

указать число шагов, приводящих к разделению. К сожалению, это является общим недостатком большинства известных методов построения линейной дискриминантной функции [1-5].

**Литература:** 1. *Биргер И.А.* Техническая диагностика. М.: Машиностроение, 1978. 239 с. 2. *Фор А.* Восприятие и распознавание образов. М.: Машиностроение, 1989. 271 с. 3. *Фукунага К.* Введение в статистическую теорию распознавания образов. М.: Наука, 1979. 368 с. 4. *Ту Дж., Гонсалес Р.* Принципы распознавания образов. М.: Мир, 1978. 412 с. 5. *Якунин А.В.* Кусочно-линейные процедуры диагностики: достижения и проблемы // Коммунальное хозяйство городов. 1998. Вып. 16. С. 129-135. 6. *Горелик А.Л., Гуревич И.Б., Скрипкин В.А.* Современное состояние проблемы распознавания: Некоторые аспекты. М.: Радио и связь, 1985. 161 с. 7. *Алберт А.* Регрессия, псевдо-

инверсия и рекуррентное оценивание. М.: Наука, 1977. 223 с. 8. *Bierman G.J.* Factorization methods for discret sequential estimation. N. Y.: Academic Press, 1977. 241 p.

9. *Регуляризованные  $U^T D U$ -факторизации симметричных матриц и их применение/ В.И. Мелешко, В.М. Задачин, Т.В. Ткаченко, И.Ф. Шматько.* К.: Ин-т кибернетики, 1986. 28 с.

Поступила в редколлегию 21.07.99

**Рецензент:** д-р техн. наук, проф. Раскин Л.Г.

**Якунин Анатолий Викторович**, канд. техн. наук, доцент кафедры высшей математики Харьковской государственной академии городского хозяйства. Научные интересы: численный анализ, распознавание образов, нестационарная гидродинамика. Увлечения: музицирование, шахматы. Адрес: Украина, 310002, Харьков, ул. Революции, 12, тел.45-90-30.

УДК 681.324.001.57

## МОДЕЛЬ ПРОТОКОЛА TCP-RENO С БЕСКОНЕЧНЫМ ИСТОЧНИКОМ ЗАЯВОК

*ГУСАК О.Ю., КОБЗЕВ И.В., РУДЕНКО Д.А.*

В настоящее время Transmission Control Protocol (TCP) является стандартным протоколом транспортного уровня для глобальных сетей, таких как Internet. Рассматривается аналитическая модель TCP версии - TCP-Reno, которая является наиболее используемым протоколом Internet. В нашей модели предполагается, что данные передаются от источника постоянно, а источником является сервер мультимедийной системы.

Наиболее распространенным протоколом транспортного уровня, который фактически стал стандартом глобальных вычислительных сетей, является протокол TCP, принадлежащий к семейству протоколов с n-возвращениями [1]. Его последняя версия TCP-Reno (далее протокол), позволяет адаптивно управлять параметрами активного соединения (размером окна) в зависимости от загруженности канала передачи.

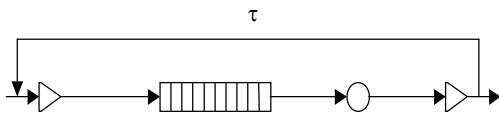
Существующие аналитические модели TCP протокола в основном ориентированы на стандартную версию протоколов с n-возвращениями и не учитывают адаптивные возможности новой версии, протокола TCP-Reno. Более того, входными параметрами для такого рода моделей служат распределение интенсивности работы источника TCP пакетов, вероятность потери пакета данных в виду ошибок канала соединения и прочее. В реальных системах связи данные параметры не всегда удается определить, либо полученные характеристики не позволяют применять последние в существующих моделях. Так большинство аналитических моделей строится на предположении о пуассоновском распределении входного потока пакетов. Принимая во внимание подавляющее присутствие систем, предназначенных для передачи аудио-видео информации, генерирующих трафик высокой интенсивности, в настоящей работе в качестве источника данных TCP соединения рассматривается бесконечный источник заявок. Наконец, разработанная концепция комплексной модели

сети [3-5] тербует создания простой модели протокола транспортного уровня, являющегося в настоящее время стандартом де-факто, которая впоследствии может быть включена в общую модель компьютерной сети.

TCP является классическим протоколом транспортного уровня, использующим стратегию "окна", обеспечивающую эффективную и надежную передачу данных. Максимальный размер окна определяется принимающей стороной в период установления соединения и зависит от физических особенностей данного узла (объем свободной памяти, скорость обработки получаемых данных и прочее).

