КОМПЬЮТЕРНАЯ МАТЕМАТИКА

С целью реализации эффективной обработки, кодирования и шифрования данных на абонентских системах беспроводных сетей в работе обоснован комплекс выполняемых базовых математических операций с учетом требований к быстродействию и точности обработки исходных массивов данных, степени сжатия информации, требований к криптостойкости и помехоустойчивости пакетов информации, отправляющиеся в открытые каналы связи с шумами.

УДК 681.31

Б.М. ШЕВЧУК

ОБ ЭФФЕКТИВНЫХ АЛГОРИТМАХ ОБРАБОТКИ, КОДИРОВАНИЯ И ШИФРОВАНИЯ ДАННЫХ НА АБОНЕНТСКИХ СИСТЕМАХ БЕСПРОВОДНЫХ СЕТЕЙ

Введение. Наше время характеризуется бурным развитием и применением компьютерных сетей, систем и устройств. Широкое применение компьютерных сетей в различных областях человеческой деятельности, в быту обусловлено высокими темпами развития информационно-коммуникационных технологий. Особенно быстро развиваются беспроводные персональные, сенсорные, локально-региональные и наземно-космиче-ские радиосети. Повышение эффективности функционирования действующих и перспективных беспроводных сетей достигается путем реализации абонентами сети (т. е. в местах образования первичных информационных потоков) информационно-эффективной обработки, кодирования и шифрования данных, подлежащих передаче в каналах связи компьютерных сетей [1, 2]. Поскольку минимальной единицей посылки данных в радиоканале является информационный пакет (ИП), то эффективность передачи данных, надежность доставки информации и защищенность радиосетей определяется информационной емкостью (информативностью) битовых и канальных посылок ИП, защищенностью их как от доступа к двоичным данным несанкционированных пользователей сети, так и от подмены данных злоумышленниками, а также защищенностью посылок ИП от действия канальных помех. Соответственно, в канал связи абонентские системы (станции) беспроводных сетей должны передавать безизбыточные, крипто-

стойкие и помехоустойчивые пакеты информации. При этом эффективность функционирования беспроводных сетей, надежность и защищенность передачи данных существенно зависит от производительности вычислительных средств абонентских систем (АС), эффективности алгоритмов компактного кодирования данных, шифрования/дешифрования данных с заданной степенью криптозащиты, алгоритмов помехоустойчивого кодирования/декодирования данных, а также от энергетического соотношения сигнал/шум битовых и канальных посылок ИП.

Цель работы – обоснование комплекса выполнения математических операций для реализации абонентами беспроводных сетей оперативной информационно-эффективной обработки, кодирования и шифрования данных в местах их образования. При этом в результате комплексной обработки и кодирования данных в сеть передачи информации отправляются достоверные, безизбыточные (псевдохаотические) порции данных в виде компактных, криптостойких и помехоустойчивых пакетов информации с учетом достижения заданного уровня криптозащиты данных в сети и защиты данных от текущих канальных помех.

Методологические и алгоритмические основы эффективной обработки, кодирования и шифрования данных на АС. Основой комплексной обработки, кодирования и шифрования данных на АС беспроводных сетей являются математические методы оперативной фильтрации, сжатия сигналов и изображений с учетом ввода и компактного кодирования достоверных и информативных отсчетов сигналов (видеосигналов), компактного кодирования массивов данных, криптостойкого шифрования и помехоустойчивого кодирования данных, подлежащих передаче по каналам связи с шумами, а также накоплению в базах данных и на электронных накопителях. При этом важно оптимизировать процесс обработки, кодирования и шифрования данных на АС по быстродействию и точности кодирования (шифрования) с учетом достижения заданных величин степени защиты информации в сети для поддержки необходимого уровня криптозащиты данных и защиты данных от искажений импульсными и промышленными помехами, проникающие в радиоканалы. Для достижения надежной передачи информации по радиоканалам в процессе формирования ИП целесообразно использовать шумоподобные сигналы (ШПС) с большой базой, позволяющие реализовать криптостойкую и помехоустойчивую передачу информации, скрытую в шумах радиоканала [1–3].

