ИСП РАН

Автоматическая генерация сигнатур сетевых протоколов и приложений

Алексей Дурнов

18 апреля 2024 г.

МФТИ, кафедра системного программирования, ИСП РАН

Введение

- Методы классификации сетевого трафика:
  1. основанные на идентификации по номеру порта
  2. основанные на DPI подходе
     - сигнатурный
  3. основанные на статистических характеристиках
- Свойства сигнатур для сетевых протоколов и приложений:
  1. короткие общие подстроки
  2. несколько потоков с разным набором подстрок
  3. необходимость частого обновления

Цель

Целью данной работы является разработка и реализация метода автоматической генерации сигнатур полезной нагрузки сетевого трафика для классификации этого трафика в соответствии с использующимся протоколом или приложением в режиме реального времени.

Задачи

- Провести исследование литературы по соответствующей теме.
- Собрать набор сетевых трасс для последующего тестирования и сравнения методов.
- Разработать формат хранения сигнатуры.
- Разработать алгоритм генерации сигнатур.
  1. Выбрать методы для автоматической генерации сигнатур.
  2. Найти ограничения рассматриваемых методов.
  3. Выбрать оптимальный набор параметров метода.
- Разработать классификатор сетевого трафика для проверки сгенерированных сигнатур.
  1. Выбрать и реализовать алгоритм сопоставления сигнатур
  2. Выбрать метрики, по котором можно оценить качество классификации сигнатур
- Встроить генератор сигнатур и классификатор как модули в систему анализа высокоскоростного сетевого трафика, разрабатываемую в ИСП РАН.

Спасибо за внимание