УДК 004.5; 004.8; 007.85

ОРГАНИЗАЦИЯ ОТКАЗОУСТОЙЧИВОЙ МАРШРУТИЗАЦИИ ДАННЫХ В СЕТЯХ ДАТЧИКОВ

КУЗЕМИН А.Я., КЛИМОВ И.Н., ЛЕВЫКИН В.М.

Рассматриваются принципы организации отказоустойчивой маршрутизации данных, их недостатки при использовании в сетях датчиков, альтернативные алгоритмы реализации

1. Введение

Повсеместное развитие глобальной сети (Internet) привело к тому, что разработка эффективных протоколов организации маршрутизации данных стала вестись преимущественно в направлении обеспечения эффективного пиринга (обмена данными) между автономными системами сети Internet. Подобные исследования завершились разработкой протоколов BGP и OSPF [1] (так называемые link-state protocols- протоколы состояния линии), направленных на использование в компьютерных сетях. Однако зачастую проблема эффективного обмена данными возникает не только при использовании компьютеров, но и различного рода датчиков, работающих в автоновном режиме и передающие информацию согласно установленному графику. Подобная проблема особо актуальна в условиях, когда непосредственный доступ к этим устройствам невозможен, либо сопряжен со значительным риском. Одним из таких примеров является получение информации с устройств лавиноконтроля, размещенных на лавиноопасном склоне. Реализация вышеупомянутых протоколов значительно повышает требования к микропроцессорной части изделия, возможность же непосредственной связи с приемной станцией зачастую невозможна из-за особенностей рельефа. Используемая технология получения данных путем отправки их на летательный аппарат (зачастую беспилотный) имеет один существенный недостаток: именно частые вылеты могут стать одной из главных причин схода лавины.

Предметом исследования являются существующие протоколы организации маршрутизации, их преимущества и недостатки.

Задача – разработка алгоритма эффективной отказоустойчивой маршрутизации, применимого для реализации в системах с ограниченными вычислительными мощностями.

Для решения подобной проблемы предлагается использовать сеть из устройств, оснащенных маломощными (а значит дешевыми) радиопередатчиками и самоорганизующуюся для осуществления полной связности между устройствами.

2. Моделирование структуры сети

Моделирование – это устоявшаяся и общепринятая инженерная методика. Модель является упрощенным представлением реальности, в данном случае информационной сети. В общем – это визуальное и функциональное представление проектируемой системы, в котором учтены существенные и опущены малозначимые свойства системы на данном уровне абстракции. Модель может быть структурной, подчеркивающей организацию системы, или поведенческой, т.е. отражающей ее динамику. В разработанной системе моделирования и анализа сетей используется смешанная модель (модель структуры сети – размещение, топология и модель функционирования сети – маршруты прохождения информационных потоков и анализ устойчивости). Анализ структуры сети производится с использованием стека TCP/IP v4 и TCP/IP v6 как наиболее распространенных протоколов, обеспечивающих гарантированную доставку данных. Фактически, на данном этапе смоделированная сеть представляет собой граф (зачастую дерево), в котором каждая вершина – датчик или узел сети (управляемый свитч, коммутатор, сервер сети) – характеризуется максимальной пропускной способностью (0 для узлов сети с 1 связью), а также характером и типом создаваемого трафика; ребра же характеризуются пропускной способностью, скоростью и создаваемыми задержками.

3. Устойчивость сети

В разработанной системе под сбоем в сети понимается выход из строя одного из узлов сети или каналов связи, который вызывает нарушение маршрута прохождения информации. Система позволяет проверить поведение сети при подобных сбоях, провести анализ изменения информационных потоков и потери информации в сети. В процессе анализа может быть предложена альтернативная маршрутизация, либо изменение топологии сети. При проведении анализа также могут быть учтены различные характеристики линий связи, такие как длина, стоимость, сложность установки и т.д., что позволяет провести широкий комплекс моделирования функционирования сети и анализ на отказ в различных ситуациях.

Простейший пример моделируемого участка приведен на рис. 1.

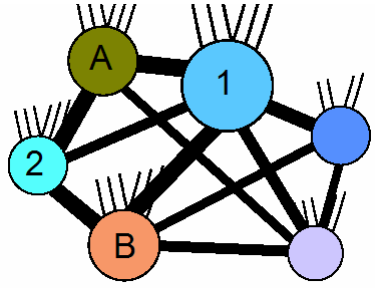

Рис. 1. Моделируемый участок сети

На рис. 1 приведена схема обмена трафиком абстрактной группы датчиков. Окружностями изображены

