6. Frequency and Network Planning Aspects of DVB-T2. Report TECH 3348 − EBU, Switzerland, Geneva, May 2011. pp. 33-35.
7. ETSI ES 201 980 V4.1.1 Digital Radio Mondiale (DRM). System Specification, France, 2014. pp. 134-142, 145-148.
8. Recommendation ITU-R SM.1541-3 Unwanted emissions in the area of off-frequency emission. International Telecommunication Union, Geneva, 2011. pp. 40-43, 47-48.
9. Recommendation ITU-R SM.1046-2 Determination of the radio-frequency spectrum usage and the radio system efficiency. International Telecommunication Union, Geneva, 2011. pp. 1-4.
10. Yu.B. Zubarev, M.I. Krivosheev, I.N. Krasnoselsky, *Tsifrovoe televizionnoe veshchanie. Osnovy, metody, sistemy* [Digital television broadcasting. Fundamentals, methods, systems]. Moscow, Scientific Research Institute of Radio (NIIR), 2001. 568 p.

Received 05.09.2017

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 681.322

СТЕГАНОГРАФИЧЕСКОЕ ВНЕДРЕНИЕ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ В СЕМПЛЫ ЦИФРОВЫХ ЗВУКОВЫХ СИГНАЛОВ

Алексеев А.П.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: apa_ivt@rambler.ru

Общепринятым подходом при скрытой передаче информации в мультимедийных контейнерах является использование лишь самых младших разрядов цифровых данных (метод LSB). В работе описывается способ внедрения дополнительной информации в звуковые файлы, при котором используются не только последние (младшие) разряды отсчетов, но и старшие. Приведено экспериментальное обоснование возможности такого внедрения. При этом установлена зависимость слухового восприятия человека от номера использованного разряда отсчёта и временного интервала появления информационных семплов. Повышение криптостойкости описанного подхода достигнуто за счет псевдослучайного выбора звукового канала, номера отсчета, номера использованного разряда.

Ключевые слова: отсчёты, формат, последний значащий бит, информационный семпл, маскирующий семпл, старшие разряды, генератор псевдослучайных чисел

Введение

Совершенствование методов защиты информации идет по пути создания большого числа труднопреодолимых барьеров. Эти барьеры включают в себя криптографию, стеганографию, распыление информации в пространстве и времени [1-2]. Совершенствование каждого из перечисленных барьеров идет непрерывно. В данной работе рассматривается новый стеганографический способ скрытой передачи информации в звуковом файле формата WAV. Особенностью рассматриваемого способа является то, что сокрытие осуществляется не только в самом последнем (младшем) разряде цифрового отсчета (семпла), но и в старших разрядах.

Такой подход противоречит классическому способу внедрения данных, который называется LSB (Least Significant Bit) и согласно которому внедрение дополнительной информации должно производиться лишь в младшие разряды [3]. Возможность незаметного внедрения информации в старших разрядах звукового файла подтверждена экспериментальными исследованиями.

Состояние рассматриваемого вопроса

Существует большое число способов внедрения дополнительной информации в мультимедийные контейнеры. Возможно незаметное размещение скрытой информации на HTML-страницах с помощью непечатаемых знаков, в TCP-пакетах за счёт изменения длины пакетов [4], в MIDI-файлах благодаря незначительному изменению громкости и

длительности звучания нот [5], в текстовых файлах посредством использования дополнительных пробелов [6], в видеоклипах путем внедрения информации в отдельные кадры.

Скрытно передать информацию можно за счет использования особенностей формата мультимедийных контейнеров с помощью форматной стеганографии [7], а также с помощью других методов [8-9]. При этом скрывать можно не только текстовые сообщения, но и использовать более экзотичные варианты внедрения, например скрытая передача звукового файла в графическом файле. Примером такого внедрения может служить стегосистема для сокрытия цифровых данных в графических или звуковых файлах [10].

