Лекция 12

1. Анонимные сети

Анонимные сети

Первой успешной анонимной сетью был коммерческий сервис Freedom, существовавший в период с 1998 до 2001 года. Компанией ZKS были установлены выделенные серверы, с которыми клиенты «общались» посредством криптографического протокола. Узел, на который приходили пакеты от пользователя Freedom, не мог идентифицировать настоящего отправителя. Сама сеть функционировала на уровне протокола IP.

В последствии было разработано множество различных анонимных сетей с разной степенью защищенности и разной функциональностью, которые условно можно разделить на две большие группы: децентрализованные и гибридные анонимные сети.

Анонимные сети

- Freenet
- Invisible Internet Project (I2P)
- Java Anon Proxy (JAP)
- ANts P2P
- BitBlinder
- Filetopia
- GNUnet
- Gnutella, Gnutella2
- Manolito
- MUTE
- Netsukuku
- RShare
- Turtle
- WASTE
- Psiphon
- The Onion Router (TOR)
- Virtual Private Network
- Skype

Freenet

Freenet работает на основе объединения в общий фонд (пулинга) предоставленной пользователями (членами сети) своей полосы пропускания и дискового пространства своих компьютеров для публикации или получения из Freenet разного рода информации.

Freenet использует разновидность маршрутизации по ключам, похожей на распределённую хеш-таблицу, для определения местонахождения пользовательских данных

В настоящее время Freenet не может быть использован для создания или распространения динамического контента, такого, который использует базы данных или скрипты.

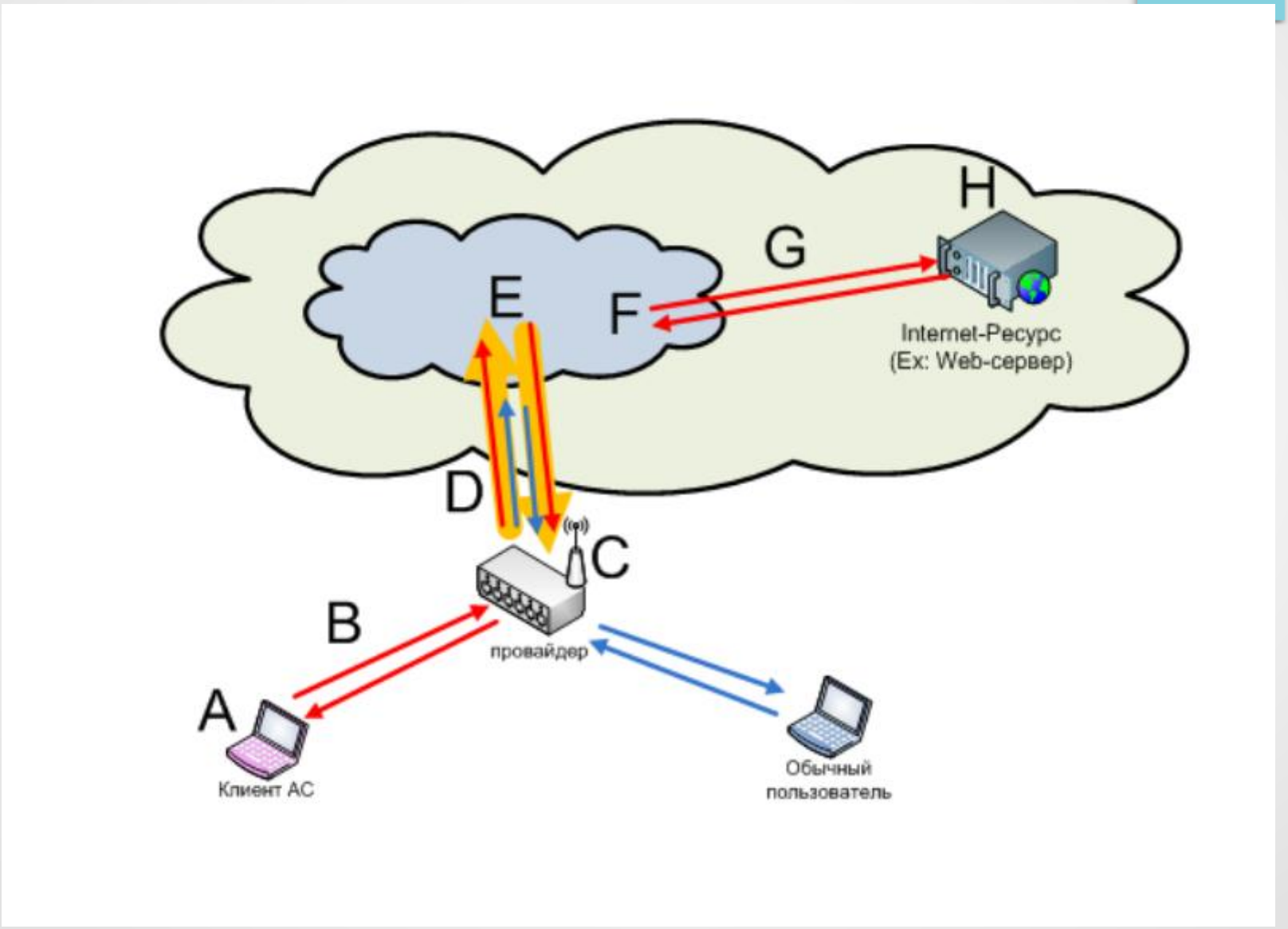
Freenet может рассматриваться как огромное, потенциально ненадёжное устройство хранения информации. Когда пользователь сохраняет файл в это устройство, то он получает ключ, с помощью которого можно получить доступ к хранящейся информации. Это устройство хранения данных распределено по всем узлам, подключенным к Freenet.

