Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет информатики
и радиоэлектроники»

ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ, АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

МАТЕРИАЛЫ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА
(Минск, ноябрь – декабрь 2018 г.)

TELECOMMUNICATIONS: NETWORKS AND TECHNOLOGIES, ALGEBRAIC CODING AND DATA SECURITY

Минск, 2018

УДК 654:004.056
ББК 32.88+32.973.202
Т31

Т31 **Телекоммуникации**: сети и технологии, алгебраическое кодирование и безопасность данных : материалы Международного научно-технического семинара (Минск, ноябрь – декабрь 2018 г.) Telecommunications: Networks and Technologies, Algebraic Coding and Data Security – Минск : БГУИР, 2018. – 108 с.

ISBN 978-985-488-834-7.

Сборник содержит статьи, тематика которых посвящена научно-теоретическим разработкам в области сетей телекоммуникаций, информационной безопасности, алгебраического кодирования и обработки изображений.

Предназначен для научных сотрудников в области телекоммуникаций, преподавателей, аспирантов, магистрантов и студентов технических вузов.

Научное издание

Корректор *О.В. Бойправ*
Ответственный за выпуск *В.К. Конопелько*
Компьютерный дизайн и верстка *В.В. Чепикова*

Подписано в печать 08.12.2018. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 10,46. Уч.-изд. л. 8,9. Тираж 50 экз. Заказ 760.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/264 от 14.04.2014. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6

ISBN 978-985-488-834-7

СОДЕРЖАНИЕ

CONTENTS

УДК 004.932.72

СЖАТИЕ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ АДАПТИВНОГО RLE-КОДИРОВАНИЯ С ПЕРЕМЕННОЙ РАЗРЯДНОСТЬЮ СЧЕТЧИКА СЕРИИ

А.Г. ЛОПАТО, В.Ю. ЦВЕТКОВ

Белорусский государственный университет информатики и радиоэлектроники, Реуспблика Беларусь

Поступила в редакцию 16 ноября 2018

Аннотация. Предложена модификация алгоритма кодирования длин серий для сжатия полутоновых изображений без потерь, отличающийся от базового алгоритма изменением разрядности счетчика серий в зависимости от вероятности длины серии.

Ключевые слова: сжатие изображений, кодирование длин серий.

Введение

В настоящее время для сжатия изображений без потерь широко используются алгоритмы JPEG [1] и JPEG 2000 [2]. Они основаны на энтропийном кодировании коэффициентов дискретно-косинусного и вейвлетного преобразований. Для сжатия изображений без потерь часто используются также универсальные алгоритмы архивации данных: RAR и входящие в состав архиватора ZIP алгоритмы Deflate и LZMA, кодирующие значения пикселей [3]. Данные алгоритмы позволяют сжимать изображения без потерь примерно в 2 раза, однако их использование требует значительных вычислительных ресурсов. В случае когда временные и вычислительные ресурсы ограничены, для сжатия изображений необходимо использовать более простые алгоритмы эффективного кодирования, например, алгоритм кодирования длин серий RLE (Run-Length Encoding) [4], основанный на учете повторов символов. В RLE последовательности одинаковых символов заменяются двумя символами – значением серии и счетчиком серии. Один из недостатков данного алгоритма заключается в отсутствии адаптации разрядности счетчика серии к вероятности длины серии, что приводит к сравнительно низким коэффициентам сжатия.

Целью работы является разработка модификации алгоритма кодирования длин серий, основанного на изменении разрядности счетчика серии в зависимости от вероятности длины серии.

Адаптивный алгоритм кодирования длин серий

Предлагается модификация алгоритма кодирования длин серий RLE для сжатия полутоновых изображений, основанная на изменении разрядности счетчика серии в зависимости от вероятности длины серии. Сущность алгоритма состоит в уменьшении длины счетчика серии на один разряд при многократном повторении серий, кодирование длин которых не задействует старший разряд счетчика серии, и в увеличении длины счетчика серии на один разряд при кодировании длины серии, для учета которой разрядности счетчика серии недостаточно.

При достижении определенной битовой плоскости кодирование длин серий перестает обеспечивать коэффициент сжатия превышающий единицу. Когда длина поля адаптивно достигает двух бит, алгоритм переходит на реализацию встраивания в код несжатой последовательности бит. При этом для каждых 30 бит определяется количество изменений символа, т. е. количество последовательностей. Тем самым выявляется необходимость возврата к кодированию длин последовательностей.

Экспериментально установлено, что прирост коэффициента сжатия в данном алгоритме достигается за счет введения раздельных переменных значений разрядности счетчика серии для единиц и нулей, поскольку старшие битовые плоскости являются гораздо более разреженными, чем младшие. Переход к встраиванию несжатой последовательности при этом осуществляется при достижении длин нулевых и единичных серий наименьшего значения.

Для повышения эффективности алгоритма сжатия исходного изображения целесообразно выполнить его обратимое преобразование, в результате которого уменьшаются значения пикселей.

Исследованы дифференциальное кодирование и вейвлет-преобразование (последнее обеспечило наибольший коэффициент сжатия). Преобразования приводят к появлению отрицательных значений (единиц в старших битовых плоскостях для отрицательных коэффициентов, в том числе и близких к нулю), что обуславливает увеличение количества последовательностей. Это негативно сказывается на коэффициенте сжатия. Эффективным решением данной проблемы является переход от дополнительного кода к структуре, хранящей знаковый бит в младшем разряде и модуль значения пикселя в старших разрядах.

Алгоритм имеет несколько параметров, изменение которых сказывается на коэффициенте сжатия:

– изначальные значения длин последовательностей (для единиц выбирается намного меньшее значение, чем для нулей);

– длина серии последовательностей, не использующих старший бит поля, после достижения которой уменьшается его размер;

– количество переходов к противоположному символу при встраивании несжатой последовательности за последние 30 бит.

Пошаговое описание алгоритма

Блок-схема предлагаемого алгоритма представлена на рис. 1. Для его выполнения необходимо предварительно выполнить двумерное вейвлетное преобразование, квантование с определенными коэффициентами (опционально) и переход от дополнительного кода к прямому для каждого пикселя.

Поскольку алгоритм работает с отдельными битами, необходимо реализовать развертку изображения. Для ускорения аппаратного выполнения алгоритма (распараллеливания, конвееризации) его необходимо разрабатывать таким образом, чтобы отдельные участки изображения кодировались независимо друг от друга. Эксперименты показали, что увеличение размеров блока приводит к увеличению коэффициента сжатия. Однако при аппаратной реализации это ведет также к увеличению необходимого размера буфера. Удовлетворительным по коэффициенту сжатия является размер блока 4096 пикселей.

Апробированы два варианта развертки – по блокам (64×64) и по вертикальным линиям (512×8, 1024×4, 2048×2, 768×5,33). При сравнении этих вариантов установлено, что коэффициент сжатия при линейной развертке лишь немного уступает блочной, однако проводить линейную развертку аппаратно гораздо менее ресурсозатратно, т. к. исключается необходимость дополнительной буферизации данных во внутренней памяти ПЛИС. Такой вариант является предпочтительным. Если размер изображения не кратен 4096 пикселям, то при линейной развертке можно добавить недостающее число нулевых пикселей.

Следующим этапом является определение номера старшей битовой плоскости, в которой есть единичные биты, и запись его в результирующую последовательность. С этой плоскости начинается кодирование. При аппаратной реализации это можно сделать при последовательном занесении каждого пикселя в буфер кодера.

Далее выполняется адаптивное кодирование длин серий. Первоначально проводится инициализация переменных значений алгоритма (длин полей нулей и единиц, флагов состояния кодера: флага включения несжатых бит в результирующую последовательность и флага первого бита в последовательности).

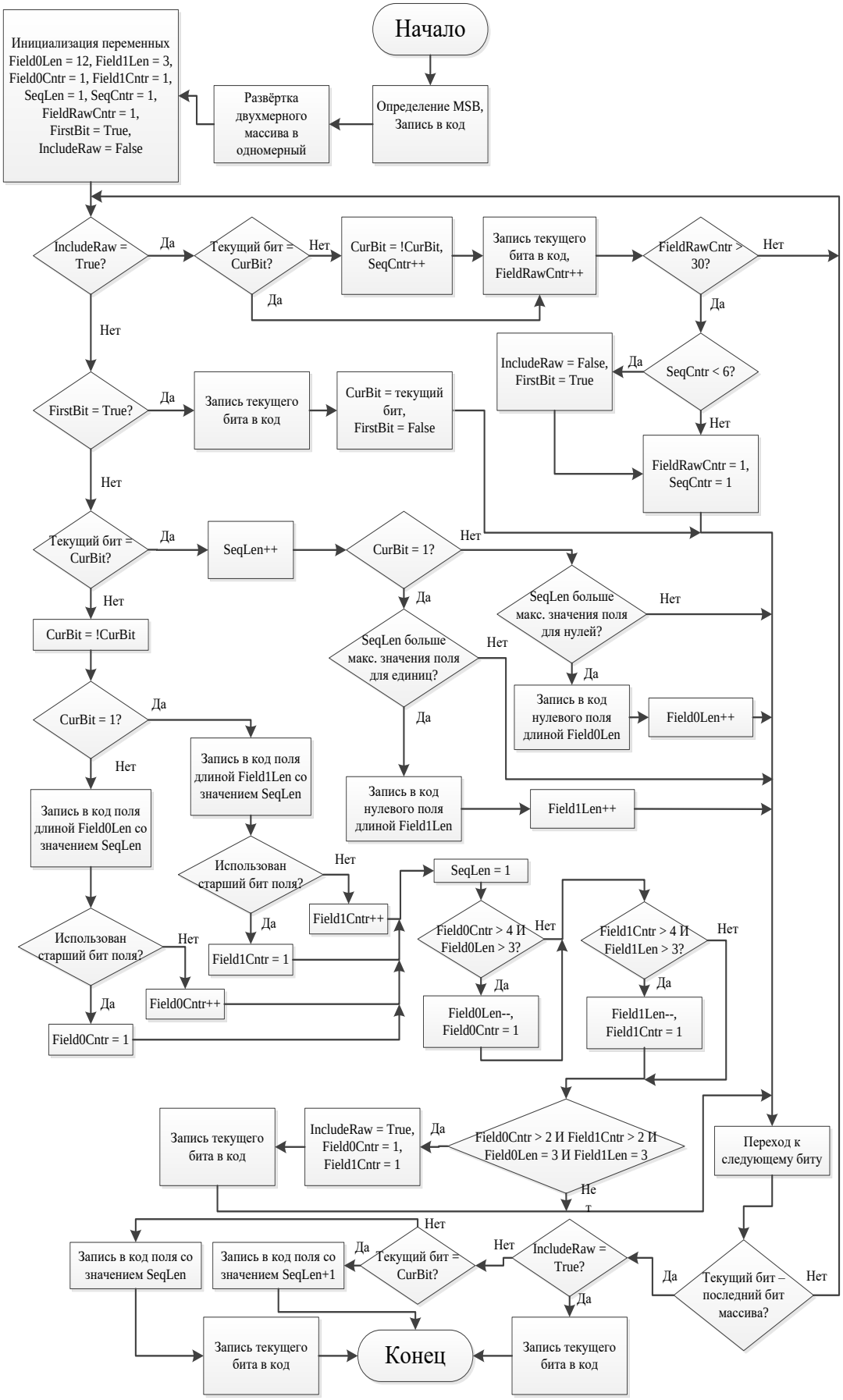


Рис. 1. Алгоритм адаптивного кодирования длин серий

В процессе выполнения алгоритма осуществляется проход по каждому писклею каждой битовой плоскости. При этом формируется сжатый поток данных, состоящий из блоков переменной длины, что при программной реализации проще выполнить в виде последовательного двоичного массива. При аппаратной реализации необходимо непосредственно на этапе кодирования формировать выходной поток с определенной длиной слова, равной разрядности шины данных (16 бит в данном случае). Для этих целей выделяются регистр, разрядность которого равна двукратной разрядности шины, и указатель на его биты. При кодировании очередного некратного блока данных он заносится в регистр по адресу указателя, а значение указателя увеличивается на размер этого блока. Если указатель переходит на старшую половину регистра, то его младшая половина выгружается на шину, старшая сдвигается в младшую половину и значение указателя уменьшается на значение разрядности шины.

При кодировании пикселя изначально проверяется флаг включения несжатых данных (IncludeRaw). Если он равен единице, бит заносится в результирующую последовательность. Так же при этом проводится оценка частоты смены бит. Если за 30 бит ноль сменяется единицей (и наоборот) менее шести раз, что говорит о достаточном для сжатия количестве последовательностей в коде, то флаг IncludeRaw сбрасывается в ноль и далее снова начинает выполняться кодирование длин серий. Если флаг IncludeRaw сброшен в ноль, то для текущего бита проверяется флаг первого бита в последовательности (FirstBit). Если он установлен в единицу, то бит заносится в последовательность, чтобы в последствии при декодировании его можно было восстановить. При нулевых значениях обоих флагов проверяется значение текущего бита. Если оно совпадает с предыдущим, то соответствующее значение длины последовательности увеличивается на единицу. При этом значение может превысить максимально возможное для текущей длины поля. Если это происходит, длина поля увеличивается на единицу, а для информирования об этом декодера в результирующую последовательность заносится нулевое поле текущей длины.

При несовпадении текущего бита с предыдущим в результирующую последовательность вносится поле со значением длины последовательности бит. Если при этом не задействуется старший бит поля, то инкрементируется значение соответствующего счетчика полей избыточной длины (Field0Cntr или Field1Cntr). Если значение этого счетчика превышает четыре, то размер поля уменьшается на единицу. Поскольку данный процесс происходит и в кодере, и в декодере, то нет необходимости включать в код дополнительную информацию об этом.

Если значения обоих переменных Field0Cntr и Field1Cntr достигли наименьшего значения, то путем установки флага IncludeRaw выполняется переход к вставке в код несжатых данных.

Оценка эффективности использования алгоритмов кодирования длин серий для сжатия полутоновых изображений

Для тестовых изображений, представленных на рис. 2, в таблице приведены коэффициенты сжатия, полученные для предложенного адаптивного алгоритма RLE, а также алгоритмов SPECK и JPEG2000.

Из таблицы следует, что разработанный алгоритм находится на одном уровне по коэффициенту сжатия с алгоритмом SPECK, но уступает алгоритму JPEG2000. Однако кодирование изображений с помощью данного алгоритма в среде MATLAB выполняется в 2–2,5 раза быстрее, чем с помощью JPEG2000.

В случае аппаратной реализации адаптивного кодирования длин серий на обработку одного бита изображения затрачивается приблизительно один такт работы ПЛИС, что многократно превосходит JPEG2000, в котором необходимо выполнить несколько проходов по одним и тем же битам. При этом адаптивный кодер RLE уступает кодеру SPECK, реализация которого позволяет за один такт обрабатывать четыре и более бит. Однако отдельное ядро сжатия RLE в кристалле ПЛИС фирмы Xilinx серии Kintex-7 занимает всего порядка 600 таблиц истинности, что за счет распараллеливания позволяет увеличить эффективность использования ресурсов и подобрать необходимую пропускную способность для конкретной задачи путем вариации числа ядер.

а *б* *в*

Рис. 2. Тестовые изображения: *а* – М1 (128×128 пикселей); *б* – М2 (256×256 пикселей); *в* – М3 (512×12 пикселей)

Размеры кода при сжатии тестовых изображений без потерь

Алгоритм	Коэффициент сжатия		
	Airplane_1024	Airport_1024	Island_1024
RLE	1,79	1,54	1,73
SPECK	1,77	1,57	1,80
JPEG2000	1,91	1,71	1,97

Заключение

Предложена модификация алгоритма кодирования длин серий для сжатия без потерь полутоновых изображений, отличающиеся от базового алгоритма RLE изменением разрядности счетчика серии в зависимости от вероятности длины серии. Установлено, что предложенный алгоритм обеспечивает коэффициент сжатия изображений без потерь в области дискретного вейвлет-преобразования, близкий к коэффициенту сжатия алгоритма SPECK (1,5–1,7 раза), и скорость кодирования, в 2 раза превышающую скорость кодирования алгоритма JPEG2000.

COMPRESSION OF HALF-TONE IMAGES BASED ON ADAPTIVE RLE-CODING WITH VARIABLE DISTRIBUTION OF A SERIES COUNTER

A.G. LOPATO, V.Yu. TSVIATKOU

Abstract. A modified run-length coding algorithm for lossless compressing grayscale images is proposed. It differs from the baseline algorithm by adaptively changing run-lengths.

Keywords: images compression, run-length encoding.

Список литературы

1. Pennebaker W.B., Mitchell J.L. JPEG Still Image Compression Standard. New York, 1993.
2. Ebrahimi T. // Proc. of the SPIE. San Diego, July–August 2000. Vol. 4115. P. 446–454.
3. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М., 2003.
4. Golomb S.W. // IEEE Transactions on Information Theory. 1966. July. P. 399–401.

УДК 621.391.14

НОРМЕННОЕ ДЕКОДИРОВАНИЕ БЧХ-КОДОВ С ПЕРВОЙ НУЛЕВОЙ КОМПОНЕНТОЙ СИНДРОМА

В.К. КОНОПЕЛЬКО, А.В. КУРИЛОВИЧ, А.Н. ПРИГОН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 16 ноября 2018

Аннотация. Работа посвящена развитию метода сжатия норм синдромов путем приведения к нулю первой компоненты синдрома. Представлены результаты исследований для БЧХ-кодов длиной n = 31, корректирующих ошибки кратности 4; 5; 6.

Ключевые слова: образующий вектор ошибок, преобразования ошибок малой кратности в ошибки большой кратности, нулевая компонента синдрома, нормы синдромов.

Введение

Известно, что при увеличении кратностей корректируемых ошибок число норм резко возрастает [1, 2]. В [2] для уменьшения анализируемых норм предложен метод сжатия при коррекции ошибок кратности $t=3$ БЧХ-кодом длиной $n=31$ с помощью преобразования синдрома $S=(S_1,S_2,S_3)$ в синдром $S=(0,S_2^{**},S_3^{**})$, что позволяет уменьшить число анализируемых норм до одной при использовании S_2^{**} или S_3^{**} вместо трех норм. В представляемой работе исследуется применение метода сжатия для идентификации образующих векторов ошибок кратности $t=2\div 6$ БЧХ-кодами длиной $n=31$.

Норменное декодирование БЧХ-кодов на основе преобразования ошибок малой кратности в ошибки большей кратности с основными и зависимыми нормами

Проводимые исследования заключались в вычислении синдромов S, сдвигах синдрома с ненулевой компонентой $S_1 \neq 0$ до получения S_1^*, суммировании полученного синдрома с синдромом одиночной ошибки $S=(\alpha^0,\alpha^0,\ldots,\alpha^0)$, вычислении норм синдромов, выборе идентификационных параметров. Для БЧХ-кодов длиной $n=31$ и кратностью корректируемых ошибок t=2÷6 в результате проведения вычислительного эксперимента установлено следующее.

После отмеченных преобразований для $t=2$ множество образующих векторов $E_{\text{обр}}$ БЧХ-кодов $n=31$ преобразуется в 15 векторов трехкратных ошибок с нулевой первой компонентой $(0, \alpha^{j^{**}})^T$. Для их идентификации можно использовать синдром S_2^{**}.

Множество образующих векторов ошибок $E_{\text{обр}}$ кратности $t=3$ (для 5 образующих векторов ошибок с первой нулевой компонентой циклические сдвиги не осуществляются) преобразуются в 140 векторов четырехкратных ошибок с нулевой первой компонентой S_1^{**}. Так как значение оставшейся одной нормы N_3^{**} не может охватывать всех $E_{\text{обр}}$, то в качестве идентификационных параметров можно использовать S_2^{**} или S_3^{**} [2]. Установлено, что 140 образующих векторов ошибок $E_{\text{обр}}$ идентифицируются одним циклотомическим классом N_3^{**}.

На рис. 1 представлено распределение образующих векторов ошибок на основе соответствующих преобразований.

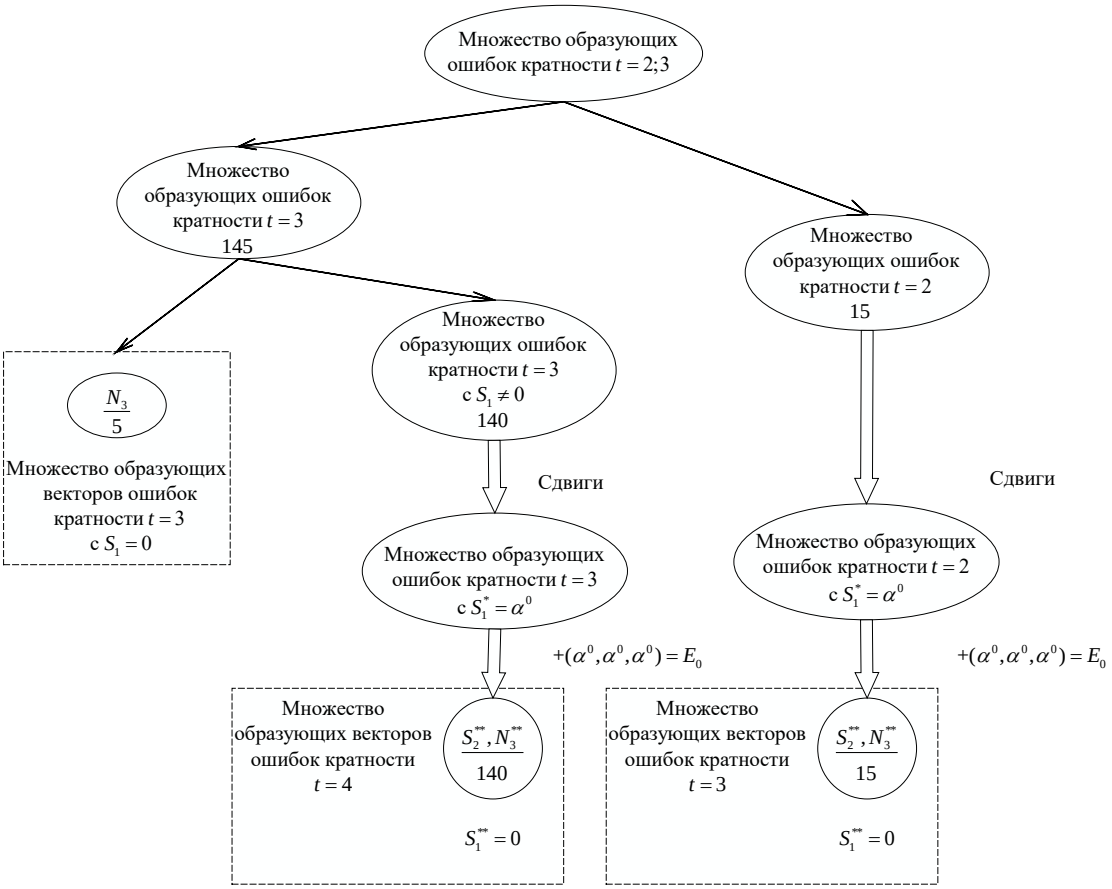


Рис. 1. Распределение образующих векторов ошибок после преобразования синдрома в синдром с первой нулевой компонентой для $t = 3$

Множество образующих векторов $E_{\text{обр}}$ кратности $t = 4$ с $S \neq 0$ (с первой компонентой синдрома S_1 =11 имеется 35 $E_{\text{обр}}$) преобразуются в 980 векторов $E_{\text{обр}}$, включающих 750 векторов пятикратных ошибок с одной нулевой первой компонентой S_2^{**}, 140 векторов ошибок кратности $t = 3$ с $S_1^{**} = 0$, по 30 векторов ошибок с двумя нулевыми компонентами S_1^{**}=S_2^{**}=0, S_1^{**}=S_3^{**}=0 и S_1^{**}=S_4^{**}=0 соответственно. При этом нормы синдромов $\left(S_1^{**}=0, S_2^{**}, S_3^{**}, S_4^{**}\right)$ вычисляются по следующим формулам:

$$\left(N_4^{**}=3z^{**}-5j^{**}\right);\ \left(N_5^{**}=3m^{**}-7j^{**}\right);\ \left(N_6^{**}=5m^{**}-7z^{**}\right). \qquad (1)$$

Анализ данных показывает, что эти нормы не идентифицируют все образующие вектора ошибок кратности $t = 4$. Поэтому для идентификации необходимо использовать и другие параметры. В качестве идентификационных параметров, как показал эксперимент, можно выбрать любой из трех синдромов: $S_2^{**}, S_3^{**}, S_4^{**}$. На рис. 2 представлено распределение образующих векторов ошибок после преобразования синдрома в синдром с первой нулевой компонентой для $t = 4$.

Множество образующих векторов ошибок кратности $t = 5$ с ненулевой первой компонентой $S_1 \neq 0$ (168 образующих векторов ошибок содержит $S_1 = 0$) преобразуется в 3903 векторов шестикратных ошибок с одной нулевой первой компонентой $S_1^{**} = 0$, по 150 векторов шестикратных ошибок с двумя нулевыми компонентами S_1^{**}=$S_2^{**} = 0$ и S_1^{**}=$S_4^{**} = 0$ соответственно, 156 векторов шестикратных ошибок с двумя ненулевыми компонентами $S_1^{**} = S_3^{**}$=0 соответственно, 6 векторов шестикратных ошибок с тремя нулевыми компонентами S_1^{**}=S_2^{**}=S_4^{**}=0 и 945 векторов ошибок кратности $t = 4$ с одной компонентой $S_1^{**} = 0$ (нормы вычисляются по формулам (1)). Анализ данных эксперимента показывает, что для их идентификации трех норм ($N_4^{**}, N_5^{**}, N_6^{**}$) недостаточно; в качестве дополнительных параметров

можно использовать один из синдромов ($S_2^{**}, S_3^{**}, S_4^{**}$). При этом выбранное множество идентификационных параметров не пересекается для векторов $E_{\text{обр}}$ кратности t= 2;3;4;5.

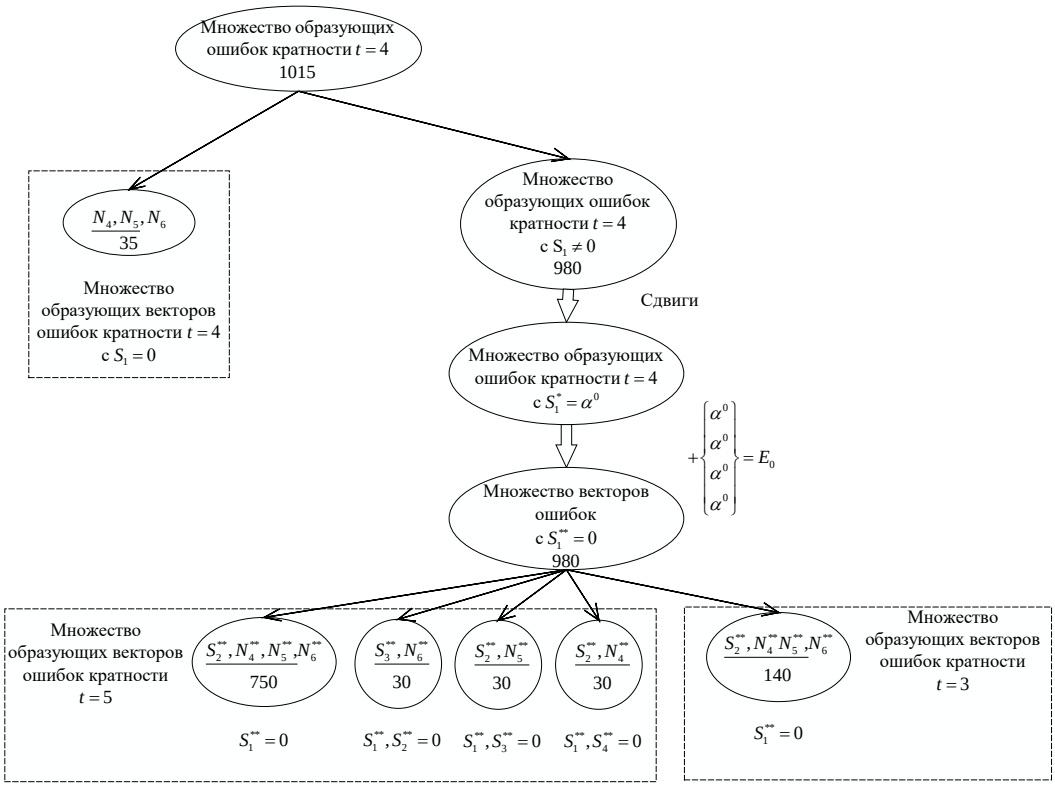


Рис. 2. Распределение образующих векторов ошибок после преобразования синдрома в синдром первой нулевой компонентой для t=4

Анализ результатов исследований для векторов $E_{\text{обр}}$ кратности $t = 6$ показывает, что оставшиеся нормы N_i^{**} также не идентифицируют все множество образующих векторов этих ошибок. Поэтому для идентификации можно использовать один из синдромов $S_2^{**}, S_3^{**}, S_4^{**}, S_5^{**}$. Это позволяет идентифицировать все множество $E_{\text{обр}}$.

В табл. 1 и 2 представлены идентификационные параметры для образующих векторов ошибок кратности ошибок t = 3÷6 БЧХ-кодами, $n = 31$.

Таблица 1. **Идентификационные параметры для образующих векторов ошибок $E_{\text{обр}}$ кратности t=3÷6 БЧХ-кодами, n = 31 при одной и двух компонентах, равных нулю**

Кратность t	Число образующих векторов ошибок (1)	Синдром S				
	Идентификационные параметры (2)	$S_1^{**} = 0$	$S_{1,2}^{**} = 0$	$S_{1,3}^{**} = 0$	$S_{1,4}^{**} = 0$	$S_{1,5}^{**} = 0$
3	(1)	140				
	(2)	S_2^{**}, N_3^{**}				
4	(1)	890	30	30	30	
	(2)	$S_2^{**}, N_4^{**}, N_5^{**}, N_6^{**}$	S_3^{**}, N_6^{**}	S_2^{**}, N_5^{**}	S_2^{**}, N_4^{**}	
5	(1)	4695	150	156	150	
	(2)	$S_2^{**}, N_4^{**}, N_5^{**}, N_6^{**}$	S_3^{**}, N_6^{**}	S_2^{**}, N_5^{**}	S_2^{**}, N_4^{**}	
6	(1)	20185	681	681	681	681
	(2)	$\frac{S_2^{**}, N_5^{**}, N_6^{**}, N_7^{**}}{N_8^{**}, N_9^{**}, N_{10}^{**}}$	$\frac{S_3^{**}, N_8^{**}}{N_9^{**}, N_{10}^{**}}$	$\frac{S_2^{**}, N_6^{**}}{N_7^{**}, N_{10}^{**}}$	$\frac{S_3^{**}, N_5^{**}}{N_7^{**}, N_{10}^{**}}$	$\frac{S_3^{**}, N_5^{**}}{N_6^{**}, N_8^{**}}$

Таблица 2. **Идентификационные параметры для образующих векторов ошибок $E_{обр}$ кратности t=3÷6 БЧХ-кодами, n = 31 при трех компонентах, равных нулю**

Кратность t	Число образующих векторов ошибок (1)	Синдром S					
	Идентификационные параметры (2)	$S^{**}_{1,2,3}=0$	$S^{**}_{1,2,4}=0$	$S^{**}_{1,2,5}=0$	$S^{**}_{1,3,4}=0$	$S^{**}_{1,4,5}=0$	$S^{**}_{1,4,5}=0$
5	(1)		6				
	(2)		$\underline{S^{**}_3}$				
6	(1)	35		35	35	26	35
	(2)	$\underline{S^{**}_4, N^{**}_{10}}$		$\underline{S^{**}_3, N^{**}_8}$	$\underline{S^{**}_2, N^{**}_7}$	$\underline{S^{**}_2, N^{**}_6}$	$\underline{S^{**}_2, N^{**}_5}$

В табл. 2 приведены идентификационные параметры (подчеркнутые значения $S^{**}_i, N^{**}_i, ..., N^{**}_j$) при использовании основных и дополняющих норм для БЧХ-кодов, корректирующих ошибок кратности t=3;4;5;6. Анализ данных табл. 1, 2 для этого случая показывает, что в некоторых случаях число идентификационных параметров меньше, чем при использовании основных и зависимых норм (например, при t = 6 требуется на три нормы меньше при S^{**}_1=0).

Анализ данных, представленных в табл. 1, 2, показывает, что число идентификационных параметров на основе сведения ошибок малой кратности в ошибки большей кратности путем установления первой компоненты синдрома $S_1 = 0$ меньше, чем число основных и зависимых норм из [1, 2] (при t = 3;4;5;6 соответственно на две, три, семь, восемь норм при применении, кроме того, одного из синдромов S^{**}_5). Это позволяет уменьшить сложность идентификатора для нахождения образующих векторов ошибок $E_{обр}$ при реализации норменного декодера.

Норменное декодирование БЧХ-кодов на основе преобразования ошибок малой кратности в ошибки большей кратности с основными и дополняющими нормами

Как показано в [3, 4], число основных и дополняющих норм меньше, чем число основных и зависимых норм. Проведенный вычислительный эксперимент по анализу множества норм образующих векторов ошибок, полученных с применением преобразования синдрома в синдром с первой компонентой, равной нулю, на основе основных и дополняющих норм, показал следующее. Для БЧХ-кода с $t = 3$ число норм и дополнительных идентификационных параметров (синдромов S^{**}_i) остается одним и тем же (N_3 при $S_1 = 0$ и S^{**}_2, N^{**}_3) при $S_1 \neq 0$). Для БЧХ-кода с $t = 4$, при S^{**}_1=0 и $S^{**}_2, S^{**}_3, S^{**}_4 \neq 0$ известно, что норма N^{**}_6 является зависимой нормой. Она выражается через нормы N^{**}_4 и N^{**}_5 следующей формулой: $3N^{**}_6 = 5N^{**}_5 - 7N^{**}_4$. Поэтому при идентификации образующих векторов ошибок с S^{**}_1=0 и $S^{**}_2, S^{**}_3, S^{**}_4 \neq 0$ не используется N^{**}_6 (рис. 3).

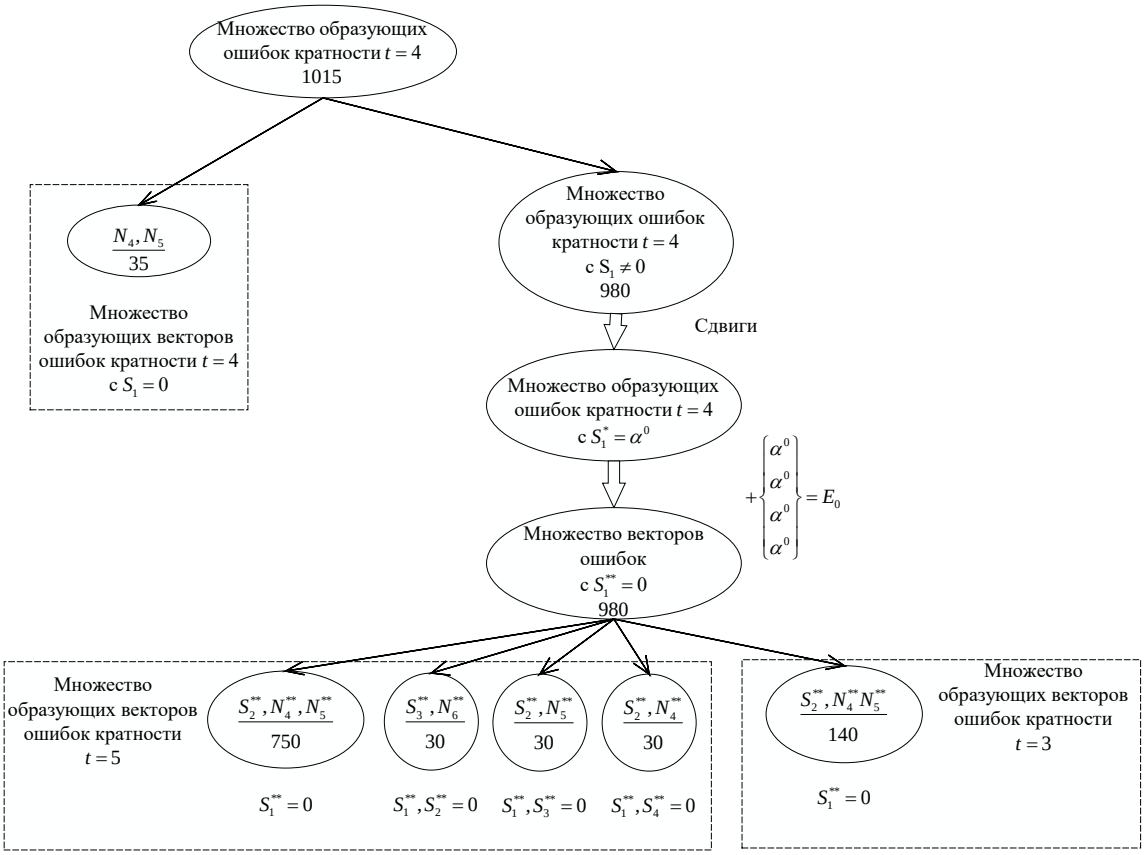


Рис. 3. Распределение образующих векторов ошибок после преобразования синдрома в синдром с первой нулевой компонентой для $t = 4$ при использовании основных и дополняющих норм

Заключение

Приведенный анализ данных вычислительных экспериментов показал, что норменное декодирование БЧХ-кодов на основе преобразования синдрома в синдром с первой нулевой компонентой позволяет уменьшить число анализируемых норм на $2;3;7;8$ по сравнению с числом основных и зависимых норм при идентификации ошибок кратности $t = 3;4;5;6$ соответственно. Установлено, что при этом необходимо использовать один из сдвинутых синдромов в качестве дополнительного идентификационного параметра. Также показано, что число идентификационных параметров при применении основных и дополняющих норм на $1;1;3$ уменьшается по сравнению с применением основных и зависимых норм при идентификации образующих векторов ошибок кратности $t = 4;5;6$ соответственно.

THE NORM DECODING FOR BCH CODES WITH THE FIRST ZERO COMPONENT OF THE SYNDROME

V.K. KONOPELKO, A.V. KURILOVICH, A.N. PRIGON

Abstract. The work is devoted to the development of the compression method of the norms of syndromes with the first zero component of the syndrome. Study results for BCH-codes of length $n = 31$, correcting errors of multiplicity 4; 5; 6 are given.

Keywords: generatrix of errors, conversion of errors of small multiplicity into errors of large multiplicity, zero component of the syndrome, norms of the syndromes.

Список литературы

1. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.
2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
3. Курилович А.В., Конопелько В.К., Липницкий В.А. // Докл. БГУИР. 2005 № 6. С. 28–30.
4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М., 1979.

УДК 004.056.5

СПЕКТРАЛЬНО-КОДОВАЯ СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ИЗОБРАЖЕНИЯ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

С.Б. САЛОМАТИН, Ю.Е. ЯВОРКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 13 ноября 2018

Аннотация. Рассмотрены алгоритмы каскадной спектрально-кодовой стеганографической защиты изображения в распределенных системах с использованием дискретного преобразования Фурье на первом этапе и метода разделения секрета (алгоритма Гарнера) – на втором.

Ключевые слова: стеганография, преобразование Фурье, разделение секрета, китайская теорема об остатках.