датчики и узлы сети (размер окружности соответствует максимальной пропускной способности), толщина линий соответствует емкости каналов между узлами. Как очевидно из рисунка, не все системы имеют возможность обмена трафиком между ними (это может быть связано как с отсутствием непосредственного прямого физического соединения, так и особенностями рельефа). Тем не менее, благодаря работе на всех узлах протоколов динамической маршрутизации, обеспечивается свободное прохождение трафика из системы в систему. Рассмотрим ситуацию, когда узел №2 так или иначе находится в зависимости от узла №1 (допустим узел №1 является геологической станцией, на которую узел №2 как и любой датчик обязан каждые заданные промежутки времени сообщать о состоянии окружающей среды). Так как наиболее распространенный протокол маршрутизации BGP стремится к минимизации количества узлов при транзите трафика, то будет использован прямой канал между узлами 1 и 2. В то же время использование транзитных точек A и B позволяет передавать большее количество данных в единицу времени. Для решения подобных проблем в протоколе BGP предусмотрено создание «виртуальных» узлов, искусственно удлиняющих путь между узлами [2]. Для соединения 1–2 необходимо дополнительное создание двух виртуальных узлов. При этом это соединение автоматически получит меньший приоритет, чем связи 1-A-2 и 1-B-2, так как они имеют на один транзитный узел меньше, чем новый наполовину «виртуальный» маршрут. К сожалению, поддержание подобных «виртуальных» маршрутов в актуальном состоянии – достаточно трудоемкая задача и требует от администраторов постоянного слежения за изменениями в структуре наблюдаемой сети, что невозможно, так как при тяжелых метеоусловиях (метель, сход лавины), положение датчиков, а соответственно структура сети могут изменяться ежесекундно. Система NetArchitect призвана автоматически контролировать подобные ситуации и вносить соответствующие изменения в таблицу маршрутизации оборудования при изменении структуры соединения узлов наблюдаемого региона. Также выполняется автоматическое переконфигурирование системы для достижения оптимального быстродействия при выходе из строя любого из каналов (не обязательно принадлежащих стартовому узлу), используемого для маршрутизации трафика.

Использование интеллектуальных методик маршрутизации также позволяет эффективно обрабатывать «эффект Нового года» [3]. Этот эффект получил свое название от планируемых сбоев в работе мобильных операторов, вызванных чрезвычайно высокой активностью абонентов в новогоднюю ночь. Однако, несмотря на предсказуемость этого явления, операторы не идут на увеличение мощности, поскольку содержание не используемых в иное время технических ресурсов на протяжении года нерентабельно для продавцов услуг. Для минимизации сбоев необходимо применение отказоустойчивых протоколов, способных с минимальными задержками оценивать уровень загрузки смежных узлов сети и корректировать маршрутизацию для улучшения качества связи. Согласованное координирование потоков данных нескольких смежных автономных систем позволяет с минимальными потерями снизить загрузку оборудования с критического уровня без введения в строй дополнительного резервного аппаратного обеспечения. При согласованной схеме координирования потоков приоритетным каналом по передаче данных текущего соединения становится наименее загруженный канал (при условии соответствия его заданным в системе параметрам качества). Применение подобного «жадного» алгоритма равномерно распределяет загрузку в узле и позволяет эффективно предсказывать объем входящих соединений по тому или иному каналу.

4. Безопасность сети и ограничение доступа

Исключая из рассмотрения вопросы безопасности отдельных узлов сети, нельзя не рассматривать также вопрос безопасности сети в целом. При выходе из строя сетевой подсистемы любого узла возможно создание паразитного трафика, результатом которого может стать нарушение нормального функционирования сети. Способность сети противостоять «атакам» такого рода заключается не в обеспечении эффективной связности между узлами при отказе тех или иных соединений, а в способности спроектированной сети эффективно выделять паразитный трафик и отключать его. Подобное ограничение доступа осуществляется с помощью создания профилей соединений, в которых хранится характерный для данного узла тип трафика, количественное соотношение принятой/переданной информации, а также пиковые значения загрузок подобных систем. Эти профили строятся автоматически на основе информации об использовании сервисов за прошедшее время. Также возможно их автоматическое создание на основе приписанных прав DMZ (демилитаризованной зоны), в которую выносятся ресурсы (пример: сервер метеостанции), которые должны быть доступны из интернета. Таким образом производится автоматическое разделение спроектированной сети на три зоны – внутренняя сеть (не доступна из Интернет, доступ в Интернет контролируется и лимитируется ресурсами демилитаризованной зоны), демилитаризованная зона (ресурсы доступны из Интернет, контроль доступа производится ресурсами внешней сети) и внешняя сеть (располагается обычно 1 ресурс с максимальными настройками безопасности и осуществляющий контроль доступа во внутреннюю сеть) [3]. Таким образом возможно автоматическая передача метеостанцией обработанных данных через Интернет, не подвергая сомнению достоверность этих данных (т.к. датчики находятся в недоступной из интернет зоне).

