Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology
ISSN: 2278-5140
Volume 14 Issue 01, 2025

OptiSecure: Hybrid SVM and ACO-based Intrusion Detection with Feature Optimization

Ms. Annu
Assistant Professor, Department of Computer Science & Engineering
MERI College of Engineering & Technology, Bahadurgarh, India.

Peer Review Information

Submission: 11 May 2025

Revision: 10 June 2025

Acceptance: 22 June 2025

Keywords

Intrusion Detection System (IDS)
Ant Colony Optimization (ACO)
Support Vector Machine (SVM)
Cybersecurity
Anomaly Detection

Abstract

In the era of modern networking, detecting cyber threats with high accuracy and minimal computational overhead has become increasingly vital. This paper presents an enhanced anomaly-based intrusion detection system (IDS) using a hybrid model combining Ant Colony Optimization (ACO) and Support Vector Machine (SVM). The CICIDS2017 dataset is used to evaluate the proposed approach, representing real-world traffic with diverse attack patterns including DoS, DDoS, Brute Force, Botnet, and Infiltration attacks. Experimental results show that the ACO-SVM model achieves a detection rate of 90.56%, false alarm rate of 9.44%, and time complexity of 0.32 seconds, outperforming ACO-ANN, ACO-NB, and PSO-SVM models. The results confirm that ACO combined with SVM provides efficient, scalable, and accurate intrusion detection performance.

Introduction

Cybersecurity challenges have escalated due to the rapid growth of connected systems and the evolving sophistication of network attacks. Traditional detection systems like firewalls and VPNs are unable to identify complex or zero-day attacks effectively. Anomaly-based Intrusion Detection Systems (IDS)(6) are designed to identify deviations from normal network behavior, making them suitable for detecting previously unseen attacks.

Machine learning-based IDS have shown significant promise in improving accuracy and adaptability. Among these, Artificial Neural Networks (ANN) and Support Vector Machines (SVM) are two of the most effective supervised classifiers. However, high-dimensional network data introduces redundancy, reducing performance. To mitigate this, optimization algorithms such as Ant Colony Optimization (ACO) can be employed for feature selection, improving detection efficiency. This study introduces an ACO-SVM hybrid framework evaluated on the CICIDS2017 (7) dataset, offering improved detection accuracy and reduced computational cost.

Related Work

Recent research emphasizes the integration of optimization algorithms with machine learning techniques to improve IDS performance. Shrivastava and Richariya (2012) proposed ACO with classification algorithms to improve detection accuracy. Pervez and Farid (2014) demonstrated that SVM-based classifiers, when combined with optimal feature selection, outperform ANN-based methods on benchmark datasets. CICIDS2017, developed by the Canadian Institute for Cybersecurity, has emerged as a modern benchmark dataset

© 2025 The Authors. Published by MRI INDIA.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

capturing realistic traffic for evaluating intrusion detection systems.

Numerous researchers have explored machine learning-based approaches to enhance the performance and accuracy of intrusion detection systems (IDS). Aditya Nur Cahyo et al. [1] performed a comparative analysis of anomaly-based IDS using Artificial Neural Networks (ANN) and Support Vector Machines (SVM), demonstrating that SVM generally achieved better classification accuracy for large-scale datasets. Similarly, Namita Shrivastava and Vineet Richariya [2] proposed the integration of Ant Colony Optimization (ACO) with classification algorithms, showing that bio-inspired optimization techniques can significantly improve detection rates by selecting optimal feature subsets.

Muhammad Shakil Pervez and Dewan Md. Farid [3] applied SVMs for intrusion classification on the NSL-KDD dataset, emphasizing the importance of effective feature selection in minimizing false alarm rates. The CICIDS2017 dataset [4], developed by the Canadian Institute for Cybersecurity, offers realistic and modern network traffic characteristics, making it a benchmark for evaluating recent IDS models. Earlier, Mahbod Tavallaee et al. [5] provided a detailed analysis of the KDD Cup 99 dataset, identifying its redundancy and limitations, which led to the creation of improved datasets like NSL-KDD and CICIDS2017.

Annu and Monika Poriye [6] integrated ANN with ACO for feature optimization, demonstrating enhanced accuracy and reduced training time in anomaly detection. More recently, Faraz Ahmad Khan et al. [7] introduced a balanced multi-class network intrusion detection model using machine learning, addressing the challenge of class imbalance and improving the reliability of multi-class attack classification.

Proposed Methodology

The proposed ACO–SVM Intrusion Detection Framework consists of four main phases: Data Preprocessing, Feature Extraction, Feature Selection using ACO, and Classification using SVM. The overall architecture aims to enhance detection accuracy, reduce computational complexity, and achieve a more generalized intrusion detection capability.

A. Data Preprocessing

The CICIDS2017 dataset is used as the benchmark dataset, which contains both normal and various attack traffic types. Preprocessing includes several essential steps:

- **Data Cleaning:** Removal of duplicate records, incomplete entries, and inconsistent attribute values to ensure data integrity.
- **Data Normalization:** features are scaled using Min-Max normalization to ensure uniform feature contribution and to prevent bias due to varying magnitudes.
- **Label Encoding:** Categorical attributes are converted into numerical form to facilitate processing by the learning algorithms.
- **Data Splitting:** The dataset is divided into training (70%) and testing (30%) subsets to evaluate model generalization.

