ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ШИРОКОВЕЩАТЕЛЬНЫХ КАНАЛАХ СВЯЗИ

М. В. Костин, А. В. Костина (Санкт-Петербург)

Введение

По оценкам большинства специалистов наметившийся в последние годы интерес к использованию широковещательных каналов связи в различных телекоммуникационных приложениях должен привести в ближайшее время к существенному росту рынка телекоммуникационных услуг, основанных на использовании спутниковых, эфирных и кабельных цифровых сетей связи. В частности, эта тенденция обусловлена возможностью трансляции в одном цифровом широковещательном канале связи множества дифференцированных информационных сервисов, отличающихся типом информации, требованиями к пропускной способности канала связи, задержкам передачи, качеству обслуживания и т.д. Например, в одном спутниковом, эфирном или кабельном канале связи стандарта DVB [5, 6], может одновременно передаваться несколько цифровых телеканалов, радио, ретранслируемый трафик сети INTERNET, программное обеспечение, сервисная информация [4]. Актуальность развития данного направления в России становится особенно очевидной в свете заявленной правительством РФ программы повсеместного перевода общенационального эфирного телевидения в цифровые форматы. По мнению многих аналитиков и экспертов в области цифровых телекоммуникаций существует несколько объективных причин, существенно ограничивающих темпы развития данного направления. К основным проблемам относятся: сложность и высокая стоимость проектирования и обслуживания систем с различным видом трафика, защита передаваемых сервисов от несанкционированного доступа, обеспечение конфиденциальности передаваемой информации. В большинстве своём, эти проблемы обусловлены такими особенностями спутниковых, эфирных и кабельных каналов связи, как большая зона покрытия и большое число потенциальных пользователей, общедоступность передаваемой информации, вероятностный характер трафика, сложность, а иногда невозможность организации обратного канала связи.

Классификацию информационных сервисов в данном случае целесообразно проводить, во-первых, по чувствительности к задержкам передачи и, во-вторых, по требованию к конфиденциальности (рис. 1).

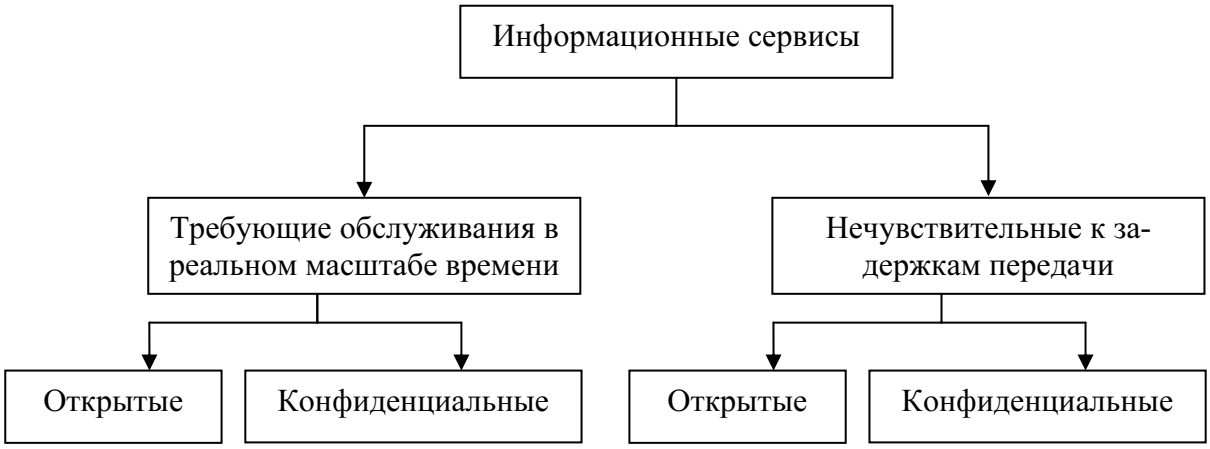

Рис. 1. Классификация информационных сервисов

Решение проблем обеспечения конфиденциальности передаваемой информации и защиты информации от несанкционированного доступа является основной задачей систем условного доступа (СУД) [3]. Эффективность функционирования таких систем во многом зависит от качества и оптимальности реализованных методов и алгоритмов передачи и приёма сервисной информации. В свою очередь, эффективность использования каналов связи для передачи информационных сервисов зависит от качества системы условного доступа, обслуживающей данный канал.

