Труды МАИ. 2024. № 139
Trudy MAI. 2024. No. 139. (In Russ.)

Научная статья
УДК 621.391
URL: https://trudymai.ru/published.php?ID=183460
EDN: https://www.elibrary.ru/PRAXTJ

АЛГОРИТМ СИНХРОННОЙ ВЫРАБОТКИ КЛЮЧЕВОЙ ИНФОРМАЦИИ НА ОСНОВЕ СОСТОЯНИЯ КАНАЛА СВЯЗИ МЕЖДУ МОБИЛЬНЫМИ РАДИОСРЕДСТВАМИ

Александр Александрович Бахтин[1]✉, Владислав Владимирович Дымников[2], Александр Евгеньевич Баскаков[3]

[1,2,3]Национальный исследовательский университет «Московский институт электронной техники»,

Москва, Зеленоград, Россия

[1]bah@miee.ru

[2]vv.dymnikov@gmail.com

[3]9999924816@yandex.ru

Аннотация. В статье рассмотрена реализация синхронной выработки случайных последовательностей на узлах радиосвязи без обмена по открытому каналу связи. Метод основан на использовании временной динамики средней мощности принимаемого сигнала (RSSI). В результате был предложен и реализован в виде ПО алгоритм, кроме того, получены результаты его работы на радиотрассе. Проведен анализ качества полученной последовательности.

Ключевые слова: случайная последовательность, многолучевой релеевский канал, мелкомасштабные замирания

Для цитирования: Бахтин А.А., Дымников В.В. Баскаков А.Е. Алгоритм синхронной выработки ключевой информации на основе состояния канала связи между мобильными радиосредствами // Труды МАИ. 2024. № 139. URL: https://trudymai.ru/published.php?ID=183460

Original article

ALGORITHM FOR SYNCHRONOUS GENERATION OF KEY INFORMATION BASED ON THE CHARACTERISTICS OF THE COMMUNICATION CHANNEL BETWEEN MOBILE RADIO DEVICES

A. Alexander Bakhtin[1]✉, Vladislav V. Dymnikov[2], Alexander E. Baskakov[3]

[1,2,3]National Research University of Electronic Technology,

Moscow, Zelenograd, Russia

[1]bah@miee.ru

[2]vv.dymnikov@gmail.com

[3]9999924816@yandex.ru

Abstract. Today, cryptographic protocols based on symmetric and asymmetric encryption algorithms are usually used to protect information in a radio network. Such security methods are associated with the need to implement a key management and distribution system.

This paper discusses an alternative approach to key information distribution for symmetric cryptographic algorithms, currently under study, available to mobile radio facilities sharing a radio channel. The paper presents the operating principle of the algorithm for synchronous

and symmetric generation of key information based on the state of the radio channel between radio facilities, as well as a specific implementation of the algorithm and the results of its field tests. The algorithm presented in the paper differs from those presented in the literature in that it has a better entropy of the resulting sequence for generating key information.

In this paper, we will consider a method for synchronous generation of key information based on the use of the time dynamics of the average received signal strength (RSSI). The choice is justified by the fact that this is a universal characteristic supported by most receivers. To measure it, two transceivers operating in a half-duplex mode with time division are sufficient, and the presence of a system with multiple antennas is not necessary.

The considered algorithm allows synchronous formation of a sequence on a pair of nodes connected by a radio communication channel, which depends on the characteristics of the radio channel - in this case, the average energy level of the received radio signal. The algorithm has good entropy indicators of the sequence being formed. The conducted full-scale tests show that the entropy of the sequence formed by the algorithm is practically independent of the type of radio path, however, radio paths with a low level of Rayleigh fading lead to a longer operation of the algorithm to form a sequence of identical length.

The conducted full-scale tests show the fundamental possibility of using algorithms of this type for the formation and simultaneous distribution of key information between land mobile radio communication facilities operating in the UHF and SHF wavelength ranges. In turn, with the increase in the frequency of use of wireless communication channels, as well as the increase in the value of information circulating in such channels and the technical capabilities of intruders, the relevance of searching for and studying new approaches to solving the classical problem of distributing key information is constantly increasing.

Keywords: random sequences, Rayleigh multipath channel, small-scale fading

For citation: Bakhtin A.A., Dymnikov V.V. Baskakov A.E. Algorithm for synchronous generation of key information based on the characteristics of the communication channel between mobile radio devices. *Trudy MAI*. 2024. No. 139. (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=183460

По сравнению с проводными каналами связи, где доступ злоумышленника к каналу связи ограничен физически, открытый широковещательный характер каналов радиосвязи не ограничивает возможностей злоумышленника по доступу к передаваемой информации, а также ее модификации, навязыванию или блокированию канала радиосвязи. С одной стороны независимость каналов радиосвязи от инфраструктуры линий связи, а также их широковещательность являются важными свойствами, обусловившими повсеместное применение радиосвязи в современном мире. С другой стороны, уязвимость каналов радиосвязи повышает актуальность разработки алгоритмов защиты доступа к передаваемой информации, а также алгоритмов защиты от модификации и навязывания информации в радиоканале.

На сегодняшний день для защиты информации в радиосети обычно используются криптографические протоколы, основанные на алгоритмах симметричного и ассиметричного шифрования. Такие методы обеспечения безопасности связаны с необходимостью реализации системы управления и распределения ключей. Наиболее эффективным из используемых подходов

представляется архитектура PKI (*public key infrastructure*, инфраструктура открытых ключей).

В данной работе рассматривается исследуемый в настоящее время [2-5] альтернативный подход к распределению ключевой информации для симметричных криптоалгоритмов, доступный мобильным радиосредствам, разделяющим радиоканал. В работе приведен принцип работы алгоритма синхронной и симметричной выработки ключевой информации на основе состояния радиоканала между радиосредствами, также рассмотрена конкретная реализация алгоритма и приведены результаты его натурных испытаний. Приведенный в работе алгоритм отличается от представленных в литературе [2-5] лучшей энтропией результирующей последовательности для формирования ключевой информации.

Проблемы защиты информации в сетях радиосвязи

Для работы алгоритмов как симметричного, так и ассиметричного шифрования необходимо распределение ключевой информации. Для решения данной проблемы существует несколько основных подходов:

Ключевая информация для взаимодействия между устройствами может быть заранее введена в каждое устройство от центра распределения ключей непосредственно или через цепочку доверенных посредников. Это является сложным процессом для больших и рассредоточенных радиосетей в силу того, что центр распределения ключей должен точно знать состав сети, на который формируется ключевая информация, а также для ключевой информации при развертывании сети

необходимо обеспечить защищенную доставку от центра до устройств не используя радиоканалы.

