МОДЕЛЬ ОЦЕНКИ ВВЕДЕНИЯ ЭЛЕМЕНТОВ БЕЗОПАСНОСТИ В СЕТЕВЫЕ ПРОТОКОЛЫ С ТОЧКИ ЗРЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ

В.Ю. Сакович, В.В. Пытляк
Беларусь, г. Минск

В сетевой отрасли все большее распространение получает термин «безопасность сетей». Изучая довольно сложный механизм системы обеспечения безопасности современных сетей, нельзя не задаться вопросом: какое влияние оказывают эти многочисленные процедуры на производительность сетевых устройств, какую часть ресурсов сети они потребляют и как это сказывается на ее пропускной способности?

В обычном плане выделяют показатели производительности на основе двух подходов:

1. Через продуктивность системы. Определяется через число отработанных в единицу времени, усредненных либо классифицированных по типу сообщений.

2. Распределение времени отклика системы на различных этапах обслуживания сообщения (заявки).

Под затратами производительности сетевых устройств на обеспечение безопасности будем понимать ту составляющую коэффициента использования устройства, которая приходится на выполнение элементов безопасности, включенных в алгоритмы обслуживания (протоколы) заявок, обслуживаемых данным устройством.

Реальные сложные системы, к которым относятся и телекоммуникационные, можно исследовать с помощью аналитических либо имитационных моделей. В аналитических моделях поведение системы записывается в виде некоторых функциональных соотношений или логических условий. Однако достаточно полное исследование не удаётся провести, если не известны явные зависимости искомых величин от параметров системы. [1]

Явления в телекоммуникационной системе с интеграцией сервисов настолько сложны и многообразны, что аналитические модели для неё становятся слишком грубым приближением к действительности. Поэтому без моделирования происходящих в них процессов просто не обойтись. [2]

Будем исходить из того, что разрабатываемая модель будет использована на этапах жизненного цикла системы, таких как индивидуальное проектирование, эксплуатация и контроль качества функционирования.

На этапе индивидуального проектирования необходимо определить трек развития сети, как по функциям, так и по количественным показателям, что возможно только с помощью моделирования.

Разработка общего формализованного описания

Исходной информацией при построении математической модели функционирования системы служат данные о назначении и условиях её работы. При использовании модели функционирования в первую очередь встаёт вопрос об адекватности описания в виде конкретных схем реальных процессов в исследуемой системе, а не о возможности получения ответа на конкретный вопрос исследования. Схему динамики системы (модель функционирования) можно рассматривать как звено при переходе от содержательного к формальному описанию процесса функционирования системы, т.е. имеет место цепочка «описательная модель – модель функционирования – имитационная модель».

Таким образом, встаёт вопрос о выборе некоторой модели описания функционирования системы. Такой моделью был выбран транзактный способ описания.

В нашем случае модель, построенная на использовании транзакций, очень удобна, поскольку она не рассматривает чётко оформленные элементы в программном или аппаратном исполнении, то есть позволяет проводить произвольное разбиение системы по структурным единицам. Таким образом, с помощью данного подхода мы можем обобщённо описывать сервис, и предоставляющие его протоколы. Работа телекоммуникационной системы, по сути своей, заключается в обработке запросов, которые, имеют естественную транзактную природу.

Концептуальная модель.

Общее формализованное описание телекоммуникационной системы может быть многоуровневым, поскольку наш моделируемый «чёрный ящик» представляет собой всю сеть, а не отдельные сетевые устройства.

Второй уровень спецификации – переход к алгоритму описания функционирования. Для этой цели наиболее подходит транзактный тип формализованного описания.

Путём уточнения деталей, а точнее благодаря описанию сервиса на разных уровнях, мы сужаем «чёрный ящик» до тех пор, пока он сам, наконец, сможет быть описан с помощью параметризуемых элементов, а из характеристик самой системы удастся получить реальные параметры этих элементов формализованного описания. Таким образом, мы заменяем элементы описания сервиса этими параметризуемыми элементами, после чего появляется возможность моделировать систему с применением данных элементов.

К характеристикам телекоммуникационной системы в данном случае относятся её ресурсы (производительность, буфера памяти, пропускная способность), данные, полученные с использованием средств мониторинга, и технические данные и показатели, характеризующие сетевые устройства, входящие в систему. Многие из этих характеристик сетевых устройств можно найти в их технических паспортах.