Детальное описание алгоритма работы протокола может быть найдено в [6]. В соответствии с данным алгоритмом, протокол может функционировать в одной из двух фаз: фазе медленного старта и фазе избежания столкновений. В первом случае, после каждой успешной передачи пакета окно протокола увеличивается на 1, а при обнаружении потери пакета по таймауту сбрасывается в начальное состояние (т.е. в единицу). В фазе избежания столкновений, протокол наращивает окно соединения на 1 при успешной передаче числа пакетов, равного размеру текущего окна. При обнаружении потери пакета через получение дублирующих уведомлений размер окна сокращается в два раза, и протокол продолжает функционировать в данной фазе.

Очевидно, что при моделировании процесса передачи интерес будет представлять случай, в котором мощность источника (потенциальная скорость отправления сообщений) и получателя (потенциальная интенсивность обработки пакетов) превосходит пропускную способность канала передачи, связывающего данные две точки сети. В противном случае время передачи файла длиной  $L$  есть  $L/l$ , где  $l = \min(l_s, l_r)$  — минимальное значение интенсивности источника и получателя сообщений соответственно. Более того, канал передачи данных обычно состоит из нескольких сегментов, однако фактором, определяющим параметры модели, будет сегмент сети, имеющий наименьшую пропускную способность. Отметим также, что в данной модели предполагается бесконечный источник заявок, т.е. станция-отправитель всегда имеет готовые пакеты на передачу. Данное предположение справедливо для систем multimedia,



ТСП-источник  $\gamma$   $\mu$  ТСП-получатель  
 Модель соединения отправитель-получатель

в которых передача аудио-видео информации происходит непрерывным потоком.

С учетом принятых допущений рассматриваемая модель может быть представлена в виде системы массового обслуживания, изображенной на рисунке.

На рисунке приняты следующие обозначения:  $\mu$  – интенсивность обработки заявок самого “узкого” сегмента сети;  $\gamma$  – размер очереди пакетов, ожидающих обслуживания; ПППППП – очередь пакетов;  $\triangleright$  – источник (получатель) пакетов;  $\triangleright$  – обработчик пакетов.

В качестве алгоритма обслуживания заявок мы рассматриваем стратегию FIFO. Величина  $\tau$  есть время передачи пакета от источника к получателю, включающее время на обработку пакета в узлах маршрутизации и время передачи пакета по всем сегментам, связывающим две данные точки сети.

В соответствии с алгоритмом работы протокола максимальное число пакетов, а значит и максимальный размер окна, могут быть определены как  $w = \mu\tau + \gamma$  [7]. Таким образом, нетрудно заметить, что в стационарном режиме (фаза избегания столкновений) размер окна  $w$  будет циклически изменяться от величины  $w/2$  до  $w$ .

Принимая во внимание бесконечный источник заявок, стартовой фазой роста окна от величины 1 пакет до  $w/2$  можно пренебречь. В течение цикла работы протокола окно соединения изменяется линейно от величины  $w/2$  до  $w$ , т.е. общее количество пакетов, переданных в течение цикла, определяется как

$$n = \sum_{i=w/2}^w i = \frac{3 \cdot w^2 + 6 \cdot w}{8} - 1. \quad (1)$$

Для определения продолжительности цикла работы протокола выделим два следующих случая, возможных в момент возобновления протоколом фазы роста окна:

- 1) очередь ограниченного ресурса сети (сегмента сети) пуста;
- 2) очередь ограниченного сегмента сети содержит пакеты предыдущей фазы.

Первый случай возможен при условии, когда величина окна меньше максимального числа пакетов, которое способен “вместить” канал передачи. Данная величина определяется соотношением  $\mu \cdot \tau \geq \gamma$ . В случае, если  $\gamma > \mu\tau$ , а соответственно и  $w/2 > \mu\tau$ , очевидно, что во времени трансляции пакетов будет добавлено время ожидания в очереди сервера, равное времени обслуживания пакетов, оставшихся в буфере сервера.

