МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»
Кафедра теории функций и стохастического анализа

АНАЛИЗ СТАБИЛЬНОСТИ РАБОТЫ СЕТЕЙ МЕТОДАМИ ТЕОРИИ СЛУЧАЙНЫХ ГРАФОВ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

Студента 2 курса 248 группы
направления 09.04.03 — Прикладная информатика
механико-математического факультета
Ал-Тамими Мустафы Нахеда Мохаммеда

Научный руководитель
доцент, к. э. н. _____ А. Р. Файзлиев

Заведующий кафедрой
д. ф.-м. н., доцент _____ С. П. Сидоров

Саратов 2022

Введение

Понимание процессов распространения в сложных сетях является центральным вопросом в области науки о сетях с приложениями в распространении слухов [2], распространении вредоносных программ [3]. В этом направлении за последнее десятилетие были достигнуты важные успехи в анализе процессов распространения по инвариантным во времени (TI) сетям (недавние обзоры см. в [4]). В предположении неизменности во времени мы находим несколько недавних прорывов в литературе, таких как строгий анализ аппроксимаций среднего поля, новые инструменты моделирования для анализа многослойных сетей.

Одна из фундаментальных философий, на которых работает Интернет, заключается в том, что это сеть с максимальной эффективностью без какой-либо поддержки резервирования или гарантий производительности. Это приводит к относительно простой, масштабируемой структуре внутренних компонентов сети, а сложности, связанные с устойчивой и надежной передачей данных, переносятся на конечные хосты. Чтобы получить хорошую общую производительность, хосты не должны загружать сеть трафиком, несоизмеримым с тем, что сеть может поддерживать в любое время. Таким образом, сетевые протоколы, такие как TCP и приложения, должны периодически проверять сеть, чтобы определять доступность ресурсов (например, полосы пропускания), доступных в сети, и адаптироваться к изменяющимся сетевым условиям [5].

Актуальность темы исследования. Наука о сетях (Network science), сформировавшаяся в начале нынешнего века, решает широкий круг задач, связанных с изучением сетей, в частности, задач их анализа и идентификации, изучения процессов развития сетей и распространения информации по сетям, исследования устойчивости к разрушающим воздействиям и т.д. Одна из

важнейших задач – это изучение и прогнозирование процессов роста сетей, поскольку задачей Network science является «изучение сетевых представлений физических, биологических и социальных явлений, ведущее к прогнозирующим моделям этих явлений» [1].

Предмет исследования . Модели и алгоритмы анализ стабильности работы сетей методами теории случайных графов.

Научная новизна исследования . Состоит в использовании методов и алгоритмов для генерации случайных сетей.

Практическая значимость. .....

Цель и задачи исследования. Данной работы является разработка метода и программного средства генерации случайных сетей, похожих на данный, соответствующих следующим требованиям: – автоматическое обучение на генерации случайных сетей; – возможность генерировать случайных сетей контролируемого размера. Для достижения поставленной цели в работе ставятся следующие задачи:

1. Исследование методы анализ стабильности работы сетей.

2. Исследование сетевая безопасность.

3. Описание модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей

Объект исследования. Оценка вероятности связности сети, построенной по модели Б.-А., при сетевых атаках (с вероятностью p удаляются ребра из сети).

Методы исследования. Решение поставленных в работе задач осуществляется с использованием методами теории вероятностей, математической статистики, численных методов, методов решения дифференциальных и разностных уравнений, а также модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей.

Структура работы определена задачами исследования, логикой раскрытия темы. Работа состоит из введения, трех глав, заключения и списка использованных источников.

Во введении обосновывается выбор темы, актуальность исследования, определяются объект и предмет, цели и задачи, методы исследования, а также практическая значимость работы.

Первая глава диссертационной работы посвящена аналитическому обзору Сетевая безопасность,и важность сетевой безопасности, эталонная модель ISO/OSI для сетей,архитектура интернета и аспекты уязвимости безопасности,модель сетевой безопасности,распространенные методы интернет-атак,технология интернет-безопасности, и также безопасность в разных сетях.

Во второй главе работы рассмотрены описание модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей , история предпочтительная присоединения, степени динамики, распределение степеней, предельные случаи, типы сетей Барабаши-Альберта, и также приложения для модели Барабаси-Альберта.