При проектировании и разработке новых СУД, а также при исследовании и оптимизации существующих систем широко применяются как аналитические модели, основанные на математическом аппарате теории массового обслуживания и теории вероятности, так и методы и средства имитационного моделирования. Основным достоинством имитационной модели является отсутствие ряда допущений, свойственных аналитическим моделям. В частности, существует возможность варьирования закона и параметров распределения интервалов времени между поступлениями пакетов на вход системы и распределения длительности обслуживания пакетов в узлах системы без серьёзного усложнения модели. Кроме того, существенными преимуществами имитационных моделей являются простота изменения дисциплин обслуживания и возможность определения функций распределения длин очередей.

Имитационная модель системы передачи конфиденциальной информации в широковещательном канале связи может применяться для решения достаточно широкого круга задач. При проектировании СУД большое значение имеет определение необходимой производительности узлов системы, требуемого размера оперативной памяти, определяемого максимально возможной длиной очередей, среднего времени задержки, вносимой СУД, при заранее известных параметрах внешнего воздействия. Также актуальна обратная задача определения предельных значений параметров входящего транспортного потока при известных значениях основных характеристик системы.

Разработка имитационной модели

Концептуальная модель системы передачи конфиденциальной информации (рис. 2) состоит из двух взаимосвязанных узлов M_1 и M_2, выполняющих, соответственно, функции шифрования транспортного потока и выравнивания скоростей (алгоритм «дырявого ведра» [2]).

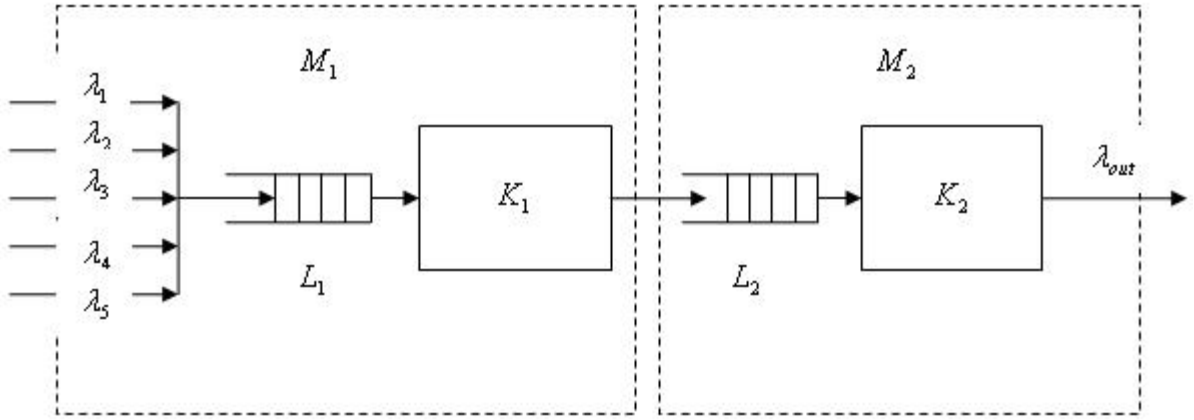

Рис. 2. Концептуальная модель системы

В соответствии с классификацией информационных сервисов (рис. 1), предположим, что на вход системы поступают транспортные пакеты, принадлежащие информационным сервисам четырёх классов. Пятый поток образуют заявки на смену ключей,

участвующих в процессе шифрования. Необходимо отметить, что в нормальном режиме функционирования системы сумма интенсивностей поступления пакетов четырёх классов не должна превышать отношение пропускной способности канала связи V_{ts} (б/с) к размеру транспортного пакета S_{tp} (Б) (1).

$$\sum_{i=1}^{4} \lambda_i \le \frac{V_{ts}}{S_{tp} * 8} \qquad (1)$$

Для транспортных пакетов, принадлежащих группе стандартов DVB, размер пакета S_{tp} = 188 байт, а пропускная способность канала связи $V_{ts} \le 100$ Мбит/с.