Идея скрытой передачи одного рисунка в другом рисунке [10] состоит в том, что исходный рисунок (см. рис. 1) и графический контейнер (см. рис. 2) разбивают на блоки одинакового размера (в рассматриваемом примере размер каждого блока 8×8 пикселей, а число блоков в рассматриваемом случае равно 16). Каждый блок передаваемого рисунка заменяют блоком контейнера, который имеет наибольшее сходство с заменяемым блоком.

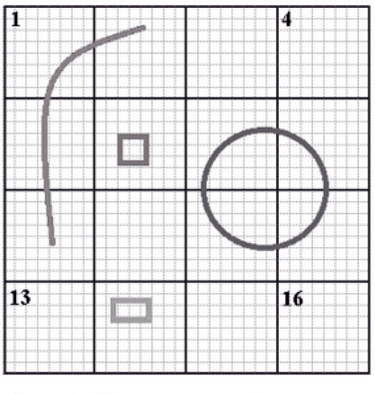

Рис. 1. Передаваемый рисунок

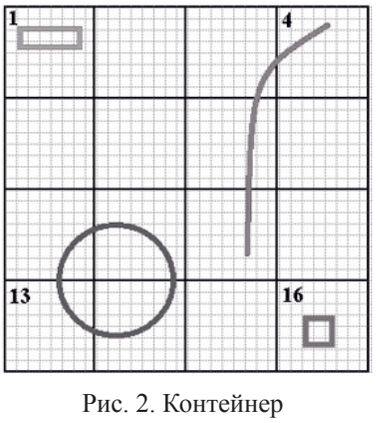

Рис. 2. Контейнер

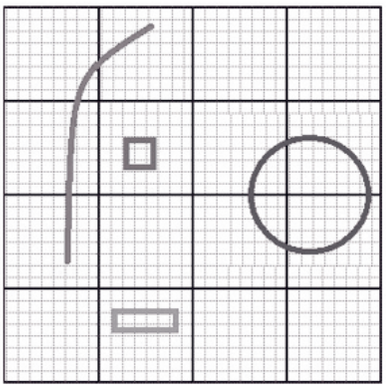

Рис. 3. Принятый рисунок

На принимающую сторону передают номера блоков контейнера в нужной последовательности. Для показанных рисунков последовательность такая: 3-4-2-2-7-16-9-10-11-2-13-14-2-1-2-2. Нумерация блоков выполнена слева направо и сверху вниз.

Таким образом, передаваемый рисунок заменяется числами (индексами). Принятый рисунок (см. рис. 3) будет отличаться от переданного, так как он состоит из фрагментов другого рисунка. Понятно, что воспроизведение на приеме будет тем точнее, чем больше найдётся полностью совпадающих блоков в передаваемом рисунке и контейнере. В приведённых рисунках полностью совпадают незаполненные (пустые) блоки, а также блок 6 передаваемого рисунка полностью идентичен блоку 16 контейнера.

Очевидно, что вид контейнера должен быть известен на передающей и приёмной сторонах.

Внедрение данных в старшие разряды семпла

Идея стеганографического внедрения дополнительной информации в семплы цифровых звуковых сигналов состоит в том, что зашифрованную скрываемую информацию в двоичной форме побитно внедряют в семплы путём замены бита семпла на скрываемый бит дополнительной информации.

Причём используемые для внедрения дополнительной информации звуковые каналы, номера разрядов семплов, интервал между используемыми для внедрения семплами выбирают в соответствии с секретным псевдослучайным ключом и с учётом психофизических характеристик человеческого слуха.

Подтверждением высокой криптостойкости заявляемого способа скрытой передачи информации являются следующие соображения.

Для извлечения информации из контейнера без ключа криптоаналитик должен решить следующие задачи:

– определить, в каких звуковых каналах имеются семплы с внедренной информацией;

– определить, в какие семплы произведено внедрение (разделить семплы на информационные и маскирующие);

– определить, в какие разряды используемых (информационных) семплов произведено внедрение;

– дешифровать полученную последовательность извлеченных битов.

Такая задача является нетривиальной и вычислительно сложной. При условии, что ключ является криптографически надежным, используется современный шифр [11], данная задача неразрешима на данном уровне науки и техники за приемлемое время.