Сеть разработана для того, чтобы сохранять высокую живучесть при полной анонимности и децентрализации всех внутренних процессов по всей сети.

Система не имеет центральных серверов и не находится под контролем каких-либо персон или организаций. Даже создатели Freenet не имеют никакого контроля над всей системой.

В разработке находится версия проекта Freenet, реализующей механизм «onion routing» (onion routing – технология анонимной коммуникации по компьютерной сети. В рамках данной технологии сообщения неоднократно шифруются и затем передаются через несколько узлов сети, названных “луковыми” маршрутизаторами), а значит – потенциально сопоставимой по функциональности с сетью Tor.

Схема организации и построения анонимных вычислительных сетей



Skype

Бесплатные возможности

- Видеочат и конференции;
- Прием и отправка файлов;
- Мгновенный обмен сообщениями;
- Голосовые звонки на Skype-клиенты;
- Перенаправление звонов другим Skype-клиентам;

Платные услуги

- Отправка SMS;
- Голосовой e-mail;
- Прием входящих звонков с обычных телефонов;
- Совершение исходящих звонов на обычные телефоны.

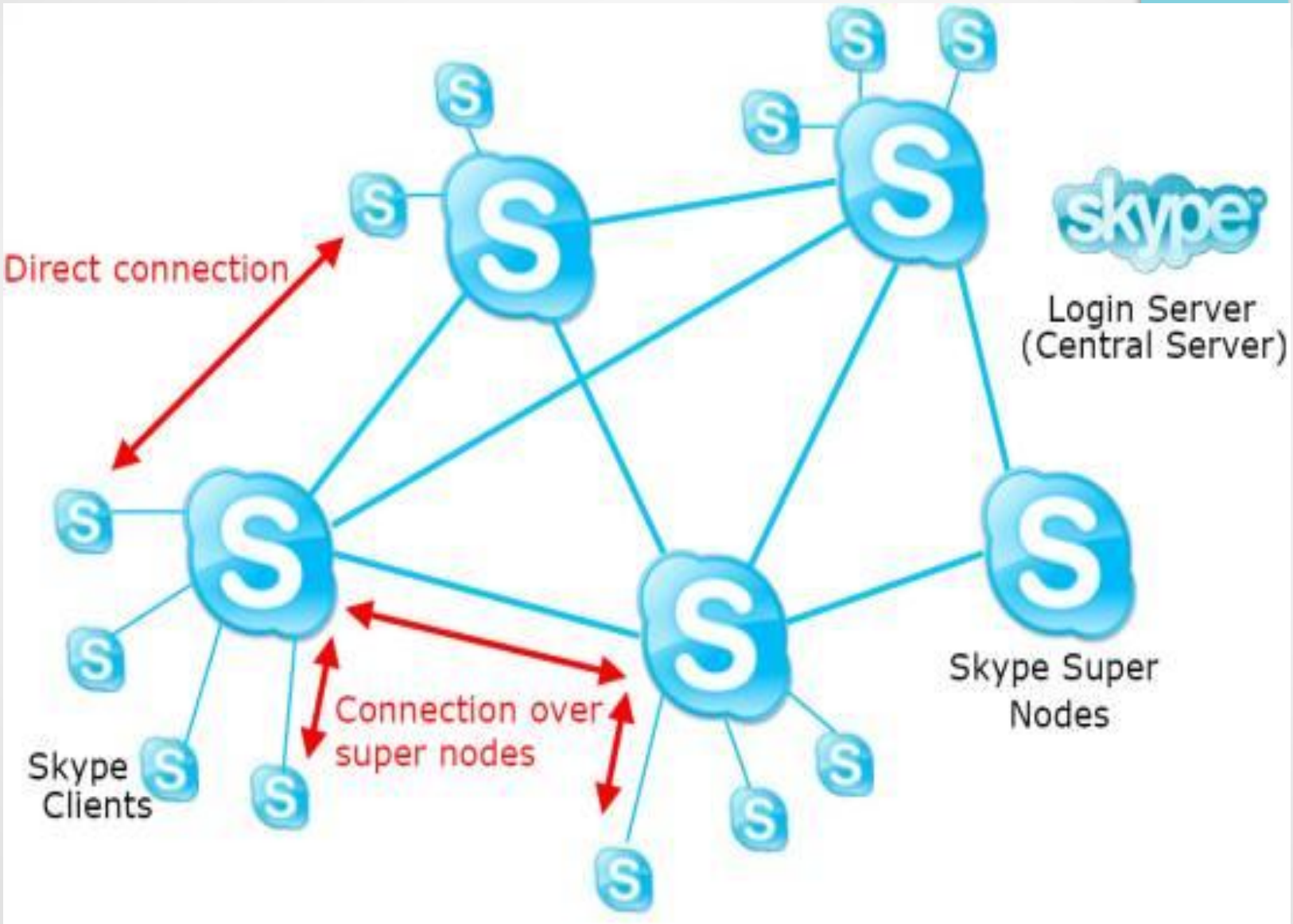
Skype

На атомарном уровне **структура skype-сети состоит из обычных узлов (normal/ordinal node/host/nest), обычно обозначаемых аббревиатурой SC, расшифровываемой как Skype Client,** и super-узлов (super node/host/nest), которым соответствует аббревиатура SN.

Любой узел, имеющий публичный IP-адрес (т.е. тот, который маршрутизируется в Интернет) и обладающий достаточно широким каналом, **автоматически становится super-узлом** и передает через себя трафик обычных узлов, помогая им преодолеть защиты типа брандмауэров или трансляторов сетевых адресов (NAT) и равномерно распределяя нагрузку между хостами.

В этом и состоит сущность самоорганизующейся распределенной децентрализованной пиринговой сети, **единственным централизованным элементом которой является Skype-login** сервер, отвечающий за процедуру авторизации Skype-клиентов и гарантирующий уникальность "позывных" для всей распределенной сети.

Skype


Direct connection
Login Server
(Central Server)
Skype Super
Nodes
Connection over
super nodes
Skype
Clients

Skype

Связь между узлами осуществляется не напрямую, а через цепочку super-узлов. "Серверов" в общепринятом смысле этого слова в Skype-сети нет и **любой узел с установленным Skype-клиентом является потенциальным сервером**, которым он автоматически становится при наличии достаточных системных ресурсов (объема оперативной памяти, быстродействия процессора и пропускной способности сетевого канала, не защищенного никакими средствами защиты).

