МОДИФИКАЦИЯ КАНАЛЬНОГО УРОВНЯ СЕТЕЙ 802.11 ДЛЯ АДАПТИВНЫХ АНТЕНН

А.Ю. Ельцов, М.А. Соколов, М.О. Шуралев

Нижегородский госуниверситет

В настоящее время большой интерес представляют дальние линки (>1,5 км) на базе технологии 802.11 (WiFi). Для их построения обычно применяются направленные антенны различных конструкций вместе со стандартным оборудованием 802.11b/g [1].

Однако при этом возникает целый ряд проблем: юстировка антенн с шириной главного лепестка в 10 градусов на расстоянии нескольких километров представляется непростой задачей, протоколы 802.11 даже при использовании направленных антенн не обеспечивают одновременную работу по нескольким направлениям. Более того, имеются проблемы связанные с большим временем распространения пакета – величина временного окна подтверждения (SIFS) оказывается недостаточной и пакет считается потерянным, в результате чего инициируется его повторная передача. И, наконец, реализация топологии типа «звезда» на больших дистанциях требует наличия на точке доступа нескольких адаптеров 802.11 и направленных антенн. При этом возникает необходимость разделения интерфейсов по частотным каналам, что не всегда возможно.

Табл. 1

Параметр	*Значение*
КНД	21 dBi
Ширина главного лепестка	10 град.
Диапазон углов перестройки	[-60;+60] град.
Время переключения	1-2 мс

Многие из обозначенных проблем могут быть решены путем применением адаптивных антенн с одновременной модификацией канального уровня 802.11 на уровне драйвера. В данной работе мы ставим задачу получения устойчивого соединения типа «один – ко многим» на больших дистанциях (>5 км), используя на точке доступа конфигурацию с одной адаптивной антенной и одним адаптером 802.11.

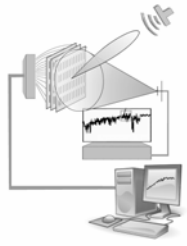

Рис. 1

Разработанная адаптивная антенная система состоит из решетки пассивных рассеивателей с управляемым импедансом и активного излучателя (см. рис. 1). Её характеристики представлены в Табл. 1.

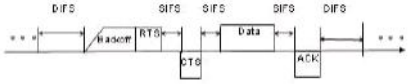

Рис. 2

Основной проблемой, препятствующей эффективному использованию адаптивных антенн в сетях 802.11, является режим DCF канального протокола 802.11(CSMA/CA) [1]. Во-первых, механизм контроля несущей блокирует все направления передачи в случае наличия несущей в канале (физической и виртуальной) и, во-вторых, как уже было отмечено выше, время распространения пакета превышает стандартные временные интервалы SIFS и DIFS (см. рис. 2), что приводит к потерям пакетов. Существует несколько классов решений указанных проблем: временное разделение (TDMA) с синхронизацией отдельных линков [2] и всей сети [3]; 802.11 PCF [1] – опциональная часть стандарта, предполагающая арбитраж со стороны точки доступа (на сегодняшний день не реализована в абсолютном большинстве доступного оборудования); асинхронные модификации с использованием направленной виртуальной несущей (DNAV) [5, 6].

Мы рассматриваем схему с временным разделением (TDMA) типа «многие – к одному» (один мастер-узел и несколько подчиненных): хорошо известно, что идеальная слотовая схема обеспечивает 100% использование канала в режиме полудуплекса, однако в нашем случае конечного времени переключения антенны (порядка 1 мс) эффективность схемы снижается. На рис. 3 представлена временная диаграмма для мастер-узла: вверху – идеальная, внизу – с конечным временем переключения антенны (слоты без обозначений), здесь RX1, TX1 – прием и передача первому подчиненному узлу соответственно, RX2, TX2 – второму подчиненному узлу. Легко видеть, что при длительности слота в 10 мс и времени переключения 2 мс теряется 20% пропускной способности. Вследствие роста задержек передачи пакетов в канале эффективность TCP также снижается, и реальная пропускная способность составляет около 50%. Кроме того, при практической реализации данной схемы поверх 802.11 невозможно обеспечить идеальную синхронность в рамках сети, поэтому пропускная способность падает до 20% от теоретического предела. Приведенная схема подразумевает модификацию драйверов как на мастер-узле (точке доступа), так и на подчиненных узлах (клиентах), что ограничивает ее применимость. Для обеспечения совместимости с клиентами 802.11 может быть предложена другая схема на базе DCF, включающая два режима: сканирования (обнаружение новых клиентов) и обмена данными, при этом сканирование должно происходить за время порядка SIFS. Для эффективной реализации описанной схемы необходимо обеспечить переключение антенны синхронно с передачей управляющих пакетов, что невозможно без серьезных доработок прошивок беспроводных адаптеров (минимальный временной интервал синхронизации, доступный на драйверном уровне составляет примерно 20 SIFS). При этом для решения проблем, связанных с большим временем распространения, все пакеты могут быть преобразованы в широковещательные, для которых подтверждение не используется.

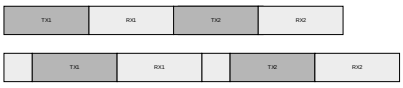

Рис. 3

В ближайшей перспективе будет проведено детальное моделирование предложенной асинхронной схемы и оценка пропускной способности каналов. Необходи-

мо уменьшить время переключения антенны и рассмотреть возможность синхронизации по управляющим пакетам. Кроме того, имеются следующие пути повышения эффективности TDMA схемы: уменьшение времени переключения антенны и применение протоколов транспортного уровня, способных эффективно функционировать в случае больших (~ 0,5 с) задержек в канале.

[1] ANSI/IEEE 802.11 Std 1999 Edition(R 2003), IEEE-SA Standard Board, 2003
[2] Raman B., Chbrolu K. // MobiCom'05. 2005. P. 156.
[3] http://www.ecel.ufl.edu/~jwang/publications_files/Milcom05_WANG.pdf
[4] Takai M., Martin J., Ren A., Bagrodia R. // MOBIHOC'02. 2002.
[5] Ramanathan R., Redi J., Santivanez C., Wiggins D., Polit S. // IEEE Journal on Selected Areas in Comm. 2005. V. 23, No.3. P. 496.

ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ И РЕАЛИЗАЦИЯ АДАПТИВНОЙ АНТЕННЫ ТИПА UDA-YAGI

В.В. Артемьев, Д.А. Ильина, М.Н. Кайнов, А. П. Смирнов

Нижегородский госуниверситет

Работа посвящена моделированию и созданию прототипа экономичной адаптивной антенны типа Uda-Yagi [1], предназначенной для организации дальних беспроводных Интернет-каналов. Антенна Uda-Yagi построена на базе полуволнового вибратора из элементов, расположенных в одной плоскости (см. рис.). Активный элемент антенны (1) представляет собой стандартный полуволновый вибратор, к которому подводится сигнал. Рефрактор (2) служит для увеличения излучения в прямом направлении и уменьшения – в обратном. Директоры (3) предназначены для увеличения коэффициента направленного действия.

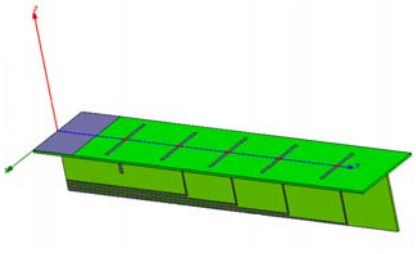

Рис.1

Основной проблемой при создании таких антенн является то, что они очень чувствительны к погрешностям в изготовлении: даже небольшая вариация геометрических размеров активных элементов антенны (±0,5 мм) либо нарушение симметрии в их расположении, может привести к сильному уменьшению коэффициента направленного действия.

В ходе выполнения работы была предложена модель антенны, позволяющая управлять электрической длиной директоров с помощью добавления в них диодов-варакторов, что позволило бы устранять влияние неточностей монтажа, флюктуаций диэлектрической проницаемости текстолита и т.д. Изменяя напряжение смещения на варакторе, можно варьировать электрическую длину директора. Для

решения этой задачи было разработано устройство управления напряжением на базе микроконтроллера MSP430F1611 со сверхнизким энергопотреблением.

Принцип работы устройства основан на формировании сигналов с широтно-импульсной модуляцией (ШИМ) и их последующего преобразования в постоянные уровни с помощью интегрирующей цепочки. Характерным отличием является, то что в устройстве заложена возможность проведение вычислений.