Решение задачи осложняется тем, что выбор звуковых каналов (левый-правый, первый-пятый-третий…), номеров используемых семплов, номеров разрядов происходит по псевдослучайному закону. Два соседних внедряемых бита могут оказаться в разных звуковых каналах, в разных семплах, а используемый разряд семпла непредсказуем. Предварительное шифрование внедряемой информации в ещё большей степени усложняет криптоанализ.

С помощью рассматриваемого способа можно организовать скрытую передачу (или хранение) различного вида информации: текстовой, графической, звуковой. В любом случае скрываемая информация должна быть перед внедрением преобразована в цифровой вид.

Реализация рассматриваемого способа скрытой передачи информации

Наиболее наглядно проиллюстрировать реализацию данного технического решения можно на примере скрытого внедрения текста (сообщения) в оцифрованный звуковой сигнал.

Внедряемый текст целесообразно предварительно зашифровать, а затем преобразовать в двоичный код (это можно сделать и в обратной последовательности: преобразовать текст в двоичный код, а затем зашифровать). Известно большое число алгоритмов шифрования, некоторые из которых стали национальными стандартами [11].

В соответствии с секретным ключом выбирается для внедрения один из каналов звукового файла. Будем считать, что в данный момент используется стереозвучание и для внедрения сеансовым ключом определён левый звуковой канал.

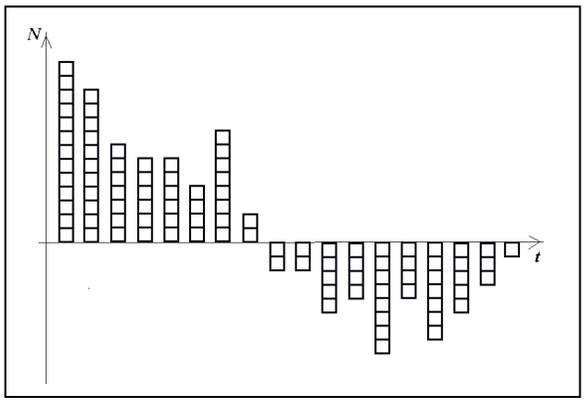

Рис. 4. Оцифрованный звук

На рис. 4 схематично показана диаграмма некоторого оцифрованного звука. В формате звука WAV при глубине звука (разрядности) более 8 отсчеты представляют положительными и отрицательными целыми числами. Семплы на рисунке условно показаны в виде многоразрядных двоичных чисел (младшие разряды располагаются вблизи оси времени). Семплы, расположенные в первом квадранте, представляют положительными числами. Отсчеты из четвертого квадранта представляют отрицательными числами. Высота семплов пропорциональна интенсивности звука.

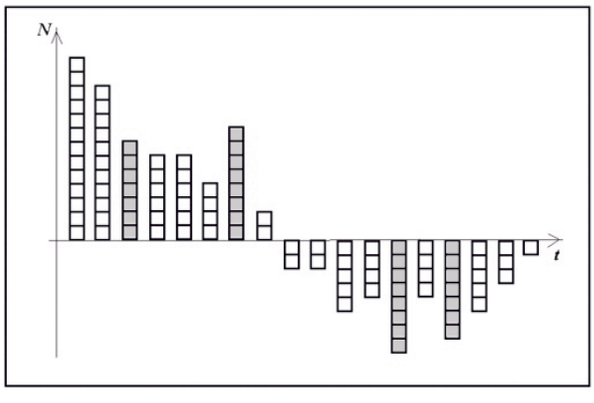

Рис. 5. Информационные семплы

На рис. 5 семплы, в которые производится внедрение дополнительной информации, заштрихованы. Такие семплы можно назвать информационными. Остальные семплы можно назвать маскирующими (неиспользуемыми), так как в них нет скрываемой информации.

Разделение семплов на информационные и маскирующие происходит в соответствии с секретным ключом. На рис. 6 темной штриховкой показаны разряды семплов, в которые производится внедрение скрываемой информации.