Использование центра сертификации и построение архитектуры PKI, в которой доверенный центр сертификации (или подчиненные распределенные серверы сертификации) на этапе ввода новых устройств в сеть регистрирует их, подписывает их открытые ключи и рассылает их узлам сети связи или публикует их. При этом зачастую передача подписанных открытых ключей ведется по открытым каналам радиосвязи, в которых защита ведется только от навязывания открытых ключей. Узлы могут вырабатывать собственные пары рабочих ключей для взаимодействия, не опасаясь навязывания информации, за счет аутентификации сторон обмена, основанной на открытых ключах, предоставляемых центром сертификации. При использовании такого подхода возникают риски, связанные с уязвимостями в протоколах нижних уровней, используемых для транспорта ключевой информации и аутентификации.

Дополнительно осложняет ситуацию распределения ключевой информации необходимость ее регулярного обновления. Обновление необходимо ввиду того, что атаки на криптоалгоритмы осуществляются за счет сбора злоумышленником передаваемой информации и выстраивании вероятностных предположений об используемом ключе. Чем больше шифротекста от одного ключа получает злоумышленник, тем выше вероятность раскрытия им данного ключа. Кроме этого, использование одного ключа в течении длительного интервала времени повышает вероятность успешной атаки на физическую реализацию устройства криптозащиты (анализ ПЭМИН, происхождение сбоя и т.д.). Перечисленным атакам в разной

степени подвержены все современные криптоалгоритмы и устройства криптозащиты. Защитой служит своевременное обновление ключевой информации.

Выработка ключей на основе характеристик канала радиосвязи

Одним из анализируемых в последнее время [2-6] способов решения проблемы распределения ключей для мобильных радиосредств является синхронная выработка ключевой информации на узлах радиосвязи без обмена этой информацией по открытому каналу связи. У канала радиосвязи между парой радиосредств существуют характеристики, которые являются уникальными. Примером таких характеристик являются: средний уровень мощности принимаемого сигнала, картина многолучевости, АЧХ и ФЧХ канала в зависимости от частоты. Перечисленные характеристики определяются сложным многолучевым распространением радиосигнала от передатчика к приемнику особенно на закрытых радиотрассах в близи поверхности земли.

В этой работе будет рассматриваться метод синхронной выработки ключевой информации, основанный на использовании временной динамики средней мощности принимаемого сигнала (*received signal strength indicator*, RSSI). Выбор обосновывается тем, что это универсальная характеристика, поддерживаемая большинством приемников. Для ее измерения достаточно двух приемопередатчиков, работающих в полудуплексном режиме с разделением времени, а наличие системы с множественными антеннами не обязательно.

Передаваемый сигнал поступает на приемник как несколько «копий» – лучей, которые проходят по разным маршрутам. Разные лучи передаваемых сигналов приходят к приемнику с разными фазами, амплитудами, доплеровскими сдвигами и разными задержками. За счет этого появляются интерференционно обусловленные колебания уровня сигнала в приемнике. Описанное явление называется замираниями в канале связи. Можно сказать, что именно замирания в их временной динамике характеризуют уникальность канала связи между двумя узлами. Относительно возможности использования канала радиосвязи как источника уникальной информации доступной обоим сторонам его образующим можно сделать следующие утверждения:

1. Факторы, определяющие замирания в канале связи, перечисленные ранее, идентичны для обоих направлений канала.

2. Свойства канала будут уникальны для двух узлов, которые связаны данным радиоканалом. Злоумышленник, расположенный на удалении большем, чем несколько длин волн используемой частоты связи от любого из узлов, будет иметь отличающийся по своим характеристикам канал с каждым из абонентов.

3. Как и в квантовой криптографии [7] возникает необходимость аутентификации второй стороны обмена. При этом идентифицировать вторую сторону возможно за счет идентичных и наблюдаемых обоими сторонами характеристик канала связи.

Можно представить радиоканал как фильтр, характеристики которого зависят от времени и пространства. Данный фильтр имеет одинаковую характеристику для

сигналов, передаваемых между узлами вне зависимости от их направленности. Измерение характеристик фильтра соответственно доступно обеим сторонам.

Используя результаты данных измерений узлы (вновь идентично квантовой криптографии [7]) должны сформировать идентичную последовательность имеющую достаточную энтропию для выработки ключевой информации, при этом избежав ошибок, свойственных физическим измерениям и процессам квантования их результатов.

Модель угроз

При анализе алгоритмов синхронного формирования ключевой информации на основе состояния канала связи авторы [8-14] рассматривают следующую модель угроз со следующими общими условиями:

-Злоумышленник может прослушивать сообщения передаваемые в канале радиосвязи обоими узлами.

-Злоумышленник может делать измерения физических характеристик канала связи между каждым из узлов и ним используя передаваемые узлами сообщения.

-Злоумышленник знает алгоритм выработки ключа и параметры, которые в нем используются.

-Злоумышленник может влиять на сам канал и измерения, полученные из него узлами, формирующими ключевую информацию, перемещая различные объекты на пути распространения радиоволн. При этом злоумышленник не может повлиять на другие, независимые от него перемещения объектов и самих узлов.

-Злоумышленник не использует атаку «человек посередине», так как аутентификация узлов выполняется сторонними средствами, не рассматриваемыми в данной работе.

-Злоумышленник из своего положения может передавать радиосигнал, интерферирующий с сигналами передаваемыми узлами, формирующими ключевую информацию. Однако, при этом злоумышленник не может навязывать измерения, потому что они проводятся только по сообщениям, полученным от аутентифицированной стороны.

-Злоумышленник не может находиться в физической близости (на расстоянии ближе нескольких длин волн используемой частоты радиосвязи) к одному из легитимных узлов. Это гарантирует, что злоумышленник имеет другой радиоканал, не коррелированный с каналом, используемым для формирования ключевой информации.

В большинстве приведенных источников модель угроз в явно виде не описывается, однако многие из перечисленных выше соображений о возможностях и ограничениях действий злоумышленника упоминаются. При этом систематизация модели угроз позволяет полнее оценить свойства разрабатываемого алгоритма.

Алгоритм синхронного формирования ключевой информации

Структура и предположения об области применения рассматриваемого в данной работе и в литературе [2-5] алгоритма синхронного формирования ключевой информации на основе состояния канала связи идентична. Предполагается, что узлы связи работают в полудуплексном режиме на одинаковой частоте в диапазоне ДМВ

или СМВ и как минимум один из узлов связи является подвижным (в рамках длинны волны) [16, 17]. Структура алгоритма включает пять основных этапов:

-Измерение характеристики канала. Измерение характеристики канала происходит по средней энергии принимаемого информационного слота. Направление передачи информационных слотов между узлами чередуется. Для корректной работы следующих этапов измерения производятся блоками определенной длины.

