Оценка значимости доминирующих парциальных лучей в многолучевой смеси радиосигнала в задачах генерации ключей шифрования

А. И. Сулимов, О. Н. Шерстюков, А. В. Карпов
Кафедра радиофизики, Институт физики
Казанский (Приволжский) федеральный университет
420008, Российская Федерация, г. Казань, ул. Кремлевская, д.18
asulimo@gmail.com, lada-sher@mail.ru, arkadi.karpov@kpfu.ru

***Аннотация* — Случайность быстрых замираний в многолучевом канале уже длительное время используется для генерации ключей шифрования. При этом защищенность порождаемого ключа базируется на предположении о невозможности перехвата всех парциальных лучей, образующих принимаемый сигнал. Однако во многих случаях принципиальная информация о характере случайных замираний и генерируемом ключе содержится всего в одном или двух доминирующих лучах. В данной работе анализируется возможность генерации частичного ключа шифрования, высоко коррелирующего с ключом легальных абонентов, если постороннему лицу известны характеристики лишь малого количества доминирующих лучей. Методом имитационного моделирования выполнены оценки корреляции частичной фазы сигнала, образованной только доминирующими лучами, с его полной фазой, образованной всей совокупностью лучей, при различном вкладе доминирующей компоненты в многолучевую смесь на входе приемника. На основе этих данных оценена вероятность перехвата ключа шифрования в фазовых системах многолучевой генерации ключей. Рассмотрено влияние сигнала прямой видимости и количества парциальных лучей на корреляцию частичной и полной фаз многолучевого сигнала. Показано, что серьёзная угроза перехвата ключа возникает, только если на доминирующую компоненту приходится свыше 95% мощности сигнала, что маловероятно на практике.**

Ключевые слова — многолучевый канал; ключ шифрования; фаза сигнала; парциальные волны; частичная фаза; частичный ключ шифрования; корреляция

I. Введение

Многолучевая генерация ключей шифрования использует случайность быстрых замираний в канале для создания в двух узлах связи A и B идентичных копий секретного ключа [1]. Для этого стороны обмениваются серией зондирующих сигналов. Распространяясь в многолучевой среде, сигналы приобретают случайную модуляцию быстрыми замираниями, детектируя которую, пункты порождают случайные последовательности key_A и key_B. Благодаря взаимности канала эти последовательности одинаковы ($key_A = key_B$) и известны только узлам A и B, что позволяет использовать их в качестве секретных ключей шифрования. Такая картина распространения сигнала типична для городских условий, поэтому описанный метод может использоваться в системах сотовой связи для порождения на базовой станции и мобильном терминале секретных ключей шифрования.

Для генерации ключей могут использоваться различные параметры принимаемого сигнала, но одними из наиболее защищенных являются фазовые методы [2][3]. Периодичность фазы сигнала вместе с неоднозначностью измерений препятствует её достоверному перехвату на расстояниях более $\lambda/2$ от легального устройства связи. Защищенность порождаемого ключа базируется на быстрой пространственной декорреляции фазы сигнала в условиях разнесённого приема. Физически, это означает, что посторонний приемник не может перехватить все парциальные лучи, регистрируемые легальным абонентом. Как правило, при анализе беспроводных систем связи в городских условиях используется модель рэлеевского канала, в которой предполагается, что все лучи имеют одинаковую мощность. Более общая модель канала, основанная на распределении Накагами, учитывает наличие в многолучевой смеси нескольких доминирующих лучей [4]. Доминирующая компонента содержит принципиальную информацию о случайных вариациях фазы и генерируемых ключах, поэтому перехват небольшого количества лучей может серьёзно скомпрометировать ключ легальных абонентов.

Другой возможной атакой на систему является внешнее навязывание модуляции, полностью компрометирующая, например, системы с амплитудной генерацией ключа [5][6]. В рамках данной атаки в окрестности легальных абонентов размещается несколько мощных передатчиков, излучающих сигнал, модулированный по известному закону, имитирующему естественные замирания в канале. Фактически, каждый посторонний передатчик имитирует один из доминирующих лучей. При этом легальные абоненты, накапливая модулированные измерения фазы, создают ключ, в подавляющей степени определяемый закономерностью, известной атакующей стороне, что компрометирует систему.

