УДК 351.746.1.355.535 (477)

І.І. ЧЕСАНОВСЬКИЙ, Д.О. ЛЕВЧУНЕЦЬ, А.Л. ПЕТРЕНКО
Хмельницький національний університет

ПОБУДОВА ЗАХИЩЕНИХ ТЕЛЕКОМУНІКАЦІЙНИХ РАДІОМЕРЕЖ З МНОЖИННИМ ДОСТУПОМ

В даній статті розглядається метод захисту радіомереж з множинним доступом, що базується на використанні додаткового (фіктивного) джерела сигналів з метою зниження відношення сигнал/шум поза зоною легітимного доступу. Отримано основні енергетичні співвідношення в зоні нелегітимного доступу, які дають змогу оцінювати енергетичну скритність каналів зв'язку в умовах відсутності структурної. Проведено аналіз отриманих співвідношень, який показав, що під час вибору граничних умов роботи в легітимній зоні і застосування додаткового джерела завад в зоні нелегітимного прийому можна значно підвищити енергетичну скритність сигналів аж до унеможливлення їх виявлення за рахунок зниження завадостійкості відвідного каналу. Показано, що забезпечення захищеної роботи енергетично та структурно відкритих телекомунікаційних радіосистем можливе лише за рахунок штучного погіршення завадостійкості в певній частині зони покриття.

Ключові слова: телекомунікаційні системи, енергетична скритність, відношення сигнал шум, завадостійкість, структурна скритність, множинний доступ.

I.I. CHESANOVSKYY, D.O. LEVCHUNETS, A.L. PETRENKO
Khmelnytsky National University

CREATION OF PROTECTED TELECOMMUNICATIONS RADIO NETWORKS WITH MULTIPLE ACCESS

In this article considered method to protect radio networks with multiple access based on the use of additional (fictitious) signal source to reduce the signal / noise outside legitimate access. Received basic energy value in the area of illegitimate access that allow secrecy to evaluate the energy channels in the absence of structural. The analysis of correlations obtained, which showed that the choice of the boundary conditions of a legitimate application area and an additional source of illegitimate interference in the reception area can significantly increase energy secrecy signals up to prevent their detection by reducing the noise immunity of the outlet channel. It is shown that ensuring secure energy and structural work of public radio telecommunication systems is possible only through artificial deterioration of immunity to some of the coverage.

Keywords: telecommunication systems, power stealth, ratio signal noise, immunity, structural reticence, multiple access.

Ключовим напрямком розвитку сучасних телекомунікаційних мереж, є використання бездротових технологій, що поєднують високу пропускну здатність каналів, в умовах стохастичного множинного доступу, із мобільністю та неоднорідністю завантаження окремих сегментів. Поряд з цим, окремим, важливим аспектом функціонування засобів телекомунікацій, є необхідність забезпечення високої захищеності окремих каналів зв'язку від несанкціонованого доступу. Враховуючи особливості побудови та функціонування телекомунікаційних радіосистем з множинним доступом (ТРМД), що полягають в енергетичній відкритості (загальнодоступності) каналів, із відомих на сьогоднішній день методів [1, 4] захисту інформації, придатними до застосування є лише криптографічний та структурний, хоча відносно останнього, є значні сумніви в його придатності, що підтверджується практикою побудови таких систем. Це додатково можна обґрунтувати застосуванням ортогональних кодів (піднесучих), які виходячи із бази, завжди характеризуються кінцевою розмірністю векторного простору, в наслідок чого не представляють значних труднощів для здійснення атак в умовах енергетичної відкритості системи. Слід також зазначити, що енергетичне відкритість багатостанційної телекомунікаційної системи значно знижує стійкість засобів інформаційного (криптографічного) захисту, оскільки зловмиснику доступний цілий ряд інформаційних потоків, які є додатковою, ефективною базою для успішної реалізації атаки на систему.

На сьогоднішній день, широкого поширення при побудові ТРМД отримало мережеве обладнання стандарту IEEE 802.11, що передбачає застосування лише криптографічного захисту інформації. При цьому, структурі мереж такого типу притаманна певна корпоративність, що як правило, характеризується певною просторовою конфігурацією. А отже, як показано в [2–5] з'являється гіпотетична можливість забезпечення енергетичної скритності в зоні нелегітимності мережі (рис. 1).

