Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm

RESEARCH PAPER PRESENTATION

Course Name: Artificial Intelligence Laboratory (CSE 3812)
Course Teacher: Rahad Khan (RaK)
Department of Computer Science and Engineering

TEAM MEMBERS

Fardin Ehsan Ahmed (011 201 131)
Sanjida Nafin Riya (011 202 065)
Shakin Shahria (011 201 055)
Subhey Sadi Rahman (011 212 074)

AGENDA

04 Abstract

05 Introduction

06 Literature Review

07 Methodology

08 Results

09 Findings

10 Our Idea

Abstract

- Rapid increase and complexity of IPv6 network traffic.
- Adoption of lightweight KNN optimization algorithm for DoS intrusion detection in IPv6 network environment.
- Double dimensionality reduction of features through information gain rate.
- Optimization of sample Euclidean distance measurement using information gain rate as weight
- Improved overall detection performance for IPv6 network traffic characteristics.

Introduction

- Exhaustion of traditional IPv4 network addresses and the development of NAT technology
- Introduction of IPv6 protocol to address the problem of insufficient addresses
- Differences between IPv6 and IPv4 in terms of address availability and protocol structure
- Increase in DoS attacks related to IPv6 despite the introduction of IPv6 protocol
- Challenges in detecting DoS attacks in IPv6 networks due to increasing traffic volume and poor adaptability of IDS based on specific rules.

Literature Review

- IPv6 Network Traffic
- Intrusion Detection Systems (IDS)
- DoS Attacks in IPv6
- K-Nearest Neighbors (KNN) Algorithm
- Dual Dimensionality Reduction
- Information Gain Rate
- GR-AD-KNN Algorithm
- Advancing DoS Intrusion Detection in IPv6

Methodology

- Ensuring algorithm classification verification:
    - It retains small groups.
    - Random selection of diverse sample based on size.
- Experiment divides into:
    - Dual Dimensionality Reduction with information gain rates
    - Evaluating GR-AD-KNN algorithm performance.
- Optimizing KNN Algorithm for Intrusion Detection
- Developed GR-AD-KNN algorithm
- Evaluation metrics:
    - F1 - score = (Precision * Recall) / (Precision + Recall)

Results

- F1- Score of GR-KNN vs GR-AD-KNN
- F1- Score Average of TAD-KNN vs GR-AD-KNN

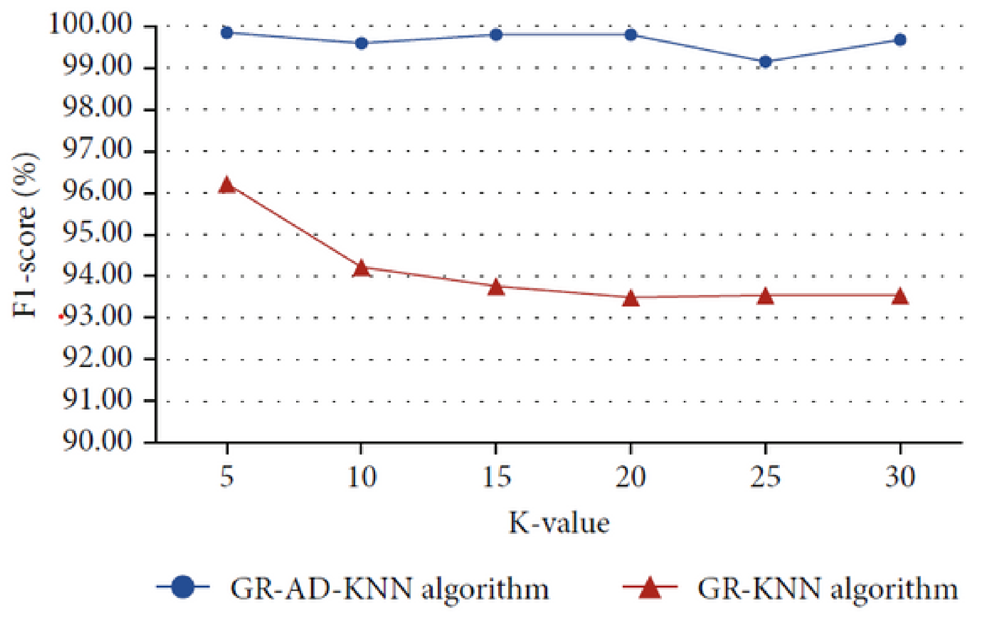

Figure 2: GR-KNN algorithm and GR-AD-KNN algorithm detection.

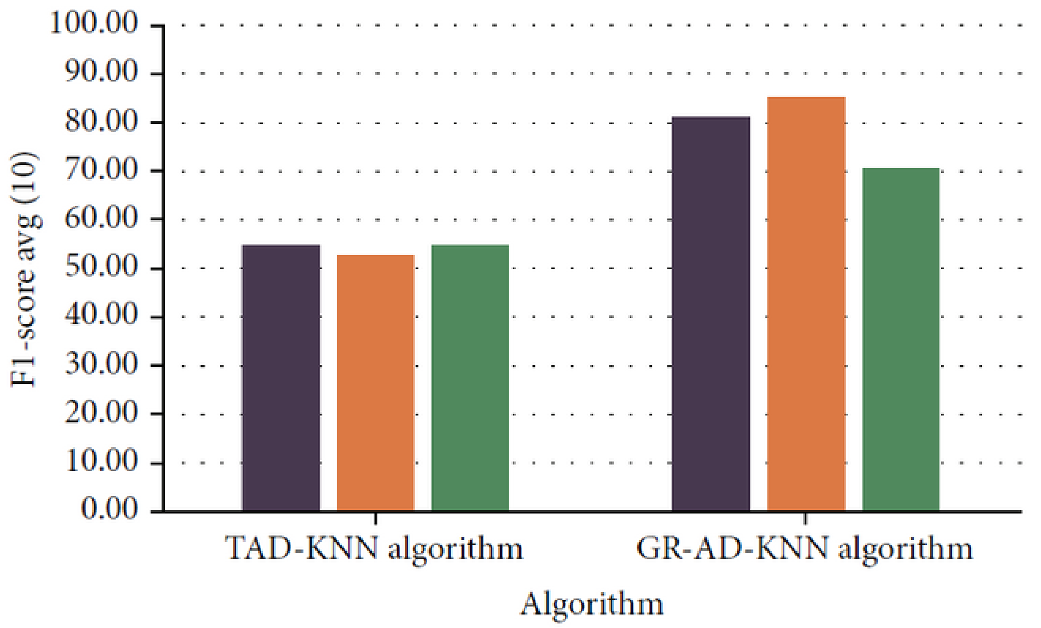

Figure 3: Ten average F1-Score detection results of Teardrop attack.

Findings

Evaluation of feature importance, enhanced classification efficiency and essential feature impact.

GR-AD-KNN Algorithm has beter performance than GR-KNN and TAD-KNN

Improvement of classification accuracy, algorithm stability and addresses challenges with distant sample effects and small group classification

Our Idea

- No specific detection accuracy was provided.
- The test result is not based on IPv6 related dataset. The dataset is an IPv4 KDD Cup 99 dataset.
- ML-based IDS is outdated because of low throughput and high false-positive rates.
- Deep Learning based techniques such as RNN, LSTM, GRU etc. could be used.
- Include additional evaluation metrics such as Precision, Recall, Detection Rate, FAR, DR, FP etc.

THANK YOU!

DO YOU HAVE ANY QUESTIONS?