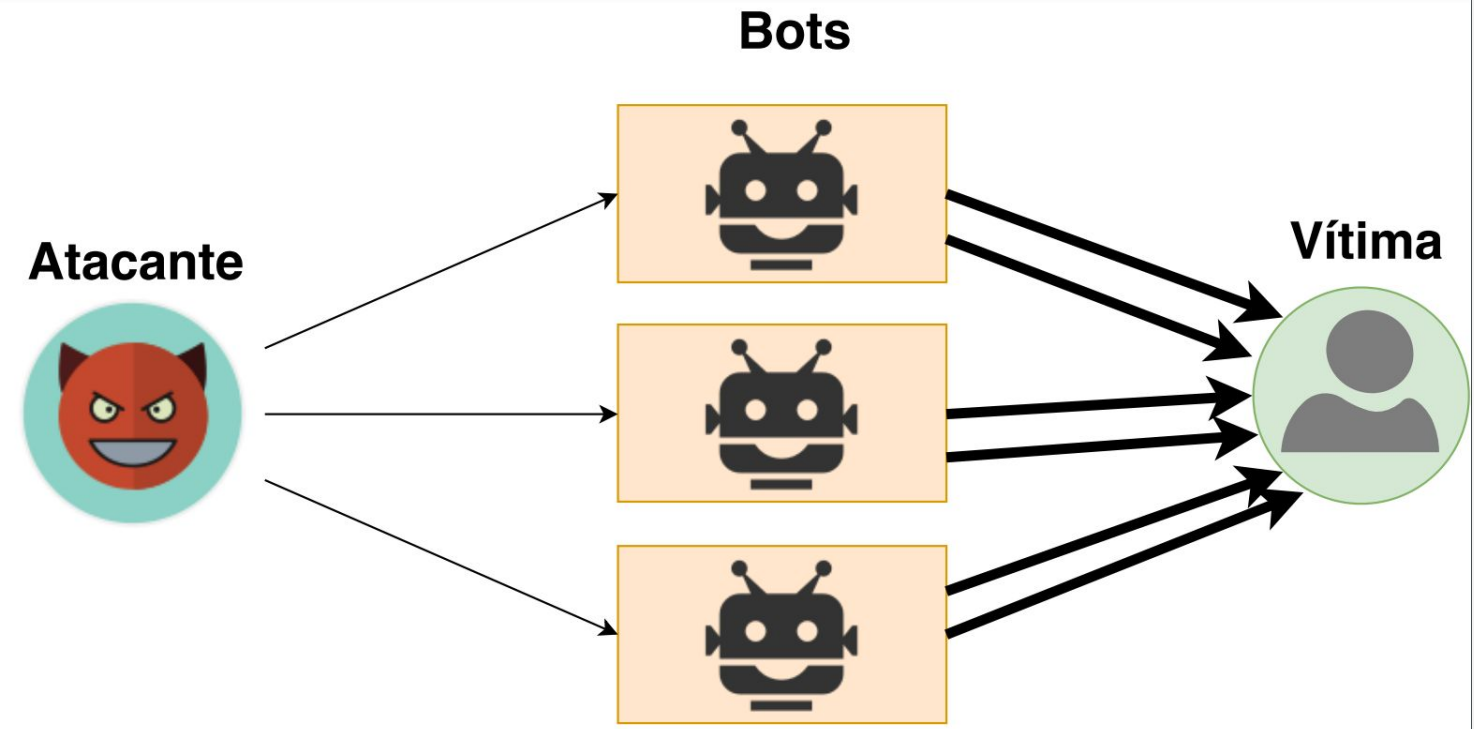
UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA

Agenda

- Ataques DDoS
- Ataques DRDoS
- Objetivos da Pesquisa
- 2018 - Machine Learning and Deep Learning Methods for Cybersecurity
- 2021 - Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions
- 2017 - Characterization of Tor Traffic using Time based Features
- 2019 - Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy
- 2019 - The hybrid technique for DDoS detection with supervised learning algorithms
- 2021 – Tensor based framework for Distributed Denial of Service attack detection