Введение.

В современных инфокоммуникационных технологиях широко используются распределенные системы передачи и обработки данных. Одна из задач информационной безопасности в таких системах связана со стеганографической защитой мультимедийных данных. При этом алгоритмы стеганографического кодирования, которые отображают структуру изображения в случайную структуру фона, могут изменить фрактальный характер изображения и привести к потерям при применении алгоритмов сжатия [1, 2].

Одним из путей решения такого рода задач является выполнение кодирования источника с помощью стеганографического спектрального преобразования Фурье и распределенного кодирования на основе метода разделения секрета для повышения криптостойкости.

Алгоритм стеганографического пробразования Фурье

1. Изображение определяется как массив данных $d\left(n_1, n_2\right)$, $n_1, n_2 = 0,1,...N-1$

2. Выполняется преобразование Фурье:

$F\{d\left(n_1, n_2\right)\} = \{D\left(m_1, m_2\right),\ m_1, m_2 = 0,1,...N-1$.

3. Выполняется сдвиг фаз компонент спектра на случайную величину $\theta_{rand}\left(0-2\pi\right)$.

4. В спектральной области выделяются области (кластеры), удовлетворяющие условию

$m-0,5 < \sqrt{m_1^2 + m_2^2} < m+0,5.$

Компонентам, попавшим в один и тот же кластер, ставится в соответствие одна и та же частота.

5. Частотные компоненты D_m в выделенных областях (кластерах), удовлетворяющих условию $m-0,5 < \sqrt{m_1^2 + m_2^2} < m+0,5$, заменяются случайными значениями φ_{rand} .

6. Вычисляются значения дисперсий σ_m^2 по формуле:

$$\sigma_m^2 = \left\langle \left(\upsilon_m\right)^2 \right\rangle = \frac{1}{N_m} \sum_{m-0,5<\sqrt{m_1^2+m_2^2}<m+0,5} \upsilon_{m_1,m_2}^2 ,$$

где N_m соответствует количеству компонент в кластере.

7. Выполняется масштабирование:

$$D'_m = D_m \cdot \frac{m^{\frac{\beta_1+1}{2}}}{m^{\frac{\beta_2+1}{2}}} = D_m m^{\Delta\beta/2},$$

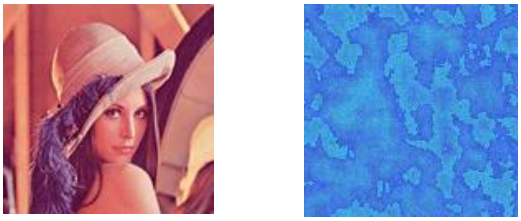
где β_1, β_2 – спектральные экспоненты исходного и преобразованного изображений, $\Delta\beta = \beta_1 - \beta_2$

7. Осуществляется переход в пространственную область с помощью нормированного обратного БПФ.

В результате было получено изображение (рис. 1), которое имеет случайные фазы спектральных составляющих $\theta'_{m_1,m_2} = \theta + \theta_{rand}$, а дисперсии амплитудных составляющих удовлетворяют условию фрактального распределения исходного изображения

$$\left\langle \left(D_m \right)^2 \right\rangle \propto 1/f^{\beta} \propto 1/m^{\beta}.$$

Процедура декодирования использует обратные операторы.



а *б*

Рис. 1. Результат применения стеганографического преобразование Фурье:
а – исходное изображение Lena; *б* – спектр стеганографического преобразования

Алгоритм вычисления отображений на основе метода разделения секрета

1. Выбирается число t, и массив данных преобразуется в новый массив B в виде матрицы из m строк и t столбцов.

2. Для каждой k-й строки матрицы и заданного значения x, вычисляется полином

$$s_k(x) = s_0 + s_1 x + \ldots + s_{t-1} x^{t-1} \pmod p.$$

3. Результаты вычислений образуют m строк массива A_x.

4. Массив A_x преобразуется в матрицу размером $a \times b$, которая является возвращаемым отображением.

5. Изменяя значение x и повторяя шаги 2 и 3 алгоритма, формируется множество n различных отображений.

Предположим, что имеется n различных отображений и используется (t,n)-схема разделения секрета [3]. Любая комбинация из t различных отображений позволяет построить алгоритм восстановления. Определим массив $X = \{x_0, x_1, \ldots, x_{t-1}\}$ для хранения значений x, соответствующих выбранным t отображениям.

Алгоритм восстановления массива данных по отображениям.

1. Все A_x-матрицы t отображений преобразуются в массивы длиной m.

2. Элемент с номером i каждого массива задается как $s_i(x_l)$, где l – индекс соответствующего массива, а x_l представляет собой l-й элемент массива X. В результате формируются t значений. $s_i(x_0), s_i(x_1), \ldots, s_i(x_{t-1})$.

3. Составляется система уравнений следующего вида

$$s_i\left(x_0\right) \equiv s_0^i + s_1^i x_0 + ... + s_{t-1}^i x_0^{t-1} \left(\mathrm{mod}\, p\right),$$

. . .

$$s_i\left(x_{t-1}\right) \equiv s_0^i + s_1^i x_{t-1} + ... + s_{t-1}^i x_{t-1}^{t-1} \left(\mathrm{mod}\, p\right).$$

Решение системы уравнения дает значения $s_0^i, ..., s_{t-1}^i$, являющиеся элементами i-й строки восстанавливаемого массива B.

4. Шаги 2 и 3 алгоритма повторяются, до тех пор, пока все элементы каждого массива не будут вычислены, что дает полный восстановленный массив B.

5. Массив B размером $m \times t$ преобразуется в массив исходного размера $H \times W$, что дает восстановление исходного массива данных.

6. Если выбрана (t, n) - пороговая схема и N – произведение наименьших t их них, а M-произведение $t-1$ наибольших. Тогда при нехватке одной части для восстановления результата недостающий множитель находится среди более, чем $\frac{N-M}{M}$ целых чисел (алгоритм Гарнера).

Из китайской теоремы об остатках следует, что можно заменять операции над числами операциями над кортежами. Каждому числу a ставится в соответствие кортеж $(a_1, ..., a_k)$, где $a_i \equiv a\left(\mathrm{mod}\, n_i\right)$. Решение дается в смешанной системе счисления:

$$a = x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 + \ldots + x_k \cdot n_1 \cdot \ldots \cdot n_{k-1}.$$

Обозначим r_{ij} через $(i = 1...k-1, j = i+1...k)$ число, являющееся обратным для n_i по модулю n_j: $r_{ij} = (n_i)^{-1} \,(\mathrm{mod}\, n_j)$.

Подставим выражение a в смешанной системе счисления в первое уравнение системы. В результате получим $a_1 \equiv x_1$. Подставим теперь выражение во второе уравнение: $a_2 \equiv x_1 + x_2 \cdot n_1 \,(\mathrm{mod}\, n_2)$. Преобразуем это выражение, отняв от обеих частей x_1 и разделив на n_1:

$$a_2 - x_1 \equiv x_2 \cdot n_1 \,(\mathrm{mod}\, n_2);\ (a_2 - x_1) \cdot r_{12} \equiv x_2 \,(\mathrm{mod}\, n_2);.\ x_2 \equiv (a_2 - x_1) \cdot r_{12} \,(\mathrm{mod}\, n_2).$$

Подставляя в третье уравнение, аналогичным образом получаем:

$$a_3 \equiv x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 \,(\mathrm{mod}\, n_3);$$

$$(a_3 - x_1) \cdot r_{13} \equiv x_2 + x_3 \cdot n_2 \,(\mathrm{mod}\, n_3);$$

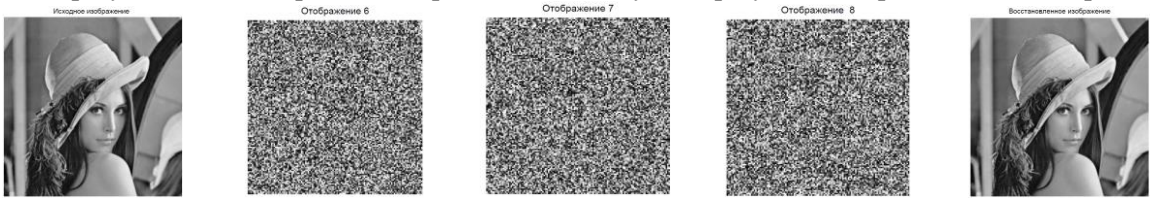
$$((a_3 - x_1) \cdot r_{13} - x_2) \cdot r_{23} \equiv x_3 \,(\mathrm{mod}\, n_3);$$

$$x_3 \equiv ((a_3 - x_1) \cdot r_{13} - x_2) \cdot r_{23} \,(\mathrm{mod}\, n_3).$$

Число a восстанавливается по формуле :

$$a = x_1 + x_2 \cdot n_1 + x_3 \cdot n_1 \cdot n_2 + \ldots + x_k \cdot n_1 \cdot \ldots \cdot n_{k-1}.$$

В результате моделирования в среде MatLab получены результаты, представленые на рис. 2.



а *б* *в* *г* *д*

Рис. 2. Моделирование алгоритма разделения секрета: *а* – исходное изображение; *б, в, г* – кодировка изображения алгоритмом разделения секрета; *д* – восстановленное изображение

Заключение

Применение ДПФ сохраняет фрактальный характер стеганографического изображения. Защита схемы каскадного кодирования обеспечивается ключом сдвига фаз спектрального преобразования и невозможностью вычислить точно t-й корень системы из $(t-1)$ уравнений при криптоанализе алгоритма разделения секрета.

SPECTRAL-CODE STEGANOGRAPHIC PROTECTION OF THE IMAGE IN DISTRIBUTED SYSTEMS

S.B. SALOMATIN, Yu.E. YAVORKO

Abstract. Algorithms of spectral code steganographic protection of the image in a distributed systems using the Fourier transform and the method of secret separation and the Garner algorithm are considered.

Keywords: steganography, Fourier transform, secret separation, Chinese remainder theorem.

Список литературы

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика К., 2006.
2. Д. Ватолин [и др.] Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М., 2002.
3. Wang S., Fang Y., Cheng S. Distributed source coding theory and practice. Wiley, 2017

УДК 621.392

МОДЕЛИРОВАНИЕ СЕТИ MANET В СИМУЛЯТОРЕ NS-3

В.А. БЕЛАН, М.М. ШАКИР, М.Ю. ХОМЕНОК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Проанализированы системные характеристики самоорганизующейся сети с динамически изменяющейся топологией, использующей технологию Manet, на базе симулятора NS-3. Представлен обзор возможностей симулятора как в исследовательских, так и в образовательных целях.

Ключевые слова: сетевой симулятор, NS-3, NetAnim, Flow Monitor, моделирование, Manet.

Введение

Для моделирования сетей используются множество сетевых симуляторов, таких как OMNet++, OPNET, NetSim, NS-2 и NS-3. Также существуют и узко специализированные симуляторы для моделирования определенного оборудования. Одним из широко распространенных симуляторов со свободным программным обеспечением в течение более трех десятков лет является NS-2, ориентированный на исследовательское применение, а также на применение в образовательных целях.

Network Simulator 3 (NS-3) – это сетевой симулятор дискретного события с открытым исходным кодом, распространяемый под лицензией GNU GPLv2 и ориентированный на устранение ограничений NS-2. Исходные коды NS-3 открыты для исследования, модификации и использования и доступны на сайте проекта http://www.nsnam.org.

NS-3 является гибким и в то же время мощным средством моделирования за счет использования C++ в качестве встроенного языка описания модулей. Помимо C++ может использоваться Python. Оба языка в симуляторе равноправны и применяются для описания моделей телекоммуникационных систем. Программа реализована под операционную систему на базе ядра Linux [1]. Наиболее используемые дистрибутивы – Ubuntu (рис. 1), CentOS, Linux Mint, Debian, Fedora, XUBUNTU, openSUSE.

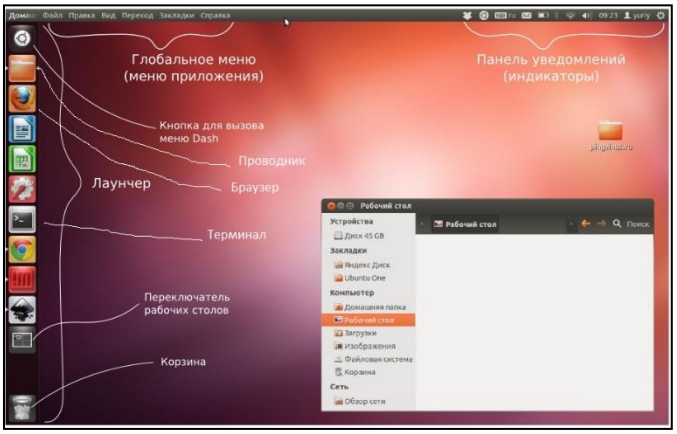


Рис. 1. Интерфейс ОС Ubuntu

Для сетей с динамически изменяющимися топологиями в NS-3 предусмотрены различные модели подвижности объектов в пространстве, например, с движущимися объектами

в трехмерном пространстве, что актуально для самоорганизующихся сетей с динамически изменяющейся топологией, таких как Manet, Vanet и Fanet. Одним из преимуществ NS-3 по сравнению с другими симуляторами является также реализация различных типов Mesh-сетей на основе стека протоколов 802.11s. NS-3 поддерживает множество протоколов маршрутизации, таких как AODV, DSDV, DSR, OLSR.

Симулятор не имеет собственного графического интерфейса, однако для средств визуализации моделей используются модули NetAnim и PyViz. Наиболее функциональным является модуль NetAnim, который помимо визуализации топологии позволяет выполнить пошаговую симуляцию, вывод таблиц маршрутизации во времени, просмотреть информацию о передаваемых пакетах и их трейсы взаимодействия. Модуль позволяет построить графики зависимостей переданных и полученных пакетов на физическом, канальном и сетевом уровнях за отведенное время симуляции [2].

NetAnim позволяет работать с модулем Flow Monitor, предоставляющем очень гибкие методы сбора самых различных показаний с моделируемых активных сетевых устройств и каналов связи. Модуль позволяет оценить характеристики сети и построить гистограммы для визуализации полученных данных. Оба модуля представляют собой XML-файлы.

На рис. 2 представлена топология расположения узлов в начальный момент симуляции Ad-Hoc сети (технология Manet) в окне аниматора NetAnim. В заданной области мобильности [1000×1000] располагаются 10 узлов, 5 из которых являются источниками, а остальные – приемниками информации, с установленными IP адресами и с ID нумерацией 0..9. Линиями показаны траектории движения узлов за время симуляции сети.

Визуализация сетевой топологии в окне аниматора NetAnim

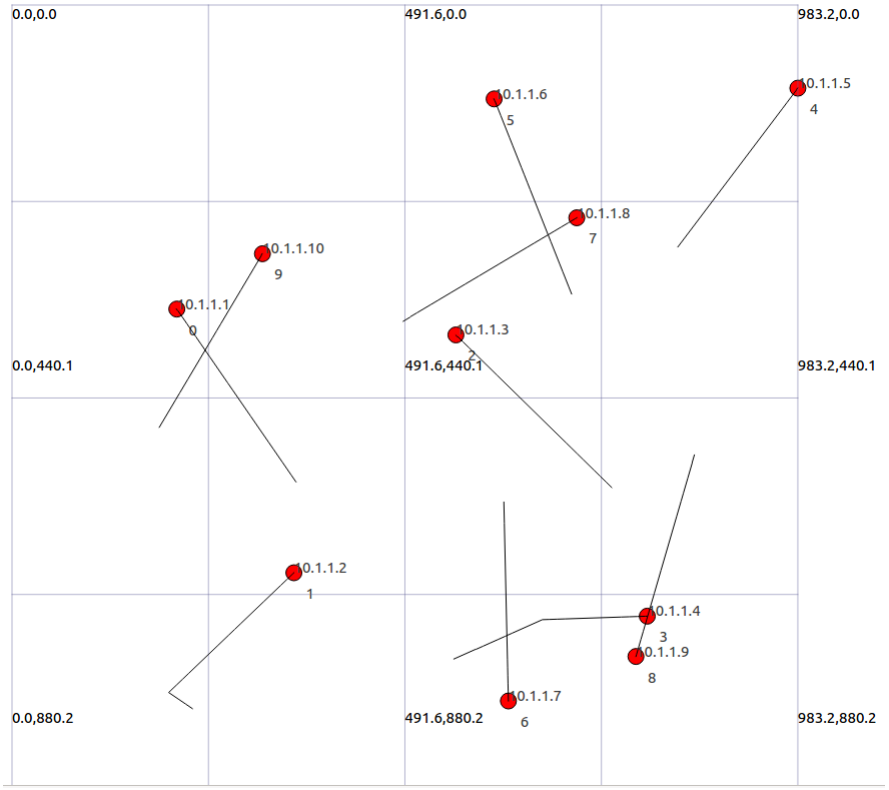


Рис. 2. Исходная топология исследуемой сети MANET: 10 узлов, модель трафика CBR, модель мобильности RWM, формат пакетов UDP, протокол маршрутизации DSDV.

Мобильность узлов соответствует случайному перемещению точки на плоскости в соответствии с моделью RWP (Random WayPoint Mobility Model) со скоростью 10 м/с и временем обновления 2 с. Узлы передают UDP потоки с постоянной скоростью передач 8 кбит/с, что соответствует типу трафика CBR (Constant Bit Rate). Протокол маршрутизации DSDV (Destination–Sequenced Distance Vector). Время симуляции проекта – 30 с.

Результат симуляции с радиусами мощностей и передаваемыми пакетами представлен на рис. 3.

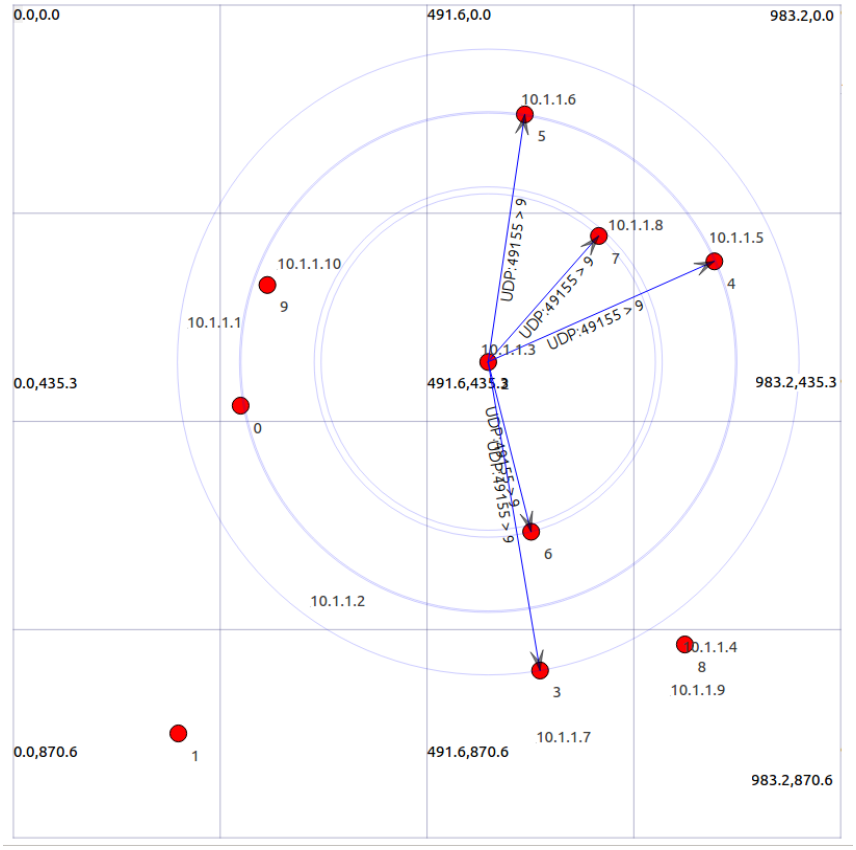


Рис. 3. Топология расположения узлов сети MANET после окончания времени моделирования

На рис. 4 представлена таблица маршрутизации для двух узлов сети.

Node: 1, Time: +29.0s, Local time: +29.0s, DSDV Routing table

DSDV Routing table

Destination	Gateway	Interface	HopCount	SeqNum	LifeTime	SettlingTime
10.1.1.1	10.1.1.1	10.1.1.2	1	12	3.905s	5.000s
10.1.1.3	10.1.1.1	10.1.1.2	3	12	3.934s	0.000s
10.1.1.4	10.1.1.1	10.1.1.2	2	12	3.934s	0.000s
10.1.1.5	10.1.1.1	10.1.1.2	3	12	3.905s	0.000s
10.1.1.6	10.1.1.1	10.1.1.2	3	10	8.933s	0.000s
10.1.1.7	10.1.1.1	10.1.1.2	2	12	3.934s	0.000s
10.1.1.8	10.1.1.10	10.1.1.2	2	12	3.961s	0.000s
10.1.1.9	10.1.1.1	10.1.1.2	4	12	3.931s	0.000s
10.1.1.10	10.1.1.10	10.1.1.2	1	12	3.924s	0.000s
10.1.1.255	10.1.1.255	10.1.1.2	0	12	-9223.855s	0.000s
127.0.0.1	127.0.0.1	127.0.0.1	0	0	-9223.855s	0.000s

Node: 2, Time: +29.0s, Local time: +29.0s, DSDV Routing table

DSDV Routing table

Destination	Gateway	Interface	HopCount	SeqNum	LifeTime	SettlingTime
10.1.1.1	10.1.1.7	10.1.1.3	2	12	3.931s	0.000s
10.1.1.2	10.1.1.4	10.1.1.3	3	12	3.938s	0.000s
10.1.1.4	10.1.1.4	10.1.1.3	1	12	3.901s	0.000s
10.1.1.5	10.1.1.9	10.1.1.3	2	12	3.902s	0.000s
10.1.1.6	10.1.1.6	10.1.1.3	1	12	3.922s	0.000s
10.1.1.7	10.1.1.7	10.1.1.3	1	12	3.904s	0.000s
10.1.1.8	10.1.1.8	10.1.1.3	1	12	3.905s	0.000s
10.1.1.9	10.1.1.9	10.1.1.3	1	12	3.902s	0.000s
10.1.1.10	10.1.1.7	10.1.1.3	3	12	3.931s	0.000s
10.1.1.255	10.1.1.255	10.1.1.3	0	12	-9223.855s	0.000s
127.0.0.1	127.0.0.1	127.0.0.1	0	0	-9223.855s	0.000s

Рис. 4. Таблица маршрутизации узлов 1 и 2 в момент времени окончания симуляции

По таблицам маршрутизации можно определить адрес назначения, узел, через который направлен пакет, и количество скачков до узла назначения, если между узлами нет прямой связи.

Визуализация результатов моделирования анализатором потока FlowMonitor и анализатором пакетов Wireshark

Для вывода результатов симуляции проекта используется модуль Flow Monitor. Это модуль мониторинга потоков, который упрощает сбор и сохранение в постоянном

хранилище общего набора показателей производительности сети. Модуль автоматически обнаруживает все потоки, проходящие через сеть, и сохраняет о них сведения, которые могут потребоваться исследователю для их анализа (битрейты, продолжительность передачи, задержки, размеры пакетов и коэффициент потери пакетов и т. п.). На рис. 5 представлены структура модуля Flow Monitor и собираемые им данные.

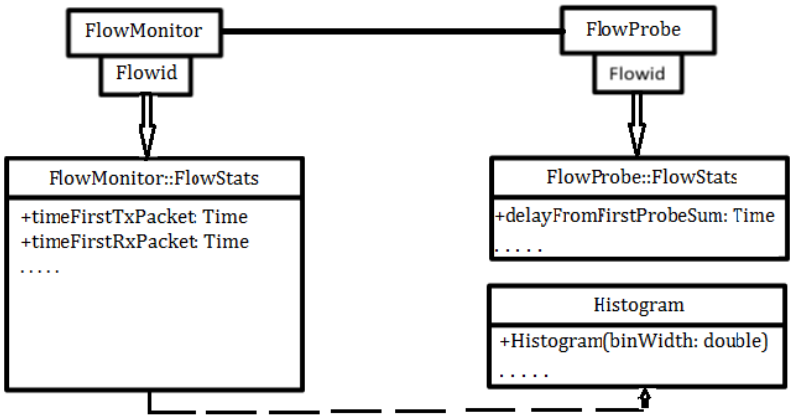


Рис. 5. Структура анализатора потоков Flow Monitor

Модуль Flow Monitor состоит из трех групп классов. Группа из основных классов включает классы FlowMonitor, FlowProbe и FlowClassifier. Класс FlowMonitor отвечает за координацию действий в отношении зондов и собирает статистику из конца в конец для потоков. Класс FlowProbe отвечает за прослушивание событий пакета в определенной точке, сообщает классу FlowMonitor сведения об этих событиях, касающиеся только пакетов, которые проходят через данный зонд. Класс FlowClassifier предоставляет методы перевода необработанных пакетных данных в параметры с идентификаторами потоков [2].

Каждый зонд будет классифицировать пакеты в следующие моменты:

– отправка пакета (трассировка SendOutgoing IPv);

– пересылка пакета (трассировка UnicastForward IPv);

– прием пакета (LocalDeliver IPv);

– отбрасывание пакета (Drop IPv).

Согласно рис. 5, модуль определяет следующие данные, собранные для каждого потока:

– timeFirstTxPacket: когда был передан первый пакет в потоке;

– timeLastTxPacket: когда был передан последний пакет в потоке;

– timeFirstRxPacket: когда первый пакет в потоке был получен конечным узлом;

– timeLastRxPacket: когда был получен последний пакет в потоке;

– delaySum: сумма всех сквозных задержек для всех принятых пакетов потока;

– jitterSum: сумма всех сквозных значений задержки для всех принятых пакетов потока, как определено в RFC 3393;

– txBytes, txPackets: общее количество переданных байтов / пакетов для потока;

– rxBytes, rxPackets: общее количество полученных байтов / пакетов для потока;

– lostPackets: общее количество пакетов, которые считываются потерянными (не сообщается более 10 с);

– timesForwarded: количество пересылок пакета;

– delayHistogram, jitterHistogram, packetSizeHistogram: версии данных для гистограмм задержки, дрожания и размеров пакетов соответственно;

– packetsDropped, bytesDropped: количество потерянных пакетов и байтов.

Статистика собирается для каждого потока, который может быть экспортирован в формате XML. Кроме этого имеется возможность напрямую обращаться к зондам, чтобы запросить конкретную статистику о каждом потоке.

Часть результатов Flow Monitor для исследуемого сетевого фрагмента представлены на рис. 6 в виде таблиц статистических данных. Поток с идентификатором ID 1 передает 25 UDP пакетов от узла с IP адресом 10.1.1.7 на узел 10.1.1.3. В результате симуляции 5 пакетов было

принято напрямую, 10 пакетов были переадресованы на другие узлы и 10 пакетов были потеряны. Соответственно, потеря пакетов Packet Loss ratio составляет около 66 %.

Анализатор потоков Flow Monitor также определяет время отправки и получения первого и последнего пакетов для определения задержки, джиттера и скорости передачи/приема пакетов.

```
Flow Id:1                                   Flow Id:2
======                                      ======
UDP 10.1.1.7/49153---->10.1.1.3/9           UDP 10.1.1.5/49153---->10.1.1.1/9

Tx bitrate:8.56667kbps                      Tx bitrate:8.56667kbps
Rx bitrate:10.3404kbps                      Rx bitrate:8.58815kbps
Mean delay:8.77185ms                        Mean delay:12.5743ms
Packet Loss ratio:66.6667%                  Packet Loss ratio:0%

timeFirstTxPacket=  5.01263e+09ns           timeFirstTxPacket=  5.05748e+09ns
timeFirstRxPacket=  5.03986e+09ns           timeFirstRxPacket=  5.07754e+09ns
timeLastTxPacket=  2.90126e+10ns            timeLastTxPacket=  2.90575e+10ns
timeLastRxPacket=  9.0165e+09ns             timeLastRxPacket=  2.80599e+10ns
delaySum=          4.38593e+07ns            delaySum=          3.01784e+08ns
jitterSum=         2.37225e+07ns            jitterSum=         4.32464e+08ns
lastDelay=         4.38593e+07ns            lastDelay=         3.01784e+08ns
txBytes=           25700                    txBytes=           25700
rxBytes=           5140                     rxBytes=           24672
txPackets=          25                      txPackets=          25
rxPackets=          5                       rxPackets=          24
lostPackets=        10                      lostPackets=        0
timesForwarded=     10                      timesForwarded=     35
```

Рис. 6. Статистические данные анализатора потоков Flow Monitor

С целью анализа процесса межузлового взаимодействия аниматор NetAnim позволяет просмотреть трейсы между узлами, а также передаваемые пакеты в анализируемый промежуток времени. Трейс-граф сети иллюстрирован на рис. 7.

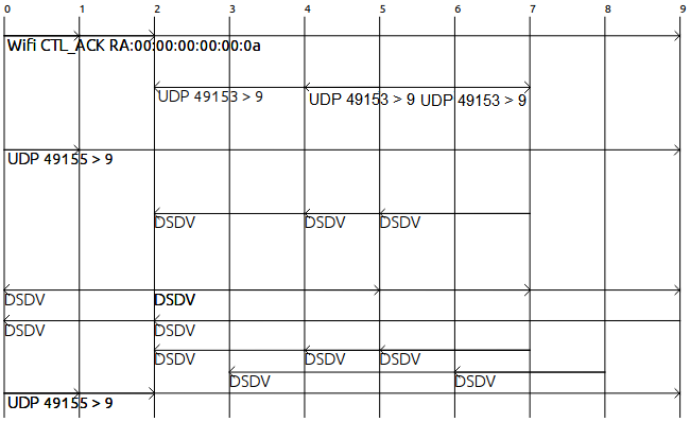


Рис. 7. Трейсы взаимодействия узлов 0–9

Вертикальными линиями представлены узлы сети, горизонтальными стрелками показано взаимодействие узлов и тип передаваемых пакетов. Кроме этого есть возможность изменения типов передаваемых пакетов между узлами на графе трейсов путем установки параметров фильтра, например, UDP, TCP, IPv4, ICMP, DSDV, AODV и т. д.

Вспомогательные объекты в NS-3 могут использоваться для создания файлов трассировки в формате pcap либо tr. Pcap означает захват и анализ структуры пакетов. Самой популярной программой, которая может читать и отображать этот формат, является Wireshark.

Это позволяет проанализировать информацию о структуре передаваемых пакетах на физическом, канальном, сетевом и транспортном уровнях. Вывод результатов в программе Wireshark представлен на рис. 8.

Первая колонка данных соответствует нумерации пакетов, вторая – определяет время симуляции, третья и четвертая соответственно исходящий адрес и адрес назначения, в пятой колонке прописывается тип передаваемого протокола, в следующей – длина пакета, а в последней колонке прописывается общая информация об анализируемом пакете.

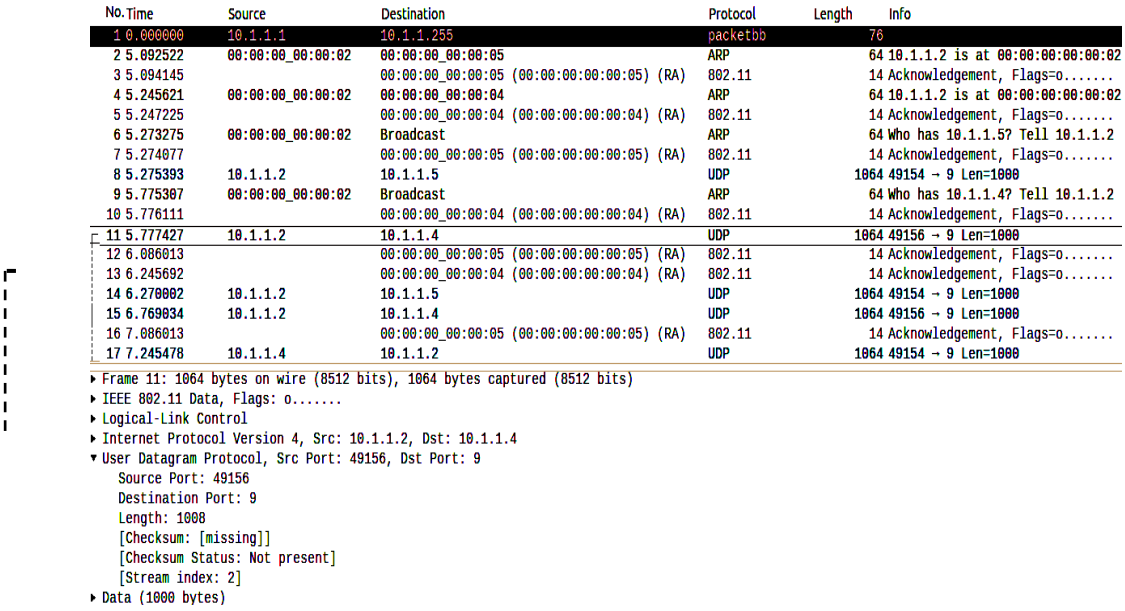


Рис. 8. Пакеты данных Frames 2-17 и формат пакета Frame 11

Кроме анализатора пакетов Wireshark, симулятор NS-3 позволяет создавать файлы трассировки ASCII в формате tr, содержащие данные о типе передаваемых пакетов и информацию о доставке пакетов. Для визуализации результатов, кроме анализатора потоков Flow Monitor, может быть использована утилита gnuplot. Gnuplot предназначена для представления результатов расчета в графической форме, а расчет может проводиться как самой утилитой по формулам, так и независимо, например, программами C++. При этом утилита gnuplot предоставляет возможность выборки данных из файлов.

В процессе имитационного моделирования фрагмента сети Manet модулем Flow Monitor сформировано 45 потоков. Результаты статистической оценки системных параметров анализируемой сети представлены на рис. 9 в виде гистограмм скоростей передачи (Flow_bitrates), количества потерянных пакетов (Number_of_lost_packets) и задержки (Delay) по каждому направлению потоков (Number_of_flows).

Общее число переданных пакетов за время моделирования составило 1125, количество полученных – 838, а процент доставки пакетов – 82. Соответственно средняя пропускная способность сети – 6,77 кбит/с, средняя задержка – 0,064 с, а среднее значение джиттера – составляет 0,05 с.

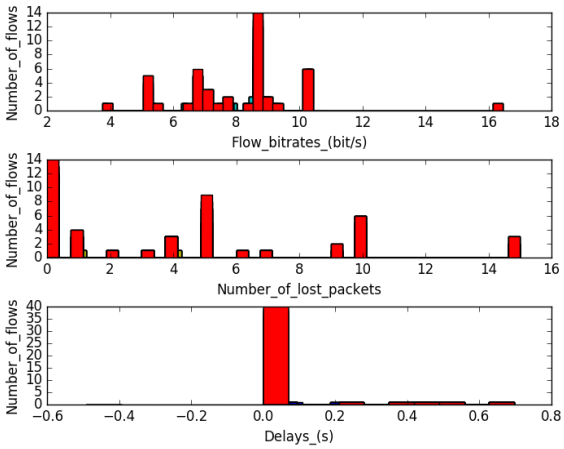


Рис. 9. Результаты статистической обработки по всем потокам

Из гистограмм видно, что для проектируемой сети для большинства потоков характерны минимальная задержка и потеря пакетов, а пропускная скорость варьируется от 4 до 10 кбит/с.

Заключение

Беспроводные сети резко расширили область своего применения, благодаря актуальности двух задач: последней мили и построения децентрализованных сетей. Задача последней мили заключается в организации доступа к сервисам традиционной проводной инфраструктурной сети для конечных пользователей. В рамках архитектуры «клиент-сервер» доступ к среде может осуществляться централизованным или распределенным методами.

В первом случае точка доступа монопольно управляет доступом к среде, предотвращая одновременную передачу пакетов разными станциями, а во втором – доступ к среде осуществляется на конкурентной основе, когда все клиентские станции, а также сама точка доступа соревнуются за право передать пакеты. Децентрализованные сети, или сети класса ad hoc, – это самоорганизующиеся сети, создаваемые из равнозначных станций, и когда это необходимо – без проводной инфраструктуры.

Отказ от архитектуры «клиент-сервер» при построении сетей класса ad hoc делает решения обеих задач существенно разными, а развертывание таких сетей независимо от их применения требует проведения изыскательских и исследовательских программ с целью расширения зоны покрытия сети и обеспечения бесперебойной работы движущихся станций, выполнение которых предполагает владение навыками компьютерного моделирования. Эффективность такого подхода иллюстрируется результатами, представленными в статье.

MODELING MANET NETWORK IN SIMULATOR NS-3

V.A. BELAN, M.M. SHAKIR, M.Yu. HOMENOK

Abstract. The system characteristics of a self-organizing network with a dynamically changing topology which use the Manet technology on base of the NS-3 simulator were analyzed. A review of the capabilities of the simulator for both research and educational purposes was performed.

Keywords: modeling, NS-3, simulator, Manet, NetAnim, flow monitor.

Список литературы

1. NS-3 [Электронный ресурс]. URL: http://clone.nsnam.org/ns-3-allinone (дата обращения: 10.11.2018).
2. NetAnim [Электронный ресурс]. URL: https://www.nsnam.org/wiki/NetAnim (дата обращения: 10.11.2018).

УДК 004.732

ОПТИМИЗАЦИЯ РАБОТЫ ЗАЩИЩЕННОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

С.Ю. ЛОСКОТ, А.В. МУРАШКО, О.А. ХАЦКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Предложен метод оптимизации работы и повышения информационной безопасности корпоративной мультисервисной сети связи при помощи использования межсетевого экрана. Представлена подробная классификация межсетевых экранов. Выполнена оценка эффективности работы защищенной мультисервисной сети.

Ключевые слова: межсетевой экран, мультисервисная сеть, базы данных, WAN-соединение.

Введение

Для эффективной разработки и внедрения в эксплуатацию мультисервисных сетей связи необходимо предусмотреть своевременную защиту программ и баз данных, средств хранения, обработки и передачи информации. Основные требования, предъявляемые к мультисервисной сети связи, заключаются в следующем: высокий уровень информационной безопасности; организация четкой аутентификации и идентификации всех пользователей автоматизированной информационной системы; организация системы централизованного управления и др. [1].

Классификация межсетевых экранов

Межсетевой экран, сетевой экран – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа, реализуемого с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами. Помимо защитной функции, межсетевые экраны позволяют отфильтровывать нежелательный трафик и блокировать его попадание в сеть или в отдельно взятые ее сегменты [2].

Имеется множество классификаций и вариантов реализации межсетевых экранов. К основным можно отнести реализации, предложенные компанией Cisco [3].

1. *Прокси-сервер*. Прокси-сервер служит шлюзом между сетями для конкретного приложения. Прокси-серверы могут выполнять дополнительные функции, например, кэширование и защиту контента, а также препятствовать прямым подключениям из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

2. *Межсетевой экран с контролем состояния сеансов*. Он пропускает или блокирует трафик с учетом состояния, порта и протокола, а также осуществляет мониторинг всей активности с момента открытия соединения и до его закрытия. Решения о фильтрации принимаются на основании правил, определяемых администратором, а также контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению.

3. *Межсетевой экран UTM (unified threat management)*. Сочетает такие функции, как контроль состояния сеансов, предотвращение вторжений и антивирусное сканирование. Также оно может включать в себя дополнительные службы, а зачастую – и управление облаком. Основные достоинства UTM – простота и удобство эксплуатации.

