

Інтелектуальна система ідентифікації мережевого трафіка

Москаленко В.В., *асистент*; Коробов А.Г. *студент*
Сумський державний університет, м. Суми

Швидкий розвиток цифрових мультисервісних мереж сприяє зростанню кількості інтерактивних і мультимедійних додатків, що обумовлює необхідність пріоритезації трафіка відповідно до вимог рівня обслуговування користувачів та якості мережевих сервісів.

Для ефективного розподілу ресурсів транспортних мереж з комутацією пакетів, що є основою для розгортання сучасної мультисервісної інфраструктури, необхідно мати інструмент точної ідентифікації та класифікації трафіка. При цьому поширення мережевих додатків, які динамічно змінюють порти транспортних протоколів, та засобів інформаційної безпеки, які основані на шифруванні та тунелюванні трафіка унеможливають достовірну класифікацію на основі портів чи корисного навантаження. Крім того, реалізація методів маскування трафіка в умовах параметричної невизначеності інформаційних процесів, які генерують мережевий трафік, знижує ефективність класифікації на основі аналізу статистичних характеристик потоку пакетів, що особливо критично проявляється при екстремальній незбалансованості накопичених статистичних даних.

Підвищення точності класифікації мережевого трафіка запропоновано здійснювати шляхом інформаційного синтезу класифікатора з адаптивним кодуванням первинних ознак розпізнавання та оптимізацією геометричних параметрів розбиття двійкового простору вторинних ознак на класи еквівалентності [1]. При цьому словник ознак складається із статистичних характеристик двонаправленого потоку пакетів. Навчальні набори даних сформовані в процесі трасування трафіку з наступним формуванням потоків і обчисленням ознак розпізнавання. Априорна класифікація реалізацій навчального трафіку основана на результатах моніторингу сокетів.

Таким чином, реалізовано інформаційно-екстремальний класифікатор трафіків з ієрархічною структурою обчислювально ефективних вирішальних правил, який навчається за незбалансованими вибірками.

1. А.С. Довбиш, *Основи проектування інтелектуальних систем* (Суми: СумДУ: 2009).