Таким образом, для случая  $\mu \cdot \tau \geq \gamma$ , при пустой очереди сервера, данное окно передается за время прохождения пакета  $\tau_c = 1/\mu + \tau$  от источника к получателю и обратно. По мере увеличения окна, при наличии одного пакета в очереди, время передачи

окна возрастает до величины  $\tau_c + 1/\mu$  и в момент переполнения очереди достигает значения  $\tau_c + \gamma/\mu$ . На основании приведенных рассуждений длительность цикла изменения окна протокола определяется так:

$$d = (w - w/2) \cdot \tau_c + 1/\mu \cdot \sum_{i=1}^{\gamma} i = w/2 \cdot \tau_c + \frac{\gamma^2 + \gamma}{2}.$$

Используя число пакетов (1), передаваемых в течение длительности цикла, определим интенсивность работы системы (скорость передачи пакетов):

$$\lambda = \frac{n}{d} = \frac{(3w^2 + 6w - 8) \cdot \mu}{4[w \cdot (1 + \mu\tau) + \gamma^2 + \gamma]}, \quad \mu\tau \geq \gamma.$$

Эффективность работы протокола определяется как отношение  $1/\mu$  (при использовании “чистого” канала пакеты транслируются с частотой  $\mu$ ). Подставляя значение для величины окна протокола, получаем:

$$\rho = \frac{\lambda}{\mu} = \frac{(3(\mu\tau + \gamma)^2 + 6(\mu\tau + \gamma) - 8)}{4[(\mu\tau + \gamma) \cdot (1 + \mu\tau) + \gamma^2 + \gamma]}, \quad \mu\tau \geq \gamma.$$

В случае, когда  $\gamma > \mu\tau$ , протокол начинает цикл передачи при наличии  $R$  оставшихся пакетов в очереди сервера. Тогда оставшееся число пакетов в очереди сервера может быть определено так:

$$R = w/2 - \mu\tau,$$

длительность цикла передачи  $d$  при  $\gamma > \mu\tau$  равна:

$$d = \frac{w}{2} \left( \tau_c + \frac{\gamma - \mu\tau}{2} \right) + \frac{1}{\mu} \cdot \sum_{i=1}^{w/2} i = \frac{w}{2} \left( \tau_c + \frac{\gamma - \mu\tau}{2} \right) + \frac{1}{\mu} \cdot \frac{w^2 + w}{8}.$$

Наконец, скорость передачи  $l$  и эффективность работы протокола  $\rho$  для данного случая имеют следующий вид:

$$\lambda = \frac{3w^2 + 6w - 8}{\frac{w}{2} \left( \tau_c + \frac{\gamma - \mu\tau}{2} \right) + \frac{1}{\mu} \cdot \frac{w^2 + w}{8}} = \frac{(3w^2 + 6w - 8) \cdot \mu}{3w^2 + 6w}.$$

$$\rho = \frac{\lambda}{\mu} = \frac{(3w^2 + 6w - 8)}{3w^2 + 6w}. \quad (2)$$

Как видно из выражения (2), при больших  $w$  эффективность работы протокола приближается к 1. Данный результат является очевидным, так как очередь сервера никогда не остается пустой, т.е. обслуживание пакетов происходит с интенсивностью  $\mu$ .

Таким образом, в данной работе рассмотрена модель протокола транспортного уровня ТСП-Reno для случая с “настойчивым” источником, соответствующего источнику систем multimedia. Настоящая модель базируется на особенности протокола ТСП-Reno – адаптивном изменении размера окна соединения в зависимости от загруженности канала передачи. В качестве выходных параметров модели определены информационная скорость передачи данных и эффективность работы протокола при различных условиях функционирования последнего. Построенная модель может быть применена при расчетах реальных компьютерных сетей, так как оперирует

всегда доступными параметрами сети, такими как физическая скорость передачи данных каналом соединения, длительность передачи пакета между источником и получателем и др. Более того, настоящая модель может с успехом использоваться как составная часть комплексной модели [3-5] сети передачи данных, которая в свою очередь является эффективным инструментом, применяемым на фазе проектирования и эксплуатации компьютерных сетей.

**Литература:** 1. Шевчук А.С., Гусак О.Ю. Протокол TCP – модель, функции, спецификации // Компьютеры + Программы, 1996. N8. С.16-22. 2. Schwartz M. Telecommunication Networks: Protocols, Modeling and Analysis // Addison-Wesley, 1987. С.32-41. 3. Шевчук А.С., Кобзев И.В., Гусак О.Ю. К вопросу о построении математической модели локальной вычислительной сети // АСУ и приборы автоматики, 1997. N2. С.94-97. 4. Gusak O., Dayar T. A generalization of a TCP Model: multiple source-destination case with arbitrary LAN as the access network, Proceedings of The Fourth Symposium on Computer Networks (BAS'99), 20-21 May 1999, Istanbul, Turkey. P. 102-111. 5. Gusak O. An analytical model of a client-server system functioning on top of TCP, Proceedings of The Sixth International Conference on Distributed Multimedia Systems (DMS'99), July 26-30, 1999, Aizu, Japan. P. 212-213. 6. Stevens W. R. TCP/IP Illustrated, Volume 1, The Protocols // Addison-Wesley, 1994. 576 pp. 7. Heyman D.P., Lakshman T.V., Neidhardt A. L. A New

Method for Analysing Feedback Protocols with Applications to Engineering Web Traffic over the Internet, Performance Evaluation Review, 1997. P. 24-38.

