УДК 621.371.332

И. Е. АНТИПОВ, д-р техн. наук, А. А. КОСТЫРЯ, канд. техн. наук, М. А. ШЕРНИН

ИСПОЛЬЗОВАНИЕ МЕТЕОРНОГО РАДИОКАНАЛА ДЛЯ ФОРМИРОВАНИЯ СЛУЧАЙНОЙ ЧИСЛОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Широко известное явление метеор связано с вторжением в атмосферу мелких космических частиц. Благодаря отражению радиоволн от метеорного следа возможна радиосвязь на расстояния до 2000 *км*. Связь прерывистая, с небольшой средней скоростью передачи [1].

Использование метеорного радиоканала (МРК) сопряжено со многими случайными факторами. Неизвестными являются момент возникновения следа, его длительность, амплитуда принимаемого сигнала и её поведение в течение времени существования следа. Время распространения сигнала по трассе также является случайным, как и само местоположение следа в пространстве. Для работы систем метеорной связи применяются специальные алгоритмы, позволяющие работать в таких условиях.

Но существует область применения, где эта случайность не только не мешает решению задач, а наоборот, способствует. Это формирование случайной последовательности, которая может быть использована для последующей криптографической защиты информации.

Как известно, криптографические системы в зависимости от типа используемых криптографических алгоритмов подразделяются на 3 класса: симметричные, асимметричные, комбинированные (симметричные + асимметричные). Рассмотрим возможность использования симметричного алгоритма. Его особенностью является то, что ключи, которые используются для шифрования $K_З$ и для дешифрования $K_Р$, совпадают, т. е. $K_З = K_Р$ (или один из них может быть выражен через другой не более чем с полиномиальной сложностью.) Под ключом подразумевается совокупность случайных значений переменных параметров криптографического преобразования информации. Ключевые данные в симметричных криптосистемах распределяются и распространяются с использованием специальных носителей (ключевых документов) [2].

Формирование случайной последовательности может быть основано на численном анализе какого-либо случайного процесса. Например, существуют физические генераторы шума, в основе которых лежит использование природных шумовых процессов в реальных физических элементах (резисторах, полупроводниках и т. д.). В частности применяется датчик шума на основе полупроводниковых устройств с Зенеровским пробоем (стабилитронов) [3]. Эти генераторы способны формировать случайные числовые последовательности, которые могут быть использованы в качестве ключа.

Уязвимым местом такого способа формирования является то, что сформированную последовательность (ключ) необходимо каким-то образом доставить второму корреспонденту, поскольку сформировать две одинаковые последовательности в приемном и передающем пунктах невозможно.

С этой точки зрения метеорный радиоканал с его многочисленными случайными характеристиками можно представить как случайный природный процесс, наблюдаемый одновременно из двух пунктов. Перечислим, какие именно характеристики МРК являются случайными:

– момент возникновения радиоотражения;
– длительность радиоотражения;
– интервал между радиоотражениями;
– время распространения сигнала по трассе;
– местоположение следа в пространстве;
– форма амплитудно-временной характеристики.

Каждая из этих характеристик в отдельности или их совокупность может быть использована для формирования случайной числовой последовательности.

Идея использования МРК для формирования ключа ранее рассматривалась и другими авторами. В частности, в работах [4, 5] рассмотрена возможность дистанционной генерации

ключа, при которой ключ не передается от одного абонента к другому, а создается на передающей и приемной сторонах метеорного радиоканала одновременно путем измерения одного и того же процесса, который не доступен криптоаналитику. Принцип состоит в том, что в приемном и передающем пунктах системы метеорной связи измеряется случайное для данного метеорного радиоотражения время распространения сигнала по трассе. Благодаря высокой стабильности и взаимности канала результаты получаются одинаковыми в обоих пунктах. Производительность такого способа авторы [4] оценивают в 100 *бит* в час.

Недостатком такого способа является то, что для его реализации и обеспечения указанной производительности в обоих пунктах необходимо иметь высокоточные эталоны времени со шкалами, сведёнными с погрешностью не хуже 1 *нс*.

В статье предлагается способ формирования случайной числовой последовательности, основанный на определении местоположения следа.

Отражение от метеорного следа может происходить в любой точке пространства, для которой выполняется условие зеркальности [1]. На рис. 1 представлено полученное расчётным путём положение так называемых «горячих зон» – областей, в которых концентрируются полезные для связи метеорные следы для трассы длиной 300 *км*, по данным работы [6]. В работе [1] приводятся результаты моделирования для трассы длиной 450 *км* (рис. 2). Следует добавить, что представленные рисунки не отображают высотного диапазона следов, который составляет 80 – 100 *км*. Следовательно, метеорные следы могут возникать в достаточно большом объёме пространства. При этом определить, в каком месте и в какое время возникнет каждый новый метеор невозможно.

