УДК 621.396.74

В.М. ШОКАЛО, д-р. техн. наук, А.А. СТРЕЛЬНИЦКИЙ, канд. техн. наук,
Мухаммед К. АБДУЛ-ХУССЕЙН, Е.В. ЯГУДИНА

УСОВЕРШЕНСТВОВАННАЯ МОДЕЛЬ РАСЧЕТА ПРЕДЕЛЬНОЙ СЕКРЕТНОЙ ПРОИЗВОДИТЕЛЬНОСТИ Wi-Fi КАНАЛА СВЯЗИ

Введение

Актуальной задачей исследований в области беспроводных технологий является поиск новых путей повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне модели OSI. Эта задача применительно к повышению скрытности каналов связи частично решена в данной работе. В статье исследовалась энергетическая скрытность беспроводных каналов уровня LAN, характерным признаком которых является многолучевость [1]. В многолучевом канале наиболее часто употребляемым, описывающим его статистические характеристики коэффициента передачи, является закон Рэлея [1]. В цифровых системах передачи информации (ЦСПИ) уровня LAN замирания в каналах связи можно считать квазистатическими [2].

Для оценки уровня скрытности легитимных каналов с квазистатическим замиранием в [3] введено понятие секретной производительности:

$$C_{пр}(P_{об}) = \log_2 \frac{(S/N)_л \cdot P_{об} + 1}{(S/N)_о \cdot (1 - P_{об}) + 1}, \qquad (1)$$

где $(S/N)_{л,о}$ – среднее значение соотношения сигнал/шум в легитимном (ЛК) и в отводном (ОК) каналах; $P_{об}$ – заданное значение вероятности обнаружения.

При $C_{пр}(P_{об}) \geq 0$ канал связи считается засекреченным [3], т.е. не обнаруживается. Параметр S/N – это энергетический параметр ЦСПИ. Другой известный путь оценки потенциальных характеристик многоканальных ЦСПИ – это их представление в виде функциональных зависимостей от габаритных (в долях длины волны) размеров излучающих структур на приемной и передающей стороне системы связи. Такое представление позволяет на ранних стадиях проектирования ЦСПИ прогнозировать необходимое число пространственных каналов для обеспечения заданных ее характеристик. Однако указанный подход пока не распространен для случая ЦСПИ с отводным каналом, что не позволяет исследовать зависимость $C_{пр}$ от размера апертуры ОК и ее расположения относительно апертур ЛК. Другая разновидность формулы (1) имеет следующий вид [2]:

$$C_{пр}(P_{об}) = \log_2 \left(\frac{P_{об} + \dfrac{1}{(S/N)_л}}{\left(\dfrac{r_л}{r_о}\right)^n \cdot (1 - P_{об}) + \dfrac{1}{(S/N)_л}} \right) = 0, \qquad (2)$$

где $r_л$, $r_о$ – расстояние от передатчика до приемников легитимного и отводного каналов соответственно; n – показатель степени, отражающий, согласно [4], те или иные условия распространения радиоволн (РРВ).

Формула (2) позволяет исследовать зависимость величины $C_{пр}$ от условий РРВ, придавая различные значения показателю n. Однако выражение (2) справедливо, как известно из [4], только для дальней зоны излучения. Особенность же работы Wi-Fi радиоканалов состоит в том, что они функционируют и в ближней, и в промежуточной зонах.

Цель работы – исследованиЕ зависимости величины $C_{пр}$ от размера апертуры ОК и ее расположения относительно апертур ЛК, а также от условий распространения радиоволн в ближней, промежуточной и дальней зонах.

Основная часть

Представим ЦСПИ с отводным каналом по аналогии с [5] в виде трех взаимодействующих апертур (рис. 1). Две из них образуют легитимный многолучевой канал. Передающая апертура является сферой с диаметром a, внутри которой находятся как излучатели, так и рассеиватели. Наличие рассеивателей позволяет увеличить, как известно из [6], число каналов передачи информации в MIMO системах. Приемная апертура легитимного канала имеет размер $a_л$. Отводной многолучевой канал располагается по отношению к оси легитимного канала под углом γ и имеет приемную апертуру с размером $a_о$. В легитимном канале апертуры удалены на расстояние $r_л$, а в отводном – на расстояние $r_о$.

