протоколов обмена данными, с учетом требований, определяемых соглашением о качестве обслуживания информационных потоков. Данная схема может быть использована при тестировании соответствия криптографических алгоритмов, модулей и защищенных протоколов обмена данными и управления ключами общей идеологии информационного обмена в NGN.

Список литературы: 1.Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA–3) family. Federal Register Vol. 72, No. 212, 2 Nov 2007, 2007. pp. 62212-62220. 2.FIPS-140-3 Draft security requirements for cryptographic modules. National Institute of Standards and Technology, Information Technology Laboratory, 2009, 63 p.3.*Hardy W.* Measurement and evaluation of telecommunications quality of service – John Wiley & Sons. Inc, 2001, 245 p.4.ITU-T P.564 ITU-T Recommendation P.564 (2007), Conformance testing for voice over IP transmission quality assessment models, 2007, 32 p.5.ITU-T Y.2001. Рекомендация МСЭ-Т Y.2001 (2004), Общий обзор СПП, 2004, 32 с.6.ITU-T Y.2704 ITU-T Recommendation Y.2012 (2010), Security mechanisms and procedures for NGN, 2010, 58 p. 7.RFC 3272 Awduche D. Overview and Principles of Internet Traffic Engineering, 2002. – 71 p. 8.RFC 4869 Law L. Suite B Cryptographic Suites for IPsec, 2007. – 8 p.9.Бакланов И.Г. NGN: принципы построения и организации [Текст] – М.: Эко-Трендз, 2008. – 400 с. 10.*Бешелев С.Д.* Математико-статистические методы экспертных оценок [Текст] / С.Д. Бешелев, Ф.Г. Гурвич. – М.: Статистика , 1980. – 263 с. 11.*Бронштейн О.И.*Модели приоритетного обслуживания в информационно-вычислительных системах [Текст] / О.И. Бронштейн, И.М. Духовный. М.: издательство «Наука», 1976. – 220 с.12.*Вегешна Ш.* Качество обслуживания в сетях IP [Текст] : пер. с англ. - М.: Издательский дом «Вильямс», 2003. - 368 с. 13.Исследование рынка услуг связи в России, предоставляемых на базе технологических решений [Электронный ресурс] / NGN J'son & Partners management consultancy. – Режим доступа: http://web.json.ru/markets_research/analytical_reports/detail/?report_id=3904 – 20.07.2011 г. – Загл. с экрана. 14.*Поповский В.В.* Защита информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2006. 15.*Поповский В.В*. Основы криптографической защиты информации в телекоммуникационных системах. В 2-х т. [Текст] / В.В. Поповский, А.В. Персиков. - Х.: СМИТ, 2010. 16.*Столлингс В.* Криптография и защита сетей: принципы и практика. – М.: Издательский дом «Вильямс», 2001. – 672 с.

Поступила в редколлегию 17.07.2011

УДК 621.391

НАОРС И. АНАД, асп. ХНУРЭ, Харьков
Я.Т. ХУСЕЙН, асп. ХНУРЭ, Харьков

СОВЕРШЕНСТОВАНИЕ МЕХАНИЗМОВ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУПА В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

Проведен аналіз алгоритмів множинного випадкового доступу з вирішенням конфлікту, що використовуються в системах абонентного радіодоступу і їх застосовність в типових умовах інтенсивного і нестаціонарного трафіку. Запропонована адаптивна процедура, що містить алгоритм оптимальної стохастичної оцінки і знаходжувач порогу, що сигналізує про необхідність переходу на новий алгоритм.

Проведен анализ алгоритмов множественного случайного доступа с разрешением конфликта, используемые в системах абонентного радиодоступа и их применимость в типовых условиях интенсивного и нестационарного трафика. Предложена адаптивная процедура, содержащая

алгоритм оптимальной стохастической оценки и обнаружитель порога, который сигнализирует о необходимости перехода на новый алгоритм.

The analysis of algorithms of plural casual access is conducted with permission of conflict applied in the systems of subscriber radioaccess and their applicability in the typical conditions of intensive and unstationary traffic. Adaptive procedure, containing the algorithm of optimum stochastic estimation and registr threshold signaling about the necessity of transition on a new algorithm, is offered.

