УДК 04 **Информационные технологии**

Печникова Юлия Олеговна, *студент*
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, РФ, г. Санкт-Петербург

ИССЛЕДОВАНИЕ СПОСОБА ФОРМИРОВАНИЯ СЕКРЕТНОГО КЛЮЧА В СЕТЯХ СВЯЗИ НА ОСНОВЕ MIMO ТЕХНОЛОГИИ

Аннотация: В данной статье рассматривается способ передачи ключа в радиоканале, основой построения которого служит технология MIMO. Предлагается способ формирования ключа с целью повышения защиты передачи от незаконного перехвата.

Ключевые слова: MIMO канал, секретный ключ, передача ключей, безопасная передача.

Annotation: This article shows key distribution method in radio channel based on MIMO technology. It gives an overview on the key forming method in order to raise transmission secrecy from illegal receivers.

Key word: MIMO channel, secret key, key distribution, secret transmission.

В современных сетях связи актуальным вопросом является уязвимость среды передачи информации. В качестве защиты информации применяются криптографические преобразования, в основе которых лежит использование криптографических ключей.

В данный момент в беспроводные сети активно внедряется технология MIMO (рис 1.) (Multiple Input Multiple Output) [3]. Она обеспечивает быструю передачу, благодаря использованию нескольких антенн как на приеме, так и на передаче. Так же можно оптимизировать передачу сигнала таким образом, чтобы нелегитимные пользователи не смогли распознать сигнал или

детектировали его без какой-либо полезной информации. Благодаря увеличению спектральной эффективности за счет использования нескольких антенн одновременно на передающей и на приемной стороне, значительно повышается пропускная способность и/или помехоустойчивость системы связи по сравнении с традиционной схемой, использующейся на приемной и передающей стороне по одной антенне (SISO).

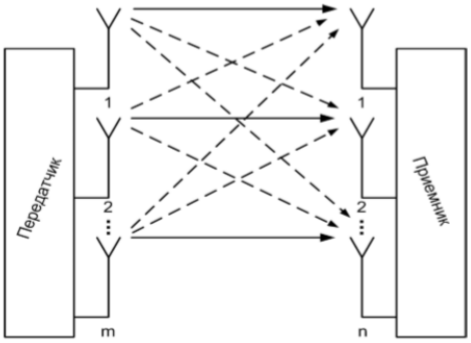

Рисунок 1. Принцип работы MIMO

В данной статье приводится способ использования расширенной пространственно-временной передачи для повышения секретности передачи между двумя легитимными пользователями, основа которого лежит в [1] для MISO и [2] для MIMO каналов. Секретность достигается тем, что с оптимально заданной случайностью можно предотвратить оценивание канала нарушителем посылая ему сигнал с большим количеством ошибок, в то время как на сторону авторизированных пользователей поступит качественный и надежный сигнал без ошибок.

Рассмотрим беспроводную сеть, как показано на рисунке 2. Обозначим базовую станцию – БС, мобильным пользователем – МП, а всех остальных пользователей (нарушителей) - Е. БС использует несколько антенн: часть антенн используется для передачи по секретному каналу, а остальные для передачи по открытому каналу.

Процесс передачи будет выглядеть следующим образом:

1) МП передает тестовый сигнал в сторону БС.

2) БС принимает сигнал с помощью антенн и получает матрицу канала передачи $\boldsymbol{H}$.

3) На основе известного коэффициента передачи БС формирует сигнал x и передает x и передает биты ключа b.

4) МП принимает пространственно-временной сигнал и детектирует биты ключа $\hat{b}$.

Так как нарушитель не знает матрицу канала $\boldsymbol{H}$, он не может правильно детектировать сигнал. Мы рассматриваем только пассивного противника, т. е. Е может только пассивно слушать передачи, а не активно изменять или ретранслировать пакеты.

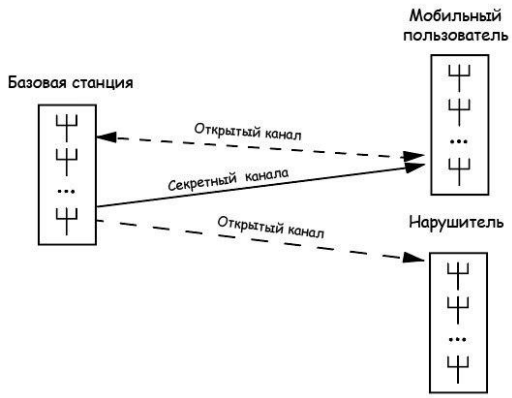

Рисунок 2 Модель передачи секретного ключа с использованием MIMO

Модель процесса передачи показана на рисунке 3. Биты ключей вектора $b(n)$ поступают на блок весовых коэффициентов **W**(n), определяющих мощность сигналов, передаваемых каждой из J антенн. Сигнал $s(n)$ каждой антенны проходит в радиоэфире через фильтр, тем самым образуя матрицу $\boldsymbol{H}$.

