Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of Informatics and Radioelectronics

UDC 004.056.53

Pan Huiqin

Methods and Algorithms for Protecting Against Distributed DOS Network Attacks

Abstract to master degree thesis

Specialty 7-06-0611-02 Information Security

_____

Supervisor:
N.V. Nasonova, Dr., Assoc. Prof.

_____

Minsk 2026

GENERAL DESCRIPTION OF WORK

The Research Aim and Objectives

The aim of the thesis is to develop methods and algorithms for protection against distributed DoS network attacks based on machine learning and to verify their effectiveness in an experimental environment.

To achieve this aim, the following objectives were formulated:

1. To analyze the mechanisms of distributed DoS attacks and existing approaches to their detection and mitigation.
2. To develop a four-stage protection methodology including pre-configuration, detection, blocking, and mitigation of attack consequences.
3. To prepare and adapt the training data, including dataset analysis, preprocessing, and alignment of the feature space with real-traffic conditions.
4. To design, implement, train, and evaluate machine learning models for DoS attack detection, including feature importance analysis and determination of a minimum sufficient feature subset.
5. To develop an experimental testbed based on Mininet and the Ryu controller for implementing and validating the proposed protection methodology in conditions close to a real network environment.
6. To assess the effectiveness, limitations, and practical applicability of the proposed approach, including detection quality, feature-space reduction effects, and automatic attack-blocking performance.

Work Connection with Priority Areas of Scientific Research

The topic of the thesis corresponds to paragraph 6 Ensuring the security of humans, society and the state (means of technical and cryptographic information protection, cryptology and cybersecurity) of the list of priority areas of scientific, scientific-technical and innovative activities for 2021–2025, approved by the Decree of the President of the Republic of Belarus dated 07.05. 2020 No. 156.

Thesis Results Approbation

The main results of the dissertation were reported and discussed at the 61st Scientific conference of Graduate Students, Master Students and Students of BSUIR (Minsk, April 21–25, 2025), and the 62st Scientific conference of Graduate Students, Master Students and Students of BSUIR (Minsk, April 13–17, 2026).

INTRODUCTION

With the rapid development of Internet technologies and digital services, ensuring the security and availability of infocommunication networks remains an important task. Among the most serious threats are distributed Denial-of-Service (DDoS) attacks, which overload network bandwidth, processing capacity, or connection resources and disrupt normal service operation. Due to their destructive impact and relative ease of launch, such attacks continue to be one of the major cybersecurity challenges.

Traditional DoS and DDoS protection methods are often based on fixed thresholds, predefined rules, or signature matching. Although these approaches are still widely used, they are not always effective against evolving attack patterns and dynamic traffic conditions. In modern programmable and software-defined network environments, this creates the need for more adaptive protection methods that combine traffic monitoring, attack detection, automated blocking, and mitigation within a unified framework.

Machine learning offers promising opportunities for this purpose, since it allows models to learn traffic behavior patterns from labeled data and distinguish legitimate from malicious traffic more flexibly than rigid rule-based methods. However, strong offline performance on public datasets does not guarantee reliable operation in deployment conditions, where traffic structure, feature distribution, and feature availability may differ. Therefore, the practical problem includes not only model training, but also data adaptation, feature-space alignment, and integration of the detection module with network control mechanisms.

This thesis is aimed at developing methods and algorithms for protection against distributed DoS network attacks based on machine learning and at verifying their effectiveness in an experimental environment. In accordance with this aim, the research addresses the analysis of distributed DoS attack mechanisms and protection approaches, the development of a four-stage protection methodology, the preparation and adaptation of training data, the design of machine learning models for attack detection, the implementation of an experimental testbed based on Mininet and the Ryu controller, and the assessment of the effectiveness and practical applicability of the proposed approach.

The main contribution of the work is the development and experimental validation of a machine-learning-based four-stage protection methodology for distributed DoS attacks in a software-defined networking environment. The proposed approach combines adapted training data, feature-space reduction, Random Forest-based attack detection, and automated controller-driven blocking of malicious traffic. The study also investigates how the number of available features affects detection quality and identifies a minimum sufficient feature subset for stable classification of BENIGN, SYN_FLOOD, and UDP_FLOOD traffic.

MAIN PART

The first chapter presents an analysis of distributed DoS attack mechanisms and existing approaches to protection. It examines the classification of DDoS attacks, including flooding, reflection, and amplification attacks, and reviews both traditional and modern protection methods. The chapter also formulates the research problem and defines the objectives of the thesis, showing the need for adaptive and practically deployable protection methods for modern infocommunication networks.