4. *Межсетевой экран нового поколения (Next-Generation Firewall).* Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем состояния сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений. Эти экраны должны включать в себя такие функции как контроль состояния сеансов; система предотвращения вторжений; учет и контроль особенностей приложений, позволяющих распознавать и блокировать приложения, предотвращения вторжений; функции учета и контроля особенностей приложений, позволяющие распознавать и блокировать приложения, представляющие опасность; схема обновления, позволяющая учитывать будущие каналы информации; технологии защиты от постоянно меняющихся и усложняющихся угроз безопасности.

5. *NGFW (Next-Generation Firewall) с активной защитой от угроз.* Эти экраны обеспечивают защиту от угроз путем интеллектуальной автоматизации безопасности в динамическом режиме. Обладают такими функциями, как определение ресурсов, наиболее подверженых риску; быстрое реагирование на атаки, благодаря интеллектуальной автоматизации безопасности, которая устанавливает политики и регулирует защиту в динамическом режиме; выявление отвлекающей и подозрительной деятельности путем применения корреляции событий в сети и на оконечных устройствах; использование ретроспективных средств обеспечения безопасности, которые осуществляют непрерывный мониторинг на предмет подозрительной деятельности и поведения даже после первоначальной проверки; применение унифицированных политик, обеспечивающих защиту на протяжении всего жизненного цикла атаки.

Для проведения исследования в рамках настоящей работе был выбран межсетевой экран с контролем состояния сеансов.

Описание разработанной модели. Результаты исследования.

В качестве объекта исследования была выбрана сеть ЗАО «Технопром». Организация имеет два офиса. Каждый офис имеет собственную локальную сеть. Суммарное количество рабочих станций в двух локальных сетях – 500. Пользователи имеют доступ к серверу базы данных, где хранится информация о клиентах, а также к электронной почте и HTTP-серверу. Некоторые сотрудники компании загружают мультимедиа контент, замедляя доступ к сети Интернет другим сотрудникам. В целях обеспечения необходимо уровня безопасности и оптимизации работы мультисервисной сети организацией используется брандмауэр.

Моделирование мультисервисной сети выполнено в программе Riverbed Modeler 17.5. Она представляет собой объектно-ориентированный инструмент моделирования сетей связи, который располагает обширным пакетом различных моделей сетевых элементов, библиотеками протоколов сетей связи. Кроме того, с помощью этой программы можно выполнять расчет основных характеристик с учетом параметров QoS для различных типов трафика [4]. Результаты моделирования представлены в виде графиков, которые отражают процент загрузки WAN-соединения, время отклика базы данных и время отклика Web-страницы.

Были смоделированы два случая работы сети: без установки брандмауэра и с установкой брандмауэра. При моделировании в первом случае были получены следующие данные: время отклика базы данных составляет более 1 с (рис. 1); время отклика Web-страницы – более 3 с (рис. 2); процент загрузки WAN-соединения равен в среднем 80 (рис. 3), что приводит к некорректной работе приложений в сети.

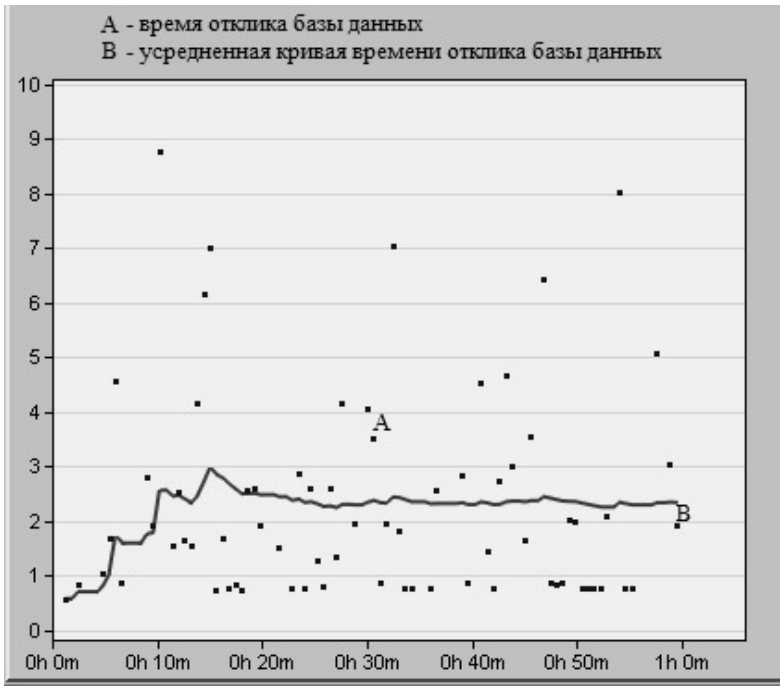


Рис. 1. График отклика баз данных без использования брандмауэра

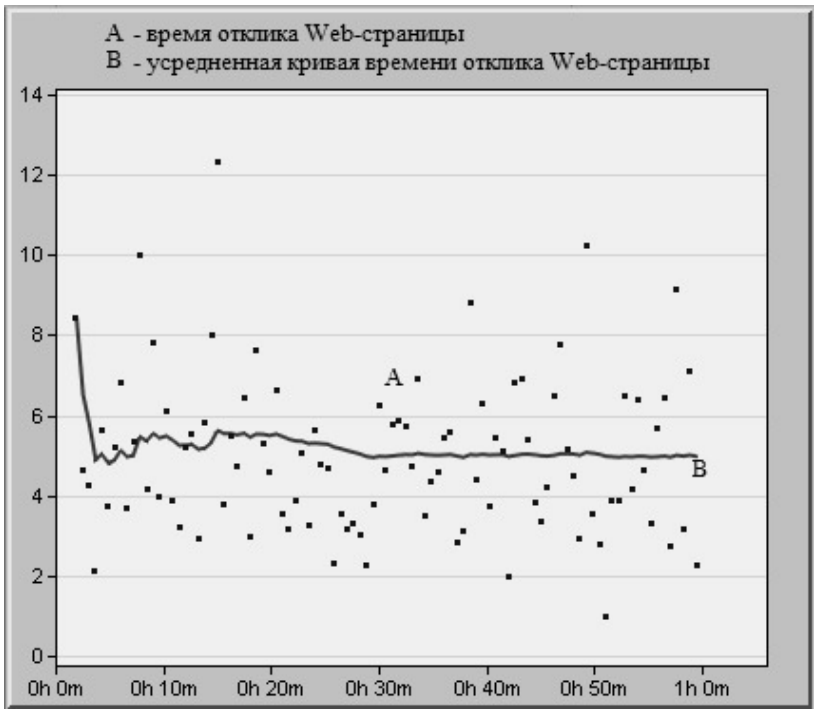


Рис. 2. График отклика Web-страниц без использования брандмауэра

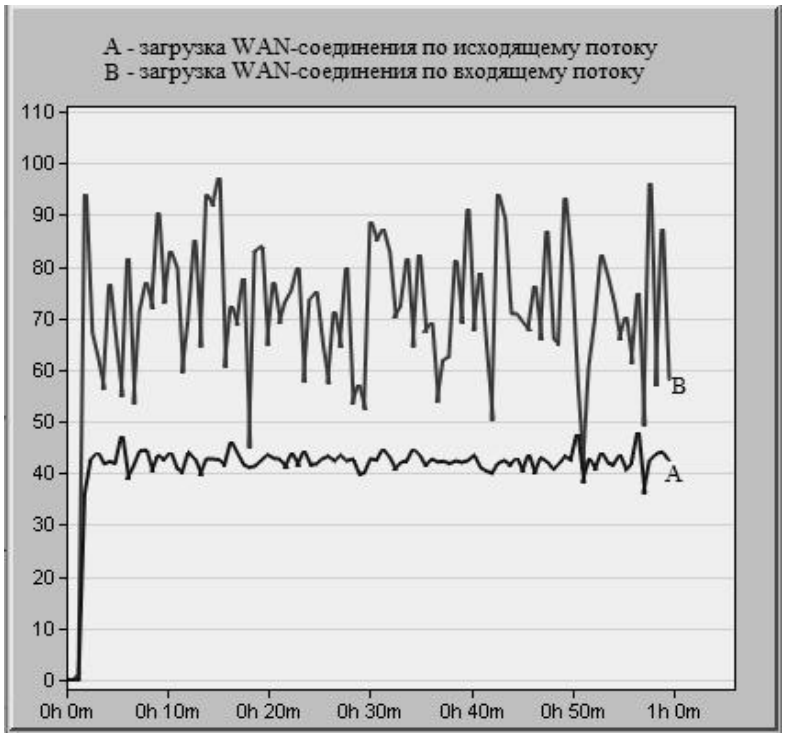


Рис. 3. Графики загрузки общего WAN-соединения без использования брандмауэра

При моделировании во втором случае были получены следующие данные: время отклика базы данных составляет 1 с (рис. 4); время отклика Web-страницы – 3 с (рис. 5); процент загрузки WAN-соединения уменьшился с 80 до 40 %(рис. 6).

Рис. 4. Графики сравнения отклика баз данных без использования и с использованием брандмауэра

Рис. 5. Графики сравнения отклика Web-страниц без использования и с использованием брандмауэра

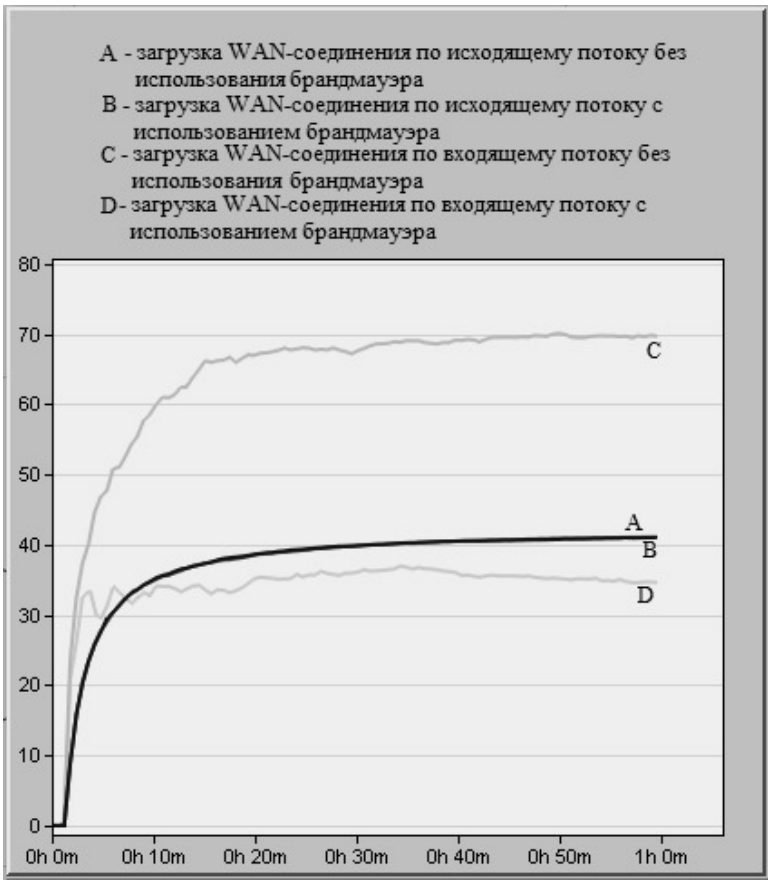


Рис. 6. Графики сравнения загрузки общего WAN-соединения без использования и с использованием брандмауэра

Заключение

Предложенный в работе метод моделирования мультисервисной сети позволил наглядно проиллюстрировать способ оптимизации ее работы и повышения ее информационной безопасности с помощью межсетевого экрана.

В результате моделирования доказана возможность снижения времени отклика базы данных и времени отклика Web-страницы с 3 до 1 с и с 5 до 3 с соответственно, а также возможность уменьшения процента загрузки WAN-соединения с 80 до 40 %.

Проведенные исследования показывают, что при использовании в сети устройства защиты от несанкционированного доступа и его правильной конфигурации можно оптимизировать работу мультисервисной сети, улучшить ее производительность и обеспечить необходимый уровень безопасности.

OPTIMIZATION OF WORK OF PROTECTED MULTISERVICE NETWORK

S.Yu. LOSKOT, A.V. MURASHKO, O.A. KHATSKEVICH

Abstract. A method of optimizing the work and increasing the information security of a corporate multiservice communication network by using the firewall is proposed. Detailed classification the firewalls is submitted. Efficiency of secure multiservice network is evaluated.

Keywords: firewall, multiservice network, database, WAN-connection.

Список литературы

1. Мультисервисные сети следующего поколения. [Электронный ресурс]. URL: http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html (дата доступа: 10.11.2018)
2. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. МГТУ им. Н. Э. Баумана, 2002.
3. Типы межсетевых экранов [Электронный ресурс]. URL: http://www.cisco.com/c/ru_ru/products/security/firewalls/what-is-a-firewall.html (дата доступа: 10.11.2018)
4. Тарасов В.Н. [и др.] Проектирование и моделирование сетей связи в системе Riverbed Modeler. Самара, 2016.

УДК 004.056

МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА К СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

А.И. ГОССА, А.Е. ЛАГУТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 31 октября 2018

Аннотация. Разработана модель разграничения доступа системы облачных вычислений. Основой для нее явилась математическая модель разграничения доступа. Описана политика информационной безопасности. Определены множества объектов и субъектов доступа для системы облачных вычислений. Определены перечни возможностей для объектов и субъектов доступа, построена иерархическая структура ролей.

Ключевые слова: система облачных вычислений, модель разграничения доступа, иерархия ролей.

Введение

Постоянное усложнение сетевой инфраструктуры, увеличивающаяся скорость процессов обмена данными и широкое использование технологий распределенных сервисов предъявляют высокие требования к эффективности функционирования систем разграничения доступа (РД) к информационным ресурсам. В Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, определено, что под информационной безопасностью является состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1]. Данное понятие является первичным и основным для определения компетенции государственных органов по обеспечению информационной безопасности, а также для установления государственной политики в информационной сфере. Фундаментальным понятием в сфере защиты информации компьютерных систем является политика безопасности. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз [1]. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т.д.) называют моделью безопасности. Среди программно-технических методов защиты информации в первую очередь выделяют разграничение доступа. Разграничение доступа непосредственно обеспечивает конфиденциальность информации, а также снижает вероятность реализации угроз целостности и правомерной доступности. На сегодняшний день разработано множество моделей разграничения доступа, основанных на различных признаках (матрицы доступа, роли, задачи, события и пр.), что объясняется обширной природой современных систем. Каждая из моделей имеет свои достоинства и недостатки при ее использовании в той или иной системе.

Актуальность разработки модели разграничения доступа и частных политик информационной безопасности (ИБ) объясняется необходимостью планирования и управления ИБ на всех этапах жизненного цикла информационной системы. В случае разработки частной политики безопасности информационных систем облачных технологий (ИСОТ) на основе модели разграничения доступа необходимо учитывать специфику межоблачных взаимодействий между поставщиком и потребителем услуг. С помощью правильно составленной политики ИБ можно обеспечить безопасное, доверенное и адекватное управление системой облачных вычислений (СОбВ), поддержку непрерывности межоблачного взаимодействия, повышение

уровня доверия потребителя к поставщику облачных услуг и, как следствие, минимизацию рисков нарушения информационной безопасности в системе облачных вычислений. Основой построения модели разграничения доступа является модель ролевого разграничения доступа или RBAC – технология контроля доступа, использование которой актуально в современных компьютерных средах. В ролевой политике разрешения ассоциированы с ролями, и пользователи соотносятся с соответствующими ролями, получая таким образом разрешения ролей. Это упрощает управление всей СОбВ в целом. Кроме того, ролевая политика безопасности позволяет избежать угроз информационной безопасности, связанных с неопределенностью ответственности в СОбВ.

Постановка решаемой задачи

В статье решаются задачи усовершенствования ролевой модели разграничения доступа и разработки матрицы доступа к информационным объектам в СОбВ. Для этого необходимо определить множество сущностей в СОбВ (информационные субъекты и информационные объекты), а также построить иерархию ролей и сформировать матрицу разграничения доступа.

Построение иерархической структуры ролей

Основными элементами математической модели ролевого разграничения доступа являются [2]:

– U – множество пользователей;

– R – множество ролей;

– P – множество прав доступа к объектам СОбВ;

– S – множество межоблачных сессий пользователей;

– $(L, \geq)$ – решетка уровней конфиденциальности информации;

– $PA: R \to 2^P$ – функция, определяющая для каждой роли множество прав доступа, при этом для каждого $p \in P$ существует $r \in R$ такая, что $p \in PA(r)$;

– $UA: U \to 2^R$ – функция, определяющая для каждого пользователя множество ролей, на которые он может быть авторизован в облаке;

– $user: S \to U$ – функция, определяющая для каждой межоблачной сессии пользователя, от имени которого она авторизована;

– $roles: U \to 2^R$ – функция, определяющая для каждого пользователя множество ролей, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s))$;

– c: $U \to L$ – функция уровня доступа пользователя;

– c: $O \to L$ – функция уровня конфиденциальности объекта облака;

– $A = \{read, write\}$ – виды доступа;

– AR – множество административных ролей $(AR \cap R = \varnothing)$;

– AP – множество административных прав доступа $(AP \cap P = \varnothing)$;

– $ARA: AR \to 2^{AR}$ – функция, определяющая для каждой административной роли множество административных прав доступа, при этом для каждого $p \in AP$ существует $r \in R$ такая, что $p \in ARA(r)$;

– $AUA: U \to 2^{AR}$ – функция, определяющая для каждого пользователя множество административных ролей;

– $roles: S \to 2^R \cup 2^{AR}$ – функция, определяющая для пользователя множество ролей, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s)) \cup UA(user(s))$.

Для реализации модели ролевого разграничения доступа в СОбВ необходимо установить уровни конфиденциальности, а также определить множество специфических для СОбВ информационных объектов доступа и сформировать множество возможных субъектов доступа.

Установим три уровня конфиденциальности СОбВ и примем для них следующие обозначения: ОИ – открытая информация, К – конфиденциально, СК – строго конфиденциально.

В результате исследований разработано и предложено множество информационных объектов доступа для системы облачных вычислений (табл. 1).

Таблица 1. **Множество информационных уровней СОбВ**

Обозначение	Наименование	Уровень конфиденциальности
o1	Сайт поставщика облачных услуг	ОИ
o2	Множество логинов и паролей личных кабинетов сотрудников потребителя облачных услуг	К
o3(1)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
o3(2)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
o4(1)	Информационные ресурсы по проекту 1, хранящиеся в облачном хранилище	СК
o4(2)	Информационные ресурсы по проекту 2, хранящиеся в облачном хранилище	СК
o5	Файлы СОбВ, относящиеся к конфигурированию собственных виртуальных машин	СК
o6(1)	Файлы СОбВ, относящиеся к управлению внутриоблачным пространством, осуществляемым поставщиком облачных услуг	СК
o6(2)	Файлы СОбВ, относящиеся к сервисам безопасности поставщика облачных услуг	СК
o7	Данные о серверном времени, скорости данных, объем в хранимых данных	К
o8	Данные о фактическом распределении доступа в фактическом пуле облака	СК
o9	Объем предоставленных потребителю услуг	К
o10(1)	Информационные ресурсы по проекту 1, хранящиеся на стороне потребителя облачных услуг	К
o10(2)	Информационные ресурсы по проекту 2, хранящиеся на стороне потребителя облачных услуг	К
o11(1)	Экземпляры отдела, работающего по проекту 1, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК
o11(2)	Экземпляры отдела, работающего по проекту 2, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК

Множество ролей пользователей (субъектов доступа) системы облачных вычислений, разработанное в ходе исследований, представлено в табл. 2

Таблица 2. **Множество субъектов доступа в СОбВ**

Обозначение	Наименование	Уровень доступа
1	2	3
*L*1	Технический директор поставщика облачных услуг	СК
*LT*1	Сотрудник первой линии техподдержки поставщика облачныхных услуг	К
*LT*2	Сотрудник второй линии техподдержки поставщика облачныхных услуг	СК
*LT*3	Сотрудник третей линии техподдержки поставщика облачныхных услуг	К
*S*1	Руководитель службы автоматизации ИСОТ	СК
*S*2	Главный специалист по ИСОТ	СК
*S*3	Администратор инфраструктуры ИСОТ	К
*S*4	Эксперт по виртуализации в облачных вычислениях	К
*AV*1	Начальник службы безопасности облачного поставщика	СК
*AV*2	Специалист по защите программного обеспечения и платформ поставщика услуги SaaS	К
*AV*3	Специалист по защите облачной инфраструктуры поставщика услуги SaaS	К
*AV*4	Специалист по защите кластера физических серверов поставщика	К
*P*1	Технический директор потребителя облачных услуг	СК
*P*2,*P*3	Руководители подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес процессами	СК

Продолжение таблицы 2

1	2	3
*A*1	Начальник отдела автоматизации и безопасности потребителя	СК
*A*2	Администратор безопасности потребителя облачных услуг	СК
*A*3	Работник, осуществляющий интеграцию и сопровождение SaaS ИСОТ (менеджер ИСОТ)	СК
*A*4	Администратор средств защиты потребителя	К
*P*4,*P*5	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия	К
*P*6,*P*7	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия	К
*P*8,*P*9	Сотрудники потребителя облачных услуг, работающие по проектам 1 и 2 соответственно, не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами.	ОИ
*P*10	Сотрудники потребителя облачных услуг, не работающие по проектам 1 и 2 соответственно и не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ

На рис. 1 представлена разработанная иерархическая структура ролей для множества субъектов доступа в СОбВ.

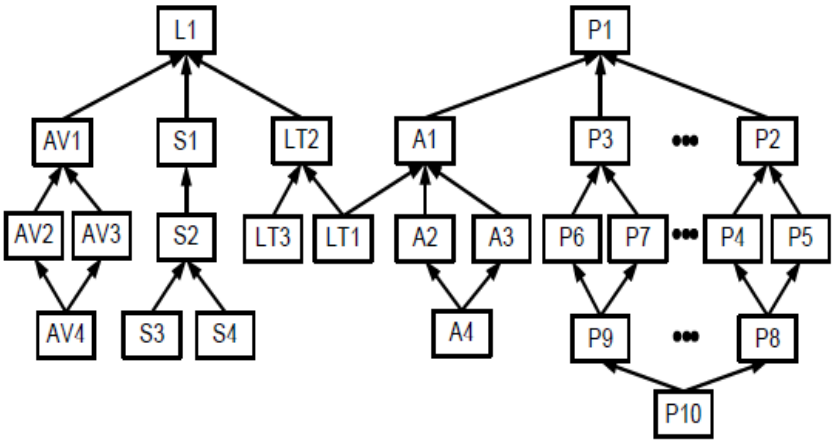


Рис. 1. Иерархическая структура ролей в СОбВ

Так как система облачных вычислений – это система, в которой взаимодействуют поставщик и потребитель облачных услуг, будем модифицировать ролевую модель разграничения доступа таким образом, что каждая из представленных сторон (потребитель и поставщик) имеет свою максимальную роль в иерархии, в отличие от известной ролевой модели разграничения доступа, где максимальная роль в иерархи может быть только одна. Для поставщика облачных услуг максимальной ролью является роль технического директора поставщика (*L*1), для потребителя, − роль технического директора потребителя облачных услуг (*P*1).

В общем случае иерархия ролей потребителя будет иметь больше уровней и будет более распределенной. В примере, проиллюстрированном иерархией ролей на рис. 1, потребитель облачных услуг имеет два подразделения, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами. В каждом из подразделений минимальная роль отводится сотрудникам потребителя облачных услуг, не имеющим права эксплуатировать СОбВ в соответствии с бизнес-процессами (*P*8, *P*9, *P*10), а максимальная − руководителям подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами (*P*2, *P*3). Кроме того, в иерархии учтено, что два подразделения потребителя могут выполнять работу в СОбВ над разными проектами (проекты 1 и 2), которые, в соответствии с бизнес-процессами, не имеют общих и пересекающихся ресурсов и активов. Таким образом, сотрудники подразделения, работающего по проекту 1, не имеют доступ к информационным ресурсам и активам СОбВ подразделения, работающего по проекту 2, и наоборот.

В иерархии потребителя облачных услуг, помимо двух подразделений, работающих по проектам 1 и 2, есть третье подразделение, отвечающее за автоматизацию и информационную

безопасность компании. Максимальная роль в этом подразделении отводится начальнику отдела автоматизации и безопасности потребителя облачных услуг (*A*1), а минимальная – администратору штатных средств защиты (*A*4), под которыми понимаются традиционные средства защиты, не входящие в систему безопасности облачной среды потребителя.

Иерархия поставщика облачных услуг, где максимальная роль отведена техническому директору поставщика (*L*1), состоит из трех служб-отделов: служба поддержки потребителей облачных услуг, службы автоматизации облачной среды и службы информационной безопасности поставщика облачных услуг.

Служба поддержки потребителей состоит из трех линий поддержки (*LT*1, *LT*2, *LT*3 соответственно), которые взаимодействуют напрямую с потребителями облачных услуг и помогают конкретному поставщику решать возникающие вопросы и проблемы в реальном масштабе времени. В ходе исследований были выделены три возможные линии технической поддержки облаков [3]:

– сотрудники первой линии техподдержки поставщика облачных услуг, которые при обращении к ним потребителя ликвидируют технические сбои в инфраструктуре, влияющие на предоставляемые пользователям сервисы; эти сотрудники не обладают высокими привилегиями в СОбВ, не имеют доступа к сервисам безопасности СОбВ;

– сотрудники второй линии техподдержки поставщика облачных услуг – группа специалистов высокого профиля, которые обладают достаточной компетенцией и способны решать проблемы как с инфраструктурой СОбВ, так и с сервисами;

– сотрудники третьей линии техподдержки поставщика облачных услуг являются сотрудниками разработчика и производителя технологии облачных вычислений (Amazon, Google, Microsoft).

Служба автоматизации облачной среды отвечает за разработку и процесс интеграции в SaaS облачных вычислений со стороны потребителя облачных услуг; сотрудники службы занимаются вопросами оптимального управления облачными сервисами в условиях существующих ограничений сети потребителя облачных услуг. Максимальной ролью в данной службе будет обладать руководитель службы автоматизации ИСОТ (*S*1), а минимальными ролями – администратор инфраструктуры ИСОТ (*S*3) и эксперт по виртуализации в облачных вычислениях (*S*4).

Служба информационной безопасности поставщика облачных услуг отвечает за безопасность облачной среды со стороны поставщика облачных услуг [3]. В данной службе роли распределены на три составляющие защиты облака: защита программного обеспечения и платформ поставщика услуги SaaS (роль *AV*2), защита облачной инфраструктуры поставщика услуги SaaS (роль *AV*3) и защита кластера физических серверов поставщика облачных услуг (роль *AV*4). Максимальной в данной службе будет роль начальника службы безопасности облачного поставщика (*AV*1), а минимальной – роль специалиста по защите кластера физических серверов поставщика облачных услуг (*AV*4).

Иерархия ролей пользователей СОбВ задает на множестве R отношения частичного порядка «$\le$», при котором выполняется условие: для $u \in U$, если $r_i, r_j \in R, r_j \in UA(u)$ и $r_i \le r_j$, то $r_i \in UA(u)$. При этом для $r_i \le r_j$ выполняется одно из условий:

1) $r_i = x_i \_ read, r_j = x_j \_ read, x_i \le x_j;$

2) $r_i = x_i \_ write, r_j = x_j \_ write, x_j \le x_i,$

где U – множество пользователей, R – множество ролей.

Модель контролирует назначение пользовательской роли посредством отношения $can-assign \subseteq ARxCRx2^R$. Отношение $can-assign(x, y, \{a, b, c\})$ означает, что член административной роли *x* (или член административной роли, которая является старшей для *x*), может назначать пользователя, текущее членство (или отсутствие членства) которого в постоянных ролях удовлетворяет условию необходимой предпосылки *y*, членом постоянных ролей *a, b* или *c*.

Для иерархии ролей пользователей СОбВ выполняются следующие ограничения:

1) ограничение функции UA – для каждого пользователя $u \in U$ выделяется роль:

$x\_read = \oplus(UA(u) \cap \{y\_read \mid y \in L\})UA(u)$ (здесь $x = c(u)$) и

$x\_write = \oplus\{y\_write \mid y \in L\} \in UA(u)$ (здесь $x = \oplus L$);

2) ограничения функции roles – для каждой сессии $s \in S$ выделяется множество ролей:

$roles(s) = \{x\_read, x\_write\};\ x = c(o)$

3) ограничения функции PA – для каждого $x \in L$ доступ $(o, read) \in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write);$ для каждого доступа $(o, read)$ существует единственная роль $x\_read : (o, read) \in PA(x\_read)$ (здесь $x = c(o)$).

Разработана матрица доступа ролей пользователей (субъектов доступа) СОбВ к множеству объектов доступа (рис. 2).

	o1	o2	o3 (1)	o3 (2)	o4 (1)	o4 (2)	o5	o6 (1)	o6 (2)	o7	o8	o9	o10 (1)	o10 (2)	o11 (1)	o11 (2)
L1	rw	w	-	-	-	-	-	rw	rw	rw	rw	rw	-	-	-	-
LT2	rw	w	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
LT1	r	-	-	-	-	-	-	-	-	rw	rw	r	-	-	-	-
LT3	r	-	-	-	-	-	-	w	-	-	-	-	-	-	-	-
S1	rw	-	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
S2	rw	-	-	-	-	-	-	rw	-	r	rw	r	-	-	-	-
S3	r	-	-	-	-	-	-	rw	-	r	-	r	-	-	-	-
S4	r	-	-	-	-	-	-	rw	-	r	r	r	-	-	-	-
AV1	r	w	-	-	-	-	-	r	rw	r	r	r	-	-	-	-
AV2	r	w	-	-	-	-	-	r	rw	-	-	-	-	-	-	-
AV3	r	-	-	-	-	-	-	-	rw	r	r	r	-	-	-	-
AV4	r	-	-	-	-	-	-	-	rw	-	-	-	-	-	-	-
P1	r	rw	rwe	rwe	rw	rw	rw	-	-	rw	rw	r	rw	rw	rw	rw
A1	r	rw	rw	rw	-	-	rw	-	-	rw	rw	-	-	-	rw	rw
A3	r	rw	-	w	-	-	rw	-	-	rw	-	-	-	-	w	w
A2	r	rw	-	w	-	-	-	-	-	r	-	-	-	-	w	w
A4	r	rw	-	-	-	-	-	-	-	r	-	-	-	-	-	-
P2	r	rw	re	-	rw	-	-	-	-	r	-	r	rw	-	rw	-
P4,5	r	r	re	-	rw	-	-	-	-	-	-	-	rw	-	rw	-
P8	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P3	r	rw	-	re	-	rw	-	-	-	r	-	r	-	rw	-	rw
P6,7	r	r	-	re	-	rw	-	-	-	-	-	-	-	rw	-	rw
P9	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Рис. 2. Матрица прав доступа ролей пользователей СОбВ

Заключение

Представлены результаты разработки усовершенствованной модели разграничения доступа, которая была описана частной политикой информационной безопасности системы облачных вычислений. Предложенная модель построена с помощью формальной модели, основанной на математической модели ролевого разграничения доступа. Ее достоинством является возможность исключения пользователей, получающих по иерархии ролей права суперпользователей, которые могут напрямую обращаться к результирующим потокам данных потребителя облачных услуг, а также управлять всеми конфигурационными файлами СОбВ. Предложено ввести в иерархию формальной модели две максимальные роли: одну – со стороны поставщика облачных услуг (роль технического директора поставщика облачных услуг) и одну – со стороны потребителя облачных услуг (роль технического директора потребителя облачных услуг), которые имели бы одновременно и максимально необходимую роль в собственном подразделении облака сообщества и минимально необходимую роль для поддержки бизнес-процессов СОбВ. Соблюдение требований частной политики безопасности СОбВ позволит существенно снизить риски использования облачных вычислений как со стороны поставщика, так и со стороны потребителя облачных услуг, и как следствие, позволит увеличить доверие потенциальных потребителей к ИСОТ.

MODEL OF ACCESS CONTROL TO CLOUD COMPUTING ENVIRONMENT

A.I. GOSSA, A.E. LAGUTIN

Abstract. Model for access control of a cloud computing system was developed. The basis for the model was a mathematical model of access control. Information security policy was described. The sets of objects and subjects of access for a cloud computing system were defined. The lists of opportunities for objects and subjects of access were defined, a hierarchical structure of roles was built.

Keywords: cloud computing system, access control model, role hierarchy.

Список литературы

1. Указ президента Республики Беларусь от 9.11.2010 № 576 «Об утверждении концепции национальной безопасности».
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.:2012.
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: 2011.

УДК 621.396.624

ВЛИЯНИЕ ДОПЛЕРОВСКОГО ЭФФЕКТА НА ЧУВСТВИТЕЛЬНОСТЬ ПРИЕМНИКА ИНФРАКРАСНОГО ДИАПАЗОНА В КАНАЛЕ МЕЖСПУТНИКОВОЙ СВЯЗИ

С.А. ЛУКАШЕВИЧ, В.Н. УРЯДОВ, Я.В. РОЩУПКИН,
В.Н. КИЙКО, А.С. ЗЕЛЕНИН, Т.В. ПОЛУЯН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 18 октября 2018

Аннотация. Рассмотрено влияние доплеровского эффекта на наиболее перспективные методы приема оптических сигналов инфракрасного диапазона длин волн в канале связи между нестационарными искусственными спутниками Земли.

Ключевые слова: гомодинный метод приема, двоичная фазовая манипуляция, метод прямого фотодетектирования с предварительным усилителем, амплитудная манипуляция, доплеровский эффект, инфракрасное излучение.

Введение

Основной проблемой при использовании фазовых и частотных методов модуляции, как при прямом фотодетектировании, так и при когерентном приеме в спутниковых системах связи, является наличие доплеровского эффекта. В оптическом канале связи между низкоорбитальным (Low-Earth Orbit – LEO) и геостационарным (Geosynchronous Equatorial Orbit – GEO) спутниками существует частотный разброс, порожденный доплеровским сдвигом частот, ввиду взаимного перемещения спутников. Доплеровский сдвиг для двух объектов определяется исходя из следующих параметров: взаимная скорость движения ν, частота несущей f_0 и угол между траекториями движения объектов α.

Доплеровский сдвиг рассчитывается по формуле:

$$f = f_0 \frac{\sqrt{1-\frac{\upsilon^2}{c^2}}}{1-\frac{\upsilon}{c}\cos\alpha}$$

Величины доплеровского сдвига для различных максимальных взаимных скоростей перемещения искусственных спутников земли (ИСЗ) и различных длин волн источников излучения приведены в табл. 1.

Таблица 1. **Величина доплеровского сдвига при различных условиях**

Максимальная скорость взаимного перемещения спутников, км/с	Доплеровский сдвиг для длины волны 1550 нм, ГГц
10	±6,5
12	±7,5
16	±10

При максимальной взаимной скорости движения спутников 12 км/с доплеровский сдвиг составляет 7,5 ГГц, а скорость изменения частоты – около 10 МГц/с. Такие значения лежат далеко за пределами типичных характеристик систем фазовой автоподстройки частоты ФАПЧ, что, в свою очередь, требует либо расширения полосы входного оптического фильтра,

что негативно скажется на чувствительности приемника [1], либо компенсации до значений в несколько МГц. Отмечено, что доплеровский сдвиг может быть предсказан, если известны высоты подвеса спутников, их орбиты и длины волн передающих лазеров. В радиочастотном диапазоне уже используется такой подход, и он позволяет получить результаты с погрешностью 250 Гц для несущей частоты 2,4 ГГц [2]. Для оптических межспутниковых систем связи ошибка расчетов доплеровского сдвига ожидается в пределах ±15 МГц.

Анализ литературы [3–9] позволил построить графики зависимостей коэффициента ошибки от чувствительности, для гомодинных и гетеродинных приемников для различных типов модуляции (рис. 1).

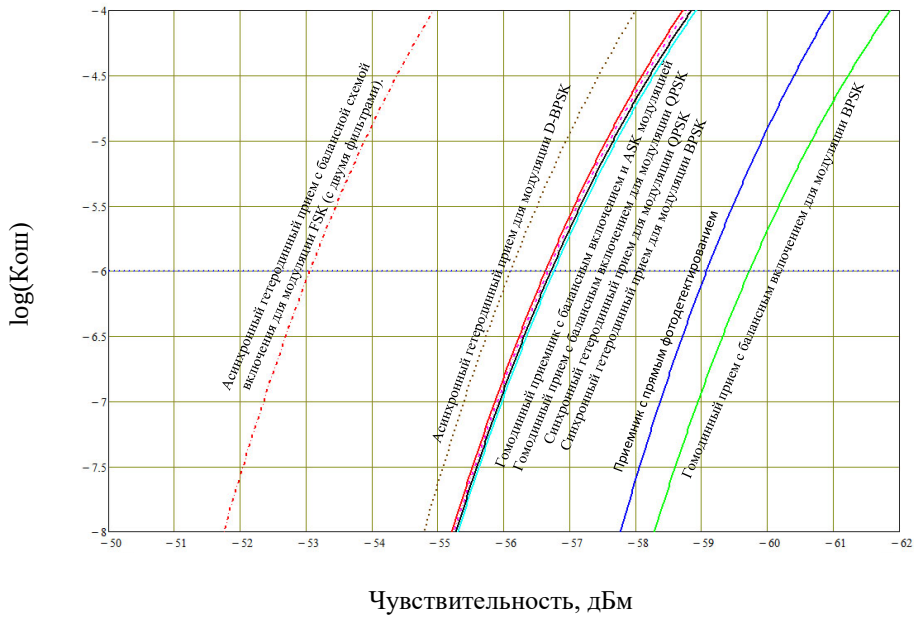


Рис. 1. Зависимость коэффициента ошибок от чувствительности приемника для длины волны излучения 1550 нм

Из графиков (рис. 1) видно, что из всех сравниваемых типов приемников, наибольшей чувствительностью обладают приемники прямого фотодетектирования и гомодинный с балансным включением с двоичной фазовой модуляцией (BPSK – Binary Phase Shift Keying).

Принцип работы приемника прямого фотодетектирования с предусилителем

Оптический предусилитель, установленный перед традиционным приемником прямого фотодетектирования, улучшает чувствительность оптического приемника и расширяет энергетический потенциал системы. Самым распространенным предусилителем в волоконно-оптических линиях связи является волоконно-оптический усилитель на оптическом волокне, легированном ионами эрбия, усилитель типа EDFA (Erbium Doped Fibre Amplifier). Его применение ограничено окном прозрачности 1550 нм.

Принцип работы оптического усилителя основан на использовании волокна, легированного редкоземельными элементами. Такой подход дает возможность создать усилитель, работающий на различных длинах волн из диапазона от 500 до 3500 нм. Структурная схема оптического усилителя представлена на рис. 2. Предусилитель состоит из двух активных элементов: активного волокна и оптической накачки, которая представлена полупроводниковым лазерным источником излучения. Для подмешивания сигнала накачки в волокно применяется оптический разветвитель.

Выигрыш чувствительности приемника с применением оптического предусилителя составляет 15…20 дБ.