B. Feature Extraction

In this phase, the dataset's raw network traffic attributes are transformed into meaningful statistical features. Time-based and flow-based characteristics such as packet size, flow duration, source/destination bytes, and inter-arrival times are computed. This helps in capturing both temporal and spatial traffic behaviors, enabling better differentiation between normal and malicious patterns.

C. Feature Selection using Ant Colony Optimization (ACO):

ACO is employed to select the most informative features by mimicking the foraging behavior of ants.

- Initially, each ant represents a possible subset of features.
- The **pheromone trail** is updated iteratively based on classification accuracy obtained from SVM.
- Features that lead to better classification performance receive stronger pheromone reinforcement, guiding subsequent ants toward promising subsets.
- The selection process balances **exploration and exploitation** to avoid local optima and to reduce redundant or irrelevant features.

This phase ensures dimensionality reduction while retaining discriminative power.

D. Classification using Support Vector Machine (SVM)

The optimized feature subset from ACO is input to the SVM classifier, which constructs an optimal decision boundary between normal and attack classes.

- The Radial Basis Function (RBF) kernel is used to handle non-linear separability in high-dimensional space.

- Parameter tuning of the kernel (C and γ) is performed to maximize detection accuracy.
- The classifier output is a binary label indicating "normal" or "attack" traffic.

E. Performance Evaluation

Finally, the model's performance is evaluated using key metrics such as Accuracy, Precision, Recall, F1-Score, and Detection Rate. Comparative analysis with ACO–ANN and other baseline models is also conducted to validate the robustness and efficiency of the proposed approach.

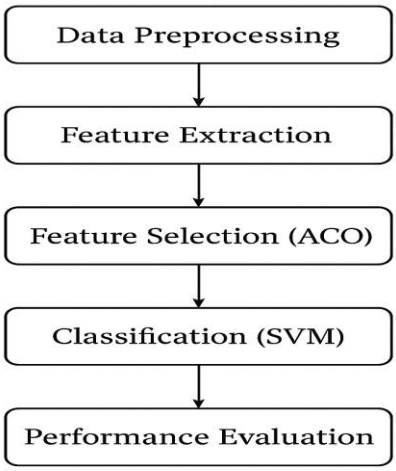


Fig. 1. Flowchart of the Proposed ACO–SVM Framework

Fig1: illustrates the overall workflow of the proposed ACO–SVM model. The process begins with **data preprocessing**, where redundant and inconsistent data from the CICIDS2017 dataset are removed and normalized for uniform scaling. In the **feature extraction** stage, relevant network attributes are identified. The **Ant Colony Optimization (ACO)** algorithm is then employed to select the optimal subset of features by simulating pheromone-based exploration behaviour. The selected features are passed to the **Support Vector Machine (SVM)** classifier for final **classification** into normal or attack categories. The model's performance is finally evaluated through **quantitative metrics** and **comparative analysis** to ensure reliability and effectiveness.

Performance Analysis

The performance of the ACO-SVM model is evaluated using Detection Rate (DR), False Alarm Rate (FAR), and Time Complexity (TC). These metrics are derived from the confusion matrix based on true positives, false positives, true negatives, and false negatives. The results are compared against ACO-ANN, ACO-NB, and PSO-SVM models on the CICIDS2017 dataset.

Classifier / Approach	Detection Rate (%)	False Alarm Rate (%)	Time Complexity (Sec)
ACO + SVM	90.56	9.44	0.32
ACO + ANN	88.29	11.70	0.34
ACO + NB	84.54	15.77	1.25
PSO + SVM	85.00	15.00	4.20