Для учета влияния напряжения смещения на варакторах на характеристики антенны была разработана оптимизационная программа, осуществляющая подбор необходимых значений напряжений смещения при помощи специального адаптационного алгоритма, работающего в режиме реального времени. Его основой стал генетический алгоритм (ГА) [2], являющийся комбинацией переборного и локально-градиентного методов, где механизмы скрещивания и мутации реализуют переборную часть метода, а отбор лучших решений – градиентный спуск.

Кроме того, ГА обеспечивает возможность быстрого нахождения антенным комплексом источника сигнала при первом запуске системы или при разрыве канала связи. ГА обладает следующими преимуществами [3]:

- не требует никакой дополнительной информации о целевой функции;
- устойчив к попаданию в локальные экстремумы;
- хорошо работает при решении задач многомерной оптимизации;
- может быть использован для широкого класса задач;
- прост в реализации.

Было выполнено численное моделирование и оптимизация параметров антенны для ее последующей реализации.

В результате проведенных исследований была получена антенная система со следующими характеристиками: коэффициент усиления – 8dBi; входное сопротивление антенны – 60 Ом; ширина главного лепестка – 60^0. Использование варакторов позволило варьировать электрическую длину директоров в диапазоне ±2 мм.

Были решены следующие задачи:

- электродинамическая задача – разработка адаптивной антенны Uda-Yagi, составленной из элементов, лежащих в одной и той же горизонтальной плоскости с настраиваемыми электрическими длинами директоров.
- алгоритмическая задача – разработка оптимизатора, работающего на персональном компьютере для управления напряжениями смещения на нагрузках, в целях максимизации уровня мощности принимаемого сигнала;
- схемотехническая задача – разработка аппаратного управляющего устройства с логической схемой, которая генерирует напряжения смещения варакторов.

[1] Ротхаммель К., Кришек А. Антенны. Том 2 / Пер. с нем., 2005. 416 с.
[2] Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы /Под ред. В.М. Курейчика. 2-е изд., испр. и доп. М.: ФИЗМАТЛИТ, 2006. 320 с.
[3] Miller B.L., Goldberg D.E. Genetic algorithms, selection schemes, and the varying Effects of noise // Evolutionary Computation. 1997. V.4(2). P.113.

ИСПОЛЬЗОВАНИЕ ФИКСИРОВАННОГО КОЭФФИЦИЕНТА КОРРЕКЦИИ В ПРОТОКОЛАХ СИНХРОНИЗАЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

В.О. Анисимов[1)], А.А. Садков[2)]

[1)]*Рижский технический университет*
[2)]*Нижегородский госуниверситет*

Особенностью беспроводных сенсорных сетей является энергосберегающий режим работы приемника, который включается только в момент обмена данными. Однако существует проблема расхождения локального времени узлов сети, требующая использования протоколов синхронизации.

Стандартные методы синхронизации, такие как GPS или UTC (например, в протоколе Remote Clock Reading [1]), регулярно используются в протоколах обычных сетей, но для беспроводных сенсорных сетей эти решения не подходят из-за следующих ограничений: энергия, пропускная способность, аппаратные возможности и нестабильные соединения в сети.

В беспроводных сенсорных сетях временные расхождения в основном возникают по двум причинам:

1. сетевые задержки и время обработки сообщения аппаратным и программным обеспечением;
2. нестабильность кварцевого осциллятора.

Рассинхронизации временных осцилляторов возникает из-за усреднения локального времени в момент исправления. При длительности интервала между исправлениями меньшей, чем несколько сотен секунд, узлы рассинхронизируются из-за сетевых задержек, а при большем интервале – из-за нестабильности кварцевого осциллятора [2].

Протоколы в беспроводных сенсорных сетях обеспечивают временную синхронизацию сенсорных узлов от нескольких (RBS) до сотен микросекунд (Sichitiu). Однако использование любого протокола требует интенсивного обмена сообщениями, а объем служебного трафика резко возрастает при увеличении количества узлов в сети. При этом стоит отметить, что энергия, необходимая для передачи 1 бита на расстояние 100 метров, составляет 3 джоуля, что достаточно для исполнения 3 миллионов инструкций [3]. Это доказывает, что обмен данными между узлами сети является намного более энергоемким процессом, чем вычисления. Фактически, в малоэнергетических радиосетях посылка, прием сообщений и прослушивание канала требуют даже больше энергии, чем в проводных сетях [4].

Таким образом видно, что точная временная синхронизация, требующая интенсивного обмена сообщениями между узлами, сильно уменьшает эффект регулярного отключения приемников. Одним из возможных вариантов уменьшения количества служебных сообщений между узлами является использование протоколов с вероятностной синхронизацией. Такие протоколы позволяют уменьшить служебный трафик между узлами благодаря использованию вероятной, а не рассчитанной, ошибки. К тому же эти протоколы позволяют, увеличивая максимально возможную

ошибку между узлами, уменьшить обмен данными и сэкономить вычислительные и энергетические ресурсы сенсорного узла [1, 5].

Некоторым приложениям, требующим относительного, а не абсолютного хронометража событий, хватает достаточно редкой синхронизации времени. При таких интервалах между исправлениями (раз в несколько минут), расхождение в локальном времени узлов возникает, в основном, из-за нестабильности кварцевого осцилятора.

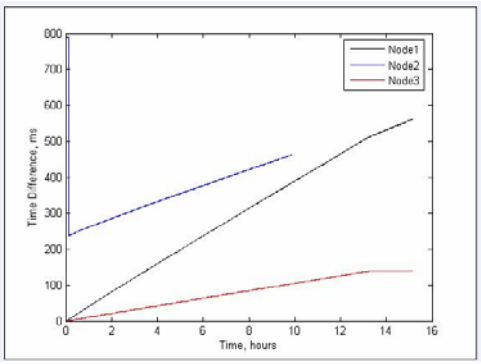

Рис. 1. Расхождение локальных часов сенсорных узлов

Авторами проведен эксперимент, в рамках которого была попытка найти зависимость в расхождениях локального времени узлов сети. Результаты эксперимента показали стабильную рассинхронизацию узлов (рис.1).

Используя линеаризацию каждой кривой, рассинхронизацию можно выразить линейной функцией с фиксированным коэффициентом расхождения:

$$T_{offset} = k \cdot T_{base}, \quad (1)$$

где T_{offset} – разница во времени, k – коэффициент рассинхронизации, T_{base} – локальное время базовой станции.

Линеаризация позволяет при начальном кратковременном обмене данными рассчитать коэффициент рассинхронизации для каждого из узлов сети. Зная коэффициент рассинхронизации, каждый узел может корректировать свое локальное время, используя только свои вычислительные ресурсы. Благодаря этому, можно существенно уменьшить объем служебного трафика, необходимого для синхронизации узлов.

Однако при практическом использовании данного метода могут появиться два осложнения: необходимость первоначального поиска узла в сети с самым быстрым временным осциллятором и подверженность кварцевого резонатора температурным колебаниям.

Необходимость поиска узла с самым быстрым временным осциллятором обусловлена соблюдением порядка возникновения событий в сети даже при регулярном изменении локального времени узлов [6]. При выполнении этого условия все события в сети будут привязаны к самому быстрому временному осциллятору, а остальные сенсорные узлы должны корректировать свое время под самый быстрый узел.

Вторая проблема заключается в том, что при температурных изменениях коэффициент корректировки может меняться (рис. 2, 3).

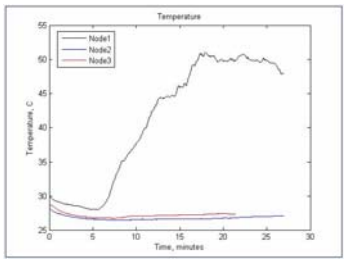

Рис. 2. Изменение температуры.

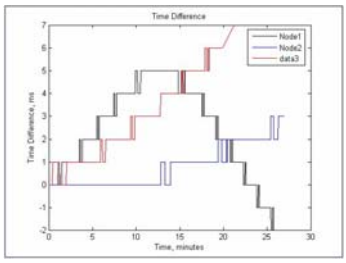

Рис. 3. Влияние температуры на расхождение локальных часов

Результаты эксперимента показывают, что функция расхождения времени при температурных изменениях хоть и меняется, но все равно сохраняет линейность. Т.е., если температурные колебания не являются скачкообразными и постоянными, то этот метод не теряет актуальности, а только требует перерасчета коэффициента изменения в случае изменения температуры.