Рис. 2. Структурная схема оптического предусилителя

Принцип работы когерентного приемника

Использование лазерного местного гетеродина, благодаря выбору соответствующей мощности, позволяет подавить все шумы от любого источника, кроме шумов местного гетеродина. Это способствует обеспечению максимального отношения сигнал/шум в приемной системе. Также достоинством использования указанного гетеродина является легкость усиления на промежуточной частоте. Отношение сигнал/шум гораздо выше, чем при прямом фотодетектировании.

При гомодинном методе приема частоты входного оптического сигнала и оптического колебания лазерного местного гетеродина должны быть одинаковыми, а фазы – синхронизированными. Таким образом, оптического сигнала ПЧ, а, следовательно, и электрического, не будет, так как разностная частота будет равно нулю. Структурная схема приемника будет состоять только из оптического сумматора, фотодетектора, усилителя, электрического выходного фильтра, лазерного местного гетеродина, системы фазовой автоподстройки частоты и системы автоматического контроля над поляризацией. Структурная схема оптического приемника, реализующего метод гомодинного приема, приведена на рис. 3.

По сравнению с методом прямого детектирования когерентный прием имеет следующие преимущества: возможность определения фазы и частоты когерентного оптического сигнала; прием при спектральном мультиплексировании с меньшим разносом канала приема и передачи; меньшая чувствительность к нежелательному внешнему фоновому оптическому излучению; повышенное отношение сигнал/помеха.

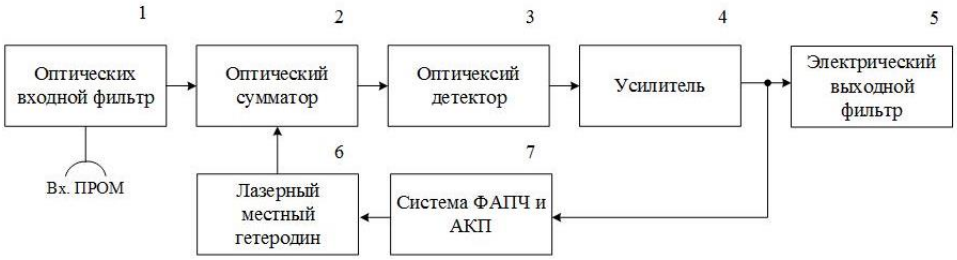


Рис. 3. Структурная схема оптического гомодинного приемника

Недостатком является сложность системы связи. Необходимым условием когерентного приема является синхронизация принимаемого оптического излучения и оптического излучения гетеродина. То есть поляризация этих оптических сигналов должна быть одинакова, а частота и фаза согласованы. Это предъявляет высокие требования к лазерам, которые должны быть одночастотными, иметь минимальные флуктуации фазы, частоты и интенсивности излучения, то есть отличаться высокой стабильностью. Кроме того, лазер-гетеродин должен синхронизироваться с принимаемым оптическим сигналом путем адаптивной подстройки фазы и частоты с использованием обратной связи по фазе.

Анализ влияния доплеровского сдвига на чувствительность приемника прямого фотодетектирования с предварительным усилителем

Изменение частоты вследствие эффекта Доплера оказывает негативное влияние на чувствительность приемника прямого детектирования с оптическим предварительным усилителем, поскольку для приема сигнала необходимо увеличивать полосу пропускания оптического фильтра на входе предусилителя. На рис. 4 приведен график зависимости чувствительности по средней мощности от ширины полосы пропускания входного оптического фильтра.

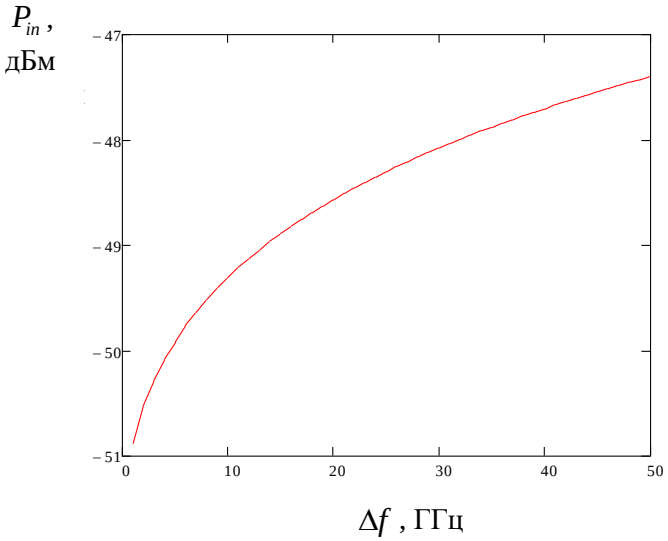


Рис. 4. Зависимость чувствительности приемника с предусилителем от ширины полосы пропускания оптического фильтра

Для фазовых методов модуляции при прямом фотодетектировании важную роль играет изменение фазы оптической несущей вследствие эффекта Доплера. Основной составной частью приемника является схема преобразования фазовой модуляции в модуляцию интенсивности, выполненная на интерферометре Маха–Цендера, в одно из плеч которого введена линия задержки. Данная схема производит сравнение фаз текущей посылки и задержанной, следовательно, время задержки должно точно соответствовать длительности одного бита для выбранной скорости передачи. При изменении частоты вследствие эффекта Доплера между посылками возникнет набег фаз, зависящий от скорости передачи и величины частотного сдвига. Для скорости передачи 1,25 Гбит/с и длины волны 1550 нм величина набега фазы приведена в табл. 2.

Таблица 2. **Величина набега фазы в результате доплеровского сдвига**

Максимальная скорость взаимного перемещения спутников, км/с	Доплеровский сдвиг, ГГц	Набег фазы, Рад
10	±6,5	±10,4π
12	±7,5	±12π
16	±10	±16π

Необходимо отметить, что данный набег фазы возникает за время приема одного бита, и поскольку доплеровский сдвиг меняется медленно, набег фазы будет накапливаться с каждым последующим битом, что делает невозможным использование фазовых методов модуляции без подстройки линии задержки.

Способ компенсации доплеровского сдвига при когерентном приеме

Для решения проблемы доплеровского сдвига существует несколько подходов, которые существенно усложняют схемотехническое исполнение приемника и (или) источника излучения.

Например, постоянная подстройка частоты передающего лазера на основании информации о траектории движения и скоростях спутников, подстройка частоты местного гетеродина при помощи системы ФАПЧ, использование гетеродинного приема с широким полосовым фильтром и др. В то же время оптическая фазовая автоподстройка частоты не позволяет компенсировать большой разброс частот без дополнительных мероприятий.

Для наземных систем нет надобности в применении оптической фазовой автоподстройки частоты (ОФАПЧ), однако в высокоскоростных волоконно-оптических системах передач (ВОСП) используется цифровой метод компенсации (подстройки) фазы несущей после соответствующего вычисления фазовой ошибки в цифровом сигнальном процессоре (DSP – Digital Signal Processor). В случае наличия достаточной надежности высокоскоростных интегральных схем для использования на борту ИСЗ когерентный оптический приемник является наилучшим вариантом [10].

В цифровых когерентных приемниках наиболее часто применяется «Feedforward»-метод оценки фазы несущей для ее синхронизации, так как он является наиболее простым для аппаратной реализации [11].

В начале исследований «Feedforward»-алгоритм ограничивал допустимое отклонение частот между передатчиком и локальным генератором в пределах нескольких мегагерц. Новые алгоритмы позволяют обрабатывать более широкий диапазон несовпадения частот (±5 ГГц) [12]. Однако даже последние наработки в области цифровой обработки сигналов не позволяют перекрыть диапазон подстройки частот ±7 ГГц, необходимый для устойчивого когерентного приема в условиях доплеровского сдвига в межорбитальных оптических каналах.

В работе [13] представлен практический подход к компенсации доплеровского сдвига, применимый к гомодинному оптическому когерентному приемнику межорбитальных спутниковых систем связи. Подход компенсации доплеровского сдвига основан исключительно на изменении частоты локального генератора. Пример работы схемы компенсации доплеровского сдвига приведен на рис. 5. Лазер передатчика работает в одномодовом режиме без перескока моды, к излучению которого применена BPSK-модуляция (рис. 5, *а*). После достижения приемника в сигнале появляется доплеровский сдвиг, описанный выше. В начале процедуры захвата частоты (Frequency acquisition) оба излучения, как передающего лазера, так и локального генератора, находятся в своих частотно-неопределенных полосах с большим промежутком между ними ввиду доплеровского эффекта (рис. 5, *б, в*). Далее к локальному генератору применяется частотный сдвиг, равный вычисленному значению доплеровского сдвига, в соответствие с известной информацией о траекториях и скоростях движения спутников. На этом этапе остаточная ошибка несовпадения частот несущей и локального генератора может составлять до 30 МГц вследствие неточностей численного метода предсказания. Такой разброс не может быть захвачен системой ФАПЧ, имеющей полосу порядка десятков килогерц. После этого частота локального генератора «скользит» в диапазоне ±20 МГц таким образом, что сигнал попадает в полосу ФАПЧ (рис. 5, *г*).

Оптический гомодинный приемник состоит из местного генератора (лазера), поляризационно-квадратурного смесителя, двух балансных оптических приемников, схемы ФАПЧ типа петли Костаса, генератора «скольжения» частоты и предсказателя-компенсатора доплеровского сдвига. Структурная схема такого приемника приведена на рис. 6.

Поляризационно-квадратурный смеситель объединяет принятый оптический сигнал и сигнал местного генератора. Синфазный сигнал при этом смешении попадает в I-порт, а квадратурный – в Q-порт. Каждая пара выходов поляризационно-квадратурного смесителя объединена в два балансных приемника с полосой пропускания 10 ГГц. Выходные сигналы балансных приемников поступают на схему ФАПЧ типа петли Костаса для детектирования разницы фазы несущей, как и сигнал ошибки основой полосы на основании BPSK-модулированных I- и Q-сигналов, который, в свою очередь, посылается на пьезо-актуатор местного генератора (лазера). Для предварительной (грубой) подстройки частоты цепь «скольжения» генерирует осциллирующее напряжение, которое добавляется к управляющему сигналу пьезо-актуатора. Цепь «скольжения» частоты основана на генераторе с мостом Вина, который автоматически запускается от нестабильных компонент остаточных ошибок цепи ФАПЧ петли Костаса.

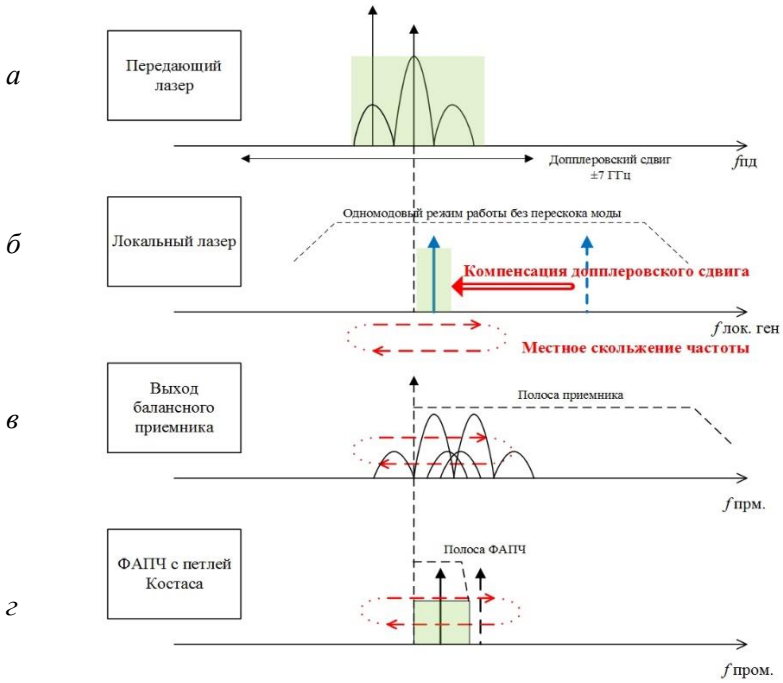


Рис. 5. Диаграммы работы схемы подстройки частоты

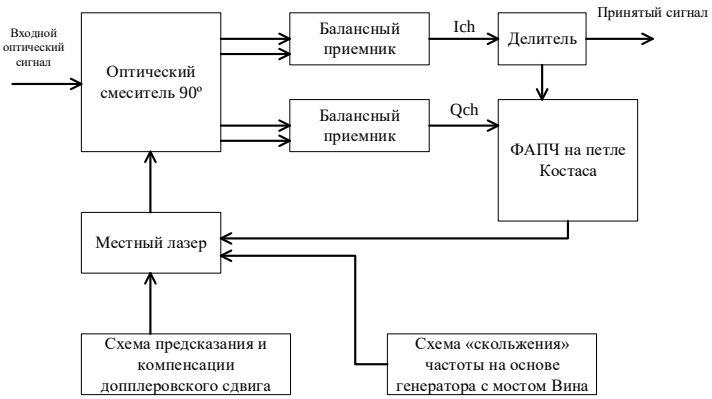


Рис. 6. Структурная схема гомодинного приемника с компенсацией доплеровского сдвига

Заключение

С точки зрения выбора метода приема и типа модуляции, если не обращать внимание на сложность конструкции приемника и множество проблем при его проектировании, стоит выделить гомодинный прием с использованием BPSK-модуляцией, т. к. именно такая комбинация приемника и типа модуляции дает наибольший выигрыш, что позволяет получить значения чувствительности –56,17 дБм, при использовании схемы компенсации доплеровского сдвига и параметрах $\eta = 0{,}85$, $\lambda = 1550$ нм, $B = 1{,}25$ Гбит/с. Полученное значение находится достаточно близко к расчетному пределу чувствительности балансного гомодинного приемника с применением BPSK-модуляции. Дополнительные потери, порядка 3,3 дБ, в основном, порождены применением поляризационно-квадратурного смесителя. Они могут быть снижены по мере улучшения его технических характеристик, что позволит увеличить чувствительность еще приблизительно на 2 дБ.

Сравнивая кривые чувствительности когерентных приемников и приемника прямого фотодетектирования, следует отметить, что последний в идеальном случае требует в среднем 8 фотонов/бит для достижения коэффициента ошибок $<10^{-6}$. Это значение лишь немногим больше по сравнению с гомодинным приемником с использованием BPSK-модуляции и существенно ниже по сравнению с гетеродинными приемниками. Тем не менее, такая чувствительность приемника прямого фотодетектирования на практике не достижима,

вследствие наличия теплового шума, темнового тока и многих других факторов. Поэтому реальная чувствительность приемника прямого фотодетектирования с предусилителем и полосой входного оптического фильтра 20 ГГц для компенсации доплеровского эффекта – составляет –48,5 дБм. С точки зрения аппаратной реализации приемник прямого фотодетектирования с оптическим предусилителем является наиболее простым и имеет меньшие по сравнению с гомодинным массо-габаритные параметры.

INFLUENCE OF DOPPLER EFFECT ON THE RECEIVER SENSITIVITY IN INFRARED INTER-SATELLITE CHANNEL OF COMMUNICATION

S.A. LUKASHEVICH, V.N. URJADOV, Ya.V. ROSHCHUPKIN, V.N. KIYKO, A.S. ZELENIN, T.V. POLUYAN

Abstract. The influence of the Doppler effect on the most promising methods of receiving optical signals in infrared wavelengths in the communication channel between non-stationary satellites is considered.

Keywords: method of homodyne reception, binary phase shift keying, method of direct photodetection with optical pre-amplifier, amplitude keying, Doppler effect, infrared radiation.

Список литературы

1. Schaefer S., Mark G., Werner R. // Photonische Netze. 2015. № 7. P. 69–74.
2. You M.-H., Lee S.-P., Han Y. // ETRI Journal. 2000. Vol. 22, iss. 4. P. 31–39.
3. Agrawal P. Fiber-Optic Communications Systems. John Wiley & Sons, 2002.
4. Тсанг У. Фотоприемники. Техника оптической связи. М., 1988.
5. Урядов В. Н., Стункус Ю.Б. // Докл. БГУИР. 2006. № 3 (15). С. 48–53.
6. Фриман Р.Л. Волоконно-оптические системы связи / Под ред. Н.Н. Слепова. М, 2003.
7. Xu C. Liu X., Wei X. // IEEE J. Sel. Top. Quantum Electron. 2004. Vol. 10, iss. 2. P. 281–293.
8. Ho K.-P., Gnauck A. // Optical Fiber Communication Conference, 2003. Paper ThE1.
9. Gnauck A.H., Liu X., Wei X., Gill D.M., Burrows E.C. Comparison of modulation formats for 42.7-Gb/s single-channel transmission through 1980 km of SSMF / IEEE Photonics Technol. Lett, 2004. Vol. 16. P. 909–911.
10. Toyoshima M. [et al.] // 26th AIAA ICSSC. 2008. P. 13–18.
11. Ly-Gagnon D.-S., Tsukamoto S., Katoh K. // J. Lightw. Technol. 2006. № 24. P. 12–21.
12. Li L., Tao Z., Oda S. // OFC/NOFOEC 2008, OWT4. P. 120–128.
13. Ando T., Haraguchi E., Tajima K. // International Conference on Space Optical Systems and Applications. 2011. P. 30–37.

УДК 621.396.624

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПОСОБОВ ПОСТРОЕНИЯ ОПТИЧЕСКИХ ПРИЕМНИКОВ В ЦИФРОВЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ

Н.В. ТАРЧЕНКО, Ю.С. МОЙСИЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию12 ноября 2018

Аннотация. Разработаны математические модели оптических приемников цифровых сигналов, позволяющие оценить отношение сигнал/шум на выходе этих приемников (на входе устройства принятия решения) и выявить степень влияния на его значение таких показателей, как уровень информационного сигнала и сигнала гетеродина, полосы пропускания оптического приемника.

Ключевые слова: волоконно-оптическая система передачи, непосредственный прием, когерентный прием, гетеродинный прием, гомодинный прем, отношение сигнал/шум, оптический приемник.

Введение

При классификации волоконно-оптических систем передачи (ВОСП) по способу детектирования оптического сигнала выделяют системы с непосредственным и когерентным (гомодинным или гетеродинным) приемом. Качество функционирования приемных оптических модулей определяется электрическим отношением сигнал/шум (ЭОСШ) в точке регенерации сигнала [1, 2].

Целью исследовательской работы является создание математической модели методов детектирования оптических сигналов и дальнейшее моделирование этих методов в среде MathCad с целью выявления тех из них, которые являются наиболее приемлемыми для использования в данных условиях функционирования. В статье рассмотрен случай приема оптического сигнала в виде видеоимпульсов.

Шумовая модель приемных оптических устройств

При анализе ЭОСШ определены источники шума приемных оптоэлектронных модулей. Основными источниками шума оптического приемника являются дробовые шумы, вызванные оптическим информационным сигналом, фоновым излучением и темновым током, и тепловой шум входных цепей приемника [3, 4].

В силу того, что сегодня используются, как правило, оптические системы со спектральным разделением каналов, работающие на большие расстояния, необходимо учитывать и оптический шум, накапливаемый в линии, источниками которого являются оптические передатчики и линейные усилители. Эти шумы учитываются фоновым излучением.

Полный шум для всех видов приема рассчитывается по формуле:

$$P_{\text{Ш}} = 2qM^2M^xB(I_{\text{С}} + I_{\text{Т}} + I_{\text{Ф}})R_{\text{Н}} + \frac{4kTBF_{\text{Ш}}}{R_{\text{Н}}},$$

где q – заряд электрона, Кл; M – коэффициент лавинного умножения или внутреннего усиления фототока; M^x – коэффициент избыточного шума лавинного умножения, B – полоса пропускания выходного фильтра оптического приемника, Гц; $I_{\text{С}}$ – средний ток полезного сигнала, А;

$I_{\text{Т}}$ – средний темновой ток; I_{Φ} – средний ток фонового излучения, А; $R_{\text{Н}}$ – нагрузочное сопротивление оптического приемника, Ом; k – постоянная Больцмана, Дж · с; T – абсолютная температура, К; $F_{\text{Ш}}$ – коэффициент шума предварительного усилителя.

Первое слагаемое соответствует формуле Шотки, которая описывает дробовый шум. Второе слагаемое выражает собственные шумы электронных схем приемных оптических устройств, приведенных к входу предварительного усилителя.

Сопротивление нагрузки фотодетектора зависит от полосы частот принимаемого сигнала и от схемы реализации оптического приемника. Для низкоимпедансного приемника оно определяется, исходя из формулы:

$$R_{\text{Н}} = \frac{1}{2\pi \Delta f C},$$

где Δf – полоса частот принимаемого сигнала, Гц; C – емкость фотодетектора, Ф.

Оптический приемник прямого детектирования

В приемном устройстве прямого детектирования, схема которого показана на рис. 1, полезный сигнал и фоновое излучение проходят через оптический полосовой фильтр и затем попадают на фоточувствительную площадку детектора. Информационный электрический сигнал усиливается, фильтруется низкочастотным выходным фильтром с полосой пропускания B0, равной полосе частот информационного сигнала.

Рис. 1. Схема приемника прямого детектирования

ЭОСШ на выходе приемника определяется по формуле:

$$\text{ЭОСШ} = \frac{\left(M \frac{\eta q}{h\nu_{\text{С}}} P_{\text{С ВХ}} \right)^2 R_{\text{Н}}}{2qM^2 M^x B_0 \left[\frac{\eta q}{h\nu_{\text{С}}} \left(P_{\text{С ВХ}} + P_{\Phi} \right) + I_{\text{Т}} \right] R_{\text{Н}} + \frac{4kTB_0 F_{\text{Ш}}}{R_{\text{Н}}}},$$

где $P_{\text{С ВХ}}$ – мощность оптического сигнала, поступающего на вход приемника, Вт; P_{Φ} – мощность фонового излучения на входе оптического приемника, Вт; S_i – токовая чувствительность фотодиода, А/Вт; η – квантовая эффективность; $\nu_{\text{С}}$ – частота оптической несущей, Гц.

Гетеродинный приемник

В оптическом приемнике с гетеродинным приемом, схема которого показана на рис. 2, лазерное излучение комбинируется на фоточувствительной поверхности с опорным излучением местного генератора. При оптическом смешении входного сигнала и колебания местного генератора выделяется колебание промежуточной частоты $f_{\text{ПЧ}} = \nu_{\text{С}} - \nu_0$. Сигнал промежуточной частоты сохраняет модуляцию входного лазерного сигнала. После прохождения через полосовой фильтр (полоса пропускания $B_{\text{ПЧ}} \geq 2B_0$) электрический сигнал поступает на второй детектор, где и выделяется полезная информация.

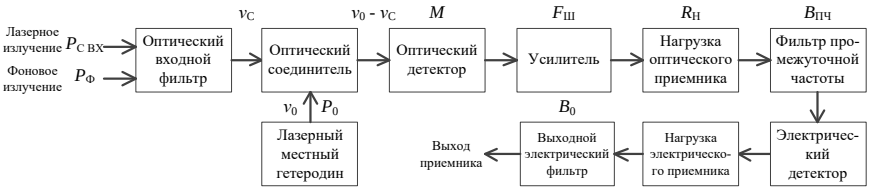


Рис. 2. Схема гетеродинного приемника

ЭОСШ на выходе приемника в соответствии с приведенной схемой приемника определяется по формуле:

$$\text{ЭОСШ} = \frac{\left(M\frac{\eta q}{h\nu_{\text{С}}}\right)^2 P_{\text{С ВХ}} P_0 R_{\text{Н}}}{qM^2 M^x B_0\left[\frac{\eta q}{h\nu_{\text{С}}}\left(P_{\text{С ВХ}}+P_0+P_{\Phi}\right)+I_{\text{Т}}\right]R_{\text{Н}}+\frac{2kTB_0F_{\text{Ш}}}{R_{\text{Н}}}},$$

где P_0 – мощность сигнала гетеродина, Вт.

Гомодинный приемник

В оптическом гомодинном приемнике, схема которого показана на рис. 3, частота и фаза колебания местного гетеродина совпадают с частотой и фазой входного излучения, т. е. получается полная синхронизация двух колебаний. Как и для гетеродинного приема, оптическое смешение осуществляется на поверхности фотодетектора. Выходной сигнал фотодетектора содержит информационный сигнал на фоне шумов.

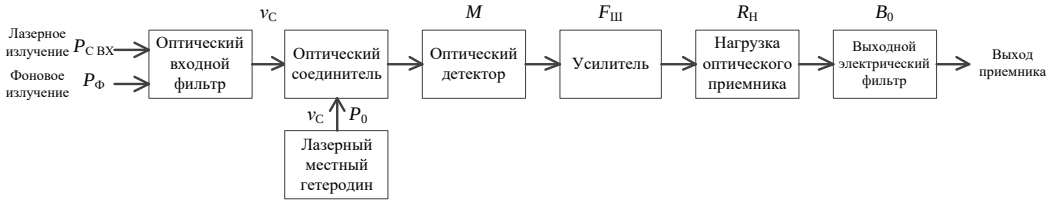


Рис. 3. Схема гомодинного приемника

ЭОСШ на выходе приемника определяется по формуле:

$$\text{ЭОСШ} = \frac{2\left(M\frac{\eta q}{h\nu_{\text{С}}}\right)^2 P_{\text{С ВХ}} P_0 R_{\text{Н}}}{qM^2 M^x B_0\left[\frac{\eta q}{h\nu_{\text{С}}}\left(P_{\text{С ВХ}}+P_0+P_{\Phi}\right)+I_{\text{Т}}\right]R_{\text{Н}}+\frac{2kTB_0F_{\text{Ш}}}{R_{\text{Н}}}}.$$

Сравнительный анализ схем детектирования оптического сигнала

Электрическое ОСШ определяется как отношение $P_{\text{С ВЫХ}}/P_{\text{Ш}}$, а оптическое ОСШ (ООСШ) – $P_{\text{С ВХ}}/P_{\Phi}$. В таблице приведены выражения для определения мощности полезного сигнала на выходе оптического приемника $P_{\text{С ВЫХ}}$, а также формулы расчета максимального ЭОСШ, когда тепловыми шумами оптического приемника можно пренебречь. Это соответствует упрощенной модели расчета ОСШ.

Мощность полезного сигнала и ЭОСШ на выходе фотодетектора

Параметр	Непосредственный прием	Когерентный прием	
		Гетеродинный	Гомодинный
$P_{\text{С ВЫХ}}$	$\left(MS_i\right)^2 P_{\text{С ВХ}}^2 R_{\text{Н}}$	$2\left(MS_i\right)^2 P_{\text{С ВХ}} P_0 R_{\text{Н}}$	$4\left(MS_i\right)^2 P_{\text{С ВХ}} P_0 R_{\text{Н}}$
ЭОСШ$_{max}$	$\frac{\eta P_{\text{С ВХ}}}{2h\nu_{\text{С}} M^x B}$	$\frac{\eta P_{\text{С ВХ}}}{h\nu_{\text{С}} M^x B}$	$\frac{2\eta P_{\text{С ВХ}}}{h\nu_{\text{С}} M^x B}$
ЭОСШ$_{max}$ с учетом ООСШ	$\frac{\eta}{2h\nu_{\text{С}} M^x B}\cdot\frac{P_{\text{С ВХ}}}{\left(1+\frac{1}{\text{ООСШ}}\right)}$	$\frac{\eta}{h\nu_{\text{С}} M^x B}\cdot\frac{P_0}{\left(1+\frac{1}{\text{ООСШ}}+\frac{P_0}{P_{\Phi}}\right)}$	$\frac{2\eta}{h\nu_{\text{С}} M^x B}\cdot\frac{P_0}{\left(1+\frac{1}{\text{ООСШ}}+\frac{P_0}{P_{\Phi}}\right)}$

Как видно из таблицы, гетеродинный прием обеспечивает выигрыш в 2 раза по сравнению с непосредственным приемом, а гомодинный – в 4 раза.

Моделирование в среде MathCad

В процессе моделирования использовались следующие исходные значения: ν_C = 200 ТГц, η = 0,6, $F_Ш$ = 5, $I_T = 1 \cdot 10^{-9}$ А. В качестве детектора применяется *p-i-n* фотодиод. Сопротивление нагрузки $R_Н$ определяется с учетом изменения полосы пропускания в зависимости от скорости передачи (за базовое принято значение B = 10 Гбит/с).

В результате получены зависимости ЭОСШ от скорости передачи, мощности поступающего на вход оптического детектора сигнала и мощности местного гетеродина. Графики приведены на рис. 4–6, где использованы следующие обозначения: 1 – непосредственный прием, 1* – непосредственный прием (упрощенная модель), 2 – гетеродинный прием, 3 – гомодинный прием.

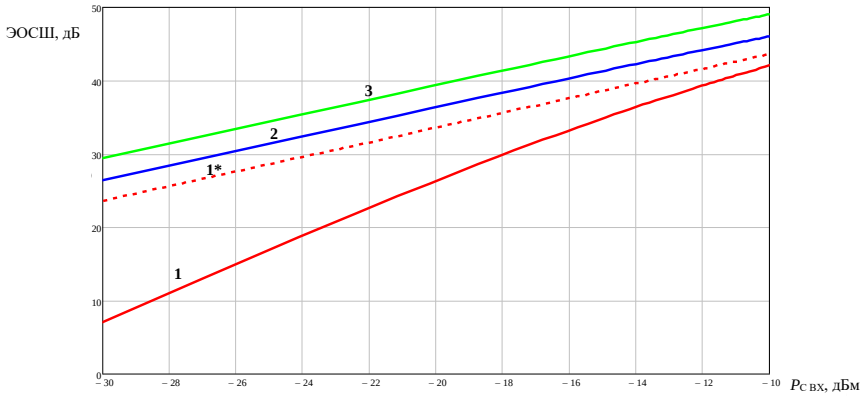


Рис. 4. Зависимость ЭОСШ от мощности сигнала на входе оптического приемника $P_{C\,ВХ}$

На основе результатов моделирования установлено, что для когерентных методов детектирования в инженерных расчетах можно использовать упрощенную модель расчета $ЭОСШ_{max}$, т. к. в рабочем диапазоне входных сигналов учет влияния всех источников шума ухудшает ОСШ не более чем на 0,5 дБ. Для непосредственного детектирования необходимо учитывать полный шум оптического приемника (отклонение значений упрощенной модели от значения ЭОСШ с учетом всех источников шумов составляет 3–15 дБ).

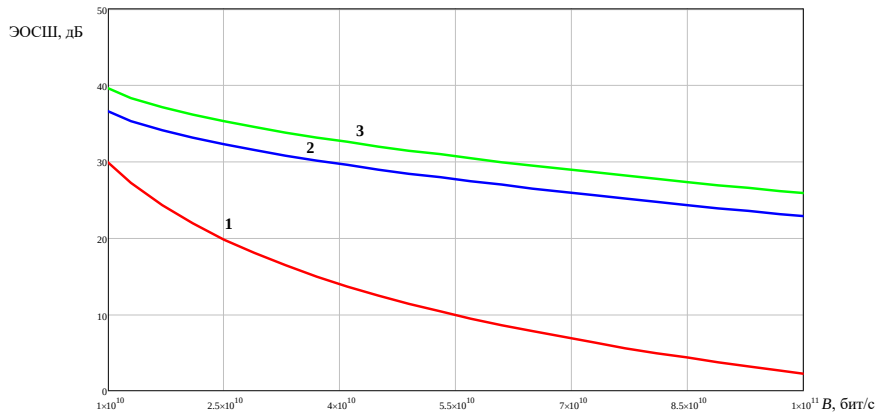


Рис. 5. Зависимость ЭОСШ от скорости передачи оптического сигнала B

Согласно рис. 5 видно, что выигрыш от использования когерентных методов приема увеличивается с ростом скорости передачи. При построении графика, представленного на рис. 6, мощность входного сигнала была принята равной –30 дБм. Из рисунка видно, что оптимально стоит выбирать мощность гетеродина, превышающую мощность сигнала на 18–20 дБ. Дальнейшее увеличение мощности гетеродина приводит к повышению ЭОСШ не более чем на 1 дБ при изменении мощности гетеродина на 5 дБ.

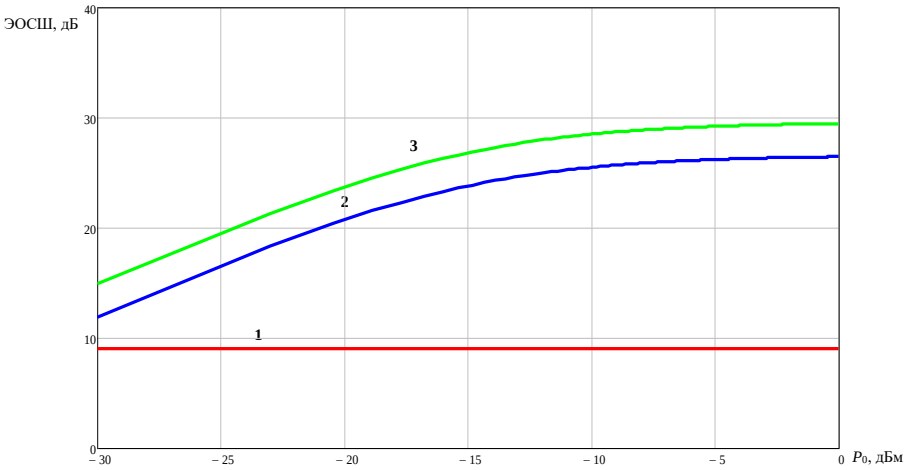


Рис. 6. Зависимость ЭОСШ от мощности сигнала гетеродина P_0

Заключение

Предложенные модели позволяют при проектировании цифровых ВОСП оценить параметры оптических приемников и выбрать наилучший метод приема, при котором обеспечиваются требуемое качество при максимальной чувствительности и максимальная протяженность участка регенерации в системах со спектральным разделением каналов.

COMPARATIVE ANALYSIS OF METHODS FOR CONSTRUCTING OPTICAL RECEIVERS IN DIGITAL FIBER-OPTIC TRANSMISSION SYSTEMS

N.V. TARCHENKO, Yu.S. MAISIYEVICH

Abstract

Mathematical models of optical receivers for digital signals have been developed, which allow to evaluate the signal-to-noise ratio at the output of such receivers (at the input of a decision-making device) and to determine the degree of influence on its value of such indicators as the level of the information signal, signal of a heterodyne and bandwidth of the optical receiver.

Keywords: fiber-optic transmission system, direct reception, coherent reception, heterodyne reception, homodyne reception, signal-to-noise ratio, optical receiver.

Список литературы

1. Фокин В.Г. Когерентные оптические сети. Новосибирск, 2015.
2. Леонов А.В., Наний О.Е., Слепцов М.А., Трещиков В.Н. // Прикладная фотоника. 2016. Т. 3, № 2. С. 123–145.
3. Гордиенко В.Н. Оптические телекоммуникационные системы. М., 2011.
4. Урядов В.Н. Волоконно-оптические системы передачи. Минск, 2008

UDC 004.42

DEVELOPMENT OF COMPUTER SOFTWARE AND TOOLS FOR ELECTRONIC DOCUMENT MANAGEMENT

I.I. ASTROVSKY, V.S. DANILCHUK, M.V. SOROKO, I.M. AL-RUBAI

Belarusian state university of informatics and radioelectronics, Republic of Belarus

Submitted 25 October 2018

Abstract. It is proposed to develop training computer programs and manuals for studying electronic document management tools. It is shown that the modern education system uses information technology and computer telecommunications, however, training on real equipment, as a rule, is unacceptable because of security threats. It is proposed to replace real hardware with virtual telecommunication devices and networks.

Keywords: electronic document management, telecommunication systems, security, virtualization, electronic manuals.

Introduction

At the present stage of development of computer and telecommunication technologies, each enterprise is already capable of having its own computer network both for internal communication and interaction, and for accessing the Internet and communicating with representatives of other enterprises, customers and charterers.

Recently, many enterprises and organizations are equipped with videoconferencing systems in connection with the advantages of this type of communications and reasonable costs for its organization. An electronic document can be used in all areas of activity where software and hardware are used to create, process, store, transmit and receive information. With the help of electronic documents, transactions and settlements can be made (contracts are concluded), correspondence and transfer of documents and other information are carried out. Electronic documents can be sent using any means of communication, including information systems and networks.

Information Security

Electronic document management systems have caused a number of problems, one of which is the security of data processing and transmission. The data transmitted in global telecommunication networks turned out to be especially “defenseless”. Currently, a large number of specialists in almost all economically developed countries of the world are working on the problem of the security of information transmitted over networks. It can be said that information security has been formed into a separate rapidly developing discipline. However, despite the efforts of numerous organizations involved in the protection of information, ensuring information security continues to be an extremely acute problem.

Certain difficulties are associated with changes in information processing and transmission technologies. On the one hand, the use of information technologies provides a number of obvious advantages: increasing the efficiency of management processes, processing and transmitting data, etc. It is no longer possible to imagine a large organization without the use of the latest information technologies, ranging from the automation of individual workplaces to the construction of corporate distributed information systems.

On the other hand, the development of networks, their complication, mutual integration, openness lead, to the emergence of qualitatively new threats, an increase in the number of intruders who have the potential to influence the system.

To ensure the protection of information, it is required not only the development of private protection mechanisms, but the implementation of a system approach that includes a set of interrelated measures (use of special technical and software tools, organizational measures, legal acts, moral and ethical countermeasures, etc.). The complex nature of the defense stems from the complex actions of intruders seeking by any means to obtain important information for them.

The complexity of the computer network requires additional special protection tools in addition to those available in standard network systems. To do this, it is necessary to study cryptographic security methods in telecommunication systems and security methods in existing web-server networks, develop of methods and algorithms for improving security in web-server networks. Regardless of the objects of management, it is desirable that the management system performs a number of functions that are defined by international standards, summarizing the experience of using control systems in various fields.

Specialist training

Training of specialists who are able to design and maintain these systems on the equipment of real-life networks, as a rule, is unacceptable for many reasons, and primarily because of the threat of violation of security policies. It is hard to forecast what might happen if a large number of students grant the rights of administrators to reveal passwords and allow experiments to be performed at their discretion on real equipment.

Therefore, the modern education system uses information technology and computer telecommunications. The system of distance education is especially dynamically developing, where electronic textbooks are widely used. The advantages of these textbooks are follow. Firstly, work on virtual devices and systems that are not related to real hardware, which reduces the cost and makes the learning process completely safe. Secondly, accessibility due to the presence of computers and software, which allow to model complex systems with functionality close to the capabilities of real systems. Thirdly, the adequacy of the level of development of modern scientific knowledge. Fourthly, a computer program can train, control, assist and evaluate learning. On the other hand, the creation of electronic textbooks contributes to the solution of such problems as the constant updating of information material, exercises and examples. In addition, with the help of electronic textbooks and programs, effective training and knowledge control, computer testing, is carried out.

Conclusion

The theoretical part of the electronic manual developed by the authors contains a large number of examples, figures, diagrams. All material is divided into small sections and subsections, which greatly facilitates the perception and contributes to a better assimilation of information.

Testing includes only those questions whose answers can be found in the electronic textbook. If there are errors, the user can analyze them, since the program provides the ability to view all erroneously performed tasks and suggests ways to find the correct answers. If necessary, the student has the opportunity to re-take the test.

Bibliography

1. Konopelko V.K., Tsvetkov V.Yu, Astrovsky I.I. // Education Quality Management: Experience, Problems and Perspectives: Proc. X intercollegiate conference. Minsk, 2010. p. 230
2. Shangin V.F. Protection of information in computer systems and networks M., 2012.