Поступила в редколлегию 02.07.99

Рецензент: д-р техн. наук Петров Э.Г.

**Гусак Олег Юрьевич**, аспирант факультета компьютерной инженерии Университета Билькента (Анкара, Турция). Научные интересы: компьютерные сети, программное обеспечение, моделирование. Адрес: Турецкая республика, Анкара, 06533, Университет Билкент, факультет компьютерной инженерии, e-mail gusak@cs.bilkent.edu.tr

**Кобзев Игорь Владимирович**, канд. техн. наук, доцент кафедры информационных систем и технологий в деятельности ОВД Университета внутренних дел. Научные интересы: стохастическое моделирование, программное обеспечение. Украина, 310166, Харьков, ул. Новгородская, 44, кв. 19, тел. 30-71-75.

e-mail k\_infsis@adm.univd.kharkov.ua

**Руденко Диана Александровна**, канд. техн. наук., ассистент кафедры применения ЭВМ ХТУРЭ. Научные интересы: управление сложными объектами, программное обеспечение. Адрес: Украина, 310012, Харьков, ул. К.Маркса, 13/15, кв. 33, тел. 23-13-96.

УДК 681.3+681.5:007

## СИНТЕЗ ПОМЕХОУСТОЙЧИВЫХ К НЕРЕГУЛЯРНЫМ ВОЗМУЩЕНИЯМ АЛГОРИТМОВ ПОИСКА ТОЧКИ ЭКСТРЕМУМА УНИМОДАЛЬНОЙ ФУНКЦИИ

АЛИПОВ Н.В., БУЛАХ Е.В.

Дальнейшее развитие нового направления в криптографии с использованием дискретных автоматов требует разработки алгоритмов поиска точки экстремума унимодальной функции при воздействии на процесс поиска возмущений с различными характерными признаками. В статье описывается разработка таких алгоритмов в условиях воздействия симметричного нерегулярного возмущения. Приводятся логические схемы построения алгоритмов, которые позволяют для конкретных параметров построить помехоустойчивые к симметричным нерегулярным помехам алгоритмы поиска точки и тем самым определить функционирование дискретных автоматов для систем защиты информации.

Новым в совершенствовании методов защиты информации при ее передаче является направление, связанное с использованием теории дискретных автоматов [1]. Нами получен ряд оригинальных результатов, изложенных в работе [2]. Основу предложенных методов составляют помехоустойчивые алгоритмы поиска точки экстремума в условиях воздействия на процесс поиска регулярных симметричных возмущений, так называемых  $A_{2,8}$ -последовательностей. Существуют и нерегулярные возмущения. В статье рассматриваются помехоустойчивые алгоритмы поиска точки экстремума в условиях

воздействия на процесс поиска нерегулярных симметричных возмущений, так называемых  $A_{2,3}$ -последовательностей. Характерной особенностью этих последовательностей является то, что длительность возмущения – случайная величина, распределенная по некоторому закону в интервале  $[l_1, l_2]$ , где  $l_1, l_2$  – соответственно минимально и максимально возможные значения длительности возмущения.

Рассмотрим помехоустойчивые к  $A_{2,3}(a, l_1, l_2, H)$  – последовательности алгоритмы поиска точки экстремума унимодальной функции.

Пусть  $H > l_2$  и некоторым образом выбрана точка первого эксперимента. Тогда на первом шаге алгоритма (это уже известно [2]) может появиться один из исходов типа  $a$ ).

Применяя на втором шаге алгоритма к этому исходу смешанную стратегию [2], получаем один из исходов:

$$b_1) f \mathcal{E}_1^2 \ominus \max_{\rho} \{ f \mathcal{E}_{\rho}^2 \Phi$$

$$b_2) f \mathcal{E}_{q_1}^2 \ominus \max_{\rho} \{ f \mathcal{E}_{\rho}^2 \Phi q_1 = \overline{2, k-1};$$

$$b_3) f \mathcal{E}_k^2 \ominus \max_{\rho} \{ f \mathcal{E}_{\rho}^2 \Phi$$

Исход  $b_1$ ) свидетельствует о действии  $A_{2,3}$ -последовательности на одном из первых шагов алгоритма. На последующих  $[k-1]$ -шагах применяют в полуоткрытом интервале  $[x_{q-1}^{1,1}, x_2^2]$  (непомехоустойчивый алгоритм поиска.