И.Н. Кутовой, И.В. Манторова

Internet и сети “p2p” – проблемы сосуществования

Компьютерные сети прочно вошли в нашу жизнь. В Интернете много сервисов, которые облегчают работу пользователя. Несмотря на кажущееся разнообразие, основные сервисы достаточно централизованы. Вся информация проходит через единые центры и хранится там. При этом возникает ряд проблем.

Проблема первая. Сегодня мы доверяем свою информацию обезличенным корпорациям. Остается надеяться на то, что во многих корпорациях работают порядочные люди. Но в корпорациях могут быть люди, которые распоряжаются вверенной им информацией, преследуя свои умыслы.

Проблема вторая. Во всех странах правительственные службы на законодательном уровне контролируют информационные потоки. У каждого интернет-провайдера установлено оборудование спецслужб, которое полностью отслеживает трафик. Считается, что правительства всегда поступают честно. Но среди государственных служащих могут быть люди, которые преследуют интересы определенных групп.

Проблема третья. Центральные точки в сети подвержены риску выйти из строя или быть уничтоженными во время внешнего вторжения. Кроме того, некоторые владельцы просто останавливали свои серверы, иногда даже без уведомления клиентов. Централизованные сервисы физически уязвимы и подчинены воле определенных лиц.

Изначально термин peer-to-peer (P2P) был использован в 1984 г. компанией IBM при разработке сетевой архитектуры для динамической маршрутизации трафика через компьютерные сети с произвольной топологией (Advanced Peer to Peer Networking).

Существует мнение, что согласно первоначальному замыслу, Всемирная сеть должна была основываться на концепции пиринга, т.е. уже тогда предполагалось, что каждый пользователь сети должен являться активным автором и редактором, создающим и соединяющим информационные ресурсы для формирования взаимопереплетенной «паутины» ссылок.

Подлинная пиринговая технология дает небольшим командам разработчиков возможность с успехом конкурировать с гигантами бизнеса в области создания новых программных продуктов и компаний. Настоящая пиринговая технология, попадая на насыщенный рынок, производит взрывной эффект и по праву называется подрывной технологией.

По своей идее пиринговая сеть представляет собой объединение компьютеров, базирующиеся на полном равноправии всех участников, называемых пирами. От клиент-серверной архитектуры, основы постро-

ения Интернета, такие сети отличаются тем, что подобная организация способна сохранить работоспособность совершенно всей пиринговой сети при любом количестве доступных узлов (пиров), а также при любом их сочетании. То есть при работе с обычными сетями все зависит от пропускной способности самого сервера, а в случае пиринговых сетей такого существенного недостатка нет.

В основе технологии лежит принцип децентрализации: все узлы в сети P2P равноправны, что обеспечивает преимущества технологии P2P перед клиент-серверным подходом:

- отказоустойчивость при потере связи с несколькими узлами сети;
- увеличение скорости получения данных за счет копирования одновременно из нескольких источников;
- возможность разделения ресурсов без «привязки» к конкретным IP-адресам;
- огромная мощность сети в целом и др.

Сейчас на технологии P2P основано огромное число популярных сетевых сервисов – от простого обмена файлами до речевой и видеосвязи, можно производить распределенные вычисления, позволяющие задействовать удаленные компьютеры пользователей для выполнения сложной обработки данных.

В Интернете более половины всего трафика приходится на трафик файлообменных сетей, а размеры самых крупных из них перевалили за отметку в миллион одновременно работающих узлов, содержащих петабайты информации. Общее количество зарегистрированных участников сетей P2P во всем мире составляет порядка 100 млн.[1]

Сеть P2P – это множество узлов (компьютеров, смартфонов и пр.), объединенных в единую систему и взаимодействующих посредством собственного протокола, обеспечивающего возможность создания и функционирования сети равноправных узлов. Протоколом определяется логическая топология сети, механизм подключения к ней и отключения от нее узлов, алгоритм их взаимодействия, решение задач коррекции ошибок, регламентирование форматов сообщений, служебных запросов и откликов, маршрутизация в условиях постоянного подключения и отключения узлов. Протоколы P2P (в модели стека сетевых протоколов TCP/IP) относятся к прикладному уровню семиуровневой модели взаимодействия. Таким образом, P2P-сеть является наложенной (overlay), функционирующей поверх Интернета и использующей существующие транспортные протоколы.