-Квантование выборок. Из полученных измерений уровней сигнала необходимо получить последовательность бит. Для этого применяется алгоритм квантования. Необходимо выбрать граничные значения измеряемой характеристики, относительно который будут образовываться биты. Преимущественно алгоритмом квантования определяются основные характеристики метода синхронной выработки ключевой информации– энтропия полученной последовательности и время ее выработки. Каждый алгоритм является компромиссом между повышением энтропии последовательности и замедлением скорости выработки. Самый простой алгоритм, имеющий высокую скорость выработки последовательности, но при этом низкую энтропию и высокое рассогласование описан в работе [2]. Используемый в работах [2-3] алгоритм – квантование в привычном понимании этого процесса. Выбираются границы, относительно среднего значения и полученные измерения квантуются относительно них. В работе [4] был предложен алгоритм, который рассчитывает значения границ исходя из среднего значения и стандартного отклонения. В работе [5] был предложен алгоритм, имеющий низкую энтропию, но при этом использующий дополнительные методы усиления конфиденциальности.

В предлагаемой в данной работе реализации используется алгоритм квантования с двумя адаптивными границами. Границы выбираются в соответствии с особенностями распределения мощности принимаемого радиосигнала. Математическое описание распределения мощности принимаемого радиосигнала в условиях работы алгоритма может быть достигнуто рэлеевским распределением. Рэлеевское распределение описывает распределение полученных значений мощности принятых информационных слотов, однако не определяет временной динамики значений мощности. Временная динамика определяется мобильностью объектов (препятствий) на радиотрассе и узлов, формирующих последовательность. Поскольку выдвинуть априорные предположения о модели мобильности затруднительно, то границы формируются адаптивно. Две границы уровней мощности определяются таким образом, чтобы попадание измерений в каждую из трех, образованных ими областей было равновероятно. Границы пересчитываются для каждых 100 измерений заново. Алгоритм квантования использует вычисленные границы следующим образом: если значение меньше нижней границы формируется 0, если значение выше верхней границы, то формируется 1, условием перехода к формированию следующего бита является попадание сигнала в область между двумя границами. Алгоритм квантования представлен на рисунке 1.

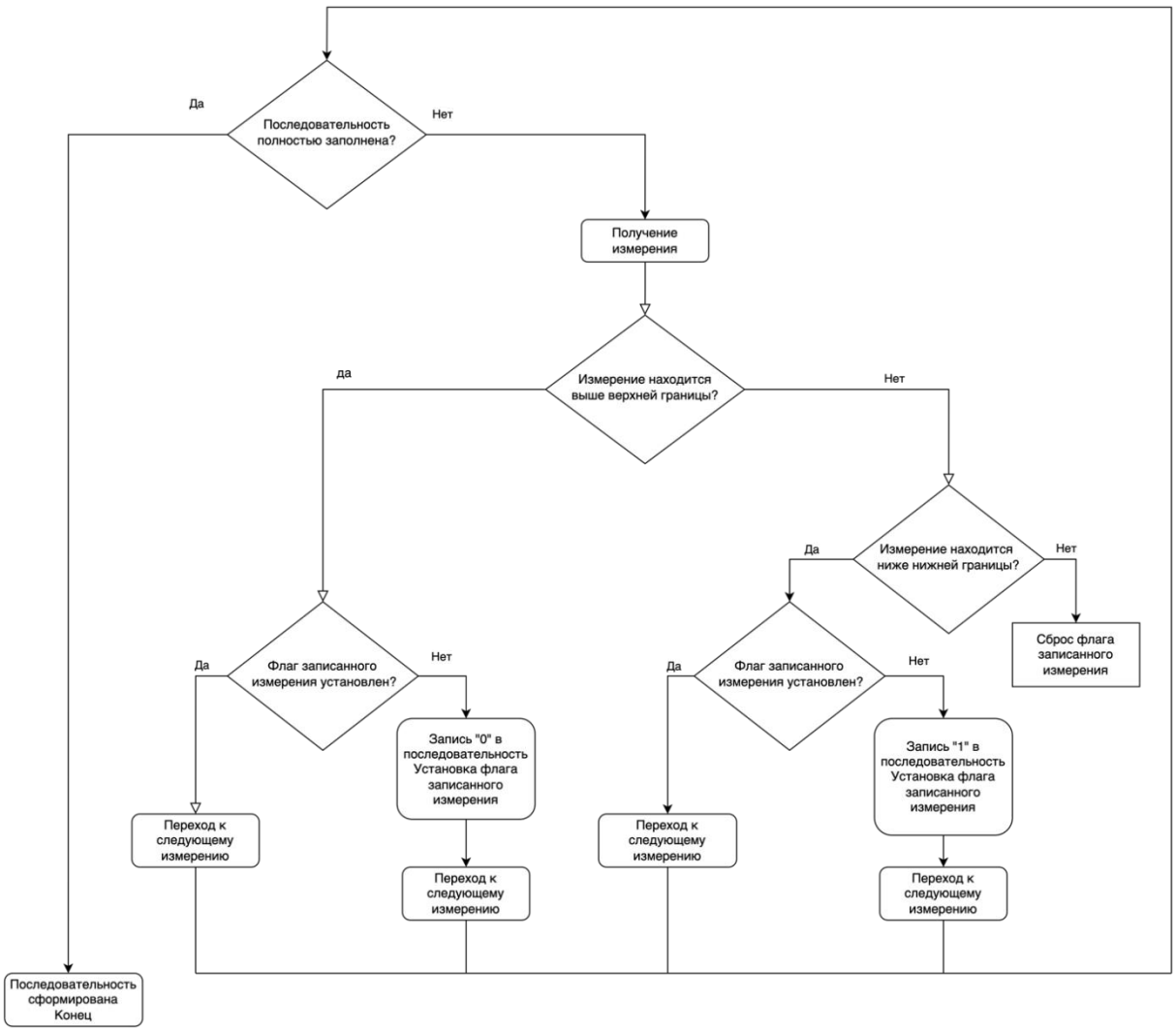

Рисунок 1 – Алгоритм квантования

Таким образом, вырабатываемая последовательность будет состоять в основном из труднопредсказуемых эффектов смены уровня принимаемой мощности, вызванных мобильностью объектов на радиотрассе или узлов. При выборе длительности временного слота, который используется для измерения мощности принимаемого радиосигнала, стоит учитывать скорость движения узлов и частоту связи (чем выше скорость и выше частота связи, тем более короткими должны быть слоты для сохранения идентичности картины интерференции лучей на интервале выполнения измерений обоими сторонами), а также наличие искажений при оценке

уровня мощности принимаемого сигнала вызванное объектами на радиотрассе с более высокой скоростью мобильности, шумами и импульсными помехами (чем длиннее слот, тем меньше шумов в получаемой оценке значения мощности принимаемого радиосигнала). Количество накоплений для адаптации границ должно выбираться исходя из степени мобильности узлов, а также исходя из достоверности получаемой статистической оценки вероятности попадания в каждую область, используемую в алгоритме квантования.

