МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра теоретических основ компьютерной безопасности и криптографии

ОБНАРУЖЕНИЕ СЕТЕВОГО P2P ТРАФИКА МЕТОДОМ АНАЛИЗА ЕГО ПОВЕДЕНИЯ

КУРСОВАЯ РАБОТА

студента 3 курса 331 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Стаина Романа Игоревича

Научный руководитель
доцент _____ А. В. Гортинский

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов

Саратов 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Ввёл я не понимаю

1 пир ту пир

P2P (**p**eer-**to**-**p**eer), также известные как одноранговые, децентрализованные или пиринговые сети, — это распределенная архитектура приложения, которая разделяет зачачи между узлами (peer). Узлы имеют одинаковые привилегии в приложении и образуют сеть равносильных узлов.

Узлы делают свои ресурсы, такие как вычислительная мощность, объем диска или пропускная способность напрямую доступными остальным членам сети, без необходимости координировать действия с помощью серверов. Узлы являются одновременно поставщиками и потребителями ресурсов, в отличие от стандартной клиент-сервер модели, где поставщик и потребитель ресурсов разделены.

1.1 История

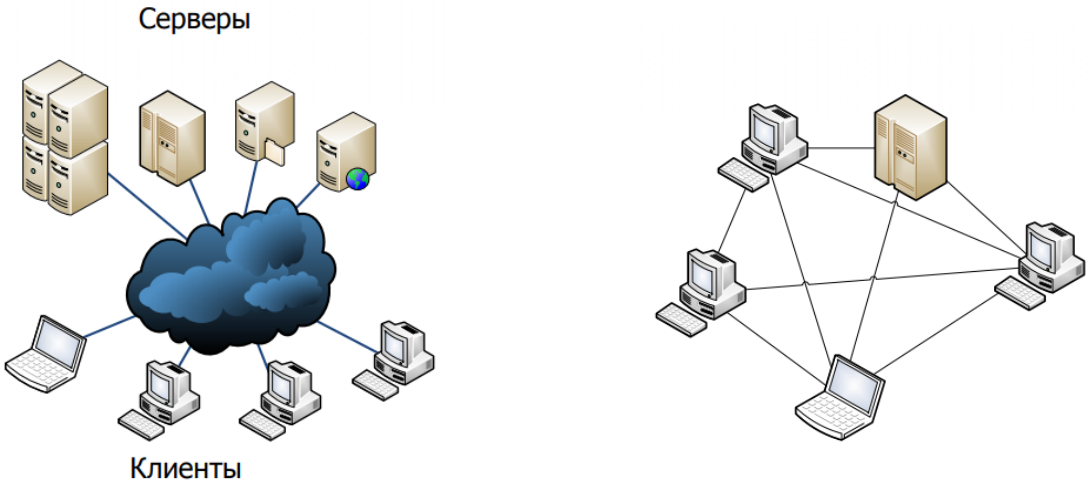
В то время как P2P системы использовались во многих доменных приложениях, архитектура популяризовалась благодаря файлообменной системе Napster, разработанной в 1999 году. Концепция вдохновила новую философию во многих областях человеческого взаимодействия. P2P технология позволяет пользователям интернета образовывать группы и коллаборации, формируя, тем самым, пользовательские поисковые движки, виртуальные суперкомпьютеры и файловые системы. Основная идея P2P систем исходит из первых принципов метода Request for Comment (RFC). Видение Всемирной паутины Тима Бернерса-Ли было близко к P2P сети, в том смысле что каждый пользователь является активным создателем и редактором контента.

Ранней версией P2P сетей является USENET — распределенная система обмена сообщениями. USENET был разработан в 1979 году и представлял собой систему, обеспечивающую децентрализованную модель управления. Основа представляет собой клиент-серверную модель, предполагающую самоорганизацию группы серверов. Тем не менее, сервера взаимодействуют друг с другом как равноправные узлы, распространяя информацию по всей сети USENET.

В мае 1999 года, в Интернет с более чем миллионом пользователей, Шон Фэннинг внедрил приложение файлообменник Napster. Napster стал началом P2P сети, такой какую мы знаем её сейчас, пользователи участвуют в создании виртуальной сети, полностью независимой от физической, без администрирования и каких-либо ограничений.

2 Архитектура

P2P сеть строится вокруг понятия равноправных узлов — клиенты и серверы одинаково взаимодействуют с другими узлами сети. Такая модель построения сети отличается от модели клиент-сервер, где взаимодействие идет с центральным сервером. На рисунке 1 а) изображены архитектура клиент-сервера и б) архитектура P2P. Типичным примером передачи файла в модели клиент-сервер является File Transfer Protocol (FTP), в котором программы клиента и сервера разделены: клиент инициирует передачу, а сервер отвечает на запросы.



