данных - а именно, число таких троек будет равно квадрату общего числа пикселей изображения. Имея даже изображение 10x10, нам потребуется обработать 10000 троек. Сложность задачи растет быстро - как квадрат площади изображения.

В качестве решения данной проблемы можно предложить распределенную обработку изображения на кластере при помощи технологии MapReduce. Кластер это группа компьютеров, объединенных в общую сеть при помощи линий связи. Это могут быть как быстрые Infiniband, так и более медленные Ethernet.

MapReduce это подход к обработке данных, сформированный компанией Google. Ее принцип заключается в том, чтобы разделить все операции с данными на два этапа: map и reduce. На map шаге рабочие узлы получают задание и головного на предварительную обработку данных. На reduce шаге рабочие ноды осуществляют свертку результатов обработки после map шага. После выполнения этого шага, головной узел получает итоговый результат.

В качестве фреймфорка для разработки можно выбрать Apache Hadoop [3]. Он создавался с учетом этой модели и позволяет создать надежную систему на большом числе узлов(вплоть до тысяч и сотен тысяч), и единственным ограничением является объем памяти головного узла, которая хранит метаданные. Кроме того, он достаточно прост в разработке и отладке.

В качестве файловой системы используется распределенная HDFS [4], оптимизированная для однократной записи и многократного считывания. Файл хранится в виде набора реплицируемых (для отказоустойчивости) блоков. Hadoop предоставляет API и консольную программу для работы с данной файловой системой.

Hadoop реализован на языке программирования Java и имеет свою реализацию MapReduce. Поэтому для определения своих операций map и reduce необходимо реализовать определенные классы - Mapper и Reducer. Это интерфейсы, которые имеют методы map и reduce соответственно. Для обмена данными используется класс Context.

На рисунке 1 приведен результат расчета гистограммы при помощи указанной технологии. Она является результатом суммирования трехмерной гистограммы по двум координатам.

Достоинством данного подхода является масштабируемость. На кластере можно за короткое время обрабатывать как крупные изображения, так и множество небольших. При недостатке производительности достаточно добавить одну или несколько новых нод. Еще один плюс - относительная дешевизна, поскольку как правило новое оборудование стоит дешевле дополнительных человеко-часов, которые необходимо затратить на улучшение существующего ПО.

У данного метода есть недостатки. Очевидно, что с учетом накладных коммуникационных расходов между отдельными нодам в кластере. Это приводит к тому, что вычисление при помощи других технологий на одной ЭВМ (напрмиер, с помощью CUDA) оказывается более эффективным.

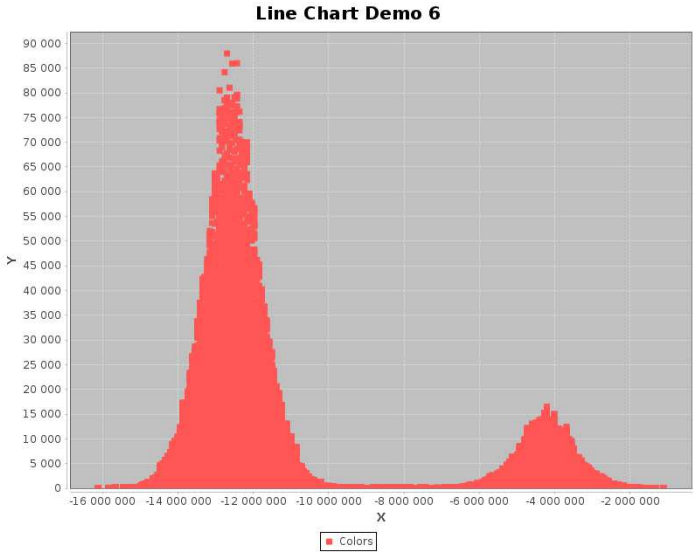

Рисунок 1 – Гистограмма изображения

Литература

1. Zone System & Histograms [Электронный ресурс]. - Режим доступа: http://www.illustratedphotography.net/basic-photography/zone-system-histograms

2. Куприянов, А.В. Анализ текстур и определение типа кристаллической решетки на наномасштабных изображениях [Текст] / А.В. Куприянов // Компьютерная оптика - 2011. - Т. 35.-2.-С.145-152.

3. Apache Hadoop 2.7.2 [Электронный ресурс]. - Режим доступа: http://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-common/FileSystemShell.html

4. HDFS Architecture Guide [Электронный ресурс]. - Режим доступа: https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html

Д.О. Маркин, А.С. Галкин, П.А. Архипов

ПОСТРОЕНИЕ АНОНИМНОЙ СЕТИ НА БАЗЕ ТЕХНОЛОГИИ ВЕБ-ПРОКСИ

(Академия Федеральной службы охраны Российской Федерации)

Существующие современные условия удаленного доступа к информационным ресурсам позволяют говорить о том, что простое обращение к информационному сервису оставляет значительное количество "следов" такого обращения в информационных log-файлах провайдеров услуг связи, промежуточных узлах на пути следования данных, а также программном обеспечении и удален-

ных базах данных разработчиков программного обеспечения, которое использует пользователь. Такое положение дел свидетельствует об установлении негласного тотального наблюдения за пользователями глобальной сети, что в ряде случаев является недопустимым и, в том числе, прямым нарушением права человека на тайну связи, являющемся неотъемлемым правом личности, признанном на международном уровне.

