NATIONAL INSTITUTE OF TECHNOLOGY, KARNATAKA.

DETECTING A DoS ATTACK USING MACHINE LEARNING.

Project Proposal

Prepared for: Internet and Technology and Applications.

Prepared by: Siddhartha Chowdhuri (15CO246), Ved Choupane(15CO212), Aswin Manoj(15CO209)

January 5, 2018

EXECUTIVE SUMMARY

Abstract

One of the major security flaws experienced by WSNs is denial of service (DoS) which can even lead to the breakdown of the complete system or to wrong decisions being made by the system that can cause adverse results.Our project aims to detect the the probability of a DoS attack by using Machine Learning techniques.

Implementation

We plan to generate the dataset by using Vanderbilt Simulator which simulates a DoS attack. In the simulator we take the normalized key parameters as features for our model. We will take 100 training examples and 30 testing examples as our train-test split (70-30) and build a model with it.Primarily, we focus on doing a comparative study of models such as SVM,Neural Networks and XGBoost and build a model with the highest accuracy.

Hardware/Software Requirements:

Dataset Generation : Vanderbilt Simulator, Models : SVM, Neural Networks, XGBoost, Decision Trees, Libraries: scikit-learn, matplotlib, pandas, numpy, seaborne.

Work Distribution.

- Siddhartha Chowdhuri : Work on building the model and tuning the hyper parameters for best accuracy.
- Ved Choupane : Generate the dataset and work on visualization of the data.
- Aswin Manoj : Work on data extraction, preprocessing and feature-engineering in order to get the best features.

WORKFLOW OF THE PROJECT :