ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Том 22
2016
№ 4

ТЕОРЕТИЧЕСКИЙ И ПРИКЛАДНОЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с ноября 1995 г.

УЧРЕДИТЕЛЬ
Издательство “Новые технологии”

СОДЕРЖАНИЕ

Информация о журнале доступна по сети Internet по адресу **http://novtex.ru/IT.**
Журнал включен в систему Российского индекса научного цитирования.
Журнал входит в Перечень научных журналов, в которых по рекомендации ВАК РФ должны быть опубликованы научные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

INFORMATION TECHNOLOGIES
INFORMACIONNYE TEHNOLOGII

Vol. 22
2016
No. 4

THEORETICAL AND APPLIED SCIENTIFIC AND TECHNICAL JOURNAL

Published since November 1995

ISSN 1684-6400

CONTENTS

Complete Internet version of the journal at site: **http://novtex.ru/IT.**
According to the decision of the Higher Certifying Commission of the Ministry of Education of Russian Federation, the journal is inscribed in "The List of the Leading Scientific Journals and Editions wherein Main Scientific Results of Theses for Doctor's or Candidate's Degrees Should Be Published"

УДК 004.7

С. М. Авдошин, канд. техн. наук, проф., руководитель департамента программной инженерии факультета компьютерных наук НИУ ВШЭ, savdoshin@hse.ru,
А. В. Лазаренко, студент, avlazarenko@edu.hse.ru
Национальный исследовательский университет "Высшая школа экономики" (НИУ ВШЭ)

Технология анонимных сетей

Представлен обзор использующихся в настоящее время анонимных сетей, построенных на основе технологии луковой маршрутизации и пиринговых сетей. Описаны ключевые особенности сетей, приведена их сравнительная характеристика.

Ключевые слова: *анонимные сети, луковая маршрутизация, невидимый Интернет, оверлейные сети, пиринговые сети, слоистое шифрование*

Введение

На сегодняшний день количество контента в сети Интернет растет в объеме и сложности за счет блогов, видео, музыки, персонализированных вебстраничек и программ. Веб 2.0 обеспечил людей такими технологиями, как вики, подкасты, новостные ленты, социальные сети, хостинг-сервисы и поисковые системы. До тех пор пока пользователи создают контент в открытых источниках, любого автора можно отследить, установить личность создателя, среагировать вовремя на передачу планов о совершении вооруженного нападения или минировании аэропорта. Но что если человек хочет скрыть свое авторство, передать незаметно для спецслужб какие-либо цифровые файлы и свести к минимуму свой след в глобальной сети?

В таком случае на арену выходят анонимные сети. Они позволяют анонимизировать Интернет-коммуникации, сделать сложной возможность связать участников взаимодействия (например, пользователя и веб-сервер, который он посетил).

Совершенно понятно, зачем такие сети нужны злоумышленникам, но зачем они нужны обычным людям? Наиболее очевидная причина использования инструментов для анонимизации в сети — предотвращение возможности слежки рекламными компаниями за пользователями в сети, получение доступа к заблокированным сетевым ресурсам. Правительства используют анонимные сети для разведки и слежки, а люди в странах, лишенных свободы слова, используют их для общения друг с другом.

Актуальность исследования анонимных сетей вызвана необходимостью разработки методов деанонимизации и атак на такие сети, поскольку эти сети широко используют террористы и продавцы нелегальных товаров. Правительства различных стран используют как технические механизмы противодействия анонимности сетей, финансируя программы по кибербезопасности, так и юридические, например, ФСБ РФ готовит закон против анонимности в Интернете [1, 2].

Ниже приведены используемые в работе термины и сокращения:

AES (*Advanced Encryption Standard*) — алгоритм блокового шифрования с симметрическим ключом.

API (*Application Programming Interface*) — программное обеспечение, предоставляющее условия для взаимодействия между другими программами.

BGP (*Border Gateway Protocol*) — динамический, дистанционно-векторный протокол маршрутизации.

Cjdns — сетевой протокол и его реализация, с помощью которого можно создать масштабируемую, безопасную и простую в настройке сеть.

DARPA (*Defense Advanced Research Projects Agency*) — агентство правительства США.

DNS (Domain Name System) — система доменных имен, представляющая распределенную компьютерную систему преобразования символьного имени в IP-адрес и наоборот.

F2F (*Friend-to-Friend*) — специфическая форма P2P сети, где пользователи могут осуществлять прямые соединения только с друзьями или пользователями, которым они доверяют.

I2P (*Invisible Internet Project*) — проект с открытым исходным кодом, пытающийся создать анонимную сеть для коммуникаций через Интернет.

ID — уникальный идентификатор.

IP (*Internet Protocol*) — коммуникационный протокол цифровых форматов сообщений, использующийся при обмене сообщениями между компьютерами в одной сети или серией соединенных сетей, использующих протокол TCP/IP.

ISP (*Internet Service Provider*) — организация, предоставляющая клиентам доступ к Интернету.

OSPF (*Open Shortest PathFirst*) — основанный на ссылках маршрутизационный протокол, исполь-

зующий алгоритм Дейкстры для вычисления кратчайшего пути между известными устройствами.

P2P (*Peer-to-Peer*) — пиринговая сеть, состоящая из группы равноправных компьютеров, каждый из которых выполняет роль узла для распространения информации в группе.

PFS (*Perfect Forward Secrecy*) — совершенная прямая секретность. Свойство кодирования данных, удостоверяющее, что сессионные ключи не скомпрометированы при компрометации одного из долговременных ключей.

QSPN (*Quantum Shortest Path Netsukuku*) — маршрутизационный алгоритм сети Netsukuku.

SDK (*Software Development Kit*) — набор инструментов, использующийся для разработки приложений, предоставляемый поставщиками железа или программного обеспечения.

SOCKS — сетевой протокол, позволяющий пересылать пакеты от клиента к серверу через прокси-сервер прозрачно (незаметно для них) и таким образом использовать сервисы за межсетевыми экранами.

