

Таким образом, данному узлу замены соответствует четыре булевых функции от четырех переменных (данный узел замены отображает входную последовательность из четырех бит в выходную четырех битовую последовательность).

В приложениях используется итеративный алгоритм создания узлов замен. Схема работы данного метода при создании узла замены, содержащего m колонок, выглядит следующим образом: пусть заданы минимальное приемлемое значение нелинейности N и максимальное приемлемое динамическое расстояние M .

1. Положить количество колонок $nr \leftarrow 1$.
2. Создать уравновешенную булеву функцию f_{nr} .
3. Проверить следующие два условия для всех линейных комбинаций f_1, \dots, f_{nr} :
 - a) превосходит ли нелинейность значение N ;
 - b) превосходит ли M динамическое расстояние порядка 1 от текущей линейной комбинации булевых функций.
4. Если оба условия выполнены, добавить f_{nr} в узел замены, увеличить nr , иначе перейти на шаг 2.
5. Если $nr = m$, то построение узла замены закончено, иначе перейти на шаг 2.

Данный алгоритм позволяет строить узлы замен, содержащие булевые функции высокой нелинейности, линейные комбинации которых также обладают заданной нелинейностью. При этом сами функции могут удовлетворять строгому лавинному критерию, как и их линейные комбинации, в зависимости от задания параметров алгоритма.

Помимо данного метода в приложениях также реализовано создание узлов замен, содержащих бент-функции наподобие того, как это было сделано при реализации блочного шифра CAST. Бент-функции не уравновешены – следовательно, такие узлы замен должны быть уязвимы к корреляционному криптографическому анализу. Однако разработчики блочного шифра CAST пошли несколько другим путем, положив в основу создания узла замен следующее предложение: в среднем все булевые функции узла замены должны быть уравновешены. В силу того что бент-функции от n переменных могут иметь только следующие значения веса Хэмминга: $2^{n-1} \pm 2^{n/2-1}$, данное предложение можно выполнить для любых узлов замен с четным количеством колонок.

СПИСОК ЛИТЕРАТУРЫ

1. Логачев О.А., Сальников А.А., Ященко В.В. Булевые функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
2. Fuller J.E. Analysis of affine equivalent Boolean functions for cryptography // Ph.D. thesis. Queensland University of Technology Brisbane, Australia, 2003.

3. Seberry J., Zhang X. Highly Nonlinear 0-1 Balanced Boolean Functions Satisfying Strict Avalanche Criterion // Department of Computer Science, The University of Wollongong, Australia, 1993.

О МЕТОДЕ АДАПТИВНОЙ МАРШРУТИЗАЦИИ В ЗАМКНУТЫХ СЕТЬЯХ МАССОВОГО ОБСЛУЖИВАНИЯ

И.П. Фокина, И.Е. Ганапко

Рассматривается замкнутая экспоненциальная сеть массового обслуживания Γ [1, 2], содержащая $L+1$ одноприборных систем массового обслуживания S_i , $i = 0, \dots, L$. В сети обслуживаются требования $L+1$ классов – по одному требованию классов $1, \dots, L$, называемых *информационными*, и Q требований класса $L+1$, называемых *сетевыми*. Интенсивности обслуживания информационных и сетевых требований в S_i , $i = 1, \dots, L$, соответственно равны μ_{i1} и μ_{i2} . Интенсивность обслуживания информационных требований в S_0 равна μ_0 . Информационные требования имеют абсолютный приоритет в обслуживании по отношению к сетевым требованиям. Топология сети определяется матрицей смежности $W = (w_{ij})$, $i, j = 0, \dots, L$, соответствующего сети ориентированного графа G с множеством вершин $\mathcal{L} = \{0, \dots, L\}$ и множеством дуг, соответствующих возможным переходам требований между системами сети. Маршрутизация информационных требований класса k , $1 \leq k \leq L$, (k -требований) осуществляется маршрутной матрицей $\Theta^{(k)} = (\theta_{ij}^{(k)})$, $i, j = 0, \dots, L$. Маршрутизация сетевых требований в сети Γ – маршрутной матрицей $\Theta^{(L+1)} = (\theta_{ij}^{(L+1)})$, $i, j = 0, \dots, L$, где $\theta_{ij}^{(L+1)}$ – вероятность перехода сетевого требования после обслуживания в системе S_i в систему S_j , причем $\theta_{i0}^{(L+1)} = 0$, $i = 0, \dots, L$. Обозначим λ_i – интенсивность потока сетевых требований в систему S_i , s_i – число сетевых требований в системе S_i , $i = 1, \dots, L$.

Предполагается, что система S_0 осуществляет функции управления и реализует метод адаптивной маршрутизации в подсети из систем S_i , $i = 1, \dots, L$. Функционирование сети Γ с управлением можно представить в виде последовательности циклов с номерами $l = 1, 2, \dots$. Каждый цикл содержит два этапа функционирования сети: ординарный этап и этап сетеметрии. Предполагается, что длительности этапа сетеметрии τ и ординарного этапа φ являются параметрами метода адаптивной маршрутизации, которые не изменяются в процессе функционирования сети, причем $\tau < \varphi$.