В системах беспроводной связи (абонентского радиодоступа) типа Wi-Fi, WiMAX важное значение имеет выбранный метод случайного доступа (МСД) абонентских станций (АС) к общей базовой станции (БС). Исторически первым МСД был предложен алгоритм Aloha. Конфликтная ситуация в этом алгоритме разрешается за счет случайных механизмов, при этом возможности повторной передачи, после разрешения конфликта, абонент может ожидать достаточно продолжительное время T_K . Более эффективными с точки зрения минимизации времени задержки $\tau_з$ и максимизации коэффициента кратности K разрешения конфликта $V = K / T_K$ являются древовидные алгоритмы [1,2] и алгоритмы с двойными экспоненциальными отсрочками (откатами) [3,4]. Известно также [1], что при значительной загрузке сети более производительной технологией является метод циклического опроса (поллинга).

Все упомянутые технологии в различных ситуациях, при различной интенсивности поступающей нагрузки λ обладают тем или иным преимуществом. Рассмотрим более подробно данные технологии и проанализируем их применимость в типовых условиях интенсивного и нестационарного трафика.

Обзор технологий случайного множественного доступа.

Основной проблемой, определяющей эффективность тех или иных систем абонентского радиодоступа, является реализация метода случайного множественного доступа с разрешением конфликта. Известные системы IEEE 802.11 и IEEE 802.16 обладают рядом особенностей, позволяющих реализовать эффективные методы доступа. К числу этих особенностей относится синхронность работы всей системы. При этом время работы системы разделяется на слоты (окна), которые формируют циклическую смену кадров. В каждом слоте возможно возникновение одного из трех событий: “успех”, “пусто” или “конфликт”. При этом к концу каждого слота на АС за счет нисходящего канала от БС становится известно о происшедшем в этом слоте событии.

Древовидные алгоритмы являются потенциально наиболее производительными и среди них различают стандартные древовидные алгоритмы (СДА) и модифицированные древовидные алгоритмы (МДА). От БС, в нисходящем канале, ко всем АС передается оперативная и служебная информация. С помощью служебного канала осуществляется управление передачей АС и передается информация о качестве её передачи в восходящем канале. Так, в случае возникновения конфликта при одновременной передаче двумя (A и B) или тремя (A,B,C), или большим количеством АС станций, БС может заблокировать дальнейший прием пакетов до разрешения конфликта (до конца периода разрешения конфликта).

Конфликт трех АС (рис.1) разрешается следующим образом. БС идентифицирует номера конфликтующих станций и ещё до конца текущего слота дает информацию всем АС о возникновении конфликта и одновременно дает разрешение одной из конфликтующих АС (станции А) передать свой пакет в следующем (втором) слоте. Третий слот отдается для передачи оставшихся пакетов, однако там снова возникает два конфликтующих пакета В и С. Поскольку этим станциям (В и С) был дан второй приоритет, то следующий слот – свободен, а далее начинается новый период разрешения конфликта для В и С. На рис.1а представлена временная последовательность передачи пакетов A,B,C. Модифицированный алгоритм (МДА) отличается тем, что после пропуска 4-го слота повтора передачи конфликтных пакетов не предусмотрено, т.е. период разрешения конфликта сокращается на один слот, что приводит к возрастанию коэффициента V.

Существует и дальнейшая модернизация древовидных алгоритмов SIC – Successive Interference Cancellation – процедура последовательного погашения интерференции (компенсации помех). Суть данной процедуры в том, что из смеси конфликтующих пакетов А и В в следующем слоте передается пакет А, а поскольку имеется его “чистая” реализация, то без дополнительной передачи из смеси А+В вычитается (компенсируется) А и таким образом удается выделить В: $(\hat{A}+\hat{A})-\hat{A}=\hat{A}$. Для такой процедуры требуется достаточный объем памяти.