SSH (*Secure Shell*) — криптографический протокол и интерфейс для запуска сетевых сервисов и безопасных сетевых коммуникаций с удаленного компьютера.

TCP (*Transmission Control Protocol*) — протокол, который предоставляет коммуникационную безопасность между клиент-серверными приложениями, которые взаимодействуют друг с другом через Интернет.

TLS (*Transport Layer Security*) — криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет.

Tor (*The Onion Router*) — свободное программное обеспечение с открытым исходным кодом, позволяющее пользователям защитить свою приватность и безопасность в Интернете.

UDP (*User Datagram Protocol*) — часть протокола Интернета, использующаяся программами, запущенными на разных компьютерах в сети.

Беспроводная ячеистая сеть (*wireless mesh network*) — коммуникационная сеть, созданная из узлов, соединенных беспроводным способом, имеющая ячеистую топологию.

ЛМ — луковая маршрутизация.

ЛП — луковый прокси.

Микс — устройство для передачи и хранения, принимающее какое-то количество сообщений фиксированной длины от нескольких источников, совершающее криптографическую трансформацию сообщений и затем передающее сообщение к следующему пункту назначения в случайном порядке.

Оверлейная сеть (*Overlay Network*) — общий случай логической сети, создаваемой поверх другой сети.

Проверка целостности (*Integrity Checking*) — проверка программ на прочность программного продукта на каждой фазе разработки.

Публичная сеть — тип сети, в которой любой пользователь имеет доступ и возможность соединения с другими сетями в Интернете.

Служба каталогов (*Directory Service*) — программные системы, которые хранят, организуют и предоставляют доступ к информационным директориям в порядке объединения ресурсов сети.

ЧМ — чесночная маршрутизация.

Эфемерный ключ — такой ключ, который создан специально для выполнения только одного распределения ключей.

Ячеистая топология (*Mesh Topology*) — сетевая топология компьютерной сети на принципе ячеек, в которой каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети с возможным принятием на себя функций коммутатора для других рабочих станций.

1. Луковая маршрутизация

Так называемая луковая маршрутизация (далее — ЛМ) была разработана в середине 1990-х годов в *U.S. Naval Research Laboratory* для защиты коммуникаций в сети разведки США [3]. Впоследствии дорабатывалась компанией *Advanced Research Projects Agency*, запатентована флотом в 1998 году [4].

ЛМ является инфраструктурой общего назначения для приватных коммуникаций в публичной сети. ЛМ имеет интерфейсы для стороннего программного обеспечения через специализированный прокси, что позволяет без проблем интегрировать ее с существующими системами. Первые прототипы использовали с июля 1997 года.

ЛМ работает через динамическое построение анонимных соединений, с помощью миксов Чаума [5] в реальном времени. Сеть ЛМ из луковых маршрутизаторов является распределенной и контролируемой несколькими административными доменами, так что никакой единичный луковый маршрутизатор не может разрушить всю сеть или скомпрометировать приватность пользователя.

Анонимные соединения ЛМ являются протокол-независимыми и существуют в трех фазах: установка соединения, продвижение данных, закрытие соединения. Установка начинается, когда инициатор создает так называемую луковицу, определяющую путь соединения через сеть. Под луковицей понимается рекурсивная слоистая структура данных, специфицирующая свойства соединения в каждой точке, т. е. она осуществляет криптографический контроль информации. Каждый луковый маршрутизатор на протяжении маршрута использует свой публичный ключ для дешифровки всей луковицы, которую он получает. Данная операция позволяет выявить следующий луковый маршрутизатор и встроенную луковицу. Луковый маршрутизатор подгоняет встроенную луковицу для соответствия фиксированному размеру и посылает ее в следующий луковый маршрутизатор. После установки соединения данные можно посылать в обоих направлениях. Данные от инициатора каждый раз повторно шифруются с использованием алгоритмов и ключей, установленных в луковице. Во время движения данных через анонимное соединение каждый

луковый маршрутизатор убирает один слой шифрования, заданный криптографическим контролем информации в луковице, установившей дорогу, так что данные адресат получает уже простым текстом.

Вся информация (луковицы, данные, сетевой контроль) посылается через сеть порциями одинакового размера. Все ячейки пребывают в луковый маршрутизатор через фиксированные интервалы времени и смешиваются вместе. Луковица и ячейки с данными на разных участках сети имеют различный вид вследствие слоистого шифрования.

Временные и емкостные характеристики развертывания ЛМ достаточно малы. Так, временная сложность установки соединения обычно составляет менее одной секунды. Вычислительно-дорогое шифрование с открытым ключом используется только для передачи симметричного секретного ключа, во время фазы установки соединения. Фаза продвижения данных использует только AES-шифрование с переданным ключом, что намного быстрее по сравнению с шифрованием с открытым ключом. Задержка данных определяется числом луковых маршрутизаторов на протяжении соединения и может различаться в зависимости от длины маршрута.

В работе [6] можно найти описание модели автомата для протокола луковой маршрутизации, в которой анонимность и несвязность являются гарантированными. Ресурс [7] является официальным сайтом луковой маршрутизации. Работа [8] описывает вероятностный анализ луковой маршрутизации в виде черного ящика.

2. Tor — луковая маршрутизация второго поколения

Tor была создана в центре высокопроизводительных вычислительных систем исследовательской лаборатории Военно-морских сил США в рамках проекта Free Haven совместно с DARPA по федеральному заказу. В 2002 г. эта разработка была рассекречена, исходные тексты переданы независимым разработчикам, создавшим клиент-серверное приложение и опубликовавшим его под свободной лицензией.

Проект поддерживает правозащитная организация *Electronic Frontier Foundation*, существенную финансовую помощь оказывают Министерство обороны и Государственный департамент США, Национальный научный фонд.