В эксперименте сделана попытка найти альтернативу стандартным протоколам временной синхронизации узлов. Результаты эксперимента показывают, что использование фиксированного коэффициента корректировки хоть и не исключит полностью, но позволит снизить объем служебного трафика в сети. Однако малое количество служебных сообщений ограничивает возможности применения данного метода в средах с большой вероятностью потери пакетов.

[1] Cristian F. Probabilistic Clock Synchronization. Distributed Computing, 3. Springer-Verlag, 1989. P. 146.
[2] Sullivan D.B., Allan D.W., Howe D.A. and Walls F.L. (Eds.). // National Institute of Standards and Technology Technical Note 1337. 1990. U.S. Government Printing Office. TN61.
[3] Pottie G. and Kaiser W. Wireless Integrated Network Sensors. Communications of the ACM. 2000. V.43(5). P. 51.
[4] Elson J., Romer K. // Proc. First Workshop on Hot Topics In Networks (HotNets-I), Princeton, New Jersey. 2002. V.10.
[5] PalChaudhuri S., Saha A., Johnson D.B. // Technical Report TR 03-418, Department of Computer Science, Rice University, 2003.
[6] Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM. 1978. V. 21(7). P. 558.

СТЕНОГРАФИЯ В СЕНСОРНЫХ СЕТЯХ

М.О. Смирнов, М.С. Царев

Нижегородский госуниверситет

Для обеспечения безопасной передачи данных необходимо осуществлять их шифрование. Используемый алгоритм должен обеспечивать достаточную надежность защиты информации, но, вместе с тем, сенсорная сеть предъявляет к алгоритму высокие требования по его экономичности.

Классическим подходом к задаче шифрования являются блочные шифры [1]. Такие шифры обеспечивают высокую (часто даже избыточную) надежность, но вместе с тем являются весьма ресурсоемкими при исполнении. Кроме того, все они осуществляют шифрование данных пакетами фиксированной длины, что увеличивает потери при передаче информации, т.к. весь блок должен быть передан целиком.

Альтернативой блочным шифрам являются шифры поточные (стенографические) [2], отличающиеся большой производительностью, как за счет быстродействия, так и из-за возможности шифрования пакета данных любой длины. Обычно такие шифры применяются там, где необходимо осуществлять быстрое шифрование объемов информации в реальном времени (например, A5 – алгоритм, используемый в мобильной связи). Особенностью таких алгоритмов являются высокие требования к каналу передачи данных. В обычном случае потеря одного пакета приводит либо к «падению» канала данных, либо к потере группы последующих, что делает невозможным их применение в условиях нестабильной связи.

В работе рассмотрена возможность применения таких алгоритмов для использования в сенсорной сети. Для алгоритма SEAL [3] нами был предложен метод, позволяющий обойти ограничения, накладываемые на канал. В алгоритме SEAL шифрование/дешифрование пакета зависит от его номера в списке пакетов. При потере пакета нумерация сбивается, что делает расшифровку последующих пакетов невозможной. Предлагается при ошибке дешифрования увеличивать номер сообщения до получения корректного результата или же до определенного числа неудачных попыток. Это число определяется в зависимости от параметров сети: должна быть пренебрежимо мала вероятность потери n пакетов, идущих подряд (n – максимальное число попыток дешифрования) при «нормальных условиях», в отсутствии атаки на сеть. Потеря большего числа пакетов будет означать атаку, и в этом случае лучшим выходом является прерывание связи с атакованным сенсором.

Проведено сравнительное тестирование алгоритма SEAL и алгоритма ГОСТ с использованием среды разработки MSP CrossWoks.

Результаты показали высокую эффективность SEAL по сравнению с ГОСТ (на шифрование одного сообщения – 33 тыс. циклов SEAL, 100 тыс. циклов – ГОСТ). Проведено моделирование канала, в котором возможны ошибки, приводящие к потере пакета. На графике изображены затраты на дешифрование принятых сообщений (в тысячах циклов) при ста переданных в зависимости от вероятности возникновения ошибок. При количестве ошибок до 30% алгоритм SEAL по скорости

превзошел ГОСТ более чем в два раза. Затраты процессорного времени оказываются равными только при 66% ошибок (см. рис.).

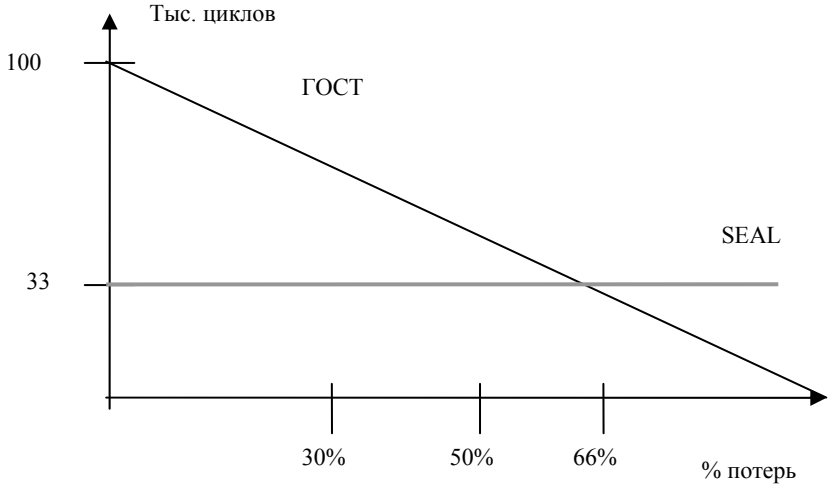

Рис.

Таким образом, применение алгоритма SEAL позволяет достичь значительной экономии процессорного времени и, как следствие, повышения времени автономной работы сенсора. Для получения полного представления о преимуществах поточного шифрования необходимо учесть, что график построен при условиях, оптимальных для блочного шифрования: длина пакета равна длине блока шифрования. На практике несоответствие между их длинами может значительно увеличить затраты на передачу при использовании блочных шифров. Например, если длина полезного сообщения равна половине длины шифруемого блока (при небольших размерах пакетов сенсорной сети это возможно), то затраты на передачу будут различаться вдвое.

По результатам проведенных исследований можно сделать вывод о высоком потенциале применения отдельных стенографических алгоритмов в сенсорных сетях. В дальнейшем планируется реализовать предложенные методики в рамках протокола передачи данных в сенсорной сети.

Выражаем признательность компании Интел за поддержку проводимых исследований.

[1] Чмора А.Л. Современная прикладная криптография. М.: Гелиос АРВ, 2002.

[2] Асоков А.В., Иванов М.А., Мирский А.А., Рузин А.В, Сланин А.В., Тютвин А.Н. Поточные шифры. М.: КУДИЦ-ОБРАЗ, 2003.
[3] Rogaway P., Coppersmith D. A software-optimized encryption algorithm, Fast Software Encryption, Lecture Notes in Computer Science, New York: Springer-Verlag, 1994.

АНАЛИЗ КРИПТОСТОЙКОСТИ ЭЛЛИПТИЧЕСКОЙ КРИПТОГРАФИИ

И.Д. Лысенков

Нижегородский госуниверситет

Криптостойкость эллиптической криптографии основана на сложности задачи дискретного логарифма на эллиптической кривой (ECDLP), так как при взломе протокола злоумышленник сталкивается с этой задачей. Поэтому для анализа криптостойкости нужно проанализировать ECDLP и методы её решения. ECDLP состоит в том, что по данной эллиптической кривой E над полем F_q, точке P из $E(F_q)$ порядка n и точке Q из $\langle P\rangle$ требуется найти x из Z_n такое, что $Q = xP$. ECDLP является очень сложной задачей, самые быстрые алгоритмы её решения (из опубликованных) имеют экспоненциальную сложность [1].

Сложность ECDLP зависит от порядка точки эллиптической кривой, которая является основанием логарифма. Порядок основания логарифма напрямую связан с длиной используемого в протоколе ключа, поэтому главной целью анализа должно быть получение формулы, выражающей необходимое число операций для решения ECDLP от порядка основания логарифма.

Для получения искомой формулы необходимо проанализировать время работы известных алгоритмов решения ECDLP в зависимости от порядка основания логарифма. При этом нельзя ограничиться рассмотрением только асимптотически самых быстрых алгоритмов, так как при небольших порядках основания, возможно, быстрее будут работать более просто устроенные алгоритмы, но менее быстрые асимптотически. Выбрав самый быстрый алгоритм для каждого порядка основания и оценив время его работы, можно получить искомую формулу.