В третьей главе рассмотрены оценки вероятности связности сети, построенной по модели Б.-А., при сетевых атаках

В заключении сформулированы основные результаты диссертационной работы, отмечены ее научная значимость и практическая ценность, определены перспективы дальнейшей работы.

В первой главе «Сетевая безопасность» рассматривается понятие целом Сетевая безопасность , которая привлекает все больше внимания по мере расширения Интернета. Угрозы безопасности и интернет-протокол были

проанализированы для определения необходимой технологии безопасности. Технология безопасности в основном основана на программном обеспечении, но используются многие распространенные аппаратные устройства. Текущее развитие сетевой безопасности не очень впечатляет.

Первоначально предполагалось, что с учетом важности области сетевой безопасности будут активно исследоваться новые подходы к безопасности, как аппаратные, так и программные. Было неожиданностью увидеть, что большая часть разработок происходит в тех же технологиях, которые используются в настоящее время. Встроенная безопасность нового интернет-протокола IPv6 может предоставить множество преимуществ интернет-пользователям. Несмотря на то, что были обнаружены некоторые проблемы с безопасностью, интернет-протокол IPv6, по-видимому, избегает многих популярных в настоящее время атак. Совместное использование IPv6 и инструментов безопасности, таких как брандмауэры, средства обнаружения вторжений и механизмы аутентификации, окажутся эффективными для защиты интеллектуальной собственности в ближайшем будущем. Сфере сетевой безопасности, возможно, придется развиваться более быстрыми темпами, чтобы бороться с угрозами в будущем.

Во второй главе «Описание модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей » рассмотрим в модели Барабаши — Альберт (Б.-А.) который С 1999 года безмасштабные сети Барабаси-Альберта стали очень модными, и в этих сетях Барабаши-Альберта также моделировались спины Изинга. Таким образом, будет обсуждаться специальная модель в статистической механике, такая как сети Барабаши-Альберта. Сети Барабаши-Альберта (БА) или безмасштабные сети очень известны с 1999 года и совсем недавно были преобразованы в полунаправленные (SDBA) сети.

В этой главе объясняется модель Барабаси-Альберта и история концепции предпочтительная присоединения для достижения сетей Барабаси-Альберта, а также обсуждается сеть, степени динамики и степени распределения. В конце

главы я упомянул несколько сетевых приложений Альберта Барабаши.

В третьей главе «.....» .....

Заключение. Проведенное исследование позволяет сделать следующие выводы.

В этом работе предложены анализа модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей. Эффективная и надежная защита компьютерной сети невозможна без предварительного анализа возможных угроз ее безопасности, среди которых наиболее сильными являются таргетированные компьютерные атаки. Таргетированные компьютерные атаки и способность противодействовать их реализации является ключевыми факторами, определяющими устойчивость компьютерных сетей. Оценка свойства устойчивости компьютерной сети в условиях таргетированных компьютерных атак, под которым понимается ее возможность противостоять различным видам пассивных и активных атак и сохранять показатели своего функционирования в условиях воздействия этих атак, является достаточно важной и сложной задачей. Аналитическое моделирование таргетированных компьютерных атак во многом помогает эффективному решению этой задачи. В работе предлагается применять Исследование модели Барабаши — Альберт (Б.-А.) для генерации случайных сетей для аналитического моделирования различных типов таргетированных компьютерных атак и использовать результаты моделирования для решения задачи оценки устойчивости компьютерной сети.

N – число вершин графа.

P – вероятность удаления ребра.

M – число новых ребер на каждом шаге

Проверятся вероятность связанности графа, построенного по модели Барабаши-Альберт, в случае удаления ребер с вероятностью p.

СПИСОК ЛИТЕРАТУРЫ

1- Network science /National Research Council. – Washington, DC: The National Academies Press, 2005. – 124 p. – ISBN 978-0-309-7.

2- P. Van Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,” IEEE/ACM Transactions on Networking, vol. 17, pp. 1–14, 2009.

3- M. Garetto, W. Gong, and D. Towsley, “Modeling malware spreading dynamics,” in IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, 2003, pp. 1869–1879.

4- R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, “Epidemic processes in complex networks,” Reviews of Modern Physics, vol. 87, pp. 925–979, 2015

5- Лапонина, О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапонина. - М.: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2013. - 536 с.