Каждый узел Skype-сети хранит перечень IP-адресов и портов известным ему super-узлов в динамически обновляемых кэш-таблицах (Host Cache Tables, HC-tables). Начиная с версии Skype 1.0, кэш-таблицы представляют собой простой XML-файл, в незашифрованном виде записанный на диске в домашней директории пользователя.

Протокол обмена между Skype-клиентами совершенно недокументирован и поэтому информация с его описанием отсутствует. Поскольку существует огромное множество версий Skype-клиентов, существенно отличающихся между собой, то **любое создаваемое описание протокола может содержать неточности.**

Skype

Сразу же после своего запуска Skype-клиент открывает TCP и UDP порты, номера которых случайным образом задаются при инсталляции и могут быть в любой момент изменены через диалог конфигурации, что затрудняет блокирование Skype-трафика на брандмауэре. Помимо этого, Skype открывает 80 (HTTP) и 443 (HTTP-over-TLS) порты.

Skype шифрует трафик, активно используя технологии "обфускации" (от англ. obfuscation - буквально: запутывание), препятствующие выделению постоянных сигнатур в полях заголовков.

Алгоритмы шифрования меняются от версии к версии, плюс к тому же выпущено множество специальных версий для разных стран мира, чьи законы налагают определенные ограничения на длину ключа или выбранные криптографические алгоритмы

The Onion Router (TOR)

TOR — наиболее известная и развитая среди существующих анонимных сетей, несмотря на раннюю стадию разработки.

Сеть не является полностью децентрализованной — существуют 3 центральных сервера каталогов, хранящие подписанный актуальный список узлов сети Tor с их реальными адресами и отпечатками открытых ключей.

Клиент формирует цепочку из трёх произвольно выбранных узлов сети Tor. Среди них есть входной (entry node) по отношению к клиенту узел и выходной (exit node). Сеть Tor при этом функционирует как шлюз между клиентом и внешней сетью.

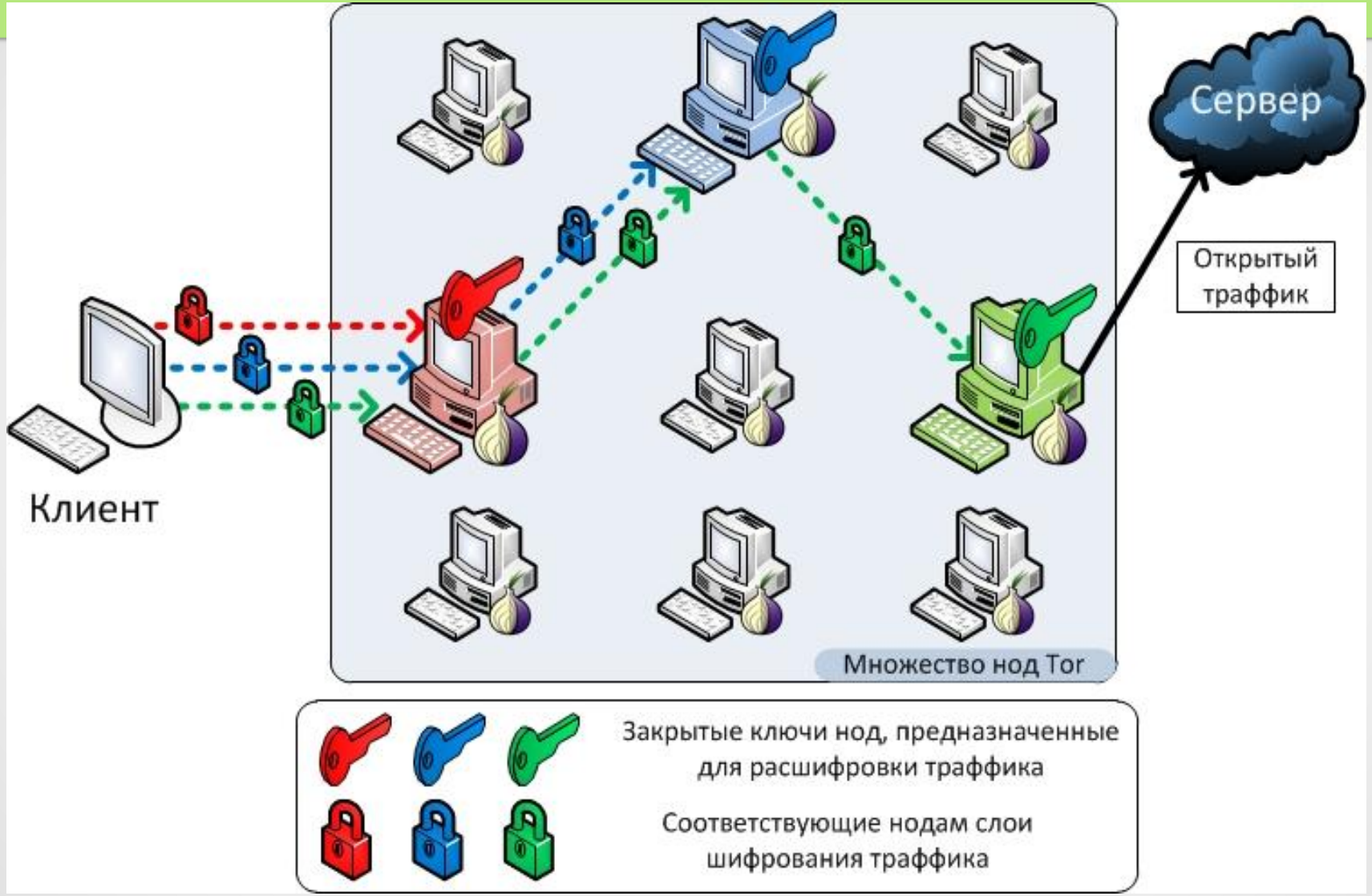
The Onion Router (TOR)

