Сравнительный анализ средств натурного моделирования Kathara и Containerlab на задаче распространения компьютерного вируса

И. О. Ищенко and А. А. Мишина

Российский университет дружбы народов им. Патриса Лумумбы, ул. Миклухо-Маклая, д. 6, Москва, 117198, Российская Федерация

Предпосылки Эпидемиологические модели SIR, SEIR и SEIRS широко используются в исследовательских работах. Применение теоретических моделей заражения в работе позволяет сконцентрироваться на изучении системных параметров эмулятора Kathara, а не на математической точности результатов эмуляции. Изучение средства моделирования необходимо для его использования в будущих исследованиях. **Цель** Проанализировать технические показатели производительности средства натурного моделирования Kathara на примере распространения компьютерного вируса. **Методы** Компартментные эпидемиологические моделей SIR, SEIR и SEIRS используются для анализа динамики распространения инфекций и оценки параметров системы в условиях воспроизводимого натурного эксперимента в Kathara. Построены дискретно-временные реализации моделей с параметрами β, σ и γ. Вычислительный эксперимент организован как сеть взаимодействующих узлов, один из которых является нулевым пациентом и запускает процесс заражения. **Результаты Заключение**

Ключевые слова: Натурное моделирование, Kathara, эпидемиологическая модель, SIR, SEIR, SEIRS

1. Введение

Данное исследование посвящено проведению натурного эксперимента по моделированию заражения компьютерным вирусом в эмуляторе Kathara. Изучение механизмов распространения вируса позволяет проанализировать возможности системы, в которой проводятся исследования, и ее устойчивость к вредоносному трафику. Традиционно для исследования динамики распространения вирусов применяются математические модели, заимствованные из эпидемиологии [1], такие как модели SIR (Susceptible-Infected-Recovered), SEIR (Susceptible-Exposed-Infected-Recovered) и SEIRS (Susceptible-Exposed-Infected-Recovered-Susceptible). Эти модели позволяют описывать процессы заражения, инкубации и восстановления в популяции узлов сети.

Средство моделирования Kathara дает возможность создавать виртуальные сетевые топологии и исследовать их поведение в контролируемых условиях. Несмотря на растущую популярность рассматриваемого эмулятора в академическом сообществе [2] [3], систематический анализ его технических характеристик и производительности при моделировании процессов распространения компьютерных вирусов остаётся недостаточно изученным вопросом. Эта работа направлена на оценку возможностей системы при работе с различными эпидемиологическими моделями, а также понимание ограничений платформы с точки зрения масштабируемости и точности результатов.

И. О. Ищенко: 1132226529@rudn.ru

А. А. Мишина: 1132226532@rudn.ru

Использование хорошо изученных эпидемиологических моделей SIR, SEIR и SEIRS в качестве теоретической основы позволяет сосредоточить внимание именно на системных параметрах эмулятора: использовании память, потреблении памяти и метриках сетевого трафика.

2. Основная часть

2.1. Эпидемиологические модели

Компартментные модели - математическая модель, которая описывает процессы взаимодействия различных субъектов (например, особей) из разных групп (компартментов) в течение времени. Каждый субъект принадлежит одной группе, при этом внутри каждой группы субъекты неразличимы.

Одной из простейших компартментных моделей является модель распространения эпидемий SIR. Эта модель была создана Уильямом Кермаком и Андерсоном МакКендриком в 1927 году. Все особи популяции в данном модели делсятся на три группы:

- S (susceptible) - здоровые особи, подверженные заболеванию;
- I (infectious) - зараженные особи, распространяющие болезнь;
- R (recovered) - переболевшие особи, приобретшие иммунитет.

Однако, во многих болезнях есть икубационных период, во время которого особь заражена, но не пока заразна. Так появилась модель SEIR, где присутвует четвертая группа E (exposed) - особи, находящиеся в латентном периоде заболевания. Такая модель повышает точность моделирования инфекционных заболеваний, например, COVID-19.

Мы будем рассматривать замкнутую популяцию, где отсутствуют процессы рождаемости и смертности. Тогда можно описать эволюцию особи следующей диаграммой:

$$S \xrightarrow{\beta} E \xrightarrow{\sigma} I \xrightarrow{\gamma} R$$

Модель описывается системой дифференциальных уравнений:

$$\begin{aligned}
\frac{dS}{dt} &= -\frac{\beta SI}{N}, \\
\frac{dE}{dt} &= \frac{\beta SI}{N} - \sigma E, \\
\frac{dI}{dt} &= \sigma E - \gamma I, \\
\frac{dR}{dt} &= \gamma I, \\
N &= S(t) + E(t) + I(t) + R(t),
\end{aligned}$$

где

- β - коэффициент заражения (вероятность того, что контакт между восприимчивым и заражённым приводит к новому заражению) $(S \to E)$;
- σ - коэффициент инкубационного перехода (вероятность того, что зараженный индивид становится заразным) $(E \to I)$;
- γ - коэффициент выздоровления (вероятность того, что заражённый индивид выздоравливает) $(I \to R)$.

