РАЗРАБОТКА КОМБИНАТОРНЫХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ КОЛИЧЕСТВА ДОПУСТИМЫХ МАРШРУТОВ В ОДНОРАНГОВЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ИНИЦИАТОРА И ПОЛУЧАТЕЛЯ В КАЧЕСТВЕ ПРОМЕЖУТОЧНЫХ УЗЛОВ

***П.Б. Болдыревский**, д.ф.-м.н, профессор, Нижегородский государственный университет им. Н.И. Лобачевского, bpavel2@rambler.ru;*
***В.Д. Зюзин**, Нижегородский государственный университет им. Н.И. Лобачевского, v.d.zyuzin@gmail.com.*

УДК 004.056:004.7:004.272.7:529.7

Аннотация. В статье рассматриваются подходы к разработке комбинаторных моделей для оценки количества допустимых маршрутов в одноранговых сетях. Предложенные методы позволяют повысить устойчивость маршрутизации к анализу трафика и минимизировать риски компрометации анонимности узлов. Рассматриваются три основных подхода: вычитание ложных маршрутов, декомпозиционный подход и прямой комбинаторный анализ. Проведен сравнительный анализ методов на примере сети с двумя промежуточными узлами. Все предложенные формулы подтверждены экспериментальными данными для сетей с различным числом узлов. Полученные результаты могут быть использованы для проектирования защищенных распределенных систем и автоматизированного анализа безопасности одноранговых сетей.

Ключевые слова: одноранговые сети; маршрутизация; комбинаторные модели; анализ безопасности; анонимность; распределенные системы.

DEVELOPMENT OF COMBINATORIAL MODELS FOR ASSESSING THE NUMBER OF FEASIBLE ROUTES IN PEER-TO-PEER NETWORKS

***Pavel Boldyrevskii**, Doctor of Physical and Mathematical Sciences, N.I. Lobachevsky State University of Nizhny Novgorod;*
***Vladislav Zyuzin**, N.I. Lobachevsky State University of Nizhny Novgorod.*

Annotation. The article examines approaches to the development of combinatorial models for assessing the number of feasible routes in peer-to-peer (P2P) networks. The proposed methods enhance the resilience of routing against traffic analysis and reduce the risk of node anonymity compromise. Three main approaches are considered: subtracting false routes, the decomposition approach, and direct combinatorial analysis. A comparative analysis of these methods is conducted using a network with two intermediate nodes as an example. All proposed formulas have been validated with experimental data for networks of various sizes. The results can be used for designing secure distributed systems and automated security analysis of peer-to-peer networks.

Keywords: peer-to-peer networks; routing; combinatorial models; security analysis; anonymity; distributed systems.

Введение

Одноранговые (*Peer-to-Peer – P2P*) сети представляют собой децентрализованные системы, в которых каждый узел может выполнять роль как инициатора, так и получателя данных [1, 2]. Важнейшим аспектом в подобных системах, особенно в условиях растущих угроз информационной безопасности,

является способность обеспечивать анонимность и защищенность передачи. С увеличением количества кибератак и развитием методов анализа трафика [3-5] актуальность совершенствования маршрутизации в *P2P*-сетях возрастает.

Одним из ключевых подходов к повышению устойчивости сети к анализу трафика являются маршруты, сформированные с участием нескольких промежуточных узлов. Аналогии с системами *Tor* [6] и *I2P* [7] показывают, что варьирование количества и типа промежуточных узлов затрудняет действия злоумышленников, пытающихся установить соответствие между инициатором и получателем. Однако существующие решения имеют ограничения, связанные с правилами выбора промежуточных узлов, что в ряде случаев снижает комбинаторное разнообразие маршрутов.

В данной работе предлагается расширить модель выбора промежуточных узлов, включив в множество доступных для маршрутизации узел-инициатор (A) и узел-получатель (D) [8, 9]. Рассматриваются математические формулы, позволяющие строго оценить количество допустимых маршрутов с учетом различных ограничений, исключающих ложные или невозможные сценарии для сети с двумя промежуточными узлами.

Описание проблемы и постановка задачи

В существующих реализациях систем *Tor* и *I2P* имеется недостаток, связанный с ограничением выбора промежуточных узлов. Для маршрутов с двумя и более промежуточными узлами предлагается включать узел-инициатора и узел-получателя в список возможных промежуточных узлов.