На рисунке 2 представлен график зависимости среднего уровня мощности принимаемого сигнала за определенный период времени и проиллюстрирована работа алгоритма квантования.

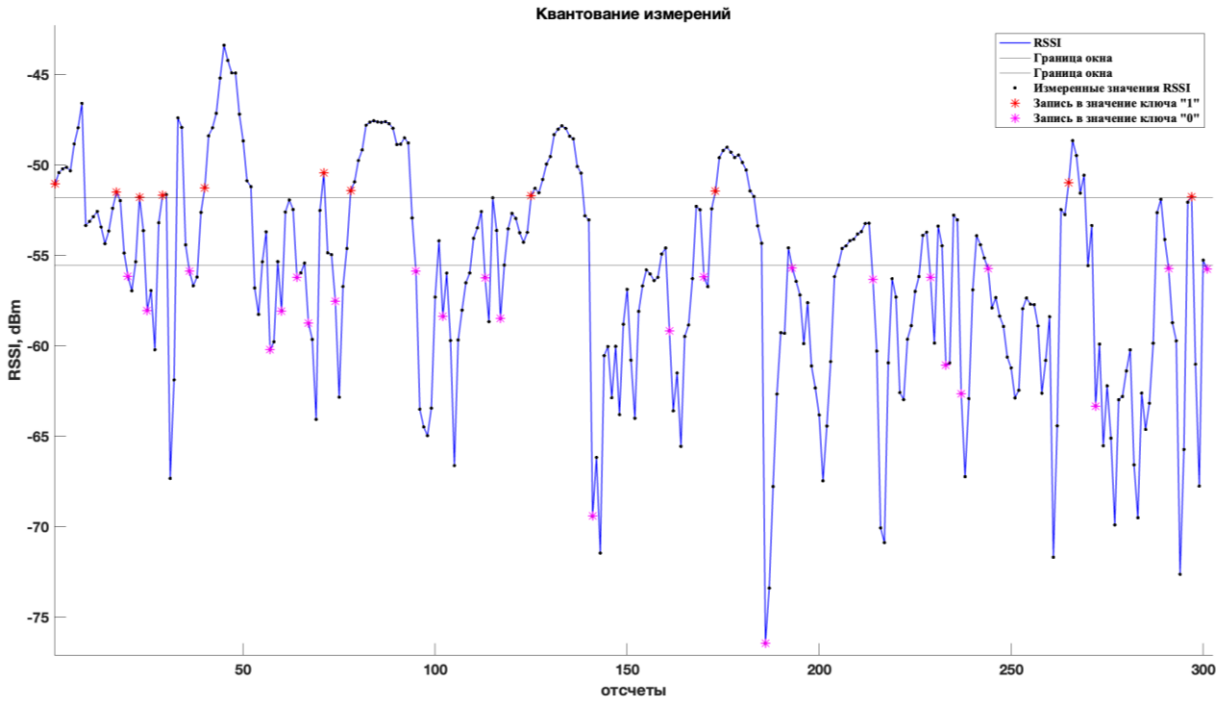

Рисунок 2 – График зависимости RSSI от времени, иллюстрирующий работу алгоритма квантования

Т.к. алгоритм рассчитан на применение в полудуплексных схемах обмена, то измерения характеристик канала, проводимые узлами, будут смещены во времени минимум на длину информационного слота (15 мс в нашем случае). Смещение во времени вызывает дополнительные к ошибкам физического измерения несовпадения результатов алгоритмов квантования. Одной из основных проблем, которые могут возникнуть при использовании описанного ранее алгоритма квантования, является появление измерений со значениями в окрестности адаптивно определяемых границ областей. Поскольку границы также базируются на результатах измерений, содержащих погрешности, то и сами границы не будут совпадать точно на обоих узлах. Измерения со значениями в окрестности границ областей могут приводить к тому, что квантование на узлах даст различное количество бит. Это означает, что образованная исходная последовательность на узлах будет содержать не только битовые ошибки, но и вставки\удаления бит, что значительно усложнит согласование полученных последовательностей. В данной работе использовалась отбраковка последовательностей измерений, в которых в результате квантования на узлах получилось различное количество бит. Такая отбраковка показала, что остающиеся последовательности, имеют хорошую корреляцию на обеих сторонах при различных шаблонах мобильности узлов и различных радиотрассах [19, 20]. Повышение строгости отбраковки необходимой для синхронизации измерений снижает скорость работы алгоритма формирования исходной последовательности. Поэтому авторы рассматривают возможность смены алгоритма отбраковки на алгоритм, допускающий незначительное смещение адаптивных границ областей квантования

если таковое обеспечит совпадение числа бит, формируемых алгоритмом квантования.

Следующий этап – согласование квантованных бит. Как было указано ранее в последовательностях, сформированных алгоритмом по результатам первых трех этапов, возможны битовые ошибки. Для их исправления возможно воспользоваться корректирующими кодами. Этот этап существуют во всех описанных реализациях [2-5] метода выработки ключей из состояния канала. Используемые методы варьируются в разных реализациях. Популярным решением для этой задачи является применение модификаций алгоритма Cascade [8], пришедшего из области прикладной квантовой криптографии. Алгоритм Cascade представляет собой адаптивный способ исправления ошибок, который дает злоумышленнику минимальную информацию с учетом достижения узлами цели исправления найденных ошибок. При его использовании, одна сторона перемешивает последовательность, делит ее на блоки и отправляет информацию о перестановках и четности каждого блока. В случае появления отличий выполняется бинарный поиск ошибки. Такой метод требует неопределенного количества итераций на его выполнение, взамен он может раскрыть меньшее количество информации, чем другие методы. В предлагаемой реализации используется турбо-код Хэмминга [21, 22], который всегда раскрывает злоумышленнику фиксированное количество информации о выработанной последовательности, но требует всего одной итерации обменов данными.

Следующий шаг – это усиление конфиденциальности. При согласовании квантованных бит по открытому каналу раскрывается часть информации о

сформированной последовательности. Этап согласования квантованных бит включает в себя передачу бит четности по открытому каналу, которые могут был получены злоумышленником. Исходят из этого, злоумышленник может строить предположения относительной выработанной узлами последовательности. Однако если энтропия сформированной последовательности велика, даже с учетом информации, раскрытой злоумышленнику (превосходит битность формируемого ключа), то можно применить алгоритм преобразования информации, который должен: иметь лавинный эффект, обеспечивать чтобы от значения каждого биты выходной последовательности зависели от большого битов входной последовательности, не допускал обращения. Соответствующий алгоритм, очевидно, можно построить на базе криптографической хеш-функции – каждый неизвестный злоумышленнику бит внесет изменения в выходную последовательность и ему останется атака на выходную последовательность перебором.