Еще одной модификацией модели SIR является модель SEIRS. В жизни у определенной части переболевших особей иммунитет со временем ослабевает. Модель SEIRS допускает перехо особей из состояния выздоровевших в восприимчивое состояние.

Диаграмма эволюции особи выглядит следующим образом (рис. 1).

Система дифференциальных уравнений для модели SEIRS имеет вид:

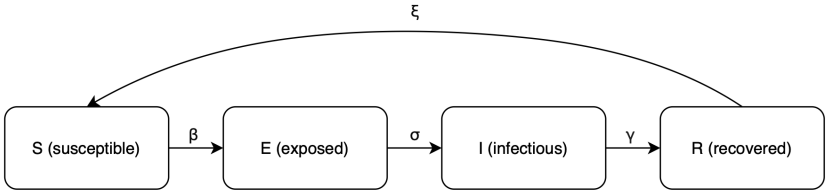

Рис. 1: Диаграмма эволюции особи в модели SEIRS

$$\begin{aligned}
\frac{dS}{dt} &= -\frac{\beta SI}{N} + \xi R, \\
\frac{dE}{dt} &= \frac{\beta SI}{N} - \sigma E, \\
\frac{dI}{dt} &= \sigma E - \gamma I, \\
\frac{dR}{dt} &= \gamma I - \xi R \\
N &= S(t) + E(t) + I(t) + R(t),
\end{aligned}$$

где

- ξ - вероятность потери иммунитета (вероятность того, что выздоровевший индивид со временем возвращается в категорию восприимчивых) ($R \to S$).

Если приток восприимчивых в популяцию достаточно велик, система в установившемся состоянии переходит в эндемическое равновесие (устойчивое состояние системы, в котором инфекция сохраняется на постоянном уровне: не исчезает и не угасает), сопровождаемое затухающими колебаниями численности заболевших.

2.2. Моделирование

Для реализации эксперимента использовались два инструмента эмуляции сетей: Kathará и Containerlab. Kathará – система эмуляции сетей на основе docker-контейнеров с открытым исходным кодом, поддерживаемое на всех основных операционных системах (Linux, macOs, Windows). Она предназначена для демонстрации взаимодействия узлов сети в изолированной среде и разработки новых сетевых протоколов.

Containerlab – инструмент, предоставляющий интерфейс командной строки для оркестрации и управления сетевыми лабораториями на основе контейнеров. Для создании лабораторной топологии Containerlab поднимает контейнеры, создает виртуальную связь между ними и самостоятельно управляет жизненным циклом всей лаборатории. Эмулятор использует YAML-формат для описания топологии и поддерживает интеграцию с Docker.

В данной работе использовались стандартный образ на базе Debian с предустановленными сетевыми утилитами (kathara/base) в Kathará и кастомный образ на базе debian:bookworm-slim с openssh-server, openssh-client, python3, iproute2 в Containerlab.

Топология сети одинакова для обоих инструментов: плоская сеть со ста узлами. Первый узел хоста (pc1) является нулевым пациентом, т. е. он инфицирован изначально. Этот узел и запускает распространение вируса. Переходы реализованы как стохастические процессы: каждые t секунд хост проверяет вероятность перехода в следующее состояние. В работе задействован принцип червя Морриса: если хост уязвим, то происходит дальнейшее распространение с помощью копирования Python-скрипта по SCP и удалённый запуск ”вируса” через SSH. Каждый узел в свою очередь прослушивает TCP-порт 4000 для обмена информацией о текущем состоянии с соседями. В то же время ведется логирование событий, а именно переходов между состояниями, в CSV-файл. Для мониторинга процесса был написан внешний

скрипт, опрашивающий все узлы и собирающий общую статистику по состояниям S, E, I, R (S, I, R для модели SIR). Параметры эмуляций отражены в таблицах (табл. 1, табл. 2, табл. 3).

Таблица 1: Параметры модели SIR

Параметр	**Обозначение**	**Значение**
Вероятность заражения	β	0.8
Вероятность выздоровления	γ	0.1
Интервал проверки $I \to R$	—	5 с
Задержка между сканированиями	—	0.2 с

Таблица 2: Параметры модели SEIR

Параметр	**Обозначение**	**Значение**
Вероятность заражения	β	0.4
Вероятность активации	σ	0.4
Вероятность выздоровления	γ	0.3
Интервал проверки $E \to I$	—	3 с
Интервал проверки $I \to R$	—	5 с
Задержка между сканированиями	—	2 с

Таблица 3: Параметры модели SEIRS

Параметр	**Обозначение**	**Значение**
Вероятность заражения	β	0.7
Вероятность активации	σ	0.5
Вероятность выздоровления	γ	0.15
Вероятность потери иммунитета	ξ	0.25
Интервал проверки $E \to I$	—	3 с
Интервал проверки $I \to R$	—	8 с
Интервал проверки $R \to S$	—	15 с
Максимум циклов реинфекции	—	3
Задержка между сканированиями	—	1 с

3. Результаты

По результам эмуляций были построены графики для каждой модели. Для этого был создан скрипт-анализатор логов, который построил графики, используя известную библиотеку matplotlib. Значения на оси абсцисс отражают время эксперимента, а на оси ординат - число хостов.