В настоящей работе проведён анализ по описанной схеме. Установлено, что при любых n, представляющих интерес для криптографии, ρ-метод Полларда [2] с использованием автоморфизмов [1,3] будет самым быстрым алгоритмом для решения ECDLP. Поэтому для решения ECDLP требуется $\sqrt{n\pi}/2$ групповых операций, то есть сложений точек эллиптической кривой. Если одна групповая операция требует m умножений в поле (в среднем m=12 [4]), то, обозначив $n = 2^l$ и учитывая, что в протоколах эллиптической криптографии $q \approx n$, можно найти число операций C, необходимое для решения ECDLP:

$$C = m\frac{\sqrt{\pi}}{2}2^{\frac{l}{2}}l^2.$$

Эта формула позволяет судить о криптостойкости системы по длине используемого ключа.

Выразив l через C, получим вторую формулу:

$$l = \frac{4}{\ln 2} W\left(\frac{\ln 2}{\sqrt{8m\sqrt{\pi}}} \sqrt{C} \right),$$

где $W(x)$ – W-функция Ламберта, определяемая формулой $W(x)e^{W(x)} = x$.

Полученная формула позволяет судить о минимальной длине ключа, необходимой для обеспечения заданного уровня криптостойкости.

ρ-метод Полларда является вероятностным алгоритмом, и все предыдущие оценки рассматривали математическое ожидание числа операций, которые должен выполнить ρ-метод Полларда для решения ECDLP. Однако на самом деле алгоритму может потребоваться как большее число операций, так и меньшее. Поэтому важен вопрос о зависимости вероятности решения ECDLP от количества проделанных операций. Проанализировав алгоритм, получим формулу:

$$P\left(\mu m \frac{\sqrt{\pi}}{2} 2^{\frac{l}{2}} l^2 \right) = 1 - e^{\frac{-\pi}{4}\mu^2},$$

где $P(x)$ – вероятность решить ECDLP, выполнив x операций, μ – доля проделанных итераций от среднего числа итераций, требующихся для взлома.

Эта формула позволяет судить о вероятности успешности атаки на криптосистему с заданной длинной ключа, если злоумышленник выполнит заданное количество операций. Например, если $\mu = 1$, то есть злоумышленник выполнит как раз количество операций, равное математическому ожиданию числа операций, нужных для взлома, то оказывается $P(x) \approx 0{,}544$.

Выразим l через число операций C, проделанных алгоритмом, и вероятность p нахождения дискретного логарифма:

$$l = \frac{4}{\ln 2} W\left(\frac{\ln 2}{4\sqrt{m}} \sqrt{\frac{C}{\sqrt{-\ln(1-p)}}} \right).$$

Полученная формула позволяет судить о минимальной длине ключа, который сможет обеспечить необходимую вероятность успешности атаки на протокол при проделанном злоумышленником объёме вычислений.

Работа выполнена при поддержке компании Интел.

[1] Hankerson D., Menezes A.J., Vanstone S.A. Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004.
[2] Pollard J. // Mathematics of Computation. 1978. №32. С. 918.
[3] Gallant R., Lambert R., Vanstone S. // Mathematics of Computation. 2000. №69. С. 1699.
[4] Lenstra A.K., Verheul E.R. // J. Crypto. 2001. №14. С. 255.

ЛЁГКАЯ ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ

М.О. Смирнов

Нижегородский госуниверситет

Каждый год совершенствуются и улучшаются технологии построения сенсорных сетей, радиометок и других устройств с малой мощностью. В связи с этим представляется актуальным разработка криптографических алгоритмов для таких сетей. Большинство криптографических методов рассчитано на 32-х битные платформы и сравнительно мощные персональные компьютеры. Для маломощных устройств важно реализовать криптографию с открытым ключом, так как она позволит решить проблемы распределения секретных ключей, авторизации и аутентификации.

В криптографии с открытым ключом распространены два подхода: RSA-подобные алгоритмы и алгоритмы, основанные на эллиптических кривых. Первые не удовлетворяют требованием сенсорных сетей, так как длина безопасного ключа составляет 1024 бита, что не приемлемо для сенсорных сетей. Проблема использования эллиптической криптографии связана с вычислительной сложностью алгоритма. На сегодняшний день безопасной длиной ключа для эллиптической криптографии является 160 бит [1].

Сенсорные сети дают возможность оптимизации криптографических алгоритмов за счёт небольшого времени актуальности информации в них. Задача заключается в создании метода построения эллиптической криптографии для сенсорных сетей, учитывая небольшое время жизни информации.

В эллиптической криптографии используются эллиптические кривые над полем $GF(2^{160})$ или $GF(2^{163})$. Для ускорения алгоритмов применяют различные методы уменьшения сложности умножения скаляра на точку и деления [2].

Мы предлагаем уменьшить длину ключа, что оправдывается небольшим временем жизни информации. Необходимую длину ключа можно вычистить по формуле [3]:

$$C = m\frac{\sqrt{\pi}}{2}2^{\frac{l}{2}}l^2.$$

Где $m = 12$ – небольшая константа, l – степень расширения поля Галуа, C – количество операций, необходимое для взлома. Степень расширения поля Галуа совпадает с длиной ключа.

При данном подходе возникает проблема подбора кривых, удовлетворяющих требованиям криптостойкости. Для $l = 160$ эти кривые хорошо изучены (см., например, [4]). Для других показателей набор таких кривых не является тривиальной задачей.

Для проверки на криптостойкость эллиптической кривой $Ep(a, b)$, заданной уравнением

$$Y^2 = X^3 + a\,X + b\ ,$$

где a, b – элементы выбранного поля, необходимо [2]:

- Выбрать характеристику поля p – большое случайное простое число.
- Выбрать a, b – коэффициенты кривой такие что $a, b \bmod p \neq 0$.
- Проверить неравенство дискриминанта $\mathrm{D} = 4a^3 + 27b^2$ нулю (условие несингулярности).
- Найти n – количество точек на кривой и наибольший простой делитель q числа n.
- Проверить неравенство $q \neq p$.
- Проверить неравенство $p^k - 1 \bmod q \neq 0$ для $0 < k < 32$.

При выполнении всех этих условий получим эллиптическую кривую (a, b, p), отвечающую требованиям криптостойкости.

Наиболее сложной является проблема определения количества точек на кривой n и простого делителя q . Она может быть решена за полиномиальное время методом Схоуфа (Rene Schoof) со сложностью $O(\log^6 p)$ [1]. Проблема поверки на простоту решается при помощи методов вероятностного доказательства простоты [5].

В настоящей работе предлагается более простой путь поиска. Для кривых Коблица над $GF(2^k)$:

$$Y^2 + XY = X^3 + X^2 + 1$$

Доказано [6], что число точек на этой кривой равно:

$$E(GF(2^k)) = 2^k + 1 - \frac{(1-\sqrt{-7})^k + (1+\sqrt{-7})^k}{2^k}$$

Воспользовавшись этой формулой и методом проверки чисел на простоту, найдём эллиптические кривые размерности меньше $k = 160$. Проанализируем время взлома. Так как на сегодняшний момент безопасным считается ключ в 160 бит, рассчитаем, какое количество операций необходимо, чтобы взломать его с вероятностью 50%. Рассчитаем такие же параметры для наших длин ключей. Отношение полученных величин к сложности взлома для 160 биного ключа будет относительной криптостойкостью.

Для k=160 бит число операций равно $3 \cdot 10^{29}$.

k	Криптостойкость	q (большое простое)
101	$2 \cdot 10^9$	1267650600228230886142808508011
107	$2 \cdot 10^8$	81129638414606692182851032212511
109	$1 \cdot 10^8$	324518553658426701487448656461467
113	$2 \cdot 10^7$	5192296858534827627896703833467507

В результате выполнения расчетов были найдены эллиптические кривые, удовлетворяющие всем требованиям криптостойкости с длиной ключа меньше 160 бит, а также были рассчитаны границы применимости этих кривых.

Выражаем признательность компании Интел за поддержку проводимых исследований.

[1] Ростовцев А.Г. // Проблемы информационной безопасности. Компьютерные системы. 1999, № 3. С. 37.
[2] Рябко Б.Я., Фионов А.Н. Основы современной криптографии. М.: Научный мир, 2004.
[3] Лысенков И. Д. // Труды XII научной конференции по радиофизике. 7 мая 2008 г. /Ред. А.В.Якимов. Н.Новгород: ННГУ, 2008.
[4] Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. М.: МЭИ, 2000.
[5] http://www.cse.iitk.ac.in/news/primality.pdf
[6] Молдовян Н.А., Молдовян Ф.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритвом. СПб: БХВ-Петебург, 2004.
[7] Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. New York: Springer–Verlag, 2004.
[8] Digital Signature Standard (DSS) / National Institute of Standards and Technology, 2000.
[9] The Elliptic Curve Digital Signature Algorithm (ECDSA) / Certicom Corporation 2001.

ИНТЕГРАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

М.О. Смирнов, Е.А. Солдатов

Нижегородский госуниверситет

Криптография с открытым ключом реализуется в виде множества различных алгоритмов и протоколов. При всем их разнообразии, все они основаны на математических задачах, имеющих NP–сложность. В настоящее время наиболее широко используются три такие задачи: факторизация (разложение на сомножители) больших чисел, вычисление дискретного логарифма и вычисление аналога дискретного логарифма на эллиптической кривой [1].

Безопасность этих криптографических методов основана на том, что в настоящее время не созданы общие математические подходы, позволяющие решать соответствующие математические задачи [2], не прибегая к перебору огромного числа возможных вариантов. Однако есть теоретическая возможность существования таких подходов и алгоритмов. Их открытие привело бы к разрушению почти всех современных криптографических систем. Учитывая это обстоятельство, необходимо создавать новые, альтернативные подходы к решению криптографических задач, которые бы гарантировали криптографическую стойкость.

Мы предлагаем использовать в криптографии с открытым ключом методологию, основанную на понятии некорректно поставленных задач. В данной области

эти математические задачи имеют то преимущество, что теоретически доказана невозможность их точного решения [3].

Существуют приближённые методы решения таких задач, например, регуляризация Тихонова [3], оптимальная фильтрация Винера и другие. Однако методы неприменимы, если некорректная задача поставлена в поле Галуа. В качестве такой задачи можно использовать умножение неквадратной матрицы на вектор, где и вектор и матрица состоят из элементов поля Галуа.

В рамках концепции обратных задач, наряду с криптографическими задачами могут быть рассмотрены также задачи помехоустойчивого кодирования информации. При этом существует возможность совмещения помехоустойчивого и криптографического кодирования в виде единого алгоритма.

Для реализации концепции некорректно поставленных задач можно использовать систему уравнений в поле Галуа, связывающую исходное сообщение, с сообщением, закодированным помехоустойчивым кодом. Этой системе уравнений соответствует неквадратная матрица помехоустойчивого кода, в которой количество строк меньше количества столбцов. Для криптографического кодирования используются квадратные невырожденные матрицы. Это такие матрицы, в которых порядок равен длине закодированного помехоустойчивым кодом сообщения. Матрица помехоустойчивого кода дополняется нулевыми строками так, чтобы число ее строк стало равным числу столбцов. Эта матрица является вырожденной. Результат умножения двух матриц (помехозащитной и криптографической) является вырожденной матрицей, что соответствует некорректно поставленной задаче восстановления исходного сообщения по его коду. Это порождает некорректно поставленную задачу восстановления исходного сообщения из закодированного сообщения. Матрица кодирования интегрирует в себе свойства криптографического и помехоустойчивого кодов.

Кодирование заключается в умножении этой матрицы на информационное слово. Для декодирования необходимо последовательное решение задач снятия криптографического и помехозащитного кодов. Криптоаналитик не может решить данную задачу, потому что для этого необходимо выполнить какую-либо из следующих операций:

1) Декодирование интегрального (помехоустойчивого и криптографического) кода (например, на основе построения обратного оператора).
2) Выделение из кодирующей матрицы (открытого ключа) матриц помехоустойчивого и криптографического кодов.

Построение обратного оператора – это некорректно поставленная задача, так как матрица интегрального кода является вырожденной. Учитывая невозможность применения приближённых алгоритмов, декодирующий оператор можно построить лишь путём полного перебора. Декодирование несистематического кода с порождающей матрицей является NP– полной задачей [4].

Факторизация целочисленных матриц является более сложной задачей, чем факторизация чисел, тем более что мы не предполагаем наличия у используемых нами матриц каких-либо специальных свойств.

Предложен алгоритм позволяющий совместить криптографию с открытым ключом и помехоустойчивое кодирование. Сложность интегрального кодирования связана только со сложностью умножения вектора на матрицу, что позволит использовать данный код в маломощных устройствах. Операция взлома кода является некорректной задачей для обеспечения гарантированной криптостойкости кода.

[1] Молдовян Н.А., Молдовян Ф.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритвом. СПб.: БХВ-Петербург, 2004.
[2] Рябко Б.Я., Фионов А.Н. Основы современной криптографии. М.: Научный мир, 2004.
[3] Тихонов А.Н., Арсенин В. Я. Методы решения некорректных задач. М.: Наука, 1979.
[4] Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. СПб.: ГУАП, 2004.
[5] Блейхут Р.Е. Теория и практика кодов контролирующих ошибки. М.: Мир, 1986.
[6] Гантмахер Ф. Р. Теория матриц. М.: Физматлит, 2004.
[7] Крук Е.А., Овчинников А.А. Лекции по теории кодирования. СПб.: ГУАП, 2004.

РАСШИРЕННОЕ ЦВЕТОВОЕ ПРЕОБРАЗОВАНИЕ YUV (E-YUV) ДЛЯ СИСТЕМ СЖАТИЯ ИЗОБРАЖЕНИЙ

В.О. Минченков, А.В. Сергеев

Санкт-Петербургский государственный университет аэрокосмического приборостроения

В работе рассмотрены основные принципы цветовых преобразований, используемых в алгоритмах сжатия изображений, и предложена схема на основе стандартного цветового преобразования YCbCr, позволяющая улучшить результаты сжатия синтетических изображений.

Пусть *rgb* – некоторое изображение из множества изображений RGB. Исходя из теории информации, можно точно сказать, что ни одна система кодирования не сможет затратить меньше бит, чем H(*RGB*) на кодирование одного *rgb* [1].

В идеальном случае цветовое преобразование обладает двумя свойствами. Во-первых, оно является взаимообратным, H(*RGB*)=H(*YUV*). Во-вторых, для новых компонент выполняется равенство p(*yuv*)=p(*y*)p(*u*)p(*v*). Из предыдущих двух свойств вытекает следующее: H(*RGB*)=H(*Y*)+H(*U*)+H(*V*), что объясняет возможность кодирования компонент независимо друг от друга.

Для большинства существующих цветовых преобразований можно сказать, что H(*RGB*)<=H(*Y*)+H(*U*)+H(*V*). Точно проверить данное неравенство нельзя, т.к. неизвестны распределения ни *RGB,* ни *YUV*, и судить о наличии зависимостей между компонентами можно только на качественном уровне.

Преобразование YCbCr [2] дает хорошие результаты при разложении фотореалистичных изображений на компоненты, т.е. получаемые на выходе коэффициенты

сжатия компонент после кодирования имеют более высокие значения по сравнению с RGB. Но для синтетических изображений (таких, как снимки с рабочего стола) коэффициенты сжатия не так высоки, как можно было бы ожидать. В действительности, если рассмотреть компоненты YCbCr от такого синтетического изображения (см. рисунок), то четко просматривается большая избыточность информации.

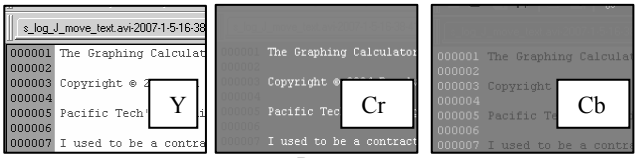

Рис.

Если внимательно посмотреть на преобразование YCbCr, то можно заметить следующий факт: существуют две точки (набор для черного цвета RGB = 0,0,0 и набор для белого цвета RGB=255,255,255) для которых можно однозначно определить по одной комбинации YCbCr (чёрный YCbCr=0,0,0 и белый YCbCr=255,128,128). И эти значения *Y* (0 и 255) возникают только для таких наборов RGB. Следуя из выше описанных фактов, можно ввести утверждение (1): если RGB=(0,0,0), то YCbCr=(0,0,0), и если *Y*=0, то RGB=(0,0,0). Т.е., при обратном переопределении значения CbCr не используются, и, следовательно, допустима их подмена. Это означает, что, если обрабатывается какое-либо изображение на черном фоне (YCbCr=0,0,0), то в компонентах CbCr можно заменить все полученные нули на такие значения, которые сделают вид этих компонент более “гладким”. Утверждение (2): если RGB=(0,0,0), то *Y*=0, а в Cb и Cr можно записать любые значения.