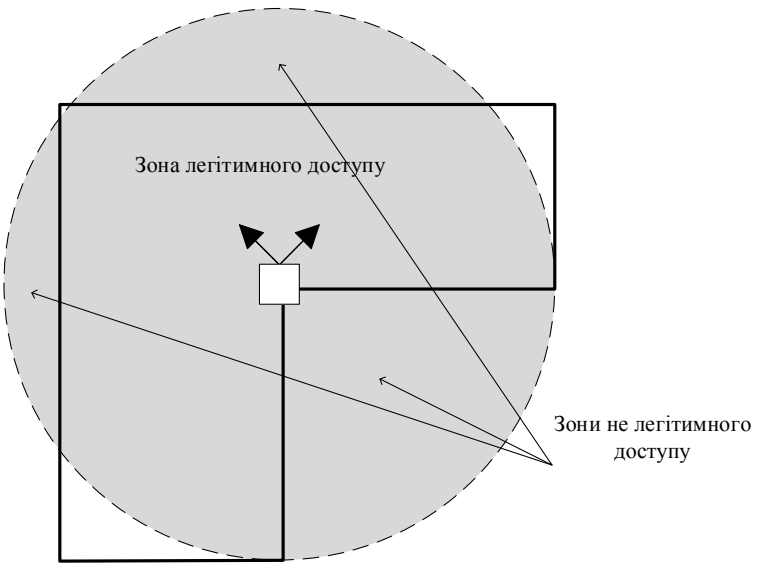

Рис. 1. Схема розподілу легітимної та нелегітимної зон доступності ТРМД

Оскільки, просторова конфігурація мережі дає змогу чітко виділити зони можливого нелегітимного доступу до мережі, за умови фізичного обмеження можливості доступу стороннього обладнання в зону легітимного доступу, потенційно можливо забезпечити енергетичну скритність системи за рахунок додаткових заходів, а саме: застосуванням спрямованих антен «базового» обладнання (застосування складної конфігурації зони покриття) або застосуванням сторонніх (фіктивних) мереж, що характеризуються вищою енергетикою в зонах не легітимного доступу.

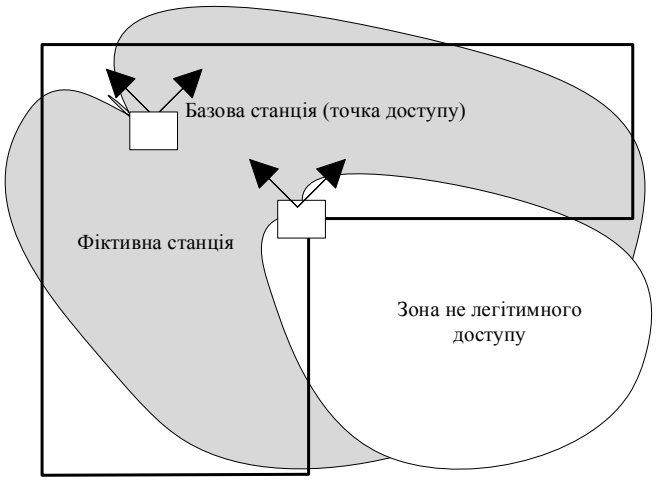

Рис. 2. Схема розподілу легітимної та нелегітимної зон доступності ТРМД при застосуванні фіктивних мереж

В роботі [2] розглядається варіант застосування генератору шуму для навмисного погіршення енергетичних співвідношень у відвідному каналі. Такий підхід є ефективним, але при забезпеченні певного ступеня корельованості шуму з інформаційним потоком на рівні структурної скритності сигналів. Проте, як було обумовлено вище, в мережах стандарту IEEE 802.11 основним інструментом захисту, є забезпечення інформаційної скритності, а отже для реального подавлення відвідного каналу необхідно забезпечити корельованість шуму і сигналу саме на інформаційному рівні. Для оцінки ефективності застосування такого підходу, а саме підходу, що передбачає структурну відкритість $p_{стр} = 1$ і максимальну потенційну інформаційну скритість $p_{інф} = \min$ необхідно провести аналіз енергетичної скритності p_e з метою пошуку оптимальної конфігурації зон легітимного та не легітимного доступу, а також параметрів інформаційного і фіктивного каналів в даних зонах. Відповідно схеми, що приведена на рис. 3, слід формалізувати задачу побудови системи виходячи із умови

$$\begin{aligned} p_{с.л}(q) &= 1 - p_{інф.л} p_{стр} p_{е.л}(q) = \min; \\ p_{с.н}(q) &= 1 - p_{інф.н} p_{стр} p_{е.н}(q) = \max. \end{aligned} \tag{1}$$