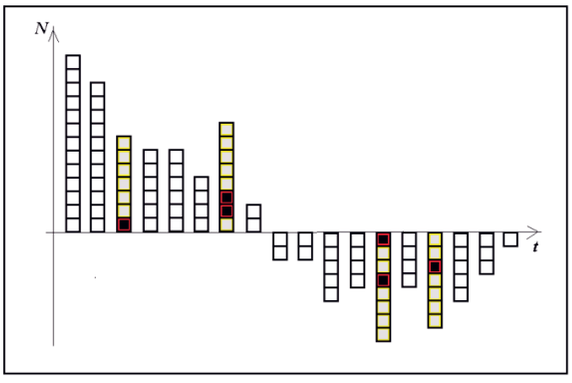

Рис. 6. Выбранные разряды семплов

Таким образом, для технической реализации заявляемого способа потребуется три генератора псевдослучайных чисел.

С помощью первого генератора псевдослучайных чисел (ГПСЧ) на передающей стороне выбирается звуковой канал для внедрения. Например, для стереофонической системы последовательность, формируемая ГПСЧ 1, может быть такой: левый-левый- правый-левый-правый-правый… Для шестиканального звукового файла последовательность используемых каналов может быть такой: 3-4-2-2-6-1-2-5-5-6-3-1…

С помощью ГПСЧ 2 производится деление всех файлов на информационные и маскирующие. Удобнее всего формировать псевдослучайные числа, которые показывают, сколько маскирующих семплов располагается после информационного семпла. Например, число 0 говорит о том, что два информационных семпла следуют друг за другом. Число 1 говорит, что между информационными семплами располагается один маскирующий семпл. Число 2 сигнализирует, что между информационными отсчетами находятся два «пустых» семпла, и т.д. Генератор ГПСЧ 3 выбирает разряды отсчётов для внедрения дополнительной информации в выбранный семпл.

Порядок работы устройства на передающей стороне будет таким. Устройство синхронизации после формирования маркера начала работы криптосистемы запускает ГПСЧ 1, который определяет, в какой звуковой канал производится первое внедрение. Затем включается ГПСЧ 2, который выбирает номер информационного семпла. Наконец, срабатывает ГПСЧ 3, который указывает, в какие разряды семпла происходит внедрение дополнительной информации. Естественно, что три аналогичных ГПСЧ с теми же начальными установками и в той же последовательности должны работать на приемной стороне. Этим осуществляется синхронизация выбора звукового канала, номера и разряда семпла.

При ознакомлении с порядком работы генераторов ГПСЧ 2 и ГПСЧ 3 может сложиться впечатление, что все семплы и разряды информационных семплов выбираются по случайному закону. На самом деле существуют ограничения, которые определены на основании экспериментальных исследований психофизических особенностей слуха человека. И эти ограничения заложены в конструкцию генераторов псевдослучайных чисел.

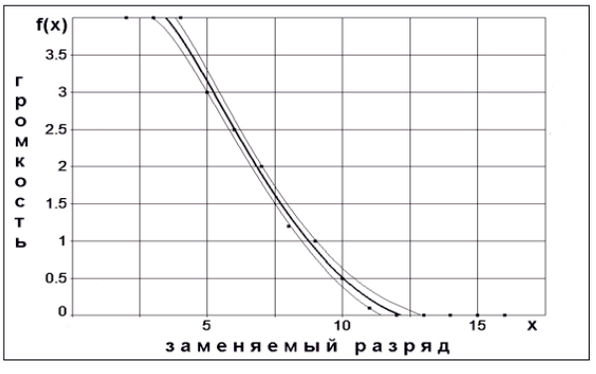

Рис. 7. Зависимость слышимости от номера использованного разряда

На рис. 7 показана зависимость слышимости звукового сигнала $f(x)$ от номера разряда, в который было произведено внедрение дополнительной информации. Были использованы 16-разрядные семплы, причем нумерация разрядов производилась от старших разрядов к младшим (старший разряд имел порядковый номер 1, а младший – номер 16). В экспериментальных исследованиях участвовали 20 студентов, которые оценивали громкость звучания предъявленных 555 файлов по пятибалльной системе (от 0 до 4). Файлы представляли собой запись «тишины» и отличались друг от друга тем, что производилась запись единицы в разные семплы и разные разряды. Наибольшей громкости звучания соответствовал балл 4, а файлу без вложения («полная тишина») соответствовал балл 0.