Заявка i-го класса может быть однозначно определена совокупностью четырёх исходных параметров: интенсивностью поступления заявок в систему λ_i (1/с), длительностью обслуживания заявки в устройстве K_1 ν_i (с), приоритетом заявки pr_i и длительностью обслуживания заявки в устройстве K_2 ν_{k2} (с).

В качестве основных исследуемых характеристик определим следующие:

– задержка, вносимая системой шифрования в передачу транспортного потока и выражаемая полным временем нахождения транспортного пакета, требующего шифрования в подсистеме, T_{delay} (с);

– пропускная способность подсистемы, C (пакетов/с);

– требуемый объём оперативной памяти, R (байт).

Для удобства и точности разработки имитационной модели представим алгоритм функционирования системы в виде диаграммы состояний (рис. 3).

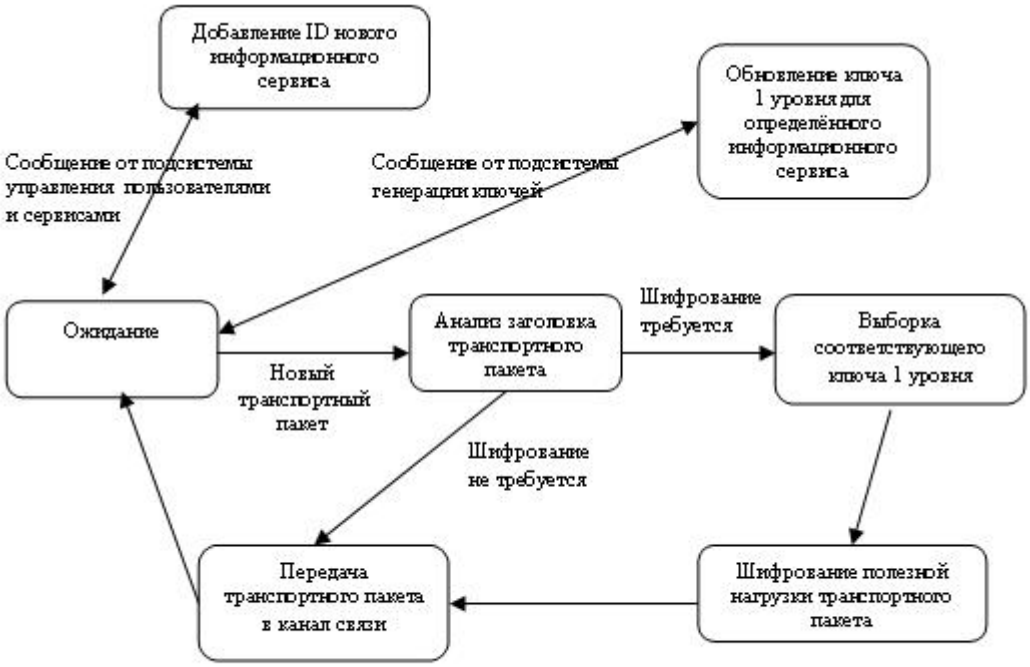

Рис. 3. Диаграмма состояний системы шифрования информационных сервисов

В качестве основного инструмента моделирования воспользуемся пакетом GPSS World, сочетающим в себе простоту и возможности универсальной системы имитационного моделирования с возможностью интеграции в модель функций и библиотек, реализованных на языках программирования высокого уровня. При планировании экс-