Применение этапа усиления конфиденциальности также может решить проблему, связанную с возможной неравновесностью бит в выходной последовательности, полученной в ходе работы предыдущих этапов. Кроме этого, обеим сторонам необходимо удостовериться в совпадении результирующей последовательности, для этого можно использовать блок информации, получающийся на следующей (за последней используемой) итерации преобразования информации.

Разработанная реализация описанного ранее алгоритма разделяет устройства на ведущее и ведомое. Управляющие команды, принятые от ведущего устройства, имеют наивысший приоритет выполнения. Ведущее устройство обрабатывает все

полученные результаты в процессе работы алгоритма и назначает новые состояния устройств. Конечные автоматы ведущего и ведомого устройств представлены на рисунках 3 и 4.

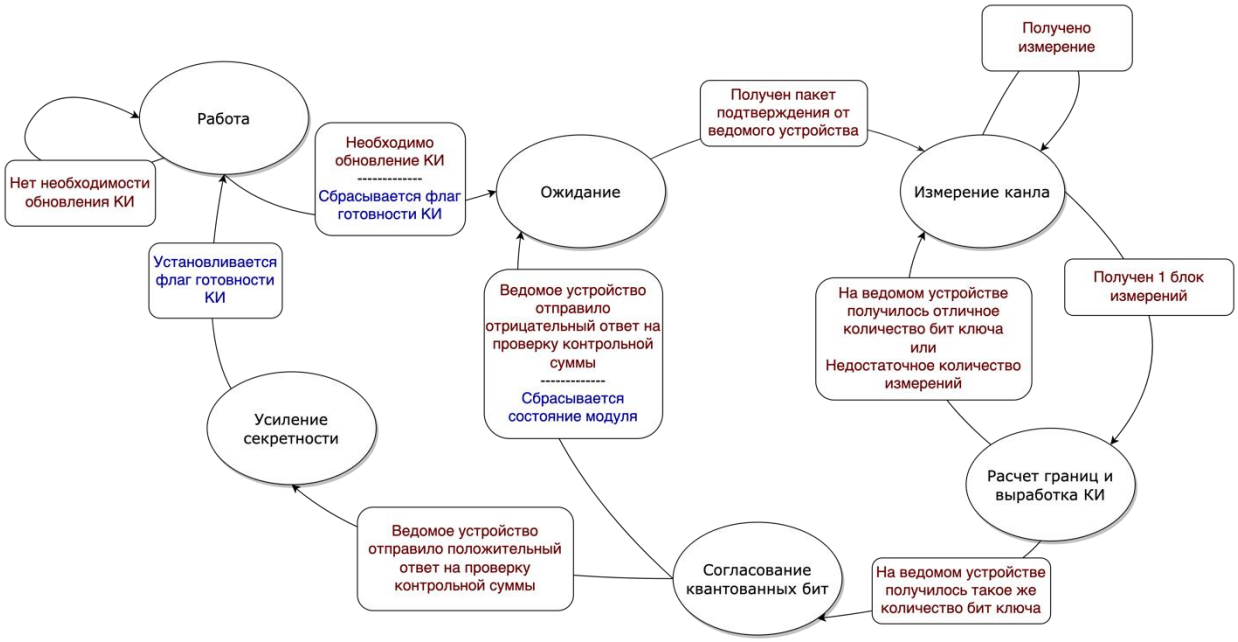

Рисунок 3 – Конечный автомат ведущего устройства

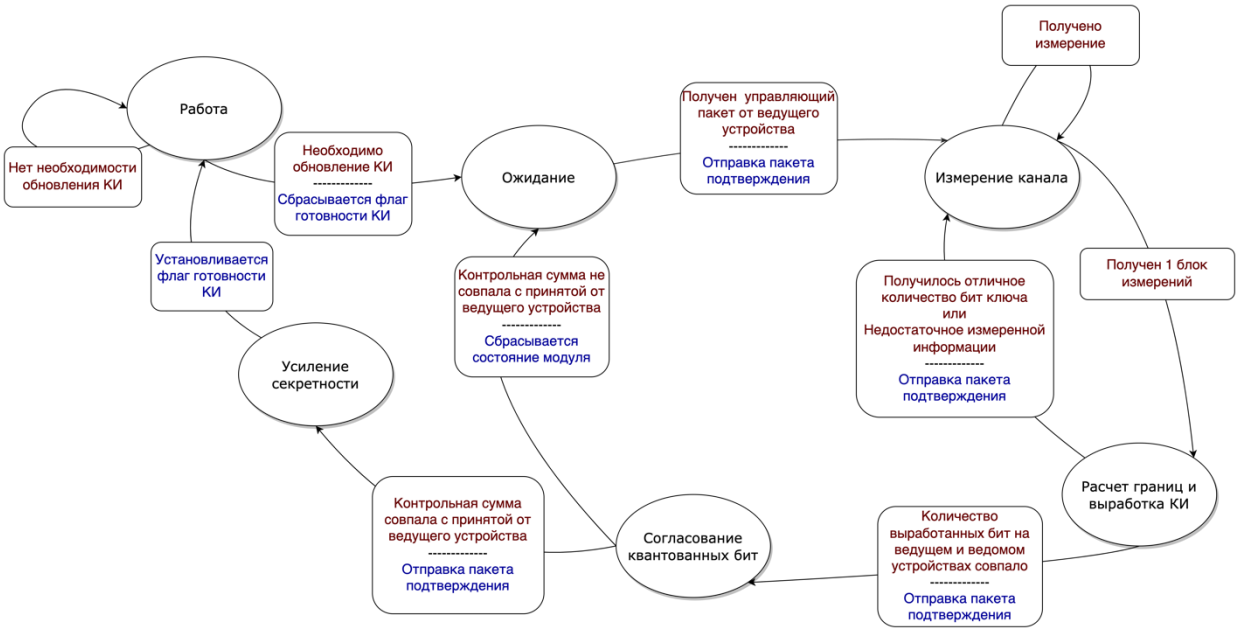

Рисунок 4 – Конечный автомат ведомого устройства

Натурные испытания алгоритма

В ходе проверки алгоритма было проведено его тестирование в различных условиях. Основными типами радиотрасс, на которых может отличаться поведение алгоритма, являются:

-Радиотрассы с преобладанием амплитуды одного луча, например, канал прямой радиовидимости. На таких радиотрассах релеевские замирания почти не проявляются. Для работы представленного ранее алгоритма такие условия являются наихудшими.

-Радиоотрассы с выраженной многолучевостью, например приземные радиотрассы в условиях городской застройки. На таких радиотрассах релеевские замирания в значительной степени определяют энергию принимаемого радиосигнала. Для работы представленного алгоритма такие условия являются оптимальными при ограничении мобильности узлов теми скоростями, при которых можно рассчитывать на симметричность проводимых радиоизмерений уровня сигнала с учетом длительности временных слотов.