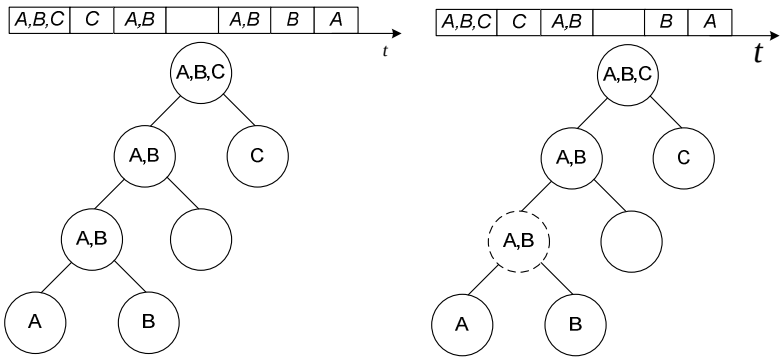

Рис. 1 Временная диаграмма и структура древовидных алгоритмов СДА-а, МДА-б

Алгоритмы с двойной экспоненциальной отсрочкой (Binary Exponential Backoff – BEB) требует выделение отдельного слота, в котором размещаются мини-окна, где принимаются запросы (заявки) абонентских станций на передачу информационного пакета. Структура кадра для алгоритма BEB представлена на рис. 2. БС, приняв заявку или обнаружив конфликт, в нисходящем канале дает разрешение или запрет на передачу, и эта информация всем АС становится известной до конца данного слота, выделенного для заявок. Таким образом, в алгоритме BEB конфликт возникает не в период передачи информационных пакетов в окнах, а при передаче заявок в мини-окнах. За один кадр АС может подать одну заявку, при этом она произвольно равновероятно выбирает номер мини-окна. При наличии конфликта в мини-окне в следующем кадре номер мини-окна удваивается (происходит двойной откат) и так удвоение продолжается на каждом очередном кадре до максимально возможного номера.

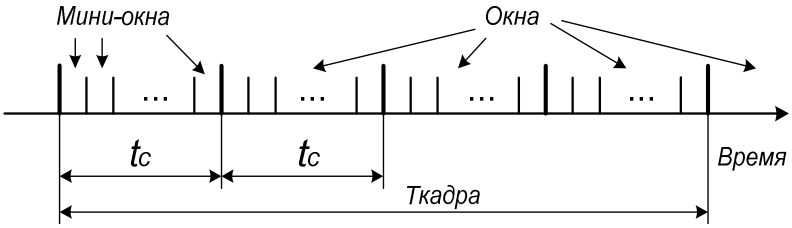

Рис. 2 Структура кадра для алгоритма двойной экспоненциальной отсрочки

Затем, попытки передачи заявки повторяются.

Анализ качества алгоритмов случайного множественного доступа.

Одним из основных показателей качества алгоритмов случайного множественного доступа является коэффициент кратности разрешения конфликта, представляющий собой предел отношения кратности конфликта K к среднему времени разрешения данного конфликта T_K :

$$V = \lim_{K\to\infty} \frac{K}{T_K}, \qquad (1)$$

где T_K выражено в единицах слотов. Доказано в [1,4], что значение V может быть определено из выражения:

$$\left(\frac{2}{\ln 2} + c\right)^{-1} < V < \left(\frac{2}{\ln 2} - c\right)^{-1}, \qquad (2)$$

где $c = 3{,}127 \cdot 10^{-6}$.

Очевидно, что V может интерпретироваться также как относительная скорость разрешения конфликта. Исследования показывают, что значение этой скорости V может достигать 0,3-0,38. Для алгоритмов SIC, SICTA [4] эта цифра может достичь 0,693.

Другой важной характеристикой систем абонентского радиодоступа является значение средней задер-жки при различной абонентской нагрузке.

Задержка пакета $\tau_з$ определяется как время от первого запроса до того, как передача пакета будет успешно завершена. Если АС успешно передает свой пакет с 1-й попытки, то

$$\tau_з = \tau_1 + T_k + \tau_2, \qquad (3)$$

где τ_1, τ_2 – соответственно: время передачи запроса и время передачи пакета.

Длительность кадра T_k включает нисходящий и восходящий подкадры и их цикл синхронизации. Если первая попытка окажется неудачной, то ко времени T_k добавляется время M кадров и общая задержка сотав-ляет:

$$\tau_з = \tau_1 + \sum_{j=0}^{j} M^{(j)} T_k + \tau_2. \qquad (4)$$

Среднее время задержки $\tau_{\sum з} = \tau_з + \tau_c$ обретаемое в системах радиодоступа складывается с другими составляющими задержки τ_c имеющими место на более высоких уровнях: сетевом и траспортном. Именно $\tau_з$ является важным ограничением для реализации сервисов реального времени: речи и видео. Воспользуемся результатами анализа [3,4], полученными для идеальных (в отсутствии шумовых помех) условий.

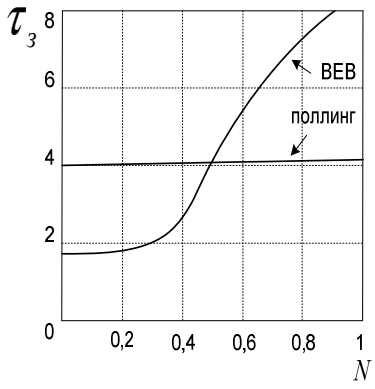

Рис.3. Графики зависимости среднего времени задержки для алгоритмов BEB и для циклического опроса (поллинга)

На рис.3 представлены графики
зависимости среднего времени задержки от параметра $N = np / L$, где n – число активных АС, p – вероятность появления запроса АС, L – число мини-окон, в которых принимаются запросы от АС на передачу пакета.