5. Анализ устойчивости структуры сети. Алгоритм альтернативной маршрутизации

При построении структуры сети представляется интересным моделирование сбоев участков сети и анализ

устойчивости работы сети при выходе из строя некоторых каналов связи. В данной статье предлагается один из вариантов поиска альтернативных путей при обрыве канала связи, с целью полностью перенаправить поток данных. Целью данного анализа является не алгоритм маршрутизации при функционировании сети, а моделирование сбойной ситуации и проверка возможности существования альтернативного пути на стадии проектирования с возможностью визуально отследить такой процесс.

В качестве разрывов будем рассматривать выход из строя канала связи между двумя подсетями.

Представим сеть в виде графа $G=(X,E)$, где $X=\{x_i\}, i=\overline{1,n}$ – множество вершин графа, в данном случае подсетей по TCP/IP классификации; $E=\{(i,j,q)\}$ – множество дуг – каналов связи, соединяющих подсети x_i и x_j, а q – показатель качества данного канала связи. Для больших сетей этот показатель качества обычно рассчитывается как $q=k_1S/p-k_2D(1+l/100)$, где S – скорость данного канала связи, p – совокупная стоимость владения активным каналом, D – средняя задержка прохождения пакетов в этом канале, l – процент потерь пакетов при их прохождении через этот канал. Варьируя коэффициенты k_1 и k_2 возможно получить различные классические политики предоставления услуг доступа в глобальную сеть. Так для физических лиц k_2 обычно приравнивают к 0, таким образом жертвуя качеством связи в обмен на использование максимально дешевых каналов передачи. Для клиентов, требующих повышенного качества связи (видеоконференции, потоковое видео, онлайн-игры) $k_2>>k_1$, гарантируя таким образом передачу данных без потерь. Для маршрутизатора подсети x_i задана таблица маршрутизации $RX_i=\{(x_j,x_k)\}$, где $x_j, j=\overline{1,n}$ – маска подсети направления потока, $x_k, k=\overline{1,n}$ – адрес подсети, на которую перенаправляется поток, адресованный на x_j.

Разрыв канала связи представляется как неработоспособность дуги (i,j).

Определяется наличие маршрутов через неработоспособный канал связи, т.е. наличие пар $(x_k,x_j)\in RX_i, k\in(1,n)$ либо пар $(x_m,x_i)\in RX_j, m\in(1,n)$. Отсутствие таких пар будет означать, что через данный канал не проходят потоки данных и разрыв не скажется на работоспособности сети при выбранной топологии.

Теперь допустим, что на множестве RX_i найдено несколько пар

$$\overline{RX_i}=\{(x_k,x_j)\}, \qquad (1)$$

где x_k принадлежит непустому подмножеству $\overline{X}\subset X$. Это означает, что существует определенный поток данных, проходящий через канал связи (i,j).

Дуга (i,j) исключается из множества E. Затем на графе одним из способов поиска кратчайшего пути между вершинами находится путь от вершины x_i к вершине x_j. Отсутствие такого пути означает, что для данного информационного потока при данном разрыве невозможна доставка данных и необходимо перестраивать структуру сети для обеспечения альтернативного пути.

Пусть найдены альтернативные пути

$$\begin{aligned} x_{l_1}&=x_i,x_{i_2},x_{i_3},\ldots,x_{i_{k-1}},x_{i_k}=x_i,\\ x_{l_2}&=x_j,x_{j_2},x_{j_3},\ldots,x_{j_{k-1}},x_{j_k}=x_j. \end{aligned} \qquad (2)$$

Каждый найденный путь характеризуется показателем качества связи q, вычисляемого как $q_l=\min(q_1,q_2,\ldots,q_{n-1},q_n)$, где $q_1\ldots q_n$ – качества путей между вершинами, входящими в альтернативный путь. Путем нахождения максимального показателя q для всех альтернативных путей выбирается оптимальный путь прохождения поток. Для обеспечения его прохождения в направлении $\overline{X}$ через оптимальный путь из (2) обеспечивается добавлением в таблицы маршрутизации $RX_{l_j}, j=\overline{1,k-1}$ для каждой вершины из (2) пар $(a,x_{l_{j+1}})$, $\forall a\in\overline{RX_i}$. При этом пары вида $(a,b), b\in X$ удаляются из RX_{l_j}.

6. NetArchitest

Результатом исследования данной проблемы была разработка автоматизированной системы организации маршрутизации NetArchitest. Система представляет собой графическую среду визуального проектирования сетей датчиков. Процесс оптимизации маршрутизации состоит из двух стадий. На стадии построения структурной модели сети производится размещение объектов сети на модели реального склона и их связывание с указанием соответствующих параметров объектов и линий связи.

Типичный пример структуры сети показан на рис. 2.

Рис. 2. Схема сети

Следующим шагом является анализ динамики системы.