Работа выполнена при поддержке Программы Повышения Конкурентоспособности Казанского Федерального Университета.

Целью данной работы является оценка возможности генерации частичного ключа шифрования, высоко коррелирующего с ключом легальных абонентов, если постороннему лицу известны лишь характеристики малого количества доминирующих лучей. В работе будут представлены оценки корреляции частичной фазы сигнала, образованной лишь доминирующими лучами, с полной фазой, образованной всей совокупностью лучей, при различном вкладе доминирующей компоненты в многолучевую смесь. Путем бинарного квантования отсчётов полной и частичной фазы будет выполнена генерация эталонной и частичной ключевых последовательностей, сопоставление которых позволит оценить вероятность перехвата ключа. Указанные оценки будут выполнены при условиях наличия и отсутствия сигнала прямой видимости, а также при типичном (12 лучей) и малом (3 луча) количестве парциальных лучей.

Дальнейшее содержание статьи будет придерживаться следующей структуры. В разделе II будет представлена модель рассматриваемой задачи. Методика и параметры имитационного моделирования будут изложены в разделе III. В разделе IV будут представлены результаты оценок корреляции частичной фазы доминирующей компоненты и полной фазы сигнала. Результаты оценок вероятности перехвата генерируемых ключей будут представлены в разделе V. В заключении будут сформулированы основные выводы исследования.

II. Модель Системы

В этом разделе будет описана исследуемая система, представлено математическое описание многолучевого сигнала с доминирующими лучами, а также указаны условия осуществления пассивной и активной атак.

В рамках исследования рассматривается многолучевое распространение в типичных городских условиях. Два пункта связи A и B (например, базовая станция BTS и мобильный терминал MT системы сотовой связи) обмениваются серией зондирующих сигналов в полудуплексном режиме с интервалом разделения по времени порядка 0,1-10 мс. Стороны зондируют канал длительными радиоимпульсами с немодулированным заполнением несущей частотой f порядка 1-5 *ГГц*. При приеме стороны детектируют фазу несущей φ_A и φ_B, которая случайна из-за замираний канала. В силу взаимности канала, измерения обеих сторон совпадают ($\varphi_A = \varphi_B$). Стороны накапливают по N измерений фазы и подвергают выборки $\{\varphi_A\}_N$ и $\{\varphi_B\}_N$ бинарному квантованию, чем формируют экземпляры ключевой последовательности key_A и key_B. В реальной практике схема генерации ключа сложнее и может включать в себя дополнительные этапы по устранению битовых ошибок, улучшению статистических характеристик ключа и усилению конфиденциальности. Поскольку целью данного исследования является анализ возможности перехвата ключа на физическом уровне, то мы ограничимся описанной выше упрощенной схемой генерации ключа.

A. Модель сигнала

В рамках модели предполагается, что канал зондируется немодулированной гармоникой с частотой f. Принимаемый сигнал представляет собой интерференцию (n+1) парциальных лучей, из которых два луча являются доминирующими, а нулевой луч соответствует сигналу прямой видимости. Комплексная амплитуда принимаемого многолучевого сигнала описывается выражением:

$$A \cdot e^{i\varphi} = \sqrt{2k_R} \cdot A_0 \cdot e^{i\varphi_0} + G_1 A_1 \cdot e^{i\varphi_1} + G_2 A_2 \cdot e^{i\varphi_2} + \sum_{k=3}^{n} A_k \cdot e^{i\varphi_k}, \quad (1)$$

где A_k и φ_k – амплитуда и фаза парциальных лучей, k_R – коэффициент Райса, а G_1 и G_2 – коэффициенты доминирования первого и второго лучей, соответственно. Количество лучей n является случайным процессом с Пуассоновским распределением и средним $E(n)$. В рамках модели (1) предполагается, что амплитуды лучей A_k подчиняются логнормальному закону распределения со средним значением, нормированным на мощность принимаемого сигнала P_R:

$$E(A_k) = \sqrt{\frac{P_R}{\{E(n) - 2 + G_1^2 + G_2^2\} \cdot (2k_R + 1)}}. \quad (2)$$

В свою очередь, мощность сигнала P_R и дисперсия амплитуды лучей $var(A_k)$, обусловленная медленными замираниями канала, прогнозируются согласно выбранной модели распространения сигнала. В нашем исследовании использовалась усовершенствованная модель Хата для короткодействующих устройств связи (extended Hata-SRD model) [7]. Фазы лучей φ_k в подавляющей степени определяются задержкой по времени и имеют близкое к равномерному распределение.