Ataques DDoS

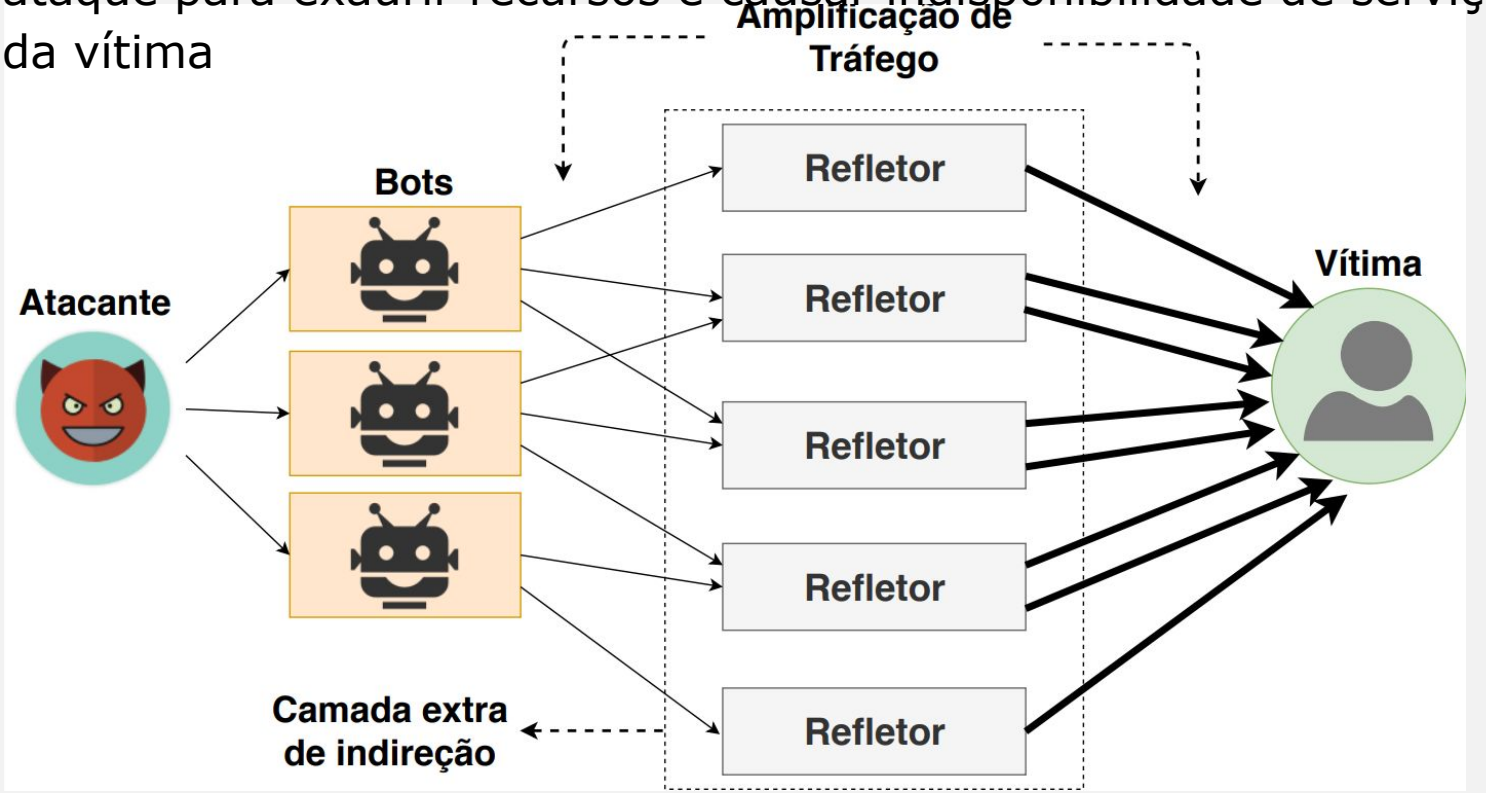
- DDoS (Distributed Denial of Service) - Técnica em que um atacante controla N dispositivos na rede e coordena o envio de tráfego à vítima com o objetivo de exaurir recursos e causar indisponibilidade de serviço do alvo



(HEINRICH, 2019)

Ataques DRDoS

- DRDoS (Distributed Reflection Denial of Service) - Técnica em que um atacante controla N dispositivos na rede (Bots) e coordena o envio de tráfego à vítima através de refletores que amplificam o tamanho da requisição, intensificando assim o ataque para exaurir recursos e causar indisponibilidade de serviço da vítima



(HEINRICH, 2019)

Objetivo da Pesquisa

- Para caracterizar ataques DDoS ou DRDoS no meio de requisições legítimas, algumas técnicas podem ser utilizadas, como por exemplo algoritmos de aprendizado de máquina para detectar padrões nas requisições

- Então, foi revisado e observado como outros trabalhos realizam a extração de seus dados, ou quais conjuntos de dados são utilizados para treinar o algoritmo para que seja possível utilizar em conjuntos de dados não rotulados.