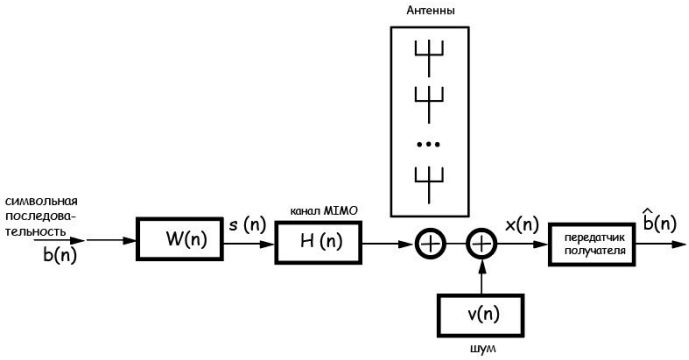

Рисунок 3 Модель пространственно-временной передачи

На приемной стороне сигналы от каждой из антенн передатчика суммируются. К полученному сигналу добавляется шумовой сигнал $\boldsymbol{v}(n)$. В итоге формируется принимаемый сигнал $x(n)$.

При синхронизированных J передатчиках для канала распространения с релеевскими замираниями полученный сигнал на стороне МП будет выглядеть так

$$x(n) = \boldsymbol{H}\boldsymbol{s}(n) + \boldsymbol{v}(n), \tag{1}$$

где $v(n)$ – вектор белого гауссовского шума с нулевым средним значением и дисперсией ${\sigma_{\text{ш}}}^2$.

$$\boldsymbol{s}(n) = \boldsymbol{W}(n)\boldsymbol{b}(n), \tag{2}$$

Переданный сигнал $\boldsymbol{s}(n)$ можно записать в виде

где $\boldsymbol{b}(n) = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_J \end{bmatrix}$, где $b_J = \begin{cases} +1 \\ -1 \end{cases}$, $\boldsymbol{W}(n) = \begin{bmatrix} w_{11} & w_{12} & \dots & w_{1k} \\ w_{21} & w_{22} & \dots & w_{2k} \\ \dots & \dots & \dots & \dots \\ w_{j1} & w_{j2} & \dots & w_{jk} \end{bmatrix}$– матрица весовых коэффициентов на передаче.

Матрица $\boldsymbol{H}$ представляется в следующей форме:

$$\boldsymbol{H} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1k} \\ h_{21} & h_{22} & \dots & h_{2k} \\ \dots & \dots & \dots & \dots \\ h_{j1} & h_{j2} & \dots & h_{jk} \end{bmatrix} \tag{3}$$

$$\boldsymbol{h}_{jk} = \boldsymbol{h}_c + i\boldsymbol{h}_s, \tag{4}$$

где $\boldsymbol{h}_c$ и $\boldsymbol{h}_s$ - действительные гауссовские случайные векторы, распределенные по нормальному закону со средним $\mu = 0$ и дисперсией $\sigma^2 = 1$; $i = \sqrt{-1}$.

Предполагается, что Е не может получить идентичный сигнал как у МП. Такая разница объясняется главным образом тем, что каналы не являются ни тождественными, ни сильно коррелированными. До тех пор, пока расстояние между МП и Е больше, нескольких длин волн, их каналы можно считать независимо затухающими. Поэтому мы используем разницу каналов, а не разницу шумов, чтобы добиться секретности передачи информации.

Теперь рассмотрим метод построения матрицы весов $\boldsymbol{W}(n)$ при случайном выборе его компонент. Выберем случайным образом $K\ x\ K$ подматрицу $\boldsymbol{H}_0$. В таком случае матрица будет выглядеть следующим образом

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_0 \\ \boldsymbol{H_1} \end{bmatrix}. \tag{5}$$

То есть вектор весовых коэффициентов на передаче имеет вид

$$\boldsymbol{W}(n) = P \begin{bmatrix} \boldsymbol{H}_0{}^{-1}[A - \boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)] \\ \boldsymbol{W}_1(n) \end{bmatrix}, \tag{6}$$

где A – константа, определяющая мощность передачи.

С помощью матрицы Р часть матрицы $\boldsymbol{W}(n)$ в (6) может быть перемещена на любое место, если случайно выбрана матрица $\boldsymbol{H}_0$, а любая другая матрица $\boldsymbol{H}_i$.