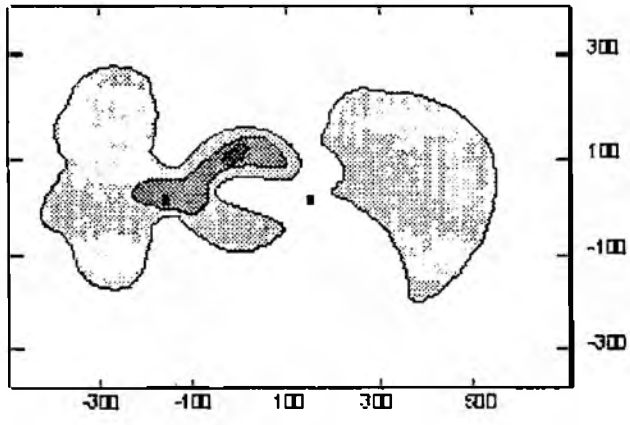

Рис. 1 [6]

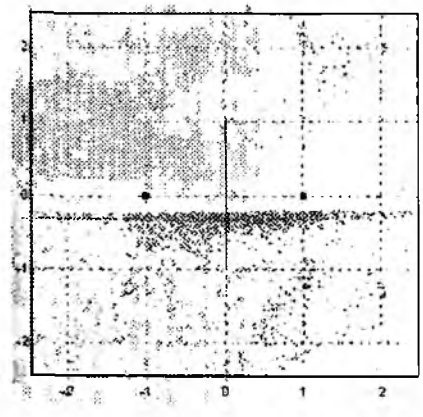

Рис. 2 [1]

Условие зеркальности метеорного отражения не только накладывает ограничение на возможные места возникновения метеорного следа, но и ограничивает область возможного приёма сигнала, отражённого от него. На рис. 3 представлен экспериментально полученный график зависимости вероятности перехвата сообщения, передаваемого по МРК, в зависимости от расстояния от пункта связи [7]. Физически это обусловлено тем, что отражение от метеорного следа подобно отражению от маленького зеркала, расположенного на большой высоте.

Область возможного приёма на земной поверхности в каждом случае можно представить в виде «солнечного зайчика», размеры которого зависят от длины трассы и меняются от положения и ориентации следа в пространстве. По этой причине более или менее уверенный перехват принимаемой информации возможен на расстоянии всего 5 – 10 *км* от места расположения каждого из корреспондентов.

Можно сказать, что метеорный след, через который осуществляется связь между двумя удалёнными корреспондентами, является их «персональным метеором». Никто посторонний не сможет ни принять передаваемую по нему информацию, ни определить параметры этого метеора, в частности, его координаты.

Авторов публикаций [1, 6] координаты следа интересовали лишь с точки зрения того, куда ориентировать антенны, чтобы получить максимальный коэффициент заполнения МРК.

Для этой задачи многообразие возможных мест возникновения следов даже нежелательно, поскольку вынуждает применять слабонаправленные, а потому, малоэффективные антенны. А с точки зрения задачи, обсуждаемой в статье, это обстоятельство даёт возможность использовать координаты метеорного следа в качестве основы для формирования случайной числовой последовательности, которая не известна никому постороннему.

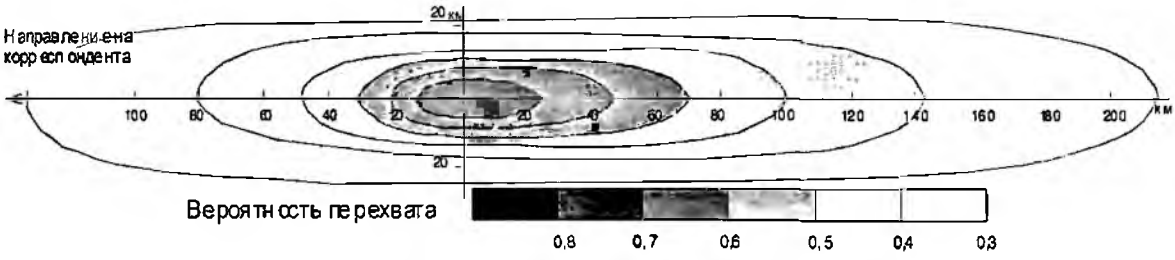

Рис. 3

Для определения координат метеора можно воспользоваться методом, предложенным в работах [8, 9]. В [8] решается задача определения координат отражающей точки метеорного следа в локационном режиме. Для этого пять антенн располагаются в форме «креста», как показано на рис. 4. Изменению направления на метеорный след будет соответствовать изменение разности фаз в приёмных антеннах. Зная расстояние между антеннами и разность фаз, можно рассчитать угловые координаты следа.