То есть, в данном случае при выборе первого промежуточного узла будет не $n-2$, а $n-1$, за исключением только узла-инициатора. При выборе второго промежуточного узла также будет $n-1$, так как исключению подлежит только узел-инициатор или предыдущий узел. Такой подход обеспечивает увеличение комбинаторики выбора путей передачи данных, затрудняя идентификацию конечных участников взаимодействия. Формула для расчета количества возможных маршрутов в данном случае будет следующей:

$$F_{\text{возм.маршр.}} = \prod_{i=1}^{k}(n-1), \quad (1)$$

где: $F_{\text{возм.маршр.}}$ – количество возможных маршрутов соединения узла-инициатора с узлом-получателем через k промежуточных узлов; n – количество узлов в сети; k – количество промежуточных узлов.

Рассмотрим пример сети, состоящей из четырех узлов (A, B, C, D). Пусть узлом-инициатором будет (A), а узлом-получателем – (B).

Получается семь возможных маршрутов:

$$A \to B \to A \to B$$
$$A \to B \to C \to B$$
$$A \to B \to D \to B$$
$$A \to C \to A \to B$$
$$A \to C \to D \to B$$
$$A \to D \to A \to B$$
$$A \to D \to C \to B$$

Но по формуле (1) получается:

$$F = (4-1)^2 = 9$$

Избыточные два маршрута оказались ложными, поскольку они заканчиваются последовательностью ($B \to B$), недопустимой в реальной системе.

$$A \to C \to B \to B$$
$$A \to D \to B \to B$$

Аналогично был запрещен выбор узла-инициатора (A) в качестве первого промежуточного узла ($A \to A$), но формула (1) уже исключает этот факт.

Таким образом, для достижения строгого соответствия между теоретической оценкой и реальным числом возможных маршрутов необходимо модифицировать формулу (1) с учетом рассмотренных ограничений.

Разработку искомой формулы, корректирующей первоначальный результат, можно осуществить тремя принципиально разными подходами:

1. Подход через вычитание ложных маршрутов ($B \to B$) из формулы (1).
2. Декомпозиционный подход.
3. Подход прямого комбинаторного анализа.

Подход вычитания ложных маршрутов

Начнем с упрощенной верхней оценки, в которой уже были учтены некоторые ограничения, а именно – недопустимость использования узла-инициатора (A) в качестве первого промежуточного узла (формула (1)). Данная величина переоценивает количество маршрутов, включив в себя также нереализуемые комбинации, особенно те, которые завершаются последовательностью ($B \to B$).

Полноценный маршрут (на примере системы с двумя промежуточными узлами) выглядит следующим образом:

$$A \to X_1 \to X_2 \to B,$$

где: A – узел-инициатор;B – узел-получатель; X_1 – первый промежуточный узел; X_2 – второй промежуточный узел.

Рассмотрим подробнее количество таких ложных (нереализуемых) маршрутов. Ложный маршрут имеет вид:

$$A \to X_1 \to B \to B,$$

где второй промежуточный узел $X_2 = B$ приводит к недопустимой ситуации «узел-получатель направляет пакет самому себе».

Промежуточный узел (X_1) не может быть узлом-инициатором (A), поскольку формула (1) исключает маршруты типа ($A \to A$) на начальном этапе. Аналогично, промежуточный узел (X_2) не может выступать в роли узла-получателя (B), т.к. формула (1) также запрещает маршруты типа ($B \to B$) в процессе маршрутизации, предотвращая повторное использование узла-получателя (B) в качестве промежуточного. Таким образом, промежуточным узлом (X_1) может быть любой узел сети, кроме узла-инициатора (A) и узла-получателя (B), что формально выражается следующей формулой:

$$F_{1\ \text{пр.уз.}} = n - 2 \quad (2)$$

Исключая эти ложные маршруты из общей оценки (формула (1)), на примере системы с двумя промежуточными узлами получаем:

$$F_{\text{реал.возм.маршр.}} = (n-1)^2 - (n-2), \quad (3)$$

где: $F_{\text{реал.возм.маршр.}}$ – количество реальных возможных маршрутов в системе с двумя промежуточными узлами подходом вычитания ложных маршрутов; n – количество узлов в сети.