Модель сигнала (1) позволяет рассматривать различные распределения мощности сигнала между прямой волной и доминирующими лучами, что позволяет анализировать их вклад в результирующую фазу сигнала φ. Отметим, что в рамках модели (1) огибающая сигнала A подчиняется уже не одномодовому, а двухмодовому распределению Райса.

B. Модель пассивного перехвата ключа

В рамках пассивной атаки предполагается, что постороннее устройство связи «C» работает только на прием, не излучая никаких сигналов в эфир. Для перехвата ключа устройство «C» размещается на некотором расстоянии от одного из абонентов, например, абонента «B». Устройство «C» полностью идентично устройствам «A» и «B», а также идеально синхронизировано с ними по частоте. Далее предполагается, что пункту «C» с нулевой погрешностью известны координаты пунктов «A» и «B», координаты рассеивателей S_1 и S_2, порождающих доминирующие лучи 1 и 2, принимаемые абонентом «B», а также амплитуды G_1A_1 и G_2A_2 этих лучей. Поскольку прямая волна не содержит случайности, предполагается,

что характеристики нулевого луча также известны пункту «*C*». На основании этих данных, путем решения комплексного уравнения (3), вычисляется частичная фаза φ_{012} многолучевого сигнала:

$$A_{012} \cdot e^{i\varphi_{012}} = \sqrt{2k_R} \cdot A_0 \cdot e^{i\varphi_0} + G_1 A_1 \cdot e^{i\varphi_1} + G_2 A_2 \cdot e^{i\varphi_2}, \qquad (3)$$

которая принимается в качестве оценки измеренной «*B*» полной фазы: $\hat{\varphi}_B = \varphi_{012}$. С использованием этих оценок пункт «*C*» создаёт частичный ключ key_{012}, коррелированный с эталонным ключом *key*, создаваемым легальными абонентами из измерений полной фазы φ.

Для анализа вклада различных лучей, помимо фазы φ_{012}, в качестве оценки φ_B использовались также и усеченные частичные фазы $\{\varphi_1, \varphi_{01}, \varphi_{12}\}$.

C. Модель активного перехвата ключа

В отличие от пассивного случая, при активной атаке на систему посторонний субъект «*C*» может не только принимать, но и излучать имитационные сигналы. В пассивном случае предполагалось, что атакующий субъект с нулевой погрешностью оценивает характеристики обоих доминирующих лучей, принимаемых легальным абонентом «*B*», что трудно осуществимо на практике. Гораздо более реалистичный сценарий предполагает, что атакующий субъект самостоятельно формирует доминирующие лучи. Для атаки на систему посторонний субъект размещает в окрестности легальных пунктов «*A*» и «*B*» две пары мощных передатчиков $\{C_{A1}; C_{A2}\}$ и $\{C_{B1}; C_{B2}\}$, которые имитируют для каждой из сторон доминирующие лучи. Так как закон модуляции этих «лучей» по амплитуде, фазе и временной задержке задаётся атакующим субъектом, то ему известны их характеристики на стороне легального приемника (например, абонента «*B*»). В остальном, характер атаки и алгоритм оценки частичного ключа аналогичны случаю пассивной атаки.

III. Методика Моделирования Канала

Для корреляции частичной и полной амплитуд многолучевого сигнала $corr(A_{012}, A)$ могут быть получены компактные аналитические выражения. К сожалению, это невозможно при рассмотрении корреляции фазовых характеристик сигнала, поэтому для решения этой задачи целесообразно привлечь методы имитационного моделирования.

