

иболее разнообразные значения интегралов на разных участках числовой оси.

Выводы

Предложен метод шифрования, основанный на замене символов открытого текста двумя вещественными числами. Одно из чисел генерируется с помощью датчика случайных чисел. Особенностью шифра является использование интегральных преобразований для получения второго числа. Другой особенностью описанного шифра является формирование таблицы замен,

в которой символы распылены по числовой оси. Криптоанализ усложняется благодаря генерации двух случайных чисел (значения интеграла и одного из пределов). Секретный ключ определяет форму таблицы замен и вид подынтегральной функции.

Литература

1. Алексеев А.П. Информатика 2007. М.: СОЛОН-ПРЕСС, 2007. – 608 с.
2. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002. – 512 с.

ТЕХНОЛОГИИ ТЕЛЕКОММУНИКАЦИЙ

УДК 621.392

БЕСПРОВОДНЫЕ MESH-СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Легков К.Е., Федоров А.Е.

В настоящее время наиболее распространенной технологией беспроводного доступа, которая повсеместно применяется для передачи большого количества трафика различного вида, является стандарт беспроводных локальных сетей IEEE 802.11. Одним из самых перспективных направлений развития технологии Wi-Fi стали mesh-сети, описываемые в стандарте IEEE 802.11s. В статье рассмотрена возможность применения данного стандарта для сетей специального назначения и работа одного из известных алгоритмов назначения каналов в сетях IEEE 802.11s – Нуасинт с централизованным способом назначения каналов.

Перспективный класс широкополосных беспроводных сетей передачи мультимедийной информации – mesh-сети, которые являются одним из направлений развития технологии Wi-Fi [1] и описываются в стандарте IEEE 802.11s [2]. Одним из главных принципов построения mesh-сети является принцип самоорганизации архитектуры, обеспечивающий такие возможности, как реализацию топологии сети «каждый с каждым»; устойчивость сети при отказе отдельных компонентов; масштабируемость сети; динамическую маршрутизацию трафика; контроль состояния сети и т.д. Mesh-технология становится особенно необходимой при отсутствии проводной инфраструктуры для соединения станций.

Эти положительные качества неуклонно приводят к вопросу о применении таких технологий для обеспечения управления в силовых структурах при выполнении специальных задач. Благодаря низким ценам на оборудование Wi-Fi, а также легкости в установке, возможно его массовое

применение и в организациях специального назначения. Границу автоматизации, как общепринятого способа повышения эффективности функционирования любой системы, можно довести до отдельного сотрудника. Такой процесс давно происходит в армиях и организациях специального назначения ведущих государств мира, в частности в США. В комплект оснащения для каждого сотрудника могут входить вычислительный комплекс, набор датчиков, видео- и инфракрасные камеры, шлем со встроенным монитором, отображающим цифровую карту и местонахождение своих и чужих подразделений, и устройство беспроводной связи. Технология передачи мультимедийных данных в условиях единого информационного пространства мест проведения операций должна функционировать по особым правилам.

Остановившись на mesh-сетях IEEE 802.11s [2], необходимо отметить, что данная спецификация рекомендует применять станции (узлы), содержащие несколько радиointерфейсов. Это позволяет одновременно использовать несколько частотных каналов для передачи информации. Общаясь с каждым из своих соседей, узел использует конкретный интерфейс (интерфейсы). Каждый интерфейс использует определенный канал. Механизмы назначения каналов (и другие механизмы функционирования) влияют на производительность сети, которая к тому же зависит от особенностей трафика. В системах управления специального назначения особенности трафика проявляются в его направлении, приоритетах, пульсации и др. С достаточной степенью

достоверности можно предположить, что преобладающим трафиком будет вертикальный. Для такого случая целесообразно использовать один из наиболее известных алгоритмов назначения каналов в сетях IEEE 802.11s – алгоритм Nuacinth с централизованным способом назначения каналов [3-4]. Рассмотрим типичную mesh-сеть, в которой каждый из узлов может одновременно работать как точка доступа, так и в качестве mesh-станции [3]. Некоторые устройства могут быть еще и шлюзами во внешнюю сеть. Каждое из mesh-устройств содержит в себе несколько радиоинтерфейсов, каждый из которых настроен на определенный канал на относительно долгое время (минуты, часы, дни). Задача назначения предполагает определить, во-первых, с помощью какого интерфейса узел общается с каждым из своих соседей, а во-вторых, какой канал использует каждый из интерфейсов.