Декомпозиционный подход

Данный подход заключается в том, что общее количество маршрутов разбивается на логические категории: маршруты через два «обычных» узла, маршруты с «петлей» через инициатора (A) и маршруты с «петлей» через получателя (B) и далее суммируются.

1. Базовые маршруты через два разных «обычных» промежуточных узла, исключая рассмотрения маршрутов узел-инициатор (A) и узел-получатель (B). Ранее была получена формула:

$$F_{\text{возм.маршр.через 2 пр.узл.}} = (n-2)(n-3), \quad (4)$$

где: $F_{\text{возм.маршр.через 2 пр.узл.}}$ – количество возможных маршрутов соединения узла-инициатора с узлом-получателем через два промежуточных узла; n – количество узлов в сети.

2. Маршруты с «петлей» через узел-инициатор (A) имеют вид:

$$A \to X_1 \to A \to D,$$

где второй промежуточный узел $X_2 = A$.

Такие маршруты позволяют использовать узел-инициатор (A) в качестве одного из промежуточных узлов, но не создавая ситуацию ($A \to A$) в начале. Выбор первого промежуточного узла (X_1) возможен из $n-1$ вариантов (все узлы, кроме узла-инициатора (A)), следовательно:

$$F_{\text{петля через } A} = (n-1), \quad (5)$$

где: $F_{\text{петля через } A}$ – количество возможных маршрутов с «петлей» через узел-инициатор (A).

3. Маршруты с «петлей» через узел-получатель (B) имеют вид:

$$A \to B \to X_2 \to B,$$

где первый промежуточный узел $X_1 = D$.

Такие маршруты позволяют использовать узел-получатель (B) в качестве одного из промежуточных узлов, но не создавая ситуацию ($B \to B$) в конце.

Промежуточный узел (X_2) не может быть узлом-получателем (B), поскольку формула (1) исключает маршруты типа ($B \to B$) в процессе маршрутизации. То есть, фактически, аналогично с маршрутами с «петлей» через узел-инициатор (A),

маршруты с «петлей» через узел-получатель (B) высчитываются по формуле (5). Но возникает ситуация следующего типа:

$$A \to B \to A \to B,$$

которая учитывается в маршрутах с «петлей» через узел-инициатор (A) и с «петлей» через узел-получатель (B). В связи с этим предлагается убрать этот вариант и вывести формулу маршрутов с «петлей» через узел-получатель (B), кроме маршрута типа $A \to B \to A \to B$, то есть за исключением первого варианта:

$$F_{\text{петля через } B} = (n-2) \tag{6}$$

Складывая все три части, получаем:

$$F_{\text{реал.возм.маршр.}} = (n-2)(n-3) + (n-1) + (n-2), \tag{7}$$

где: $F_{\text{реал.возм.маршр.}}$ – количество реальных возможных маршрутов в системе с двумя промежуточными узлами декомпозиционным подходом; n – количество узлов в сети.

Подход прямого комбинаторного анализа

Данный подход включает в себя последовательный разбор вариантов для промежуточных узлов X_1 и X_2.

Первая позиция X_1 не может быть узлом-инициатором (A), оставляя $n-1$ возможных узлов. Среди них один узел может быть узлом-получателем (B), и еще $n-2$ – это обычные (не A и не B) узлы.

Если $X_1 = B$, то для X_2, учитывая уже занятый узел (B) и отсутствие необходимости исключать его в этой же позиции (он уже использован), остается $n-1$ вариантов.

Если X_1 – обычный узел (то есть не узел-инициатор и не узел-получатель), всего таких вариантов $n-2$. Теперь для X_2 нельзя использовать (B) (последний промежуточный узел маршрута не может быть узлом-получателем), а также нельзя повторять уже выбранный на первом шаге узел. Изначально оставалось $n-1$ узлов после выбора X_1, исключая из них (B), получаем $n-2$ вариантов для X_2.

Подытожим: варианты с $X_1 = B$ дают $n-1$ маршрутов, а варианты с X_1 – обычным узлом дают $(n-2)(n-2) = (n-2)^2$ маршрутов и, складывая их, получаем:

$$F_{\text{реал.возм.маршр.}} = (n-1) + (n-2)^2, \tag{8}$$

где: $F_{\text{реал.возм.маршр.}}$ – количество возможных маршрутов соединения узла-инициатора с узлом-получателем через два промежуточных узла подходом прямого комбинаторного анализа; n – количество узлов в сети.