- Além disso, quais os tipos de algoritmos de aprendizado de máquina esses trabalhos utilizam para identificar e rotular os dados.

Artigos Revisados

- Revisão
  - 2018 - Machine Learning and Deep Learning Methods for Cybersecurity
  - 2021 - Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions

- Demais
  - 2017 - Characterization of Tor Traffic using Time based Features
  - 2019 - Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy
  - 2019 - The hybrid technique for DDoS detection with supervised learning algorithms
  - 2021 - Tensor based framework for Distributed Denial of Service attack detection

2018 - Machine Learning and Deep Learning Methods for Cybersecurity

- Revisão literária
- Tráfegos de provedores de internet ISP
- pcap e flow

dataset

DARPA INTRUSION DETECTION DATA SETS
- 1998, 1999, 2000

KDD CUP 99 DATASET
- DARPA 1998

NSL-KDD DATASET
- KDD CUP 99 DATASET

ADFA DATASET
- 2013

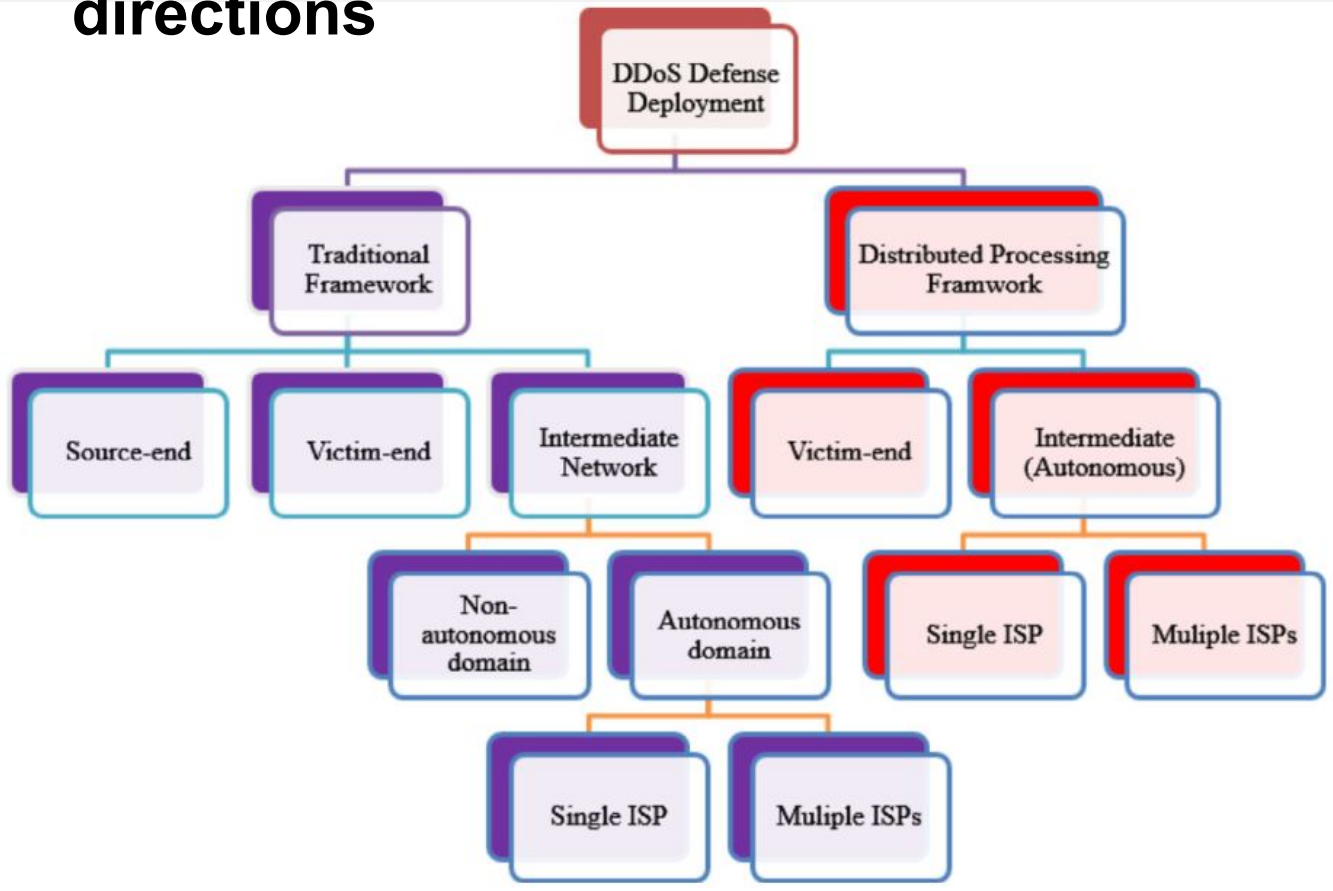
técnicas ML usadas

- SUPPORT VECTOR MACHINE (SVM)
- K-NEARESTNEIGHBOR (kNN)
- DECISION TREE
- DEEP BELIEF NETWORK (DBN)
- RECURRENT NEURAL NETWORKS (RNN)
- COVOLUTIONAL NEURAL NETWORKS (CNN)

2018 - Machine Learning and Deep Learning Methods for Cybersecurity

- Os dados foram definidos de modo categórico
- Foram analisados 39 trabalhos
- A maioria dos conjuntos de dados utilizados pelos trabalhos eram públicos
- O conjunto de dados mais utilizado foi o "KDD Cup 99" utilizado por mais de 50% dos trabalhos
- Os algoritmos utilizados pelos trabalhos foram aproximadamente:
  - 25% SVM (Support vector machines)
  - 25% KNN (k-nearest neighbors algorithm)
  - 25% DT (Decision Tree)
  - 25% Outros (C4.5, DBN, RNN, LSTM, GRU, CNN)

2021 - Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions



