Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1811–1819
DOI : 10.47974/JIOS-2014

Enhanced DDoS attack detection using instance-based transfer learning with Q TRANSFER and Gaussian membership function

Saswati Chatterjee [§]
Faculty of Information Technology and Computer Science
Parul University
Ta.Waghodia 391760
Dist. Vadodara
Gujarat
India

Deepthi Godavarthi [†]
VIT- AP University
Amaravati 522237
Andhra Pradesh
India

Suneeta Satpathy *
Center of Cyber Security
SOA University
Bhubaneswar 751030
Odisha
India

Abstract

DDoS attacks pose a significant threat to networks due to their ease of execution and the difficulty in mitigating them. Machine learning-based detection faces challenges due to limited accessible training data. This paper presents an instance-based transfer learning algorithm for DDoS detection, leveraging publicly available datasets for knowledge transfer. The approach filters and reconstructs instances using gain-based selection, TrAdaBoost, Q TRANSFER, and a Gaussian membership function to refine instance weighting. This enhances model generalizability to new attack types, ensuring robust detection. The

[§] *ORCID-ID:* 0009-0004-8568-1227
* *ORCID-ID:* 0000-0002-6943-171X

[§] *E-mail:* cshiv68@gmail.com
[†] *E-mail:* saideepthi531@gmail.com
* *E-mail:* suneeta1912@gmail.com (Corresponding Author)

proposed method improves adaptability to evolving threats, strengthening the reliability of DDoS detection technologies.

Subject Classification: *68M12, 68T07, 68T05.*

Keywords: *DDoS Attack, Gaussian membership function, Machine learning, Q-learning, Transfer learning, TrAdaBoost.*

1. Introduction

A Distributed Denial of Service (DDoS) attack is one in which many computers combine efforts to send data to a specific system, making it difficult for actual users to access such a system. In this way, attackers launch these attacks from different geographical locations coordinated against the underlying network infrastructure, leading to disruptions. In contrast to conventional attacks, DDoS costs very little to the attacker yet causes significant costs to the prospective defender. The research study in [1] proposed a knowledge-based hybrid model comprising various models to detect anomaly attacks. However, these machine-learning techniques often assume that training and test data adhere to the same probability distribution [2]. In conventional models, when the distribution alters for instance new types of attacks over time, the method necessitates expensive redeployment with fresh samples of data, which may not be possible in some cases. Transfer learning provides a solution to these problems that are closely related to fields such as natural language processing and visual recognition [3-5]. Transfer learning is based on knowledge obtained in one sphere, a definite set of materials, or a similar sphere [6-9]. Although it appears highly effective in various other fields, its utilization in network intrusion detection has received considerably less attention [10-12]. Over the past decade, datasets like KDDCUP99 and NSL-KDD have been widely used to evaluate NIDS performance. The Q-TRANSFER framework, based on deep transfer learning can enhances knowledge transfer between domains for improved adaptability and accuracy. However, conventional algorithms show low True Positive Rates while handling new attack types [13-15]. To address high false detection rates in traditional models like KNN, particularly on newer datasets such as UNSW-NB15, the instance-based TrAdaBoost algorithm is applied, demonstrating improved detection of emerging threats and enhanced generalization capability in intrusion detection systems with lower false positives. The proposed approach makes an integration of Q-TRANSFER, Gaussian membership functions, and TrAdaBoost which can significantly boost accuracy and

adaptability to emerging DDoS attacks. Further section 2 explains the methodology adopted in the present study followed by results in Section 3 and concluding remarks of the study in Section 4.

2. Proposed Methodology

The proposed methodology begins with the detection and collection of raw network traffic data, which is then subjected to data cleaning to remove noise, handle missing values, and standardize the format. After preprocessing, relevant features are extracted to form a structured feature dimension that effectively represents the underlying patterns in the traffic. These features are then used to train a TriAdaBoost classifier enhanced with a Gaussian Membership Function. The said approach combines the strength of boosting with fuzzy logic to improve classification accuracy and robustness in detecting cyber threats within network traffic. Figure 1 depicts the proposed methodology for identifying the DDoS Model. The model adopts NSL-KDD dataset which is an enhanced version of KDD'99 and CIC-IDS dataset, offering realistic features for evaluating intrusion detection systems. To ensure compatibility, its dimensions were expanded to 79, while the CIC-IDS dataset was reduced to 42 dimensions through feature selection.

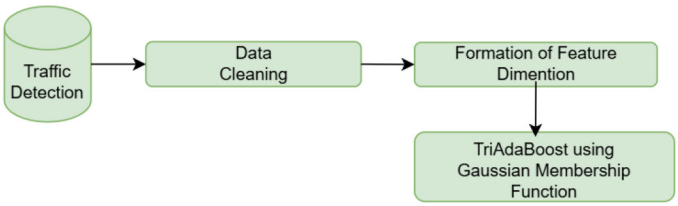

Figure 1

Proposed DDoS Detection Model

2.1 *TrAdaBoost for Efficient Knowledge Transfer with Q-learning and Gaussian Membership Function*

TrAdaBoost is a transfer learning algorithm adapted from the AdaBoost algorithm. This framework leverages both the source and target domain datasets for training. The steps for the Q-Learning Based Weighted TrAdaBoost methods are as follows.