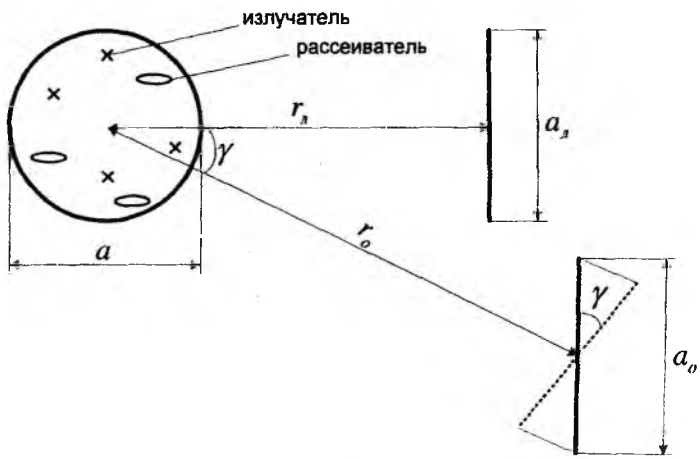

Рис. 1

Используя формулу Найквиста и теорему Шеннона [6], получим соотношение для определения количества пространственных каналов, необходимых при передаче информации с заданным отношением S/N:

$$C = 2 \cdot \log_2 M, \tag{3}$$

$$C = \log_2(1 + SNR), \tag{4}$$

где C – производительность ЦСПИ, M – количество дискретных сигналов, необходимых для передачи информации с заданной производительностью.

Далее будем считать, исходя из исследований проведенных в [5], что для передачи M дискретных сигналов нужно M различимых пространственных каналов. Приравнивая на этом основании правые части выражений (3) и (4), получим равенство

$$S/N = M^2 - 1, \tag{5}$$

которое позволяет определить необходимое число M при заданной величине S/N.

Воспользовавшись результатами работы [5], можно записать числа $M_л$ и $M_о$ для легитимного и отводного каналов через геометрические параметры ЦСПИ:

$$M_л = \frac{a}{r_л} \cdot \frac{a_л}{\lambda}, \tag{6}$$

$$M_о = \frac{a}{r_о} \cdot \frac{a_о}{\lambda} \cdot \cos\gamma, \tag{7}$$

где λ – длина волны.

Теперь с учетом (6)-(7) можно вывести такие соотношения:

$$(S/N)_л = \left(\frac{a \cdot a_л}{r_л \cdot \lambda}\right)^2 - 1, \tag{8}$$

$$(S/N)_o = \left(\frac{a \cdot a_o}{r_o \cdot \lambda} \cdot \cos\gamma\right)^2 - 1. \tag{9}$$

Используя полученные формулы (8), (9), запишем выражение для $C_{пр}$, учитывающее влияние размеров и взаимного расположения апертур антенн легитимного и отводного каналов на предельную секретную производительность:

$$C_{пр}(P_{об}) = \log_2 \frac{\left[\left(\frac{a \cdot a_л}{r_л \cdot \lambda}\right)^2 - 1\right] \cdot P_{об} + 1}{\left[\left(\frac{a \cdot a_o}{r_o \cdot \lambda} \cdot \cos\gamma\right)^2 - 1\right] \cdot (1 - P_{об}) + 1}. \tag{10}$$

Результаты расчетов по формуле (10) отражены на рис. 2, 3.

Из приведенных ниже графиков можно определить условия, при которых $C_{пр} = 0$ и ЦСПИ становится рассекреченной.

Одно из таких условий (рис. 2) – это $a_o \approx 1{,}5 \cdot a_л$ при $\gamma = 0^\circ$ и $a_o \approx 2 \cdot a_л$ при $\gamma = 40^\circ$.