Исходя из построенной конфигурации, производится автоматическое назначение таблиц маршрутизации, после чего запускается процесс симуляции работоспособности сети. В соответствии с заданными характеристиками, программа моделирует передачу данных между узлами. В случайные моменты времени моделируется отказ того или иного участка сети и производится (если возможно) автоматическая корректировка маршрутизации для обеспечения качества. Для каждого узла сети ведется учет качества прохождения пакетов, пример которого можно увидеть на рис.3.

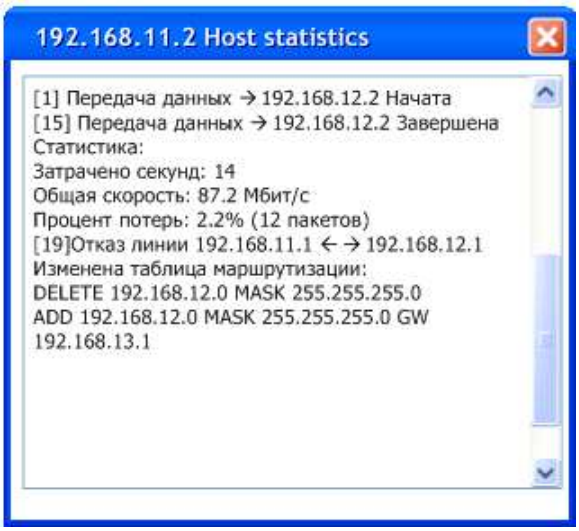

Рис. 3. Статистика по узлу сети

В нем можно видеть статистику передачи данных между узлами сети, а также изменения таблиц маршрутизации, вносимые интеллектуальным модулем. На рис. 4. Виден общий журнал системы, позволяющий отслеживать динамику работы сети. По нему возможно принятие решений о размещении дополнительных датчиков в той или иной зоне для обеспечения связности сети, а также оценка возможного влияния схода лавины на том или ином участке на работу общей сети датчиков.

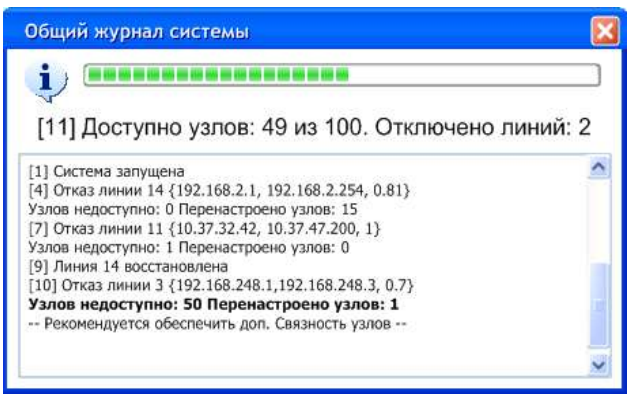

Рис. 4. Общий журнал системы

7. Выводы

Применение данной системы в процессе построения сети снижает общее время процесса, сокращая переход от проектирования структуры к непосредственно физическому построению сети. Моделирования и анализ поведения сети позволяет сократить будущие эксплуатационные затраты. Перестроив структуру сети на этапе моделирования, проанализировав информационные потоки и сбойные ситуации, можно избежать больших затрат в будущем.

Научная новизна: предложен алгоритм оценки альтернативной маршрутизации, применимый к использованию во встраиваемых устройствах и датчиках, построена система моделирования его работы.

Практическое значение работы: Разработанное программное обеспечение позволяет оценить работу сети датчиков в том или ином регионе, принять меры по улучшению качества и скорости потока получения данных на конечной станции.

Литература: 1. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД «ДС», 2001. 688с. **2.** *Shullzrinne H., et al* Link-state protocols overview // RFC 1692, Internet Engineering Task Force, Jul. 2002, 71p. **3.** *Самойленко В.И.* Атаки на отказ в обслуживании в компьютерных сетях Спб. «Вильямс», 2007. 343с.

Поступила в редколлегию 12.09.2007

Рецензент: д-р техн.наук, проф. Сироджа И.Б.

Климов Илья Николаевич, студент ХНУРЭ. Научные интересы: информационная безопасность, искуственный интеллект, отказоустойчивые системы. Адрес: Украина, 61189, Харьков, ул. Мира, 118, 55, тел: 99-28-55.

Куземин Александр Яковлевич, канд. техн. наук, проф. кафедры информатики, начальник инновационно-маркетингового отдела ХНУРЭ. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел.: 8 (057) 702-15-15, e-mail: kuzy@kture.kharkov.ua.

Левыкин Виктор Макарович, д-р техн. наук, проф., зав. кафедрой ИУС ХНУРЭ. Научные интересы: разработка информационно-управляющих систем. Адрес: Украина, 61166 Харьков, пр. Ленина, 14, тел.: 8 (057) 702-15-15, e-mail: ius@kture.kharkov.ua.