Рассмотрим подробнее и сравним графики обоих инструментов по модели SEIRS (рис. 2), (рис. 3).

Из графиков видны различия в динамике распространения инфекции. В Kathará эпидемический процесс развивается быстрее, что выражается в более раннем пике инфицированных узлов и ускоренном перераспределении состояний между компартментами S, E, I и R. Напротив, в Containerlab наблюдается более растянутая динамика. Различия темпа эмуляции могут указывать на различия используемых docker-контейнеров, ведь контейнер Kathará применяется минималистичный образ, тогда как в Containerlab более тяжелое окружение.

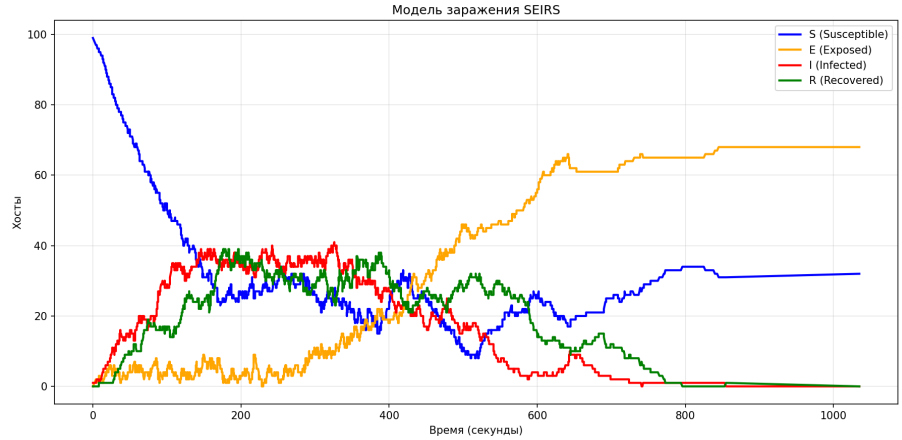

Рис. 2: График процесса заражения по модели SEIRS на Kathará

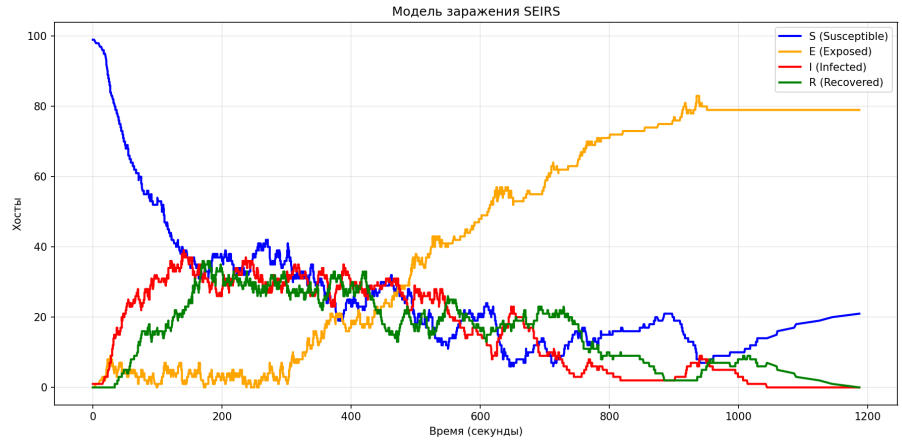

Рис. 3: График процесса заражения по модели SEIRS на Containerlab

4. Обсуждение

5. Заключение

Исследование было посвящено моделированию эпидемиалогических моделей в эмуляторах Kathara и Containerlab с целью их дальнейшего сравнения и анализа параметров систем. Получилось создать воспроизводимые эксперименты в двух средах, результаты которых оказались сопоставимы и похожи. Поведение теоретических моделей не выдало непредсказуемых результатов. Для исследуемых процессов технически сильнее оказался эмулятор „„„„ВСТАВИТЬ„„„„, поэтому в дальнейшем он будет приоритетным для решения задач кибербезопасности.

Благодарности

Авторы выражают глубокую признательность своему научному руководителю Анне Владиславовне Корольковой за ценные рекомендации и поддержку в ходе выполнения исследования. Отдельная благодарность профессору Дмитрию Сергеевичу Кулябову за постановку задачи и содержательные замечания.

Список литературы

1. *Hoang M. T.* A simple approach for studying stability properties of an SEIRS epidemic model // Journal of Applied Analysis. — 2025. — Т. 31, № 1. — С. 143—156. — DOI: doi:10.1515/jaa-2024-0019.
2. *Huu V. L. N.*, *Chau K. K.* Enhancing Computer Network Learning with Hands-on Lab Exercises // Software Engineering: Emerging Trends and Practices in System Development / под ред. R. Silhavy, P. Silhavy. — Cham : Springer Nature Switzerland, 2025. — С. 327—338.
3. *Usmanov O.*, *Muthanna A.*, *Paramonov A.* Analysis of SDN Traffic using Full-scale Modeling //. — Moscow, Russia : IEEE, 2018. — С. 1—4. — DOI: 10.1109/ICUMT.2018.8631205.