Другое условие (рис. 3) – $r_л \approx 1{,}5 \cdot r_o$ при $\gamma = 0^\circ$ и $r_л \approx 2 \cdot r_o$ при $\gamma = 40^\circ$.

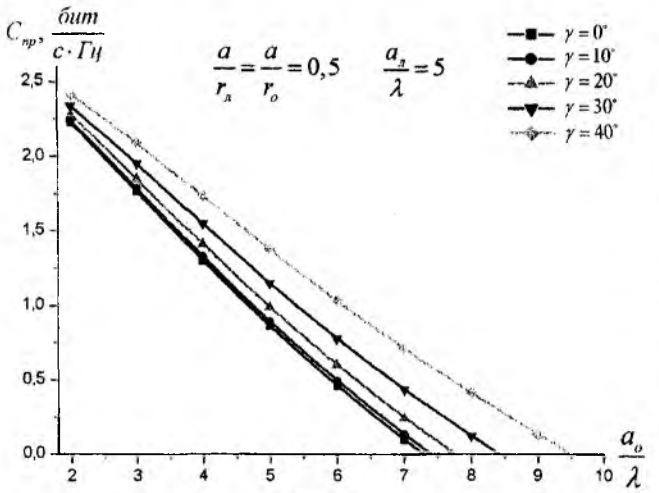

Рис. 2

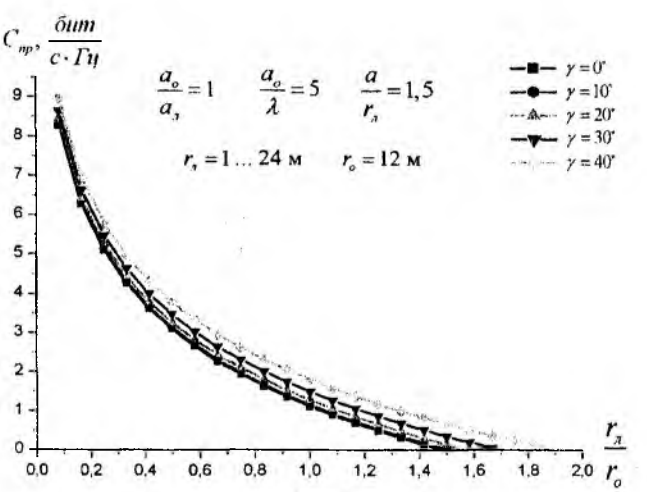

Рис.3

Изучались также зависимости $C_{пр}$ от механизмов многолучевого распространения радиоволн: на открытом пространстве с одной подстилающей поверхностью, в помещении и в волновых каналах, образованных архитектурными сооружениями (ВКАС) [7]. Для этого в формуле (1) соотношения сигнал/шум были представлены в следующем виде:

$$(S/N)_л = \frac{S(r_л, \theta_1, \theta_2)}{N(r_л, \theta_2)}, \tag{11}$$

$$(S/N)_o = \frac{S(r_o, \theta_1, \theta_3)}{N(r_o, \theta_3)}, \tag{12}$$

где θ_1, θ_2, θ_3 – текущие углы отсчетов значений ненормированных угловых интенсивностей напряженности поля (УЗИП) передающей антенны $F_П(r_л, \theta_1)$ и приемных антенн легитимного $F_л(r_л, \theta_2)$ и отводного $F_o(r_o, \theta_3)$ каналов в местной системе координат.

Тогда выражения (11) и (12) можно записать так:

$$\frac{S(r_л,\theta_1,\theta_2)}{N(r_л,\theta_2)}=\frac{S(r_э)}{N(r_э)}\cdot\alpha\left(\frac{r_э}{r_л}\right)\cdot F_П^2(r_л,\theta_1)\cdot F_л^2(r_л,\theta_2), \tag{13}$$

$$\frac{S(r_o,\theta_1,\theta_3)}{N(r_o,\theta_3)}=\frac{S(r_э)}{N(r_э)}\cdot\alpha\left(\frac{r_э}{r_o}\right)\cdot F_П^2(r_o,\theta_1)\cdot F_o^2(r_o,\theta_3), \tag{14}$$

где $S(r_э)/N(r_э)$ – экспериментально измеренное на эталонном расстоянии $r_э$ [4] соотношение сигнал/шум в максимуме интенсивности излучения; $\alpha(r_э/r_л)$, $\alpha(r_э/r_o)$ – функциональные зависимости затухания сигнала в легитимном и отводном каналах.