Система ЛМ второго поколения имеет множество преимуществ по сравнению с оригинальной версией: свойство совершенной прямой секретности; контроль перегрузки; серверы каталогов; проверка целостности; настраиваемые политики выхода и практичный дизайн для сервисов со скрытой локацией. Tor работает в глобальной сети Интернет, не требует специальных привилегий и модификаций ядра, требует совсем небольшой синхронизации между узлами и предлагает разумный компромисс между анонимностью, удобством использования и эффективностью [9].

Сеть Tor представляет собой группу волонтерских серверов. Пользователи Tor используют эту сеть через подключение к серии виртуальных туннелей, что позволяет делиться информацией через публичные сети без компрометирования приватности.

Посмотреть, кто и зачем использует Tor, можно на ресурсе [10]. Пользователи Tor являются той частью, которая делает его столь защищенным. Tor прячет пользователя между другими пользователями в сети. Таким образом, чем больше пользовательская база Tor, тем сильнее защищается их анонимность. На сегодняшний день число людей, ежемесячно использующих Tor, приблизилось к 2 млн, а число волонтерских серверов в сети ежедневно превышает 6000.

Сеть Tor является оверлейной. Каждый луковый маршрутизатор запускается как нормальный процесс на уровне пользователя, без каких-либо специальных привилегий. Каждый пользователь запускает локальное программное обеспечение, называемое луковым прокси (далее — ЛП), для получения директорий, установки цепи и обеспечения цепи соединений. Эти ЛП принимают TCP-потоки и размножают их через цепи. Луковый маршрутизатор на другой стороне цепи соединяется с запрошенной конечной точкой и передает данные.

Трафик проходит через соединения в сообщениях фиксированного размера. Каждое сообщение имеет длину 512 байт и состоит из заголовка и полезной информации. Заголовок содержит идентификатор цепи, специфицирующий принадлежность цепи (много цепей могут быть размноженными в одном TLS-соединении).

Оригинальная луковая маршрутизация строила одну цепь для каждого TCP-потока, однако в Tor каждая цепь может быть поделена между несколькими TCP-потоками.

Для создания приватного пути прохождения через сеть с помощью ЛМ пользовательское программное обеспечение или клиент последовательно строят цепи защищенных соединений через ретрансляторы в сети. Каждый ретранслятор на пути знает только то, какой ретранслятор отправил ему данные и какому ретранслятору он должен их передать. Никакой отдельный ретранслятор не знает полного пути, который проделывает пакет данных внутри сети.

Как только цепь устанавливается, пользователь получает возможность анонимно пользоваться Интернетом и просматривать скрытые службы Tor. Tor работает только для TCP-потока и может быть использован любым приложением с поддержкой сетевого протокола SOCKS.

В работе [11] приведен обзор скрытых служб сети Tor, недоступных в обычном Интернете (такие порталы имеют доменную зону .onion и называются Tor hidden services). Ресурс [12] содержит различные метрики, относящиеся к Tor. Ресурс [13] описывает анализ трафика внутри сети Tor и типичное поведение пользователей. Работа [14] содержит аналитическое исследование скрытых служб Tor в Интернете.

3. Пиринговые (P2P) анонимные сети

Под пиринговой (P2P) сетью понимается одноранговая сеть, состоящая из группы равноправных компьютеров. В такой сети каждый компьютер может выступать клиентом, сервером или узлом для распространения информации в группе. Сети P2P разделяют на централизованные и децентрализованные. В свою очередь, децентрализованные сети делят на структурированные, неструктурированные и гибридные [15]. Пиринговые анонимные сети, которые мы рассматриваем далее в этом разделе, являются децентрализованными и гибридными. Различают три поколения пиринговых сетей [16].

Tarzan — отказоустойчивая, масштабируемая и легкоуправляемая сеть, представляющая собой пиринговый анонимизирующий оверлей [17]. Инициатор сообщения выбирает путь для пакетно-ориентированной маршрутизации через псевдослучайно выбранные узлы ограниченной топологии, таким образом Tarzan предоставляет анонимность как клиенту, так и серверу.

Узлы сети Tarzan коммуницируют через последовательности ретрансляторов, выбранных из пула узлов-волонтеров. Разработчики предоставили технологию для открытия и выбора других узлов в качестве коммуникационных ретрансляторов: все узлы могут быть потенциальными организаторами трафика, т. е. потенциальными ретрансляторами.

Tarzan позволяет приложениям-клиентам взаимодействовать с Интернет-серверами через специальные туннели. Два конца туннеля — узлы Tarzan, на которых запущено клиентское приложение, и узел Tarzan, на котором запущен транслятор сетевого адреса. Tarzan полностью прозрачен для клиентских приложений и серверов. Так что он должен быть установлен и настроен на всех участвующих узлах.

MorphMix обеспечивает подключение к системе простым способом любого человека, имеющего доступ к Интернету, и эффективно оперирует большим числом участвующих узлов, даже несмотря на динамическую среду и присутствие ненадежных узлов [18].

Процесс шифрования организуется следующим образом. До того как участник n_1 посылает сообщение участнику n_2, он заголовок шифрует в соответствии с правилами шифрования ссылок между n_1 и n_2 [18], используя симметрический ключ k_{l1}. Когда n_2 получает сообщение, он убирает шифрование ссылки, используя k_{l1}, убирает один слой шифрования, используя k_{n1}, определяет следующее промежуточное соединение в соответствии с идентификатором в заголовке, устанавливает поля в заголовке для следующей ссылки, шифрует его в соответствии с шифрованием ссылок между n_2 и n_3, используя k_{l2}, посылает все это участнику n_3. Это продолжается до тех пор, пока не достигается финальный узел, ретранслирующий данные на сервер, с которым n_1 хочет осуществить взаимодействие. Сообщения посылаются обратно n_1 точно так же, но в обратном порядке — каждый узел добавляет слой шифрования.