UDC 621.392

APPLICATION OF FUZZY LOGIC TECHNIQUE IN MEDICINE

AL SABEEH AMJAD KARIM, NGUEN HONG KUAN, M.Yu. HOMENOK

Belarusian state university of informatics and radioelectronics, Republic of Belarus

Submitted 1 November 2018

Abstract. The article presents a brief analysis of three areas of using of fuzzy logic technology in medicine: the fuzzy logic for making decisions in medical diagnostics based on a fuzzy expert system, a fuzzy inference system for remote monitoring of vital functions and a healthcare system for individual physiological monitoring using a wireless body network with a routing algorithm based on the fuzzy logic.

Keywords: fuzzy logic, fuzzy expert systems, making decision, healthcare system, medical diagnosis, wearable sensor, routing algorithm, wireless body area network.

Introduction

Fuzzy set theory and fuzzy logic have a number of characteristics that make them highly suitable for modelling uncertain information upon which medical concept forming, patient state interpretation and diagnostic as well as therapeutic making decision is usually based. Firstly, medical entities such as symptoms, signs, test results, diseases and diagnoses, therapeutic and prognostic information can be defined as fuzzy sets. The inherent vagueness of these entities will thus be conserved. Secondly, fuzzy logic offers reasoning methods capable of drawing strict as well as approximate inferences. Medicine demands this broad range of possibilities because the body of medical theory includes definitional, causal, statistical, and heuristic knowledge. Practical medicine even has to accept incomplete medical theories where only vague and uncertain empirical information guides the necessary medical procedures. Finally, fuzzy automata may be used as high level patient monitoring devices with real time access to medical information systems.

A Fuzzy logic system (FLS) is mainly comprised of four components: fuzzifier, defuzzifier, fuzzy rule base and fuzzy inference engine. These components are arranged as follows in any Fuzzy Logic System.

Fuzzification is the first process that takes place in the FLS. A numeric or crisp input value is given to the fuzzifier. The crisp input value is required to be converted to the corresponding fuzzy value as the rules for determining the result, are defined for fuzzy inputs. This task is performed by the fuzzifier and then the fuzzy input values are supplied to the fuzzy inference engine, which is responsible for computing the set of outputs based on the IF-THEN rules defined in the fuzzy rule base.

Usually, when more than one inputs are required, AND operator is used to combine them. The last process in the FLS is defuzzification. It coverts the fuzzy output values into their corresponding crisp values. There are different methods for fuzzification and defuzzification. Some widely used fuzzifiers are singleton fuzzifier, gaussian fuzzifier and trapezoidal or triangle fuzzifier. Singleton fuzzifier is the simplest fuzzifier which basically assigns a precise value to the given input and hence no fuzziness is introduced by fuzzification in this case. Gaussian and triangular fuzzifiers are used to suppress the noise in the given inputs. Examples of defuzzifiers are maximum defuzzifier, mean of maxima defuzzifier, centroid defuzzifier, height defuzzifier, modified height defuzzifier, center of sets and center of sums.

The advantages of fuzzy logic are its simplicity, flexibility of combining conventional control techniques, ability to model nonlinear functions and imprecise information, use of empirical knowledge

and dependency on heuristics. Due to the basic characteristics of ad hoc networks like uncertainty due to dynamic topology and mobility of nodes, limited resources and unstable links; a precise and accurate model is not possible to implement. In such an environment, fuzzy logic theory has been proved a good approach for routing compared to other routing methods. Fuzzy logic can be used to solve the problem of routing in ad hoc networks where the final outcome is based on the factors with uncertainty.

The fuzzy logic for making decisions in medical diagnostics based on a fuzzy expert system

Clinical decision support systems (CDSS) are broadly classified into two main groups (Fig. 1): knowledge based CDSS, non-knowledge based CDSS.

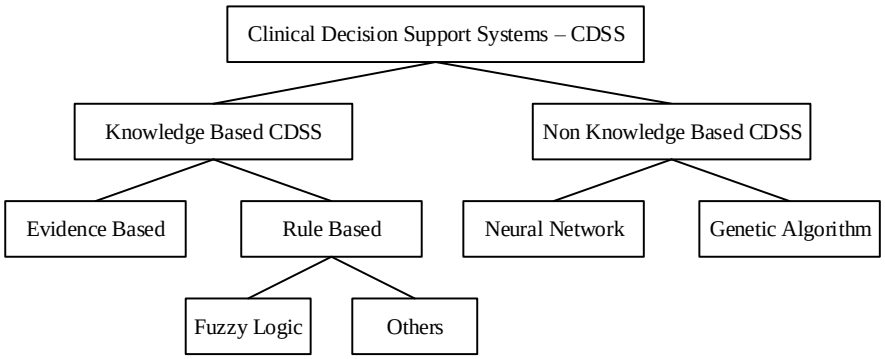


Fig. 1. Types of clinical decision support systems

The knowledge based clinical decision support system contains rules mostly in the form of IF/THEN statements. The data is usually associated with these rules. For example, if the pain intensity is up to a certain level then generate warning. The knowledge based generally consists of three main parts: knowledge base, inference rules and a mechanism to communicate. Knowledge base contains the rules, inference engine combines rules with the patient data and the communication mechanism is used to show the result to the users as well as to provide input to the system.

Rule-based systems and evidence based systems tend to capture the knowledge of domain experts into expressions that can be evaluated as rules. When a large number of rules have been compiled into a rule base, the working knowledge will be evaluated against rule base by combining rules until a conclusion is obtained. It is helpful for storing a large amount of data and information. However it is difficult for an expert to transfer their knowledge into distinct rules. CDSS without a knowledge base are called as nonknowledge based CDSS. These systems instead used a form of artificial intelligence called as machine learning. Non-knowledge based CDSS are then further divided into two main categories: neural network and genetic algorithms.

To derive relationship between the symptoms and diagnosis, neural networks use the nodes and weighted connections. This fulfills doesn't need to write rules for input. However, the system fails to explain the reason for using the data in a particular way. So its reliability and accountability can be a reason. Genetic algorithms are based on evolutionary process. Selection algorithm evaluates components of solutions to a problem. Solution that comes on top are recombined and the process that runs again until a proper solution is observed. The generic system goes through an iterative procedure to produce the purpose the best solution of a problem.

Diagnostic systems are used to monitor the behavior of a process and identify certain pre-defined patterns that associate with well-known problems. These problems, once identified, imply suggestions for specific treatment. Most diagnostic systems are in the form of a rule-based expert system: a set of rules is used to describe certain patterns. Observed data are collected and used to evaluate these rules. If the rules are logically satisfied, the pattern is identified, and a problem associated with that pattern is suggested. Each particular problem might imply a specific treatment.

Most current health monitoring systems only check the body's temperature, blood pressure, and heart rate against individual upper and lower limits and start an audible alarm should each signal move out of its predefined range (either above the upper limit or below the lower limit). Then, human experts will have to examine the patient and probe the patient's body further for additional data that lead to proper diagnosis and its corresponding treatment.

Other more complicated systems normally involve more sensors that provide more data but still follow the same pattern of independently checking individual sets of data against some upper and lower limits. The warning alarm from these systems only carries a meaning that there is something wrong with the patient.

In a life threatening situation, reducing the time between the warning and the time proper treatment is given to the patient by preparing proper equipment for specific treatment in advance would significantly increase the patient's chance of surviving.

The term «medical knowledge» is a superimposed concept for the relationships between symptoms and diagnoses a physician may find in books, journals, monographs, but also in practical experience. Fuzzy logic and neural networks are complementary technologies and when brought together can provide intelligent systems. Neuro-fuzzy model incorporates the generic advantages of artificial neural networks in modeling imprecise data and qualitative knowledge as well as transmission of uncertainty. Researchers used the neuro-fuzzy approaches to build more intelligent decision making systems and presented the applications and supportive tools for the physicians.

The Adaptive neuro-fuzzy inference system (ANFIS) is a simple data learning technique that uses fuzzy logic to transform given inputs into a desired output with the help of highly interconnected Neural Network processing elements and information connections, which are weighted to map the numerical inputs into an output. ANFIS combines the benefits of the two machine learning techniques (fuzzy logic and neural network) into a single technique.

The ANFIS system training process begins by obtaining a training data set (input/output data pairs) and testing data sets. Two vectors are used to train the ANFIS system: input and output. The training data is a set of input and output vectors. It is used to find the premise parameters for the membership functions. A threshold value for the error between the actual and desired output is determined. The consequent parameters are found using the least squares method. If this error is larger than the threshold value, then the premise parameters are updated using the gradient decent method. The process is terminated if the error is less than the threshold value. ANFIS training learning rules use hybrid learning, combining the gradient descent and the least squares method. Aim of using ANFIS for health monitoring is to achieve the best performance possible. ANFIS training begins by creating a set of suitable training data in order to be able to train the neuro-fuzzy system.

A fuzzy inference system for remote monitoring of vital functions

The wearable wireless sensor network is applied to monitor the physiological information (heart rate, blood oxygen, breath, blood pressure, body temperature, etc.) and movement information (the speed, gait, trajectory, and the consumption of energy in the sport) of human body and the external environment (temperature, humidity, gas composition, location) dynamically and continuously for a long time.

To improve clinician performance, fuzzy logic-based expert systems have shown potential for imitating human thought processes in the complex circumstances of clinical decision. A key advantage of using fuzzy logic in such situations is that the fuzzy rules can be programmed easily, and as a result they are easily understood by clinicians. It is different from neural networks and other regression approaches, where the system behaves more like a black box to clinicians. Here fuzzy logic holds great promise for increasing efficiency and reliability in health care delivery situations requiring decisions based on vital signs information.

Fuzzy logic control system is capable of generating accurate result from approximate, insufficient or vague information. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may rage between completely true or completely false.

The expert system must check for combinations of data instead of individual data and for example a fuzzy rule-based expert health monitoring system with three basic sensors: body temperature, heart rate, and blood pressure will identify twenty-seven different scenarios instead of three in the conventional system.

Fig. 2 shows the block diagram of health condition using fuzzy logic system to interpret the results of the most commonly used medical measurements: blood pressure and temperature.

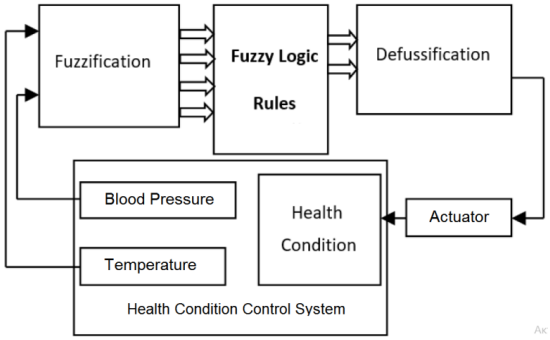


Fig. 2. Block diagram of health condition using fuzzy logic system

Fuzzification process for two variables need two separate fuzzifiers. Each fuzzifier consists of input BP value to crisp value, operation region of a crisp value detector, fuzzy set membership function value and selection arrangement. The design of fuzzifier is shown in Fig. 3.

An inference engine is a component of the system that applies logical rules to the knowledge base to deduce new information. For Fig. 3 the system's inference engine accepts four inputs from fuzzifier and applies the MIN-MAX composition to attain the output R values. Fig. 4 shows this type of inference process where the MIN-MAX inference method uses MIN-AND operation among the four inputs.

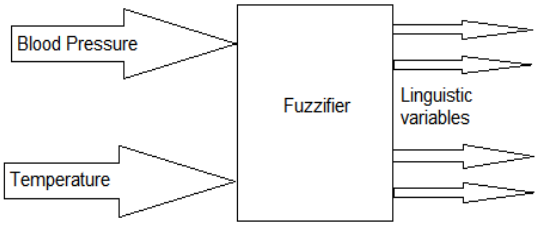


Fig. 3. Fuzzifier block

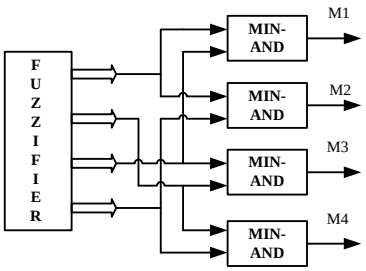


Fig. 4. Block diagram of min-max inference engine

Number of active rules = a^b, where a is maximum number of overlapped fuzzy sets and b is number of inputs. For example if $a = 5$ and $b = 2$, so the total number of active rules are 25.The total number of rules is equal to the product of number of functions accompanied by the input variables in their working range.

A healthcare system for individual physiological monitoring using a wireless body network with a routing algorithm based on the fuzzy logic

Focus on the wearable wireless sensor network among bodies, the wearable sensor node which is placed on the mobile human bodies constitutes the sensor network, the network topology of which changes fiercely (Fig. 5).

The wearable wireless sensor network which is applied in the individual physiological information monitoring is currently in the continuous research. And because the mobility of the human body is bigger and the topology changes dramatically, these require that sensor nodes transmit data in real time with high reliability and the energy of the nodes consumes balance which can prolong the network life. Therefore, new requirements for traditional wireless sensor network routing protocol are put forward.

The typical protocol of wireless sensor network mostly takes into account single performance. Many papers make improvement for these protocols: some take into account reducing the time delay performance and some take into account the energy utilization performance to make the network balance. All of them rarely involve the multiobjective optimization problem. Which are important for the application of the wireless sensor network in the wearable field.

The wireless sensor network (WSN) uses the CTP routing protocol (Collection tree protocol) to communicate between the sink node and sensor nodes. In order to guarantee the safety of communication, communication between the sensor nodes can be encrypted. The sensor node

transmits its data or others nodes' data to the sink node by multihops transmission. The sink node collects all the data and then uploads them to a central data receiving control platform.

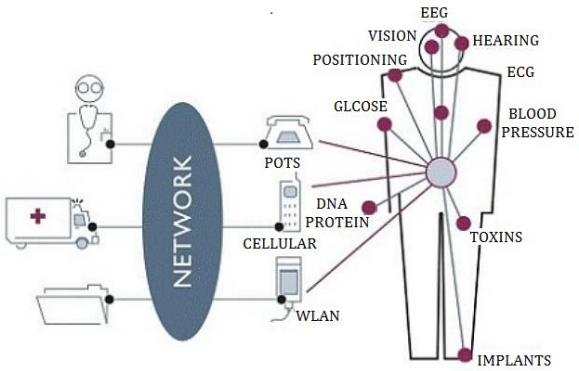


Fig. 5. Remote system for individual physiological monitoring of vital signs

Collection tree protocol is an aggregation protocol based on tree structure and sensor node delivery data to the sink node by unicast multihop. CTP uses the *ETX* value as the routing gradient (expected transmission count), and the *ETX* value of sink node is 0, the *ETX* of the other nodes is the *ETX* of its parent node plus the *ETX* of its parent link. The calculation of *ETX* is formulas (1) and (2). In formula (1), data_total represents the total packet delivered between two sensor nodes, and data_success represents the packet delivered successfully between two sensor nodes. In formula (2), EXT_{parent} presents *ETX* value of parent node, and $EXT_{linkparent}$ presents *ETX* value of parent link:

$$ETX = 10\,[\text{data\_total}/\text{data\_success} - 1] \tag{1}$$

$$EXT_{node} = EXT_{parent} + EXT_{linkparent} \tag{2}$$

Where EXT_{node} presents the *ETX* value of sensor node in wireless sensor network, when the nodes choose the path, they choose the path with the smallest *ETX* as the routing path. Formulas above show that when the sensor node chooses the next hop CTP only considers the packet transmission success rate, which is the reliability performance that we are concerned with.

For the requirements of the wearable wireless sensor network that is applied in the field of individual physiological monitoring, authors propose a routing selection algorithm based on the fuzzy logic to improve the CTP protocol. The basic idea of routing on fuzzy logic is calculating a reasonable value by fuzzy logic taking into account three parameters: reliability, time delay, and energy to replace the original *ETX* value.

The routing algorithm can be divided into three phases. The first phase is defining the input and output parameters, respectively, and choosing the membership functions which use the language set to express the parameters. Then, it is necessary to fuse the language information using fuzzy rules and get the evaluation results of candidate parent node. At last, it is necessary to defuse the evaluation results by center of gravity method and choose the best path.

The transmission model of the wireless networks and the coverage range mission region are shown in figure 6, where *A*, *B*, *C* and *D* are *A* neighbors which organize a neighbor node set.

Fuzzy logic algorithm includes three input and one output parameters. The first input parameter is a reliability $R(A, B)$ which calculates the probability of packets that are successfully transmitted between two sensor nodes A and B according to expression: $R(A,B)=n/m$, where m is the number packets to B from A with a certain time, and the number of packets B successfully received is n. The second input parameter is time delay T which calculates the average time delay that B successfully receives packets from A. Let the send time series is $\{T_1, T_2,..., T_{m-1}, T_m\}$ (the send time of m packet) and the receiving time series is $\{T^*_1, T^*_2,..., T^*_m\}$ (the receiving time of n packet), ignoring the lost package then $T(A,B) = \sum_i (T_i^* - T_i)$.

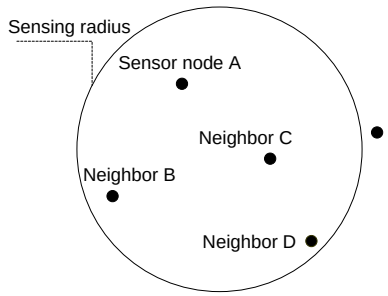


Fig. 6. The transmission model for the sensor networks

Third input parameter is energy parameter E which calculates the proportion of residual energy of one node accounted for the largest energy. Assume that E_r represents the residual energy of B and $E_{\max}$ represents the largest energy among the neighbor nodes then $E=E_r/E_{\max}$.

The fuzzy rules are composed of a series of fuzzy conditional statements in IF/THEN type. Part of the fuzzy rules are shown in Table.

Fuzzy rules

Rule	Reliability	Delay	Energy	Output
1	High	Small	Enough	Perfect
2	High	Small	General	Good
3	High	Small	Few	Acceptable
4	High	Medium	Enough	Good
5	High	Medium	General	Acceptable
6	High	Medium	Few	Unperfected
7	High	Large	Enough	Acceptable
8	High	Large	General	Unperfected
9	High	Large	Few	Bad

Center of gravity (COG) method may be used to defuzzify the fuzzy result. Since the fuzzy logic can reconcile conflicting objectives, this step can provide a quick ranking of multiple candidates (neighbor nodes). Each node maintains a routing table using the IF/THEN criterion. Forms of typical triangular membership functions of input and output variables are shown in Fig. 7–10: three for the input variables and six for output variable.

The presented analysis of the algorithm for choosing the optimal route based on fuzzy logic requires further execution of computer simulation and experimental verification taking into account the actual network topology and its comparison with the classical CTP routing protocol.

A Wireless sensor network is a special network that requires adaptive methods and techniques to meet the application requirements. Optimizing the energy consumption and enhancing the network lifetime while routing data from sensor nodes to the base station is the subject of extensive research works.

So the evaluation should be performed not only for energy efficient cluster-based routing protocol that uses a fuzzy logic module during the cluster-head election process but to increase the network lifetime. The objective of this research could be not to minimize the whole network consumption, but to balance the consumption over nodes to increase the network lifetime.

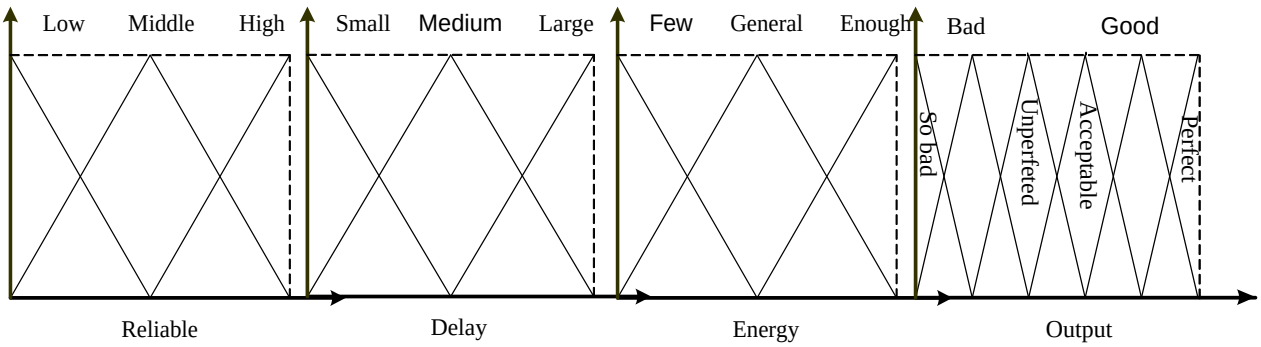


Fig. 7. The membership functions of R

Fig. 8. The membership functions of T

Fig. 9. The membership functions of E

Fig. 10. The membership functions of output

Conclusion

The performed analysis of the use of the laws of thinking, invented by the creator, confirms their effectiveness for developing decision-making devices under uncertainty, although the construction of the surrounding world is carried out in accordance with the laws of clear logic. Virtually any control system can be replaced by a fuzzy logic control system with making decision based on a fuzzy inference system with or without a feedback loop. As result the theory of fuzzy logic is used in many applications, such as artificial intelligence, pattern recognition, control of unmanned military vehicles, and in knowledge-based systems such as weather forecasting, stock trading, traffic control, and medical diagnostics.

With regard to medicine, fuzzy logic is the basis for the development of such systems as the interpretation of medical data, the differentiation of the syndrome and the diagnosis of diseases, the optimal choice of treatment and real-time monitoring of patient data. Modern technologies based on fuzzy expert systems and wearable wireless body sensor networks have potential to tender a wide range of assistance to patients, medical personnel, and society through continuous monitoring in the ambulatory environment, early detection of abnormal conditions, supervised restoration and potential knowledge discovery through data mining of all gathered information.

References

1. Fuzzy Set Theory and Fuzzy Logic in Medicine. Klaus-Peter Adlassnig [Electronic resource]. URL: https://www.meduniwien.ac.at/kpa/publications/EUFIT_1999_Fuzzy_Set_Theory_and_Fuzzy_Logic_in_Medicine.pdf (date of access: 01.11.2018).
2. Fuzzy Expert System for Medical Diagnosis. Varinder Pabbi. [Electronic resource]. URL: https://pdfs.semanticscholar.org/4993/34f7af018ef9ccee5caab684d8e3a38416f2.pdf?_ga=2.74302231.426016097.1542122771-1088071245.1542122771 (date of access: 01.11.2018).
3. Human Blood Pressure and Body Temp Analysis Using Fuzzy Logic Control System. Syeda Binish Zahra, Talmeez Hussain, Ayesha Atta, M. Saleem Khan. [Electronic resource]. URL: http://paper.ijcsns.org/07_book/201712/20171232.pdf (date of access: 01.11.2018).
4. The Routing Algorithm Based on Fuzzy Logic Applied to the Individual Physiological Monitoring Wearable Wireless Sensor Network. Jie Jiang, Yun Liu, Fuxing Song, Ronghao Du, and Mengsen Huang. [Electronic resource]. URL: https://www.hindawi.com/journals/jece/2015/546425/ (date of access: 01.11.2018).

УДК 621.391

ПОИСК ЛОКАЛЬНЫХ ЭКСТРЕМУМОВ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ЦЕНТРАЛЬНО-СИММЕТРИЧНОГО СКАНИРОВАНИЯ

А.Т. НГУЕН, В.Ю. ЦВЕТКОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 18 ноября 2018

Аннотация. Предложен алгоритм поиска однопиксельных экстремумов полутоновых изображений на основе центрально-симметричного сканирования. Показано, что алгоритм работает значительно быстрее, чем лучшие известные алгоритмы обнаружения ключевых точек изображений.

Ключевые слова: поиск локальных экстремумов, центрально-симметричное сканирование.

Введение

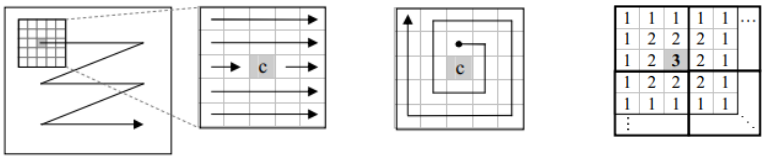
Поиск локальных экстремумов является базовой операцией для множества задач обработки изображений. Известен алгоритм NMS (Non-maximum Suppression – подавление немаксимальных значений), который первоначально использовался для уменьшения длительности откликов при детектировании тонких линий [1]. Алгоритм NMS является одномерным (1-D) и работает перпендикулярно к краям. В работе [2] предложен способ модификации алгоритма NMS для определения ключевых точек (реперов) изображения в двухмерном пространстве пикселей изображения (2-D). Ключевые точки выбираются как локальные максимумы изображения над некоторой окрестностью. Этот подход к обнаружению углов был принят многими детекторами ключевых точек [3–5]. При исследовании эффективности поиска локальных экстремумов берется ориентир на алгоритмы, требующие минимального использования памяти.

Известные алгоритмы NMS требуют фиксированного количества сравнений на пиксель независимо от размера окрестности исключения. Одномерный максимальный фильтр, например, требует трех сравнений на пиксель [6–8]. При последовательной реализации двухмерный максимальный фильтр использует шесть сравнений на пиксель. В работе [9], опубликованной в 2006 году, предложен алгоритм разбиения блоков, который уменьшает количество сравнений до 2,39 на пиксель. Однако, 20-ю годами ранее, в работе [10] предложен алгоритм, имеющий аналогичную вычислительную сложность. В любом случае для большинства известных алгоритмов поиска локальных экстремумов необходимо выполнять более двух сравнений на пиксель. В работе [1] модифицированы алгоритмы, предложенные в [9, 10] с целью уменьшения количества сравнений на пиксель до значения менее двух.

Алгоритмы поиска локальных экстремумов на изображениях

Прямой подход к поиску экстремумов в двухмерном массиве представлен на рис. 1, *а*. Пиксели исходного изображения анализируются в порядке растрового сканирования (слева направо, затем сверху вниз). Каждый анализируемый пиксель сравнивается с другими пикселями в своей окрестности размером 5×5 пикселей также в порядке растрового сканирования [9]. Центральный пиксель C не является максимальным, если найден любой более значимый или равный соседний пиксель. Затем алгоритм переходит к следующему пикселю в строке сканирования. Прямой подход требует $(2n+1)\times(2n+1)/2$ сравнений на пиксель для $(2n+1)\times(2n+1)$-окрестности. Наилучшему варианту сооветствует ситуация, когда вектор

интенсивности меняется на противоположный. При этом прямой подход требует только одного сравнения на пиксель. В среднем, однако, данный подход требует $O(n)$ сравнений на пиксель.



а *б* *в*

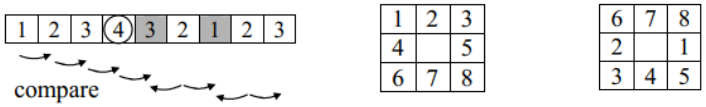
Рис. 1. Представление способов сканирования изображений: *а* – растровое сканирование; *б* – спиральное сканирование; *в* – Block partitioning

Сложность алгоритма растрового сканирования может быть значительно уменьшена путем анализа соседних пикселей в другом порядке. В работе [10] представлен такой алгоритм с локальным спиральным порядком (рис. 1, *б*). Сначала, в результате сравнения, центральный пиксель, возможно, будет локальным максимумом в 3×3-окрестности. Затем он проверяется в большей окрестности. Так как количество локальных максимумов в 3×3-окрестности в изображении обычно невелико (≤ 25 % от общего количества пикселей), алгоритм спирального порядка быстро находит любые немаксимальные значения, пропускает их и переходит на следующий пиксель. Число локальных максимумов в окрестности с размером $(2n+1)\times(2n+1)$ пикселей также быстро уменьшается, поскольку размер окрестности увеличивается. В результате вычислительная сложность этого алгоритма примерно постоянна (не более 5 сравнений на пиксель для обнаружения в 3×3-окрестности немаксимальных пикселов) независимо от размера окрестности.

В работе [9] представлен эффективный алгоритм NMS, который требует 2,39 сравнений на пиксель в среднем и 4 сравнения на пиксель в худшем случае. Они отметили, что максимальный пиксель в окрестности размером $(2n+1)\times(2n+1)$ пикселя также является максимальным для любого окна размером $(n+1)\times(n+1)$ пикселей. Входное изображение разбивается на неперекрывающиеся блоки размера $(n+1)\times(n+1)$ пикселей и локальный максимум каждого блока детектируется (рис. 1, *в* иллюстрирует это для $n=2$). Затем для максимального размера блока $(2n+1)\times(2n+1)$ пикселей за исключением охватывающего блока $(n+1)\times(n+1)$ пикселей. Используя только одно сравнение на пиксель, шаг разбиения блока уменьшает количество локальных максимумов с фактором $(n+1)\times(n+1)$. В результате метод достаточно эффективен для больших размеров окрестностей. Решение уменьшить количество дополнительных сравнений на одного кандидата до $2+O(1/n)$, значительно увеличивает сложность алгоритма и использование памяти.

Метод NMS для окрестности 3×3 пикселей часто решается с помощью математической морфологии [11, 12], в результате чего входное изображение сравнивается с его дилатацией серого цвета. Пиксели, где два изображения равны, соответствуют локальным максимумам. Однако математическая морфология не возвращает строгие локальные максимумы, где центральный пиксель строго больше, чем все соседние пиксели. С точки зрения вычислительной сложности морфология также неэффективна – реализация дилатации для 3×3-окрестности полутонового изображения требует шести сравнений на пиксель [6, 7].

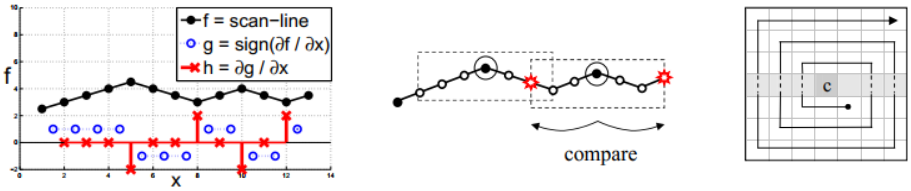
В [13] предложен алгоритм 3×3 сканирующей линии для NMS, который требует не более 2 сравнений на пиксель. Алгоритм сначала ищет одномерные локальные максимумы вдоль линии сканирования. Затем каждый максимальный уровень сканирования сравнивается с соседними пикселями в соседних строках. Две двоичные маски сохраняются для текущей и следующей строк сканирования в буфере. По мере обработки нового центрального пикселя соседние ему пиксели маскируются, если они меньше центрального пикселя. Маскированные пиксели будут пропущены, когда наступит их очередь обработки (рис. 2). В результате этот алгоритм NMS для окрестности 3×3 пикселей требует не более двух сравнений на пиксель.



а *б* *в*

Рис. 2. Маски сканирующей линии 3×3 – окрестности: *а* – 1-D Non-maximum Suppression [13]; *б* – растровое сканирование; *в* – Scan-line [13]

Алгоритм сканирующей линии для 3×3 -окрестности может быть расширен до блоков $(2n+1)\times(2n+1)$ пикселей при $n\geq1$ [13]. Предположим, что максимумы $(2n+1)$-окрестности на текущей линии сканирования расположены так, как показано на рис. 3, *б* (пиксели в окружностях). Эти 1-D максимумы служат кандидатами на двумерные максимумы. Каждый кандидат проверяется на экстремум в $(2n+1)\times(2n+1)$-окрестности в спиральном порядке, аналогичном методу Forstner [10]. При этом соседние пиксели, расположенные на одной линии сканирования, уже были сопоставлены и потому могут быть пропущены (серые пиксели на рис. 3, *в*). Это приводит к тому, что максимум для $2n\times(2n+1)$-соседей сравнивается с каждым кандидатом. В результате среднее количество сравнений на один кандидат намного меньше благодаря порядку перемещения по спирали.



а *б* *в*

Рис. 3. Сканирующий алгоритм NMS для $(2n+1)\times(2n+1)$-окрестности ($n=3$): *а* – 1-D обнаружение пиков; *б* – 1-D исключение не-максимумов; *в* – спиральное сканирование

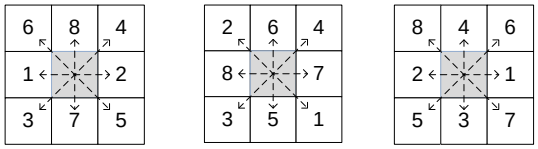
Обнаружение максимумов в $(2n+1)$ – окрестности на одномерной сканирующей линии функции f подробно показано на рис.3 а. Если g – знак конечной разности функции f, значение g равно либо –1, 0 или 1 в зависимости от локального наклона f. Следовательно, гонечная разность h, равна –2 на локальных пиках, +2 в локальных желобах и 0 в другом месте. Таким образом, для обнаружения 1-D пика и минимума требуется только одно сравнение на пиксель. Затем каждый 1-D экстремум сравнивается с его участком в $(2n+1)$ – окрестности со знанием экстремума детектора h. Соседние пиксели, которые находятся на последовательном склоне вниз от локального пика, т. е. $\{x\,|\,h(x)=0\}$, по определению меньше, чем текущий пик, поэтому их не нужно повторно сравнивать. Пиксели, расположенные вне закрывающих впадин текущего пика, требуются дополнительного сравнения. Число дополнительных сравнений для получения максимумов $(2n+1)$-окрестности из исходного списка максимумов 3×3-окрестности очень мало для гладкой функции f.

Недостатками рассмотренных выше алгоритмов являются низкая скорость поиска, наличие ошибок обнаружения экстремумов на границах блоков изображения, пропуск локальных минимумов. В этой связи актуальной является задача поиска всех локальные однопиксельных экстремумов (как максимумов, так и минимумов) на изображении с низкой вычислительной сложностью без использования дополнительной памяти. Предлагаемый алгоритм позволяет быстро найти все локальные однопиксельные экстремумы.

Алгоритм поиска локальных экстремумов полутоновых изображений

Для поиска на изображении однопиксельных экстремумов предлагается алгоритм на основе центрально-симметричного сканирования (SSEF – SymmetricScan-based Extreme Finding). Сущность алгоритма состоит в выборе пикселей изображения в порядке строчной развертки, оценке распределения яркости в окрестностях размером 3×3 пикселей, фиксировании центрального пикселя в качестве экстремума, если все пиксели в его окрестности

имеют меньшие или большие значения. Предлагаемый алгоритм отличается от известных алгоритмов поиска однопиксельных экстремумов порядком выборки пикселей в окрестности анализируемого на экстремум пикселя, который осуществляется центрально-симметрично – поочередно с различных направлений относительно центра области анализа (рис. 4). Центральный пиксель *C* не является максимальным, если найден любой более значимый или равный ему пиксель. Немаксимальный пиксел затем передается на этап поиска локальных минимумов. Если найден любой менее значимый или равный пиксель, то центральный пиксель *C* также не является минимальным и алгоритм переходит на следующий пиксель по порядку сканирования изображения. Процедура поиска продолжается до тех пор, пока все пиксели не будут обработаны.



а *б* *в*

Рис. 4. Виды центрально-симметричной окрестности размером 3×3 пикселя

Алгоритм поиска состоит из следующих шагов

1. Инициализация. На данном шаге осуществляется буферизация исходного изображения $I=\|i(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ размером *YX* пикселей. Формируется матрица разметки экстремумов $E=\|e(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$, элементы которой определяются с помощью выражений $e(y,x)\leftarrow1$ при $y=\overline{0,Y-1},\ x=\overline{0,X-1}$.

Формирование вектора индексов центрально-симметричного сканирования с помощью выражения $RC=\|rc(k)\|_{(k=\overline{0,7})}$, элементы которого определяются следующим образом: $rc(k)\leftarrow[0\ -1;\ 0\ \ 1;\ 1\ -1;-1\ \ 1;\ 1\ \ 1;-1\ -1;-1\ \ 0]$ при $k=\overline{0,7}$ (рис.4 а).

2. Начало цикла поиска локальных однопиксельных экстремумов

2.1. Поиск локальных однопиксельных максимумов. Осуществляется формирование матрицы разметки значений максимумов $E=\|e(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ с помощью выражения

$$\forall(e(y,x)=1)\Rightarrow$$
$$\Rightarrow e(y,x)=\begin{cases}0\ \text{ при }\exists k(k\in[0,7])(i(y+rc(k,1),x+rc(k,2))\le i(y,x))\\1\ \text{иначе (есть местоположение максимумов)}\end{cases}\qquad(1)$$

при $y=\overline{0,Y-1},\ x=\overline{0,X-1}$.

2.2. Поиск локальных однопиксельных минимумов. Осуществляется формирование матрицы разметки значений минимумов $E=\|e(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ с помощью выражения

$$\forall(e(y,x)=0)\Rightarrow$$
$$\Rightarrow e(y,x)=\begin{cases}2\text{ при }\exists k(k\in[0,7])(i(y+rc(k,1),x+rc(k,2))\ge i(y,x))\\0\ \text{иначе (есть местоположение минимумов)}\end{cases}\qquad(2)$$

при $y=\overline{0,Y-1},\ x=\overline{0,X-1}$

2.3. Проверка условия окончания цикла: $y\le Y$ и $x\le X$. Если выполняется условие, то осуществляется переход к шагу 2.1. Если это условие не выполняется, то осуществляется выход из алгоритма.

Вычислительная сложность алгоритма определяется числом вещественных операций сложения (алгоритм имеет нулевую вычислительную сложность умножения) с помощью выражения

$$A_{\text{слж}}=2\times CPP\times Y\times X.\qquad(3)$$

где CPP – число сравнений на пиксель (Comparisons Per Pixel), Y, X – размеры исходного изображения.

В результате выполнения данного алгоритма формируется матрица разметки локальных экстремумов, значение каждого элемента которой указывает на экстремум изображения (значение 1 – максимум, значение 0 – минимум), которому принадлежит пиксель разметки изображения с соответствующими координатами. Эти данные используются для последующей обработки изображений.

Оценка эффективности алгоритма поиска локальных экстремумов на основе центрально-симметричного сканирования

Выполнено сравнение предложенного алгоритма с некоторыми известными алгоритмами, описанными в среде Matlab и Matlab ®Image Processing Toolbox (R2015a): imdilate и imerode, которые использовались для реализации морфологии [11, 12]. Для этого эксперимента были выбраны три изображения размером 512×512 пикселей: Lena, Barbara и Airfield (рис. 5).

а *б* *в*

Рис.5. Тестовые полутоновые изображения: *а* – «Lena»; *б* – «Barbara»; *в* – «Airfield»

В таблице приведены значения экстремумов, экспериментально установленные для трех полутоновых изображений различных типов (Lena – студийное низкочастоное с размером 512×512 пикселей с преобладанием участков с плавным изменением яркости; Barbara – студийное высокочастотное с размером 512×512 пикселей с преобладанием участков с резким измениением яркости; Airfield – аэроизображение с размером 512×512 пикселей), значения времени поиска и числа сравнений на пиксель в среде Matlab 2015a, экспериментально полученные для алгоритмов Straightforward, Forstner [10], Neubeck [9], Scanline3x3 [13], Scanline-spiral [13] и предложенного SSEF. Количество сравнений на пиксель и средняя продолжительность выполнения были установлены для каждого тестового изображения в системе Intel Core i5 2.3 ГГц с 4 ГБ ОЗУ.