Обозначим $\Delta = 1/\mu_0 + \delta$, где δ – максимальная суммарная задержка информационных требований на пути из S_0 в S_i и из S_i в S_0 для $i=1,...,L$. Пусть $\tau = N\Delta$, где $N > 0$ – целое число. Система S_0 за интервал времени длительностью Δ направляет информационные требования в соответствующие системы S_i , $i=1,...,L$. Требование класса k получает данные о числе сетевых требований в системе S_k и доставляет эти данные в систему S_0 с использованием маршрутной матрицы $\Theta^{(k)}$. Таким образом, в системе S_0 в течение этапа сетеметрии накапливается L выборок объемом N значений случайных величин s_i , $i=1,...,L$. Эти выборки далее используются системой S_0 для вычисления оценок математических ожиданий (м.о.) длительностей пребывания требований в соответствующих системах. Длительность τ этапа сетеметрии выбирается таким образом, чтобы обеспечить сбор выборок достаточного объема для вычисления значений требуемых статистик с необходимой точностью. По окончании этапа сетеметрии информационные требования в подсеть систем S_i , $i=1,...,L$, не направляются.

После окончания этапа сетеметрии системой S_0 вычисляются значения задержек сетевых требований во всех системах сети, с учетом которых выбираются оптимальные маршруты для сетевых требований, обеспечивающие минимальные суммарные задержки требований при прохождении поенным маршрутам. Обозначим через $U = (u_i)$, $i=1,...,L$, вектор задержек, где u_i – оценка м.о. длительности пребывания требований в системе S_i .

Метод формирования оптимальных маршрутов для сетевых требований системой S_0 заключается в следующем. Пусть каждая вершина $i \in \mathcal{L}$ графа G имеет вес, равный u_i . Назначим каждой дуге (i, j) , $i, j \in \mathcal{L}$, для которой $w_{ij} = 1$, вес u_j . Значения весов вершин и дуг являются переменными величинами, зависящими от характеристик выборок, полученных системой S_0 в течение очередного этапа сетеметрии. Используя известный метод поиска всех кратчайших путей на графах [3], строится множество оптимальных путей V между всеми системами сети. Путь называется *оптимальным*, если его вес, равный сумме весов принадлежащих ему дуг, является *минимальным*. Пусть $V = (v^y)$, $i, j \in \mathcal{L}$, где v^y – оптимальный путь из вершины i в вершину j в графе G , $v^y = (v_m^y)$, $m=1,...,|v^y|$, где v_m^y – номер вершины графа G m -й по счету в пути из i в j . Поскольку найденные оптимальные пути в графе G представляют собой кратчайшие маршруты в сети Γ для сетевых требований, обеспечивающие общее минимальное время прохождения по маршруту, то необходимо скорректировать используемую в течение текущего цикла l маршрутную матрицу

$\Theta^{(l+1)}$ для увеличения интенсивностей потоков требований по этим оптимальным маршрутам за счет увеличения вероятностей переходов требований по соответствующим дугам, принадлежащим оптимальным путям.

Алгоритм корректировки матрицы $\Theta^{(l+1)}$ с параметром ε .

- Обозначение: $\varepsilon \in \mathbb{R}$ – параметр метода, $\varepsilon > 0$.
1. Для всех $i, j \in \mathcal{L} \setminus \{0\}$: $w_{ij} = 0$ выполнять п. 2 – 6.
 2. $l := 2$.
 3. Если $|v^y| > 1$, то перейти на п. 1, иначе выполнить п. 4 – 6.
 4. Пусть $m = v_{l-1}^y$ и $n = v_l^y$, тогда

$$\theta_{mn}^{(l+1)} := \theta_{mn}^{(l+1)} + \varepsilon.$$

5. $l := l + 1$.
6. Перейти на п. 3.
7. Формирование новой матрицы $\Theta^{(l+1)} = (\theta_{ij}^{(l+1)})$, где

$$\theta_{ij}^{(l+1)} := \frac{\theta_{ij}^{(l+1)}}{\sum_{m=1}^L \theta_{im}^{(l+1)}}, \text{ для всех } i, j \in \mathcal{L}.$$

Конец алгоритма.

Целью маршрутизации в сетях передачи данных с коммутацией пакетов является передача пакетов от источника к адресату по маршрутам с минимальной задержкой. Достижение цели управления маршрутизацией осуществляется решением задачи оптимизации задержки пакетов, усредненной по всем парам узлов коммутации (системная оптимизация). Системная оптимизация осуществляется, как правило, в задаче маршрутизации с централизованным принятием решения [4]. Поэтому предложенный метод управления маршрутизацией в замкнутых экспоненциальных сетях массового обслуживания может быть использован при решении задач проектирования протоколов канального и сетевого уровней передачи данных с коммутацией пакетов и централизованным управлением маршрутизацией.

СПИСОК ЛИТЕРАТУРЫ

1. Митрофанов Ю.И. Анализ сетей массового обслуживания. Саратов: Науч. книга, 2005. 175 с.
2. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. 512 с.
3. Кристофидес Н. Теория графов. Алгоритмический подход. М.: Мир, 1978. 432 с.
4. Протоколы и методы управления в сетях передачи данных / Под ред. Ф.Ф. Куо. М.: Радио и связь, 1985. 480 с.