Рис. 7 показывает, что внедрение единицы в 16, 15, 14 и 13 разряды слушателями не воспринимаются даже при воспроизведении «тишины» (паузы между музыкальными произведениями). Очевидно, что с увеличением громкости звукового сигнала становится допустимым внедрение информации в более старшие разряды.

Экспериментально было установлено, что органолептическое восприятие звука зависит от частоты появления громких звуков. Наличие ред-

ких даже громких звуков человеком не воспринимается из-за инерционности слуха. На рис. 8 показано, как зависит слышимость (громкость звучания) от наличия вложений при изменении интервала между информационными семплами (внедрение осуществлялось в разряд 12).

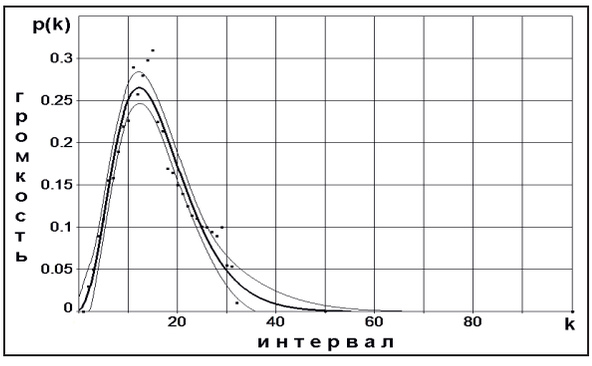

Рис. 8. Зависимость слышимости от интервала между информационными семплами

На рис. 8 видна нелинейная частотная зависимость слуховой системы людей. Наибольшая чувствительность наблюдается на частоте около 3,4 кГц. Это хорошо согласуется с ранее опубликованными данными. Из рисунка также видно, что если между информационными семплами располагается 60-70 маскирующих семплов, то звуковой сигнал не слышен даже при внедрении во фрагменты звукового файла с записью полной «тишины».

Параметры генераторов ГПСЧ 2 и ГПСЧ 3 связаны между собой: чем больше интервал между информационными семплами, тем в более старшие разряды можно внедрять информацию. При выборе параметров ГПСЧ 2 и ГПСЧ 3 рекомендуется ориентироваться на данные таблицы 1, содержание которой нужно трактовать следующим образом.

Таблица 1. Данные для выбора параметров ГПСЧ 2 и ГПСЧ 3

Интервал, k	20	100	1000	10000
Разряд, x	13	11	10	9

Если для настройки выбрать данные из второй колонки, то ГПСЧ 3 должен случайно генерировать числа 13, 14, 15, и 16, то есть во второй строке таблице указан старший разряд семпла, разрешённый для внедрения (напомним, что младший разряд здесь имеет номер 16). При этом ГПСЧ 2 должен генерировать псевдослучайное число, указывающее на число маскирующих семплов, расположенных между двумя соседними информационными семплами. В данном случае это число должно быть 20 и более. Верхнюю границу случайных чисел, генерируемых ГПСЧ 2, выбирают из соображений необходимой криптостойкости и производительности. Чем больше верхняя граница чисел, тем выше криптостойкость, но меньше производительность, то есть в единицу времени передаётся меньшее количество дополнительной информации.

Остальные данные таблицы 1 трактуются аналогично. Например, числа в третьем столбце говорят, что псевдослучайно должны формироваться числа номеров используемых разрядов 11, 12 … 16 и числа маскирующих семплов должны быть более 100. Необходимо также отметить, что таблица 1 составлена с учетом использования фрагмента звуковой картины с минимальной интенсивностью звука (наихудший возможный случай). Это гарантирует отсутствие слышимости вложений в реальных звуковых файлах.