Основой эффективного функционирования АС беспроводных сетей является программно-аппаратная реализация разнообразных по типу (функциональному назначению) и уровню (сложностью и эффективностью соответствующих методов и алгоритмов) адаптационных процессов во время ввода, обработки, кодирования и шифрования данных, а также адаптивной передачи ИП с учетом текущего уровня шумов в радиоканале. Поскольку каналом связи считаются все ресурсы и средства, находящиеся между отправителем и получателем информации, то повышение эффективности функционирования программно-аппаратных средств АС достигается повышением эффективности работы средств информа-

ционного уровня (уровня ввода, обработки, кодирования, шифрования данных, фомирования интервально-импульсных и шумоподобных сигналов) и средств радиотехнического уровня (средств многопозиционной модуляции, формирования ортогональных несущих и поднесущих, интеллектуальных антенных систем). Для обеспечения надежной и высокоскоростной передачи ИП в беспроводных сетях без существенного усложнения радиотехнического оборудования АС целесообразно реализовать децентрализованную передачу информации от соседней к соседней АС с самоорганизацией ретрансляции пакетов информации и с учетом наличия альтернативных путей передачи (ретрансляции) ИП. При этом в процессе встановления связи соседние абоненты должны оперативно определять уровень шумов в радиоканале и выбирать минимально необходимую базу канальных сигналов $B_{\min}$ [2], а каждый абонент в местах образования информационных потоков формирует компактные, криптостойкие и помехоустойчивые пакеты информации. Следует отметить, что от качества алгоритмов обработки, кодирования, шифрования данных, формирования канальных сигналов, которые по своим характеристикам должны соответствовать необходимому энергетическому соотношению сигнал/шум в радиоканале, существенно зависят характеристики всей системы передачи данных.

Алгоритмической основой информационно-эффективной обработки и кодирования данных являются методы и алгоритмы оперативной фильтрации, сжатия и защиты компактных массивов данных (криптозащиты и помехоустойчивого кодирования) [2] в местах их образования. Наиболее информационно емкими являются измерительные сигналы и изображения (фиксированные и подвижные). В сигналах и видеосигналах наиболее информативными являются экстремумы и точки перегиба, амплитудно-временные характеристики которых в процессе сжатия и кодирования/декодирования должны быть неизменными (точными) или приблизительно точными. После фильтрации, сжатия и криптостойкого кодирования данных программно-аппаратными средствами АС формируются псевдохаотические безизбыточные массивы данных, подлежащие помехоустойчивому кодированию. В интегрированных и разветвленных (многоячейковых) сетях пакеты информации от пары абонентов (отправитель – получатель ИП) передаются с использованием ресурсов промежуточных абонентов-ретрансляторов. Поэтому для надежной защиты данных (для защиты от подмены данных и от доступа к содержанию информации) в разветвленных сетях только соответствующие пары абонентов должны владеть секретными (закрытыми) ключами. Поэтому основная проблема защиты инфомации в распределенных компьютерных сетях состоит в распространении секретных ключей, которые используются в процедурах аутентификации и шифрования данных. Для обеспечения полной секретности передачи данных необходимо, чтобы при передаче каждого пакета данных текущий секретный шифр использовался только один раз.