Результаты тестирования, представленные далее, были получены в многоэтажном помещении на движущихся узлах. Такая радиотрасса по наблюдениям авторов представляет собой нечто среднее между типами трасс, представленными ранее. Зачастую материалы, применяемые в строениях, являются радиопрозрачными для ДМВ и СМВ диапазонов длин волн, однако наличие отражающих поверхностей может приводить к образованию в точке приема лучей с соизмеримой амплитудой и как следствие – к возникновению рэлеевских замираний. На рисунке 5 изображен график зависимости среднего уровня мощности принимаемого сигнала от времени за

один период формирования случайной последовательность длинной 256 бит. Формирование последовательности длинной 256 бит потребовало примерно 180 секунд работы алгоритма.

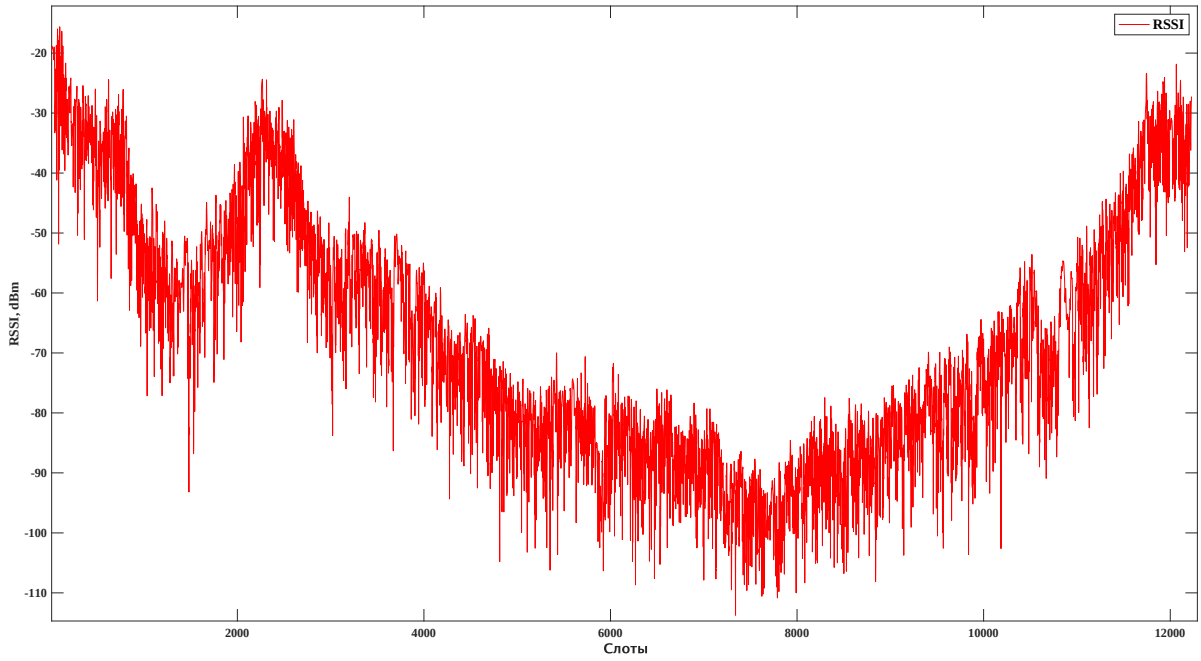

Рисунок 5 – График зависимости RSSI от времени за период формирования последовательности длинной 256 бит

По результатам представленных на рисунке 5 измерений была сформирована следующая последовательность (рисунок 6). Основной определяющей характеристикой сформированной последовательности будет информационная энтропия, рассчитанная до этапа усиления конфиденциальности. Энтропию последовательности, предполагая некоррелированность символов, вычислим по формуле:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i),$$

где $p(x_i)$ – вероятность появления символа x_i, алфавит X – набор из n символов x_i. В данном случае в качестве символа рассматривается бит, а множество $X = \{0, 1\}$. По представленной на рисунке 6 последовательности её энтропия $H(\{0, 1\})$ примерно равна 0.7.

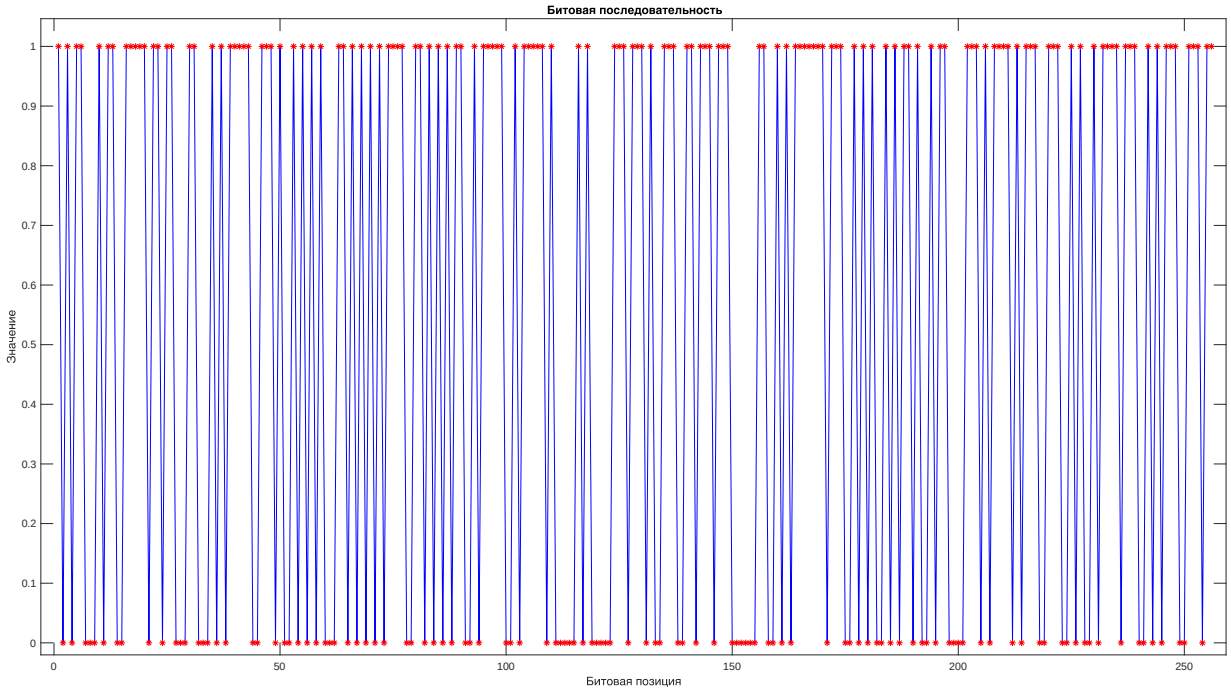

Рисунок 6 – Сформированная последовательность для сигнала с RSSI, представленного на рисунке 5

Важным показателем качества выработанной последовательности и правильности работы алгоритма является статистика по биграммам, которая позволяет оценить корреляцию между соседними сформованными битами. Она показывает способность работы алгоритма с каналом, имеющего долговременную когерентность. Статистическая характеристика последовательности представлена на рисунке 7.