С технической точки зрения важно понимать, где оперирует сеть: на верхушке IP-слоя или на уровне приложения. В верхушке IP-слоя система прозрачна для транспортного протокола и протокола приложения. Данные поступают от инициатора после прохождения IP-слоя и посылаются через сеть с использованием UDP. На уровне приложения программа доступа, запущенная на компьютере инициатора, устанавливает TCP-соединение.

В настоящее время сети Tarzan и MorphMix, относящиеся к пиринговым сетям первого поколения, не используют. В данной статье мы их рассматриваем, поскольку они оказали значительное влияние на последующие разработки.

Freenet оперирует как сеть идентичных узлов, обеспечивающих место для хранения данных и маршрутизацию запросов к ним. Учитывается желание пользователя физически разместить данные в том или ином домене [19]. Трансляционный поиск или централизованный каталог расположений не используется. Обозначения файлов не позволяют определить их физическое расположение, поэтому невозможно обнаружить первоисточник или пункт назначения файла, продвигающегося через сеть. У каждого узла есть свое собственное хранилище данных, которое он делает доступным для чтения и записи в сети. Freenet дает возможность пользователям делиться своим свободным пространством на диске.

Запросы для ключей пересылаются от узла к узлу, через цепочки прокси-запросов, в которых каждый узел принимает решение о том, куда посылать запрос дальше. Маршрут определяется в зависимости от запрошенного ключа. Алгоритмы маршрутизации для хранения и получения данных были специально разработаны для адаптивной настройки маршрутов в реальном времени.

Каждому запросу дается лимит выхода из промежуточного соединения, аналогичный времени жизни IP-соединения. Время жизни уменьшается в каждом узле для предотвращения возникновения бесконечных цепей. Любому запросу приписывается псевдоуникальный случайный идентификатор. Поэтому узлы могут предотвращать циклы посредством отказа выполнять те запросы, которые они уже обрабатывали. При возникновении такой ситуации узел выбирает другой узел для дальнейшего соединения. Этот процесс продолжается до тех пор, пока запрос не будет выполнен или не исчерпает свое время жизни.

I2P-сеть является полностью распределенной, автономной, масштабируемой, эластичной и безопасной [20]. Все компоненты сети поставляются с открытым исходным кодом. Примечательной особенностью I2P-сети является то, что она может как выступать в роли оверлейной сети, использующейся в качестве надстройки над Интернетом, так и работать автономно, независимо от Интернета.

С технологической точки зрения I2P строит сеть P2P, которая берет преимущества анонимности и безопасности сетей, основанных на миксах Чаума [5]: свободную маршрутизацию и микс-каскады, производительность, масштабируемость и устойчивость распределенных хэш-таблиц, глобальную совместимость с Интернетом.

Сеть не нуждается в информации о пункте назначения сообщения. Аналогично, при получении сообщения, посланного через I2P, никто не знает, откуда оно поступило или кто его послал, однако отправитель может включить эту информацию. Более того, у машин, направляющих письмо из своего компьютера в точку назначения, нет информации об отправителе сообщения и точке назначения.

В сети используется локальная независимость. Это означает, что во время отправления в пункт назначения для сети неважно, где он находится физически. I2P включает не только сетевое программное обеспечение, но и I2P SDK, у которого есть API на нескольких языках, есть реализация маршрутизаторов, которые поддерживают коммуникации только с локальными конечными точками.

Вместо фокусирования на анонимном доступе в публичный Интернет ключевой целью проекта I2P является предоставление анонимного хостинга сервисов (аналог скрытых сервисов Tor).

Каждый узел I2P является маршрутизатором, так что нет четких различий между сервером и клиентом. I2P не использует централизованные серверы каталогов для подключения к узлам, а применяет вместо этого распределенные хэш-таблицы, описанные в работе [21].

Вместо ссылок на другие роутеры и сервисы I2P использует криптографические идентификаторы, при этом отсутствует DNS-подобный сервис.

Криптографический идентификатор маршрутизатора отличается от идентификатора сервиса, поэтому, если сервис будет запущен на каком-то маршрутизаторе, установление связи между этими двумя идентификаторами представляет собой трудную задачу. I2P использует вариант луковой маршрутизации, который называют чесночной маршрутизацией (Garlic Routing) [20].

Многие сервисы, такие, например, как Bittorent, eDonkey и т. п., могут находиться внутри сети I2P [22]. Основные приложения, доступные в сети I2P: Susimail — почтовый клиент [23], SusiDNS — DNS-клиент [24], I2Psnark — торрент-клиент [25], iMule — свободный анонимный клиент файлообменной сети [26].

В работе [27] исследованы внутренние сервисы I2P с точки зрения сайтов, находящихся внутри сети.

Netsukuku представляет собой ячеистую сеть с P2P-протоколом, генерирующим и поддерживающим себя автономно. Этот протокол разработан для обработки неограниченного числа узлов с минимальной нагрузкой на процессор и память [28].

Сеть устанавливается через компьютеры, соединенные друг с другом физически, таким образом, она не является оверлейной. Netsukuku строит маршруты, которые соединяют все компьютеры в сети и является самоуправляемой и автономной. При добавлении узла к Netsukuku сеть автоматически переписывает топологию, прокладывая самые быстрые и эффективные маршруты для коммуникаций с вновь прибывшими узлами. При увеличении числа узлов в сети она становится более эффективной. В Netsukuku отсутствует разница между приватными и публичными сетями.

Эта сеть является децентрализованной и распределенной. IP-адрес, определяющий компьютер, выбирается случайно, поэтому невозможно ассоциировать его с каким-то конкретным физическим местом. Маршруты, созданные огромным числом узлов, имеют высокую сложность и плотность. Единственный способ контролировать сеть — получить над ней физический контроль, поскольку каждый узел сети является ее частью.