Defesa DDoS baseada em estruturas de processamento tradicional e distribuído

2021 - Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions

Dataset	Year	Dataset class	Dataset scope	IP address	Limitations
MIT LLSDDoS 1.0[113] & LLSDDoS 2.0.2	1998, 2000	Synthetic	DDoS	Real IPs	• Asymmetric flows (not well-balanced) • Outdated dataset (compared to today's high speed network traffic)
CAIDA[114]	2007	Real	DDoS	Mapped IPs	• Asymmetric flows (not well-balanced) • Pseudonymized IPs (due to security) • Captured at network layer (hidden application specific details)
FIFA WorldCup98[115]	1998	Real	Flash	Mapped IPs	• Asymmetric flows and no distributed denial of service (DDoS) flows • Pseudonymized IPs (due to security) • Obsolete dataset
CIC DoS[116]	2017	Synthetic	DoS	Real IPs	• No DDoS traffic flows • Asymmetric flows (not well-balanced)
BoT-IoT[117]	2018	Synthetic	DDoS DoS	Real IPs	• Short length of captured packets • Not considered Flash event scenarios
CICDDoS2019[118]	2019	Synthetic	DDoS	Real IPs	• Asymmetric flows (attack traces 1500 times more than benign traces) • Not considered Flash event scenarios

2021 - Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions

técnicas ML usadas

Precision (PR): PR

Detection rate/Recall (DR): DR

False Positive Rate (FPR): FPR

False Negative Rate (FNR): FNR

True Positive Rate (TPR): TPR

Confusion matrix

True Negative Rate (TNR): TNR

F-Measure (FM): FM

Negative Predictive Value (NPV)

F-Measure Complement (FMC):

Classification rate/detection accuracy (CR)

Balance accuracy (Bacc): Bacc

Misclassification rate (MR):MR

- Pcap Flow

UDESC

2017 - Characterization of Tor Traffic using Time based Features

- Rotular conjunto de dados
- Testar classificadores
- Descobrir qual tipo de aplicação está utilizando a rede Tor e para que.