Очевидно показатель N – характеризует относительную нагрузку системы.

Из графиков (рис.3) следует, что при увеличении нагрузки алгоритм BEB резко теряет эффективность и при определенных условиях время задержки сравнивается и далее намного превышает задержку в алгоритме с циклическим опросом.

На практике нагрузка изменяется в течении суток, времени года и при других случайных изменениях. При этом использование одного и того же метода случайного доступа особенно в часы наибольшей нагрузки может привести к заметным потерям эффектив-ности. В данном случае целесообразно использовать адаптивные методы самоорганизации [5], позволяющие осуществлять рациональный выбор режима доступа.

Методы адаптации к изменению нагрузки

Суть предлагаемого метода адаптации состоит в том, чтобы на основе наблюдения за интенсивностью поступающей на БС нагрузки своевременно выбрать тот или иной алгоритм случайного доступа, например, при увеличении $N > 0{,}5$ перейти на алгоритм циклического опроса, гарантирующего определенный уровень задержки. Таким образом, для построения адаптивной процедуры следует произвести оценку поступающей от всех АС нагрузки и обнаружить допустимое превышение определенного порога, когда $N \geq N_{доп}$, что является сигналом для перехода на иной алгоритм доступа. Структурная схема, реализующая такую процедуру, представлена на рис.4

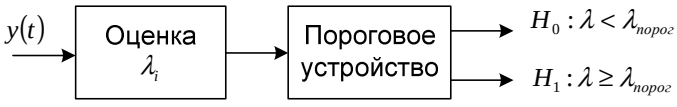

Рис. 4. Структурная схема адаптивного алгоритма оценки и обнаружения

Суммарный групповой сигнал абонентских станций на входе БС $y(t)$ образует нестационарный поток, интенсивность которого зависит от времени $\lambda(t_i)$. Очевидно интенсивность потока $\lambda(t_i)$ можно представить виде случайного процесса, значение которого x_i равняется численно числу заявок на i - интервале времени. Нестационарный процесс x_i можно представить в виде суммы стационарно изменяющегося случайного компонента $\lambda_{ст}$ и нестационарного тренда $\lambda_{НТ}$, который может быть линейным или нелинейным. Нас в данном случае не интересует стационарный случайный компонент $\lambda_{ст}$, поскольку он отображает локальные изменения трафика. Тренд же нестационарности $\lambda_{НТ}$ как раз несет информацию о среднем возрастании или уменьшении нагрузки. Этот тренд подлежит оценке.

Для нахождения оценки тренда нестационарности $\tilde{\lambda}_{НТ}$ методы выборочной оценки не подходят, поскольку неясно какие брать выборочные интервалы и как интерпретировать кусочно-нестационарную оценку интенсивности. Более

конструктивной является рекурсивная оценка интенсивности на интервалах $\Delta t = i-(i-1)$ с использованием алгоритма стохастической аппроксимации [5]:

$$\tilde{\lambda}(i) = \tilde{\lambda}_{НТ}(i-1) + \mu(i)\left[y(i) - \tilde{\lambda}(i-1) \right], \qquad (5)$$

где $\mu(i)$ – масштабирующий коэффициент, выбор которого зависит от шага дискретизации i. Опыт показывает, что процедура (5) устойчиво работает и при $\mu(i) = const \le 1$.

Следует отметить, что процедура (5) не предназначена для оценки нестационарных процессов, более того: можно доказать, что она оптимальна для сугубо стационарных процессов типа $x(i+1) = x(i)$. Вместе с тем процедура (5) обладает сглаживающим эффектом, т.е. она слабо реагирует на быстрые изменения. То-есть выбирая процедуру (5), оцениваем среднее значение $\lambda_{ср}$, условное по наблюдению $y(i)$. Именно это сглаживающее свойство используется для оценки тренда нестационарности.

Для анализа качества алгоритма (5) был проведен машинный эксперимент. Для этого была использована цифровая модель входного процесса:

$$y(i) = y_{ст}(i) + y_{НТ}(i) + \nu(i), \qquad (6)$$

где $y_{сò}(i), y_{НТ}(i)$ – соответственно: стационарный и нестационарный компоненты модели, $\nu(i)$ – белый гауссов шум в канале наблюдения.