Одним из решением данной проблемы является использование анонимных сетей, представляющих собой компьютерные сети, построенные поверх глобальной сети, в основе которых лежит распределенный характер ее узлов, а также многоуровневая криптографическая защита адресной информации.

Построение анонимных сетей на базе веб-прокси

Основой для построения анонимных сетей являются прокси-сервера. Отдельной категорией прокси-серверов выделяют *веб-прокси*, представляющее собой веб-приложение (например, на базе Perl, Python или PHP-скрипта), установленное на веб-сервере.

Использование веб-прокси в отличие от классических программно-аппаратных платформ имеет ряд преимуществ:

– может быть использована арендованная или бесплатная программно-аппаратная платформа, не требующая существенных материальных и временных затрат для развертывания;

– установка и настройка программного обеспечения веб-прокси не требует глубоких специальных знаний и позволяет в сжатые сроки получить работоспособный прокси-сервер;

– существует большое количество доступных программно-аппаратных платформ – хостингов, которые могут быть использованы в качестве веб-прокси за сравнительно низкую плату или вовсе бесплатно.

Совокупность данных факторов предопределяет высокую доступность технологии веб-прокси, а современные технические возможности веб-серверов и серверных расширений, позволяющих обрабатывать Perl, Python, PHP и другие скрипты, предоставляют широкие возможности для разработчиков.

Построение анонимных сетей на базе веб-прокси является достаточно тривиальной задачей, однако не получила широкого распространения в связи с рядом проблем, связанных с ограниченной функциональностью веб-серверов. К таким проблемам относятся:

– внесение адреса веб-сервера, на котором функционирует веб-прокси в список запрещенных, и, соответственно, блокирование доступа к нему на уровне сети;

– низкая скорость соединения между веб-прокси и удаленными ресурсами (другими веб-прокси);

– наличие скриптов в коде удаленного информационного ресурса, которые исполняются на клиентской стороне и должны в "прозрачном" режиме передаваться через веб-прокси.

Данные ограничения в той или иной степени являются устранимыми, однако в то же время снижают привлекательность веб-прокси для массового использования.

Веб-прокси выступающий в качестве посредника между пользователем и информационными ресурсами глобальной сети позволяет частично решить задачу анонимного доступа к ресурсам или обойти ограничения локальной сети пользователя, однако он достаточно уязвим к обнаружению и блокированию как со стороны администраторов локальной сети пользователя, так и со стороны ресурсов глобальной сети.

В случае построения анонимной сети на базе веб-прокси повышается вероятность сохранения конфиденциальности доступа, а также вероятность раскрытия ее параметров

Технологии луковой и чесночной маршрутизации при построении анонимных сетей

Для решения задачи построения анонимной сети необходима реализация технологии анонимного обмена данными через компьютерные сети, например, технология луковой маршрутизации [1], реализованная в анонимной сети Tor [2]. Сущность луковой маршрутизации заключается в том, что каждый маршрутизатор анонимной сети удаляет слой шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторяется. Таким образом, промежуточные узлы не знают источник, пункт назначения и содержание сообщения.

Для функционирования сети луковой маршрутизации необходима организация системы распределения криптографических ключей и, соответственно, наличие третьей доверенной стороны. Ее функции может выполнять центр сертификации, которому "доверяют" узлы анонимной сети.

При необходимости технология луковой маршрутизации может быть усилена за счет дробления пакетов и передачи их разными маршрутами. Такая технология была реализована в анонимной сети I2P [3] и является одним из расширения сети Tor.

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. Один "чеснок" в момент его формирования перед отправкой закладываются множество "зубчиков", являющихся зашифрованными сообщениями как нашего узла, так и чужими – транзитными. Является ли тот или иной "зубчик" в "чесноке" нашим сообщением или это чужое транзитное сообщение, которое просто проходит через нас, знает только тот, кто создал "чеснок", никто иной узнать эту информацию не может. Чесночная технология применяется тогда, когда нужно отправить зашифрованное сообщение через промежуточные узлы, у которых не должно быть доступа к этой информации.

Применение концепции активных данных и технологий терминальных программ при построении анонимной сети на базе веб-прокси

Технологии луковой и чесночной маршрутизации по созданию анонимной сети как системы защиты от раскрытия источника данных, как и любое средство защиты, обладают рядом слабых мест, поэтому продолжают совершенствоваться. Одним из направлений совершенствования таких механизмов защиты является использования концепции активных данных и так называемых терминальных программ, описанных в [4]. Активные данные, одновременно являясь терминальными программами, способны настраивать программно-определяемое оборудование, требуемое для их распространения, и могут управлять процессом своего распространения в коммуникационной среде.