Луковая маршрутизация — это технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции, и отослать сообщения на следующий маршрутизатор, где все повторится. Таким образом промежуточные узлы не знают источник, пункт назначения и содержание сообщения.

The Onion Router (TOR)

С **каждым пересылаемым пакетом,** включая саму команду открытия туннеля, **ассоциируется симметричный ключ шифрования и идентификатор следующего узла туннеля. Эти данные зашифровываются последовательно открытыми ключами всех выбранных серверов, начиная с последнего, образовывая структуры, называемые «луковицами» (onions).** Для межсерверных коммуникаций используется TLS. Образованные цепочки **каждые 10 минут перестраиваются** таким образом, что через каждый узел сети проходит ограниченный объём данных от каждого клиента. Для каждой вновь образованной цепочки серверов **генерируется новый сеансовый ключ**, а для противодействия атакам анализа трафика блок данных имеет постоянный размер в 512

The Onion Router (TOR)



The Onion Router (TOR)

Просмотр и модификация сообщения

На последнем узле цепочки Tor исходное сообщение от клиента окончательно расшифровывается для передачи его серверу в первоначальном виде. Соответственно:

Первый узел цепочки знает настоящий адрес клиента;

Последний узел цепочки видит исходное сообщение от клиента, хотя и не знает истинного отправителя;

Сервер-адресат видит исходное сообщение от клиента, хотя и не знает истинного отправителя;

The Onion Router (TOR)

Раскрытие отправителя

При работе с сетью Tor к сообщениям пользователя может добавляться техническая информация, полностью либо частично раскрывающая отправителя.

Техническая информация о прохождении пакетов, их адресатах и получателях может оставляться некорректно настроенными, либо злоумышленными узлами сети Tor;

Техническая информация об адресе сервера-получателя может выдаваться клиентом путем DNS-запросов к своему DNS-серверу, легко перехватываемых провайдером. Решением этой проблемы будет настройка разрешения имен через сеть Tor, либо блокирование файрволом доступа Tor к DNS путем запрета исходящих соединений на удаленный порт 53 или использование сторонних DNS-серверов, таких как OpenDNS или TorDNS;

Сервером может запрашиваться, а клиентом выдаваться техническая информация об адресе клиента и конфигурации его операционной системы и браузера. Запрос может идти как через исполнение в браузере сценариев языка JavaScript и Java, так и другими способами. Эта проблема может быть решена отключением в браузере соответствующих сценариев и языков, а также использованием фильтрующих прокси-серверов, таких как Polipo, Privoxy и Proxomitron.