Тогда сигнал на передаче запишется в виде

$$\boldsymbol{s}(n) = \begin{bmatrix} s_0 \\ s_1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{H}_0{}^{-1}[A - \boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)]\boldsymbol{b}(n) \\ \boldsymbol{W}_1(n)\boldsymbol{b}(n) \end{bmatrix}, \tag{7}$$

где

$s_0(n) = \boldsymbol{H}_0{}^{-1}[A - \boldsymbol{H}_1(n)^H \boldsymbol{W_1}(n)]b(n) = \boldsymbol{H}_0{}^{-1} A\, \boldsymbol{b}(n) - H_0{}^{-1}\boldsymbol{H}_1(n)^H \boldsymbol{b}(n),$

$s_1(n) = \boldsymbol{W}_1(n)\boldsymbol{b}(n).$

Сигнал на приеме у легального пользователя

$$x(n) = \boldsymbol{H}(n)^H \boldsymbol{s}(n) + \boldsymbol{v}(n), \tag{8}$$

где $\boldsymbol{v}(n)$ – шумовая компонента – гауссовский сигнал с нулевым математическим ожиданием μ и дисперсией $\sigma_{\text{ш}}{}^2$.

Рассмотрим произведение

$$\begin{aligned} \boldsymbol{H}^H(n)\boldsymbol{s}(n) &= [\boldsymbol{H}_0{}^H \quad \boldsymbol{H}_1{}^H]\begin{bmatrix}\boldsymbol{s}_0(n)\\ \boldsymbol{s}_1(n)\end{bmatrix} = \boldsymbol{H}_0 s_0(n) + \boldsymbol{H}_1{}^H \boldsymbol{s}_1(n) \\ &= H_0 H_0{}^{-1}[A - \boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)]\boldsymbol{b}(n) + \boldsymbol{H}_1{}^H(n)\boldsymbol{W}_1(n)\boldsymbol{b}(n) \\ &= A\boldsymbol{b}(n) - \boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)\boldsymbol{b}(n) + \boldsymbol{H}_1{}^H(n)\boldsymbol{w}_1(n)\boldsymbol{b}(n) = A\boldsymbol{b}(n). \end{aligned} \tag{9}$$

Таким образом, имеем

$$x(n) = \boldsymbol{H}(n)^H \boldsymbol{s}(n) + \boldsymbol{v}(n) = A\boldsymbol{b}(n) + \boldsymbol{v}(n). \tag{10}$$

Так как $A > 0$, и значение вектора $v(n)$ – как гауссовская случайная величина симметричная относительно 0, то очевидно, что правило решения имеет вид

$$\hat{b}(n) = \begin{cases} 1, \text{если } sign\, x(n) \geq 0, \\ -1, \text{если } sign\, x(n) < 0, \end{cases} \tag{11}$$

где $sign$– знак перед $x(n)$.

Таким образом, установлено, что и при случайном векторе $\boldsymbol{W}(n)$ законный пользователь может правильно детектировать переданный сигнал.

Теперь же рассмотрим случай приема сигнала нелегальным приемником. Принимаемый сигнал запишется в виде

$$\begin{bmatrix} x_{u,1}(n) \\ \vdots \\ x_{u,M}(n) \end{bmatrix} = \begin{bmatrix} h_{u,1,1}(0) \dots & h_{u,1,J}(0) \\ \vdots & \vdots \\ h_{u,M,1}(0) \dots & h_{u,M,J}(0) \end{bmatrix} x \begin{bmatrix} w_1(n)b(n) \\ \vdots \\ w_J(n)b(n) \end{bmatrix} + \begin{bmatrix} v_{u,1}(n) \\ \vdots \\ v_{u,M}(n) \end{bmatrix} \qquad (12)$$

или

$$\boldsymbol{x_u}(n) = \boldsymbol{H}_u \boldsymbol{w}(n)\boldsymbol{b}(n) + \boldsymbol{v}_u(n), \qquad (13)$$

где $\boldsymbol{H}_u$ – канальная матрица, $\boldsymbol{v}_u(n)$ – вектор шума.

Для нахождения ключа $\boldsymbol{b}(n)$ нарушителю необходимо определить $\boldsymbol{H}_u$. Для этого могут исследоваться следующие подходы

1) Если канал между БС и МП имеет обратную связь, то нарушитель Е может оценить сигнал, передаваемый от МП к БС. Прежде чем использовать обратную связь, необходимо установить метод инициализации. Поэтому БС передает тренировочную последовательность. МП оценивает ее, а результаты передает по каналу обратной связи обратно БС. При этом нарушитель по тренировочной последовательности может оценить матрицу $\boldsymbol{H}_u$. Если нарушитель, принимая данные из обратной связи $y(n)$, $n = 1, 2, \dots, J$, вычисляет $\boldsymbol{y_u}(n) = \boldsymbol{H}_u \boldsymbol{w}(n)$, $n = 1, 2, \dots, J$, то он так же может извлечь вектор $\boldsymbol{h}^H \boldsymbol{H}^{-1}$ – а отсюда и ключ $\boldsymbol{b}(n)$.