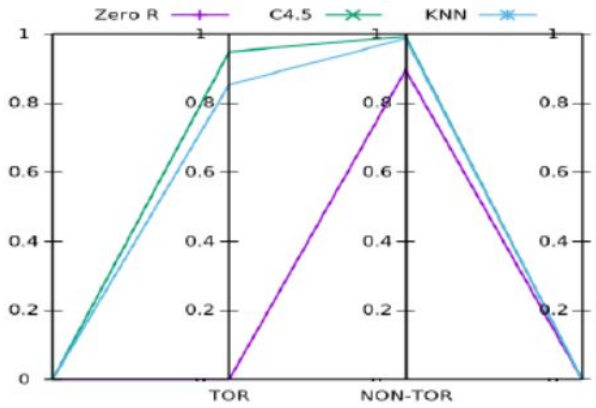
- A estratégia está sendo aplicada na rede de nodes de uma rede distribuída de servidores conhecida como Tor

- As técnicas de ML usadas:
  - Zero R
  - C4.5
  - KNN
  - Random Forest

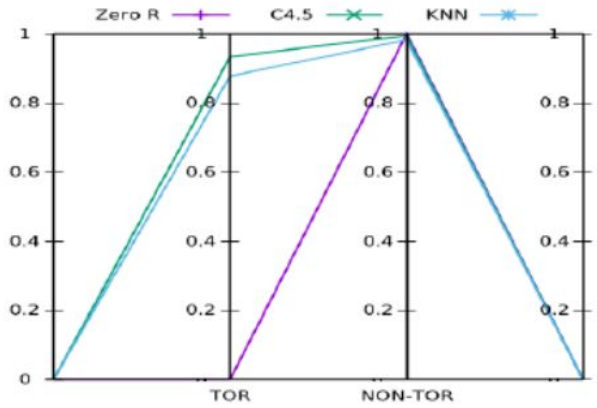
- pcap

- Dados categóricos utilizado para identificar protocolos de compartilhamento de arquivo como o Bittorrent e utilizaram Vuze

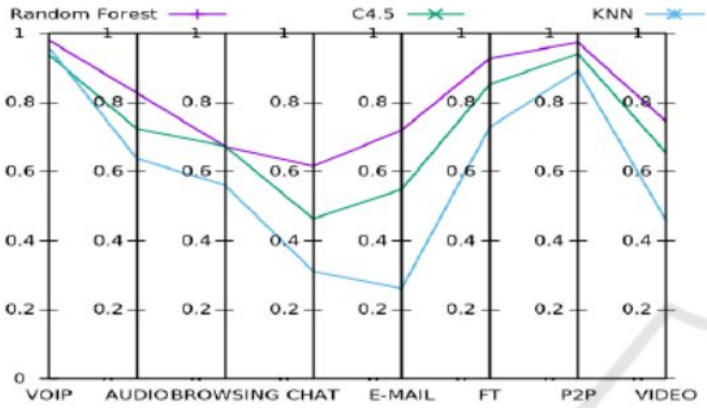
2017 - Characterization of Tor Traffic using Time based Features



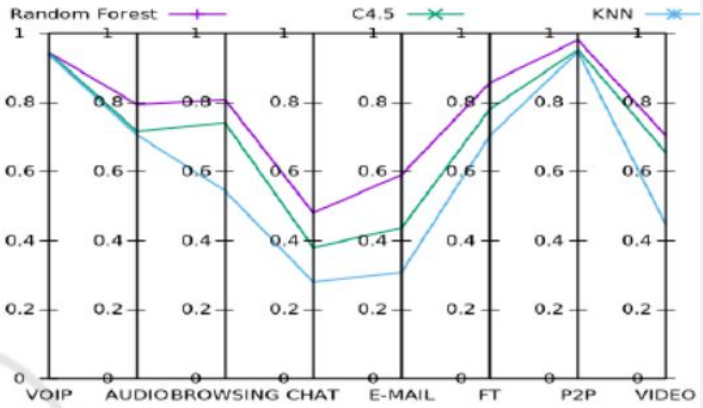
(a) Tor VS. Non-Tor Precision



(b) Tor VS. Non-Tor Recall



(c) Tor Characterization Precision



(d) Tor Characterization Recall

Figure 3: Precision and Recall of Validation experiments.