Invisible Internet Project (I2P)

«Проект Невидимый Интернет» — это анонимная одноранговая распределённая коммуникационная среда, с которой могут работать как любые традиционные сетевые службы и протоколы, такие как E-Mail, IRC, HTTP, Telnet, так и распределённые приложения, вроде баз данных, Squid и DNS.

До мая 2009 года авторы проекта всеми силами удерживали пользователей от активной рекламы I2P сети, указывая на возможную нестабильность и beta-статус разработки.

Названия сайтов в сети I2P имеют вид: «http://название_сайта.i2p» Внутри сети I2P работает собственный каталог сайтов, электронные библиотеки, а также торрент-трекеры.

Сеть I2P схожа по своей структуре с традиционным Интернетом и отличается лишь невозможностью цензуры благодаря использованию механизмов шифрования и анонимизации.

В I2P сети нет никаких центральных серверов и нет привычных DNS-серверов, также сеть абсолютно не зависит от внешних DNS, что приводит к невозможности уничтожения, блокирования и фильтрации сети, которая будет существовать и функционировать, пока в сети останутся хотя бы два компьютера.

В качестве механизма распределения имен в сети I2P, используется модифицированный DHT Kademlia.

Сеть предоставляет приложениям простой транспортный механизм для анонимной и защищённой пересылки сообщений друг другу. В сети реализован дейтаграммный метод передачи пакетов, при котором каждый пакет может передаваться независимо по отдельному маршруту.

Сеть I2P в первую очередь преследует цель анонимного доступа к внутренним ресурсам I2P. Внутренние ресурсы сети I2P, идентифицируемые доменным суффиксом i2p, предоставляют сервисы анонимных блогов («Syndie»), анонимного доступа в сеть IRC («ircProxy»), анонимной электронной почты («Susimail»), передачи файлов, групп новостей, шлюзы сетей Freenet и Mnet. Существуют и выходные узлы для анонимного веб-сёрфинга посредством анонимного HTTP-прокси, «eepProxy».

Invisible Internet Project (I2P)

Сеть изначально была спроектирована таким образом, что все промежуточные узлы являются скомпрометированными или попросту злонамеренными (принадлежащие злоумышленнику и собирающие проходящую через них информацию), поэтому для противодействия был введен ряд активных мер.

Весь трафик в сети шифруется от отправителя до получателя. В сумме при пересылке сообщения используется четыре уровня шифрования, перед шифрованием в каждый сетевой пакет автоматически добавляется небольшое случайное количество случайных байт, чтобы еще больше обезличить передаваемую информацию и затруднить попытки анализа содержимого и блокировки передаваемых сетевых пакетов. В качестве адресов сети используются криптографические идентификаторы, представляющие собой открытые криптографические ключи, которые не имеют абсолютно никакой логической связи с реальным компьютером. IP адреса в сети I2P не используются, поэтому определить истинный адрес какого либо узла в сети затруднительно.

Invisible Internet Project (I2P)

Каждое сетевое приложение на компьютере строит для себя отдельные шифрованные, анонимные туннели. Все передаваемые сетевые пакеты имеют свойство расходиться по нескольким разным туннелям, что делает бессмысленным попытки прослушать и проанализировать с помощью сниффера проходящий поток данных. Также происходит периодическая смена уже созданных туннелей на новые, с новыми цифровыми подписями и ключами шифрования.