Labeled datasets: Td and Ts
Unlabelled dataset: S
Weak classifier: Decision Tree
Maximum iterations: N

Initialization:

a. Initialize weight vector w
b. Set Gaussian membership function parameters (mean μ, variance σ^2)
c. Initialize Q-learning parameters (learning rate α, discount factor γ, exploration rate ϵ)

Steps:

a. **Combine Datasets:**
   Combine labeled and unlabeled datasets: T = Td ∪ Ts
b. Initialize Weights:
   For each instance i in T:
      If i is in Td, set wi = 1 / (2 |Td|)
      If i is in Ts, set wi = 1 / (2 |Ts|)
c. Iterative Training:
   For t = 1 to N:
   - Train weak classifier ht on the weighted dataset T
   - Calculate error ϵt of ht on Ts
   - Update weights:
     For each instance i in T:
        If ht(xi) = c(xi):
           wi=wi*exp (Gaussian (μ, σ^2, xi))
        Else:
           wi=wi*exp (Gaussian (μ, σ^2, xi))
     Normalize weights
   - Update Q-values for weak classifiers using Q-learning:
     Q(ht) = Q(ht) + α * (reward + γ * max(Q(ht+1)) - Q(ht))
   - Adjust exploration rate ϵ for exploration-exploitation trade-off
d. Final Hypothesis:
   Combine weak classifiers to form the final hypothesis:
      hf(x) = sign(-1^N * Σ ht(x))

Output:

Final hypothesis hf(x) for classifying new instances

2.2 *Comprehensive Analysis of Q-Learning Enhanced Weighted TrAdaBoost Algorithm*

The proposed algorithm integrates boosting, Q-learning, and Gaussian membership functions for classification. It begins by initializing weights, then iteratively updates them based on classification errors, increasing weights for correctly classified points and decreasing them for misclassified ones. A Gaussian function ensures smooth updates, while Q-learning optimizes the selection of weak classifiers through reward-based feedback. The final prediction is made by aggregating the weighted outputs of all weak classifiers, enhancing performance through the combination of probabilistic modeling and reinforcement learning.

3. Experimental Analysis

The experiment results of Cyber threat detection experiments on the CIC-IDS and NSL-KDD datasets were conducted, comparing the proposed method with traditional classifiers such as Decision Tree, Isolation Forest, Random Forest, and SVC. Results indicated that TrAdaBoost achieved the highest accuracy across both datasets, as shown in Figure 2, while Figure 3 illustrates a heatmap of model performance.

Model/Algorithm	Dataset	Accuracy (%)	Precision (%)	Score (%)	Positive Rate (FPR)
Decision Tree	CIC-IDS	94.2	93.7	94.0	0.04
	NSL-KDD	93.5	92.9	93.2	0.05
Isolation Forest	CIC-IDS	92.4	90.3	91.3	0.05
	NSL-KDD	91.8	89.7	90.7	0.06
Random Forest	CIC-IDS	96.2	95.1	95.6	0.03
	NSL-KDD	94.5	93.8	94.1	0.04
Support Vector Classifier (SVC)	CIC-IDS	94.7	93.2	93.9	0.04
	NSL-KDD	93.5	92.7	93.1	0.05
TrAdaBoost Algorithm	CIC-IDS	97.8	96.9	97.4	0.02
	NSL-KDD	95.9	95.3	95.6	0.03

Figure 2

Results of Transferring NSL-KDD TO CIC-IDS

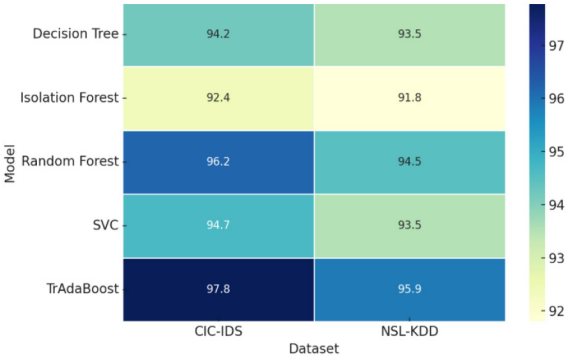

Figure 3

Comparative Performance Analysis of Machine Learning Models on CIC-IDS and NSL-KDD Datasets

3.1 *Comparative Analysis with the existing work*

In contrast to previous works, the proposed work augments a novel approach that significantly enhances with a precise description of the TrAdaBoost algorithm and thus features a notably improved performance in terms of classification accuracy with low false favorable rates compared to classical models shown in Table 1.

Table 1

Comparative Analysis of Machine Learning Models for Anomaly Detection: Proposed Study vs. Existing Work

Reference	Model/Algorithm	Dataset	Accuracy (%)	Precision (%)	Score (%)	Positive Rate (FPR)
Li *et al.* [14]	Decision Tree	CIC-IDS	94.2	93.7	94.0	0.04
		NSL-KDD	93.5	92.9	93.2	0.05
Ahmed *et al.* [9]	Isolation Forest	CIC-IDS	92.4	90.3	91.3	0.05
		NSL-KDD	91.8	89.7	90.7	0.06

Contd...

