План ВКР

Введение

Во введении обосновывается актуальность исследования сетевых моделей распространения вредоносного программного обеспечения и эпидемий в компьютерных сетях. Рассказывается о том, что такое имитационное моделирование. Указывается, что современные инструменты сетевой эмуляции — Mininet, Kathará и Containerlab — позволяют создавать полноразмерные виртуальные сети, близкие по структуре к реальным сетям. Это делает возможным тестирование сценариев распространения инфекции, построенных на основе компартментальной моделей SEIRS-NIMFA, в условиях, близких к реальным.

Также во введении формулируется цель работы — сравнить различные инструменты для имитационного моделирования сетей на основе моделирования эпидемического процесса, путем проведения экспериментов. Определяются основные задачи, такие как обзор моделирующих средств, анализ математических моделей SEIR-класса, построение сетевых топологий, написание скрипта Morris Worm и выполнение самих экспериментов.

1. Теоретическая часть

1.1. Описание моделирующих инструментов

В данном разделе описываются инструменты моделирования и их возможности.

1.1.1. Mininet

Mininet — это лёгкий сетевой эмулятор, позволяющий создавать виртуальные сети на одной машине с использованием Linux-namespaces и виртуальных коммутаторов Open vSwitch. Описывается его архитектура, механизм работы, возможности по созданию сетевых топологий и запуску приложений в изолированных контейнерах-хостах. Подчёркивается его преимущество — высокая производительность и нативная поддержка SDN-контроллеров. Рассматриваются ограничения: однопроцессорность хостов, упрощённые модели пропускной способности и сложности масштабирования сверх нескольких сотен узлов.
Также расписывается установка Mininet на разные ОС.

1.1.2. Kathará

Kathará — имитационный инструмент, основанный на network-namespaces и Docker-like механизмах, позволяющий моделировать сложные сети с использованием сетевых маршрутизаторов (FRRouting, BIRD, Quagga, VPP). В отличие от Mininet, Kathará поддерживает запуск пользовательских файловой структуры и стартовых скриптов для каждого узла, что делает его удобным для сетевых экспериментов на уровне маршрутизации. В разделе описывается структура проекта Kathará (lab.conf, .startup, папки shared), способы задания линков, подсетей и конфигураций. Отмечается возможность масштабирования до 1000+ узлов за счёт контейнеризации и оптимизированной сетевой подсистемы Linux.
Также расписывается установка Kathará на разные ОС.

1.1.3. Containerlab

Containerlab применяется для моделирования сетей операторского класса с участием реальных сетевых образов — Nokia SR Linux, Arista cEOS, Juniper vMX/vJunos и др. Инструмент использует полноценные контейнеры с аппаратным ускорением dataplane. Описываются возможности по описанию топологии в YAML, автоматическому управлению жизненным циклом контейнеров, поддержке кластера Docker/Podman. Подчёркивается, что Containerlab наиболее близок к промышленным сетям и позволяет проверять эпидемические сценарии при наличии реальных протоколов маршрутизации, но требует больших вычислительных ресурсов.
Также расписывается установка Containerlab на разные ОС.

1.2. Описание SEIR-класса моделей

1.2.1. SIR

Сначала объясняется классическая SIR-модель — её структура, три компартмента, базовые параметры β (заражение) и γ (выздоровление). Поясняется, что модель является основой всех последующих расширений.

1.2.2. SEIR

Модель SEIR вводит латентный период E (exposed), описывающий задержку между заражением и появлением симптомов. Дается система ОДУ и её интерпретация применительно к компьютерным сетям: задержка на активацию вредоносного ПО, период скрытой инфекции.

1.2.3. SEIRS

SEIRS добавляет возможность возвращения иммунных обратно в S (утрата иммунитета). В сетевом контексте это означает, что узел после очистки может снова стать

восприимчивым (например, при отключении антивируса, истечении срока лицензии или человеческом факторе).

1.2.4. SEIRS-NIMFA

SEIRS-NIMFA — приближённая стохастическая модель, используемая в сетевой эпидемиологии для описания распространения атак через граф узлов. Приводится её отличие от классического SEIRS — здесь вероятность заражения зависит от структуры сети и степеней узлов. Формально NIMFA работает на матрице смежности A и описывает динамику заражений на графах любой сложности. Этот раздел описывает математические свойства модели.

2. Практическая часть

2.1. Эксперимент на Mininet и Kathará

В этой части описывается методика построения виртуальной сети из сотен узлов в Mininet и Kathará. Для Mininet вводится подход к созданию топологии в виде Python-скриптов, способ запуска программ-клиентов и настройки линков (потери, пропускная способность, задержка). Для Kathará описывается использование файлов .startup для автоматической конфигурации узлов, генерация сетей с помощью скриптов, методы логирования (ping, iperf) и сбор данных. Также описывается скрипт worm.py, который и будет запущен после создания сети.

Раздел включает описание методики проведения эксперимента:

— определение параметров SEIR/SEIRS-NIMFA;
— запуск сетевой симуляции;
— запись состояния узлов (S/E/I/R) на каждом шаге;
— построение графиков развития инфекции;
— анализ производительности: нагрузка на CPU, RAM.

Проводится сравнение Mininet и Kathará по масштабируемости, скорости и удобству конфигурации.

2.2. Эксперимент на Mininet и Containerlab

В Containerlab создаются сети операторского уровня с использованием реальных маршрутизаторов. Описывается процесс подготовки YAML-файла топологии, выбор образов (например, Nokia SR Linux), настройка маршрутизации (OSPF, IS-IS или BGP). Далее моделируется распространение “инфекции” между узлами в сети с использованием того же файла worm.py.

Основные шаги эксперимента:

— запуск реальных сетевых ОС;
— выполнение логики заражения;
— измерение скорости распространения по протоколам маршрутизации;
— сравнение с Mininet и Kathará по точности и натуралистичности поведения сети.

Отдельно анализируются вычислительные затраты Containerlab по сравнению с Mininet: потребление RAM, нагрузка на CPU, чувствительность к топологии.

Заключение

В заключении формируются выводы о том, какой инструмент моделирования наиболее эффективен для анализа сетевых эпидемий в зависимости от масштаба, уровня детализации и доступных вычислительных ресурсов. Сравниваются результаты экспериментов, делается вывод о применимости SEIRS-NIMFA к сетевым топологиям и приводятся рекомендации для дальнейших исследований.