а) б)

Рисунок 1 – Архитектура клиент-сервера и P2P

2.1 Маршрутизация

P2P сети обычно реализуют некоторую форму виртуальной сети, наложенную поверх физической сети, где узлы образуют подмножество узлов в физической сети. Данные по-прежнему обмениваются непосредственно над базовой TCP/IP сетью, а на прикладном уровне узлы имеют возможность взаимодействовать друг с другом напрямую, с помощью логических связей. Наложение используется для индексации и обнаружения узлов, что позволяет системе P2P быть независимой от физической сети. На основании того, как узлы соединены друг с другом внутри сети, и как ресурсы индексированы и расположены, сети классифицируются на **неструктурированные** и **структурированные** (или как их **гибрид**).

2.1.1 Неструктурированные сети

Неструктурированная P2P сеть не формирует определенную структуру сети, а случайным образом соединяет узлы друг с другом. Так как не существует глобальной структуры формирования сети, неструктурированные сети легко организуются и доступны для локальных оптимизаций. Кроме того, поскольку роль всех узлов в сети одинакова, неструктурированные сети являются весьма надежными в условиях, когда большое количество узлов часто подключаются к сети или отключаются от нее.

Однако, из-за отсутствия структуры, возникают некоторые ограничения. В частности, когда узел хочет найти нужный фрагмент данных в сети, поисковый запрос должен быть направлен через сеть, чтобы найти как можно больше узлов, которые обмениваются данными. Такой запрос вызывает очень высокое количество сигнального трафика в сети, требует высокой производительности, и не гарантирует, что поисковые запросы всегда будут решены.

2.1.2 Структурированные сети

В структурированных P2P сетях наложение организуется в определенную топологию, и протокол гарантирует, что любой узел может эффективно участвовать в поиске в файла или ресурса, даже если ресурс использовался крайне редко.

Наиболее распространенный тип структурированных сетей P2P реализуется распределенными хэш-таблицами (DHT), в котором последовательное хеширование используется для привязки каждого файла к конкретному узлу. Это позволяет узлам искать ресурсы в сети, используя хэш-таблицы, хранящих пару ключ-значение, и любой участвующий узел может эффективно извлекать значение, связанное с заданным ключом.

Тем не менее, для эффективной маршрутизации трафика через сеть, узлы структурированной сети должны обладать списком соседей, которые удовлетворяют определенным критериям. Это делает их менее надежными в сетях с высоким уровнем оттока абонентов (т.е. с большим количеством узлов, часто подключающихся к сети или отключающихся от нее).

2.1.3 Гибридные модели

Гибридные модели представляют собой сочетание P2P сети и модели клиент-сервер. Гибридная модель должна иметь центральный сервер, который

помогает узлам находить друг друга. Есть целый ряд гибридных моделей, которые находят компромисс между функциональностью, обеспечиваемой структурированной сетью модели клиент-сервер, и равенством узлов, обеспечиваемой чистыми одноранговыми неструктурированными сетями. В настоящее время гибридные модели имеют более высокую производительность, чем чисто неструктурированные или чисто структурированные сети.

2.2 Безопасность

Как и любой другой форме программного обеспечения, P2P приложения могут содержать уязвимости. Особенно опасно для P2P программного обеспечения, является то, что P2P приложения действуют и в качестве серверов и в качестве клиентов, а это означает, что они могут быть более уязвимы для удаленных эксплоитов.

2.2.1 Маршрутизационные атаки

Поскольку каждый узел играет роль в маршрутизации трафика через сеть, злоумышленники могут выполнять различные «маршрутизационные атаки», или атаки отказа в обслуживании. Примеры распространенных атак маршрутизации включают в себя «неправильная маршрутизация поиска», когда вредоносные узлы преднамеренно пересылают запросы неправильно или возвращают ложные результаты, «неправильная маршрутизация обновления», когда вредоносные узлы изменяют таблицы маршрутизации соседних узлов, посылая им ложную информацию, и «неправильная маршрутизация разделения сети», когда новые узлы подключаются через вредоносный узел, который помещает новичков в разделе сети, заполненной другими вредоносными узлами.

2.2.2 Поврежденные данные и вредоносные программы

Распространенность вредоносных программ варьируется между различными протоколами одноранговых сетей. Исследования, анализирующие распространение вредоносных программ по сети P2P обнаружили, например, что 63% запросов на загрузку по сети Limewire содержали некоторую форму вредоносных программ, в то время как на OpenFT только 3% запросов содержали вредоносное программное обеспечение. Другое исследование анализа трафика в сети Kazaa обнаружили, что 15% от 500 000 отобранных файлов, были инфицированы одним или несколькими из 365 различных компьютерных вирусов.