The second chapter describes the proposed protection methodology and the overall system architecture. It introduces the four-stage protection concept, including pre-configuration, detection, blockage, and mitigation, and explains the role of each stage in the overall defense process. Special attention is paid to the integration of a machine-learning-based detection module with SDN control mechanisms, which makes it possible to move from attack recognition to automated network response [2-A].

The third chapter is devoted to the development of the ML-based DDoS attack detection module. It formalizes the multiclass network flow classification task, describes the CIC-DDoS2019 dataset and the traffic feature space, and presents the selected quality metrics for model evaluation. The chapter also includes data preparation, feature analysis and interpretability, comparison of detection models and algorithms, hyperparameter tuning, and validation. Based on the experiments, it was established that the Random Forest model achieved the best performance, with Accuracy = 0.999 and Macro-F1 = 0.997. It was also shown that stable detection quality can be maintained with a reduced feature space of 4 features, while reducing the feature set to 3 features leads to a noticeable degradation in the main metrics. The experiments further demonstrated that the relationship between the number of features and detection quality is nonlinear [1-A, 2-A].

The fourth chapter presents the implementation and testing of the developed protection technique. An experimental testbed based on Mininet, the Ryu controller, and an ML-based detection module was implemented, where model outputs were automatically transformed into traffic control actions through drop-rule installation. The models were trained on an adapted dataset aligned with the feature extraction mechanism intended for subsequent operation on real traffic collected in the experimental testbed for the BENIGN, SYN_FLOOD, and UDP_FLOOD classes. Experimental evaluation confirmed the effectiveness of the developed four-stage anti-DDoS protection technique and demonstrated its practical applicability for protecting infocommunication networks against distributed DoS attacks [2-A].

CONCLUSION

This study proposes a comprehensive detection framework based on machine learning for methods and algorithms to defend against DDOS attacks. Based on the experimental results, the following conclusions are drawn:

1) A four-stage DDoS protection technique was developed and validated, including environment pre-configuration, ML-based detection, blocking, and mitigation of attack consequences.

2) An experimental testbed based on Mininet, the Ryu controller, and an ML-based detection module was implemented, where model decisions were automatically converted into traffic control commands through drop-rule installation.

3) The models were trained on an adapted dataset aligned with the feature extraction mechanism intended for further operation on real traffic collected in the experimental testbed for the BENIGN, SYN_FLOOD, and UDP_FLOOD classes.

4) The Random Forest model achieved the best detection performance, with Accuracy = 0.999, Macro-F1 = 0.997, while stable detection quality was ensured after reducing the feature space to 4 features. Reducing it further to 3 features caused a noticeable degradation of the main metrics.

5) The relationship between the number of features and detection quality is nonlinear, which confirms the practical applicability of the proposed technique for protecting infocommunication networks against DDoS attacks.

Scientific value of the thesis: the proposed and experimentally validated four-stage DoS protection technique for a software-defined network where a machine-learning-based detection module is integrated with the Ryu controller and used for attack detection and automatic response. The study also shows that the traffic classes BENIGN, SYN_FLOOD, and UDP_FLOOD can be distinguished using a limited number of the most informative features (tcpFlags,tcpFstat,pktsRcvd,connSipDip), rather than the full feature space.

Practical value of the thesis: development and testing of the Mininet- and Ryu-based testbed that makes it possible to evaluate ML models on traffic close to real operating conditions. The proposed technique can be used for lightweight and practically deployable systems for detecting and blocking DoS attacks in intercommunication networks.

LIST OF OWN PUBLICATIONS

1-A. Pan Huiqin. Protection against various classes of DDoS attacks / Pan Huiqin, N. V. Nasonova // Information security： Proceedings of the 61st Scientific conference of Graduate Students, Master Students and Students of BSUIR, Minsk, April 21–25, 2025 / Belarusian State University of Informatics of Radioelectronics. – Minsk, 2025. – P. 147-151.

2-A. Pan Huiqin. A machine learning framework for multiclass detection of DDoS network attacks / Information security： Proceedings of the 62st Scientific conference of Graduate Students, Master Students and Students of BSUIR, Minsk, 13-17 April, 2026 / Belarusian State University of Informatics of Radioelectronics. – Minsk, 2026. – P. 38-39.