DDoS Detection in Software-Defined Networks

Raahul Natarrajan

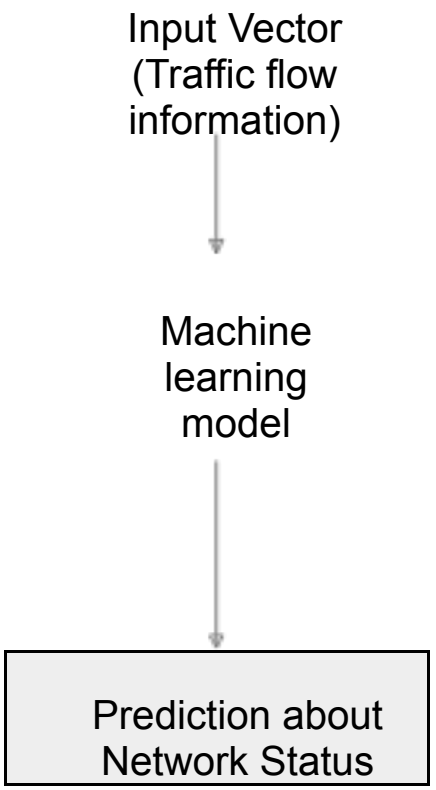
Institute for Software Integrated Systems

Overview

- Software-Defined Network (SDN) - network that uses software to control network infrastructure and traffic flow
- Distributed Denial of Service (DDoS) attack - attack where a target is overwhelmed by network traffic from multiple sources causing disruption in the target's network services
- Given traffic flow information in a SDN, how can we detect a DDoS attack on the network?

Tested Approaches

- Entropy-based
  - Calculate the network's current entropy using traffic flow information
  - Determine if the network is under attack based on anomalies in entropy
- Machine Learning
  - Use traffic flow information as a feature vector
  - Apply a machine learning model to predict the network state
  - Decision Tree, Naive Bayes Classifier, SVM, Random Forest
  - Most performant: random forest method



Results

- Entropy method works well in testing scenario
  - Manages to detect DDoS attack during replayed attack scenarios
  - Unable to detect DDoS attacks during refractory period where network is recovering from DDoS attack
- Machine Learning method works with dataset but not in testing scenario
  - Testing scenario does not exhibit same traffic pattern as learned data
  - Model needs more relevant data to perform well

Next Steps

- Create new dataset for the machine learning approach
  - Train model to accurately detect various types of malicious traffic
- Test both approaches using different network scenarios
- Investigate failure cases for DDoS detection
  - Running detection using the SDN Controller (centralized) vs. virtual switches in the SDN (localized)

Internship

- Lessons learned
  - Communicate frequently
  - Document thoughts
- Challenges
  - Initial learning curve with tools
  - Running into problems with the framework
- What went well
  - Very educational experience
  - Better understanding of the field of SDN