Формула (10) с учетом выражений (13), (14) была преобразована к виду

$$C_{пр}(P_{об})=\log_2\frac{\frac{S(r_э)}{N(r_э)}\cdot\alpha\left(\frac{r_э}{r_л}\right)\cdot F_П^2(r_л,\theta_1)\cdot F_л^2(r_л,\theta_2)\cdot P_{об}+1}{\frac{S(r_э)}{N(r_э)}\cdot\alpha\left(\frac{r_э}{r_o}\right)\cdot F_П^2(r_o,\theta_1)\cdot F_o^2(r_o,\theta_3)\cdot(1-P_{об})+1}. \tag{15}$$

Если предположить, что при любых расстояниях $r_л$ и r_o все УЗИП, входящие в выражение (15) не зависят от углов θ, то формула (15) позволяет исследовать зависимости $C_{пр}(P_{об})$ от величин затуханий $\alpha_л$ и α_o, т.е. от условий РРВ. Расчет величин α_o и $\alpha_л$ для различных условий РРВ может быть проведен по моделям, описанным в [8]. Воспользовавшись выражениями (13) - (15) можно рассчитать значения $C_{пр}(P_{об})$ для ближней, промежуточной и дальней зоны при РРВ на открытом пространстве. Результаты расчета предельной секретной производительности на открытом пространстве представлены на рис. 4. На рисунке приняты такие обозначения: 1 – ближняя зона РРВ, 2 – промежуточная зона РРВ, 3 – дальняя зона РРВ.

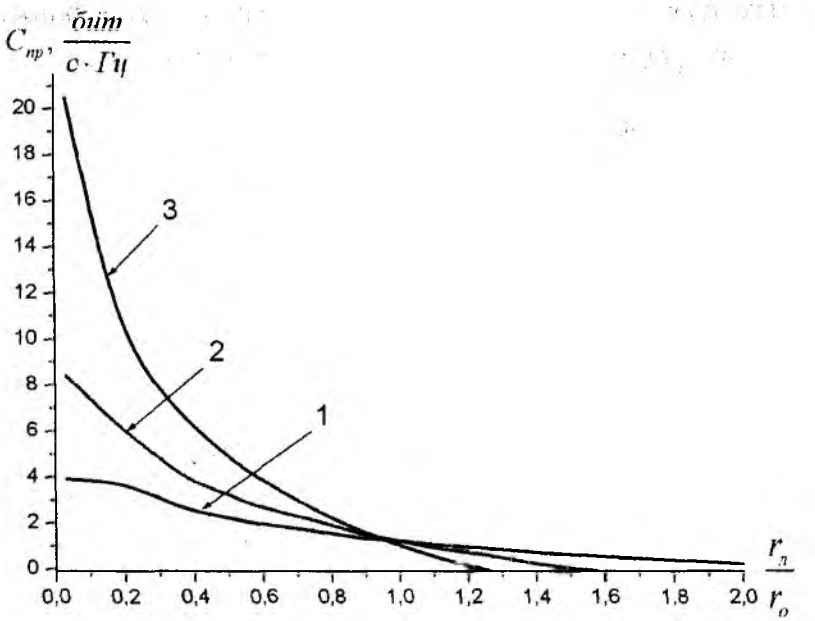

Рис. 4

Анализируя кривые на рис. 4, можно выявить следующие закономерности:

– чем ближе находится приемник легитимного канала от передатчика, тем при больших отношения $r_л/r_o$ величина $C_{пр}\to 0$; это поясняется тем, что при переходе от зоны к зоне излучения затухание возрастает в квадрат раз [8];

– вне зависимости от зоны излучения для достижения значения $C_{пр} = 0$ приемник-обнаружитель должен находиться ближе к передатчику, чем приемник легитимного канала.