Задержки в передаче по каналу, при асинхронном режиме приема/передачи зависят от его пропускной способности и имеют распределение, свойственное распределению длины поля данных в передаваемом блоке информации (сегмент для транспортного уровня, пакет для сетевого уровня, кадр для канального уровня). При синхронном режиме к вышеназванным задержкам может добавиться время ожидания поступления сигнала синхронизации.

Для определения задержек в сетевых устройствах будем исходить из следующих предположений. Известны характеристики компонентов процессорного типа; механизмы распределения ресурсов производительности специализированной операционной системы и времена выполнения алгоритмов, реализующих протокольные блоки данных. Почти все сетевые устройства реализуются в виде многопроцессорных комплексов: макроконвейер с векторным параллелизмом на некоторых стадиях конвейера (например, параллелизм микропроцессоров на портах сетевых устройств). Разрабатываемая модель должна содержать элементы распределения нагрузки на компоненты сетевого устройства и механизмы диспетчирования программ в отдельно взятых устройствах с учетом приоритетности, как обслуживаемых заявок (транзакций), так и самих программ. Необходимо предусмотреть описания механизмов расщепления и слияния транзакций. Вышестоящий протокол иногда требует от нижних уровней повторения по одному алгоритму операций над более мелкими фрагментами данных, поэтому транзакцией необходимо предусмотреть возможность реализации цикла для некоторых участков алгоритмов (протоколов). Если связь между стадиями конвейера осуществляется через общую память возможно замедление в выполнении программ процессора работающих в данной общей памяти (эффект замедления из-за общей памяти). С учетом сказанного, далее будет предложена формализация модели с параметризацией отдельных элементов формализации.

Как было отмечено ранее, одной из составляющих качества обслуживания является безопасность. Поэтому часть нагрузки на систему будут выполнять транзакции, связанные с обеспечением безопасности.

Объект моделирования представляет собой группу процессоров. В каждой группе K процессоров, $K_i = \overline{1, K^*}$, где K^* - максимально возмож-

ное количество процессоров в группе. При K_i=1 группу будем обозначать ЦПР.

Каждый из процессоров характеризуется следующими параметрами: вложенным ресурсом производительности и реализованной в нём дисциплиной диспетчирования. Вложенный ресурс производительности в данной модели задается через времена выполнения функциональных программ цепочки. Такое задание возможно только при статическом разделении нагрузки. В программе по сетевому устройству разделение нагрузки по группам – статическое. Задание вложенного ресурса производительности в виде времен выполнения функциональных программ удобно и в том смысле, что позволяет использовать результаты измерений на реально функционирующих системах.

Описание процесса функционирования модели должно включать как описание прохождения отдельной заявки в программе по сетевому устройству в соответствии с последовательной цепочкой обслуживания (транзакцией) заявок данного типа, так и совместное обслуживание заявок.

В соответствии с принятым подходом обслуживание заявки состоит в выполнении ряда последовательных процессов, задаваемых цепочкой обслуживания. Транзакция состоит из элементов нескольких типов, различные варианты перестановок из которых позволяют задавать схемы обслуживания для любой из транзакций. Количество элементов в ней может быть произвольным, количество типов элементов - ограничено. Охарактеризуем типы элементов транзакции и параметры процессов, задаваемых ими.

«Протокольный блок данных» (ПБД). Использование данного элемента наиболее предпочтительно в таком варианте, когда ему соответствует реальная программа в сетевом устройстве (СУ), подвергающаяся диспетчеризации на одном из процессоров комплекса. До перехода на выполнение этого элемента транзакции обслуживания каким-то образом должен быть задан номер процессора, на котором программа должна выполняться. Выполнение ПБД заключается в занятии процессора на время, являющееся характеристикой программы и процессора. При приоритетной дисциплине диспетчирования ПБД имеет ещё один параметр. Каждое назначение - ПБД на процессор можно считать актом диспетчирования, поэтому в модели в этом месте производится учёт затрат на диспетчирования.