периментов зададим минимальную единицу времени (time unit), равную 1 мкс, и моделируемое время проведения эксперимента, равное 7 дням, что обусловлено пульсирующим характером трафика некоторых информационных сервисов в зависимости от дней недели. Исходные данные для моделирования (табл. 1) получены на основе сбора и анализа статистической информации в реальном спутниковом канале связи с параметрами: спутник Eutelsat W4, частота 12456 Мгц, левая поляризация, FEC 3/4, пропускная способность 38 Мбит/с. В качестве алгоритма шифрования применяется метод CSA (Common Scrambling Algorithm) [7], реализованный на вычислительной платформе на базе процессора INTEL PENTIUM IV с тактовой частотой 1,8 ГГц под управлением ОСРВ VxWorks. Предположим, что интервалы времени между поступлениями пакетов i-го класса распределены по экспоненциальному закону с параметром распределения τ_i (мкс) (2). Также по экспоненциальному закону распределены длительности обслуживания пакетов в устройствах с параметрами распределения ν_i (мкс) и ν_{k2} (мкс) соответственно:

$$\tau_i = \frac{1}{\lambda_i} * 10^6. \qquad (2)$$

Таблица 1

Параметры моделирования

Класс заявки	λ_i (1/с)	τ_i (мкс)	ν_i (мкс)	pr_i	ν_{k2} (мкс)
1	17854	56	36	1	7
2	461	2169	3	1	7
3	6118	163	36	0	7
4	931	1074	3	0	7
5	2	500000	155	2	7

Результаты экспериментов и верификация модели

Для верификации разработанной модели сравним результаты экспериментов на имитационной модели и результаты экспериментов на реальной системе передачи конфиденциальной информации фирмы General Satellite при условии одинаковых исходных параметров. Целью экспериментов является определение таких характеристик системы, как среднее время нахождения пакетов в системе μ_{mean}, эквивалентное средней задержке пакета в системе T_{delay}, среднеквадратичное отклонение времени нахождения σ_μ, максимальное время нахождения пакета в системе $\mu_{\max}$, средняя длина очереди L_1 q_{L1}, среднеквадратичное отклонение длины очереди L_1 σ_{L1}, максимальная длина очереди L_1 $q_{\max L1}$, средняя длина очереди L_2 q_{L2}, среднеквадратичное отклонение длины очереди L_2 σ_{L2}, максимальная длина очереди L_2 $q_{\max L2}$. Необходимо отметить, что характеристики очередей имеют важное значение, так как используются для определения минимального объёма оперативной памяти *R* (3):

$$R = (q_{L1} + \sigma_{L1} + q_{L2} + \sigma_{L2}) * S_{tp}. \qquad (3)$$

Для оценки погрешности результатов моделирования воспользуемся формулой (4):

$$\Delta = \frac{\left| x_{real} - x_{model} \right|}{x_{real}} * 100\% , \qquad (4)$$

где x_{real} – значение характеристики после экспериментов на реальной системе, x_{model} – значение характеристики после экспериментов на модели. Результаты экспериментов для временных характеристик – в табл. 2, для характеристик очередей – в табл.3.

Таблица 2

Результаты экспериментов (временные характеристики)

Класс пакета	Model μ_{mean} мкс	Real μ_{mean} мкс	Δ %	Model σ_μ мкс	Real σ_μ мкс	Δ %
1	132	111	18	107	72	48
2	103	98	5	102	76	34
3	711	698	2	907	663	36
4	682	662	3	903	610	48
Общее	291	270	8	551	278	98

Таблица 3

Результаты экспериментов (характеристики очередей)

Очередь	Model q_{mean}	Real q_{mean}	Δ %	Model σ_q	Real σ_q	Δ %	Model q_{max}	Real q_{max}	Δ %
L_1	7	6	16	8	5	60	88	51	72
L_2	1	1	0	1	1	0	11	6	83

Анализ результатов экспериментов показывает, что погрешность средних значений характеристик находится в допустимых пределах (0 ~ 18 %), в то же время девиация среднеквадратичных отклонений и предельных характеристик может составлять значительную величину, причём значение реальных характеристик всегда меньше модельных характеристик. Это связано, в первую очередь, с допущением об экспоненциальном характере входящего трафика и об экспоненциальном распределении длительности обслуживания пакетов в устройстве. Однако очевидно, что полученные модельные характеристики всегда «хуже» реальных, следовательно, системы, разрабатываемые на базе данной модели, будут иметь дополнительный запас прочности. Таким образом, можно сделать вывод об адекватности предложенной имитационной модели реальной системе.