Обнаружено, что такие же закономерности проявляются и при распространении радиоволн по ВКАС (см. рис. 5 – предельная секретная производительность для случая Т-образного коридора).

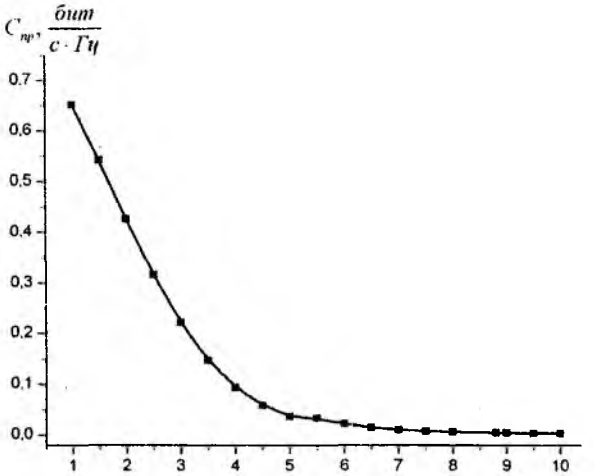

Рис. 5

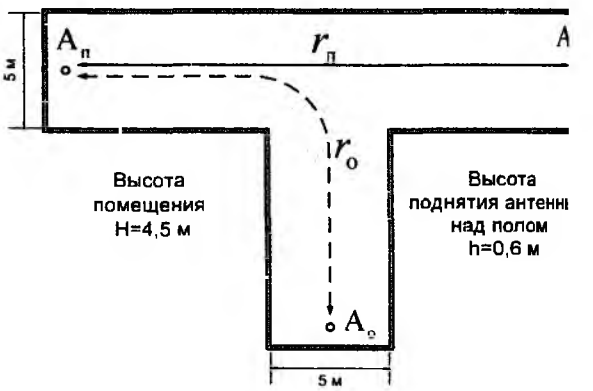

Рис. 6

Результаты, приведенные на рис. 5, получены для случая функционирования радиоканала Wi-Fi в Т-образном коридоре ХНУРЭ. Эскиз его показан рис. 6.

На графике рис. 5 кривая $C_{пр}(r_л)$ получена при $r_o = 5$ *м*, т.е. $C_{пр}(r_л) \approx 0$ при $r_л / r_o \approx 2$, что совпадает с результатами, полученными для ближней зоны открытого пространства.

Описанные закономерности проявляются и в случае работы ЦСПИ в помещении (рис. 7, кривые 1 – ближняя зона при $r_o = 6$ *м* и 2 – промежуточная зона при $r_o = 18$ *м*), только при больших значениях $r_л / r_o$, чем для открытого пространства. Для ближней зоны $r_л / r_o = 2{,}5$, а для промежуточной $r_л / r_o \approx 2{,}37$. Расчеты проводились для помещения, которое описано в [9, с. 109].