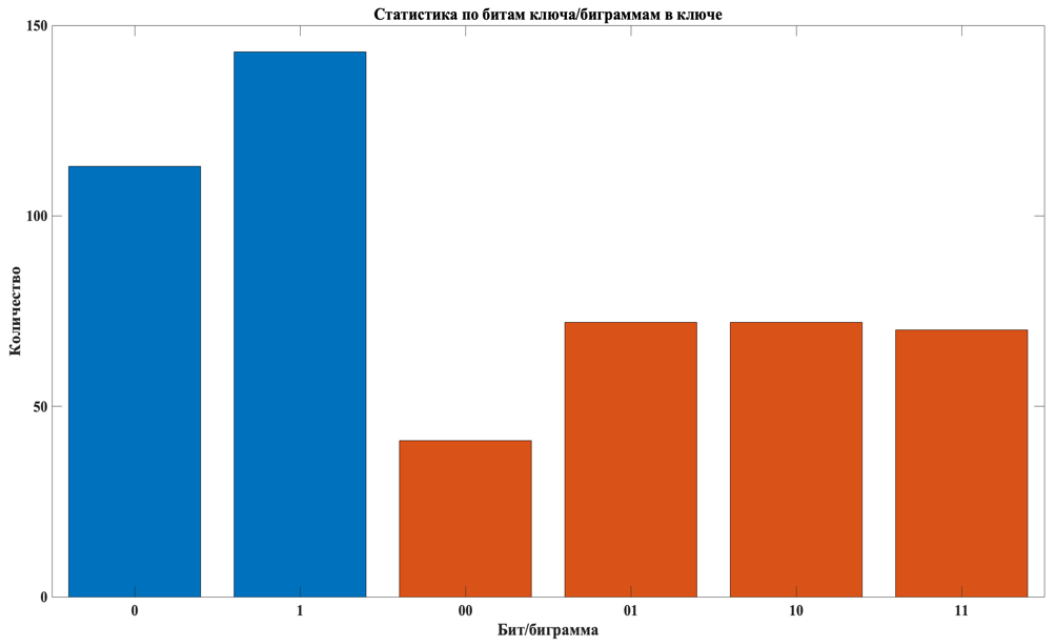

Рисунок 7 – Статистика бит/биграмм выработанной последовательности

Заниженную статистику по биграмме 00 можно объяснить свойством релеевских замираний иметь более резкие (по временной длительности) провалы в область значений меньшей энергии радиосигнала и более плавные (по временной длительности) выходы в область повышенных значений энергии радиосигнала. Прочие биграммы показывают хорошее согласование вероятности с учетом длительности последовательности, что указывает на низкую корреляцию между значениями соседних бит.

Выводы

Предложенный алгоритм позволяет синхронно формировать на паре связанных каналом радиосвязи узлов последовательность, зависящую от характеристик радиоканала – в данном случае среднего уровня энергии принимаемого радиосигнала. Алгоритм имеет хорошие, относительно представленных в литературе показатели энтропии формируемой последовательности. Проведенные натурные испытания

показывают, что энтропия формируемой алгоритмом последовательности практически не зависит от типа радиотрассы, однако работа в условиях радиотрассы с низким уровнем релеевских замираний приводит к более длительной работе алгоритма для формирования последовательности идентичной длины. Данное свойство выгодно отличает разработанный алгоритм по сравнению с известными, для которых вид трассы значительно влияет на энтропию формируемой последовательности.

Проведенные натурные испытания показывают принципиальную возможность применения алгоритмов подобного типа для формирования и единовременного распределения ключевой информации между средствами наземной подвижной радиосвязи, работающими в ДМВ и СМВ диапазонах длин волн. В свою очередь, с повышением частоты использования беспроводных каналов связи, а также повышением ценности циркулирующей в таких каналах информации и технических возможностей злоумышленников – актуальность поиска и исследования новых подходов к решению классической задачи распределения ключевой информации непрерывно возрастает.

Список источников

1. Преображенскии Н.Б., Файзулхаков Я.Р. Проблема компенсации рэлеевских замираний в радиоканалах подвижных систем голосовой связи // Информатика и ее применение. 2011. Т. 5. № 2. С. 82-89.

2. Aono T., Higuchi K., Ohira T., Komiyama B., Sasaoka H. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels // IEEE Transactions on Antennas and Propagation. 2005. V. 53, No. 11. P. 3776-3784. DOI: 10.1109/TAP.2005.858853

3. Mathur S., Trappe W., Mandayam N., Ye C., Reznik A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel // 14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008, San Francisco, California, USA, September 14-19, 2008. P. 128-139. DOI: 10.1145/1409944.1409960

4. Premnath S.N., Gowda P.L., Kasera S.K., Patwari N., Ricci R. Secret Key Extraction using Bluetooth Wireless Signal Strength Measurements // IEEE International Conference on Sensing, Communication, and Networking (SECON), 2014. P. 293-301. DOI: 10.1109/SAHCN.2014.6990365

5. Azimi-Sadjadi B., Kiayias A., Mercado A., Yener B. Robust key generation from signal envelopes in wireless networks // Proceedings of the 14th ACM conference on Computer and communications security, 2007. P. 401-410. DOI: 10.1145/1315245.1315295

6. Jana S., Premnath S.N., Clark M., Kasera S.K., Patwari N., Krishnamurthy S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments // Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom). 2009. P. 321-332.

7. Assche G. Quantum Cryptography and Secret-Key Distillation. Cambridge University Press, 2006. 276 p.

8. Brassard G., Salvail L. Secret-Key Reconciliation by Public Discussion. Lecture Notes in Computer Science. 2001. P. 410-423.

9. Shannon C.E. Communication Theory of Secrecy Systems // Bell System Technical Journal. 1949. No. 28 (4). P. 656-715.

10. Duan S. Security analysis of tetra. Master's thesis. Norwegian University of Science and Technology Department of Telematics, 2013.

11. Benantar M. The Internet public key infrastructure // IBM Systems Journal. 2001. No. 40 (3). P. 648-665. DOI: 10.1147/sj.403.0648

12. Shannon C. E. The Mathematical Theory of Communication // The Bell System Technical Journal. 1948. V. 27, No. 3. P. 379-423.

13. Akinbiyi O. Physical layer security using artificial noise. The University of Leeds School of Electronic and Electrical Engineering, 2012.