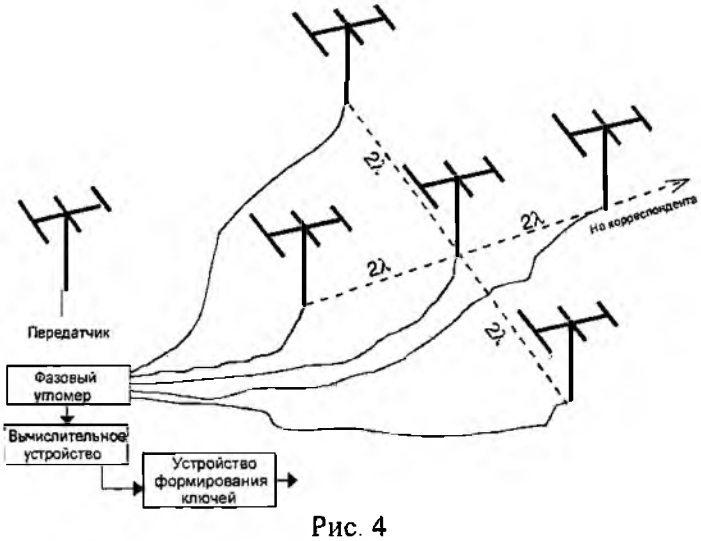

Рис. 4

Погрешность определения угловых координат следа определяется погрешностью измерения разности фаз между сигналами в антеннах и по данным [8] составляет не более 17`. В данном способе для расчетов берется погрешность не превышающая 5`

В работе [9] рассматривается аналогичная задача, но уже для режима связи. В запатентованном способе авторы предлагают определять координаты метеорного следа по излучению противоположного пункта.

На рис. 5 изображена пространственная схема радиолинии метеорной связи (РМС), где показаны углы α_1, β_1, α_2, β_2, которые измеряются с пунктов связи. Измерение углов происходит при помощи фазово-угломерного способа, используя который, находят угловые координаты метеорного следа в пространстве.

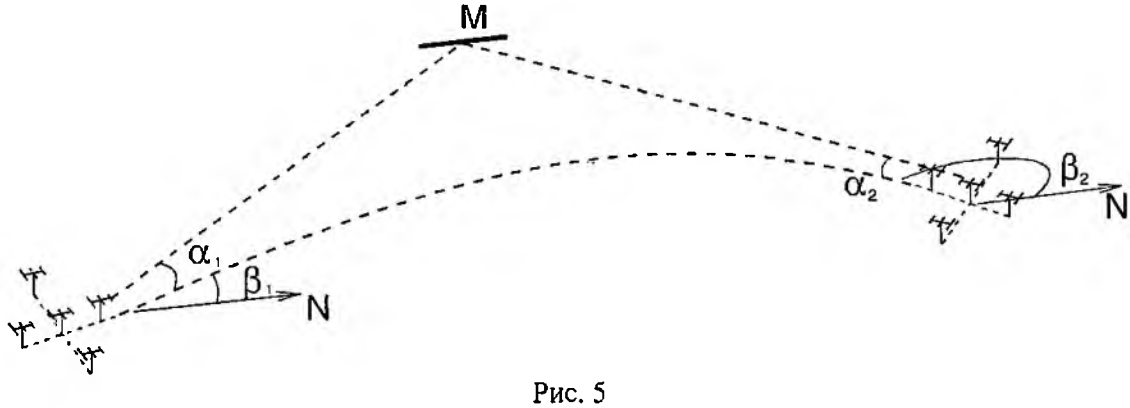

Рис. 5

При расчете угловых координат метеорного следа в пространстве следует учитывать погрешность, т.к. ошибка в определении угловых координат приведет к ошибке нахождения местоположения следа. Рабочая зона (ограниченное пространство в котором возможно появление метеоров) делится на пространственные фрагменты, у каждого три составляющих: длина *u*, ширина *r*, высота *h*.

Найдём одну из составляющих погрешности определения местоположения следа:

$$\delta_u = d\frac{\sin\delta_\alpha}{\sin\alpha}, \quad (1)$$

где d – наклонная дальность; δ_α – погрешность определения α; α – угол между наклонной дальностью и метеорным следом.

Для трассы длиной 400 при высоте следа 100 *км* данная погрешность может составлять от 820 *м* до 3030 *м*.