В настоящее время маршрутизаторами Интернета управляют разные протоколы, такие как OSPF, RIP или BGP, основанные на разных классических алгоритмах, способных найти лучший путь для достижения узла в сети.

Эти алгоритмы подходят исключительно для создания небольших и средних сетей, поскольку требуют больших затрат процессорного времени и памяти. Ни один из этих протоколов не может быть использован в такой сети, как Netsukuku, где каждый узел является маршрутизатором, поскольку карта всех маршрутизаторов требует места на каждом компьютере, подсоединенном к сети (около 10 Гбайт).

В сети Netsukuku используется собственный алгоритм, называющийся QSPN [29]. В этом алгоритме вся сеть представлена в виде фрактала для вычисления маршрутов, необходимых для подключения узла ко всем остальным.

Благодаря фрактальной структуре нужно всего лишь несколько килобайт, чтобы хранить всю карту Netsukuku.

Помимо сети Netsukuku, существуют еще несколько подобных решений. Так, например, сеть Hyperboria представляет собой автономную, пиринговую беспроводную ячеистую сеть в диапазоне 2,4 ГГц. В такой сети каждый пользователь является провайдером самому себе: с вами нельзя разорвать договор о пользовании Интернетом и подслушать сообщения специальным оборудованием. Сеть является самонастраиваемой, и каждый клиент, подключающийся к сети, увеличивает ее емкость. Современные протоколы для строительства этой сети, такие, например, как сетевой протокол Cjdn, гарантируют шифрование всего трафика, проходящего через сеть [30]. Для государства такая сеть представляет двойное явление: с одной стороны, такой тип сетей позволяет за меньшие деньги подключать к сети удаленные регионы, а с другой стороны, трафик в таких сетях не может быть перехвачен и проанализирован.

Turtle является так называемой сетью F2F, представляющей специфическую форму сети P2P,

в которой пользователи могут осуществлять прямые соединения для обмена информацией только с друзьями или пользователями, которым они доверяют [31]. В сети имеется большой набор узлов и большой набор данных. Предполагается, что у каждого узла сети есть владелец, обладающий персональным набором данных и желающий получить доступ к остальным данным в сети.

Каждый набор данных имеет свой набор свойств, состоящий из пар, содержащих атрибут и значение, которые используются во время обработки запросов пользователей. Запросы состоят из определенного числа пар (атрибут, значение), связанных логическими операторами AND, OR, NOT.

Каждый пользователь устанавливает криптозащищенное соединение между своим узлом и всеми дружественными узлами в наборе.

Во время распространения запроса генерируется дерево передачи запроса, с корнем в узле, изначально направившим запрос. Дерево строится на основе связей доверия между пользователями и используется для доставки ответа на запрос. Для того чтобы сопоставить запросы с ответами, каждый узел хранит таблицу с запросами, которые он ретранслировал, но для которых процесс ответа на запрос еще не завершен.

Ответ на запрос состоит из адреса запрашивающего узла, финального бита, идентификатора запроса, значения счетчика промежуточных соединений, ответа. Финальный бит используется для дифференциации между частичными и окончательными ответами. Узел, получающий положительный ответ от одного из своих детей-узлов в дереве трансляции запроса, немедленно доложит узлу-родителю. Узел указывает, что у него больше нет ответов для продвижения вперед, через отсылку пакета ответа с финальным набором битов.

Запрос завершается после того, как вызвавший узел получает финальный ответ от всех своих друзей. Вызвавший узел собирает все части пакетов ответа воедино. Узел сортирует все частичные ответы, чтобы установить отдельные наборы атрибутов данных. Как только пользователь выбирает результат, в котором он заинтересован, происходит выдача данных.

Сеть RetroShare — новое поколение файлового P2P обмена имеет F2F-архитектуру. Эта сеть позволяет установить шифрованное соединение между аутентифицированными друзьями [32]. Соединение используется для разных коммуникационных сервисов и файлообмена. Оно не зависит от корпоративной системы или центрального сервера, так что все данные посылаются только друзьям и в некоторых случаях ретранслируются через них их друзьям, что делает RetroShare децентрализованной социальной файлообменной сетью.

RetroShare содержит следующие коммуникационные сервисы: приватные чаты с друзьями; приватные или публичные чаты комнаты; письма друзьям; форумы; голос через IP.

Существуют и другие файлообменные сети, например Guntella, которая является полностью децентрализованной сетью второго поколения [33], сети AntsP2P [34], MUTE [35], OneSwarm [36] относятся к сетям третьего поколения и отличаются повышенной безопасностью.

Дополнительную информацию, посвященную анонимным сетям P2P, можно найти в нескольких работах. Работа [37] представляет обзор файлообменных систем P2P, предлагающих некоторую форму анонимности для пользователя. В работе [38] приведен обзор частных сетей P2P, в которых инфраструктура и ресурсы предоставляются пользователями, а новые пользователи могут присоединиться только по персональному приглашению.

Заключение

В работе приведен обзор успешно применяющихся анонимных сетей. На сегодняшний день пользователи имеют богатый выбор решений, позволяющих сохранить свою анонимность в глобальной сети Интернет и даже развернуть собственный анонимный сервис. Сети различаются по своей архитектуре, типу маршрутизации, предназначению и целевой аудитории. Однако при всем многообразии решений нет ни одного, которое могло бы предоставить абсолютную защиту от внешнего наблюдателя. Технологии деанонимизации будет посвящена следующая статья авторов.