2019 - Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy

- Rede Vítima e Rede Atacante
  - **Rede Vítima:** um servidor, um firewall, dois switches e quatro PCs;
  - **Rede Atacante:** completamente separada.

- CICFlowMeter
- flow

dataset

CICDDoS2019
- Visão total dos dados recolhidos
- 2019

técnicas ML usadas

- ID3, Random Forest (RF), Native Bayes, e logistic regression
- RandomForestRegressor class do pacote scikit-learn.

2019 - Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy

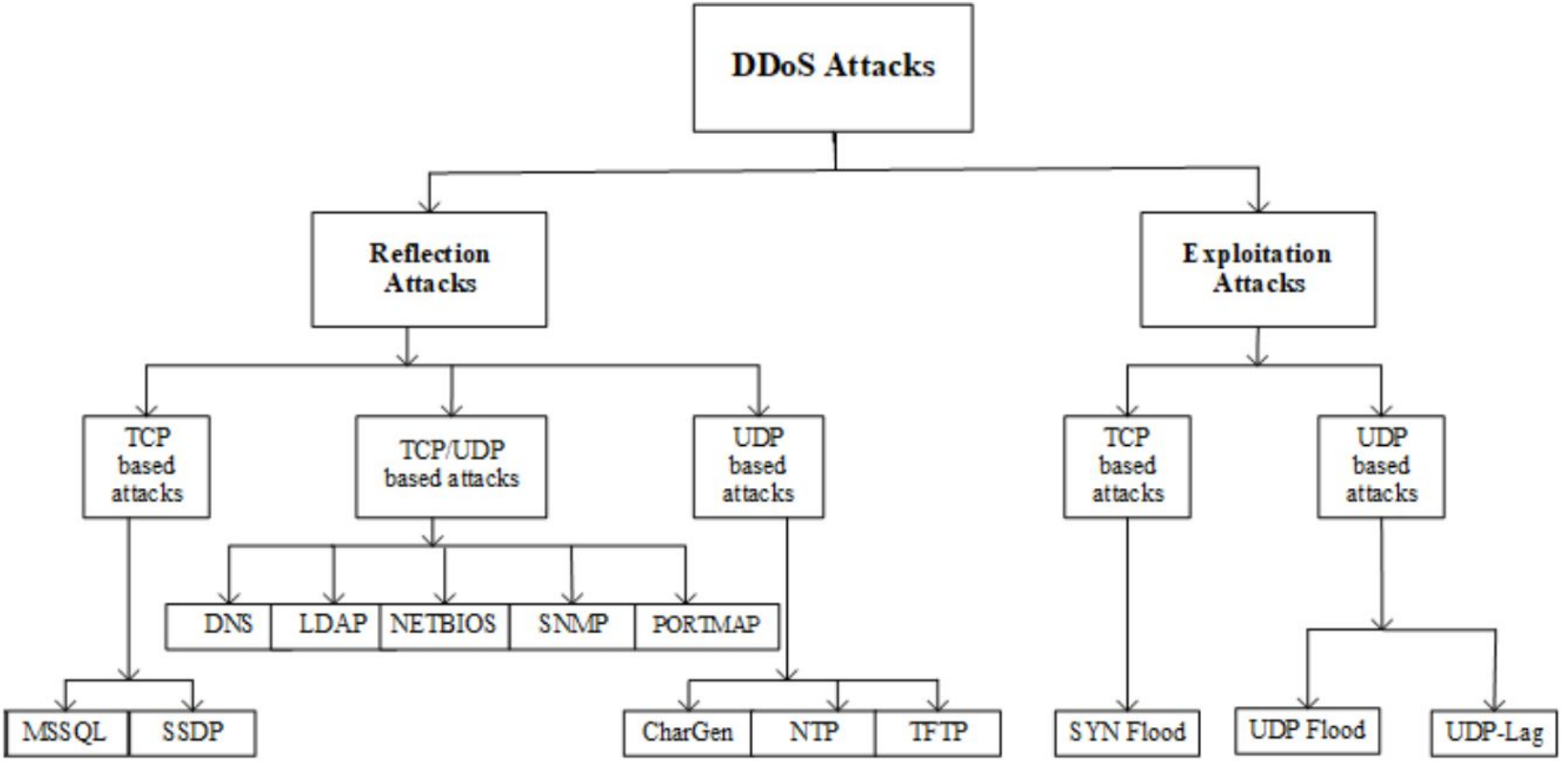


Figure 1: DDoS Attack Taxonomy

2019 - Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy

- Um algoritmo de cada vez para buscar as métricas

Precision (Pr) or Positive Predictive value: (TP + FP)