Поврежденные данные также могут быть распределены по P2P-сети путем изменения файлов, которые уже были в сети. Например, в сети FastTrack, RIAA удалось внедрить фальшивые данные в текущий список загрузок и в уже загруженные файлы (в основном файлы MP3). Файлы, инфицированные вирусом RIAA были непригодны впоследствии и содержали вредоносный код. Следовательно, P2P сети сегодня внедрили огромное количество механизмов безопасности и проверки файлов. Современное хеширование, проверка данных и различные методы шифрования сделали большинство сетей, устойчивыми к практически любому типу атак, даже когда основные части соответствующей сети были заменены фальшивыми или нефункциональными узлами.

2.3 Отказоустойчивость и масштабируемость сети

Децентрализованность P2P сетей повышает их надежность, так как этот метод взаимодействия устраняет ошибку единой точки разрыва, присущую клиент-серверным моделям. С ростом числа узлов, объем трафика внутри системы увеличивается, масштаб сети также увеличивается, что приводит к уменьшению вероятности отказа. Если один узел перестанет функционировать должным образом, то система в целом все равно продолжит работу. В модели клиент-сервер, с ростом количества пользователей, уменьшается количество ресурсов выделяемых на одного пользователя, что приводит к риску возникновения ошибок.

2.4 Распределенное хранение и поиск

Возможность резервного копирования данных, восстановление и доступность приводят как и к преимуществами так и к недостатками P2P сетей. В централизованной сети, только системный администратор контролирует доступность файлов. Если администраторы решили больше не распространять файл, его достаточно удалить с серверов, и файл перестанет быть доступным для пользователей. Другим словами, клиент-серверные модели имеют возможность управлять доступностью файлов. В P2P сети, доступность контента определяется степенью его популярности, так как поиск идет по всем узлам, через которые файл проходил. То есть, в P2P сетях нет централизованной власти, как системный администратор в клиент-серверном варианте, а сами пользователи определяют уровень доступности файла.

3 Применение

3.1 Распространение контента

В P2P сетях, пользователи передают и используют контент сети. Это означает, что в отличие от клиент-серверных сетей, скорость доступа к данным возрастает с увеличением числа пользователей, использующих этот контент. На этой идее построен протокол Bittorrent — пользователи скачавшие файл, становятся узлами и помогают другим пользователям скачать файл быстрее. Эта особенность является главным преимуществом P2P сетей.

Множество файлообменных систем, таких как Gnutella, G2 и eDonkey популяризовали P2P технологии:

- Пиринговые системы распространения контента.
- Пиринговые системы обслуживания, например повышение производительности, в частности Correli Caches.
- Публикация и распространение программного обеспечения (Linux, видеоигры).

В связи децентрализованностью доступа к данным в P2P сетях возникает проблема нарушения авторских прав. Компании, занимающиеся разработкой P2P приложений часто принимают участие в судебных конфликтах. Самые известные судебные дела это Grokster против RIAA и MGM Studios, Inc. против Grokster Ltd., где в обоих случаях технологии файлообменных систем признавались законными.

3.2 Мультимедиа

- Протоколы P2PTV и PDTP.
- Некоторые фирменные мультимедийные приложения, такие как Spotify, используют P2P сеть наряду с потоковыми серверами для потоковой передачи аудио и видео для своих клиентов.
- Peercasting для многоадресной передачи потоков.
- Университет штата Пенсильвания, MIT и Университет Саймона Фрейзера ведут проект под названием LionShare, предназначенной для облегчения обмена файлами между образовательными учреждениями во всем мире.
- Osiris — это программа, которая позволяет пользователям создавать анонимные и автономные веб-порталы, распределенные через P2P сети.

3.3 Другие приложения P2P

— Bitcoin и альтернативые криптовалюты, такие как Peercoin и NXT основаны на технологии равноправных узлов.
— I2P — сеть, используемая для анонимного использования Интернета.
— Infinit является неограниченным и зашифрованным P2P приложением общего доступа к файлам.
— Netsukuku — беспроводная общественная сеть, разработанная быть независимой от Интернета.
— Dalesa, веб-кэша для локальных сетей (на основе IP многоадресной передачи).
— Open Garden, приложение совместного пользования интернетом, раздавая подключение через Wi-Fi или Bluetooth.
— Исследования, такие как Chord project, утилита для хранения PAST, P-Grid и системы распределения контента CoopNet.
— JXTA, P2P протокол, предназначенный для платформы Java.

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