Список литературы

1. **National** Security Strategy [Electronic resource] // Whitehouse [Official website]. URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf (accessed: 8.09.2015).
2. **Зыков В.** ФСБ готовит закон против анонимности в интернете. 16 августа, 2013. [Электронный ресурс] // Известия [Официальный сайт]. URL: http://izvestia.ru/news/555552 (дата обращения: 26.08.2015 г.).
3. **Goldschlag D., Reed M., Syverson P.** Onion Routing for Anonymous and Private Internet Connections. January 28, 1999 [Electronic resource] // Onion Routing [Official website]. URL: http://www.omon-router.net/Publications/CACM-1999.pdf (accessed: 8.09.2015).
4. **Patent US 6266704** — Onion routing network for securely moving data through communication networks [Electronic resource] // Google [Official website]. URL: http://www.google.com/patents/US6266704 (accessed: 17.09.2015).
5. **Chaum D.** Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Electronic resource] // Free Haven [Official website]. URL: http://www.freehaven.net/anonbib/cache/chaum-mix.pdf (accessed: 8.09.2015).
6. **Feigenbaum J., Johnson A., Syverson P.** A Model of Onion Routing with Provable Anonymity [Electronic resource] // Yale [Official website]. URL: http://www.cs.vale.edu/homes/if/FJS.pdf (accessed: 8.09.2015).
7. **Onion** Routing [Electronic resource] // Onion Routing [Official website]. URL: http://www.onion-router.net (accessed: 8.09.2015).
8. **Feigenbaum J., Johnson A., Syverson P.** Probabilistic Analysis of Onion Routing in a Black-box Model [Electronic resource] // Yale [Official website]. URL: http://www.cs.yale.edu/homes/jf/WPES07-Aaron.pdf (accessed: 8.09.2015).
9. **Dingledine R., Mathewson N., Syverson P.** Tor: The Second-Generation Onion Router [Electronic resource] // Tor project [Official website]. URL: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (accessed: 8.09.2015).
10. **Who** uses Tor? [Electronic resource] // Tor project [Official website]. URL: https://www.torproiect.org/about/torusers.html.en (accessed: 8.09.2015).
11. **Biryukov A., Pustogarov I., Weinmann R.-P.** Content and popularity analysis of Tor hidden services. July 29, 2013 [Electronic

resource] // Cryptome [Official website]. URL: https://cryptome.org/2013/09/tor-analysis-hidden-services.pdf (accessed: 8.09.2015).

12. **Tor** Metrics [Electronic resource] // Tor project [Official website]. URL: https://metrics.torproiect.org (accessed: 8.09.2015).

13. **Chaabane A., Manils P., Kaafar M. A.** Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network [Electronic resource] // IEEE [Official website]. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5636000&url-http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5636000 (accessed: 8.09.2015).

14. **Gupta N., Malhotra H.** Analytical Study of Tor Hidden Services On Internet [Electronic resource] // International Journal of Research and Development in Technology & Management Sciences — Kailash [Official website]. URL: http://iournal.rtmonline.in/vol20iss8/05262.pdf (accessed: 8.09.2015).

15. **Scalable** and Secure P2P Overlay Networks [Electronic resource] // Wayne State University [Official website]. URL: http://www.cs.wayne.edu/~weisong/papers/shen04-overlay.pdf (accessed: 25.09.2015).

16. **Peer-to-Peer** Overlay Networks: A Survey [Electronic resource] // California state university Northridge [Official website]. URL: http://www.csun.edu/~andrzei/COMP529-S05/papers/TR-P2P.pdf (accessed: 25.09.2015).

17. **Freedman M. J., Morris R.** Tarzan: A Peer-to-Peer Anonymizing Network Layer [Electronic resource] // MIT, [Official website]. URL: http://pdos.csail.mit.edu/tarzan/docs/tarzan-ccs02.pdf (accessed: 8.09.2015).

18. **Rennhard M., Plattner B.** Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection [Electronic resource] // Free haven: (Official website]. URL: http://www.freehaven.net/anonbib/cache/morphmix:wpes2002.pdf (accessed: 8.09.2015).

19. **Clarke I., Sandberg O., Wiley B., Hong T. W.** Freenet: A Distributed Anonymous Information Storage and Retrieval System [Electronic resource] // Stanford University: [Official website]. URL: http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf (accessed: 8.09.2015).

20. **Astolfi F., Kroese J., Oorschot J.** I2P — The Invisible Project [Electronic resource] // Media Technology: [Official website]. URL: http://mediatechnology.leiden.edu/images/uploads/docs/wt2015_i2p.pdf (accessed: 8.09.2015).

21. **Maymounkov P., Mazieres D.** Kademlia: A Peer-to-peer Information System Based on the XOR Metric [Electronic resource] // MIT: [Official website]. URL: http://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf (accessed: 8.09.2015).

22. **Supported** Applications [Electronic resource] // I2P: [Official website]. URL: https://geti2p.net/en/docs/applications/supported#email (accessed: 8.09.2015).

23. **Susimail** [Electronic resource] // Susimail: [Official i2p website]. URL: http://127.0.0.1:7657/susimail/susimail (accessed: 8.09.2015).

24. **Susidns** [Electronic resource] // Susidns: [Official i2p website]. URL: http://127.0.0.1:7657/susidns/ (accessed: 8.09.2015).

25. **I2psnark** [Electronic resource] // I2psnark: [Official i2p website]. URL: http://127.0.0.1:7657/i2psnark/ (accessed: 8.09.2015).

26. **IMule** [Electronic resource] // I2P forum: [Official i2p website]. URL: http://forum.i2p/viewtopic.php?t=2213 (accessed: 8.09.2015).

27. **Crenshaw A**. Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts [Electronic resource] // Irongeek: [Official website]. URL: http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers (accessed: 8.09.2015).

28. **The Netsukuku** Wired [Electronic resource] // Netsukuku: [Official website]. URL: http://netsukuku.freaknet.org (accessed: 8.09.2015).

29. **Quantum** Shortest Path Netsukuku [Electronic resource] // Arxiv: [Official websitej. URL: http://arxiv.org/pdf/0705.0817v1.pdf (accessed: 17.09.2015).

30. **Hyperboria** — The privacy-friendly network without borders [Electronic resource] // Hyperboria: [Official website]. URL: https://hyperboria.net (accessed: 8.09.2015).

