# *An abstract on*

# Detection of DDoS Attack

# *Submitted in partial fulfillment of the requirements*

*for the award of the degree of*

#### BACHELOR OF TECHNOLOGY

*in*

## Computer Science & Engineering

## *by*

**C. Lavanya (164G1A0547)**

**B. Chandrika (164G1A0518)**

**K.N.V. Kishore Kumar (164G1A0538)**

**T. Kumuda (164G1A0542)**

Under the Guidance of

## Mr B. Sreedhar M.tech

Assistant professor



## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Srinivasa Ramanujan Institute of Technology AnantHapuramu

**(Accredited by NAAC with ‘A’ Grade & Accredited by NBA, Affiliated to JNTUA, Approved by AICTE, New Delhi)**

**2019-2020**

**ABSTRACT**

Most of the existing ML-based DDoS detection approaches are under two categories: supervised and unsupervised. Supervised ML approaches for DDoS detection rely on availability of labeled network traffic datasets.

Whereas, unsupervised ML approaches detect attacks by analyzing the incoming network traffic. Both approaches are challenged by large amount of network traffic data, low detection accuracy and high false positive rates.

In this we present an online sequential semi-supervised ML approach for DDoS detection based on network Entropy estimation,Co-clustering, Information Gain Ratio and Exra-Trees algorithm. The unsupervised part of the approach allows to reduce the irrelevant normal traffic data for DDoS detection which allows to reduce false positive rates and increase accuracy.

Whereas, the supervised part allows to reduce the false positive rates of the unsupervised part and to accurately classify the DDoS traffic.

**Date Signature of the Guide**