«Повтор участка транзакции» (ПУТ). Данный элемент сам по себе ресурс процессора не использует. Его назначением является повторение уже пройденного участка транзакции обслуживания заданное число раз.

Введение элемента ПУТ в системах связи отражает одну из их особенностей, а именно: заявка на выполнение фазы иногда может быть сформирована только после приёма некоторого числа двоичных знаков, а на обработку одного двоичного знака существуют временные ограничения, которые необходимо оценивать на моделях.

«Расщепление» (РАСЩ.) Элемент означает, что определенный участок последовательной транзакции превращается в некоторое множество параллельных идентичных процессов. Параметры элемента: количество размножаемых элементов цепочки после РАСЩ; количество размноженных процессов.

«Слияние» (СЛ) Состоит в том, что несколько последовательно поступающих сообщений объединяются в одно. Параметр элемента – количество объединяемых сообщений.

«Задержка» (ЗА,ЗП). Ресурс процессора этим элементом также не потребляется. Элемент позволяет учитывать задержки, как прогнозируемые алгоритмом обслуживания, так и задержки, связанные с принятой в СУ организацией вычислительного процесса. Задание схемы обслуживания только с помощью перечисленных выше элементов позволяет описывать только асинхронный СУ: в транзакциях обслуживания нет элемента, позволяющего искусственно упорядочивать заявки во времени. Таким элементом может быть «ЗАДЕРЖКА». При этом возможны два варианта задержки: задержка активная (ЗА) и задержка пассивная (ЗП). Для элемента ЗА определено время, через которое заявка выйдет из состояния задержки по отношению к моменту входа в неё. Для ЗП момент выхода из состояния задержки определяется посторонним источником, например, первым сигналом таймера. Итак, для ЗА задается интервал времени, для ЗП - имя (номер) источника, первый же сигнал из которого заканчивает процесс задержки.

«Однопроцессорная фаза» (ОФ). Элемент не требует ресурса процессора. Он означает, что следующий за ним участок транзакции будет относиться к одиночному на данной фазе макроконвейера процессору.

«Многопроцессорная фаза» (МПФ). Элемент означает, что следующий за ним участок транзакции относится к одному из процессоров группы.

Логика работы программы состоит в генерации переменного транзакций для каждого из видов сервиса, при этом подробная транзакция (транзакция 1) условно отображает последовательность обслуживания запроса сервиса с элементами безопасности. Обобщенная (короткая транзакция 2) характеризует суммарную нагрузку сервисов без обеспечения безопасности. Моделирование транзакций состоит в выполнении

элементов транзакций с учетом параметров, присвоенных каждому из элементов.

Логика работы программы состоит в генерации переменного транзакций для каждого из видов сервиса, при этом подробная транзакция (транзакция 1) условно отображает последовательность обслуживания запроса сервиса с элементами безопасности. Обобщенная (короткая транзакция 2) характеризует суммарную нагрузку сервисов без обеспечения безопасности. Моделирование транзакций состоит в выполнении элементов транзакций с учетом параметров, присвоенных каждому из элементов.

Заключение

1) Элементы обеспечения безопасности являются составными частями сетевых протоколов, что приводит нас к необходимости оценки производительности сетевых устройств.

2) Разработано общее формализованное описание действующих сетевых протоколов с элементами безопасности, произведен их сравнительный и функциональный анализ.

3) Предложена модель, основанная на использовании механизма транзакций для описания функционирования системы, причём свойство вложенности транзакций позволяет строить многоуровневое описание системы. Точками вложения транзакций являются сервисные точки доступа протокольных уровней.

4) Разработана концептуальная модель нагрузки создаваемой сетевыми протоколами, основанная на переходе от автоматной спецификации протоколов к модели в виде транзакции. На основе ее предложена формализованная модель для оценки затрат производительности на выполнение функций обеспечения безопасности, реализована в виде имитационной модели на языке моделирования GPSS.

5) Последнее, в свою очередь, даст нам возможность прогнозировать необходимый минимум производительности для обеспечения заданного уровня безопасности.

Литература

1. ISO/IS 8509. Information Processing Systems. Open System Interconnection. Basic reference model.

2. Кульгин М. Технологии корпоративных сетей. Энциклопедия – СПб.: Издательство «Питер», 1999. – 704 с.: ил.