31. **Popescu B. C., Crispo B., Tanenbaum A. S.** Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System [Electronic resource] // NLnet: [Official website]. URL: https://nlnet.nl/project/turtle/2004-cspw.pdf (accessed: 8.09.2015).

32. **Retroshare** — secure communications for everyone [Electronic resource] // Retroshare: [Official website]. URL: http://retroshare.sourceforge.net (accessed: 8.09.2015).

33. **Gnutella** site archive [Electronic resources] // Internet archive Wayback machine: [Official website]. URL: https://web.archive.org/web/20080525005017/http://www.gnutella.com/(accessed: 8.09.2015).

34. **Ants** P2P [Electronic resource] // Ants P2P. [Official website]. URL: http://antsp2p.sourceforge.net (accessed: 8.09.2015).

35. **Simple,** Anonymous File Sharing [Electronic resource] // MUTE: [Official website]. URL: http://mute-net.sourceforge.net (accessed: 8.09.2015).

36. **OneSwarm** — Privacy preserving peer-to-peer data sharing [Electronic resource] // OneSwarm: [Official website]. URL: http://www.oneswarm.org/index.html (accessed: 8.09.2015).

37. **Chotia T., Chatzikokolakis K.** A Survey of Anonymous Peet-to-Peer File-Sharing [Electronic resource] // Ecole Pulytechnique: [Official website]. URL: http://www.lix.polvtechnique.fr/~kostas/papers/AnonyP2PSurvey.pdf (accessed: 8.09.2015).

38. **Rogers M., Bhatti S.** How to Disappear Completely: A Survey of Private Peer-to-Peer Networks [Electronic resource] // Researchgate: [Official website]. URL: https://www.researchgate.net/publication/228700831_How_to_disappear_complet ely_A_survey_of_private_peer-to-peer_networks (accessed: 8.09.2015).

S. M. Avdoshin, PhD, professor, Head of Software Engineering School,
Faculty of Computer Science, HSE, savdoshin@hse.ru
A. V. Lazarenko, undergraduate student, Software Engineering School,
Faculty of Computer Science, HSE, avlazarenko@edu.hse.ru
National Research University Higher School of Economics (HSE)

Technology of Anonymous Networks

This paper is an overview of currently used anonymous networks based on technology of onion routing and peer-to-peer networking. It describes key features of the networks and their comparative characteristics. The main purpose of every anonymous network is to protect information from the adversaries and provide users with great level of anonymity. All networks can be clustered on two classes: onion routing and its modifications and plain-old peer-to-peer networks. In the first class the major participant is Tor, which is based on the second generation of onion routing. On the other hand, P2P networks can be divided on 2 classes: traditional peer-to-peer and friend-to-friend. Friend-to-friend is a type of routing where users connects only to those users, who are considered as friends. The first class of peer-to-peer networks contains: Tarzan, MorphMix, Freenet, I2P, Netsukuku. The second class is represented by such networks as: Turtle, RetroShare. Current paper is focused only on those networks, which were successful on practice, or have strong impact on anonymous systems. Nowadays users have a wide specter of different solutions which can be used for protecting anonymity on the Internet. Anonymous networks differ by architectures, routing types and target audiences. Unfortunately, there is no any solution, which guarantees 100 % defense from adversaries. Every technology has its own weaknesses and vulnerabilities, allowing attacker to somehow deanonimize a particular user.

Keywords: *anonymous networks, onion routing, peer-to-peer, layered encryption, invisible internet, overlay networks*

References

1. **National** Security Strategy [Electronic resource], *Whitehouse* [Official website]. URL: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_str ategv.pdf (accessed: 8.09.2015).

2. **Zykov V.** FSB gotovit zakon protiv anonimnosti v internete. [Electronic resource], *Izvestiya* [Official website]. URL: http://izvestia.ru/news/555552 (accessed: 26.08.2015 г.).

3. **Goldschlag D., Reed M., Syverson P.** Onion Routing for Anonymous and Private Internet Connections. January 28, 1999 [Electronic resource], *Onion Routing* [Official website]. URL: http://www.omon-router.net/Publications/CACM-1999.pdf (accessed: 8.09.2015).

4. **Patent US 6266704.** Onion routing network for securely moving data through communication networks [Electronic resource], Google [Official website]. URL: http://www.google.com/patents/US6266704 (accessed: 17.09.2015).

5. **Chaum D.** Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Electronic resource], *Free Haven* [Official website]. URL: http://www.freehaven.net/anonbib/cache/chaum-mix.pdf (accessed: 8.09.2015).

6. **Feigenbaum J., Johnson A., Syverson P.** A Model of Onion Routing with Provable Anonymity [Electronic resource], *Yale* [Official website]. URL: http://www.cs.yale.edu/homes/jf/FJS.pdf (accessed: 8.09.2015).

7. **Onion** Routing [Electronic resource], *Onion Routing* [Official website]. URL: http://www.onion-router.net (accessed: 8.09.2015).

8. **Feigenbaum J., Johnson A., Syverson P.** Probabilistic Analysis of Onion Routing in a Black-box Model [Electronic resource], *Yale* [Official website]. URL: http://www.cs.yale.edu/homes/jf/WPES07-Aaron.pdf (accessed: 8.09.2015).

9. **Dingledine R., Mathewson N., Syverson P.** Tor: The Second-Generation Onion Router [Electronic resource], *Tor project* [Official website]. URL: https://svn.toфroject.org/svn/projects/design-paper/tor-design.pdf (accessed: 8.09.2015).

10. **Who** uses Tor? [Electronic resource], *Tor project* [Official website]. URL: https://www.torproject.org/about/torusers.html.en (accessed: 8.09.2015).

11. **Biryukov A., Pustogarov I., Weinmann R.-P.** Content and popularity analysis of Tor hidden services. July 29, 2013 [Electronic resource], *Cryptome* [Official website]. URL: https://cryptome.org/2013/09/tor-analysis-hidden-services.pdf (accessed: 8.09.2015).