В нашем исследовании использовался метод моделирования, описанный в [8]. Модель имитировала канал связи между базовой станцией BTS (пункт «*A*») и мобильным терминалом абонента MT (пункт «*B*») системы сотовой связи. Модель генерировала n случайно распределенных в пространстве независимых рассеивателей, после чего выполняла трассировку n порожденных ими парциальных лучей в точку приёма. Мощность прямой волны и двух доминирующих лучей корректировались с учетом коэффициента Райса k_R и коэффициентов $\{G_1; G_2\}$, соответственно. Далее, согласно (1) и (2), вычислялась полная фаза сигнала φ. Частичные фазы $\{\varphi_1, \varphi_{01}, \varphi_{12}, \varphi_{012}\}$ вычислялись согласно (3) путем зануления соответствующих слагаемых. Количество лучей n моделировалось как пуассоновский случайный процесс со средним значением $E(n)$. Физически, изменчивость количества лучей в канале обусловлена случайным перемещением терминала MT. Для моделирования типичных городских условий распространения задавалось значение $E(n) = 12$, а для моделирования среды со слабой многолучевостью – значение $E(n) = 3$. Помимо парциальных лучей, на приемник действовал и сигнал прямой видимости (нулевой луч), мощность которого задавалась коэффициентом Райса k_R. Чтобы оценить влияние нулевого луча, рассматривалось два значения коэффициента Райса: 1) $k_R(dB) \to -\infty$ (отсутствие прямой волны); 2) $k_R \to 15dB$ (мощная прямая волна).

ТАБЛИЦА I Параметры Имитационного Моделирования

Технические параметры	**Значения параметров**
Протяженность радиолинии, d(*м*)	200
Несущая частота, f (*МГц*)	1000
Высота подвеса антенн	h_{BTS} = 30 *м*, h_{MT} = 1.5 *м*
Тип антенн	всенаправленные (0 *dBi*)
Отношение (сигнал/шум), *SNR* (дБ)	20
Среднее количество лучей, $E(n)$	12 / 3
Коэффициент Райса, k_R (дБ)	-∞ / 15
Коэффициент доминирования, $G_{1,2}$ (дБ)	-40…60
Скорость MT, V (*м/с*)	10
Длительность сеанса связи, T_S (*с*)	30

Для каждой комбинации значений коэффициентов $\{G_1, G_2\}$ имитировался сеанс связи длительностью T_S = 30 *с* при скорости движения MT V = 10 *м/с*. Таким образом, за время сеанса терминал покрывал расстояние порядка 300 метров. Отсчёты полной и частичных фаз сигнала вычислялись с интервалом 0,4 *мс*, что позволило синтезировать выборку объёмом 750000 отсчётов. Эти данные использовались для корреляционного анализа фазы сигнала и для генерации ключей шифрования. В Табл.1 представлены основные параметры моделирования канала.

IV. Анализ Корреляции Частичной Фазы Сигнала

Для оценки вклада доминирующих лучей в полную фазу многолучевого сигнала был выполнен цикл имитационных экспериментов. В рамках каждого эксперимента коэффициентам доминирования лучей G_i придавались различные значения из диапазона от минус 40 дБ до 60 дБ, где $G_i(dB) = 20\lg G_i$ ($i = \{1,2\}$). В качестве частного случая (G_2 = 0 дБ) рассматривался канал с одним доминирующим лучом. Кроме того, рассматривались различные соотношения мощности доминирующих лучей: 1) лучи равной мощности ($G_2 = G_1$); 2) мощность одного луча в четыре раза превосходила мощного другого ($G_2 = G_1/2$ или, эквивалентно, G_2(дБ) = G_1(дБ) – 6).

На рис. 1 представлены результаты моделирования зависимости коэффициента корреляции $R(\varphi_1, \varphi)$ частичной фазы φ_1 первого доминирующего луча с полной фазой сигнала φ от коэффициентов доминирования $\{G_1, G_2\}$.

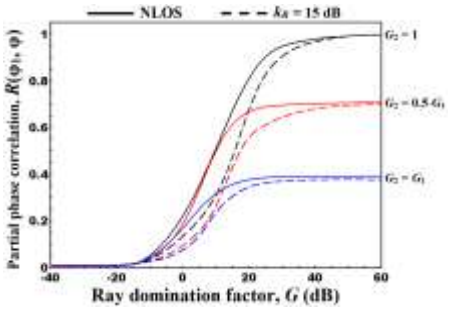


Рис. 1. Корреляция частичной и полной фаз многолучевого сигнала ($E(n) = 12$).