Результат поиска экстремумов изображений с размером 512×512

Методы	Изображение	Число экстремумов			Время, с	Число сравнений	Память
		Сумма	Поиск	Ошибка			
Straightforward	Lena	33078	23404	0	0,241	9,66	$O(1)$
	Barbara	32322	26233	0	0,240	9,81	
	Airfield	47414	33876	0	0,235	9,86	
Forstner [10]	Lena	33078	23404	0	0,107	4,47	$O(1)$
	Barbara	32322	26233	0	0,117	4,63	
	Airfield	47414	33876	0	0,116	4,85	
Neubeck [9]	Lena	33078	26395	1799	1,420	3,22	$O(1)$
	Barbara	32322	27709	1141	1,441	3,26	
	Airfield	47414	35097	977	1,415	3,45	
Scanline3x3 [13]	Lena	33078	25401	602	1,043	< 4	$2\times O(1+2/X)$
	Barbara	32322	27626	548	0,993	< 4	
	Airfield	47414	34573	318	1,113	< 4	
Scanline - spiral order [13]	Lena	33078	23304	0	0,625	< 4	$2\times O(1+2/X)$
	Barbara	32322	25894	0	0,577	< 4	
	Airfield	47414	33360	0	0,762	< 4	
Предложенный (SSEF)	Lena	33078	23404	0	0,067	4,21	$O(1)$
	Barbara	32322	26233	0	0,072	4,48	
	Airfield	47414	33876	0	0,075	4,52	

Заключение

Предложен быстрый алгоритм поиска экстремумов изображения на основе центрально-симметричного сканирования. Установлено, что алгоритм SSEF по сравнению с Forstner [10] обеспечивает уменьшение в 1,05 раза числа сравнений на пиксель и повышение в 1,5 раза скорости поиска, по сравнению с алгоритмом Straightforward – уменьшение в 2,2 раза числа сравнений на пиксель и повышение в 3,5 раза скорости поиска, по сравнению с алгоритмом Scanline3x3 [13] – увеличение в 1,05 раза числа сравнений на пиксель, но повышение в 15 раз скорости поиска, по сравнению с алгоритмом Scanline-spiral [13] – увеличение в 1,05 раза числа сравнений на пиксель, но повышение в 10 раз скорости поиска. Алгоритм Neubeck [9] обеспечивает меньшее число сравнений на пиксель, однако имеет ошибку поиска на границах блоков разбиения. Алгоритм SSEF не использует дополнительную память, что важно для многих задач компьютерного зрения, таких как обнаружение объектов и углов. Предложенный алгоритм также может быть модифицирован для обработки данных любого измерения в режиме реального времени.

SEARCH OF LOCAL EXTREMUMS OF HALF-TONE IMAGES BASED ON CENTRAL SYMMETRIC SCANNING

NGUYEN ANH TUAN, V.Yu. TSVIATKOU

Abstract. An algorithm for searching for single-pixel extremes of halftone images based on centrally symmetric scanning is proposed. It is shown that the algorithm works much faster than the best known algorithms for detecting key points of images.

Keywords: local extremum search, centrally symmetric scanning.

Список литературы

1. Rosenfeld A., Kak A. Digital Picture Processing. Academic Press, 1976.
2. Kitchen L., Rosenfeld A. // Pattern Recognition Letters. 1982. Vol. 1. P. 92–102.
3. Harris C., Stephens M. // Proc. of the Fourth Alvey Vision Conference. 1988. P. 147–151.
4. Lowe D. // IJCV. 2004. Vol. 60. P. 91–110.
5. Mikolajczyk K., Schmid C. // IJCV. 2004. Vol. 60. P. 63–86.
6. Van Herk M. // Pattern Recognition Letters. 1992. Vol. 13. P. 517–521.
7. Gil J., Werman M. // IEEE Trans. on PAMI. 1993. Vol. 15. P. 504–507.
8. Coltuc D., Bolon P. // Proc. Of EUSIPCO. 2000. P. 2425–2428.
9. Neubeck A., Van Gool L. // Proc. of ICPR. 2006. Vol. 3. P. 850–855.
10. Forstner W., Gulch E. // Proc. of Intercommission Conf. on Fast Processing of Photogrammetric Data. 1987. P. 281–305.
11. Soille P. / Morphological Image Analysis: Principles and Applications. Springer. 2006.
12. Р. Гонсалес, Вудс Р. Цифровая обработка изображений. М., 2005.
13. Tuan Q. Pham // Advanced Concepts for Intelligent Vision Systems (ACIVS). 2010. Vol. 12. P. 438–451.

УДК 004.056.53

ОСОБЕННОСТИ СОВРЕМЕННЫХ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

В.И. ГРИЦКЕВИЧ, С.Н. ПЕТРОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Проведен обзор разновидностей существующих систем обнаружения вторжений. Проанализированы особенности функционирования таких систем.

Ключевые слова: система обнаружения вторжений, сигнатура, аномальное поведение, сетевой трафик.

Введение

Средства обнаружения вторжений представляют собой программные или аппаратно-программные решения, автоматизирующие процессы сбора, хранения и анализа событий, происходящих в компьютерной системе, а также самостоятельно анализирующие эти события с целью выявления признаков нарушения информационной безопасности. Значительное увеличение количества различных типов и способов организации несанкционированного доступа к компьютерным сетям и системам приводят к тому, что средства обнаружения вторжений становятся одним из наиболее важных компонентов инфраструктуры безопасности.

Основная часть

Современные системы обнаружения вторжений (СОВ) имеют различную архитектуру (рис. 1).

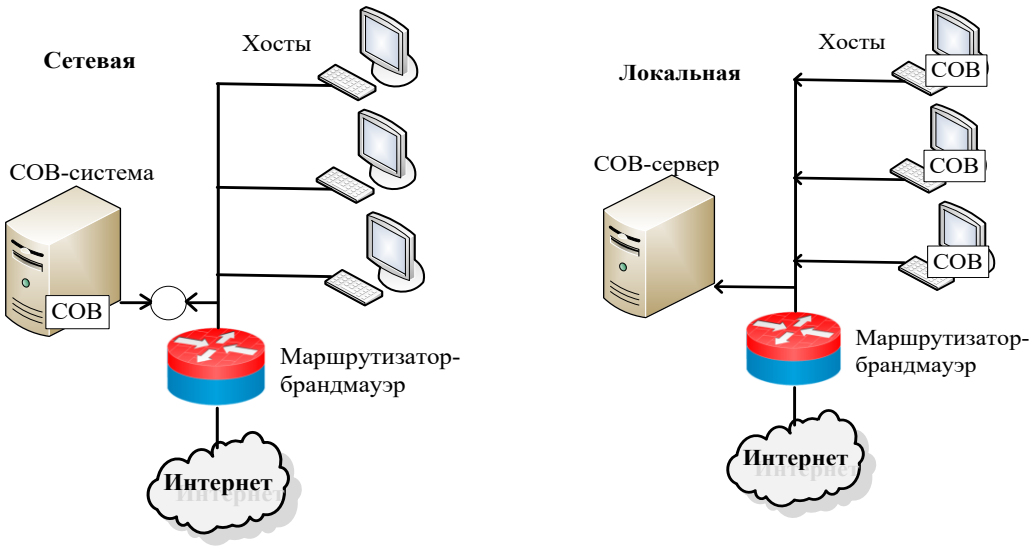


Рис. 1. Схемы сетевой и локальной СОВ

Сетевые СОВ располагаются в локальной сети предприятия и осуществляют мониторинг внутрисетевого трафика в режиме реального времени на предмет соответствия происходящих процессов заранее определенным сигнатурам атак. Признаки известных атак хранятся в базе данных системы и регулярно обновляются. Проблема такого подхода заключается в том, что постоянный мониторинг трафика серьезно снижает пропускную способность локальной сети

и производительность маршрутизатора. Тем не менее, пограничные маршрутизаторы (расположенные на стыке внутренних и публичных сетей) предоставляют отличную возможность для распознавания и пресечения атак до того, как они попадут во внутреннюю корпоративную сеть [1].

Локальные (хостовые) СОВ выполняют мониторинг и обработку событий, происходящих внутри хоста. Это отличает их от сетевых СОВ, которые отслеживают сетевой трафик. На функционирование локальных СОВ не влияет наличие в сети коммутаторов. Локальные СОВ более трудны в управлении, т. к. должны быть сконфигурированы на каждом узле локальной сети. Помимо этого, они используют вычислительные ресурсы узлов, за которыми наблюдают, что также понижает производительность системы [2].

Технологии по которым строятся СОВ делятся на две категории: обнаружение аномального поведения и обнаружение злоупотреблений.

Аномальное поведение пользователя определяется как отклонение от нормального поведения. Примером такого отклонения может служить большое число соединений за короткий промежуток времени либо высокая загрузка центрального процессора. Важной задачей является выявление среди всех подобных отклонений именно тех, которые свидетельствуют об атаке, т. к. не все аномальные отклонения являются ее следствием. Таким образом, возможны случаи, когда аномальное поведение, не являющееся атакой, определяется как атака и когда реальная атака не вызывает аномальных событий в системе. По сути, это означает, что системы обнаружения аномального поведения подвержены ошибкам первого и второго родов. Поэтому для построения профиля поведения системы следует привлекать администраторов, имеющих высокий уровень компетенций.

Детектирование атаки заключается в описании ее в виде сигнатуры и дальнейшем поиске этой сигнатуры в сетевом трафике. Сигнатурой может быть как шаблон действий, так и строка символов, которая определена как признак аномальной деятельности. Данная технология обнаружения атак похожа на технологию обнаружения вирусов. Такая система, хотя и справляется с обнаружением известных атак, не решает задачу определения неизвестных атак. Помимо этого, существует проблема описания атаки таким образом, который позволил бы в будущем зафиксировать ее возможные модификации [3].

В большинстве современных СОВ используется только сигнатурный метод распознавания атак или только поиск аномального поведения. В настоящее время существует недостаточное количество СОВ, которые реализуют сразу несколько подходов, т. е. гибридных систем. Помимо этого в системах обнаружения вторжений зачастую отсутствует встроенный имитатор атак, который проверяет корректность развернутой и эксплуатируемой системы, а также обеспечивает возможность тестирования конфигурационных параметров.

Еще одним распространенным недостатком СОВ является их низкое быстродействие и высокая степень нагрузки на локальную сеть и хосты в ней. Современные СОВ должны предусматривать возможность резервирование рубежей обороны сетевого периметра.

Заключение

Существующие СОВ отличаются используемыми методами обнаружения и их реализацией, архитектурой, уровнем детализации и типами обнаруживаемых атак. У каждой из этих систем есть свои достоинства и недостатки. Несмотря на постоянное развитие технологий, применяемых при разработке СОВ, все решения по реализации последних постоянно усложняются.

Так как алгоритмы совершения атак непрерывно совершенствуются, то к современным СОВ предъявляются все более жесткие и сильные требования. Негативным следствием этого является усложнение их развертывания и эксплуатации. В связи с вышеизложенным можно заключить, что в настоящее время представляется актуальной разработка гибридных СОВ, сочетающих в себе разные подходы к обнаружению атак.

FEATURES OF MODERN INTRUSIONS DETECTION MEANS

V.I. GRITSKEVICH, S.N. PETROV

Abstract. The review of existing intrusion detection systems is carried out. Operating features of such systems are analyzed.

Keywords: intrusion detection system, signature, anomalous behavior, network traffic

Список литературы

1. Сетевые IDS-системы. [Электронный ресурс]. URL: http://www.cnews.ru/reviews/free/oldcom/ security/ ids.shtml. (дата обращения: 22.10.2018).
2. HIDS (Host-Based Intrusion Detection System). [Электронный ресурс]. URL: https://ru.bmstu.wiki/HIDS_(Host-Based_Intrusion_Detection_System). (дата обращения: 22.10.2018).
3. Классификация систем обнаружения атак. [Электронный ресурс]. URL: http://libraryno.ru/9-3-1-klassifikaciya-sistem-obnaruzheniya-atak-shcelkunova/. (дата обращения: 22.10.2018).

УДК 621.391

ОЦЕНКА ПРИМЕНИМОСТИ МЕТОДА ОПТИЧЕСКОЙ НАВИГАЦИИ VIOLETM В УСЛОВИЯХ АНТРОПОГЕННЫХ ЛАНДШАФТОВ

В.В. ЧЕПИКОВА, К.А. ВОЛКОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

РУП «НПЦ многофункциональных беспилотных комплексов» НАН Беларуси, Республика Беларусь

Поступила в редакцию 1 ноября 2018

Аннотация. Предложен способ оценки применимости методов оптической навигации с использованием спутниковых снимков местности. Осуществлена программная реализация этого способа. Предложен метод визуальной итеративной одометрии и локации с использованием карты окружающего ландшафта. Проведено исследование практической реализации данного метода в условиях антропогенных ландшафтов и приведена карта его применимости для автоматического определения координат беспилотных летательных аппаратов на территории г. Минска.

Ключевые слова: беспилотный летательный аппарат, оптическая навигация, VIOLETM.

Введение

Задача автоматического позиционирования и движения беспилотных летательных аппаратов (БЛА) по оптическим ориентирам на местности имеет большое значение, поскольку в настоящее время сфера их практического применения ограничена условиями уверенного приема радиосигналов систем глобального позиционирования (GPS, ГЛОНАСС, Gallileo, BeiDou и др. [1]) или сигналов управления оператора. Существующие альтернативные решения для одометрии на основе бесплатформенных инерциальных навигационных систем (БИНС) характеризуются высокими весом и стоимостью [2] и при этом не обеспечивают достаточной точности исчисления координат в условиях длительного полета. Авторами предложен метод визуальной итеративной одометрии и локации с использованием карты окружающего ландшафта VIOLETM (Visual Iterative Odometry and Location using Environmental Terrain Map). В статье приводятся результаты исследования возможности его практического применения в условиях антропогенных ландашафтов и городской застройки.

Анализ условий моделирования

Существующие системы оптической навигации основаны на сопоставлении изображения, полученного с помощью бортовой фотокамеры, с известной цифровой моделью местности, над которой производится полет. При этом модель местности может быть как статичной (известной заранее по результатам спутниковой или аэрофотосьемки с последующей геопривязкой), так и динамически сформированной в процессе движения БЛА [3–5].

Сопоставление изображения модели местности с изображениями, полученными с помощью бортовой фотокамеры, в общем случае имеет ряд трудностей, обусловленных следующими факторами.

1. Наличие некомпенсированных оптических искажений на изображениях [6, 7] и артефактов цифровой компрессии [8, 9].
2. Наличие перспективных отличий из-за различных точек съемки [6].

3. Различие в форме теней объектов на изображениях из-за отличающихся условий освещенности и атмосферных явлений [10].

4. Различие в цветовой гамме, яркости и контрастности изображений из-за различных условий освещенности, атмосферных явлений, настроек и параметров съемочного оборудования [10–12].

5. Изменения в ландшафте, обусловленные естественными процессами и человеческой деятельностью.

6. Неточность определения пространственного разрешения снимка и углового положения оптической оси камеры из-за погрешностей бортовых датчиков БЛА.

7. Отсутствие на изображениях характерных контрастных фрагментов и контуров [12].

Следовательно, для практического применения любого метода оптической навигации важнейшим условием является его стабильная работа с учетом вышеперечисленных факторов. Поскольку целью описываемого эксперимента является оценка применимости метода VIOLETM для различных типов подстилающей поверхности в пределах антропогенных зон, а не его чувствительности к вариативности датчиков высоты и поворота, были приняты допущения, что камера БЛА направлена в надир и известны точное направление по азимуту и высота съемки. Приведенные допущения позволили при моделировании использовать в качестве источников изображений для камеры и опорного фотоплана подстилающей поверхности существующие тайловые базы геопривязанных космоснимков [13], сделанных в различное время года и дня. Для проведения эксперимента авторами применялись снимки, представленные в открытых источниках Google и Yandex, а именно, снимки территории г. Минска и его окрестностей общей площадью около 560 кв. км с координатами 53,80° СШ, 27,35° ЗД – 53,98° СШ, 27,76° ЗД (рис. 1). Разрешение снимков – 0,70 и 1,40 м/пикс.

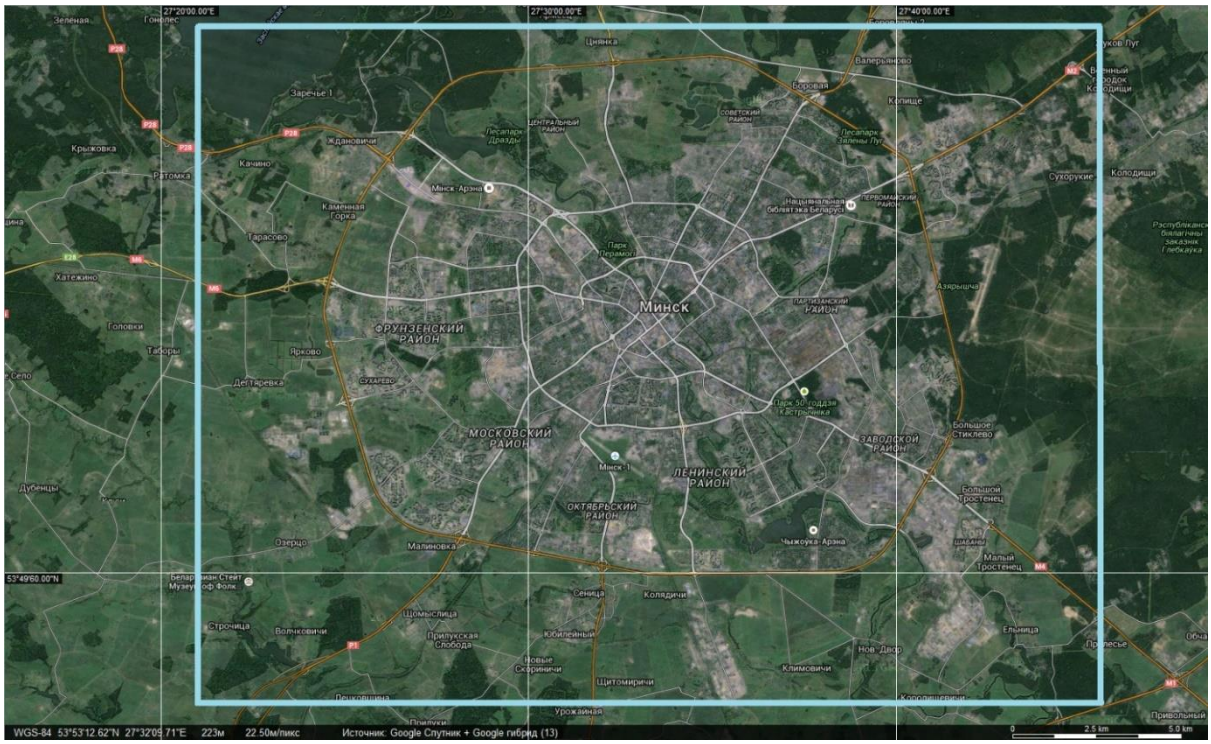


Рис. 1. Фрагмент фотоплана для исследования метода VIOLETM

Исследование работы метода

Для исследования работы метода VIOLETM была спроектирована и реализована программная система (рис. 2), состоящая из 6 основных блоков. Блок 1 используется для ввода параметров задания для моделирования: границ анализируемой территории, пиксельного размера и разрешения изображений камеры и фрагмента опорного фотоплана, используемых источников тайлов, периодичности проведения измерений (шаг по широте и долготе). Блок 2

осуществляет управление процессом моделирования на основе сформированного задания. По сигналам, полученным от Блока 2, в Блоке 4 проводится формирование изображения подстилающей поверхности для заданных координат местности с заданным размером. В Блоке 5 аналогичным образом формируется изображение для бортовой камеры, так чтобы географические координаты центров изображений совпадали. Исходные графические данные в виде тайлов спутниковых снимков поступают из Блока 3 в Блоки 4 и 5. Полученная пара изображений из Блоков 4 и 5 передается в Блок 6, реализующий логику метода VIOLETM в части определения взаимного смещения изображений (без учета возможности их взаимного поворота и масштабирования). Полученные результаты в виде определенного пиксельного смещения изображений и времени его вычисления передаются в Блок 7 для представления в табличном и графическом виде.

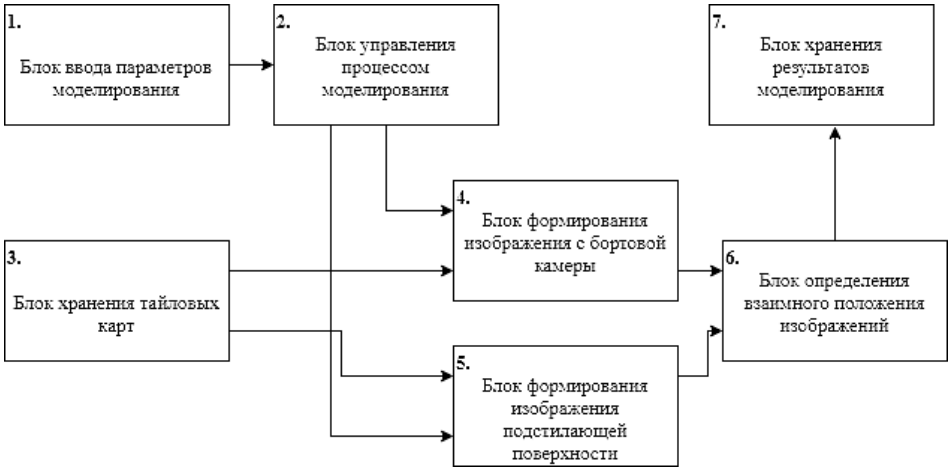


Рис. 2. Система исследования работы методы VIOLETM
с использованием тайловых спутниковых снимков

При моделировании размер изображения бортовой камеры был принят равным 720×576 пикселей, поскольку он поддерживается большинством распространенных видеокамер. Размер изображения подстилающей поверхности выбран с учетом собранных авторами статистических экспериментальных данных о погрешности расчета положения БЛА, движущегося с использованием БИНС. В таблице приведены параметры для четырех проведенных вычислительных экспериментов.

Параметры вычислительных экспериментов

Номер эксперимента	1	2	3	4
Пиксельное разрешение изображений, м/пиксель	0,70	0,70	1,40	1,40
Размер изображения с камеры, пиксели	720×576	720×576	720×576	720×576
Размер изображения с камеры на местности, м	504×403	504×403	1008×806	1008×806
Источник изображения с камеры	Google Satellite	Yandex Satellite	Google Satellite	Yandex Satellite
Размер изображения подстилающей поверхности, пиксели	3000×3000	3000×3000	3000×3000	3000×3000
Размер изображения подстилающей поверхности на местности, м	2100×2100	2100×2100	4200×4200	4200×4200
Источник изображения подстилающей поверхности	Yandex Sattelite	Google Sattelite	Yandex Sattelite	Google Sattelite
Интервал между измерениями по широте	1 / 400°	1 / 400°	1 / 200°	1 / 200°
Интервал между измерениями по долготе	1 / 200 °	1 / 200 °	1 / 100°	1 / 100°

Моделирование осуществлялось с использованием одного потока на 4-ядерном процессоре Intel Core i5-6500 3,20 ГГц, 8 ГБ ОЗУ, программа скомпилирована компилятором MinGW 5.3.0 32bit с опцией оптимизатора -O2. На рис. 3 представлено распределение вероятности времени обработки одного кадра алгоритмом VIOLETM. В среднем, время обработки составило 240 с.

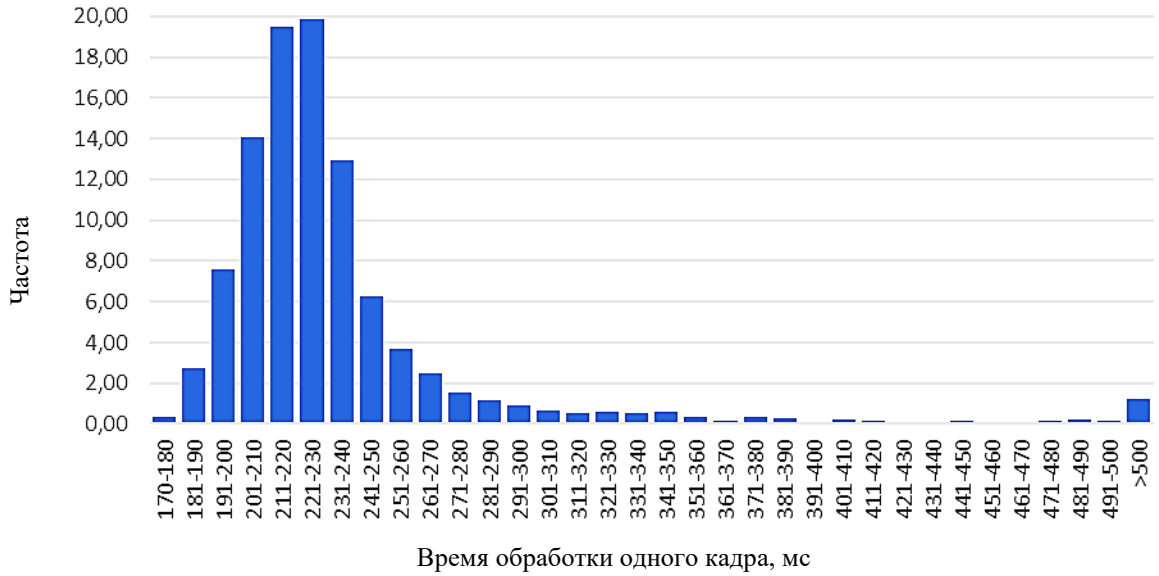


Рис. 3. Распределение вероятности времени обработки одного кадра

Согласно условиям эксперимента, изображения бортовой камеры и подстилающей поверхности имеют одинаковые географические координаты, поэтому в идеальном случае алгоритм должен определить, что взаимное смещение изображений равно нулю. Однако на практике, в силу описанных выше причин, значение смещения обычно отлично от нуля и может считаться погрешностью. На рис. 4, 5 приведена гистограмма распределения смещений для экспериментов № 1 и № 3. Для остальных экспериментов она носит аналогичный характер. Статистический анализ полученных результатов совместно с визуальной оценкой изображений, имеющих значительные смещения, позволяет сделать вывод о том, что смещение между парой изображений менее 20 пикселей может быть вызвано особенностями местности и условий фотосъемки, а большее смещение однозначно свидетельствует о невозможности определения взаимного расположения изображений исследуемым методом (рис. 6).

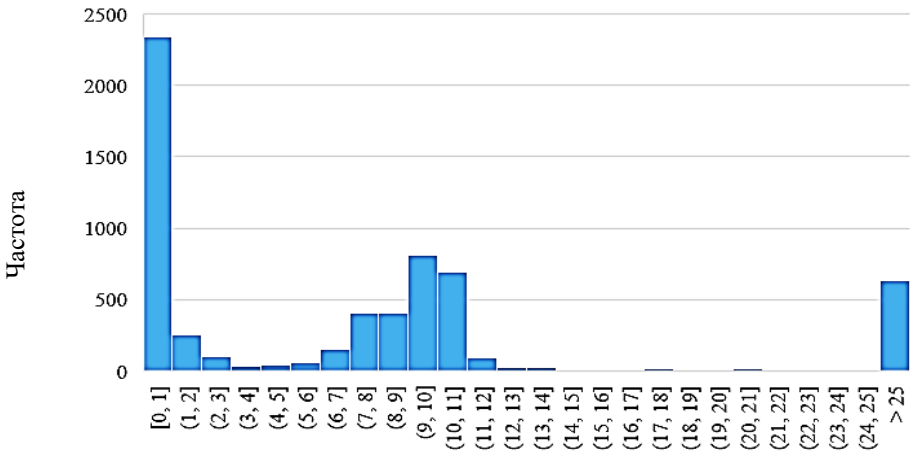


Рис. 4. Пиксельная погрешность совмещения изображений бортовой камеры и подстилающей поверхности (эксперимент № 1)

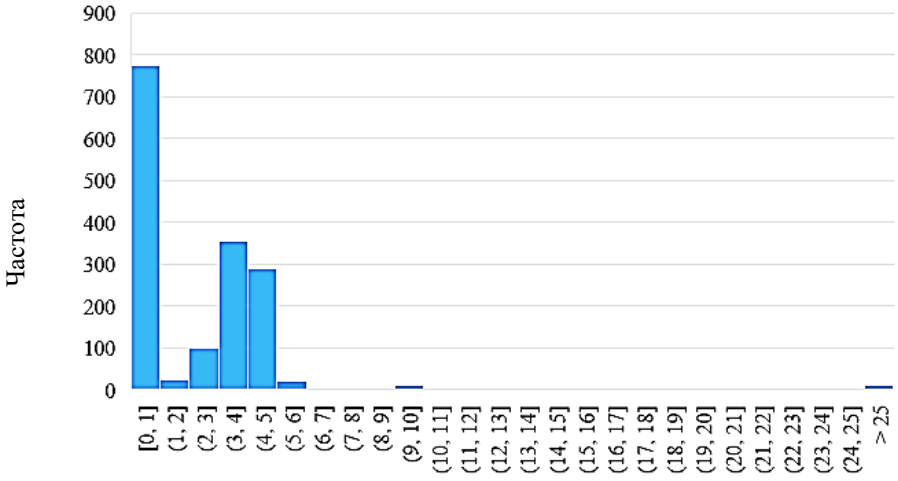


Рис. 5. Пиксельная погрешность совмещения изображений бортовой камеры и подстилающей поверхности (эксперимент № 3)

а *б*

в *г*

Рис. 6. Примеры участков местности с невозможной оптической навигацией:
а – сельскохозяйственные поля; *б* – лесные массивы;
в – поверхность водоемов; *г* – прямолинейные участки трасс

С учетом найденного порогового ограничения на величину ошибки совмещения по результатам вычислительных экспериментов были составлены карты применимости исследуемого метода в условиях антропогенных ландшафтов г. Минска (рис. 7).

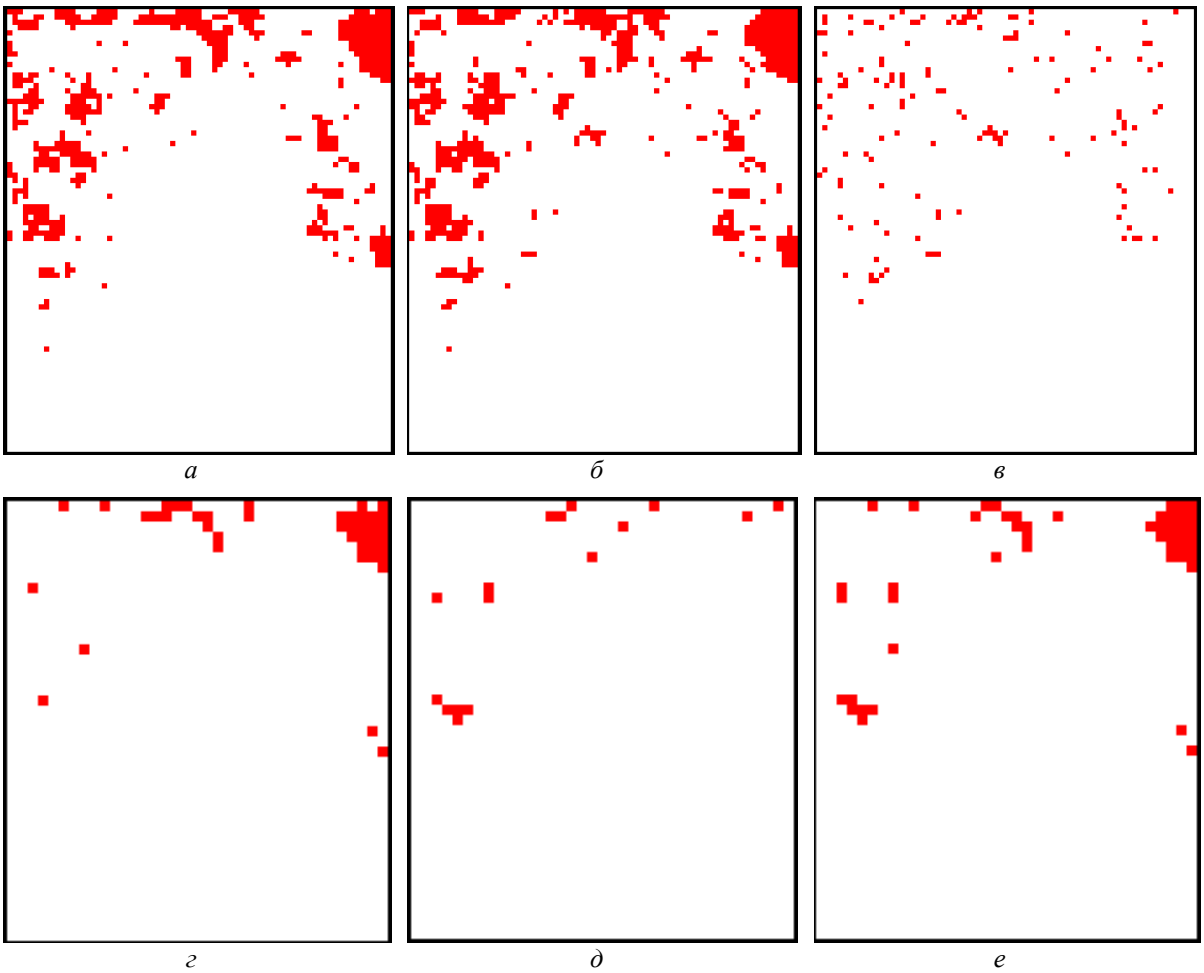


Рис. 7. Карта применимости метода VIOLETM для автоматического определения координат БЛА на территории г. Минска: *а* – эксперимент № 1; *б* – эксперимент № 2; *в* – бинарное различие результатов экспериментов № 1 и 2; *г* – эксперимент № 3; *д* – эксперимент № 4; *е* – бинарное различие результатов экспериментов № 3 и 4

На основе анализа полученных данных можно сделать вывод о том, что метод VIOLETM позволяет осуществлять точное определение положение БЛА на 90 % территории с антропогенной застройкой при разрешении изображения 0,70 м/пиксель и на 95 % – при разрешении 1,40 м/пиксель. При этом использование нескольких опорных фотопланов позволяет дополнительно повысить надежность автоматического позиционирования БЛА.

Заключение

В работе проведено моделирование работы метода VIOLETM с использованием тайловых баз спутниковых снимков антропогенных ландшафтов. Результаты эксперимента показывают, что точность вычисления координат на местности достигает 20–30 м и обеспечивает возможность примения данного метода для автономного движения БЛА. При этом частота пересчета координат составляет более 3 Гц. С помощью представленной методики возможно проведение дополетного планирования маршрута движения БЛА с учетом зон, непригодных для определения координат предложенным методом.

ESTIMATION OF THE APPLICABILITY OF VIOLETM OPTICAL NAVIGATION METHOD IN THE CONDITIONS OF ANTHROPOGENIC LANDSCAPES

V.V. CHEPIKOVA, K.A. VOLKOV

Abstract. The way of modeling of the applicability of optical navigation methods using satellite images is proposed. It's software implementation is carried out. A method of visual iterative odometry and location using a map of the surrounding landscape is proposed. A study of the practical implementation of this method in the conditions of anthropogenic landscapes is conducted and a map of its applicability for automatic determination of the coordinates of the unmanned aerial vehicle in the city of Minsk is given.

Keywords: unmanned aerial vehicle, optical navigation, VIOLETM

Список литературы

1. Косова А.Е., Кориков А.М. // Докл. ТУСУР. 2017. № 3. С.191–196.
2. Доросинский Л.Г., Богданов Л.А. // Современные проблемы науки и образования. 2014. № 5. С.69–72
3. Cadena [etc.] //IEEE Transactions on Robotics. 2016. № 32 (6). P.1309–1332.
4. Jaulin L. // IEEE Transactions on Robotics. 2011. P. 282–287.
5. Ардентов А.А. [и др.] Программные системы: теория и приложения. 2012. Т. 3. № 3-1 (12). С. 23–38.
6. Русинов М.М. Композиция оптических систем. Л., 1989.
7. Сивухин Д.В. Общий курс физики. Оптика. М., 1985.
8. Дж. Миано. Форматы и алгоритмы сжатия изображений в действии. М.,2003.
9. Сэломон Д. Сжатие данных, изображений и звука. М., 2004.
10. Иофис Е.А. Фотокинотехника. М., 1981.
11. Волосов Д.С. Фотографическая оптика. М., 1978.
12. Герман Е.В. Алгоритмы совмещения разнородных изображений в бортовых системах визуализации, диссертация на соискание ученой степени кандидата тех. наук. Рязань, 2014.
13. Волков К.А. [и др.] // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно- технического семинара. В 2 ч. Ч. 1 Минск, 2016. – С. 31–37

УДК 654.1.02:004.357

ОЦЕНКА КАЧЕСТВА ПЕРЕДАЧИ ВИДЕОТРАФИКА В КОРПОРАТИВНОЙ СЕТИ

М.А. АЛИСЕЕНКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 22 октября 2018

Аннотация. Рассмотрены возможности применения систем захвата и анализа сетевого трафика для оценки качества передаваемого видеотрафика. Проведен обзор преимуществ технологий мониторинга и анализа трафика NetFlow и NBAR.

Ключевые слова: видеоконференцсвязь, анализ сетевого трафика, NetFlow, NBAR.

Введение

Для использования современных программных систем видеоконференцсвязи (ВКС) требуется только персональный компьютер (ПК) со встроенными внешними средствами отображения и воспроизведения данных. Программные системы ВКС предназначены для локальных корпоративных сетей, имеют программный MCU-сервер для управления участниками и видеоконференциями.

Наличие ВКС увеличивает объем передаваемых данных в сети, а также поддерживают большое количество сетевых протоколов прикладного уровня. Для разработки эффективной методики оценки качества передачи видеотрафика в корпоративной сети в условиях мультимедийного трафика требуется использовать системы анализа трафика.

Особенности систем захвата и анализа трафика

Выделяют следующие области практического применения систем анализа: выявление проблем в работе сети, восстановление («прослушивание») потоков данных, предотвращение сетевых атак, сбор статистики. Задача анализа сетевого трафика разделяется на три независимые подзадачи: перехват, хранение и анализ трафика. Система анализа должна обеспечивать захват трафика, а также предоставлять эффективные методы анализа его результатов.

Захват трафика осуществляется посредством снифферов – программ или программно-аппаратных устройств, предназначенных для перехвата трафика. В рамках конкретных продуктов могут быть реализованы дополнительные возможности, например, разбор заголовков сетевых протоколов, фильтрация по заданным критериям, восстановление сессий.

В сети Ethernet существуют следующие основные возможности прослушивания трафика [1].

1. В сети на основе концентраторов весь трафик домена коллизий доступен любой сетевой станции.

2. В сетях на основе коммутаторов сетевой станции доступен ее трафик, а также весь широковещательный трафик данного сегмента.

3. Управляемые коммутаторы имеют функцию копирования трафика данного порта на порт мониторинга («зеркалирование», мониторинг порта).

4. Допустимо использование специальных средств (ответвителей), включаемых в разрыв сетевого подключения и передающих трафик подключения на отдельный порт.

5. Порт коммутатора, трафик которого необходимо прослушать, включают через концентратор, к которому, в свою очередь, подключен узел-монитор (при этом в большинстве случаев уменьшается производительность сетевого подключения).

Сниффер может быть установлен на маршрутизаторе либо на оконечном узле сети.