Для цветных фонов утверждение (2) неприменимо, т.к. нет однозначности при обратном переопределении. Например, значение *Y*=119 может быть получено из 120000 различных наборов RGB. Но вероятность возникновения ситуации, когда *Y* фонового цвета совпадет с каким-либо *Y* другого присутствующего цветового набора, при подоменном применении крайне мала. Таким образом, утверждение (2) примет следующий вид: если в домене значение *Y’* , присущее фоновому цвету, не совпадает ни с одним *Y* из всех остальных присутствующих в этом домене цветов, то тогда компоненты CbCr в точках *Y’* можно переопределить. Значения *RGB* фонового цвета записываются в отдельный поток и могут подвергнуться дополнительному сжатию.

Вопрос выбора фонового цвета и значений, которыми следует переписывать компоненты Cb и Cr, решается следующим образом: фоновым является цвет, который наиболее часто повторился в домене; значения Cb и Cr будут браться из цвета второго по частоте.

Для оценки качества работы алгоритма расширенного цветового преобразования (E-YUV) используем результаты сжатия модифицированных компонент на кодеке H264/AVC [3] в режиме без потерь (см. Табл.).

Таблица

Изображение	Стандартное YCbCr, байты	E-YUV, байты	Выигрыш, байты	Выигрыш, %
1	3030602	3030602	0	0,00%
2	395712	395712	0	0,00%
3	434445	434445	0	0,00%
4	365889	353031	12858	3,64%
5	574360	538562	35798	6,23%
6	201917	188771	13146	6,51%
7	899765	619081	280684	31,22%
8	986067	528283	457784	46,43%
9	1087062	518678	568384	52,31%

Изображения 1-3 являются фотореалистичными, и их сжатие происходит точно так же, как и при стандартном преобразовании. Изображения 4-9 являются снимками при работе на компьютере, содержащими и текст, и фотографии.

Как видно из результатов, алгоритм расширенного преобразования (при своей простоте в реализации) не имеет проигрыша при обработке фотореалистичных изображений и дает значительный выигрыш при обработке синтетических изображений.

[1] Красильников Н.Н. Цифровая обработка изображений. М.: Вузовская книга, 2001. 319 с.
[2] Ford A., Roberts A. // Color Space Conversions. 1998.
[3] Wiegand T., Sullivan G. J., Bjøntegaard G, and Luthra A. // IEEE Transactions on Circuits and Systems for Video Technology. 2003. V. 13, No.7. P. 560.

СРАВНЕНИЕ АЛГОРИТМОВ АРИФМЕТИЧЕСКОГО КОДИРОВАНИЯ: КЛАССИЧЕСКИЙ КОДЕР, RANGE-КОДЕР, RANGE-КОДЕР СУББОТИНА

А.И. Веселов

Санкт-Петербургский государственный университет аэрокосмического приборостроения

В работе сравниваются три реализации алгоритмов арифметического кодирования. В связи с тем, что собственно алгоритмы известны и описаны, в частности, рассматриваемый арифметический кодер – в работе [1], Range-кодер – в [2], а кодер Субботина – в [3], описание и обоснование алгоритмов приводиться не будет. Будет приведена только методика их сравнения и результаты этого сравнения.

Рассмотрены целочисленные реализации алгоритмов арифметического кодирования для случая входного алфавита мощности 2. Т.е., на вход кодеров поступали последовательности из 0 и 1. При этом считается, что и кодеру, и декодеру известны длины кодируемых последовательностей. При таком допущении нет необходи-

мости в добавлении некого специального символа, указывающего на конец файла. Также кодеру и декодеру известны некоторые оценки вероятностей символов алфавита, на основе которых будет осуществляться кодирование и декодирование. Это сделано для того, чтобы поставить все три кодера в одинаковые условия выполнения.

Для удобства сравнения программы, реализующие алгоритмы сжатия, были разбиты на определенные части, которые выполняют во всех трех реализациях схожие действия: начальный пересчет границ, нормализация и вывод данных. Такое разбиение позволило представить алгоритм сжатия для всех трех программ единым образом:

1.Пересчет значений границ интервала кодирования (операция 0).
2.***while*** длина интервала меньше половины интервала ***do begin***
3.***if*** интервал лежит ниже половины интервала
then выдача в выходной поток данных (операция 1).
4.***else if*** интервал выше половины интервала
then выдача в выходной поток данных (операция 2).
5.***else*** откладывание выдачи данных (операция 3).
6.***end***

Различия в программах заключались только в специфике их реализации. Стандартный арифметический кодер выдавал информацию на свой выход побитно, а Range-кодер и кодер Субботина – побайтно. Кроме того, в Range-кодере нормализация проводилась только в том случае, если она нужна, в отличие от арифметического кодера, где нормализация осуществлялась при обработке каждого входного символа. Также, в силу того, что для кодера Субботина за счет дополнительной нормализации границ невозможен перенос при их сложении, в этом кодере отсутствовало откладывание выдачи данных на выход (операция 3).

Для сравнения алгоритмов были рассчитаны следующие величины: среднее и максимальное количество операций на кодирование символа, число отложенных символов, объем избыточных данных.

Расчет этих величин осуществлялся для двух ситуаций: когда оценки вероятностей, по которым осуществлялось кодирование, были верны и неверны.

Результаты сравнения кодеров сведены в следующей таблице. В ней *razr* – разрядность используемой арифметики, $h(p)$ – двоичная энтропия, p – вероятность единицы во входном потоке.

Таблица

	арифметический кодер	Range-кодер	кодер Субботина
среднее количество операций на кодирование одного символа	$1+h(p)$	$1+0{,}125h(p)$	$1+0{,}125h(p)$
максимальное количество операций на кодирование одного символа	*razr*	(*razr*-8)/8	(*razr*-8)/8

максимальное количество избыточных символов (байт)	1	*razr*/8	*razr*/8
количество отложенных байт при правильной оценке	совпадает с геометрическим распределением с показателем 0,5	1	0
количество отложенных байт при неправильной оценке	отлично от 0	отлично от 0	0

Как видно из таблицы, побайтовые реализации алгоритма арифметического кодирования сильно выигрывают по среднему и максимальному количеству операций на кодирование одного символа. Но стандартный кодер выигрывает 1–2 % по степени сжатия у побайтных реализаций, т.к. он работает с битами. При неправильной оценке вероятностей входных символов при использовании Range-кодера или классического арифметического кодера существует ненулевая вероятность откладывания большого числа бит. В то же время, реализация кодера Субботина не требует откладывания бит как такового, но преимущество в данном пункте приводит к дополнительному проигрышу в 1–2% по степени сжатия.

В результате нельзя определить, какая из реализация является лучшей. Если нужна максимальная степень сжатия, то имеет смысл использовать стандартный кодер. Если же необходима максимальная скорость, то решением может служить кодер Субботина.

[1] Мастрюков Д.Л. Алгоритмы сжатия информации. Ч. 2. Арифметическое кодирование. М.: Монитор, 1994. №1.
[2] Schindler M. //A Fast Renormalization for Arithmetic Coding. 1979.
[3] Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: Диалог-МИФИ, 2003.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ ПРИ ИХ ПЕРЕДАЧЕ ПОСРЕДСТВОМ ЭЛЕМЕНТНОГО ТЕСТИРОВАНИЯ

И. А. Васильева[1)], А. П. Мартынов[1)], Д. Б. Николаев[2)], С. Ю. Соколов[2)]

[1)] *Саровский государственный физико-технический институт*
[2)] *Российский федеральный ядерный центр - Всероссийский научно-исследовательский институт экспериментальной физики*

В настоящее время быстрое развитие компьютерной и вычислительной техники обеспечивает автоматизацию различных процессов во всех областях человеческой деятельности. Особенно это заметно в телекоммуникационной сфере, без которой уже немыслимо современное информационное общество. Телекоммуника-

ция подразумевает передачу огромных все возрастающих массивов информации по различным каналам связи, что невозможно без применения специальных средств обеспечения безопасности, целостности и подлинности данных.

В силу своей привлекательности и отсутствия физического (материального) канала связи, все более широкое применение получают беспроводные линии связи, где основополагающим фактором является обеспечение безопасности и корректности передачи данных, т.е. использование преобразующих алгоритмов, исключающих нелегальное восстановление или изменение информации. В рамках вышесказанного актуальным является определение стойкости таких преобразующих алгоритмов с точки зрения вычислительной и временной сложности.

Задача данной работы заключается в анализе модели преобразующего алгоритма типа RSA, определении свойства её параметров, а также в разработке метода ее эффективного усовершенствования.