Предполагается, что каждый узел имеет соединение со всеми станциями, находящимися в его области устойчивого приема. Стоит заметить, что алгоритм маршрутизации зависит от пропускной способности каждого соединения, которые, в свою очередь, зависят от способа назначения каналов, а способ назначения каналов зависит от ожидаемой нагрузки на соединение, которая зависит от маршрутизации. Таким образом, получается круговая зависимость. Для ее разрешения было решено начать с оценки ожидаемой нагрузки без учета пропускной способности (см. рис. 1), а затем итеративно повторять процесс назначения каналов и маршрутизации до момента, когда пропускные способности каждой из соединений будут максимально близки к предполагаемой нагрузке. Вначале на вход алгоритма назначения каналов поступает оценка нагрузки на соединения. Выходом является пропускная способность соединений. Алгоритм маршрутизации использует их для вычисления путей, которые используются для вычисления ожидаемой нагрузки.

Если в конце итерации оказалось, что ожидаемая нагрузка больше пропускной способности, то процесс повторяется и заканчивается, если дальнейшего улучшения не происходит. Алгоритм предлагает два способа начальной оценки ожидаемой нагрузки на соединения. Во-первых, можно предположить, что все станции в области интерференции равномерно разделяют пропускную способность канала. Пропускная способность соединения l вычисляется, учитывая только число доступных каналов, пропускную способность отдельного канала и число соединений внутри области интерференции рассматрива-

емого соединения. Далее пропускные способности поступают на вход алгоритма маршрутизации, после чего на выходе будет ожидаемая нагрузка на соединения. Более точная оценка ожидаемой нагрузки на соединения вычисляется через такие параметры, как количество путей между узлами, количество путей между этими же узлами, проходящих через соединение l и ожидаемый трафик между узлами.

Соединения рассматриваются в порядке убывания ожидаемой на них нагрузки. При рассмотрении соединения канал назначается следующим образом (в предположении, что у каждого узла q интерфейсов):

- если число использованных каналов обоих узлов соединения меньше q , то соединению назначается неиспользуемый канал с наименьшей степенью интерференции;
- если узел 1 использует q каналов, а узел 2 – меньше q каналов, то выбирается один из уже используемых каналов узла 1 с наименьшей степенью интерференции;
- пусть оба узла уже используют q каналов, то есть все их интерфейсы задействованы. Если узлы используют общие каналы, то из них выбирается канал с минимальной степенью интерференции. Если общих каналов нет, то выбирается по одному каналу от каждого из узлов, и они заменяются на общий канал так, чтобы степень интерференции была минимальна.

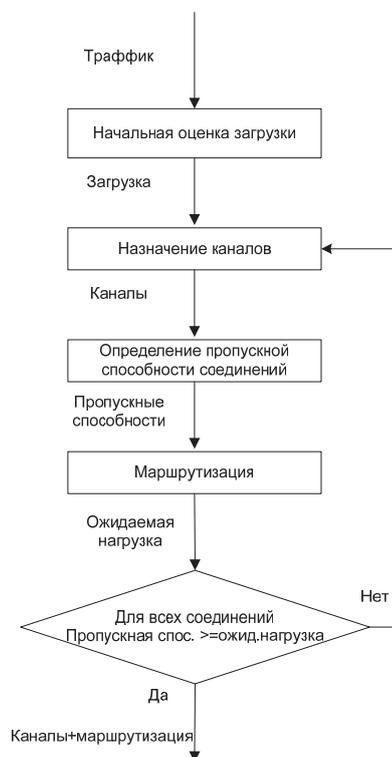


Рис. 1. Алгоритм C-Nuacinth

Под степенью интерференции понимается сумма ожидаемых нагрузок на соединения внутри области интерференции. При этом пропускная способность соединения определяется произведением ожидаемой нагрузки на соединение на пропускную способность канала, деленную на суммарную ожидаемую нагрузку.