Большинство существующих инструментов, как правило, проводит разбор заголовков сетевых протоколов, а также восстанавливает сессии. В то же время существуют достаточно специфические задачи, для решения которых может не отыскаться готовый инструмент [2]. К таким задачам относят:

– анализ туннелированных протоколов произвольной глубины;

– выделение связей между потоками данных, передаваемых по сети;

– выполнение определенных сценариев в случае обнаружения в трафике предварительно заданных сигнатур.

Выделяют два режима работы сетевых анализаторов: в реальном времени и по предварительно сохраненному трафику (отложенный анализ).

Для анализа в реальном времени требуется поддержка работы инструмента в непрерывном режиме с производительностью, достаточной для разбора трафика, поступающего на вход. При этом должна быть обеспечена возможность обработки потенциально бесконечного входного потока данных.

В случае отложенного анализа входные данные извлекаются из файла. Результаты такого анализа являются более детальными по сравнению с результатами анализа, выполняемого в режиме реального времени.

Технология NetFlow

В соответствии с NetFlow протоколом выполняется анализ пакетов, проходящих через определенный интерфейс сетевого устройства, на основе чего формируется информация в заданном формате о параметрах различных транзитных сетевых потоков интерфейса, и эта информация передается по IP сети специальной программе, называемой NetFlow коллектор. Программа NetFlow коллектор устанавливается на определенном ПК (сервере) сети и занимается сбором и первичной обработкой информации от одного или группы сетевых устройств, передающих данные в формате NetFlow. Затем используются программы, анализирующие накопленные данные и предоставляющие пользователю требуемые отчеты о работе сети.

Сетевой поток идентифицируется как однонаправленный поток пакетов между определенным источником и приемником данных, которые, в свою очередь, характеризуются IP-адресами и используемыми портами. Для уникальной идентификации потока используется 7 полей:

– IP адрес источника данных;

– IP адрес приемника данных;

– номер порта источника данных;

– номер порта приемника данных;

– тип протокола 3-го уровня;

– тип сервиса IP пакетов (ToS);

– входной логический интерфейс.

Существуют также программы-сенсоры NetFlow для компьютеров с различными операционными системами, которые позволяют формировать информацию о сетевых потоках, проходящих через интерфейсы ПК.

С помощью программного модуля на сетевом устройстве анализируются пакеты, проходящие через сетевой интерфейс, и на основании результатов анализа формируются данные по каждому сетевому потоку, проходящему через этот интерфейс в формате NetFlow протокола. Эти данные в виде отдельных записей по каждому сетевому потоку кэшируются. Каждая запись о потоке имеет уникальный идентификатор. Периодически данные из кэша пересылаются через сетевой интерфейс на ПК (сервер) с установленной программой NetFlow коллектор (см.рис. 1).

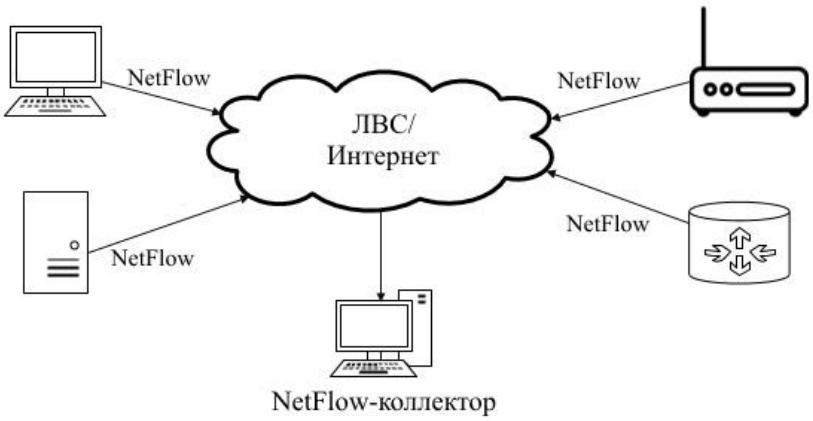


Рис. 1. Архитектура NetFlow

Таким образом, использование NetFlow протокола дополнительно загружает сетевой интерфейс, однако, благодаря высокой эффективности протокола, передаваемые данные занимают около 1,5 % от трафика коммутатора или маршрутизатора [3]. NetFlow протокол подсчитывает практически все пакеты и обеспечивает сжатый, но достаточно информативный обзор о всем сетевом трафике по интересующему сетевому интерфейсу.

Записи о сетевых потоках, которые утратили силу группируются в «NetF-low Export» дейтаграммы и экспортируются на сетевое устройство (ПК), с установленным NetFlow коллектором. Настройка NetFlow протокола выполняется для каждого интерфейса сетевого устройства. Для экспорта информации требуется указать IP адрес и номер порта устройства, где будет работать NetFlow коллектор.

Технология NBAR

Распознавание сетевых приложений Network Based Application Recognition (NBAR) − механизм, используемый в компьютерных сетях для распознавания потока данных по первому переданному пакету (рис. 2) [4].

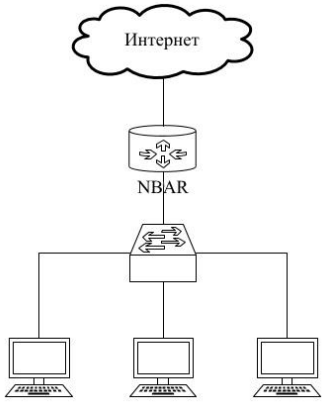


Рис. 2. Конфигурация NBAR

С помощью оборудования компьютерных сетей, использующего NBAR, анализ пакета для первого пакета в потоке данных для определения категории трафика, к которой принадлежит данный поток. Затем программное обеспечение настраивает внутренние контроллеры для соответствующей обработки потока.

Средство NBAR представляет собой механизм классификации, который распознает широкий диапазон приложений, включая протоколы WWW и другие сложно квалифицируемые протоколы, использующие динамическое назначение портов TCP/UDP. После того как приложение определено и классифицировано с помощью средства NBAR, сеть может запускать службы для данного приложения. Средство NBAR обеспечивает эффективное использование

полосы пропускания за счет классификации пакетов и использования функции QoS для классифицированного трафика.

Средство NBAR имеет новые методы классификации, позволяющие классифицировать приложения и протоколы уровней с 3 по 7:

– Статическое назначение номеров портов TCP и UDP;

– IP-протоколы, не основанные на UDP и TCP;

– Динамическое назначение номеров портов TCP и UDP;

– Классификация подпортов или классификация на основе глубокой проверки пакетов.

В средстве NBAR предусмотрена возможность классификации протоколов статических портов. Несмотря на то, что для этих целей могут использоваться и списки управления доступом (access control list, ACL), настройка средства NBAR значительно проще. Кроме того, NBAR обеспечивает статистику по классификации, недоступную при использовании списков ACL.

В NBAR входит средство распознавания протоколов (Protocol Discovery), которое представляет собой простой способ поиска протоколов приложений, работающих через определенный интерфейс. Средство распознавания протоколов позволяет идентифицировать трафик любого протокола, поддержка которого реализована в средстве NBAR. По каждому протоколу средство распознавания протоколов выполняет сбор следующих статистических данных для активированных интерфейсов: полное число входящих и исходящих пакетов и байтов, а также входящая и исходящая скорость передачи данных. Средство распознавания протоколов собирает важнейшие статистические данные по каждому протоколу в сети, который может быть использован для определения классов трафика и политик QoS для каждого класса трафика. Для расширения списка распознаваемых протоколов может быть загружен внешний модуль языка описания пакета (PDLM). Модуль PDLM также используется для улучшения существующей способности распознавания. Модуль PDLM позволяет средству NBAR распознавать новые протоколы без необходимости в новых образах Cisco IOS или перезагрузке маршрутизатора.

Средство NBAR имеет возможность классифицировать трафик приложения не только по номерам портов TCP/UDP в пакете, но и классифицировать подпорты. Средство NBAR просматривает полезную нагрузку TCP/UDP и выполняет классификацию пакетов на основе содержимого полезной нагрузки, например, идентификатора транзакций, типа сообщений или других данных.

Классификация HTTP-трафика с помощью URL-адреса, узла сети или MIME-типа является примером классификации подпорта. NBAR классифицирует HTTP-трафик посредством текста URL или полей host в запросе, с применением поиска соответствий по регулярным выражениям. Реализованное в NBAR средство классификации типа полезной нагрузки RTP не только позволяет выполнять идентификацию аудио- и видеотрафика с отслеживанием состояния, но также позволяет осуществлять разграничения на основании типа аудио- и видеокодеков для повышения точности функции QoS. Таким образом, средство классификации типа полезной нагрузки RTP для классификации пакетов RTP осуществляет тщательное сканирование заголовков RTP.

Заключение

Таким образом, система анализа должна обеспечивать захват трафика в полном объеме, а также предоставлять эффективные методы анализа и навигации по его результатам. Технология мониторинга и анализа трафика NetFlow позволяет осуществлять мониторинг на уровнях L2-L4, идентифицировать приложения по номеру порта, предоставляет информацию о потоках IP пакетов. Технология глубокого анализа пакетов NBAR анализирует данные на уровнях L3-L7, обеспечивает комбинированный метод классификации IP-трафика на основе данных канального, сетевого и транспортного уровней, и анализе содержимого пакетов. Также NBAR идентифицирует видеотрафик и разграничивает нагрузку RTP для обеспечения QoS.

VIDEOTRAFFIC TRANSMISSION QUALITY ESTIMATION IN THE CORPORATE NETWORK

M.A. ALISEYENKA

Abstract. The possibilities of use of systems for capturing and analyzing network traffic to estimate the quality of transmitting videotraffic are considered. The benefits of monitoring and analyzing traffic NetFlow and NBAR technologies are reviewed.

Keywords: video conferencing, network traffic analysis, NetFlow, NBAR.

Список литературы

1. Национальный Открытый Университет «ИНТУИТ». [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/681/537. (дата обращения: 01.11.2018)
2. Маркин Ю.В., Санаров, А.С. // Обзор современных инструментов анализа сетевого трафика – Москва, 2014. С. 1–3.
3. Cisco NetFlow Collection Engine – Retirement Notification. [Электронный ресурс]. URL: http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/netflow/nfwhite.html. (дата обращения: 01.11.2018)
4. Хилл Б. Полный справочник по Cisco. М.: «Вильямс», 2007.

УДК 004.94

РАЗРАБОТКА СЕТИ РАДИОДОСТУПА СТАНДАРТА LTE ГОРОДА ЖЛОБИН С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО КОМПЛЕКСА ATOLL

Р.А. ФИЛИМОНЧИК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 10 ноября 2018

Аннотация. Выполнено проектирование сети радиодоступа сотовой связи стандарта LTE для г. Жлобин с использованием программного комплекса Atoll. Размещены базовые станции типа «LTE: Rural». Получены карты покрытия с расчитанным уровнем сигнала покрытой территории и с результатами анализа эффективного сигнала на линии «вниз» для г. Жлобин.

Ключевые слова: мобильные сети, программный комплекс Atoll, стандарт LTE.

Введение

Программный комплекс Atoll – это система автоматизированного проектирования сетей мобильной связи, включающая в себя программное, математическое и информационное обеспечние. Atoll сочетает в себе архитектурные и функциональные возможности, которые предоставляют операторам мощную, масштабируемую и гибкую инфраструктуру для оптимизации сетей и процессов проектирования [1].

Проектирование сети радиодоступа сотовой связи стандарта LTE г. Жлобин с использованием программного комлекса Atoll

На рис. 1 приведен внешний вид панели рабочей области программы Atoll.

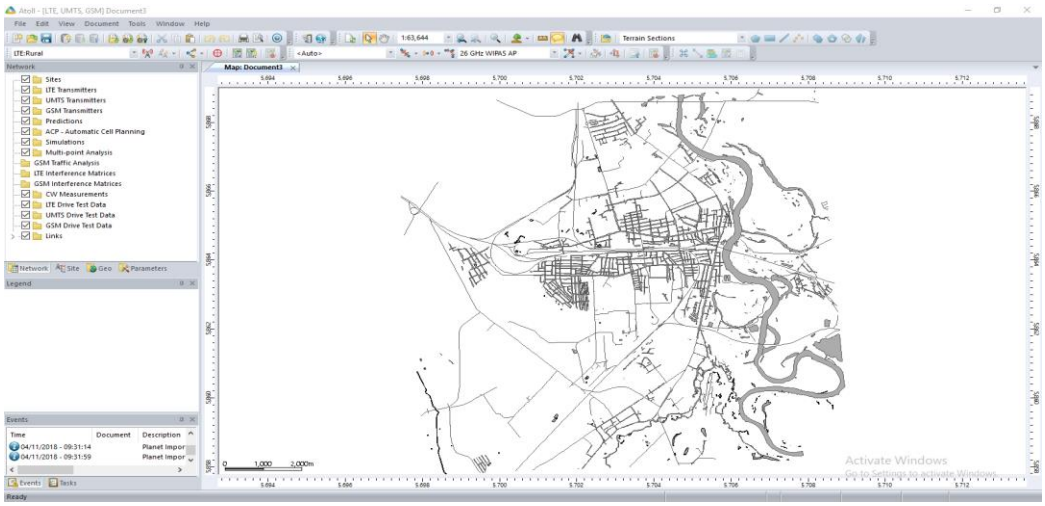


Рис. 1. Панель рабочей области программы Atoll

Для проектирования сети сотовой связи стандарта LTE г. Жлобин на карте были размещены базовые станции типа «LTE:Rural». После расстановки и корректировки положения базовых станций были осуществлены настройки каждого сайта базовой станции во вкладке «Transmitter» окна «Настройки» (рис. 2). Высота антенны – 35 м, потери 0,5 дБ, модель антенны – 1800 МГц, 65 градусов охвата, с усилением 17 дБи.

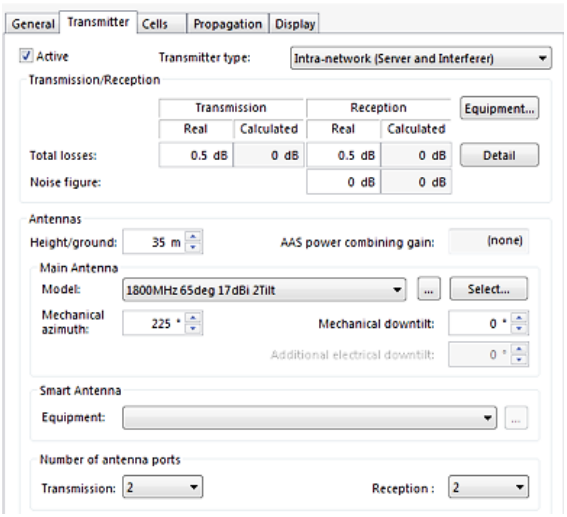


Рис. 2. Окно программного комплекса Atoll
с настройками параметров сайта базовой станции (вкладка Transmitter)

Во этом же окне во вкладке «Cells» были установлены значения, которые представлены на рис. 3.

Frequency Band	E-UTRA Band 3 - 20MHz	ICIC Configuration	
Channel Number	1 300	TDD Frame Configuration	0 - DSUUU-DSUUU
Channel Allocation Status	Not Allocated	Reception Equipment	Default Cell Equipment
Physical Cell ID	0	Scheduler	Proportional Fair
PSS ID	0	Diversity Support (DL)	AMS
SSS ID	0	Diversity Support (UL)	AMS
Physical Cell ID Status	Not Allocated	Traffic Load (DL) (%)	100
Reuse distance (m)		ICIC Ratio (DL) (%)	0
Max Power (dBm)	43	Traffic Load (UL) (%)	100
RS EPRE (dBm)	12,4	UL Noise Rise (dB)	0
SS EPRE Offset / RS (dB)	0	Angular distributions of interference (AAS)	
PBCH EPRE Offset / RS (dB)	0	AAS Usage (DL) (%)	0
PDCCH EPRE Offset / RS (dB)	0	ICIC UL Noise Rise (dB)	0
PDSCH EPRE Offset / RS (dB)	0	MU-MIMO Capacity Gain (UL)	2
Instantaneous RS Power (dBm)	35,4	Inter-technology DL Noise Rise (dB)	0
Instantaneous SS Power (dBm)	31	Inter-technology UL Noise Rise (dB)	0
Instantaneous PBCH Power (dBm)	31	Number of Users (DL)	30
Average PDCCH Power (dBm)	42,4	Number of Users (UL)	30
Average PDSCH Power (dBm)	42,8	Max Traffic Load (DL) (%)	100
Min RSRP (dBm)	-140	Max Traffic Load (UL) (%)	100
AMS & MU-MIMO Threshold (dB)		Max Number of Users	240
ICIC Delta Path Loss Threshold (dB)	0	Max number of intra-technology neighbours	16
Fractional Power Control Factor	1	Max number of inter-technology neighbours	16
Max UL Noise Rise (dB)	6	Comments	
Max PUSCH C/(I+N) (dB)	20	Physical Cell ID Domain	
Interference Coordination Support		Neighbours	...

Рис. 3. Окно программного комплекса Atoll
с настройками параметров сайта базовой станции (вкладка Cells)

В качестве частотного диапазона был выбран Band 3, который предполагает использование частоты 1800 МГц с шириной канала 20 МГц. Мощность базовой станции – 43 дБм. Максимальное количество пользователей, которое может обеспечить один сайт, – 240. Также в качестве параметра «Diversity Support» был выбран AMS. При таком параметре антенна автоматически может менять это значение с SU-MIMO на MU-MIMO.

Далее во вкладке «Propagation model» была выбрана модель «Cost-Hata» (рис. 4). Также с помощью этой модели были вручную проведены расчеты с целью нахождения радиуса охвата базовой станцией.

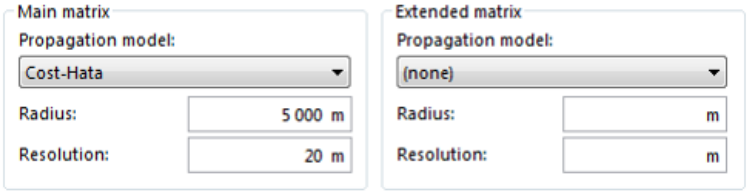


Рис. 4. Окно программного комплекса Atoll
с настройками параметров сайта базовой станции (вкладка Propogation model)

В качестве пользовательского оборудования во вкладке «Parameters – Traffic Parameters – Terminals – LTE MIMO Terminals» были выбраны параметры «UE Category 4» и «MIMO 1×2» (рис. 5).

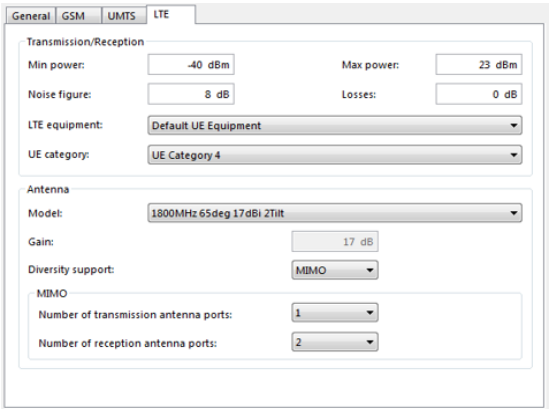


Рис. 5. Окно программного комплекса Atoll с настройками параметров абонентского оборудования

Далее был выполнен расчет параметров созданной сети LTE (вкладка «Network – Precondition»). С помощью программы были рассчитаны пропускная способность, покрытие города передатчиками, анализ эффективного сигнала, уровень сигнала на покрытой территории, уровень сигнал/шум. В результате были получены карты покрытия, представленные на рис. 6, 7.

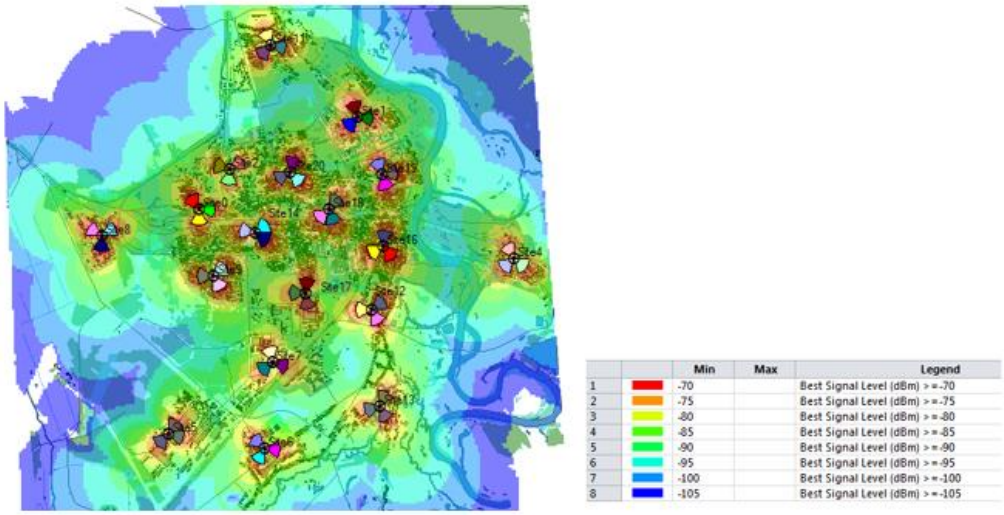


Рис. 6. Карта г. Жлобин с расчитанным уровнем сигнала покрытой территории

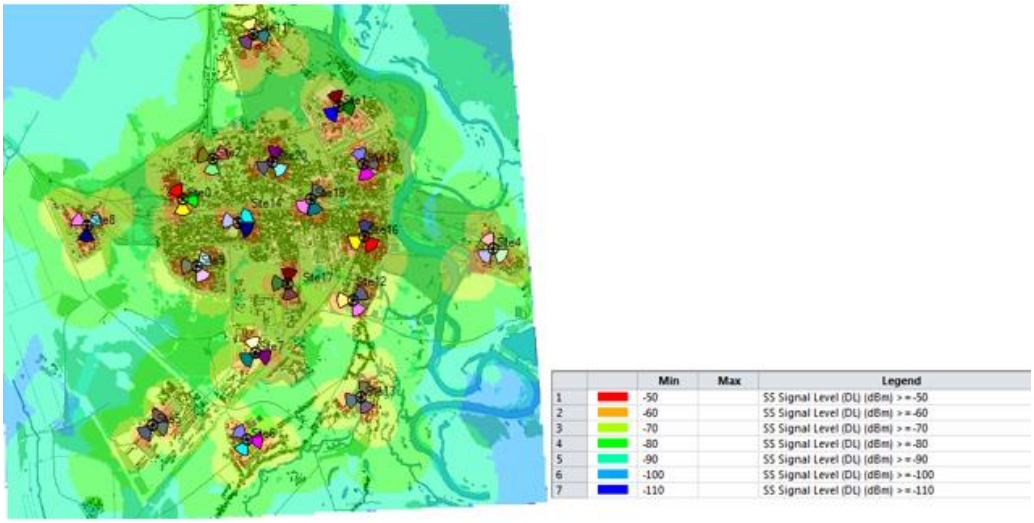


Рис. 7. Карта г. Жлобин с результатами анализа эффективного сигнала на линии «вниз»

Заключение

Программный комплекс Atoll – это продукт с обширными функциональными возможностями. Считается одним из лучших решений для радиопланирования и оптимизации различных радиотехнологий [2].

Однако для обеспечения функционирования этого комплекса требуется большой набор исходных данных, недостоверность которых может существенно повлиять на результаты планирования. К необходимым исходным данным относятся географические данные и параметры базовых и мобильных станций, а также технические характеристики оборудования. Географичекие данные содержат матрицу высот рельефа местности, тип и высоту ее застройки.

DEVELOPMENT THE LTE NETWORK OF THE ZHLOBIN CITY USING ATOLL SOFTWARE

R.A. FILIMONCHIK

Abstract. LTE network for the Zhlobin city with use of Atoll software package was designed. Base stations of «LTE: Rural» type were placed. Coverage maps with the calculated signal level of the covered territory and with the result of analysis of the effective signal on the «down» line for the Zhlobin city were developed.

Keywords: mobile networks, Atoll software, LTE.

Список литературы

1. Информационный интернет-ресурс производителя программного обеспечения Atoll. [Электронный ресурс]. URL: https://www.forsk.com/ (дата обращения: 04.11.2018).
2. Образовательный интернет-ресурс Omoled. [Электронный ресурс]. URL: http://omoled.ru/publications/view/876 (дата обращения: 04.11.2018).

УДК 004.051:004.492.3

ОЦЕНКА БЕЗОПАСНОСТИ СЕТИ С ПОМОЩЬЮ ONLINE-ПЕНТЕСТОВ

А.Д. МИХЕЙЧИК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 5 ноября 2018

Аннотация. Предложено использовать online-пентесты для повышения информационной безопасности в корпоративных сетях. Рассмотрены основные инструменты, с помощью которых можно осуществить мониторинг безопасности сети.

Ключевые слова: безопасность, пентест, сетевые атаки.

Введение

В настоящее время наблюдается непрерывное совершенствование механизмов реализации сетевых атак. В связи с этим системные администраторы и специалисты по защите информации должны периодически проверять на эффективность применяемые в их организации средства обеспечения сетевой безопасности.

Существует большое количество программных и программно-аппаратных средств, предназначенных для мониторинга безопасности корпоративных сетей. К недостаткам таких средств можно отнести дороговизну и сложность в реализации (при самостоятельной настройке). Поэтому многие специалисты часто прибегают к бесплатным online-инструментам, которые дают возможность понять, насколько защищена сеть от актуальных сетевых атак. К таким online-инструментам относятся пентесты.

Под пентестом понимается мониторинг безопасности сети с помощью проведения испытаний на проникновения. Испытания основаны на сетевых атаках, реализуемых с целью обнаружения уязвимостей и недостатков [1].

Целью работы является исследование эффективности работы online-пентестов, направленных на межсетевые экраны, антивирусные программы и веб-сайты.

Мгновенная проверка безопасности

Для проверки защищенности межсетевого экрана часто применяется сервис Check Point CheckMe [2]. Представленный сервис включает в себя несколько тестов, с помощью которых выполняется анализ компьютера пользователя и сети на предмет наличия уязвимостей, связанных с вредоносными программами, удаленным доступом, утечкой данных, кражей конфиденциальной информации, атак нулевого дня, эксплойтами и использованием анонимайзеров. Следует учитывать, что при проведении тестов на проникновения сеть не подвергается реальному риску. Для того чтобы увидеть работу сервиса Check Point CheckMe, следует выполнить следующее.

1. Зайти на сайт http://www.cpcheckme.com.
2. Запустить процесс сканирования на Интернет-браузере.
3. Просмотреть отчет о завершении сканирования после того, как произошел обмен данными между Интернет-браузером и сервисом (рис. 1).

Рис.1. Результаты работы сервиса Check Point CheckMe

Сервис Check Point CheckMe осуществляет различные сценарии, которые соответствуют следующим сетевым атакам.

1. Вредоносные программы – программы, которые могут существенно повлиять на работу компьютера и всей корпоративной сети организации.
2. Атака нулевого дня – атака, заключающаяся в неожиданном использовании злоумышленником найденной им уязвимости, о которой не было известно ранее.
3. Эксплойт – специальная программа или код, с помощью которых можно провести атаку на сеть, используя уязвимости в программном обеспечении.
4. Удаленный доступ – возможность нелегитимному пользователю дистанционно получить доступ к серверу, повысив тем самым свои привилегии.
5. Анонимайзеры – средства, предназначенные для скрытия сведений о компьютере или пользователе в сети от удаленного сервера.
6. Утечка данных – возможность для злоумышленника получить служебную информацию, циркулирующую в сети организации.
7. Кража информации – получение конфиденциальной информации (логин/пароль) с помощью поддельных веб-сайтов (фишинг).

При тестировании межсетевого экрана может возникнуть ситуация, при которой данное устройство не выполняет возложенные на него задачи (рис. 1). Это может быть связано с тем, что системные администраторы или специалисты по информационной безопасности неправильно используют функциональные возможности устройства. Например, межсетевой экран может быть настроен на фильтрацию по протоколам транспортного уровня, вместо фильтрации по приложениям. Сервис Check Point CheckMe позволяет установить и пересмотреть функционал межсетевого экрана, после чего настроить устройство и осуществить повторный тест с использованием сервиса Check Point CheckMe.

Проверка работоспособности антивирусных программ

В последнее время разработчики антивирусных программ начали использовать такие файлы, которые могут определяться антивирусным средством как вредоносные, но таковыми не являться. Это было сделано для того, чтобы пользователи смогли увидеть работу установленный ими антивирусной программы [3]. Также разработчики используют данные файлы для проведения тестов, с помощью которых осуществляется проверка работоспособности антивирусных программ. Одним из таких тестов является EICAR-Test-File [4].

Главная задача представленного теста заключается в том, чтобы показать пользователю работоспособность антивирусной программы, а также продемонстрировать, какие объекты она может проверить (происходит блокировка вирусного файла), а какие – нет (загружается вредоносный файл). Для проверки антивирусов EICAR-Test-File использует файлы формата txt, zip, а также протоколы http и https (рис. 2).

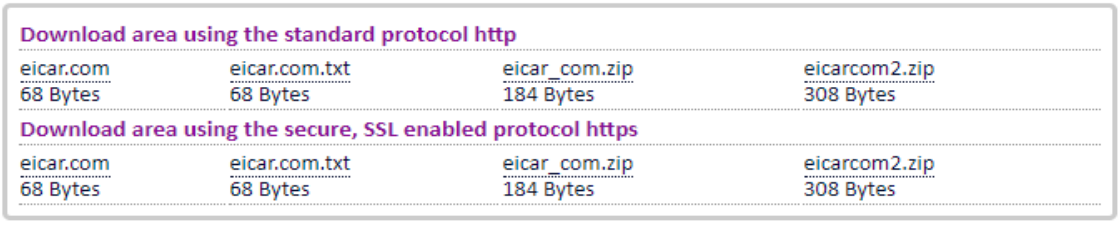


Рис. 2. Форматы файлов теста EICAR-Test-File

Для проведения тестов использована антивирусная программа Microsoft Windows 10. Перед началом проведения тестов была выполнена загрузка txt-файла. Далее была запущена антивирусная программа, после чего проверена ее работоспособность путем загрузки того же txt-файла. В конце испытаний в Интернет-браузере выполнена проверка истории загрузок (рис. 3).

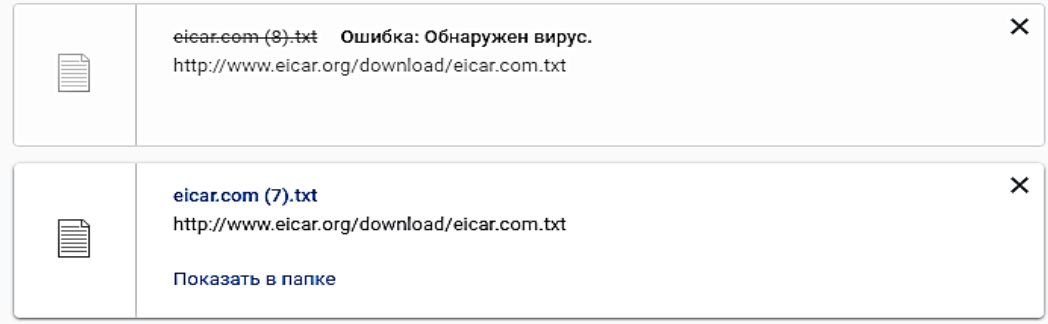


Рис. 3. Результаты проверки работоспособности антивируса Microsoft Windows 10

Как видно из рис. 3, при отключенной антивирусной программе тестовый файл загружался из Интернет-браузера на компьютер пользователя. При запущенной антивирусной прорамме тестовый файл блокировался. Таким образом, было установлено, что тестируемая антивирусная программа является работоспособной.

Проверка безопасности веб-сайтов

Одной из самых популярных сетевых атак является инъекция. Под инъекцией следует понимать возможность злоумышленником осуществить взлом сайта, внедряя в его данные произвольный код. Многие системные администраторы пренебрегают специализированными программами, которые предназначены для анализа сайтов.

На сегодняшний день существует большое количество программных средств, предназначенных для мониторинга безопасности веб-сайтов. Одним из таких средств является online-инструмент Pentest-tools [5]. Данный инструмент предназначен для проведения тестирования безопасности веб-сайта путем проведения тестов на проникновения. В качестве тестируемого веб-сайта был выбран сайт БГУИР (bsuir.by) (рис. 4). Согласно счетчику Яндекс.Метрика, среднее количество посетителей сайта bsuir.by 6100 хостов в сутки, при этом количество просмотров веб-сайта приблизительно равно 21 000 в сутки [6].

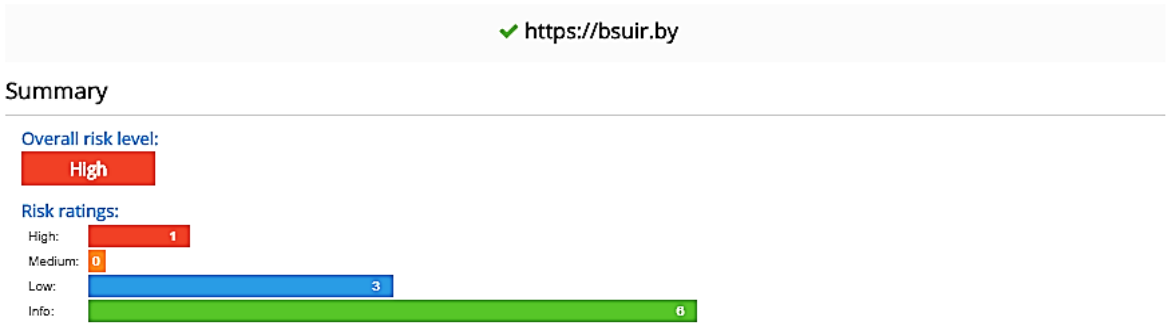


Рис. 4. Результаты анализа безопасности сайта bsuir.by, полученные с помощью Pentest-tools

Как видно из рис. 4, безопасность веб-сайта характеризуется высокой степенью риска. При более подробном анализе отчета можно прийти к выводу, что найденные уязвимости связаны с установленным веб-сервером Apache 2.4 (рис. 5).

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4
●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4
●	7.5	CVE-2013-2249	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.	N/A	http_server 2.4

Рис. 5. Перечень уязвимостей сайта bsuir.by

Под CVE понимается база данных известных на сегодняшний день уязвимостей [7]. Анализируя данные из рис. 5, можно сказать, что для решения проблемы безопасности веб-сайта следует обновить Apache HTTP Server до последней версии.

Заключение

Предложено использовать online-пентесты для проведения оценки безопасности корпоративной сети. Проведен анализ online-инструментов, направленных на межсетевые экраны, антивирусные программы и веб-сайты. В работе рассмотрены следующие online-пентесты: сервис Check Point CheckMe, тест EICAR-Test-File и online-инструмент Pentest-tools.

NETWORK SECURITY ASSESMENT WITH ONLINE PENTEST

A.D. MIHEYCHIK

Abstract. It is proposed to use online-pentest to improve information security in corporate networks. The main online-tools that can be used to monitor network security are reviewed.

Keywords: security, pentest, network attacks.

Список литературы

1. Пентестинг. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Pentesting (дата обращения: 13.10.2018).
2. Check Point CheckMe. [Электронный ресурс]. URL: http://www.cpcheckme.com/checkme/?source=Tssolution (дата обращения: 14.10.2018).
3. Тестовый вирус eicar. [Электронный ресурс]. URL: https://support.kaspersky.ru/general/products/7399 (дата обращения: 15.10.2018).
4. EICAR-Test-File. [Электронный ресурс]. URL: http://www.eicar.org/85-0-Download.html (дата обращения: 15.10.2018).
5. Pentest-tools. [Электронный ресурс]. URL: https://pentest-tools.com/home (дата обращения: 16.10.2018).
6. Яндекс.Метрика. [Электронный ресурс]. URL: https://metrika.yandex.ru (дата обращения: 16.10.2018).
7. CVE. [Электронный ресурс]. URL: https://cve.mitre.org (дата обращения: 16.10.2018).

УДК 004.716

ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ КАК СРЕДСТВО АНАЛИЗА И КОНТРОЛЯ ТРАФИКА

О.А. РОМАНЕНКО

Белорусский государственный университет информатики и радиоэлектроники, РеспубликаБеларусь

Поступила в редакцию 31 октября 2018

Аннотация. В статье рассмотрены вопросы анализа, контроля и фильтрации трафика при помощи глубокой инспекции пакетов в сетях операторов связи. Содержится общее описание технологии, а также кратко освещены этапы ее развития. Описываются способы внедрения технологии глубокой инспекции пакетов в сетях связи.

Ключевые слова: глубокая инспекция пакетов, контроль трафика, фильтрация трафика, сетевая безопасность.

Введение

DPI (Deep Packet Inspection) – это совокупное название технологии, позволяющей проводить в режиме реального времени накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого.

Технологии инспекции трафика развивались последовательно, каждая последующая наследовала часть предыдущих механизмов и добавляла новые. На рис. 1 представлены уровни развития технологии.

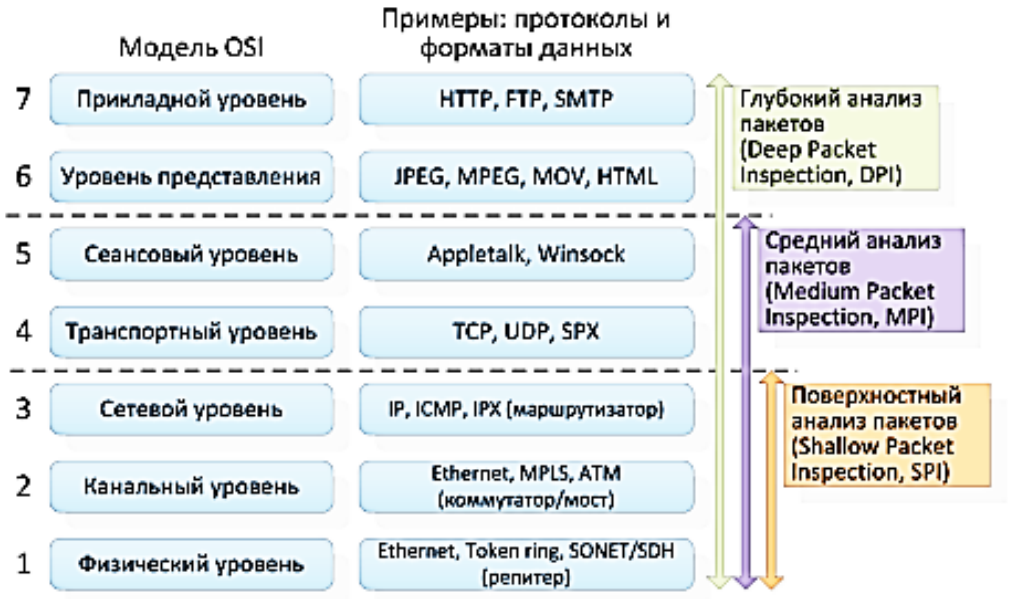


Рис. 1. Уровни развития технологии инспекции трафика

Поверхностный анализ пакетов

SPI (Shallow Packet Inspection) – технология анализа трафика, основывающаяся исключительно на анализе заголовков пакетов уровней L2–L3 модели OSI. SPI осуществляет

проверку только заголовков пакетов для оптимизации маршрутизации, обнаружения попыток злоупотребления сетью и статистического анализа. Если информация пакета находится в «черном списке», пакет отбрасывается. Средства поверхностного анализа пакетов эффективны для межсетевых экранов, которые могут отделять сети друг от друга, разрешать или запрещать трафик в зависимости от выбранного протокола передачи. В связи с тем, что технология работает на канальном и сетевом уровнях модели OSI, к вычислительным ресурсам SPI предъявляются низкие требования, что позволяет обрабатывать большие объемы трафика с высокой скоростью. Технология получила широкое распространение: на ее основе работает большинство межсетевых экранов операционных систем (в частности, в ОС Windows XP/Vista и OS X), маршрутизаторов и других сетевых устройств. На ее основе реализованы сетевые списки контроля доступа на уровне IP-адресов и портов (ACL, Access Control List)). Таким образом, технология SPI хорошо подходит для разграничения доступа извне к отдельным компьютерам и сервисам внутренней сети.