Технологии веб-прокси являются подходящим инструментом, не требующим разработки дополнительных механизмов реализации концепции терминальных программ. Иными словами, при передаче данных по анонимной сети на базе веб-прокси в качестве полезной нагрузки в данных приложения HTTP могут быть заложены инструкции в виде скрипта. Такой скрипт, попав на i-й удаленный узел – веб-прокси, после его исполнения может решать ряд задач, позволяющих существенно усилить защищенность анонимной сети, например:

– сгенерировать новый маршрут следования передаваемых данных;

– сгенерировать новый исполняемый скрипт с необходимыми функциями;

– выполнить запрос к удаленному узлу(ам) или осуществить информационный обмен со сменой протокола доступа (например, по протоколу Telnet, SSH и др.).

Принципы самомаршрутизации на основе концепции активных данных рассмотрены в работе [4]. Для реализации функций самомаршрутизации (функции, при которой пакет, попав на промежуточный узел сети, принимает решение о маршруте своего дальнейшего перемещения на основе текущих данных об инфокоммуникационном окружении) [4] должен предоставляться список "ближних соседей" – устройств, с которыми соединение уже установлено или может быть установлено непосредственно. Такой список может формироваться и обновляться в реальном времени за счет функции мониторинга коммуникационного ресурса (обеспечения осведомленности [5] о происходящих изменениях в инфокоммуникационной среде).

Таким образом, при решении задачи построения анонимной сети на базе веб-прокси может использоваться комплекс подходов, таких как луковая и чесночная маршрутизация, шифрование вложенных данных уровня приложений, исполнение вложенных данных на промежуточных узлах при реализации функций самомаршрутизации, что позволит обеспечить необходимую конфиденциальность и скрытность источника запроса. Однако в то же время необходимо решить ряд проблем, связанных с особенностями использования технологий веб-прокси, связанных в первую очередь с ограничениями, накладываемыми веб-сервером на выполнение скриптов, а также с устойчивость соединения,

которое может включать несколько промежуточных узлов. Кроме того, существенным фактором является защищенность от раскрытия параметров такой сети и надежность установленного удаленного соединения.

Литература

1. Michael G. Reed, Paul F. Syverson, David M. Goldschlag Patent US6266704 B1 USA H04L 29/06 (20060101); H04L 12/56 (20060101); G06F 015/173 (); G06F 001/24 (). Onion routing network for securely moving data through communication networks / Michael G. Reed, Paul F. Syverson, David M. Goldschlag ; assignee The United States Of America As Represented By The Secretary Of The Navy. – № US 09/086,541 ; filed. 29.05.1998 ; pub. 24.07.2001.

2. The Tor Project, Inc. Tor Project: Anonymity Online // The Tor Project, Inc. [Электронный ресурс] : сайт. – Электрон. дан. – 2015. – Режим доступа: https://www.torproject.org/index.html.en. – Дата обращения: 08.10.2015.

3. Garlic Routing Garlic Routing and "Garlic" Terminology // Garlic Routing [Электронный ресурс] : сайт. – Электрон. дан. – 2015. – Режим доступа: https://geti2p.net/en/docs/how/garlic-routing. – Дата обращения: 08.10.2015.

4. Кулешов С.В., Цветков О.В. Активные данные в цифровых программно-определяемых системах // Информационно-измерительные и управляющие системы № 6, 2014 г. С.12–19.

5. Разработка методологии комплексного мониторинга инфокоммуникационных ресурсов в распределенных сложноорганизованных системах // Отчет о НИР по ПФИ ОНИТ РАН № 2 Научные основы создания гетерогенных телекоммуникационных и локационных систем и их элементной базы, направление Алгоритмическое и программное обеспечение телекоммуникационных сетей, руководитель Александров В.В., № 01201360808.

Б.В. Мартемьянов

СШИВКА ПОЛОС ИЗОБРАЖЕНИЙ С УЧЕТОМ МЕЖМАТРИЧНЫХ ГОЛОНОМНЫХ СВЯЗЕЙ

(Самарский государственный технический университет)

Современные космические аппараты, предназначенные для дистанционного зондирования Земли, формируют изображения средствами оптико-электронных преобразователей (ОЭП), построенных на основе матриц фоточувствительных приборов с зарядовой связью (ФПЗС).

Для обеспечения достаточной ширины полосы захвата в структуре ОЭП предусматривают десятки отдельных матриц ФПЗС. Такие ОЭП будем называть многоматричными (МОЭП). Матрицы в составе МОЭП выстраиваются вдоль двух параллельных прямых так, что каждая пара смежных матриц в области их смежных сторон «перекрывается» на некоторое количество ячеек ФПЗС, порождая взаимное перекрытие «полей зрения» этих матриц. В процессе