Fig. 2 Detection Rate Comparison

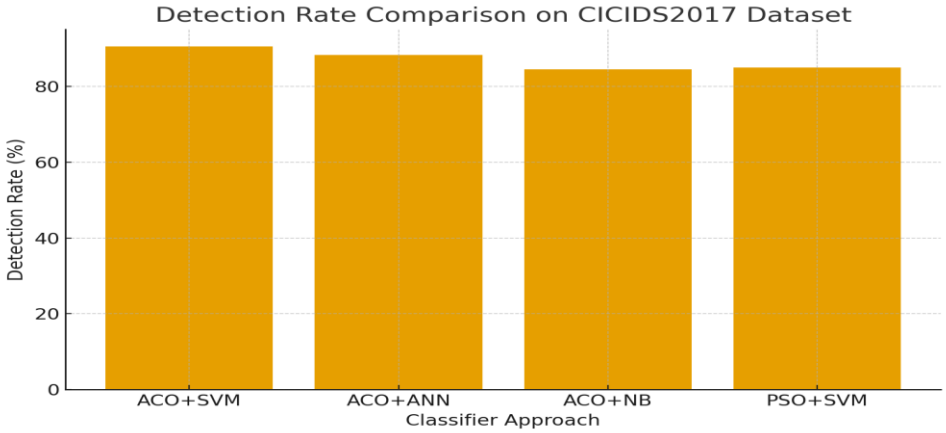


Fig. 3 False Alarm Rate Comparison

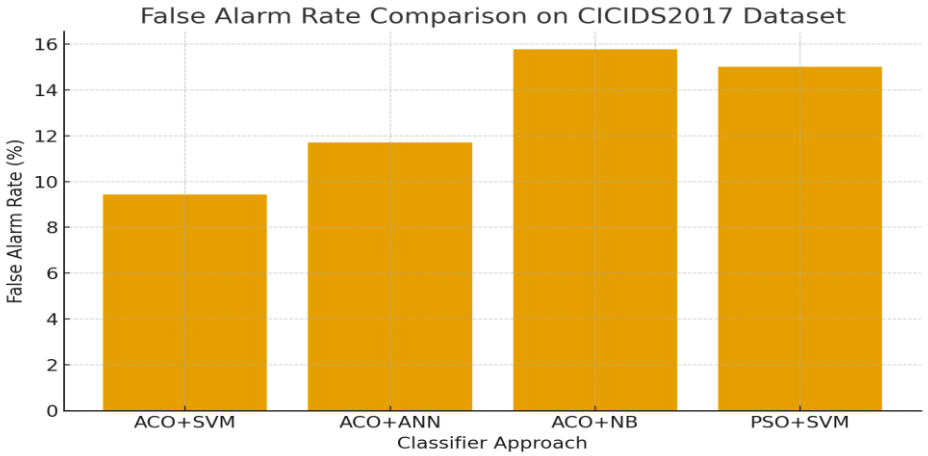
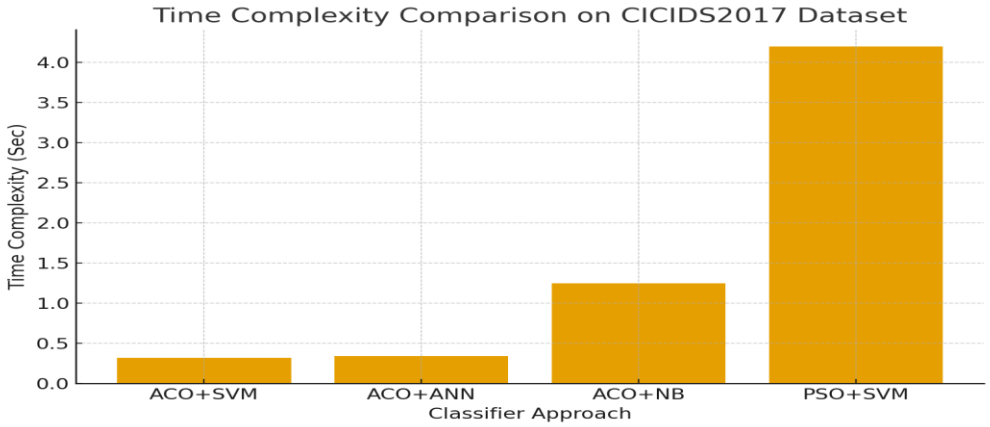


Fig. 4 Time Complexity Comparison



Conclusion and Future Work

This research demonstrates that the integration of Ant Colony Optimization (ACO) with Support Vector Machine (SVM) yields superior performance on the CICIDS2017 dataset (7). The proposed ACO-SVM model achieves a 90.56% detection rate with the lowest false alarm rate and time complexity, outperforming ANN and other machine learning models. The optimization-driven feature selection improves classification accuracy while maintaining computational efficiency. Future research will explore hybrid deep learning approaches incorporating ACO-SVM with Convolutional or Recurrent Neural Networks to further enhance real-time detection accuracy.

References

Aditya Nur Cahyo et al., Performance comparison of intrusion detection system based anomaly detection using artificial neural network and support vector machine' , Advances in Science and Technology, 2016.

Namita Shrivastava and Vineet Richariya, 'Ant Colony Optimization with Classification Algorithms used Intrusion detection', IJEM, 2012.

Muhammad Shakil Pervez and Dewan Md. Farid, 'Feature Selection and Intrusion Classification in NSL-KDD Employing SVMs', IEEE, 2014.

CICIDS2017 Dataset, Canadian Institute for Cybersecurity, University of New Brunswick, 2017.

Mahbod Tavallaee et al., 'A Detailed Analysis of the KDD CUP 99 Data Set', IEEE, 2009.

Annu and Monika Poriye, 'Anomaly-based Intrusion Detection System using Supervised Learning Algorithm Artificial Neural Network and Ant Colony Optimization with Feature Selection', IJEAT, Volume:9, Issue:3,Page No. 2475-2481, 2019-2020.

Faraz Ahmad Khan , Asghar Ali Shah , Nizal Alshammry , Saifullah Saif , Wasim Khan and Muhammad Osama Malik , 'Balanced Multi-Class Network Intrusion Detection Using Machine Learning',2024 ,IEEE Access.