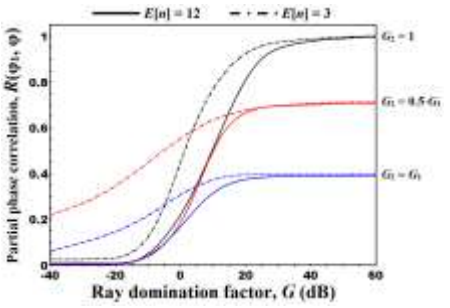


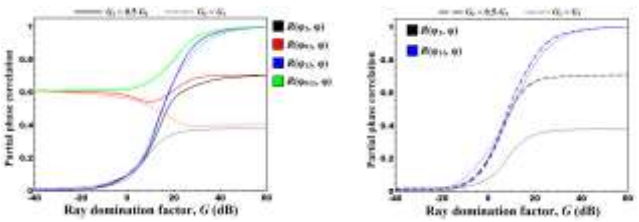
Рис. 2. Корреляция частичной и полной фаз многолучевого сигнала (NLOS).

Сплошной линией изображены результаты для канала без прямой волны (k_R = 0), а пунктирной – для канала с мощной прямой волной (k_R = 15 дБ). Оценки корреляции выполнены для различных соотношений амплитуд доминирующих лучей. При этом случай $\{G_2 = 1\}$ описывает как пассивную, так и активную, атаки на систему при наличии в канале одного доминирующего луча. Случаи $\{G_2 = G_1/2\}$ и $\{G_2 = G_1\}$ характеризуют пассивную атаку, при которой постороннему пункту «C» известны характеристики только одного из двух доминирующих лучей.

Из рис. 1 видно, что с ростом коэффициента доминирования значимость первого луча монотонно возрастает, а корреляция стремится к некоторому предельному уровню, достигая его при $G \sim 1000$. В однолучевом случае предельный уровень соответствует абсолютной корреляции. Для случаев $\{G_2 = G_1/2\}$ и $\{G_2 = G_1\}$ предельная корреляция составляет приблизительно $1/\sqrt{2}$ и $1/\sqrt{2\pi}$, соответственно. Отметим, что эти значения отличаются от интуитивных оценок 2/3 и 1/2. Наличие прямой волны ослабляло значимость доминирующего луча, снижая корреляцию на величину до 0,25. В типичной городской среде распространения ($E(n)$ = 12, k_R = 0) вклад единственного доминирующего луча в полную фазу сигнала становился определяющим, если его мощность примерно в 10-11 раз превосходила среднюю мощность одного луча, что соответствует условию равенства мощности доминирующего луча и мощности остаточной компоненты сигнала. Корреляция свыше 0,9, позволяющая примерно с 95% достоверностью перехватывать каждый бит генерируемого ключа, достигалась при коэффициенте доминирования $G_1 > 25$ дБ, что соответствует 96,5%-доле мощности сигнала.

На рис. 2 представлено сопоставление уровня корреляции частичной фазы первого луча в каналах с типичным (сплошная линия) и малым (штрихпунктир) количеством лучей в отсутствие прямой волны. Видно, что с уменьшением парциальных компонент значимость доминирующего луча возрастает. Однако предельные уровни корреляции от количества лучей не зависят, а определяются лишь долей мощности сигнала, приходящейся на рассматриваемую частичную компоненту. Вклад единственного доминирующего луча в фазу трехлучевого сигнала становился определяющим при $G_1 > 1{,}3$ дБ, а при $G_1 > 17{,}5$ дБ уровень корреляции достигал 0,9, что также соответствует доле мощности доминирующего луча порядка 96,5% от мощности сигнала.