Найдём вторую составляющую определения местоположения следа δ_r

$$\delta_r = d\sin\delta_\beta, \quad (2)$$

где δ_β – погрешность определения угла β.

Для данной трассы δ_r может составлять от 640 *м* до 1150 *м*.

Найдем третью составляющую δ_h по формуле

$$\delta_h = \frac{d\sin\delta_\alpha}{\cos\alpha}. \quad (3)$$

Для данной трассы δ_h может составлять от 290 *м* до 570 *м*.

Если представить все множество вероятных местоположений как V, то

$$V = \frac{l\,mh}{\delta_u\delta_r\delta_h}, \quad (4)$$

где l – длина, m– ширина трассы, h – высота.

W_{max} – максимально возможное количество пространственных фрагментов, которое можно закодировать N – двоичными разрядами. Применив оптимизацию, получаем $W_{max} = 461494$ вариантов

$$N = \log_2 W_{max}, \quad (5)$$

где W_{max} – максимальное количество возможных мест определения метеорных следов;

Проведя расчеты по формуле (5), получаем производительность нашего способа равную 14– 17 *бит* на метеорный след.

Данный способ обладает рядом особенностей, которые необходимо учитывать.

Во-первых, существует такое понятие, как суточный ход метеорной активности. Количество метеоров возрастает с 6 часов утра и уменьшается к 6 часам вечера. Вследствие этого скорость формирования ключей может быть неравномерной. Можно решить эту проблему при помощи накапливания ключей, а за тем равномерного распределения их по необходимым отрезкам времени.

Во-вторых, локализация по «горящим областям». Криптоаналитику известно местоположение нащих пунктов приема и передачи информации. Из этого следует, что он может вычислить наиболее вероятные места для появления метеорных следов и этим облегчить себе задачу перебора возможных координат. Для решения этой проблемы необходимо согласовать свою систему координат в двух пунктах и оптимизировать ее.

В-третьих, для увеличения производительности нашего способа следует снижать погрешность измерения углов фазовым угломером.

Из общей теории стойкости симметричных криптосистем [2] следует, что вычисляемая или безусловная стойкость шифрования обеспечивается в том случае, если ключи в криптосистеме формируются случайно, равновероятно, независимо и однородно. В радиометеорной связи достаточно много случайных характеристик, чем можно воспользоваться для решения поставленных задач.

Главное преимущество способа независимого формирования одинаковой в двух разнесенных пунктах случайной числовой последовательности в том, что нам не нужно передавать ключи каким-либо способом, а они генерируются независимо, прямо на местах их использования.

Данная система является эффективной и универсальной.

В статье показана возможность одновременной генерации одинаковых ключей в разнесенных пунктах. Рассчитана производительность данного способа равная 120 битам в час. Приведены погрешности δ_u = 0,818 – 3,03 *км* ,δ_r=0.64 – 1,15 *км*, δ_h = 0,289 – 0,566 *км*. Наименьшая ошибка определения местоположения метеорного следа по центру трассы и увеличивается к краям.

Список литературы: 1. *Антипов И. Е., Коваль Ю. А., Обельченко В. В.* Развитие теории и совершенствование радиометеорных систем связи и синхронизации; Учеб. пособие. Харьков: Коллегиум. 2006. 2. *Горбенко І. Д., Гріненко Т. О.* Захист інформації в інформаційно-телекомунікаційних системах: Учеб. пособие. Харків, 2003. 3. *Пасынков В.В., Чиркин Л. К.* Полупроводниковые приборы. М.: Высш. шк., 1987. 4. *Патент РФ № 2265957* МПК H04B7/22,H04L9/20, опубликованный 10.12.2005 Бюл. №34. 5. *Корнеев, Сидоров, Эпиктетов.* О возможности защиты информации на основе использования наносекундной синхронишкал времени по метеорным радиоотражениям // Инфор. процессы. Т. 8, 2008. № 1. С. 10-23. 6. *Weitzen J.A.* Communicating Via Meteor Bust at Short Range // IEEE. Trans. on com., vol. COM-35, N 11, November 1987. P. 1217 -1221. 7. *Кащеев Б.Л., Бондарь Б.Г.* Метеорная связь. Киев: УМК ВО, 1989. 76 с. 8. *Дистанционные* методы и средства исследования процессов в атмосфере земли / Под ред. Б. Л. Кащеева, Е. Г. Прошкина, М.Ф. Лагутина. Харьков: Харьк. нац. ун-т радиоэлектроники; Бизнес Информ, 2002. 426с. 9. Патент Україна № 67664 МПК G04G7/02, виданий 15.06.2004. Бюл.№6.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.03.2009