Необходимо отметить такое преимущество имитационной модели, как возможность построения гистограмм распределения случайных величин. В частности, можно построить гистограмму распределения числа пакетов в очереди (рис. 4), определив тем самым соответствующий закон распределения и такие характеристики, как математическое ожидание и среднеквадратичное отклонение числа пакетов, ожидающих обслуживания, что бывает крайне затруднительно вычислить при аналитическом моделировании.

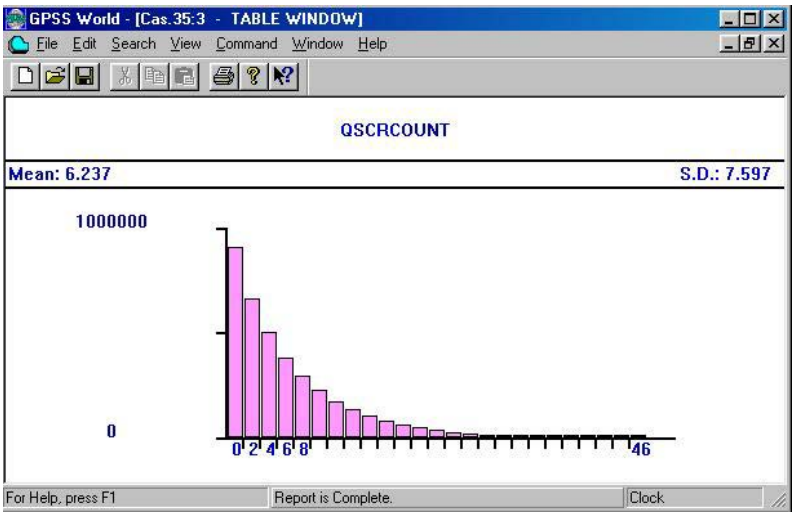

Рис. 4. Гистограмма распределения числа пакетов в очереди L_1

Выводы

В данной работе была продемонстрирована возможность применения методов и средств имитационного моделирования для решения задач анализа и синтеза систем передачи конфиденциальной информации в широковещательных каналах связи. Была разработана и исследована модель системы, позволяющая определить ряд характеристик, интересующих разработчиков и пользователей. Основной особенностью данной модели является простота её адаптации к различным исходным условиям, возможность варьирования большинства параметров и моделирования внешнего воздействия. Приведённая реализация модели позволяет определить такие характеристики системы, как средние задержки пакетов разных классов в системе, требуемый объём оперативной памяти и производительность системы. Результаты проведённой процедуры верификации модели позволяют сделать вывод о достаточной степени адекватности модели реальной системе.

Литература

1. **Альянх И.Н.** Моделирование вычислительных систем. – Л.: Машиностроение, 1988.
2. **Столлингс В.** Современные компьютерные сети. – СПб.: Питер, 2003.
3. **Костин М.В.** Системы условного доступа//Телеспутник. – 2004. – № 11.– С. 62–64.
4. **Костина А.В.** Что такое ОТА//Телеспутник. – 2004. – № 12. – С 54–57.
5. ETSI EN 300 421 v 1.1.2:1997 Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz satellite services, ETSI, 1997.
6. ETSI EN 300 468 v1.4.1:2000 Digital Video Broadcasting (DVB); Specification for Services Information (SI) in DVB systems, ETSI, 2000.
7. ETR 289:1996 Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA), ETSI, 1996.