Большой рост популярности сетей P2P обусловлен привлекательным набором сетевых характеристик данной технологии – это децентрализация, распределенность, самоорганизуемость сети, которые обеспечивают такие преимущества, как простота и дешевизна реализации и поддержа-

ния работы сети, ее отказоустойчивость и масштабируемость, увеличение скорости копирования и колоссальная мощность сети в целом. Каждый новый узел увеличивает потенциальную производительность и пропускную способность сети. Рассредоточение ресурсов, произошедшее благодаря возникновению пиринговых сетей, привело к фактическому исчезновению затрат, связанных с поддержанием гигантской централизованной инфраструктуры.

Помимо чистых P2P-сетей, существуют так называемые гибридные сети, в которых есть серверы, используемые для координации работы, поиска или предоставления информации о существующих машинах сети и их статусе (on-line, off-line и т.д.). Гибридные сети сочетают скорость централизованных сетей и надежность децентрализованных благодаря гибридным схемам с независимыми индексационными серверами, синхронизирующими информацию между собой. При выходе из строя одного или нескольких серверов сеть продолжает функционировать. К частично децентрализованным файлообменным сетям относятся например EDonkey, BitTorrent.

Использование распределенных систем имеет не только плюсы, но и минусы, связанные с особенностями обеспечения безопасности. Получить контроль над столь разветвленной и большой структурой, или использовать пробелы в реализации протоколов для собственных нужд – желанная цель для злоумышленников. Защитить распределенную структуру гораздо сложнее, чем централизованный сервер. Столь огромное количество ресурсов тяжело шифровать/дешифровать, поэтому большая часть информации об IP-адресах и ресурсах участников хранится и пересылается в незашифрованном виде. При перехвате злоумышленник не только получает собственно информацию, но также узнает и об узлах, на которых она хранится. Другая проблема – возможность подделки ID серверов и узлов. При отсутствии механизма проверки подлинности пересылаемых служебных сообщений существует возможность фальсификации сервера или узла, что приведет к компрометации всей сети или ее части.

Несмотря на широкие возможности, которые дает использование p2p-технологии, файлообменные сети служат в основном для распространения и получения нелицензионного контента. Здесь и возникает основная коллизия между правообладателями и интернет-пользователями. По отчету немецкой компании Ipoque, доля интернет-трафика, приходящегося на p2p сети, составляет от 49% на Ближнем Востоке и до 84% в Восточной Европе. По мере распространения широкополосного Интернета количество пользователей файлообменных сетей быстро увеличивается. Сайт torrents.ru вошел в пятерку крупнейших трекеров мира, собрав более миллиона зарегистрированных пользователей [2].

Правообладатели ни на секунду не прекращают борьбу с p2p-сетями

и даже добиваются локальных успехов. Пресечь распространение файла в децентрализованной пиринговой сети технически невозможно – для этого потребуется физически отключить от сети все машины, на которых лежит этот файл, а таких машин может быть очень и очень много – в зависимости от популярности файла их число может достигать сотен тысяч. Во всех развитых странах, с каждым годом ужесточается законодательство в области защиты авторских и смежных прав. Сейчас под действие антипиратских законов в США, Германии, России и некоторых других странах попадают как владельцы серверов, обеспечивающих работу p2p-сетей, так и сами пользователи, скачивающие и раздающие пиратский контент.

Такие организации, как RIAA, дискредитируют пиринговые сети, публикуя в них фальшивые файлы (содержание которых не соответствует названию, часто носит провокационный и порнографический характер). Это привело к потере популярности сети KaZaA в пользу eDonkey, имеющей более совершенную архитектуру [3].

Несмотря на то, что прекратил работу самый популярный сервер сети eD2k – Razorback, и была прекращена разработка коммерческого клиента EDonkey2000, сама сеть ED2K продолжает функционировать, т.к. не завязана на конкретные серверы и существует большое количество свободно распространяемых клиентских программ типа eMule и mlDonkey [3].

Несколько лет RIAA и другие организации безуспешно пытаются закрыть крупнейший мировой трекер The Pirate Bay. Удалось закрыть нескольких крупных серверов сети ED2k, один из крупнейших мировых BitTorrent трекеров – Demonoid.com, а также удалить из раздачи контент, права на который принадлежали компании 1С, с нескольких российских BitTorrent трекеров.

Ни в Российской Федерации, ни в Республике Беларусь нет ни одного прецедента, связанного с распространением информации в p2p сетях. Такие решения есть в США и Великобритании, однако, их количество – это капля в море по сравнению с реальными масштабами p2p сетей. Министерство юстиции Франции в январе 2007 г. обеспечило рекомендацией французские судебные власти, касающейся фактов незаконного распространения файлов, находящихся под защитой авторского права, отмечая, что подобные деяния должны преследоваться по закону и наказываться [4].