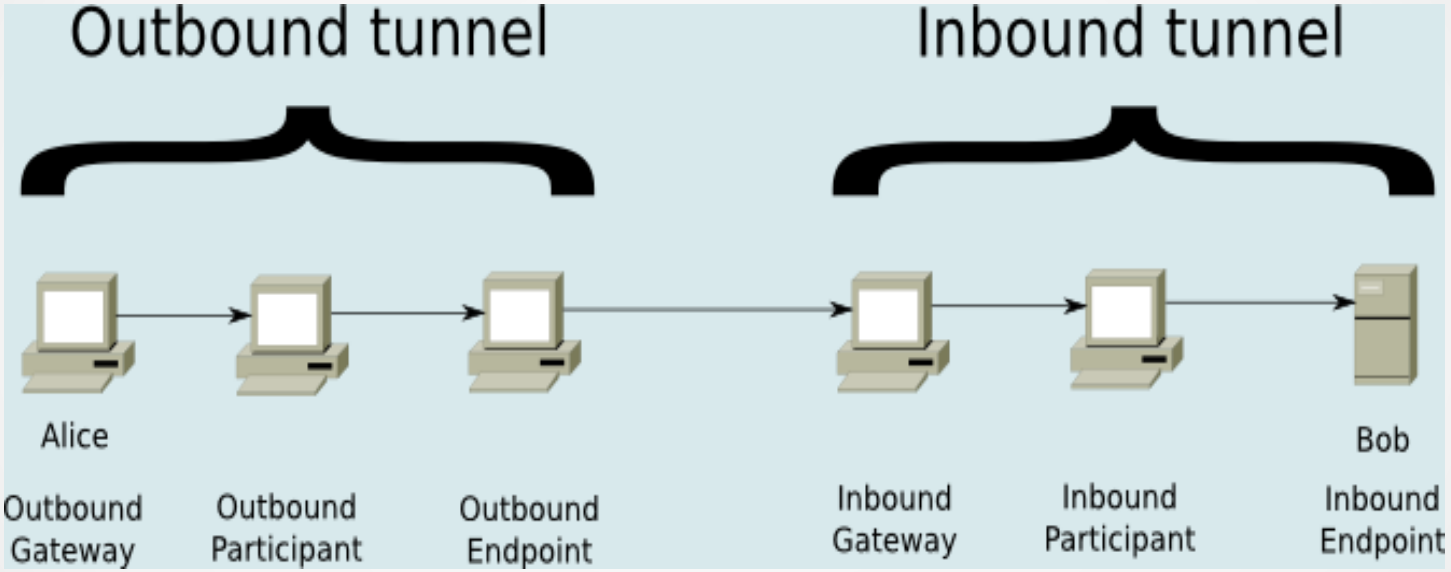
В сети I2P все пакеты зашифровываются на стороне отправителя и расшифровываются только на стороне получателя, при этом, никто из промежуточных участников обмена не имеет возможности перехватить расшифрованные данные и никто из участников не знает, кто на самом деле отправитель и кто получатель. В сети I2P используется, так называемая, "Чесночная маршрутизация" и "Чесночное шифрование".

Invisible Internet Project (I2P)

