CSE 310 Final Project Proposal

Sudara & Rediet & Merry

Proposal for UDP Flooding-Attack Detection

- What is the problem that you will be investigating? Why is it interesting?

  UDP attacks as they can disrupt servers and congest networks. SDNs are especially vulnerable to DDoS attacks.

- What method or algorithm are you proposing? If there are existing implementations, will you use them and how? How do you plan to improve or modify such implementations?

  We will be using deep learning algorithms to predict whether there is an attack or not based on a certain threshold of UDP packet in-flow.
  We will modify an existing implementation by using a different deep learning algorithm that has a better prediction on DDos attacks.

- What reading will you examine to provide context and background?

  - https://www.ciena.com/insights/what-is/What-Is-SDN.html
  - https://www.hindawi.com/journals/scn/2018/9804061/
  - https://www.researchgate.net/publication/329971957_Using_SVM_to_Detect_DDoS_Attack_in_SDN_Network
  - https://www.academia.edu/24576437/Real_Time_Detection_and_Classification_of_DDoS_Attacks_using_Enhanced_SVM_with_String_Kernels

- How will you evaluate your results? Qualitatively, what kind of results do you expect (e.g. plots or figures)? Quantitatively, what kind of analysis will you use to evaluate and/or compare your results (e.g. what performance metrics or statistical tests)?

  We will measure our results based on the accuracy by which our algorithm detects DDos attacks.

- Plan
  - ★ Week 1: Learning about SDN and UDP packets including DDos
    Testing and deploying the open source github link below:
    Link: https://github.com/supr3m3/UDP-Flood-Detection-in-SDN.
  - ★ Week 2: Generating UDP packets for both normal and abnormal traffic.
    Implement better ML algorithm to improve DDoS attack-detection
  - ★ Week 3: Test and document the implementation
  - ★ Week 4: Preparing for presentation