Свойства параметров алгоритма говорят о возможности реализации активных воздействий (восстановление конфиденциального параметра при наличии исходного и преобразованного текстов). На основе подобных воздействий можно сделать вывод, что алгоритм преобразования с открытым параметром (типа RSA) допускает утечку информации об исходных сообщениях, особенно, если сообщения не случайны. Если сообщение случайно, то восстановить весь блок исходного сообщения (вычислить обратную функцию) – сложно. В этом случае обеспечивается битовая стойкость или обеспечение безопасности элементов сообщения, то есть восстановить отдельный элемент сообщения также сложно, как и восстановить весь исходный блок. Пользователь, владеющий конфиденциальным параметром, может предоставлять не только услуги обратного преобразования, возвращая при этом в ответ на запрос цельный блок исходного текста, но и отвечать на преобразованные запросы об истинности элемента четности исходного текста преобразованного алгоритмом типа RSA, что определяет стойкость младшего значащего элемента или битовую стойкость.

Анализ битовой стойкости показал, что если исходное сообщение является случайным, то извлечь информацию об исходном тексте так же трудно, как и вычислить обратное преобразование. Этот факт можно использовать для создания более стойких систем без изменения основных преобразований, основу которых будет составлять случайный текст.

Кроме того, анализ основных причин отказов вычислительных систем и сетей в результате выполнения сложных вычислений и преобразований показал, что усложнение и усовершенствование систем обеспечения безопасности нецелесообразно без наличия соответствующих ресурсов. В этом случае, возможно использование уже известных функций алгоритмического преобразования при условии, что исходный текст является случайным, т.е. алгоритм преобразования содержит внутреннюю случайную операцию. Тогда функции алгоритмического преобразования оказываются достаточно стойкими.

ПРОТОКОЛ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В ПРОЦЕССЕ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО БЕСПРОВОДНЫМ ЛИНИЯМ СВЯЗИ

В.А. Конов[1)], С.Н. Гончаров[1)], К.О. Волков[2)], В.Е. Кулюкин[1)]

[1)]Российский федеральный ядерный центр -
Всероссийский научно-исследовательский институт экспериментальной физики
[2)] Саровский государственный физико-технический институт

Проблема обеспечения безопасности информации путем преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. Появление современных вычислительных средств ускорило разработку и совершенствование криптографических методов, позволяющих преобразовывать большие объемы информации в режиме реального времени, практически не влияя на быстродействие информационно-телекоммуникационных систем.

Однако, с одной стороны, расширилось применение компьютерных сетей, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц, а с другой стороны, появление новых мощных компьютеров, технологий сетевых и нейтронных вычислений сделало возможным компрометацию криптографических систем, еще недавно считавшихся практически не раскрываемыми.

В настоящее время очень актуально использование криптографических методов преобразования информации в телекоммуникационных системах, обеспечивающих взаимосвязь большого числа абонентов посредством применения каналов связи с различной физической структурой, в том числе и систем беспроводной связи. Использование средств обеспечения безопасности для систем такого типа весьма актуально в связи с относительной доступностью получения информации, транслируемой в эфире (направленные приемники, сканеры частот и т.д.).

Обеспечение безопасности информации имеет два аспекта: разработка средств, реализующих криптографические алгоритмы, и методика использования этих средств. Каждый из рассмотренных криптографических методов может быть реализован либо программным, либо аппаратным способом. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, безопасность. Программная реализация более практична, допускает гибкость в использовании.

Появление средств мультимедиа и сетей с высокой пропускной способностью предопределило необходимость преобразования больших потоков данных. Целью данного доклада является рассмотрение различных методов преобразования информации большого объема и выбор одного из них для построения криптографической системы.

Кроме того, проведен обзор методов проверки целостности и подлинности, применяемых при взаимодействии абонентов системы. Анализируются слабые и сильные стороны различных протоколов проверки подлинности передаваемой информации.

АГЕНТНОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ПОТОКОВ, ОБРАЗОВАННЫХ ДИСКРЕТНЫМИ ЧАСТИЦАМИ, ИМЕЮЩИМИ СЛОЖНЫЕ СЦЕНАРИИ ПОВЕДЕНИЯ

С.А. Ляшенков, А.Л. Умнов

Нижегородский госуниверситет

Агентное моделирование (АМ) является мощным и универсальным подходом, позволяющим учесть любые сложные структуры и сценарии поведения. В отличие от других методов, все агентные модели существенно децентрализованы. Вместо описания динамики системы в целом, аналитик определяет поведение на индивидуальном уровне, а глобальное поведение возникает как результат деятельности многих (десятков, сотен, тысяч, миллионов) агентов, каждый из которых следует своим собственным правилам, живёт в общей среде и взаимодействует со средой и с другими агентами. Поэтому АМ называют ещё моделированием снизу вверх. Важным преимуществом АМ является то, что разработка модели возможна в отсутствии знания о ее глобальных зависимостях: понимая индивидуальную логику поведения участников процесса, возможно построение агентной модели и вывода из неё глобальных законов поведения. И, наконец, агентную модель проще поддерживать: уточнения обычно делаются на локальном уровне и не требуют глобальных изменений.

Одним из наиболее интересных и актуальных примеров потоков, образованных дискретными частицами со сложными сценариями поведения, являются транспортные потоки. Изучение транспортных систем с помощью математического моделирования ведется уже почти 100 лет, однако трудности формализации транспортного потока стали серьезной причиной отставания результатов научных исследований от требований практики [1].

В качестве базовой модели для агентного моделирования было принято решение использовать модель следования за лидером (МСЛ).

Простейшая МСЛ предполагает, что кроме случая свободного движения, каждый водитель согласует свою скорость со скоростью впереди идущего автомобиля:

$$\ddot{x}_{i+1}(t) = \frac{1}{\tau}(\dot{x}_i(t) - \dot{x}_{i+1}(t)), \qquad (1)$$

где τ – время согласования скоростей, $\dot{x}_i(t)$ – скорость лидирующего автомобиля, $\dot{x}_{i+1}(t)$ – скорость следующего автомобиля.

Для учета свойств неустойчивости, возникновения ударных волн и заторов необходимо внести ряд модификаций:

$$\ddot{x}_{i+1}(t + t_d) = \alpha(\dot{x}_i(t) - \dot{x}_{i+1}(t)), \qquad (2)$$

где $t_d \approx 1{,}3c$ – задержка, описывающая время реакции водителя на изменение скорости лидирующего автомобиля, $\alpha = 1/\tau$ – коэффициент чувствительности, характеризующий скорость реакции водителя.

Для учета возрастания чувствительности с уменьшением дистанции до лидирующего автомобиля можно преобразовать (2) к виду [1]:

$$\ddot{x}_{i+1}(t+t_d) = \alpha(\dot{x}_{i+1}(t+t_d))^{\beta} \frac{\dot{x}_i(t) - \dot{x}_{i+1}(t)}{(x_i(t) - x_{i+1}(t))^{\gamma}}, \quad (3)$$

Все приведенные выше формулы справедливы для однополосного движения транспортных средств (или для автомобилей в пределах одной полосы для многополосного движения). В общем случае необходимо учитывать взаимодействие автомобилей на соседних полосах, описываемое функцией перестроения, которая зависит от координат и скоростей автомобилей, а также личностных характеристик водителей (решительность, опытность и т.д.).

Построенная модель позволяет изучать различные процессы, возникающие при движении транспортных потоков, как в локальном, так и в глобальном масштабе. Кроме того, она предоставляет широкие возможности для анализа и выработки оптимальных стратегий поведения водителей в ключевых ситуациях.

[1] Семенов В.В. Математические методы моделирования транспортных потоков // Нелинейный мир, 2005. №5–6.

О ПРИЧИНАХ ВОЗНИКНОВЕНИЯ КОЛЛИЗИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ СТАНДАРТА 802.15.4

В.Г. Гавриленко, А.А. Кирюшин, А.Н. Садков

Нижегородский госуниверситет

Данная работа посвящена экспериментальному исследованию причин возникновения коллизий в беспроводных сенсорных сетях (БСС) стандарта 802.15.4, использующих алгоритм доступа к каналу CSMACA (Carrier Sense Multiple Access with Collision Avoidance). В результате коллизии между двумя пакетами происходит потеря либо одного, либо обоих пакетов.

Известно, что в беспроводной сети, использующей алгоритм CSMACA, причиной возникновения коллизий является скрытый терминал [1]. Скрытым терминалом называется ситуация, при которой один передатчик не может обнаружить сигнал от другого передатчика (рис. 1a).

