Математические структуры и моделирование 2018. № 2(46). С. 95–101

УДК 004.7
DOI: 10.25513/2222-8772.2018.2.95-101

ПОДХОДЫ К РЕАЛИЗАЦИИ СЕТЕВОГО ПРОТОКОЛА ОБЕСПЕЧЕНИЯ ГАРАНТИРОВАННОЙ ДОСТАВКИ ПРИ МУЛЬТИМАРШРУТНОЙ ПЕРЕДАЧЕ ДАННЫХ

С.В. Гусс
старший преподаватель, e-mail: infoguss@gmail.com
Д.Н. Лавров
к.т.н., доцент, e-mail: lavrov@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В работе рассматривается проблема повышения надёжности передачи данных в сети с мерцающими узлами. Даются некоторые замечания по разработке алгоритмов разделения потока данных и восстановления потерянных данных. Предлагаются общие соображения, связанные с реализацией протокола многопутевой маршрутизации в самоорганизующихся динамических сетях.

Ключевые слова: маршрутизация, разделение секрета, восстановление данных, пропускная способность, сетевая отказоустойчивость.

Введение

В данной работе под узлом прежде всего понимается промежуточное устройство, способное передавать трафик. Мерцающий указывает на нестабильность работы, либо непостоянство присутствия в сети, возможно, в результате перемещения в пространстве. Предполагается, что надёжность передачи можно повысить, взяв за основу методы разделения секрета и коды, корректирующие ошибки.

Гарантированная доставка всегда была актуальной проблемой для передачи важных данных. Этот вопрос решается на нескольких уровнях модели OSI.

Традиционно можно начать с транспортного уровня. Здесь гарантированную доставку обеспечивает протокол TCP, используется механизм подтверждения полученных сегментов данных. Протокол не учитывает наличия нескольких маршрутов до сети места назначения и не использует возможность более быстрой доставки за счёт разделения сообщения. Последнюю можно было бы использовать для введения избыточности в целях повышения надёжности. В случае с TCP избыточность может привести к нестабильности работы протокола и некорректной его работе.

На сетевом уровне возможна балансировка нагрузки, которая осуществляется в большинстве случаев для равновесных маршрутов. Осуществление гарантированной доставки возлагается на протоколы вышележащих уровней.

На канальном уровне в пределах локальной сети решение возможно за счёт резервирования. Помимо надёжности резервирование в некоторых случаях способствует ускорению передачи данных, например, за счёт агрегирования каналов (технология EtherChannel), в связи с чем и создаётся возможность балансировки. Протокол STP тоже создаёт резервные пути при построении связующего дерева, но балансировка нагрузки в итоговом дереве отсутствует.

Существует ещё возможность резервирования и балансировки шлюзов с помощью протоколов HSRP и GLBP.

Рассмотрим проблему гарантированной доставки в таком варианте. Передача данных осуществляется через агрессивную среду или среду с отсутствием доверия к отдельным узлам. В такой среде может присутствовать злоумышленник, контролирующий только часть узлов, через которые могут проходить данные. Злоумышленник может быть пассивным и пытаться только просмотреть данные, либо же активным: может пытаться повредить данные, изменить и, в конце концов, не дать доставить данные до места назначения. Если первые два действия ещё могут быть защищены стандартными криптографическими средствами и технологиями типа VPN, то от последнего из перечисленных действий шифрование и алгоритмы контроля целостности не защитят — сообщение просто не сможет быть доставлено.

В настоящее время существуют подозрения, что часть выходных узлов той же TOR-сети контролируются недружественными иностранными организациями. Тогда появляется задача написать TOR-клиент, который будет с помощью алгоритмов разделения секрета разделять потоки между несколькими выходными узлами TOR-сети и таким образом гарантировать доставку до места назначения, а сами алгоритмы разделения секрета помогут восстановить уничтоженные или потерянные данные. Описанный подход может быть применён для произвольной группы прокси-серверов, не обязательно TOR-сети.