Стационарный компонент $y_{сò}(i)$ моделировался с помощью формирующего фильтра [5], на вход которого подавался шум $\xi(i)$:

$$y_{ст}(i) = e^{-\frac{\Delta t}{\tau_{кор}}} y_{ст}(i-1) + \sqrt{\sigma_\xi^2 \left(1 - e^{-\frac{\Delta t}{\tau_{кор}}} \right)} \xi(i), \qquad (7)$$

где Δt – шаг дискретизации; $\tau_{кор}$ – интервал корреляции процесса $y_{ст}(i)$; σ_ξ^2 – спектральная плотность мощности шума.

$y_{НТ}(i)$ – нестационарный компонент моделировался в виде синусоиды:

$$y_{НТ}(i) = C(i) \sin\left(i \frac{\Delta t}{\tau_{кор}} \right), \qquad (8)$$

где $C(i)$ – дополнительный множитель, который может отображать, например, скачкообразные изменения, в нашем случае $C(i) = 1$.

На рис.5 представлен фрагмент нестационарного процесса $y(i)$ полученный на выходе формирующего фильтра, при следующем наборе параметров: $\frac{\Delta t}{\tau} = \frac{1}{10}, \sigma_\xi^2 = 10, \sigma_\nu^2 = 1$.

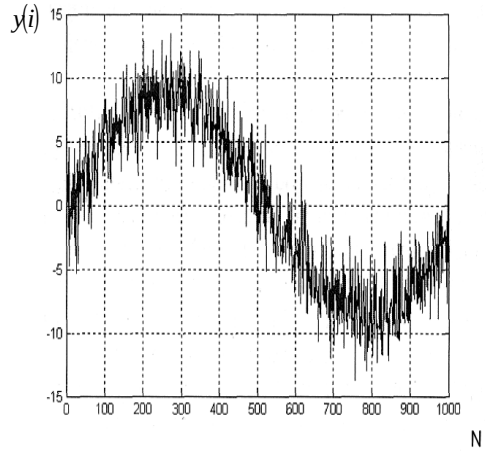

Рис.5 График наблюдаемого на входе формирующего фильтра процесса $y(i)$

На рис. 6 представлены три

реализации оценки нестационарного процесса $y(i)$ при различной величине шаговой постоянной $\mu_1 = 0{,}1; \mu_2 = 0{,}01; \mu_3 = 0{,}001$ при шаге дискретизации $\Delta t/\tau = 0{,}01$.

Из графиков видно, что с уменьшением коэффициента μ наблюдается несколько эффектов на выходе устройства оценки (5):

– заметен процесс сглаживания, сводящийся к тому, что на фоне синусоиды уменьшается уровень флуктуационной компоненты;

– снижается уровень оцениваемой компоненты;

– несколько смещается значение максимума нестационарной компоненты.

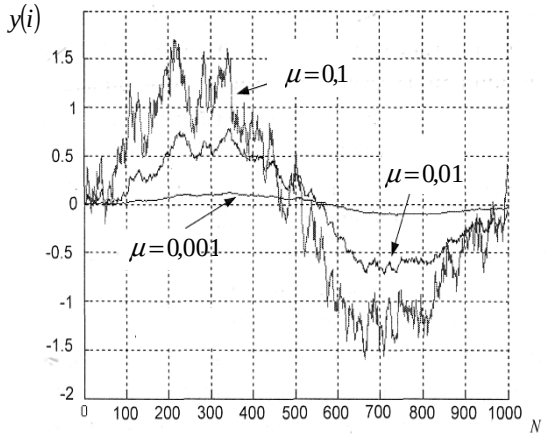

Рис. 6 Оценки нестационарного процесса на интервале N=1000 шагов

Более детальные результаты анализа можно получить из обобщенных графиков на рис.6 при $\sigma_\xi^2/\sigma_v^2 = 10$ для различных шагов дискретизации $\Delta t/\tau$.

Для получения статистического вывода о значениях уровня оцениваемой компоненты, в зависимости от выбора шаговой постоянной μ, проводилось усреднение уровней получаемых в установившемся состоянии оценок реализации исходной случайной последовательности $\lambda(i)$.