2) При отсутствии тренировочной последовательности нарушитель может оценить канал вслепую. Он не знает выбранных параметров μ и дисперсии σ^2 распределения компонент $\boldsymbol{w}(n)$.

Сигнал, принимаемый нарушителем имеет вид

$$\boldsymbol{x}_u(n) = \boldsymbol{H}_u(n)\boldsymbol{s}(n) + \boldsymbol{v}_u(n), \tag{14}$$

где $\boldsymbol{H}_u(n)$ – $(M\ x\ J)$ – матрица коэффициентов передачи канала от законного пользователя к нарушителю. Коэффициенты матрицы гауссовские случайные величины, имеющие нулевое математическое ожидание μ. Каждый элемент матрицы $H_u(n)$ не зависит от элементов вектора $\boldsymbol{h}(n)$. $\boldsymbol{v}_u(n)$ –М – мерный гауссовский вектор шума, компоненты которого независимы, имеют нулевое значение математического ожидания μ и ковариационную матрицу $\sigma_{ш}{}^2 I_м$.

Используя (6), запишем

$$\begin{aligned} \boldsymbol{x}_u(n) &= H_u \begin{bmatrix} H_0{}^{-1}[A - \boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)]\boldsymbol{b}(n) \\ \boldsymbol{s}_1(n) \end{bmatrix} + \boldsymbol{v}_u(n) \\ &= H_u \begin{bmatrix} -H_0{}^{-1}\boldsymbol{H}_1(n)^H \boldsymbol{W}_1(n)\boldsymbol{b}(n) + A\boldsymbol{H}_0{}^{-1}\boldsymbol{b}(n) \\ \boldsymbol{s}_1(n) \end{bmatrix} \\ &\quad + \boldsymbol{v}_u(n). \end{aligned} \tag{15}$$

Видим, что суммарное распределение $\boldsymbol{x}(n)$ будет зависеть от параметров $-H_0{}^{-1}\boldsymbol{H}_1(n)^H$ и ковариационной матрицы $\boldsymbol{R}$ случайной матрицы $\boldsymbol{W}_1(n)$ весовых коэффициентов. Это создает неопределенность матрицы H_u, что затрудняет оценку её параметров.

3) Если оценка вслепую не применима, то последнее, что может предпринять нарушитель – оценить канал методом грубой силы (bruteforce), перебирая все возможные состояния канала. Чтобы оценить сложность разрешения такого вопроса для E, определим количество уровней параметров канала для каждого отдельного значения (для комплексного числа их будет 2). Затем нужно выбрать по крайней мере $K^{(2J)^2}$ возможных комбинаций H_u и K^{2J} возможных комбинаций H. Это определяет общую сложность комбинаций перебора $Q = K^{2J(2J+1)}$.

При $J = 4$ и QPSK передаче, для достижения ошибки на бит (BER) ≈ 0,1,

необходимо, чтобы $K \geq 4$ даже в случае передачи без шумов. Когда $K = 4$, сложность становится $4^{2 \times 4 \times (2 \times 4 + 1)} = 2^{144}$. Если рассматривать более реалистичный BER = 0,01 при соотношении сигнал / шум (SNR) 25 дБ, K должно быть не менее 128, что дает сложность $Q = 2^{644}$. Приведенные примеры показывают, что метод грубой силы не дает нарушителю возможности получить матрицу H_u.

Таким образом, анализ возможных атак нарушителем показывает, что все они не дают возможности перехвата ключа, чем и объясняется стойкость данного способа передачи ключа.

В данном исследовании приведен способ формирования ключа пользователя с помощью преобразований вектора весовых коэффициентов для обеспечения наилучшей секретности. Избыточность в матрице передачи MIMO используется для создания сложной ситуации перехвата сигнала для противника, по оценке которой выявлено, что перехват сигнала и его идентификация нарушителем представляется критически сложным. Применение такого способа на практике, в системе MIMO в современных сетях связи позволит повысить секретность передачи сигнала между пользователями.

Библиографический список:

1. Xiaohua (Edward) Li. Conference on Information Sciences and Systems [Текст] // E. Paul Ratazzi and Xiaohua (Edward) Li. - New York: MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks, 2011, с. 1-6.
2. Xiaohua (Edward) Li. Conference on Information Sciences and Systems [Текст] // Xiaohua(Edward) Li, Mo Chen E. Paul Ratazzi – New York: A Randomized Space-Time Transmission Scheme for Secret-Key Agreement, 2005, с. 1-6.
3. Satoru Shimosaka. A Study on Stream Assignment Method for Secure MIMO Communication [Текст] // Kenta Umebayashi, Yasuo Suzuki - A Study on Stream Assignment, 2016. – с. 1-16.