1. Сети с мерцающими узлами

Концепция мерцающих узлов более применима для так называемых крупных подвижных объектов — кораблей, самолётов, поездов [1]. А сами узлы обслуживаются системами спутниковой связи. Обсуждение проблемы ведётся с точки зрения физического доступа и связи. Существуют определённые наработки в виде топологических моделей систем связи, которые также применимы к самоорганизующимся компьютерным сетям. Эти модели оказывают влияние на логику работы алгоритмов маршрутизации. Протоколы маршрутизации в таких системах могут учитывать повторения во времени топологических изменений. Главная особенность алгоритмов — невозможность гарантировать передачу информации по заданному маршруту и графику движения, плюс ко всему требуются постоянные корректировки таблиц маршрутизации, а также учёт статистических данных. В логике маршрутизации можно учитывать повторения, длительность, стабильность состояний расположения сетевых устройств и разнородность их скоростей и производительности. Может производиться «формирование базы данных характеристик движения объектов и расчёт времени

открытия и закрытия каналов между парами устройств» [1].

2. Методы разделения секрета

Предполагается разделение потока информации на несколько частей (потоков) и одновременная их передача по разным каналам связи. Это позволит наиболее полно задействовать ресурсы сети и снизить риск перехвата и восстановления отправленного сообщения [2]. Интересным решением видится обеспечение взаимозависимости между потоками. В идеале это должно усложнить восстановление сообщения в случае перехвата. Отмечается, что при передаче текстовой информации в некоторых случаях возможно задействовать особенности естественного языка, связанные с частотой появления символов и существованием зависимости между близко стоящими символами. Если принять во внимание две эти особенности, можно улучшить надёжность разделения потоков с точки зрения безопасности. В работе [3] предлагается «предварительно использовать один из оптимальных алгоритмов кодирования, позволяющий выровнять статистические характеристики текста».

3. Коды, корректирующие ошибки

Главной особенностью алгоритмов, способных обнаруживать и исправлять ошибки, возникающие в процессе передачи, является добавление избыточной информации. Всё это можно использовать не только в целях исправления ошибок и контроля целостности данных, но и для создания неблагоприятных условий для злоумышленника, пытающегося восстановить или внести изменения в передаваемую информацию. Сегодня всё чаще говорят о «внедрении интегрированных механизмов обеспечения безопасности и достоверности в протоколах обмена данными компьютерных сетей» [4].

4. Алгоритмы разделения и восстановления данных

В схемах разделения секрета при реализации защищённых распределённых вычислений традиционно присутствуют [5] постановщик задачи (тот, кто распределяет данные) и получатель результата. Первый отвечает за разделение данных и за соответствующие вопросы (избыточность, форматирование, шифрование), а второй за восстановление данных. Традиционно распределённость вычислений предполагает наличие нескольких интеллектуальных узлов, обрабатывающих информацию по определённым алгоритмам.

5. Реализация протокола многопутевой маршрутизации в самоорганизующихся динамических сетях

Алгоритм построения маршрутов в компьютерной сети зависит от выбора критерия оптимизации [6]. Учитывается изменение топологии (особенно в самоорганизующихся сетях) и нагрузка на сеть. Для стабильных сетей, с малой

или нулевой степенью изменения, маршруты строятся заранее, на что требуется определённое время для вычислений. Такой подход не годится, когда нужно по возможности быстро реагировать на изменения в топологии. Поскольку заранее не известно количество узлов сети и качество каналов связи между ними, задача построения маршрутов становится ещё сложнее.

Имеет смысл накапливать информацию в процессе работы протокола маршрутизации в конкретных условиях. Это необходимо для выявления определённой модели поведения и составления набора профилей. В процессе работы протокола такой профиль выбирается автоматически на основе анализа ситуации, определении паттерна действий и происходит настройка процесса маршрутизации согласно выбранному алгоритму, пригодному в данном конкретном случае [7]. Таким образом, предлагается подход, в котором критерий оптимизации определяется в процессе использования сетевых ресурсов. На основе критерия оптимизации выбирается наиболее приемлемый профиль, влияющий на процесс построения маршрута путём запуска того или иного алгоритма в зависимости от количества узлов в сети и её топологии на данный момент.