Recall (Rc) or Sensitivity: (TP + FN)

F-Measure (F1): precisão e recuperação

2019 - The hybrid technique for DDoS detection with supervised learning algorithms

- Data plane
- Lado do Cliente x Lado do Proxy.
- PCAP
- Múltiplos algoritmos que se beneficiam de todas as propriedades dos algoritmos simultaneamente.

dataset

NSL-KDD
- conjunto de dados aprimorado do KDDCUP'99

Alkasassbeh et al

técnicas ML usadas

- Naive Bayes classifier, random forest, decision tree, MLP e algoritmo K-NN

2021 - Tensor based framework for Distributed Denial of Service attack detection

- Desktop Intel Core i7-2600 3.40 GHz and 16 GB of RAM
- Pacote Python Scikit-Learn

- Datasets públicos
  - CICDDoS2019 e NSL-KDD 2009
    2019 e 2009

técnicas ML usadas

- AdaBoost (AB), Linear Discriminant Analysis (LDA), Logistic Regression (LR) and Random Forest (RF)
- sinais multidimensionais e algoritmos de classificação de aprendizado de máquina supervisionado

Referências

- Cert.br. 2016. Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS). [online] Available at: <https://www.cert.br/docs/whitepapers/ddos/> [Accessed 27 November 2021].
- Lashkari, A.H., Draper-Gil, G., Mamun, M.S.I. and Ghorbani, A.A., 2017, February. Characterization of tor traffic using time based features. In ICISSp (pp. 253-262).
- Maranhão, J.P.A., da Costa, J.P.C., Javidi, E., de Andrade, C.A.B. and de Sousa Jr, R.T., 2021. Tensor based framework for Distributed Denial of Service attack detection. Journal of Network and Computer Applications, 174, p.102894.
- Hosseini, S. and Azizi, M., 2019. The hybrid technique for DDoS detection with supervised learning algorithms. Computer Networks, 158, pp.35-45.
- Patil, N.V., Rama Krishna, C. and Kumar, K., 2021. Distributed frameworks for detecting distributed denial of service attacks: A comprehensive review, challenges and future directions. Concurrency and Computation: Practice and Experience, 33(10), p.e6197.
- Sharafaldin, I., Lashkari, A.H., Hakak, S. and Ghorbani, A.A., 2019, October. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-8). IEEE.
- Heinrich, T., 2019. Caracterizaçao de Ataques DRDoS Usando Honeypot (Doctoral dissertation, Dissertaçao de mestrado em Computaçao Aplicada, UDESC, Joinville (SC)).
- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C., 2018. Machine learning and deep learning methods for cybersecurity. Ieee access, 6, pp.35365-35381.

Obrigado

UDESC – Universidade do Estado de Santa Catarina

rafaeltenfen.rt@gmail.com

Classificação de tráfego DRDoS usando Aprendizado de Máquina

Mestrando: Rafael Tenfen
Orientador: Rafael Obelheiro
Joinville, 2020

UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA

Denial-of-Service Attack Detection using Machine Learning in Network-on-Chip Architectures

- Comunicação on-chip
- Detecção de ataque DoS baseado em ML
- Dataset
  - IID 1 e IID 2
    Gerado automaticamente

- Packet traces ou flits
- Dados textuais

técnicas ML usadas

Naive Bayes Classifer (NBC)	6-Layer Neural Network (6NN)
Logistic Regression (LRN)	K-Neighbors Classifier (KNN)
2-Layer Neural Network (2NN)	LightGBM Classifier (LGB)
3-Layer Neural Network (3NN)	Decision Tree Classifier (DCT)
4-Layer Neural Network (4NN)	Random Forest Classifier (RFC)
5-Layer Neural Network (5NN)	XGBoost Classifier (XGB).