Информационно-эффективная передача данных в беспроводных сетях достигается путем поддержки соседними абонентами сети минимально необходимого (оптимального) энергетического соотношения сигнал/шум в радиоканале, бесконфликтной передачи компактных, криптостойких и помехоустойчивых ИП. При заданных величинах рабочей полосы частот F и вероятности ошибочного приема элементарного дискретного сигнала или кодовой последовательности P_n эффективность функционирования сети передачи информации характеризуется показателем информационной эффективности системы $\eta = R / C$, где $R_{\max} = f(F, P_n, E_b / J_o, 1/B, K_{cm})$ – текущая скорость передачи информации, C – пропускная способность канала связи (теоретическая максимальная скорость передачи информации), E_b / J_0 – энергетическое соотношение сигнал/шум, $E_b = S \cdot T_b$ – удельная энергия битовой посылки, S – мощность сигнала, T_b – длительность битовой посылки, $J_0 = J / F$, J – средняя мощность суммарных помех в радиоканале, $B = F \cdot T_b$ – база сигнала (коэффициент расширения спектра сигнала), K_{cm} – суммарный коэффициент сжатия данных, которые подлежат как до передачи ИП, так и в процессе передачи ИП, включая сжатие данных с допустимыми (контролированными) потерями информации, которые характерны при обработке и кодировании сигналов и изображений, сжатие данных без потерь информации, сжатие данных в процессе формирования и передачи ИП [1], которое осуществляется на информационном уровне обработки и кодирования данных, а также на радиотехническом уровне путем уплотнения каналов передачи информации. Достижение максимальной текущей скорости передачи информации R_i при условии поддержки необходимого энергетического соотношения $(E_b / J_o)_n$ в радиоканале осуществляется путем адаптивного выбора минимально необходимой базы канальных сигналов $B_{\min}$, при этом скорость передачи информации определяется выражением

$$R_i = K_c \cdot L / k_s \cdot T_b \cdot B_{\min},$$

где $K_c = K_i \cdot K_{rt}$ – суммарний коэффициент сжатия данных; K_i – коэффициент сжатия данных на информационном уровне; K_{rt} – коэффициент сжатия данных на радиотехническом уровне; L – количество ортогональных ШПС, которые асинхронно (независимо) передаются в общем радиоканале $(L \le B/4)$ (величина L соответствует количеству независимых кодовых моноканалов в полосе частот F); k_s – коэффициент, учитывающий качество возобновления фронтов двоуровневых (цифровых) сигналов ($k_s > 1.4...1.8$).

Для достижения высокой информационной эффективности передачи данных с учетом требований к быстродействию и точности обработки исходных потоков данных, степени сжатия информации, требований к криптостойкости и помехоустойчивости ИП в процессе комплексной обработки, кодирования и шифрования данных на АС беспроводных сетей целесообразно реализовать совокупность различных видов адаптаций.

В процессе сжатия данных с допустимыми потерями информации целесообразно определять амплитудно-временные характеристики наиболее информативных отсчетов, включая экстремумы и точки перегиба огибающей сигнала (видеосигнала), а выходные потоки данных необходимо кодировать разностными кодами. С целью уменьшения частоты опроса (анализа) отсчетов сигналов и минимизации вычислительных операций в процессе фильтрации-сжатия сигналов необходимо определять усредненную крутизну сигнала и в зависимости от ее величины определять коэффициент прореживания исходной выборки сигнала $K_{пр}$. Оперативно текущую крутизну сигнала определяют путем вычисления текущего приращения отфильтрованного сигнала $\Delta X_i^F = X_i^F - X_{i-1}^F$, где $X_i^F -$ значение *i*-го отсчета отфильтрованного сигнала. При $\Delta X_i^F > \Delta X_{доп}$ точки перегиба не определяются, где $\Delta X_{доп} -$ предварительно заданная допустимая величина крутизны сигнала. С точки зрения реализации оперативной обработки данных коэффициент $K_{пр}$ определяется с учетом выполнения таких условий:

$$\Delta X_{i\max}^F / 2 < \Delta X_i^F \le \Delta X_{\max}^F, \qquad K_{рп} = 1;$$

$$\Delta X_{i\max}^F / 4 < \Delta X_i^F \le \Delta X_{i\max}^F / 2, \qquad K_{пр} = 2;$$

$$\Delta X_{i\max}^F / 8 < \Delta X_i^F \le \Delta X_{i\max}^F / 4, \qquad K_{пр} = 4;$$