12. **Tor** Metrics [Electronic resource], *Tor project* [Official website]. URL: https://metrics.torproject.org (accessed: 8.09.2015).

13. **Chaabane A., Manils P., Kaafar M. A.** Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network [Electronic resource[, *IEEE* [Official website]. URL: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5636000&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5636000 (accessed: 8.09.2015).

14. **Gupta N., Malhotra H.** Analytical Study of Tor Hidden Services On Internet [Electronic resource], *International Journal of Research and Development in Technology & Management Sciences — Kailash* [Official website]. URL: http://journal.rtmonline.in/vol20iss8/05262.pdf (accessed: 8.09.2015).

15. **Scalable** and Secure P2P Overlay Networks [Electronic resource], *Wayne State University* [Official website]. URL:http://www.cs.wayne.edu/~weisong/papers/shen04-overlay.pdf (accessed: 25.09.2015).

16. **Peer-to-Peer** Overlay Networks: A Survey [Electronic resource], *California state university* Northridge [Official website]. http://www.csun.edu/~andrzei/COMP529-S05/papers/TR-P2P.pdf (accessed: 25.09.2015).

17. **Freedman M. J., Morris R.** Tarzan: A Peer-to-Peer Anonymizing Network Layer [Electronic resource], *MIT* [Official website]. URL: http://pdos.csail.mit.edu/tarzan/docs/tarzan-ccs02.pdf (accessed: 8.09.2015).

18. **Rennhard M., Plattner B.** Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection [Electronic resource], *Free haven* [Official website]. URL: http://www.freehaven.net/anonbib/cache/morphmix:wpes2002.pdf (accessed: 8.09.2015).

19. **Clarke I., Sandberg O., Wiley B., Hong T. W.** Freenet: A Distributed Anonymous Information Storage and Retrieval System [Electronic resource], *Stanford University* [Official website]. URL: http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf (accessed: 8.09.2015).

20. **Astolfi F., Kroese J., Oorschot** J. I2P — The Invisible Project [Electronic resource], *Media Technology* [Official website]. URL: http://mediatechnology.leiden.edu/images/uploads/docs/wt2015_i2p.pdf (accessed: 8.09.2015).

21. **Maymounkov P., Mazieres D.** Katdemlia: A Peer-to-peer Information System Based on the XOR Metric [Electronic resource], *MIT* [Official website]. URL: http://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf (accessed: 8.09.2015).

22. **Supported** Applications [Electronic resource], *I2P* [Official website]. URL: https://geti2p.net/en/docs/applications/supported#email (accessed: 8.09.2015).

23. **Susimail** [Electronic resource], *Susimail* [Official i2p website]. URL: http://127.0.0.1:7657/susimail/susimail (accessed: 8.09.2015).

24. **Susidns** [Electronic resource], *Susidns* [Official i2p website]. URL: http://127.0.0.1:7657/susidns/ (accessed: 8.09.2015).

25. **I2psnark** [Electronic resource], *I2psnark* [Official i2p website]. URL: http://127.0.0.1:7657/i2psnark/ (accessed: 8.09.2015).

26. **IMule** [Electronic resource], *I2P forum* [Official i2p website]. URL: http://forum.i2p/viewtopic.php?t=2213 (accessed: 8.09.2015).

27. **Crenshaw A.** Darknets and hidden servers: Identifying the true IP/*network* identity of I2P service hosts [Electronic resource], Irongeek [Official website]. URL: http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers (accessed: 8.09.2015).

28. **The Netsukuku** Wired [Electronic resource], *Netsukuku* [Official website]. URL: http://netsukuku.freaknet.org (accessed: 8.09.2015).

29. **Quantum** Shortest Path Netsukuku [Electronic resource], *Arxiv* [Official website]. URL: http://arxiv.org/pdf/0705.0817vl.pdf (accessed: 17.09.2015).

30. **Hyperboria** — The privacy-friendly network without borders [Electronic resource], *Hyperboria* [Official website]. URL: https://hyperboria.net (accessed: 8.09.2015).

31. **Popescu B. C., Crispo B., Tanenbaum A. S.** Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System [Electronic resource], *NLnet* [Official website]. URL: https://nlnet.nl/project/turtle/2004-cspw.pdf (accessed: 8.09.2015).

32. **Retroshare** — secure communications for everyone [Electronic resource], *Retroshare* [Official website]. URL: http://retroshare.sourceforge.net (accessed: 8.09.2015).

33. **Gnutella** site archive [Electronic resources], *Internet archive Wayback machine* [Official website]. URL: https://web.archive.org/web/20080525005017/http://www.gnutella.com/ (accessed: 8.09.2015).

34. **Ants** P2P [Electronic resource], *Ants P2P* [Official website]. URL: http://antsp2p.sourceforge.net (accessed: 8.09.2015).

35. **Simple,** Anonymous File Sharing [Electronic resource], *MUTE* [Official website]. URL: http://mute-net.sourceforge.net (accessed: 8.09.2015).

36. **OneSwarm** — Privacy preserving peer-to-peer data sharing [Electronic resource], *OneSwarm* [Official website]. URL: http://www.oneswarm.org/index.html (accessed: 8.09.2015).

37. **Chotia T., Chatzikokolakis K.** A Survey of Anonymous Peet-to-Peer File-Sharing [Electronic resource], *Ecole Pulytechnique* [Official website]. URL: http://www.lix.polytechnique.fr/~kostas/papers/AnonyP2PSurvey.pdf (accessed: 8.09.2015).

38. **Rogers M., Bhatti S.** How to Disappear Completely: A Survey of Private Peer-to-Peer Networks [Electronic resource], *Researchgate* [Official website]. URL: https://www.researchgate.net/publication/228700831_How_to_disappear_comp letely_A_survey_of_private_peer-to-peer_networks (accessed: 8.09.2015).