Network Intrusion Detection Using SVMs

CS419 Project, IIT Bombay
Group name : The Alpha Clan
(23B2174, 23B2173, 23B2474, 23B0054, 23B2230)

Abstract

Spam and network intrusions threaten the security of modern networks, leading to potential data breaches and operational disruptions. This report explores the application of Support Vector Machines (SVMs) for detecting malicious network activities. The proposed approach involves preprocessing network datasets, training SVM models, and evaluating their performance using metrics such as accuracy and precision. The findings demonstrate the efficacy of SVMs in accurately identifying attack patterns, making them a valuable tool for network security.

1. Methodology

The methodology consists of several key steps aimed at preparing the data and building a robust SVM model.

1.1. Dataset and Preprocessing

The dataset used is the KDD Cup 1999 10% subset, which contains network connection logs labeled as either normal or specific attack types. Preprocessing steps include:

- **Label Mapping:** Target labels were grouped into two categories:
  - `smurf.` and `neptune.` mapped to -1 (attack).
  - `normal.` mapped to 1 (benign traffic).
- **Encoding Non-Numeric Data:** Non-numeric columns were encoded using `LabelEncoder`.
- **Feature Scaling:** Features were scaled using `StandardScaler`.
- **Dimensionality Reduction:** PCA was applied to reduce complexity while preserving variance.

1.2. Model Training

An SVM with an `rbf` kernel was selected to capture non-linear decision boundaries. Key hyperparameters were set as:

- **C**: 1, balancing model complexity and accuracy.
- **Gamma**: `scale`, for automatic adjustment.

The dataset was split into training (80%) and testing (20%) sets using stratified sampling.

1.3. Evaluation

The model's performance was evaluated using:

- **Accuracy:** Overall model effectiveness.
- **Precision, Recall, F1-Score:** Metrics for class-level evaluation.
- **Classification Report:** A comprehensive performance summary.

2. Results

The SVM model achieved exceptional results in both binary and multi-class classification tasks.

2.1. Binary Classification

Binary classification involved detecting attacks (`smurf.` and `neptune.`) versus normal traffic:

- **Accuracy:** 99.99%
- **Precision, Recall, F1-Score:** Near-perfect performance for both classes.

Performance Metrics:

Class	Precision	Recall	F1-Score
Attack (-1)	1.00	1.00	1.00
Normal (1)	1.00	1.00	1.00
Accuracy		99.99%	

2.2. Multi-Class Classification

The model handled multiple attack types, demonstrating strong generalization for major classes:

- **Accuracy:** 99.87%
- High precision and recall for dominant classes (`normal.`, `smurf.`).
- Limited performance on minor classes due to data imbalance.

Performance Metrics for Key Classes:

Class	Precision	Recall	F1-Score
Normal	1.00	1.00	1.00
Smurf	0.98	0.99	0.99
Neptune	0.97	0.96	0.97
Minor Attack Types	0.75	0.69	0.72
Accuracy		99.87%	

These results underline the importance of balancing class representation during training.

3. Conclusion

The SVM model demonstrated exceptional accuracy in detecting network intrusions, proving its utility in binary and multi-class classification tasks. The preprocessing steps, such as scaling and dimensionality reduction, were critical for these results.

Future work could involve:

- Hyperparameter tuning using grid search or Bayesian optimization.
- Exploring ensemble models to improve minor class performance.
- Deploying the model in real-time systems for proactive intrusion prevention.

SVMs remain a robust choice for network security applications, capable of handling complex, imbalanced datasets effectively.