$$\Delta X_i^F < X_{i\max}^F / 8, \qquad K_{пр} = 8.$$

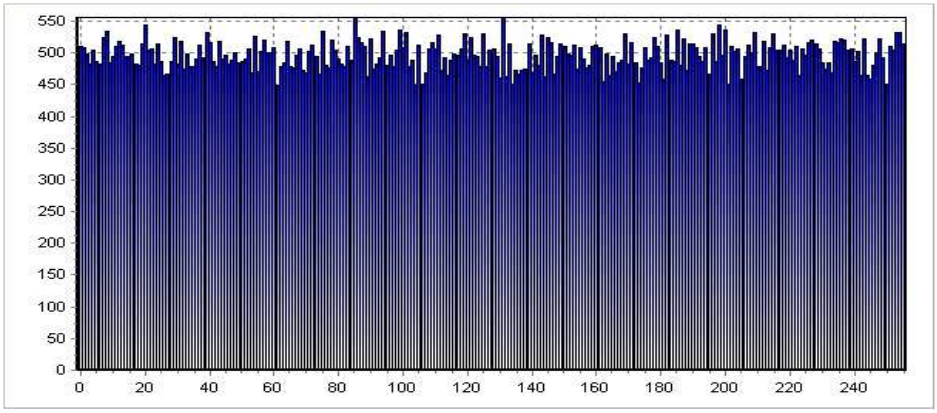
В зависимости от уровня шумов в сигнале точность кодирования информативных отсчетов сигналов может быть различной: на зашумленных участках точность определения амплитудно-временных параметров отсчетов ограничивается с учетом внесения минимальных искажений огибающей сигнала, которые не изменяют ее визуальные характеристики.

После сжатия с допустимыми потерями в выходном массиве данных присутствуют избыточные последовательности двоичных данных. Поэтому дальнейшее компактное кодирование данных достигается на основе реализации оперативных методов сжатия двоичных последовательностей без потери информации [2].

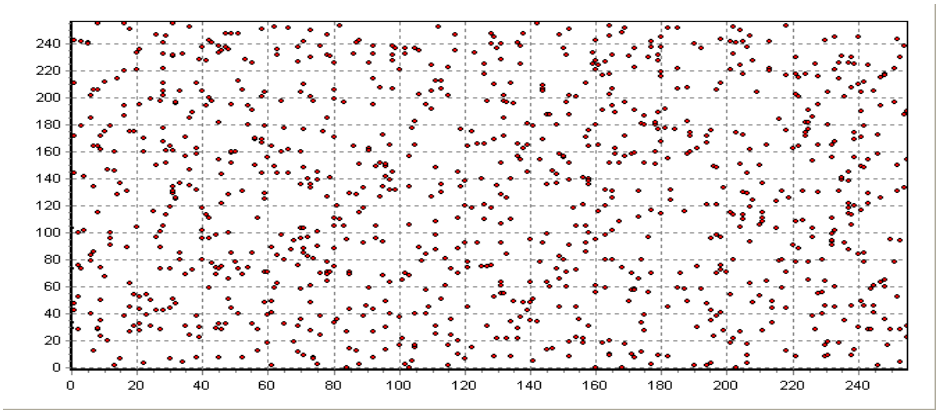
Для криптозащиты компактных массивов данных с заданной величиной защиты информации P_z необходимо шифровать *l*-битовые последовательности сжатых массивов данных с применением одноразовых шифров [1, 2], где $P_z = \max[2^l]$, где $l > 2048$. При этом основой криптографического шифрования ИП является генерация парой абонентов «отправитель ИП – получатель ИП» криптостойких псевдослучайных последовательностей, которые от пакета к пакету являются переменными. Ключевой проблемой защиты данных в сетях является проблема распространения секретных ключей, которая эффективно решается средствами ассиметричной криптографии. Учитывая, что при передаче пакетов информации между удаленными абонентами (парами отправитель-получатель информации) компьютерных сетей принимает участие большое количество промежуточных абонентов, маршрутизаторов, то средствами абонентских станций целесообразно формировать и передавать в каналы связи безизбыточные псевдохаотические, криптостойкие и помехоустойчивые пакеты информации, закодированные и зашифрованные с применением соответствующих секретных ключей, которые известны только получателю и отправителю информации. При этом дополнительные средства защиты данных на различных уровнях компьютерных сетей исключают доступ к передаваемым данным для несанкционированных пользователей сети и злоумышленников. На рисунке показаны результаты кодирования изображения авиационного цеха: а – изображение цеха; б – распределение q – битовых символов ($q = 8$) закодированного и зашифрованного изображения; в – хаосграмма (зависимость предыдущего символа от последующего) закодированного и зашифрованного изображения. Приведенные результаты анализа показывают, что результирующие массивы данных, образующих основу ИП, являются псевдохаотическими и безизбыточными данными. Для реализации криптостойкой и замаскированной (в шумах радиоканала) передачи информации неизвестными для других абонентов должны быть методы сжатия-защиты данных, методы формирования сигналов, подлежащих передаче по радиоканалу, а также структура этих сигналов. Поэтому защита данных абонентами радиосети должна быть реализована на различных уровнях: на информационном уровне, на уровне формирования сигнально-кодовых конструкций, на энергетическом уровне.