На рис.6 представлены графики уровней оцениваемой компоненты $\tilde{\lambda}(i)$ в зависимости от величины выбранной шаговой постоянной μ для трех вариантов значений шага дискретизации наблюдаемого процесса. Из графиков следует, что с уменьшением коэффициента μ уровни $\tilde{\lambda}(i)$ уменьшаются при любом шаге дискретизации $\Delta t/\tau$. Этот факт имеет важное значение при построении обнаружителя, поскольку с уменьшением уровня $\tilde{\lambda}(i)$ падает отношение сигнал/шум и теряется качество обнаружения. Поэтому μ не следует выбирать меньше $0{,}001...0{,}0001$. Смещение значения оценки $\tilde{\lambda}(i)$ по отношению к реально имеющихся значений интенсивности связано с эффектом сглаживания и по результатам экспериментов не превышает значений 0,1 квазипериода нестационарности. Таким образом алгоритм стохастической аппроксимации может быть эффективным для выделения нестационарных компонет случайных процессов. Обнаруженный таким образом порог $N_{\text{ап}}$, при котором алгоритмы ВЕВ или МДА теряют свою эффективность, является сигналом о необходимости к методам поллинга.

Выводы.1.Высокоэффективные методы случайного множественного доступа, основанные на древовидных алгоритмах и на алгоритмах двойной экспоненциальной отсрочки (ВЕВ) теряют производительность с увеличением нагрузки. Имеется предельное значение нагрузки, при котором величина задержки у этих алгоритмов сравнивается с задержками, имеющими место при

циркулярном опросе абонентов (поллинге). При дальнейшем увеличении нагрузки методы поллинга становятся намного эффективнее.

2. В условиях значительных нагрузок и при их изменениях, при нестационарном трафике целесообразно переходить на использование тех алгоритмов, которые обладают гарантированной производительностью при данной текущей нагрузке (методы поллинга). Для этого предложена адаптивная процедура, содержащая алгоритм оптимальной стохастической оценки и обнаружитель порога, сигнализирующего о необходимости перехода на новый алгоритм.

3. Для обнаружения критического тренда и других допустимых уровней нестационарного потока заявок в телекоммуникационных системах со случайным множественным доступом может быть использована рекурсивная процедура оценки интенсивности, построенная по алгоритму стохастической аппроксимации, обладающая соответствующим сглаживающим эффектом.

4. Экспериментальные исследования процедуры оценки тренда нестационарности (5) показали, что кроме ожидаемого сглаживающего эффекта, имеют место и другие, влияние которых сказывается на качестве обнаружителя: с уменьшением шаговой постоянной μ снижается уровень оцениваемой компоненты, что приводит к снижению отношения сигнал/шум, а соответственно, и к ошибкам в обнаружении. Следует рекомендовать выбор $\mu = (0{,}001...0{,}0001)$, где смещение оценки и потери уровня оцениваемой компоненты еще не столь пагубны.

5. Точность оценки, ее смещенности, и сам сглаживающий эффект зависит также от выбранного шага дискретизации $\Delta t/\tau$. Опыт показывает, что наиболее удачным в данном алгоритме будет выбор $\Delta t/\tau_{кор} = 0{,}1$.

Список литературы: 1. *Б.С. Цыбаков, В.А. Михайлов* "Свободный синхронный доступ пакетов в широковещатель-ный канал с обратной связью," Проблемы передачи информ. 1978, Т. 14, №4, С. 32-59. 2. *Rubin*, "Access-Control Disciplines for Multi-Access Communication Channels: Reservation and TDMA Schemes," IEEE Transactions on Information Theory, Vol. IT-25, No. 25, pp. 516-538, September 1979. 3.*G. Bianchi*, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," IEEE Journal On Selected Areas In Communications, 2000, Vol. 18, No. 3, p. 535 - 547. 4. *Винель А.В., Тюрликов А.М., Федоров К.А.* Использование последовательного погашения интерференции при организации случайного множественного доступа в централизованных сетях. Информационно-управляющиие системы.2009. Т.2., с, 46-55. 5. Математические основы управления и адаптации в телекоммуникационных системах: учеб. / Поповский В.В,Олейник В.Ф. – Х.:ООО “Компания СМИТ”,2011. – 362 с.

Поступила в редколлегию 27.07.2011

УДК 621.391

П.П. ВОРОБИЕНКО, докт.техн.наук, проф., ректор, Одесская НАС им. А.С. Попова
В.И. ТИХОНОВ, канд. техн. наук, доц., Одесская НАС им. А.С. Попова
О.В. ГОЛУБОВА, асп., Одесская НАС им. А.С. Попова

ПРИНЦИПЫ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ ЦИФРОВЫХ ПОТОКОВ ПО ТЕХНОЛОГИИ UA-ITT