На рис. 3 представлено сопоставление уровней корреляции различных частичных фаз с полной фазой сигнала в 12-лучевом канале как при наличии (а), так и в отсутствие (б) прямой волны. Анализ показал, что, в независимости от мощности прямой волны, численные значения уровня корреляции $R(\varphi_{12}, \varphi)$ для частичной фазы φ_{12} были близки к величинам $R(\varphi_1, \varphi)$, наблюдавшимся для частичной фазы φ_1 при $G_2 = 1$. Следовательно, частичная фаза φ_{12} для 12-лучевого канала с двумя доминирующими лучами примерно соответствует частичной фазе φ_1 для 11-лучевого канала с одним доминирующим лучом. По-видимому, этот вывод можно распространить и на каналы с бо́льшим количеством доминирующих лучей, но данный вопрос требует дополнительных исследований. Учёт прямой волны и второго доминирующего луча улучшал оценку полной фазы сигнала φ_B, измеренной легальным абонентом. При этом уровень корреляции частичной фазы, учитывающей оба доминирующих луча, слабо зависел от соотношения их мощностей. В частности, кривые, построенные для случаев $\{G_2 = G_1/2\}$ и $\{G_2 = G_1\}$, демонстрировали близкие численные результаты. Прямая волна, мощность которой на 15 дБ превосходила мощность остаточной многолучевой компоненты, играла в полной фазе определяющую роль вплоть до значений $G \sim 10$ дБ, что соответствовало примерно 50%-доле мощности прямой волны. С ростом значимости второго луча корреляция частичной фазы φ_{01} закономерно снижалась, асимптотически стремясь к предельному уровню корреляции для частичной фазы φ_1. Для всех рассмотренных частичных фаз корреляция выходила на установившийся уровень при G порядка 20–25 дБ, что соответствовало примерно 95%-доле мощности рассматриваемой доминирующей компоненты сигнала.



(a) k_R = 15 дБ (b) NLOS

Рис. 3. Корреляция частичной и полной фаз многолучевого сигнала для различных частичных компонент ($E(n) = 12$).

Сопоставление результатов на рис. 3(а) и рис. 3(б) позволяет сделать один неожиданный вывод о значимости прямой волны при атаке на систему многолучевой генерации ключей. Интуитивное представление подсказывает, что при наличии мощной прямой волны канал становится более предсказуемым, что должно упрощать оценку фазы сигнала абонента и повышать вероятность перехвата ключа. В то время как при малых коэффициентах доминирования это предположение безусловно выполняется, оно теряет силу при больших значениях G. В частности, при значениях коэффициента G_1 более 12 дБ уровень корреляции $R(\varphi_1, \varphi)$, наблюдавшийся при $k_R = 0$, превосходил корреляцию $R(\varphi_{01}, \varphi)$, полученную при $k_R = 15$ дБ. Аналогично, при G_1 более 17 дБ уровень корреляции $R(\varphi_{12}, \varphi)$, наблюдавшийся при $k_R = 0$, превосходил корреляцию $R(\varphi_{012}, \varphi)$, полученную при $k_R = 15$ дБ. Иными словами, наличие мощной прямой волны не упрощало, а затрудняло оценку полной фазы сигнала. По всей видимости, этот эффект объясняется вероятностным характером интерференции доминирующих лучей с прямой волной, что вносит в частичную фазу дополнительные осцилляции, ослабляющие её корреляцию с полной фазой сигнала.

Полученные результаты показали, что знание характеристик небольшого количества лучей, доминирующих в многолучевой смеси, при определенных условиях позволяет эффективно оценивать полную фазы сигнала, что порождает угрозу перехвата генерируемых ключей. Оценки вероятности утечки ключа будут представлены в следующем разделе.

V. Оценка Вероятности Перехвата Ключа

Для формирования ключевой последовательности выборки отсчётов полной и частичных фаз сигнала были подвергнуты обработке согласно методике [3]. На первом этапе обработки устранялись корреляционные связи в выборке. После этого отсчеты фазы подвергались бинарному квантованию, что позволило создать эталонный ключ *key*, сформированный из отсчетов полной фазы сигнала, и набор частичных ключей $\{key_1, key_{01}, key_{12}, key_{012}\}$, соответствующих частичным фазам $\{\varphi_1, \varphi_{01}, \varphi_{12}, \varphi_{012}\}$. Объём ключевых последовательностей составил приблизительно 12000 *бит*. Путем побитового сопоставления частичных ключей с эталонным оценивалась вероятность его перехвата при атаке с использованием информации о доминирующих лучах. В качестве вероятностной меры успешности перехвата определялась доля отличающихся битовых позиций p_e в сверяемых ключевых последовательностях.