Реализация (программная или аппаратная) любого сетевого протокола возможна только после того, как составлено описание алгоритма его работы: формат и последовательность сообщений, временные характеристики, условия выбора, очерёдность принятия решений. Описание протокола — общая схема, по которой могут взаимодействовать реализации различных производителей. Если протокол востребован и успешен, то возможно множество его реализаций, отличающихся стабильностью работы, удобством настройки, полнотой реализации для той или иной системы (например, операционной). Общедоступное, полное описание протокола создаётся тогда, когда он прошёл ряд испытаний и показал свою пригодность на практике. Цель исследований авторов статьи — получить в конечном итоге реализацию протокола динамической многопутевой маршрутизации в сети с непостоянной, быстроменяющейся топологией.

В многопутевой маршрутизации (multipath routing) для передачи трафика могут использоваться несколько маршрутов, пролегающих через разные каналы связи. Большая нагрузка на быстрый канал связи может сделать весь маршрут не привлекательным с точки зрения надёжности и отказоустойчивости в отсутствии правильной политики выставления приоритетов на тот или иной тип трафика. В тоже время, не факт, что канал будет нагружен постоянно. Таким образом, алгоритм построения маршрута должен основываться не только на качестве каналов связи, составляющих маршрут, но и на статистике использования каналов при построении резервных и, в идеальном случае, параллельных путей для балансировки нагрузки и ускорения передачи данных, когда есть возможность по максимуму использовать ресурсы ненагруженной сети. Вообще говоря, в этом и заключается основная задача многопутевой маршрутизации — оптимизация использования ресурсов сети, а это приводит к избавлению от перегрузок и повышению стабильности сети.

В качестве инструмента имитационного моделирования для проверки работоспособности протокола предполагается мультиагентное моделирование (agent-based modeling). В качестве объекта могут быть выбраны беспровод-

ные компьютерные, самоорганизующиеся сети (mesh, ad-hoc), тем не менее, протокол не ограничивается исключительно беспроводными сетями. Последние выбраны в связи с их динамическим характером изменения.

Для проведения исследований принято решение разработать симулятор [8], возможно, в качестве надстройки (расширения) над существующей системой имитационного моделирования. Такая система должна обладать возможностью описания агентов, проведения экспериментов и оценки функционирования. Описание среды и объектов должно проходить на трёх уровнях: микро (низкий уровень абстракции, для учёта деталей), мезо (средний), макро (высокий). В свою очередь сам процесс моделирования должен проходить на трёх уровнях. На оперативном уровне задаются параметры (моделирование физической среды): размеры, расстояния, время, скорость. На тактическом уровне составляются сценарии: возможное изменение параметров и характеристик объектов, передвижение, маршрутизация трафика (расписание, задержки). На стратегическом уровне, где происходят взаимодействие, препятствия, влияния, внешние воздействия, обратные связи, тенденции — производится вмешательство в моделируемую среду, введение непредвиденных обстоятельств. Моделирование проходит в определённой последовательности: задание характеристик, сценария (миссии) передвижения, потоков трафика (кто, кому); выбор карты, местности, локации с объектами (статическими, динамическими); выбор алгоритмов поведения агентов в различных условиях и вмешательство в процесс по ходу действия.

Аналитические способности симуляции: идентификация и прогнозирование состояния системы, рекомендации (стратегические, тактические, оперативные).

Таким образом, реализация сетевого протокола маршрутизации предполагает разработку (или расширение) программной системы имитационного моделирования. Ожидаемые возможности такого средства: выбор или создание агентов (устройства, препятствия), задание параметров и проверка соответствия стандартам и рекомендациям, возможность записи алгоритмов и сценариев на специализированном упрощённом языке (сценариев или графическом), визуализация перемещения участников сетевого взаимодействия.