Отечественные правообладатели пока недостаточно активно борются с пиратством в p2p сетях, что связано с тем, что они сравнительно недавно осознали эту проблему. Возможно, им не хватало законодательной базы. Но если крупные российские компании расценят это как угрозу или помеху своему бизнесу, то, стоит ожидать более активных действий. Борьба с p2p-сетями найдет полную поддержку со стороны крупных провайдеров. Для них p2p-сети превратились в реальную проблему, так как

их инфраструктура может просто не справиться с возрастающим объемом исходящего интернет-трафика, который генерируют такие сети.

В борьбе с правообладателями и пользователи, и хозяева p2p-сетей будут предпринимать ответные шаги. Хостинг будет переноситься в страны, где антипиратские законы менее суровы и где установить владельца такого виртуального сервера очень сложно. Пользователи будут шифровать трафик, использовать прокси, анонимайзеры, VPN-туннели, шифровать содержимое своих жестких дисков.

В мире существует несколько «островков свободы» – стран, власти которых спокойно относятся к нарушениям авторских прав на цифровой контент. В Европе это, прежде всего, Франция и Швеция. В Швеции обмен файлами властями вообще никак не преследуется и не контролируется. До недавнего времени фильмы, музыка и программное обеспечение свободно скачивались из Сети всеми желающими. В прошлом году после критики со стороны Голливуда и давления со стороны ВТО загрузка фильмов и музыки, защищенных авторским правом, была поставлена вне закона, но только формально. Relakks – первая подобная коммерческая сеть в мире. Компьютеру каждого пользователя присваивается новый IP-адрес. В системе Relakks все компьютеры имеют шведские IP-адреса, независимо от их фактического местонахождения в мире. Пользователи могут обмениваться файлами, музыкой и фильмами. При этом никакая слежка за онлайновой активностью пользователя не дает возможности установить его настоящее географическое местоположение. Пользование службой стоит 5 евро в месяц [2].

Конечно, существуют основанные на тех же принципах некоммерческие сети, как правило, в рамках определенного рода интернет-сообществ. Их родоначальниками стали хакеры, им же принадлежит и большинство современных закрытых пиринговых сетей, где они по безопасным соединениям обмениваются информацией или специфическим ПО. Похожие инструменты сокрытия личности используются сетевыми диссидентами в Китае, чтобы избежать преследования за свои действия в интернете. В абсолютном большинстве случаев подобные службы открываются для пользователя только по приглашению, а их потенциальный член перед получением полного доступа должен выложить в Сеть собственный контент, чтобы доказать свое право на членство.

Для безопасного пользования p2p-сетью будет необходима такая сумма специальных знаний, которой большинство людей сейчас не обладают – эти меры сопротивления задают высокий образовательный и технический барьер для пользователей p2p-сетями, что резко сократит количество желающих пользоваться p2p-сетями. К тому же, если владельцы контента предложат простые и удобные способы онлайн-продаж своей продукции, то у них есть хорошие шансы победить в войне за потреби-

теля. Один любопытный пример «новых технологий» распространения цифрового контента. Группа Residents сказала новое слово в звукозаписи. Их новое творение, радиопостановка под названием River of Crime, распространяется при помощи двух чистых болванок CD-R. Покупатель должен сам скачать аудиофайлы из Сети и записать их на болванки.

Есть еще один вариант продолжения неподконтрольного обмена данными. В случае исчезновения любых p2p сетей в Интернет их вполне может заменить офлайновая одноранговая сеть Dead Drops. Первая такая сеть появилась в Нью-Йорке и представляет собой флешкарту или переносной ЖД замурованный в стену. Любой желающий может подойти со своим ноутбуком и скачать, закачать все что угодно. Такие сети могут появится и у нас, вот только с нашими вандалами флешки часто придется новые замуровывать. Сейчас уже насчитывает 761 стена с торчащими USB, общим объемом в 2,3 Тб. [4].

Библиографический список

1. URL: http://wiki.shtorm.net/wiki.
2. Война в сети: корпорации против пользователей. URL: http://torrentblog.ru/vojna-v-seti-korporacii-protiv-polzovatelej.
3. Козик А.Л., Березовский К.А. Влияние возникновения и развития сетей P2P на международное право // Евразийский юридический журнал. 2009. № 2. С. 88-92.
4. URL: http://horde.me/KhRvs/chto-budet-esli-ischeznut-p2p-seti.html.