Проверка формул

Для начала упростим и раскроем формулы:

$$F_{\text{реал.возм.маршр.}} = (n-1)^2 - (n-2) = n^2 - 3n + 3$$

$$F_{\text{реал.возм.маршр.}} = (n-2)(n-3) + (n-1) + (n-2) = n^2 - 3n + 3$$

$$F_{\text{реал.возм.маршр.}} = (n-1) + (n-2)^2 = n^2 - 3n + 3$$

Все три подхода для $k = 2$ сводятся к одной формуле:

$$F_{\text{реал.возм.маршр.}} = n^2 - 3n + 3 \quad (9)$$

Рассмотрим пример сети, состоящей из трех узлов (A, B, C). Пусть узлом-инициатором будет (A), а узлом-получателем – (B), итого получилось три варианта:

$$A \to B \to C \to B$$
$$A \to B \to A \to B$$
$$A \to C \to A \to B$$

Результат расчета по формуле (9) такой же:

$$F_{\text{реал.возм.маршр.}} = 3^2 - 3 \times 3 + 3 = 9 - 9 + 3 = 3$$

Рассмотрим пример сети, состоящей из четырех узлов (A, B, C, D). Пусть узлом-инициатором будет (A), а узлом-получателем – (B). Итого получилось семь.

$$A \to B \to A \to B$$
$$A \to B \to C \to B$$
$$A \to B \to D \to B$$
$$A \to C \to A \to B$$
$$A \to C \to D \to B$$
$$A \to D \to A \to B$$
$$A \to D \to C \to B$$

По формуле (9) получилось также 7:

$$F_{\text{реал.возм.маршр.}} = 4^2 - 3 \times 4 + 3 = 16 - 12 + 3 = 7$$

Рассмотрим пример сети, состоящей из пяти узлов (A, B, C, D, F). Пусть узлом-инициатором будет (A), а узлом-получателем – (B), тогда получается 13 вариантов маршрута:

$$A \to B \to A \to B$$
$$A \to B \to C \to B$$
$$A \to B \to D \to B$$
$$A \to B \to E \to B$$
$$A \to C \to A \to B$$
$$A \to C \to D \to B$$
$$A \to C \to E \to B$$
$$A \to D \to A \to B$$
$$A \to D \to C \to B$$
$$A \to D \to E \to B$$
$$A \to E \to A \to B$$
$$A \to E \to C \to B$$
$$A \to E \to D \to B$$

По формулам (3), (7) и (9):

$$F_{\text{реал.возм.маршр.}} = 5^2 - 3 \times 5 + 3 = 25 - 15 + 3 = 13$$

При проверке со значениями $n = 3$, $n = 4$ и $n = 5$ все подходы показали правильный результат. Для упрощения работы с разработанными формулами и автоматизации анализа маршрутов было создано программное обеспечение [10], которое позволяет эффективно моделировать сложные топологии и проводить анализ безопасности в одноранговых сетях. Таким образом, предложенные модели открывают новые возможности для разработки защищенных распределенных систем и соответствуют современным требованиям в области информационной безопасности.

Сравнительный анализ подходов

В рамках данного исследования основные методы вычисления количества допустимых маршрутов были проверены на случае с двумя промежуточными узлами ($k = 2$). Все три рассмотренных подхода – вычитание ложных маршрутов, поэтапное суммирование категорий и прямой комбинаторный анализ – дают идентичный конечный результат для $k = 2$ и относительно легко реализуемы. Однако их практическая ценность и простота применения могут различаться при попытках распространить полученные результаты на большие значения k.

При $k = 2$ прямой комбинаторный анализ выглядит наиболее прозрачным и быстрым – происходит последовательное рассмотрение выбора промежуточных узлов, с учетом всех ограничений. Этот подход интуитивно понятен и не требует сложной логики. Однако при $k = 2$ он стремительно усложняется, поскольку число возможных ветвлений маршрутов возрастает экспоненциально.

Подход вычитания ложных маршрутов при $k = 2$ сравнительно прост – начинается с завышенной оценки и ее корректировки с удалением недопустимых сценариев. Этот метод вполне удобен для небольших значений k, однако при $k \geq 2$ учет большого количества новых ложных комбинаций требует значительно большей аналитической работы, усложняя процесс вычислений.