14. Wyner A.D. The Wiretap Channel // Bell System Technology Journal. 1975. V. 54, P. 1355-1387. DOI: 10.1002/j.1538-7305.1975.tb02040

15. Rehman S.U., Sowerby K.W., Alam S., Ardekani I. Radio Frequency Fingerprinting and its Challenges // IEEE Conference on Communicati.ons and Network Security. 2014. P. 496-497. DOI: 10.1109/CNS.2014.6997522

16. Sakai M., Lin H., Yamashita K. Sakai M. Intrinsic Interference Based Physical Layer Encryption for OFDM/OQAM // IEEE Communications Letters. 2017. No. 21 (5). P. 1059-1062. DOI: 10.1109/LCOMM.2017.2654442

17. Бахтин А.А., Волков А.С., Баскаков А.Е. Исследование особенностей реализации алгоритмов доступа к среде в мобильных самоорганизующихся сетях связи // Труды МАИ. 2017. № 97. URL: https://trudymai.ru/published.php?ID=87331

18. Елисеев С.О., Крюков Д.А. Система криптографической генерации идентичных данных на основе алгоритма Диффи-Хеллмана // Труды МАИ. 2018. № 101. URL:

https://trudymai.ru/published.php?ID=97041

19. Фомин А.И., Айман Хамад. Анализ надёжности связи в каналах с быстрыми и медленными замираниями // Труды МАИ. 2008. № 30. URL: https://trudymai.ru/published.php?ID=7525

20. Volkov A., Chi Jie., Gorelik A., Solodkov A., Sviridov I. Classification of radio signals in multipath fading channel using neural network // 2024 Conference Young Researchers in Electrical and Electronic Engineering (2024 ElCon), Saint Petersburg Electrotechnical University «LETI», January 29-30, 2024, Russia. P. 919-923.

21. Волков А.С., Крейнделин В.Б. Алгоритмы кодирования алгебраических недвоичных каскадных сверточных кодов уменьшенной сложности // T-Comm – Телекоммуникации и Транспорт. 2024. Т. 18. № 3. С. 11-18. DOI: 10.36724/2072-8735-2024-18-3-11-18

22. Волков А.С. Разработка имитационной модели канала с группирующимися ошибками // Труды МАИ. 2023. № 128. URL: https://trudymai.ru/published.php?ID=171396. DOI: 10.34759/trd-2023-128-12

References

1. Preobrazhenskii N.B., FaĬzulkhakov YA.R. The problem of compensation of Rayleigh fading in radio channels of mobile voice communication systems. *Informatika i ee primenenie*. 2011. V. 5, No. 2, P. 82-89. (In Russ.)

2. Aono T., Higuchi K., Ohira T., Komiyama B., Sasaoka H. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels //

IEEE Transactions on Antennas and Propagation. 2005. V. 53, No. 11. P. 3776-3784. DOI: 10.1109/TAP.2005.858853

3. Mathur S., Trappe W., Mandayam N., Ye C., Reznik A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. *14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008*, San Francisco, California, USA, September 14-19, 2008. P. 128-139. DOI: 10.1145/1409944.1409960

4. Premnath S.N., Gowda P.L., Kasera S.K., Patwari N., Ricci R. Secret Key Extraction using Bluetooth Wireless Signal Strength Measurements. *IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2014. P. 293-301. DOI: 10.1109/SAHCN.2014.6990365

5. Azimi-Sadjadi B., Kiayias A., Mercado A., Yener B. Robust key generation from signal envelopes in wireless networks. *Proceedings of the 14th ACM conference on Computer and communications security*, 2007. P. 401-410. DOI: 10.1145/1315245.1315295

6. Jana S., Premnath S.N., Clark M., Kasera S.K., Patwari N., Krishnamurthy S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments. *Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom)*. 2009. P. 321-332.

7. Assche G. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006. 276 p.

8. Brassard G., Salvail L. *Secret-Key Reconciliation by Public Discussion*. Lecture Notes in Computer Science. 2001. P. 410-423.

9. Shannon C.E. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949. No. 28 (4). P. 656-715.

10. Duan S. *Security analysis of tetra*. Master's thesis. Norwegian University of Science and Technology Department of Telematics, 2013.

11. Benantar M. The Internet public key infrastructure. *IBM Systems Journal*. 2001. No. 40 (3). P. 648-665. DOI: 10.1147/sj.403.0648

12. Shannon C. E. The Mathematical Theory of Communication. *The Bell System Technical Journal*. 1948. V. 27, No. 3. P. 379-423.

13. Akinbiyi O. *Physical layer security using artificial noise*. The University of Leeds School of Electronic and Electrical Engineering, 2012.

14. Wyner A.D. The Wiretap Channel. *Bell System Technology Journal*. 1975. V. 54, P. 1355-1387. DOI: 10.1002/j.1538-7305.1975.tb02040

15. Rehman S.U., Sowerby K.W., Alam S., Ardekani I. Radio Frequency Fingerprinting and its Challenges. *IEEE Conference on Communicati.ons and Network Security*. 2014. P. 496-497. DOI: 10.1109/CNS.2014.6997522

16. Sakai M., Lin H., Yamashita K. Sakai M. Intrinsic Interference Based Physical Layer Encryption for OFDM/OQAM. *IEEE Communications Letters*. 2017. No. 21 (5). P. 1059-1062. DOI: 10.1109/LCOMM.2017.2654442

17. Bakhtin A.A., Volkov A.S., Baskakov A.E. Research of the implementation features of environment access algorithms in mobile self-organizing communication networks. *Trudy MAI*. 2017. No. 97. (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=87331

18. Eliseev S.O., Kryukov D.A. System of cryptographic generation of identical data based on the Diffie-Hellman algorithm. *Trudy MAI*. 2018. No. 101. (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=97041

19. Fomin A.I., Aiman Khamad. Analysis of communication reliability in channels with fast and slow fading. *Trudy MAI*. 2008. No. 30. (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=7525

20. Volkov A., Chi Jie., Gorelik A., Solodkov A., Sviridov I. Classification of radio signals in multipath fading channel using neural network. *2024 Conference Young Researchers in Electrical and Electronic Engineering (2024 ElCon)*, Saint Petersburg Electrotechnical University «LETI», January 29-30, 2024, Russia. P. 919-923.

21. Volkov A.S., Kreindelin V.B. Algorithms for encoding algebraic non-binary cascading convolutional codes of reduced complexity. *T-Comm – Telekommunikatsii i Transport*. 2024. V. 18, No. 3. P. 11-18. (In Russ.). DOI: 10.36724/2072-8735-2024-18-3-11-18

22. Volkov A.S. The development of simulation model of channel with burst error arrays. *Trudy MAI*. 2023. No. 128. (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=171396. DOI: 10.34759/trd-2023-128-12

Статья поступила в редакцию 17.11.2024
Одобрена после рецензирования 19.11.2024
Принята к публикации 25.12.2024
The article was submitted on 17.11.2024; approved after reviewing on 19.11.2024; accepted for publication on 25.12.2024