Заключение

Рассмотренный способ следует использовать преимущественно для скрытой передачи текста, ключей, паролей, номеров кредитных карточек или небольших графических файлов (например логотипа фирмы-правообладателя). При его использовании для защиты авторских прав логотип фирмы может быть записан в музыкальное произведение несколько раз. При этом разделение продукта на части не позволить скрыть авторство, так как логотип будет присутствовать во всех фрагментах (во всех подмножествах мультимедийного продукта).

Разработанное техническое решение позволяет выбрать требующееся соотношение между криптостойкостью и производительностью за счёт регулировки генераторов псевдослучайных чисел, отвечающих за выбор звуковых каналов, информационных семплов и разрядов в семплах. Для получения стегосистемы, имеющей максимальную криптостойкость (стегостойкость), следует внедрение производить только в младшие разряды семплов, максимально увеличивая число маскирующих семплов (распылять вложение по всему контейнеру), и по возможности реже использовать каждый звуковой канал.

Максимальная производительность стегосистемы достигается при внедрении в несколько разрядов каждого информационного семпла, наибольшем сокращении числа маскирующих семплов и интенсивном использовании каждого звукового канала. Способ позволяет надежно

защитить авторские права, так как удалить дополнительную информацию в старших разрядах семплов и сохранить приемлемое качество звучания невозможно. Если бы запись велась только в младшие разряды семплов, то можно было бы заполнить их псевдослучайными единицами и нулями.

Литература

1. Алексеев А.П. Информатика для криптоаналитиков. Самара: ИУНЛ ПГУТИ, 2015. – 376 с.
2. Алексеев А.П., Макаров М.И. Принципы многоуровневой защиты информации // ИКТ. Т.10, №2, 2012. – С. 88-93.
3. Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. Основы компьютерной стеганографии. М.: Радио и связь, 2003. – 152 с.
4. Способ стеганографической передачи информации в сети TCP/IP. Патент RU 2463670 № 2010125304/08 (035921. Заявл. 18.06.2010, опубл 10.10.2012, бюл. №23.
5. Алексеев А.П., Аленин А.А. Методы внедрения информации в звуковые файлы формата MIDI // ИКТ. Т.9, №1, 2011. – С. 84-89.
6. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика.-М.: МК-Пресс, 2006. – 288 с.
7. Алексеев А.П., Ванютин А.Р., Королькова И.А. и др. Современные мультимедийные информационные технологии. М.: СОЛОН-Пресс, 2017. – 108 с.
8. Method of transmitting audio information and additional information in digital form. Pat. US 4750173.
9. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding. IBM Systems Journal, No. 35, 1996. – P. 313-336.
10. Cryptosystem for encrypting digital image or voice file. Pat. US 6023511 A.
11. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПБ.: БХВ-Петербург, 2009. – 576 с.

Получено 24.04. 2017

Алексеев Александр Петрович, к.т.н., доцент Кафедры информатики и вычислительной техники Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 375-08-02. E-mail: apa_ivt@rambler.ru

STEGANOGRAPHIC CONCEALMENT OF ADDITIONAL INFORMATION WITHIN DIGITAL AUDIO SAMPLES

Alekseev A.P.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: apa_ivt@rambler.ru

This paper presents a method of hidden information transmission within a WAV sound file. The hidden transmission (or storage) can be used to protect sensitive information such as copyright (the introduction of watermarks), password, key, message, file, etc. A common approach to conceal information in multimedia containers involves using only the lowest bits of digital data (LSB method). The paper describes the method of concealing additional information within sound files using both the lowest and highest bits. An experiment was conducted to prove the applicability of the proposed method. During the experiment statistical data were obtained to determine the effect of hidden bit positioning within a sample and within different time intervals on the human auditory perception. The experiment showed that steganographic strength of the described approach increases if sound channel, sample position and hidden bit position are selected pseudo-randomly.

Keywords: readouts, format, least significant bit, information sample, mask sample, high order digits, pseudo-random number generator

DOI: 10.18469/ikt.2017.15.3.13

Alekseev Alexander Petrovich, Povolzhskiy State University of Telecommunication and Informatics, 77, Moscovskoe shosse, Samara, 443090, Russian Federation; Associate Professor of the Department of Informatics and Computer Technics Department, PhD in Technical Science. Tel.: +78463750802. E-mail: apa_ivt@rambler.ru.

