МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Энтропийный подход к обнаружению аномального сетевого трафика»

Гарматная Лолита Вадимовна

Научный руководитель – кандидат физико-математических наук, заведующий НИЛ статистического анализа и моделирования, доцент кафедры математического моделирования и анализа данных Абрамович М. С.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 60 с., 10 рис., 13 табл., 15 источников, 1 прил.

Ключевые слова: СЕТЕВОЙ ТРАФИК, АНОМАЛИИ ТРАФИКА, ЭНТРОПИЯ, ОБНАРУЖЕНИЕ АНОМАЛИЙ ТРАФИКА, МАШИННОЕ ОБУЧЕНИЕ, ЭФФЕКТИВНОСТЬ КЛАССИФИКАЦИИ.

Объект исследования: алгоритмы классификации интернет трафика, основанные на энтропии.

Цель исследования: исследование возможности применения энтропии для анализа сетевого трафика.

Методы исследования: а) теоретические: изучение литературы, посвященной современным подходам к обнаружению аномалий сетевого трафика, использованию энтропии для классификации данных. б) практические: разработка алгоритма классификации данных сетевого трафика с использованием различных видов энтропии и методов машинного обучения.

Полученные результаты и их новизна: были реализованы 3 алгоритма классификации данных сетевого трафика, проведены эксперименты, выполнен анализ эффективности реализованных методов.

Область возможного практического применения: информационная безопасность, анализ сетевого трафика, системы обнаружения вторжений.

РЭФЕРАТ

Дыпломная праца: 60 с., 10 мал., 13 табл., 15 крыніц, 1 прыкл.

Ключавыя словы: СЕТКАВЫ ТРАФІК, АНАМАЛІІ ТРАФІКУ, ЭНТРАПІЯ, ВЫЯЎЛЕННЕ АНАМАЛІЙ ТРАФІКУ, МАШЫННАЕ НАВУЧАННЕ, ЭФЕКТЫЎНАСЦЬ КЛАСІФІКАЦЫІ.

Аб'ект даследавання: алгарытмы класіфікацыі інтэрнэт трафіку, заснаваныя на энтрапіі.

Цэль даследавання: даследаванне магчымасці прымянення энтрапіі для аналізу сеткавага трафіку.

Метады даследавання: а) тэарэтычныя: вывучэнне літаратуры, прысвечанай сучасным падыходам да выяўлення анамалій сеткавага трафіку, выкарыстанню энтрапіі для класіфікацыі дадзеных. б) практычныя: распрацоўка алгарытму класіфікацыі дадзеных сеткавага трафіку з выкарыстаннем розных відаў энтрапіі і метадаў машыннага навучання.

Атрыманыя вынікі і іх навізна: былі рэалізаваны 3 алгарытму класіфікацыі дадзеных сеткавага трафіку, праведзены эксперыменты, выкананы аналіз эфектыўнасці рэалізаваных метадаў.

Вобласць магчымага практычнага прымянення: інфармацыйная бяспека, аналіз сеткавага трафіку, сістэмы выяўлення ўварванняў.

ANNOTATION

Degree paper: 60 p., 10 ill., 13 tab., 15 sources, 1 app.

Key words: NETWORK TRAFFIC, TRAFFIC ANOMALIES, ENTROPY, TRAFFIC ANOMALY DETECTION, MACHINE LEARNING, CLASSIFICATION EFFICIENCY.

Object of research: entropy-based Internet traffic classification algorithms.

Purpose of research: investigation of the possibility of using entropy to analyze network traffic.

Research methods: a) theoretical: the study of literature devoted to modern approaches to the detection of network traffic anomalies, the use of entropy for data classification. b) practical: development of an algorithm for classifying network traffic data using various types of entropy and machine learning methods.

Obtained results and their novelty: 3 algorithms for classifying network traffic data were implemented, experiments were conducted, and the effectiveness of the implemented methods was analyzed.

Area of possible practical application: information security, network traffic analysis, intrusion detection systems.