Средний анализ пакетов

MPI (Medium Packet Inspection) – технология анализа трафика, основанная на инспектировании сессий и сеансов связи, инициированных приложением, но устанавливаемых шлюзом-посредником. Также применяется термин «прокси приложений» (application proxy). В рамках этой технологии содержимое пакетов анализируется частично и по предопределенным правилам. Не используются сложные методы анализа типа сигнатурного. Устройства, реализующие функциональность, размещаются между Интернет-провайдером и конечным пользователем. Данные устройства разбирают заголовки вплоть до транспортного уровня и небольшую часть данных пакета для сопоставления разобранной части с некоторым списком разбора (parse list). Списки разбора по сравнению со списками ACL являются более короткими и предоставляют более широкий диапазон действий. Набор протоколов, как правило, очень ограничен. Например, в первых версиях CheckPoint FireWall-1 (CheckPoint FW-1) поддерживались протоколы Telnet, FTP, HTTP, а в Cisco Private Internet Exchange (Cisco PI X) – FTP, HTTP, H.323, RSH, SMTP и SQLNET. В дальнейшем данные наборы незначительно расширялись.

Технология MPI более гибкая по сравнению с SPI и, помимо разграничения доступа, подходит для большего числа задач: кэширование содержимого, анализ сжатого/шифрованного трафика, ограничение функциональности отдельных протоколов путем запрета отдельных команд.

Основной недостаток технологии среднего анализа пакетов – плохая масштабируемость. Это заключается в том, что каждая команда и протокол требуют отдельного шлюза (входного и выходного портов). Кроме того, работа в режиме прокси сильно снижает скорость обработки [1]. Эти факторы ограничивают применение этой технологии на уровне Интернет-провайдеров вследствие необходимости анализа большого числа протоколов и команд.

Глубокий анализ пакетов

DPI (Deep Packet Inspection) – технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэров, DPI анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше.

Одной из важнейших функций DPI является поддержка управления эффективной загрузкой сети путем ограничения тяжелого трафика, например, файлообменных сетей P2P (Peer-to-Peer), потокового видео, а также других ресурсоемких услуг. Средства DPI позволяют выявлять принадлежность потока пакетов к конкретному приложению, а затем при необходимости блокировать или ограничивать его скорость передачи, прогнозировать уровень загрузки каналов тем или иным трафиком, распределять сетевые ресурсы между разными приложениями, не допускать перегрузок и повышать качество обслуживания. Такая возможность появляется за счет того, что технология DPI обеспечивает полный разбор первых пакетов потока трафика. В дополнение применяются статистические методы слежения за характеристиками потока.

Например, из HTTP-трафика легко извлекаются URL запрашиваемых страниц. Далее они могут использоваться для сравнения с «черными» или «белыми» списками или для ведения статистики обращения пользователей к различным ресурсам [2].

Основной метод DPI – проверка сигнатур протоколов и приложений. Под сигнатурой понимается шаблон описания данных, который однозначно соответствует приложению или протоколу. Например, это может быть поиск таких ключевых слов в данных пакета, как BitTorrent, или запросов GET/POST протокола HTTP. Простейшие сигнатуры основаны на URL-адресах в заголовке HTTP, а сам файл сигнатур вендора периодически обновляется. Часть методов DPI основана на статистических и поведенческих критериях анализа потока данных. Именно поведенческий анализ позволяет обнаружить сканирование портов, выполняемое одним источником. В более сложных случаях сигнатура основана на анализе параметров связанных потоков одного приложения. Все эти сигнатуры используются для выявления используемых потоком приложения IP-адресов и транспортных портов, а также для дальнейшего контроля над потоком данных [3].

Среди задач, которые позволяет решить технология DPI, можно выделить следующие: контроль приложений; назначение политик для трафика приложений; оптимизация полосы пропускания; предоставление новых услуг; родительский контроль; защита от DDoS-атак; антиспам; веб-фильтрация; антивирусная защита; управление абонентами; управление квотами; уменьшение P2P; оптимизация видео потоков и HTTP-трафика; визуализация сети; динамический просмотр загрузки сетевых ресурсов и построение отчетов по приложениям, абонентам, базовым станциям.

DPI-технология может быть реализована двумя путями: распределенное и локальное подключение. Распределенная система состоит из пробников (probes) для сбора данных о сетевом трафике и набора его анализаторов (collectors), которые получают данные от пробников. Локальные системы подключаются к конкретному каналу передачи данных. Они могут находиться как на стороне конечного пользователя, так и на стороне шлюза. Локальные системы на стороне конечного пользователя подключаются на уровне сетевой карты пользователя. В то время как локальные системы на стороне шлюза подключаются в точке, которая является единственным выходом в глобальную сеть для некоторой локальной подсети.

Как правило, DPI-система устанавливается на границе сети оператора таким образом, чтобы весь трафик, который покидает сеть или входит в нее, мог анализироваться этой системой. На рис. 2 представлено одно из типовых решений подключения DPI-системы на границе сети оператора.

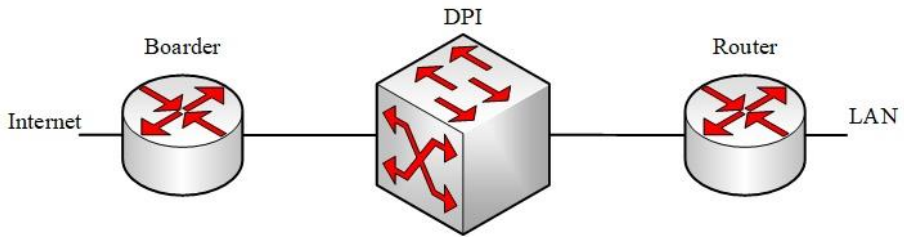


Рис. 2. Типовое решение подключения DPI системы в сеть

Для решения специфических задач систему глубокого анализа пакетов устанавливают не на границе сети, а ближе к конечным пользователям, например, на уровень BRAS/CMTS/GGSN/. Это может быть полезно тем операторам, которые по ряду причин помимо контроля внешних каналов хотят решать задачу контроля внутренних [4].

DPI-системы часто используется провайдерами для контроля трафика, а иногда и для блокировки некоторых протоколов или сайтов (целиком или отдельно взятые страницы). С помощью глубокой инспекции пакетов можно определить, какое приложение сгенерировало или получает данные, и на основании этого предпринять какое-либо действие. Кроме того, DPI-система может обнаруживать среди общего потока трафика фрагменты, соответствующие компьютерным вирусам и блокировать их, повышая тем самым безопасность сети. Технология также позволяет демонстрировать пользователю рекламу в зависимости от содержимого его пакетов.

Заключение

Системы глубокого анализа пакетов позволяют операторам в режиме реального времени проводить анализ пакетов на всех уровнях модели OSI. Помимо изучения пакетов по неким стандартным параметрам, по которым можно однозначно распознать принадлежность пакета к определенному приложению, например, по формату заголовка или номера порта, технология DPI осуществляет анализ того, как ведет себя трафик. Все это открывает большие перспективы коммерческого использования технологии оперативного перехвата и анализа трафика. Также обеспечивается корпоративная сетевая безопасность и защищенность инфокоммуникаций оператора связи.

DEEP PACKET INSPECTION AS A MEANS OF ANALYSIS AND TRAFFIC FILTRATION

O.A. ROMANENKO

Abstract. This article deals with analysis, control and filtration of traffic using deep packet inspection in the networks of telecom operators. It contains general explanation of technology as well as brief description of stages of development. The ways of implementing of deep packet inspection technology are listed in this paper.

Keywords: deep packet inspection, traffic control, traffic filtration, network security.

Список литературы

1. Гетьман А. И., Евстропов Е.Ф., Маркин Ю. В. // Препринт ИСП РАН. 2015. № 28. С. 7–8
2. Фицов В.В. //. Вестник связи. 2016. № 11. С. 25
3. Фицов В.В. // Первая миля. 2015. № 8. С. 57
4. Гольдштейн Б.С., Фицов В.В. // Вестник связи. 2018. № 09. С. 8

УДК 681.3.06

АНАЛИЗ МЕТОДОВ УВЕЛИЧЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

А.Н. ЩИТЛЯК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 31 октября 2018

Аннотация. Исследованы методы увеличения производительности клиент-серверных приложений. Проведены программные эксперименты, направленные на оценку объема трафика, создаваемого приложениями, количества запросов, обрабатываемых сервером, а также требуемого объема оперативной памяти. Обосновано, что наиболее предпочтительным методом увеличения производительности приложений является вариант, связанный с кэшированием динамических страниц и обработкой статических файлов на стороне клиента.

Ключевые слова: веб-приложение, производительность, быстродействие, кэширование.

Введение

За последние годы Интернет стал важной платформой для получения данных и запуска веб-приложений. Веб-приложения – клиент-серверные приложения, в которых клиент взаимодействует с сервером при помощи браузера. Такие приложения легкодоступны независимо от места, с которого к ним обращаются. Поэтому в настоящее время пользователи все чаще отдают предпочтение веб-приложениям. Это обуславливает повышение требований к этим приложениям, а также к их платформам и средам.

Среда веб-приложений обладает рядом особенностей, среди которых можо выделить следующие:

1. Взаимодействие пользователя и сервера происходит посредством кратковременных и часто повторяющихся запросов.

2. По глобальным телекоммуникационным сетям передаются дополнительные файлы, содержащие в себе медиаконтент, исполняемый код, справочную информацию, что способствует возникновению множества параллельных запросов, повышающих загрузку веб-серверов и каналов связи.

3. Пропускная способность каналов связи между пользователями и сервером может быть ограничена. Этот факт значительно увеличивает время обслуживания каждого клиента по сравнению со временем выполнения программных сценариев.

4. Количество одновременно работающих пользователей может быть очень большим, что требует принятия специфических мер при реализации серверных приложений.

Многие компании затрачивают большое количество времени, усилий и ресурсов на повышение производительности разрабатываемых или используемых ими веб-приложений. Сюда относятся сокращение общего объема страницы и количества объектов на ней, оптимизация кода или увеличение пропускной способности Интернет-соединения. Тем не менее, производительность веб-приложения зависит от полной цепи его доставки, где должно быть оптимизировано каждое звено, начиная с веб-сервера и сетей, соединяющих его с конечным пользователем, и заканчивая различными браузерами и клиентским ПО конечных пользователей.

Таким образом, актуально исследование способов и методов рационального использования аппаратных ресурсов путем разработки и внедрения дополнительных программных средств, модификаций существующего программного кода, улучшающих качество

информационно-вычислительной среды (производительность, требуемый объем оперативной памяти, загруженность каналов связи и т. д.).

Методы увеличения производительности веб-приложений

Объем оперативной памяти – основной ограничивающий фактор для увеличения количества одновременно обслуживаемых пользователей. Это обусловлено тем, что все процессы делят общее ограниченное адресное пространство. При этом скорость выполнения других процессов существенно замедляется, поскольку для хранения swap-файла, эмулирующего недостающую оперативную память, используется жесткий диск.

Значительное влияние на производительность веб-приложений оказывают пропускная способность и время отклика канала связи. Низкая пропускная способность канала связи ведет к увеличению времени доставки страниц пользователям. Как следствие, наблюдается увеличение количества процессов, одновременно находящихся в оперативной памяти и занятых передачей сформированных данных.

Существует множество способов, позволяющих улучшить производительность серверных приложений. В ходе работы исследовались следующие методы увеличения производительности:

1) кэширование данных на стороне сервера;

2) предварительная генерация содержимого веб-страниц в статические файлы;

3) использование многоуровневой архитектуры клиент-сервер [1].

Схема проведения исследований

В ходе экспериментов были задействованы следующие программные средства: Apache 2.4 [2] в качестве веб-сервера, PHP 5.2.5 [3] как язык выполнения серверных сценариев, MySQL 5.6 [4] в качестве сервера системы управления базой данных.

Характеристики тестовой страницы, сформированной PHP-сценарием:

1) 2 js-файла, пять графических файлов, ссылки на два ccs-файла;

2) 30 произвольных записей из таблицы базы данных, содержащей 10000 записей; каждая запись включала в себя ссылку на графический файл, заголовок и случайный текст из 2000 символов;

3) при каждой загрузке страницы создавалась или изменялась одна запись из таблицы базы данных, имеющая ссылку на графический файл и текст.

Технические характеристики: процессор Intel Core i3 2,5 ГГц, объем оперативной памяти 4 ГБ, жесткий диск объемом 500 ГБ (частота вращения шпинделя – 7200 об/мин).

В качестве программы для имитации клиентских обращений была использована программа SIEGE. Она предоставляет разработчикам возможность проверить ресурсоемкость своего кода в условиях, максимально приближенных к реальным. Также SIEGE позволяет имитировать обращения к сайту сразу нескольких пользователей. Количество запросов, отправленных к ресурсу, рассчитывается из общего количества пользователей и количества их обращений к серверу. Например, 20 пользователей, обратившись по 50 раз, создают в общей сложности 1000 запросов. Результат, выводимый программой после тестирования, включает в себя время, затраченное на проверку, общее количество переданной информации (включая заголовки), среднее время ответа сервера, его пропускную способность и число запросов, на которые пришел ответ с кодом 200. Эти данные формируются и выдаются при каждой проверке [5]. Также программа SIEGE позволяет имитировать одновременное обращение к серверу нескольких пользователей.

Варианты повышения производительности

Кэширование данных на стороне сервера. Кэширование позволяет увеличивать производительность веб-приложений за счет использования сохраненных ранее данных: ответов на сетевые запросы или результатов вычислений. Благодаря кэшу, при очередном обращении клиента за одними и теми же данными, сервер может обслуживать запросы быстрее.

Кэширование – эффективный архитектурный паттерн, т. к. большинство программ часто обращаются к одним и тем же данным и инструкциям.

Суть кэширования на стороне сервера заключается в том, чтобы записать все, что происходит на сервере, в файл, сохранить его и при последующем обращении этого либо любого другого пользователя к этой странице предоставить ему статичную копию. В результате происходит не только ускорение загрузки страниц, но и снижение нагрузки на сервер и базу данных.

В ходе эксперимента осуществлялось кэширование результатов запросов к базе данных в файлах. В результате исследований количество обращений к базе данных сократилось на 70 %. Данные кэша уничтожались при изменении записей базы данных и не имели времени актуальности. Весь кэш очищался при добавлении или удалении одной или нескольких записей. При изменении одной или нескольких записей БД удалялись только страницы, содержащие изменяемые записи. Если серверный скрипт при обращении в кэш не находил нужной ему записи, то производился запрос к базе данных и его результаты сохранялись в кэше.

Предварительная генерация содержимого в статические файлы. Веб-запросы пользователей к статическим страницам обрабатываются быстрее и требуют меньше накладных расходов (необходимость использования базы данных, объем памяти), чем запросы к динамически формируемым серверными скриптами страницам. В ходе эксперимента реализовывалось обращение к статическим документам *.js. Если такие файлы отсутствовали, то они формировались с помощью специального обработчика страницы ошибок (HTTP-код 404 – Документ не найден).

Использование многоуровневой архитектуры клиент-сервер. Многоуровневая архитектура клиент-сервер – разновидность архитектуры, в которой функция обработки данных вынесена на один или несколько отдельных серверов. Это позволяет разделить функции хранения, обработки и представления данных для более эффективного использования возможностей серверов и клиентов. Достоинствами такой архитектуры являются масштабируемость, конфигурируемость, высокая безопасность и надежность.

При использовании многоуровневой архитектуры клиент-сервер все запросы пользователя принимает клиент. Если пользователь обращается к статическому файлу, то запрос клиентом обрабатывается самостоятельно. При использовании динамически формируемых страниц, клиент формирует запросы к Apache-серверу и, получив от него данные веб-страниц, возвращает их пользователю. Этот подход значительно экономит процессорные ресурсы, поскольку клиент большую часть трудоемких операций (отправка файлов, считывание данных с диска) осуществляет асинхронно с помощью функций ядра операционной системы, получая только сигналы об их завершении.

Подход, в ходе которого осуществлялось кэширование данных на стороне сервера, оказался самым медленным из-за высокой нагрузки на базу данных. Наилучшим оказался подход, заключающийся в предварительной генерации содержимого в статические файлы. Это обусловлено тем, что при использовании данного метода обеспечивается значительная экономия передаваемого трафика и высокое быстродействие. При использовании многоуровневой архитектуры клиент-сервер были достигнуты хорошие показатели при небольшом количестве пользователей, однако при повышении нагрузки быстродействие снизилось из-за частых операций перезаписи файлов [6].

Заключение

Проведены исследования быстродействия веб-приложений при различных вариантах организации взаимодействия его пользователя с клиентом, клиента с сервером и статическими файлами. Показано, что для практического применения наиболее предпочтительным является вариант реализации веб-приложений с кэшированием динамических страниц на стороне клиента и обработкой статических файлов на стороне клиента.

ANALYSIS OF METHODS TO INCREASE PERFORMANCE OF WEB-APPLICATIONS

A.N. SHCHITLYAK

Abstract. The methods for increasing of server applications performance are researched. Program experiments for estimation of traffic volumes formed by applications, quantity of requests processed by the server and demanded volume of operative memory are carried out. It is shown that the most preferable variant, from the point of view of practical application, is the variant with processing of static files on the client side.

Keywords: web-application, performance, speed, caching.

Список литературы

1. Веллинг С., Томсон Л. Разработка клиент-серверного приложения. М., 2012.
2. Уэнрайт П. Apache для профессионалов. СПб, 2010.
3. PHP: Hypertext preprocessor. [Электронный ресурс]. http://php.net/releases/5_2_5.php (дата обращения: 31.10.2018).
4. Дюбау П. MySQL. М., 2014.
5. Siege – утилита для нагрузочного тестирования веб-серверов. [Электронный ресурс]. https://habr.com/post/65128/ (дата обращения: 31.10.2018).
6. Ботыгин И.А., Каликин К.А. Исследование методов увеличения производительности Web-приложений. Томск, 2008.

УДК 004.42:378

РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА В ОБРАЗОВАТЕЛЬНОМ ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Д.А. КУХМАР

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 11 ноября 2018

Аннотация. Разработана универсальная система разграничения прав доступа в образовательном программном обеспечении, способствующая его дополнительной защите, а также более гибкой организации учебного процесса.

Ключевые слова: образование, программное обеспечение, доступ, права, безопасность.

Введение

На сегодняшний день в различных учреждениях образования широко применяется разнообразное программное обеспечение (ПО), существенно повышающее качество учебного процесса. Оно представляется в разнообразных формах: тесты, игры, симуляторы, конструкторы, среды программирования, операционные системы. Такие программы доступны для использования на большинстве существующих платформ [1].

Важную роль в образовательном ПО играет разграничение прав доступа – совокупностьправил, регламентирующих порядок и условия доступа пользователя к объектам ПО (информации, носителям, процессам, другим ресурсам). Данные права определяют набор разрешенных над указанными объектами действий, обеспечивая тем самым дополнительную защиту ПО и баз данных, а также более гибкую организацию учебного процесса. В различных вариациях образовательного ПО используются разные схемы прав доступа, позволяющие эффективнее решать задачи конкретной образовательной программы.

Цель работы – создание универсальной системы разграничения прав доступа в образовательном ПО на примере образовательного приложения, используемого на кафедре ИКТ БГУИР.

Анализ систем прав доступа в существующем образовательном ПО

Наличие системы прав доступа в образовательном ПО и ее реализация зависят от его типа и задач, для решения которых оно было создано. Программные продукты, используемые в образовательном процессе, разделяются на следующие группы.

1. Образовательное ПО для детей. Чаще всего представляет собой игру с элементами обучения. Используется, в основном, дома или в учреждениях дошкольного образования. Примеры – GOcompis, Agnitus.

2. Системы контроля знаний – наиболее популярная группа образовательного ПО, в которую входят отдельные программы или комплексы для проверки знаний учащихся в виде тестов с различными вариантами ответа. Используются повсеместно: от учреждений среднего и высшего образования до специализированных курсов при организациях. Примеры – WebWorK [2], Экзаменатор.

3. Базы данных образовательной информации – группа программ, позволяющая собирать подборки образовательных статей, книг, журналов и читать их. Примеры – TED, Универсариум.

4. Интерактивные образовательные среды. Предназначены для проведения виртуальных экспериментов, моделирования процессов, обучения техникам в интерактивном режиме.

Используются в основном в учреждениях среднего и высшего образования. Примеры – GeoGebra, Pascal ABC.NET.

5. Симуляторы, конструкторы, среды программирования – ПО для профессионального моделирования. Как правило, оно используется для подготовки специалистов, поэтому основная область его распространения – предприятия и ВУЗы. Примеры – MathCAD, MATLAB.

6. Операционные системы –дистрибутивы профессиональных операционных систем, в которых оставлены только функции и программы, предназначенные для обучения по тому или иному направлению. Примеры – Edubuntu, Windows 10 for Education.

В зависимости от того, к какой группе принадлежит конкретное ПО и где оно используется, в нем могут применяться следующие разновидности систем разграничения прав доступа.

1. Полный доступ пользователя. В данном случае в ПО не предусмотрены администраттивные привелегии. Пользователю по умолчанию предоставлен набор прав, которые он не может отредактировать.

2. Демо-режим. Эта система практически полностью схожа с предыдущей, за исключением того, что пользователю в этом случае предоставлен только ограниченный набор функций ПО.

3. Администратор-Пользователь. В рамках этой системы пользователям могут предоставляться административные привелегии, которым соответствует набор прав, позволяющих ему редактировать данные и свойства образовательного ПО, а также в некоторых случаях предоставлять определенный набор прав пользователям с более низкими привелегиями.

4. Администратор-Редактор-Пользователь. Данная система во многом схожа с предыдущей, за исключением того, что доступ к данным (например, новым образовательным материалам) может предоставлять пользователь с привелегиями редактора (например, лаборант ВУЗа).

Исходя из вышеизложенной классификации, был проведен анализ наиболее популярных образовательных приложений, используемых в ВУЗах с техническим профилем. Результаты анализа представлены в таблице.

Сравнительный анализ образовательного ПО, используемого в технических ВУЗах

Название образовательного ПО	Группа образовательного ПО	Система разграничения прав доступа
MathCAD	Симуляторы, конструкторы, среды программирования	Демо-режим; полный доступ пользователя
MATLAB	Симуляторы, конструкторы, среды программирования	Демо-режим; полный доступ пользователя
Electronic Workbench	Симуляторы, конструкторы, среды программирования	Демо-режим; полный доступ пользователя
Программы для проведения лабораторных работ собственной разработки ВУЗа	Интерактивные образовательные среды	Полный доступ пользователя
OrCAD	Симуляторы, конструкторы, среды программирования	Демо-режим; полный доступ пользователя
Cisco Packet Tracer	Интерактивные образовательные среды	Демо-режим; администратор-пользователь
AutoCAD	Симуляторы, конструкторы, среды программирования	Демо-режим; полный доступ пользователя
Edubuntu	Операционные системы	Демо-режим; администратор-редактор-пользователь
Windows 10 for Education	Операционные системы	Демо-режим; администратор-редактор-пользователь
Microsoft Visual Studio	Симуляторы и конструкторы	Демо-режим; полный доступ пользователя
SQL Server Management Studio	Симуляторы, конструкторы, среды программирования	Демо-режим; администратор-редактор-пользователь
Онлайн-библиотека ВУЗа	Базы данных образовательной информации	Администратор-редактор-пользователь

Исходя из проведенного анализа, можно сделать вывод о том, что большинство образовательного ПО, используемого в технических ВУЗах не имеет системы разграничения

прав доступа, достаточно удобной для построения гибкого учебного процесса. И если в случае со сторонним ПО модификации либо невозможны, либо сложны и дорогостоящи, то в случае с собственным ПО ВУЗа ситуацию возможно исправить путем разработки универсальной системы разграничения прав доступа.

Реализация универсальной системы разграничения прав доступа на примере образовательного ПО кафедры ИКТ БГУИР

Для разработки универсальной схемы разграничения прав доступа необходимо определить основные проблемы, которые несет за собой отсутствие такой системы. Среди таковых можно выделить следующие.

1. Несанкционированный доступ к информации, временно или постоянно недоступной пользователю.

2. Отсутствие возможности проведения знакомства с ПО через временное отключение некоторых функций (демо-режим).

3. Нарушение функционирования ПО путем изменения его базовых настроек.

Решение этих проблем для ПО ВУЗа может быть обеспечено путем комбинирования систем типа «Демо-режим» и «Администратор-Пользователь». При применении системы типа «Демо-режим» можно проводить занятия, направленные на знакомство студентов с принципом работы ПО, а при использовании системы типа «Администратор-Пользователь» – занятия, на которых необходимо обеспечить ограниченный доступ к данным этого ПО.

Для реализации такой комбинированной системы необходимо решить следующие задачи.

1. Определить набор параметров и операций, доступных в демо-режиме и в режиме пользователя.

2. Определить принцип контроля доступа.

3. Определить типы файлов и каталогов, доступных в различных режимах.

В демо-режиме предлагается запретить доступ к файловой системе, оставив доступными лишь несколько образовательных моделей. Кроме того, необходимо запретить доступ к базовым параметрам ПО, от которых зависит их стабильная работа (например, к настроечным коэффициентам). Все это позволит без последствий для ПО и его данных провести первоначальное обучение пользователей программы.

В режиме «Пользователь» предлагается запретить редактирование и сохранение исходных файлов программы (например, настроечных файлов, относящихся к разным лабораторным работам), при этом оставив возможность открытия таких файлов, а также вывода результатов работы в файл, сохраняемый в определенный доступный каталог. Доступ к редактированию базовых параметров приложения зависит от широты их применения: если во время работы они остаются неизменными, либо меняются очень редко, то лучше заблокировать возможность редактирования в режиме «Пользователь».

В режиме «Администратор» доступны все параметры, файлы, операции и каталоги. При этом доступ к данному режиму осуществляется через ввод логина и пароля либо только пароля.

Учитывая все вышеописанное, можно заключить, что наиболее удобный принцип контроля доступа – мандатный. Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для объектов и выдаче разрешений (допуска) субъектам на обращение к объектам такого уровня конфиденциальности [3]. В этом случае в ПО должен быть предусмотрен набор переменных и условий, которые в зависимости от значений переменных открывают либо закрывают доступ к объектам программы.

Немаловажным моментом является хранение и редактирование пароля Администратора ПО. В рамках ПО ВУЗа, когда зачастую нет возможности хранить такие данные на веб-серверах, предлагается иметь встроенный в ПО базовый пароль в открытом или зашифрованном виде, который затем можно изменить. Измененный пароль в таком случае предлагается хранить в реестре операционной системы, куда, как правило, запрещен доступ обычным пользователям.

Предложенная система разграничения прав доступа на данный момент внедрена в разрабатываемый на кафедре ИКТ БГУИР комплекс моделирования сигналов и функциональных звеньев ModelSoft и зарекомендовала себя достаточно эффективной для обеспечения гибкости учебного процесса.

Заключение

Проведен сравнительный анализ схем разграничения прав доступа в существующем образовательном ПО. Установлено, что существующее образовательное ПО в большинстве случаев не имеет эффективной системы разграничения прав доступа.

Предложена система разграничения прав доступа в образовательном ПО, используемом на кафедре ИКТ БГУИР.

DISTRIBUTION OF ACCESS RIGHTS IN EDUCATIONAL SOFTWARE

D.A. KUKHMAR

Abstract.

A universal system of access rights in the educational software has been developed, providing it's additional protection for software and databases and more flexible organization of the educational process.

Keywords: education, software, access, rights, security.

Список литературы

1. Annetta L., [etc.] Computers and Education, 2014. №53, P. 74–85.
2. Pierre Tchounikine. Computer Science and Educational Software Design: A Resource for Multidisciplinary Work in Technology Enhanced Learning. Springer Science & Business Media, 2011.
3. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

UDC 004.056.5

AUDIT OF INFORMATION SECURITY OF TELECOMMUNICATION NETWORKS OF CREDIT AND FINANCIAL INSTITUTIONS

S.N. PETROV, A.M.E. ELBUAISHI, T.A. PULKO

Belarusian state university of informatics and radioelectronics, Republic of Belarus

Submitted 20 November 2018

Abstract. The urgency of the audit of credit and financial institutions telecommunication networks conducting, associated with the increase of the network infrastructure load and the increase of the remote banking systems' users number is shown. The information security auditing standards are analyzed. The basic recommendations on networks audit conducting are presented.

Keywords: information security audit, ISO/IEC 27001, network security, credit and financial institutions, penetration test.

Introduction

Information security audit is carried out in order to determine the information system's security compliance with the standards requirements, external or internal, and also to determine the degree of protection of the information system from actual informational security threats.

There are international (ISO/IEC 27001: 2013, ISO/IEC 27005: 2010, ISO/IEC 27033, PCI DSS), as well as industry and national regulations on information security for the system of credit and financial institutions (banks). Technical control of the security of information assets is carried out using special software and hardware systems (vulnerability scanners).

In addition to bank, there are non-bank credit and financial institutions, as well as non-credit financial institutions that operate on the money market and specialize in one or more banking operations. These include leasing companies, credit unions, investment companies (funds), insurance companies, pension funds and charitable funds, collectors firms, pawnshops, trust companies, billing and clearing centers. The annual penetration testing is required from the listed above organizations, depending on the volume of committed financial transactions per day (excepting microfinance organizations, consumer credit cooperatives and pawnshops).

This sphere is characterized by widespread use of information technologies, a large number of individual clients and high attractiveness for fraudsters. It resulted in the fact that in July 2018, Central Bank of the Russian Federation made mandatory annual penetration testing [1] and analysis of information security vulnerabilities of information infrastructure facilities (for the banking sector of the Russian Federation). The application software vulnerabilities analysis will be carried out by the licensed organizations.

Thus, conducting an audit is one of the important links in the chain of information security.

Specificity of computer network security audit

The ISO/IEC 27001 certificate [2] is a prerequisite for participation in many government procurement, auctions and tenders, it provides additional benefits to certificate holders, for example, it makes possible to export software to other countries. Certification involves the following steps: preparation, certification readiness verification by experts, certification check, certificate issuance. Such work is usually performed by a third-party company with the relevant experience. Also, in order to receive a certificate, it is necessary to conduct training of the staff designated as responsible

for maintaining the information security management system documentation. As a result – the high cost of certification.

In this work, the specific aspects of the ISO/IEC 27001 standard connected with network security audits, as well as the tools for conducting technical controls will be considered

In the ISO/IEC 27001 standard there are 4 information security objectives, interconnected in data networks:

Access control. Users should only access those networks and network services where they have authorization for.

Physical security and protection from natural threats. Cable protection. Supply cables, transmitting data cables or ensuring the information services operation cables should be protected from interception, interference or damage.

Information sharing security. Networks must be managed and monitored to protect information in systems and applications. Security mechanisms, service levels and management requirements should be defined for all network services and included in network maintenance agreements. Different groups of information services, users and information systems should be separated in networks. The information transmitted by electronic communications must be adequately protected.

Acquisition, development and maintenance of systems. Information used by application services transmitted over public networks should be protected from fraudulent activities, claims connected with the breach of contractual obligations, and unauthorized disclosure and modification.

Today, data is transmitted through the internal networks of banks, mail and file systems, videoconferencing systems and automated banking systems, enterprise resource management systems and customer relationship management. External networks connect banks to data centers, outsourced contact centers, SWIFT networks, etc. There has been a steady increase in the number of users of mobile and Internet banking. For example, according to statistics from the National Bank of the Republic of Belarus [3], an increasing number of Belarusians prefer to use Internet banking (3.41 million users) and mobile banking (1,22 million) to make payments and transactions (Fig. 1).

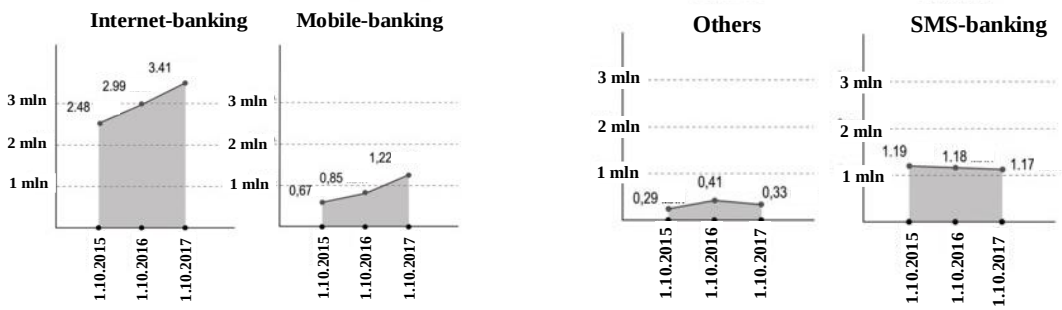


Fig. 1. Trends in using remote banking channels

The instrumental study of the network infrastructure is carried out by using software and hardware and software security analysis: security scanners, integrity monitoring systems, code analysis systems, distributions of pentest. To simplify the analysis, it is necessary to carry out a detailed elaboration, that is a division of the network structure into its constituent elements. There are several network segments, such as the demilitarized zone, local VPN-pool address, external addressing segments, closed segments (for example, bank-client segments, automated workstations of operators, videoanalytics, billing).

To conduct a perimeter inventory for the selected segments, that includes checking the methods and channels of Internet access, used external addresses, systems available from the Internet, services and protocols, authentication methods.

Conclusion

The information security audit is an effective tool to obtain the objective assessment of the current level of protection of a credit and financial institution from various informational threats. Improving the audit process will allow to increase the level of information security. The detailed description of the company's network infrastructure is one of the key aspects of the computer and telecommunication networks audit.

References

1. Proekt popravok v Polozhenie Banka Rossii № 382-P «O trebovanijah k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv i o porjadke osushhestvlenija Bankom Rossii kontrolja za sobljudeniem trebovanij k obespecheniju zashhity informacii pri osushhestvlenii perevodov denezhnyh sredstv». [Electronic resource]. URL: http://regulation.gov.ru/Files/GetFile?fileid=c9178fad-6c64-4eb7-9c57-43b1a8528a5b (date of access: 22.10.2018).
2. ISO/IEC 27001:2013 Informacionnye tehnologii - Metody zashhity - Sistemy menedzhmenta informacionnoj bezopasnosti – Trebovanija. [Electronic resource]. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (date of access: 22.10.2018).
3. O populjarnyh kanalah i budushhem DBO. [Electronic resource]. URL: https://dev.by/news/o-populyarnyh-kanalah-i-buduschem-dbo (date of access: 22.10.2018).

СВЕДЕНИЯ ОБ АВТОРАХ

1. Алисеенко Маргарита Александровна – магистрант кафедры инфокоммуникационных технологий БГУИР

2. Альбуэши Анас Муфтах Эмехммед – магистрант кафедры инфокоммуникационных технологий БГУИР

3. Аль-Рубайи Исса Мухаммед Мишааль – магистрант кафедры инфокоммуникационных технологий БГУИР

4. Аль-Субаи Амжед Карим Туама – магистрант кафедры инфокоммуникационных технологий БГУИР

5. Астровский Иван Иванович – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

6. Белан Владислав Анатольевич – магистрант кафедры инфокоммуникационных технологий БГУИР

7. Волков Кирилл Аркадьевич – к.т.н., с.н.с. РУП «Научно-производственный центр многофункциональных беспилотных комплексов» Национальной академии наук Беларуси

8. Госса Артем Игоревич – магистрант кафедры инфокоммуникационных технологий БГУИР

9. Грицкевич Владислав Игоревич – магистрант кафедры защиты информации БГУИР

10. Данильчук Владислав Сергеевич – магистрант кафедры инфокоммуникационных технологий БГУИР

11. Зеленин Александр Сергеевич – старший преподаватель кафедры инфокоммуникационных технологий БГУИР

12. Кийко Вадим Николаевич – магистрант кафедры инфокоммуникационных технологий БГУИР

13. Конопелько Валерий Константинович – д.т.н., профессор кафедры инфокоммуникационных технологий БГУИР

14. Курилович Андрей Владимирович – старший преподаватель кафедры инфокоммуникационных технологий БГУИР

15. Кухмар Дмитрий Александрович – магистрант кафедры инфокоммуникационных технологий БГУИР

16. Лагутин Андрей Евгеньевич – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

17. Лопато Андрей Геннадьевич – магистрант кафедры инфокоммуникационных технологий БГУИР

18. Лоскот Сергей Юрьевич – магистрант кафедры инфокоммуникационных технологий БГУИР

19. Лукашевич Сергей Александрович – старший преподаватель кафедры инфокоммуникационных технологий БГУИР

20. Михейчик Александр Дмитриевич – магистрант кафедры инфокоммуникационных технологий БГУИР

21. Мойсиевич Юрий Сергеевич – магистрант кафедры инфокоммуникационных технологий БГУИР

22. Мурашко Антон Вадимович – магистрант кафедры инфокоммуникационных технологий БГУИР

23. Нгуен Ань Туан – аспирант кафедры инфокоммуникационных технологий БГУИР

24. Нгуен Хонг Куан – магистрант кафедры инфокоммуникационных технологий БГУИР

25. Петров Сергей Николаевич – к.т.н., доцент кафедры защиты информации БГУИР

26. Полуян Татьяна Владимировна – магистрант кафедры инфокоммуникационных технологий БГУИР

27. Пригон Анна Николаевна – магистрант кафедры инфокоммуникационных технологий БГУИР

28. Пулко Татьяна Александрова – к.т.н., доцент кафедры защиты информации БГУИР

29. Романенко Ольга Анатольевна – магистрант кафедры инфокоммуникационных технологий БГУИР

30. Рощупкин Яков Викторович – старший преподаватель кафедры защиты информации БГУИР

31. Саломатин Сергей Борисович – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

32. Сороко Максим Викторович – магистрант кафедры инфокоммуникационных технологий БГУИР

33. Тарченко Надежда Владимировна – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

34. Урядов Владимир Николаевич – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

35. Филимончик Роман Анатольевич – магистрант кафедры инфокоммуникационных технологий БГУИР

36. Хацкевич Олег Александрович – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

37. Хоменок Михаил Юлианович – к.т.н., доцент кафедры инфокоммуникационных технологий БГУИР

38. Цветков Виктор Юрьевич – д.т.н., заведующий кафедрой инфокоммуникационных технологий БГУИР

39. Чепикова Виолетта Викторовна – ассистент кафедры инфокоммуникационных технологий БГУИР

40. Шакир Мухаммед Музахем Шакир – магистрант кафедры инфокоммуникационных технологий БГУИР

41. Щитляк Андрей Николаевич – магистрант кафедры инфокоммуникационных технологий БГУИР

42. Яворко Юлия Евгеньевна – магистрант кафедры инфокоммуникационных технологий БГУИР