References

1. Alekseev A.P. *Informatika dlya kripto-analitikov* [Informatics for cryptanalysts]. Samara, PSUTI, 2015. 376 p.
2. Alekseev A.P., Makarov M.I. Principy mnogourovnevoj zashhity informacii [Principles of multilevel information security]. *Infokommunikacionnye texnologii*, 2012, no. 2, pp. 88-93.
3. Agranovskij A.V., Devyanin P.N., Xadi R.A, Cheremushkin A.V. *Osnovy kompyuternoj steganografii* [Basics of computer steganography]. Moscow. Radio i svyaz Publ., 2003. 152 p.
4. Orlov V.V., Alekseev A.P. *Sposob steganograficheskoj peredachi informacii v seti TCP/IP* [The method of steganographic information transfer in a TCP / IP network]. Patent RF, no. 2463670, 2012.
5. Alekseev A.P., Alenin A.A. Metody vnedreniya informacii v zvukovye fajly formata MIDI [Methods for introducing information into MIDI sound files]. *Infokommunikacionnye texnologii*, 2011, no.1, pp. 84-89.
6. Konaxovich G.F., Puzyrenko A.Yu. *Kompyuternaya steganografiya. Teoriya i praktika*. Moscow, MK-Press Publ., 2006. 288 p. (In Russian).
7. Alekseev A.P., Vanyutin A.R., Korolkova I.A., Repechko D.A., Mytko S.S. *Sovremennye multimedijnye informacionnye texnologii* [Modern multimedia information technologies]. Moscow, SOLON-Press Publ., 2017. 108 p.
8. Bjiirn Bliithgen. *Method of transmitting audio information and additional information in digital form*. Patent US, no. 4750173.
9. Bender W., Gruhl D., Morimoto N., Lu A.. Techniques for Data Hiding. *IBM Systems Journal*, 1996, no. 35, pp. 313-336.
10. Wei Ming. *Cryptosystem for encrypting digital image or voice file*. Patent US, no. 6023511.
11. Panasenko S.P. *Algoritmy shifrovaniya. Specialnyj spravochnik* [Encryption algorithms. Special reference book]. St.Peterburg, BXV-Peterburg Publ., 2009. 576 p.

Received 24.04.2017

УДК 621.396.94: 004.896

МЕТОДЫ ОЦЕНКИ РАССТОЯНИЙ И КАЧЕСТВА РАДИОЛИНИЙ МЕЖДУ РОБОТАМИ В СОСТАВЕ РОЯ

Кубанов В.П., Ружников В.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: rv@psuti.ru

В статье для координации действий группы роботов перераспределения между ними ролей, создания альтернативных маршрутов передачи информации в случае удаления или потери связи с одним из узлов предлагается постоянный мониторинг расстояний до соседних узлов относительно каждого из роботов, входящего в рой. Приводятся методы оценки расстояний и качества радиолиний, которые могут быть полезны для создания прогнозных моделей и мониторинга состояния роя роботов, объединенных радиосетью.

Ключевые слова: групповая робототехника, ZigBee, IEEE 805.15.4, радиосвязь, RSSI, TOF, LQI, радиосеть

Введение

Основа для теоретической базы групповой робототехники возникла благодаря биологическим исследованиям за насекомыми, в частности за муравьями, пчелами и другими, в среде которых имеет место роевое поведение [1]. Разработка подходов к координации систем, состоящих из большого числа физически простых роботов, привела к возникновению научных направлений – роевого интеллекта, мультиагентных систем [2].

Структура роя предполагает постоянную смену участников и их ролей, что связано с адаптацией роя к окружающей среде, параметры которой заранее не определены [3]. Взаимодействие роботов в группе предполагает поддержание между ее участниками постоянной локальной связи. Для экономии энергетических ресурсов эффективнее обеспечивать связь посредством передачи информации через соседа, который находится в пределах прямой видимости. Таким образом, сеть, состоящую из группы роботов, можно представить