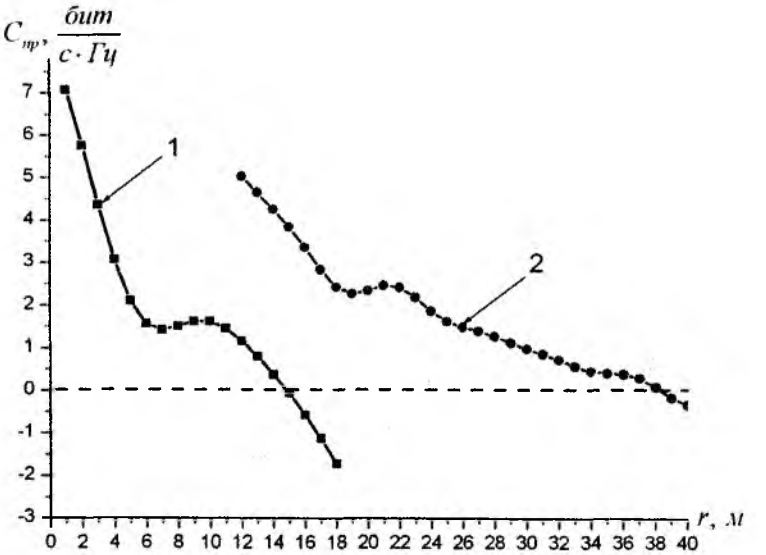

Рис. 7

Выводы

1. Впервые получены формулы, связывающие вероятность обнаружения канала ЦСПИ и его секретную производительность от размеров апертур антенн легитимного канала, апертуры антенны отводного канала и их взаимного расположения.

2. Показано, что основными факторами, влияющими на эффективность обнаружения, является удаление приемных апертур легитимного и отводного канала от апертуры системы излучателей и рассеивателей источника информации. Получены конкретные количественные данные о размерах апертур легитимного и отводного каналов, а также о взаимном их расположении при которых сигналы ЦСПИ могут быть уверенно обнаружены.

3. Выведено выражение, определяющее зависимость величины $C_{пр}$ от различных условий распространения радиоволн. Приведены результаты численных экспериментов, из которых следует, что различия в условиях РРВ существенно влияют на величины $C_{пр}$. Полученные данные являются новыми и позволяют определить условия, при которых $C_{пр} > 0$, что соответствует критерию безопасной работы многолучевых радиоканалов.

Список литературы: 1. *Радиорелейные* и спутниковые системы передачи : Учебник для вузов / А.С. Немировский, О. С. Данилович, Ю. И. Маримонт и др. / под. ред. А. С. Немировского. – М. : Радио и связь, 1986. – 392 с. 2. *Barros, J., Rodrigues, M.R.D.* Secrecy capacity of wireless channels // 2006 IEEE International Symposium on Information Theory, IEEE Press, New York. – pp. 356–360. 3. *Chrysikos, T., Dagiuklas, T., Kotsopoulos, S.* A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security // Proceedings of Security in Emerging Wireless Communication and Networking Systems (SEWCN'09). – Springer, 2010. – Vol. 42 of Lecture Notes in Computer Science. – pp. 3–12. 4. *Скляр, Б.* Цифровая связь. Теоретические основы и практическое применение. - 2-е изд. : пер. с англ. – М. : Изд. дом «Вильямс», 2003. – С. 1104. 5. *Chakraborty, K., Franceschetti, M.* Maxwell meets Shannon: space-time duality in multiple antenna channels // Proc. 44-th Allerton Conf. Communication, Control and Computing. – Monticello, 2006. – pp. 761–770. 6. *Wiretap Channels*: Implications of the More Capable Condition and Cyclic Shift Symmetry / Omur Ozel, Sennur Ulukus Submitted to IEEE Transactions on Information Theory, October 2011. 7. *Shokalo, V.M., Strelnitskiy, O.O., Tsopa, O.I.* Approximate Model for Estimation of Efficiency and Noise Immunity of Branched Street and Corridor *Wi-Fi* and *WiMAX* Communication Channels // International journal «Telecommunication and Radio Engineering». – Begell House, 2009. – Vol. 68(17). – pp. 1511–1528. 8. *Стрельницкий, А.Е., Стрельницкий, А.А., Цопа, А.И., Шокало, В.М., Ягудина, Е.В.*Оценка безопастнсти работы Wi-Fi радиоканала с различными условиями распространения радиоволн // Сучасний захист інформації. – Киев : ГУИКТ, 2011. – №3. – С. 76-82. 9. *Лихограй, В.Г., Стрельницкий, А.А., Стрельницкий, А.Е., Цопа, А.И., Шокало, В.М.* Методы прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала / под. ред. А.И. Цопы, В.М. Шокало. – Харьков : КП «Городская типография», 2011. – 501 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 17.05.2012