Kumar *et al.* [10]	Random Forest	CIC-IDS	96.2	95.1	95.6	0.03
		NSL-KDD	94.5	93.8	94.1	0.04
Lopez-Martin *et al.* [2]	Support Vector Classifier (SVC)	CIC-IDS	94.7	93.2	93.9	0.04
		NSL-KDD	93.5	92.7	93.1	0.05
Lu *et al.* [6]	TrAdaBoost Algorithm	CIC-IDS	97.8	96.9	97.4	0.02
		NSL-KDD	95.9	95.3	95.6	0.03

4. Conclusion

This study introduces TrAdaBoost, an instance-transfer learning approach for DDoS detection. Publicly available datasets with dimension reconstruction and feature integration applied were used as the source domain for model validation. TrAdaBoost minimizes misclassification during transfer and shows strong generalization across detection tasks. It adapts well to new datasets and attack types using Q-Learning and enhanced Gaussian membership functions for improved accuracy. The proposed method also boosts overall detection and resilience. Future work will enhance TrAdaBoost's flexibility through improved Q-Learning integration.

References

[1] T. K. Mohammed, D. N. Vasundhara, S. H. Mehanoor, E. Sreedevi, P. R. Kumar, C. Manihass, and S. F. Baba, "A novel fusion approach for advancement in crime prediction and forecasting using hybridization of ARIMA and recurrent neural networks," *Journal of Information Systems Engineering and Management*, vol. 10, no. 38, pp. 404–420 (2025).

[2] M. R. Z. E. Deen and G. M. Elmahdy, "Different types of odd harmonious labeling of super subdivision of various graphs," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 8, pp. 2373–2407 (2024).

[3] G. B. Mohammad, S. Shitharth, and P. R. Kumar, "Integrated machine learning model for an URL phishing detection," *Int. J. Grid Distrib. Comput.*, vol. 14, no. 1, pp. 513–529 (2021).

[4] P. Dass, V. Gupta, S. Dhingra, R. Arora, P. Katariya, and A. Kumar, "A deep learning model to predict and classify crime rate using tweets," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 8, pp. 2255–2271 (2024).

[5] B. Shilpa, P. R. Kumar, and R. K. Jha, "Spreading factor optimization for interference mitigation in dense indoor LoRa networks," in Proc. IEEE IAS Global Conf. Emerging Technol. (GlobConET), pp. 1–5 (May 2023).

[6] H. Lu, Y. Zhao, Y. Song, Y. Yang, G. He, H. Yu, and Y. Ren, "A transfer learning-based intrusion detection system for zero-day attack in communication-based train control system," *Cluster Comput.*, vol. 27, no. 3, pp. 1–16 (2024).

[7] I. Riadi, N. Sunardi, and D. Aprilliansyah, "Analysis of Anubis Trojan attack on Android banking application using mobile security labware," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 1, pp. 31–38 (2023).

[8] A. O. Almashhdani, M. Kaiiali, D. Carlin, and S. Sezer, "MaldomDetector: A system for detecting algorithmically generated domain names with machine learning," *Comput. Secur.*, vol. 93, no. 11, pp. 101787 (2020).

[9] P. R. Kumar and B. Shilpa, "An IoT-based smart healthcare system with edge intelligence computing," in Reconnoitering the Landscape of Edge Intelligence in Healthcare. Boca Raton, FL, USA: Apple Academic Press, pp. 31–46 (2024).

[10] G. Kumar, K. Thakur, and M. R. Ayyagari, "MLESIDSS: Machine learning-based ensembles for intrusion detection systems – A review," *J. Supercomput.*, vol. 76, no. 6, pp. 4192–4218 (2020).

[11] S. Velliangiri, "A hybrid BGWO with KPCA for intrusion detection," *J. Exp. Theor. Artif. Intell.*, vol. 32, no. 3, pp. 165–180 (2020).

[12] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Syst. Appl.,* vol. 41, no. 5, pp. 1690–1700 (2014).

[13] R. S. Teppawar, R. N. Ingle, and R. A. Muneshwar, "Analysis of system of fractional partial differential equations using Laplace reduced differential transform with decomposition method," *Journal of Statistics and Management Systems,* vol. 27, no. 8, pp. 1577–1594 (2024).

[14] B. Shilpa, P. R. Kumar, and R. K. Jha, "LoRa DL: A deep learning model for enhancing the data transmission over LoRa using autoencoder," *J. Supercomput.,* vol. 79, no. 15, pp. 17079–17097 (2023).

[15] F. Sağlam, T. Şanlı, and M. A. Cengiz, "ShinySurv: A survival analysis and Shiny web application," *Journal of Statistics and Management Systems,* vol. 27, no. 8, pp. 1557–1575 (2024).

Received December, 2024