На рис. 4 представлены результаты оценки вероятности рассогласования одного бита частичного ключа key_1 с эталонным ключом *key* при различных коэффициентах доминирования первого луча. Аналогично рис. 1, оценки выполнены при различной мощности прямой волны и при различных вкладах второго доминирующего луча. Оценки показали, что при учете только одного из двух доминирующих лучей существует предельно низкая вероятность рассогласования p_e. Для случая $\{G_2 = G_1/2\}$ она составила 11,5%, и 27% – для случая $\{G_2 = G_1\}$. Учет

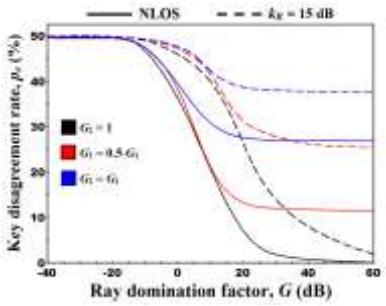
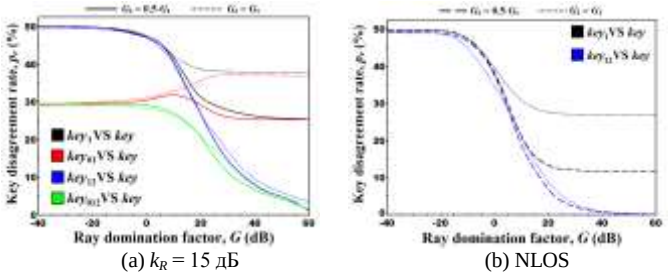


Рис. 4. Вероятность рассогласования одного бита ключа шифрования, соответствующего частичной фазе первого луча ($E(n) = 12$).

сигнала прямой видимости также значительно влияет на возможность перехвата эталонного ключа. В канале с одним доминирующим лучом и без прямой волны каждый бит генерируемого ключа может быть перехвачен с достоверностью 99%, если коэффициент доминирования G_1 превосходит 35 дБ. Последнее эквивалентно случаю, когда на доминирующий луч приходится около 99,6% от мощности сигнала. Для более реалистичного случая, когда на доминирующий луч приходится 80% мощности сигнала, величина p_e составляет 11,3%. В случае 50%-доли мощности, вероятность p_e возрастает до 20%. Из Рис. 4 также видно, что учет парциального луча, мощность которого на 17 дБ ниже мощности остальных лучей (эквивалентно доли мощности 0,2%), практически не улучшает оценки полной фазы многолучевой смеси. Такими «побочными» лучами можно пренебрегать.

На рис. 5 представлены результаты оценки вероятности рассогласования частичных и эталонного ключей шифрования при аналогичных рис. 3 параметрах моделирования. Из рис. 5 видно, что по мере роста коэффициентов G_1 и G_2 учет обоих доминирующих лучей позволяет значительно повысить вероятность перехвата ключа. При этом распределение мощности между ними слабо влияло на величину p_e. Как следует из рис. 5(а), если в канале доминирующие лучи отсутствуют, то информация о детерминированной парциальной фазе прямой волны позволяет успешно перехватывать каждый бит ключевой последовательности с вероятностью не менее 70%. Тем не менее, с ростом коэффициентов доминирования, как и отмечалось в разделе IV, наличие прямой волны повышает вероятность рассогласования ключей. В частности, в канале без прямой волны при G более 45 дБ, вероятность p_e составляла менее 0,5%, в то



(а) k_R = 15 дБ (b) NLOS

Рис. 5. Вероятность рассогласования одного бита ключа шифрования, соответствующего различным частичным фазам сигнала ($E(n) = 12$).

время как в канале с мощной прямой волной данная вероятность не опускалась ниже 5%.

Представленные оценки показали, что атака на многолучевую систему генерации ключей с использованием информации о доминирующих лучах является эффективным методом перехвата ключа только в случае их значительного (свыше 95%) доминирования в многолучевой смеси сигнала, что маловероятно на практике. Таким образом, полученные результаты доказывают высокую устойчивость фазовых систем многолучевой генерации ключей к активной атаке, основанной на навязывании внешней модуляции.