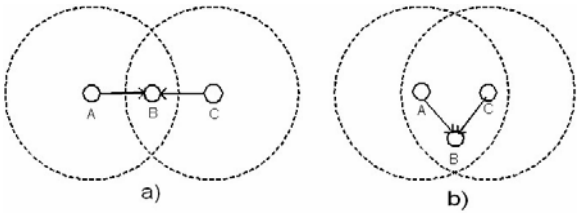

Рис. 1

Считается, что если два передатчика слышат друг друга (рис. 1b), то использование алгоритма доступа к каналу CSMA-CA позволяет полностью исключить возможность возникновения коллизий. Однако эксперименты с узлами сенсорной сети

стандарта 802.15.4 показали, что значительное их количество происходит даже когда нет скрытого терминала. Коллизия может произойти между пакетами, начало передачи которых отличается менее чем на 0.128 мс. Причиной этого является особенность реализации механизма проверки канала CCA (Clear Channel Assessment) в приемопередатчике.

CCA вычисляет среднее значение мощности сигнала за 0.128 мс и сравнивает с пороговой [2]. Если между началом передачи пакета одним узом и проверкой занятости канала другим узлом прошло менее 0.128 мс, то среднее значение мощности сигнала в канале может оказаться меньше порогового значения (рис. 2), т.е. CCA покажет, что канал свободен. В результате этого возможна коллизия.

На рис.3 показана экспериментальная зависимость количества потерянных из-за коллизий пакетов (от каждого из двух узлов) от разности мощностей сигналов на приемнике. Узлы-передатчики использовали алгоритм доступа к каналу CSMACA и были размещены таким образом, что скрытого терминала не было (рис.1b).

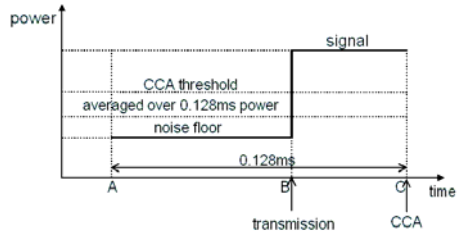

Рис. 2

При разнице мощностей сигналов более 4 dBm терялись пакеты только от узла с меньшей мощностью сигнала на приемнике. Это объясняется тем, что при коллизии между пакетами, начало передачи которых отличается менее, чем на 0.128 мс, преамбула первого пакета еще не принята, и поэтому приемник оказывается способен пересинхронизироваться со вторым пакетом (более сильный сигнал). Этот факт следует учитывать при разработке протоколов канального уровня для БСС.

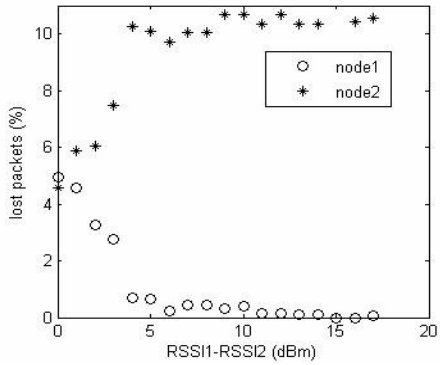

Рис. 3

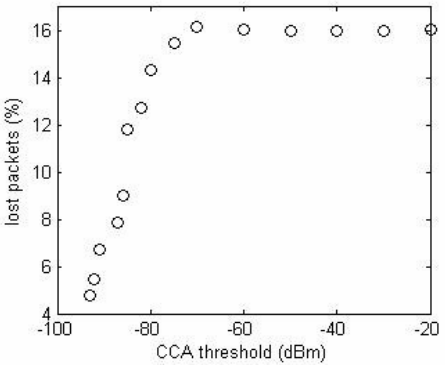

Рис. 4

Кроме того, эксперименты показали (рис.4), что если установить пороговое значение энергии ССА близким к уровню шума, то количество коллизий значительно уменьшится. Это объясняется тем, что при малом пороговом значении энергии узел способен детектировать коллизии с меньшей длительностью сигнала (интервал ВС на рис.2).

Таким образом, при разработке протоколов для БСС, а также при моделировании, необходим учет обнаруженной причины возникновения коллизий.

Работа выполнена при поддержке академической программы компании Интел.

[1] Callaway E.H. Wireless Sensor Networks: Architectures and Protocols. New York: CRC Press, 2004.
[2] CC2420 Datasheet (rev. 1.3)

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ ПОМЕХ ОТ WI-FI В БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ СТАНДАРТА 802.15.4

В.Г. Гавриленко, А.А. Кирюшин, А.Н. Садков

Нижегородский госуниверситет

Работа посвящена поиску решений, позволяющих беспроводным сенсорным сетям (БСС) стандарта 802.15.4 сосуществовать с беспроводными сетями 802.11 (Wi-Fi).

Весьма вероятно, что БСС 802.15.4, размещенная, например, внутри офисного здания, окажется в области действия одной или нескольких сетей 802.11, использующих тот же частотный диапазон: 2.4-2.4835 GHz (рис.1).

Если БСС и сеть 802.11 работают в перекрывающихся каналах, то в сенсорной сети могут быть потеряны до 90% отправленных пакетов в зависимости от величины трафика в 802.11 [1]. Такие потери делают невозможным нормальное функционирование БСС.

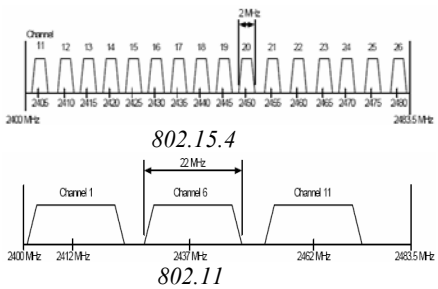

Рис. 1

Для того чтобы БСС могла успешно решать поставленную задачу, находясь в области действия сети 802.11, узлы сенсорной сети должны быть способны динамически переключаться на свободный канал при появлении помех от 802.11 в текущем канале [2]. Конкретная реализация механизма выбора канала зависит от используемого стека протоколов в данной БСС. Необходимым его элементом является алгоритм обнаружения помех от 802.11 в канале, реализованный

как самостоятельный программный модуль и совместимый с любым набором протоколов.

Поскольку активность трафика в 802.11 может резко изменяться во времени, и отсутствие потерь пакетов в 802.15.4 не означает безопасности канала, то необходимо, чтобы узлы БСС могли обнаружить 802.11 даже при малом трафике в этой сети.

Для обнаружения помех был использован встроенный во все приемопередатчики стандарта 802.15.4 индикатор мощности сигнала RSSI (Received Signal Strength Indicator), что позволило реализовать этот алгоритм без привязки к конкретному стеку протоколов.

Эксперименты показали, что если в момент измерения RSSI передавался пакет 802.11, то полученное значение оказывалось выше уровня шума. Для обнаружения сети 802.11 узел сенсорной сети в течение определенного времени (~1с) считывал значения RSSI с частотой 1kHz и сравнивал полученные значения с известным уровнем шума. Если количество значений RSSI, превышающих уровень шума, оказывалось больше порогового, то данный канал находился на одной частоте с сетью 802.11. Пороговое количество определялось исходя из того факта, что включенная точка доступа 802.11 всегда передает пакеты – маяки (beacon), обычно с интервалом 0.1024 с, и поэтому предложенный способ позволяет обнаружить 802.11 даже тогда, когда трафик в этой сети минимален.

Разработанный алгоритм был реализован в системе TinyOS 2.0 в виде отдельного модуля и протестирован на узлах БСС стандарта 802.15.4 TmoteSky.

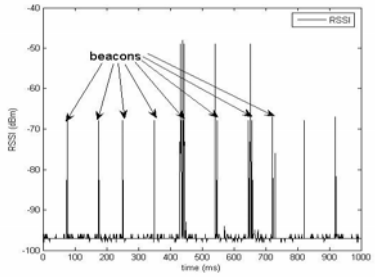

Рис. 2

Измерение RSSI энергетически малозатратно, а предложенный алгоритм использует малый объем памяти и производит только простейшие вычисления. Это является принципиально важным, поскольку узлы сенсорной сети обладают ограниченными ресурсами.

Таким образом, был разработан простой и эффективный алгоритм для узлов БСС стандарта 802.15.4, позволяющий надежно обнаружить помехи от 802.11.

Работа выполнена при поддержке академической программы компании Интел.

[1] Steibeis-Transfer Centre, Compatibility of IEEE 802.15.4 (Zigbee) with IEEE 802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4 GHz ISM-Band.

[2] Pollin S., Ergen M., Dejonghe A., Van der Perre L., Catthoor F., Moerman I., Bahai A. // Crowncom, 2006.