Алгоритм маршрутизации может быть использован любой. По сравнению с одноканальным решением, даже с использованием всего двух интерфейсов пропускная способность сети возрастает в 6-8 раз.

Необходимо добавить, что большинство работ по решению данной задачи направлено на разработку универсальных схем назначения каналов, что приводит к высокой сложности алгоритмов, усложняет их практическую реализацию и снижает их эффективность. Более эффективными являются подходы, ориентированные на конкретный сценарий использования mesh-сети.

Литература

1. IEEE Std 802.11-2007. Revision of IEEE Std. 802.11-1999. IEEE Std. 802.11-2007. IEEE Standard for Information Technology –

Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Computer Society, June 2007.

2. IEEE P802.11s/D2.0. Draft STANDARD for Information Technology – Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment: Mesh Networking [Electronic resource] // IEEE Standards Activities Department. USA: IEEE, 2008.
3. Raniwala A., Gopalan K., Chiueh T. Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks // ACM Mobile Computing and Communications Review. Vol. 8, 2004. – P. 50-65.
4. Raniwala A. Tzi-cker Chiueh. Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network // Proc. of INFOCOM '05. Vol. 3. 2005. – P. 2223- 2234.

УДК 621.395.8

ВЕРОЯТНОСТЬ НАРУШЕНИЯ СВЯЗИ В СОТОВОЙ СЕТИ МОБИЛЬНОЙ РАДИОСВЯЗИ В УСЛОВИЯХ ЗАМИРАНИЙ СИГНАЛА И ПОМЕХИ

Ильин Е.С.

Вероятность нарушения связи является основным эксплуатационным показателем качества обслуживания в сотовых системах подвижной радиосвязи. Для выполнения инженерных расчетов при проектировании сотовых систем часто используются модели распространения радиоволн, основанные на эмпирических зависимостях Хаты и Окамуры. Однако для теоретического анализа вероятности нарушения связи целесообразно использовать строгую и достаточно общую модель замираний сигналов в канале радиосвязи, основанную на четырехпараметрическом распределении комплексного коэффициента передачи каждого учитываемого сигнала. Проявляющиеся на практике виды замираний (райсовские, рэлеевские и более глубокие замирания) характеризуются определенным и фиксированным набором параметров используемого четырехпараметрического распределения. В статье представлена методика анализа, основанная на четырехпараметрическом описании замираний сигнала и помехи. Получены точные формулы для вероятности нарушения связи.

Постановка задачи

Рассмотрим сотовую сеть мобильной радиосвязи, в которой передаваемый сигнал испытывает многолучевое распространение в замирающем канале. В месте приема наряду с полезным сигналом присутствуют L сигналов соканальной помехи от БС, в которые используют одинаковые частотные группы:

$$\dot{z}(t) = \gamma_0 e^{i\theta_0} \dot{s}_0(t) + \sum_{k=1}^L \gamma_k e^{i\theta_k} \dot{s}_k(t), \quad (1)$$

где $\dot{s}_0(t)$ – полезный сигнал, а $\{\dot{s}_k(t), k = \overline{1, L}\}$ – соканальные помехи, γ_k и θ_k – амплитуда и фаза комплексного коэффициента передачи $\dot{\gamma}_k$ k -го канала.

Ограничимся рассмотрением только амплитудных характеристик каналов, считая, что:

- случайные величины γ_k , $k = \overline{0, L}$ статистически независимы;
- закон распределения случайных величин γ_k , $k = \overline{0, L}$, четырехпараметрический [1] с функциями