VI. Заключение

В данной работе выполнялась оценка вклада доминирующих парциальных лучей в полную фазу многолучевой смеси сигнала, принимаемого в городских условиях. Оценки выполнены как при наличии, так и в отсутствие сигнала прямой видимости в канале, для сред с типичным (12 лучей) и малым (3 луча) количеством парциальных лучей. Методом имитационного моделирования получены зависимости корреляции частичной и полной фазы многолучевого сигнала от доли мощности, приходящейся на доминирующие лучи. Оценки показали, что вклад единственного доминирующего луча в полную фазу сигнала становится определяющим, если его мощность сравнивается с мощностью остаточной многолучевой компоненты. Корреляция парциальной фазы с полной фазой сигнала 0,9 достигается, если на долю доминирующего луча приходится свыше 96,5% мощности сигнала, что маловероятно на практике. В канале с двумя доминирующими лучами аналогичная корреляция достигается, если суммарная мощность доминирующей компоненты составляет 98%–99% от мощности сигнала. Анализ результатов показал, что при той же суммарной доли мощности сигнала, приходящейся на доминирующую компоненту, корреляция её частичной фазы с полной фазой сигнала повышается с уменьшением количества доминирующих лучей.

Были выполнены оценки вероятности рассогласования частичных ключей шифрования с эталонным ключом, созданным путём бинарного квантования отсчётов полной фазы сигнала. Оценки показали, что в канале с одним доминирующим лучом битовая вероятность рассогласования эталонного и частичного ключей p_e не превосходит 1%, если на долю доминирующего луча приходится не менее 99,6% мощности сигнала. Для более реалистичного сценария, когда на доминирующую компоненту приходится 80% мощности сигнала, величина p_e составляет 11,3%. В случае 50%-доли мощности, вероятность p_e возрастает до 20%. Влияние парциальных лучей с долей мощности менее 0,2% от мощности сигнала пренебрежимо мало. Использование информации о детерминированной фазе прямой волны может позволить с вероятностью не менее 70% успешно оценивать каждый бит генерируемой ключевой последовательности (при k_R = 15 дБ).

Полученные результаты показали, что атака на многолучевую систему генерации ключей с использованием информации о доминирующих лучах является эффективным методом перехвата ключа только в случае их значительного (свыше 95%) доминирования в многолучевой смеси сигнала, что маловероятно на практике. Это доказывает высокую устойчивость фазовых методов порождения ключей к активной атаке, основанной на навязывании внешней модуляции.

Список литературы

[1] J. Zhang et al., “Key generation from wireless channels: a review,” IEEE Access, vol. 4, pp. 614-626, Jan. 2016.

[2] A.A. Hassan, W.E. Stark, J.E. Hershey, S. Chennakeshu, “Cryptographic key agreement for mobile radio,” Digital Signal Processing, vol.6, iss.4, pp. 207-212, 1996.

[3] A.I. Sulimov et a.l, “Experimental study of performance and security constraints on wireless key distribution using random phase of multipath radio signal,” Proc. 11th Int. Conf. on Security and Cryptography (SECRYPT-2014), pp. 411-416, Vienna (Austria), Aug. 2014.

[4] S.S. Saunders, A. Aragon-Zavala, “Antennas and propagation for wireless communication systems,” John Wiley & Sons, 553 p., 2007.

[5] S. Jana et al., “On the effectiveness of secret key extraction from wireless signal strength in real environments,” Proc. 15th Ann. Int. Conf. on Mob. Comp. and Networking (MobiCom' 09), pp. 321-332, Sept. 2009.

[6] S. Mathur et al., “ProxiMate: Proximity-based secure pairing using ambient wireless signals,” Proc. 9th Int. Conf. on Mob. systems, applications, and services (MobiSys' 11), pp. 211-224, Bethesda (Maryland, USA), June 2011.

[7] SEAMCAT: Spectrum Engineering Advanced Monte Carlo Analysis Tool. Handbook, European Communication Office (CEPT), 221p., 2010.

[8] A.I. Sulimov et al., “Analysis of frequency-correlation properties of multipath channel for encryption key generation using samples of differential phase,” Proc. Moscow Workshop on Electronic and Networking Technologies (MWENT-2018), pp. 1-7, Moscow (Russia), March 2018.