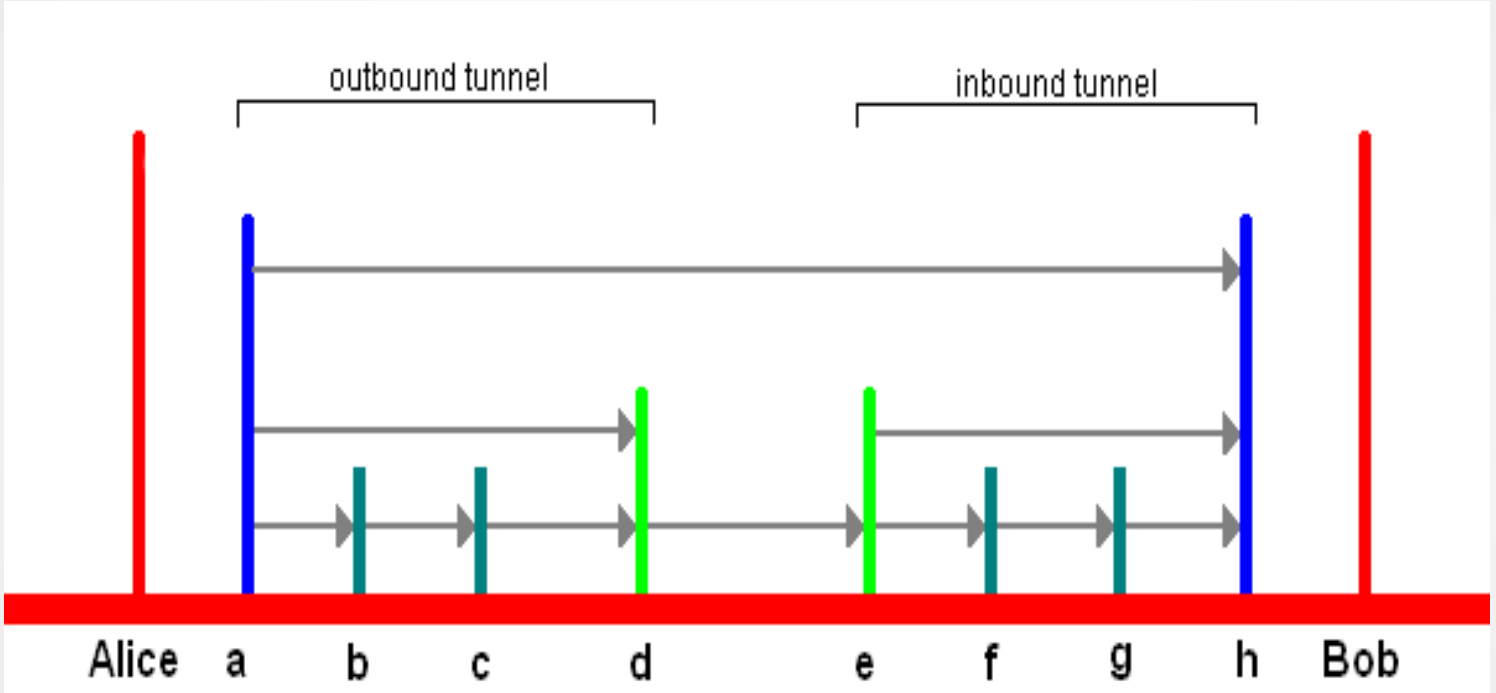
Kademlia — это реализация распределённой хеш-таблицы для одноранговых компьютерных сетей, разработанная Петром Маймунковым и Давидом Мазьером (David Mazières). Узлы сети, работающей по протоколу Kademlia, общаются между собой по протоколу транспортного уровня UDP. Узлы Kademlia хранят данные посредством распределённых хеш-таблиц (DHT). В итоге над существующей LAN/WAN (как интернет) создаётся новая виртуальная или оверлейная сеть, в которой каждый узел обозначается специальным номером («Node ID»).

“Чесночная” технология, используя многослойное шифрование, позволяет единственному сообщению (так называемому "чесноку") содержать в себе множество «зубчиков» — полностью сформированных сообщений рядом с инструкциями для их доставки. В один "чеснок" в момент его формирования перед отправкой закладываются множество "зубчиков", являющихся зашифрованными сообщениями как нашего узла, так и чужими - транзитными. Чесночная технология применяется когда нужно отправить зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации.

Invisible Internet Project (I2P)



Invisible Internet Project (I2P)



		tunnel encryption (private key AES)	a to d, e to h
garlic encryption (ElGamal/SessionTag+AES)	a to h	transport encryption (DH/STS+AES, etc)	a to b, b to c, c to d, d to e, e to f, f to g, g to h

Invisible Internet Project (I2P)

Технологическими особенностями I2P являются **дейтаграммный метод передачи пакетов**, при котором каждый пакет может передаваться независимо по отдельному маршруту, основанный на протоколе Secure Semireliable UDP (SSU) (со своими функциями аутентификации, управления потоком и пр.), и протокол NTCP и возможность поверх них стоить I2PTunnel, обеспечивающий передачу TCP-пакетов по сети I2P