Стоит сделать ряд замечаний по поводу такого подхода к реализации протокола. Поскольку в ходе моделирования необходимо задать (выбрать или описать) формулу (статистику), необходимо разбираться в моделируемой предметной области, в которой происходит сетевое взаимодействие, для некоторых областей вероятен высокий уровень вхождения и сложность использования средства моделирования без консультаций аналитика или эксперта из предметной области. Поскольку обстоятельства в моделируемых ситуациях возникают из контекста, имитационная система должна быть достаточно интеллектуальной, чтобы соответствовать действительности и вполне вероятно, что какие-то аспекты реальности будут оставлены без внимания. В любом случае это только начальная стадия разработки, где моделирование происходит в упрощённой реальности взаимодействия агентов. И первые реализации протокола могут быть только прототипами, которые на начальном этапе своей работы должны собрать достаточно информации для построения профилей и продемонстрировать свою

способность в выборе оптимального алгоритма составления маршрутов. Всё это послужит базой для получения численных результатов оценки производительности при различных схемах и сценариях сетевого взаимодействия.

Заключение

В работе была рассмотрена проблема реализации протокола гарантированной доставки данных в ненадёжной среде передачи с точки зрения прослушивания и непостоянства топологии. В планах стоят задачи реализации протокола многопутевой маршрутизации и разработка программного клиента, который будет с помощью алгоритмов разделения секрета разделять потоки между несколькими выходными узлами сети и таким образом гарантировать доставку до места назначения, а сами алгоритмы разделения секрета помогут восстановить уничтоженные или потерянные данные. Описанный подход может быть применён для произвольной группы прокси-серверов.

Благодарности

Работа выполнена в рамках гранта НИОКТР № 01-06/683.

Литература

1. Сорокин А.А., Дмитриев В.Н. Описание систем связи с динамической топологией сети при помощи модели мерцающего графа // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2009. № 2. С.134–139.
2. Дулькейт В.И., Лавров Д.Н., Михайлов П.И., Свенч А.А. Анализ надёжности алгоритма разделения секрета в сетевых потоках // Математические структуры и моделирование. 2003. Вып. 12. С. 146–154.
3. Лавров Д.Н. Схема разделения секрета для потоков данных маршрутизируемой сети // Математические структуры и моделирование. 2002. Вып. 10. С. 192–197.
4. Сумцов Д.В., Евсеев С.П., Томашевский Б.П., Король О.Г. Эффективность обмена данными в компьютерной сети при различных способах управления обменом // Збірник наукових праць ДонІЗТ. 2009. № 17. С 33–45.
5. Файзуллин Р.Т., Щерба Е.В., Волков Д.А. Схема реализации параллельных вычислений как инструмент защиты обрабатываемых данных // Доклады ТУСУРа. 2014. № 2(32). С. 195–201.
6. Шувалов В.П., Вараксина И.Ю. Классификация методов многопутевой маршрутизации // T-COMM: Телекоммуникации и транспорт. 2014. Т. 8, № 1. С. 29–32.
7. Гусс С.В. Самоорганизующиеся mesh-сети для частного использования // Математические структуры и моделирование. 2016. № 4(40). С. 102–115.
8. Гусс С.В. Имитационное моделирование беспроводных самоорганизующихся сетей с быстро меняющейся топологией // Математическое и компьютерное моделирование : сборник материалов IV Международной научной конференции (Омск, 11 ноября 2016 г.) / [отв. за вып. И.П. Бесценный]. Омск : Изд-во Ом. гос. ун-та, 2016. 111–112 с.

APPROACHES TO IMPLEMENTING A SECURE DELIVERY NETWORK PROTOCOL FOR MULTIPATH DATA TRANSFER

S.V. Guss
Senior Teacher, e-mail: infoguss@gmail.com
D.N. Lavrov
Ph.D.(Eng.), Associate Professor, e-mail: lavrov@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The paper considers the problem of increasing the reliability of data transmission in a network with flickering nodes. Some comments are given on the development of algorithms for dividing the data flow and recovering lost data. We propose general considerations related to the implementation of the protocol for multipath routing in self-organizing dynamic networks.

Keywords: routing, secret sharing, data recovery, bandwidth, network fault tolerance.

Дата поступления в редакцию: 16.05.2018