Повышение помехоустойчивости передачи ИП достигается путем перемешивания данных, которые передаются различными пакетами, реализации помехоустойчивого кодирования данных с применением кодов Галуа, передачи проверочных кодов ИП в виде шумоподобных сигналов с базой, которая позволяет надежно передать и принять проверочные последовательности.

а



б



в

РИСУНОК. Результаты кодирования и шифрования изображения авиационного цеха

Выводы. Передача компактных, криптостойких и помехоустойчивых пакетов информации в беспроводных сетях достигается на основе реализации абонентами сети оперативных алгоритмов фильтрации-сжатия данных с определением параметров экстремумов и точек перегиба огибающих сигналов, разностного кодирования данных, устранения избыточности двоичных последовательностей, шифрования данных ИП с применением одноразовых шифров, помехоустойчивого кодирования данных ИП с применением кодов Галуа и ШПС, а также применением абонентами сети средств двоключевой криптографии.

Б.М. Шевчук

ПРО ЕФЕКТИВНІ АЛГОРИТМИ ОБРОБКИ, КОДУВАННЯ І ШИФРУВАННЯ ДАНИХ НА АБОНЕНТСЬКИХ СИСТЕМАХ БЕЗПРОВОДОВИХ МЕРЕЖ

З метою реалізації ефективної обробки, кодування і шифрування даних на абонентських системах радіомереж у роботі обґрунтоване виконання комплексу базових математичних операцій з урахуванням вимог до швидкодії й точності обробки вхідних потоків даних, ступеня стиску інформації, вимог до крипостійкості та завадостійкості пакетів інформації, які відправляються у відкриті канали зв'язку з шумами.

B.M. Shevchuk

ABOUT THE EFFECTIVE ALGORITHMS OF PROCESSING, CODING AND DATA ENCRYPTION AT SUBSCRIBER SYSTEMS OF WIRELESS NETWORKS

In order to implement efficient processing, encoding, and encryption of data at subscriber wireless systems, a complex of basic mathematical operations subject to the requirements on speed and accuracy of processing incoming data streams, the degree of compression of information, the requirements on reliability and noise immunity of information packages that are sent into open communication channels with noise is justified.

1. *Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.* Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах. – К.: Наук. думка, 2010. – 370 с.
2. *Шевчук Б.М.* Оброблення, кодування та передавання даних засобами абонентських систем інформаційно-ефективних радіомереж // Комп'ютерні засоби, мережі та системи. – 2010. – № 9. – С. 130–139.
3. *Урядников Ю.Ф., Аджемов С.С.* Сверхширокополосная связь. Теория и применение. – М.: СОЛОН-Пресс, 2005. – 368 с.

Получено 04.11.2011

Об авторе:

Шевчук Богдан Михайлович,
кандидат технических наук, старший научный сотрудник

Института кибернетики имени В.М. Глушкова НАН Украины.
e-mail: incors@ukr.net