Декомпозиционный подход при $k = 2$ обеспечивает глубокое понимание внутренней структуры маршрутов, разделяя их на логические классы. В данном случае он тоже не слишком сложен, однако уже при переходе к $k = 3$ количество категорий и их взаимосвязей резко возрастает, что делает этот подход слишком громоздким.

Таким образом, при $k = 2$:

- Прямой комбинаторный анализ – наиболее простой и быстрый.
- Вычитание ложных маршрутов – понятный и умеренно сложный.
- Декомпозиционный подход – хорошо объясняет структуру, но требует чуть большей предварительной аналитической работы.

В целом, можно рекомендовать прямой комбинаторный анализ как наиболее быстрый и простой метод.

Заключение

В ходе исследования разработаны и проанализированы комбинаторные модели для оценки количества допустимых маршрутов в одноранговых сетях. Рассмотрены три подхода: вычитание ложных маршрутов, декомпозиционный подход и прямой комбинаторный анализ. Проведен сравнительный анализ методов, который показал, что все предложенные подходы корректно вычисляют

количество маршрутов для сетей с двумя промежуточными узлами. Прямой комбинаторный анализ был признан наиболее простым и интуитивно понятным для реализации.

Результаты исследования могут быть использованы для проектирования защищенных одноранговых сетей, способных противостоять анализу трафика и обеспечивать анонимность взаимодействия узлов. Разработанное программное обеспечение для автоматизации анализа маршрутов открывает новые возможности для изучения топологий сетей и повышения их безопасности.

Полученные модели соответствуют современным требованиям информационной безопасности и могут быть масштабированы для более сложных топологий и сетей с большим числом узлов. В дальнейшем планируется исследование более сложных маршрутов с большим числом промежуточных узлов и адаптация предложенных подходов для динамически изменяющихся сетей.

Литература

1. Одноранговые сети (сети без централизованного управления) // studfile.net URL: https://studfile.net/preview/2802302/page:6/ (дата обращения: 16.10.2024).
2. Xuemin Shen, Heather Yu, John Buford, Mursalin Akon (Eds.). Handbook of Peer-to-Peer Networking. Springer, 2010. – 1421 p. ISBN 978-0-387-09750-3. DOI 10.1007/978-0-387-09751-0.
3. Михайленко Н.В., Мурадян С.В., Вихляев А.В. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости, 2022. – № 1. – С. 140-145.
4. Цифровые технологии и информационная безопасность бизнес-процессов: Сборник научных статей по итогам международной научно-практической конференции, Нижний Новгород, 22 мая 2024 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. – 257 с. – EDN QPLWRU.
5. Филимонов А. В. Разработка системы оценки и управления рисками в области авиационной безопасности // Цифровые технологии и информационная безопасность бизнес-процессов: Сборник научных статей по итогам международной научно-практической конференции, Нижний Новгород, 22 мая 2024 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2024. – С. 108-118. – EDN XOADSQ.
6. Руководство пользователя браузера Tor // Tor URL: tb-manual.torproject.org/ru/ (дата обращения: 17.11.2024).
7. I2P Network Performance: Speed, Connections and Resource Management // I2P URL: geti2p.net/ru/about/performance (дата обращения: 19.11.2024).
8. Зюзин В.Д., Болдыревский П.Б. Метод множественных стартовых соединений как инструмент повышения информационной безопасности в одноранговых виртуальных частных сетях // Инженерный вестник Дона, 2024. – № 12. – URL: https://ivdon.ru/ru/magazine/archive/n12y2024/9708 (дата обращения: 20.12.2024).
9. Зюзин В.Д. Использование метода множественных стартовых соединений в задаче маскировки VPN-соединения // Труды XXVI научной конференции по радиофизике, посвященной 120-летию М.Т. Греховой: Материалы конференции, Нижний Новгород, 12-27 мая 2022 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2022. – С. 535-536. – EDN YFVKGA.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2024610455 Российская Федерация. Программный комплекс анализа сетевой

безопасности в VPN сети на основе технологии P2P (версия 1.0): № 2023689708: заявл. 22.12.2023: опубл. 10.01.2024 // В. Д. Зюзин. – EDN DHYOJP.