При такій формалізації, розв'язок задачі побудови захищеної мережі зводиться до пошуку оптимального вектору енергетичних (потужності передавачів і чутливості приймачів) та просторових (діаграм спрямованості антен при врахуванні багато променевості розповсюдження ЕМХ), що забезпечать прийнятне значення q (відношення сигнал/шум) в зоні легітимного доступу і значення q нижче критичного поза межами цієї зони.

Якщо припустити, що відвідний канал є симплексним і спрямованим лише на перехоплення інформації ($P_B = 0$), діаграма спрямованості антени базової станції є рівномірною в легітимній зоні і легітимний канал працює на рівні граничної енергетики ($E_{біт} = \min$) та мінімальній ($C = \min$) необхідній пропускній здатності , необхідна потужність передавача може бути визначена із формули

$$\frac{2P_{\min A}}{N_0} = \frac{P_Б G_Б G_A}{R_A (N_З D_З^{-1} + kT_0)}, \tag{2}$$

де $N_З, D_З$ – спектральна щільність завади та коефіцієнт спрямованої дії антени фіктивного передавача.

Враховуючи, що $G_З \approx 0$ в напрямку абонента, потужність базової станції при заданій чутливості приймача абонента визначається як

$$P_Б = \frac{R_A kT_0 2CE_{біт}}{G_Б G_A N_0}. \tag{3}$$

Для відвідного каналу, відношення сигнал/шум на вході приймача визначається

$$\frac{2P_{\min B}}{N_0} = \frac{P_Б G_Б G_B}{R_B (N_З + kT_0)}. \tag{4}$$

З урахуванням (3) і припускаючи, що чутливість приймачів легітимного і відвідного каналу однакові, отримується

$$\frac{2P_{\min B}}{N_0} = \frac{G_B}{G_A} \frac{R_A}{R_B} \frac{2CE_{біт}}{(N_З + kT_0)}. \tag{5}$$

Враховуючи, що спектральна щільність сигналу у всій смузі частот рівномірна $\frac{2P_{\min B}}{F} = V_B^2$, і замінюючи $C = 1/T$, вираз (5) може бути записаний

$$\frac{V_B^2}{N_0} = \frac{G_B}{G_A} \frac{R_A}{R_B} \frac{1}{FT} \frac{2E_{біт}}{(N_З + kT_0)}. \tag{6}$$

Аналізуючи останній вираз, можна прийти висновку, що при реалізації ТРМД з підвищеними

вимогами до скритності, основні зусилля мають бути спрямовані на забезпечення граничних умов роботи легітимного каналу за енергетичними показниками і пропускною здатністю. Саме за таких умов можна забезпечити виконання умови $\frac{V_B^2}{N_0} < 1$ при якій ймовірність енергетичного виявлення сигналів стрімко зменшується.

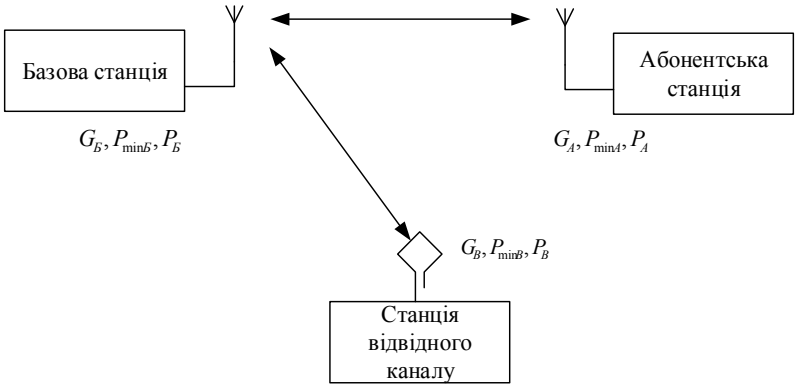

Рис. 3. Структура ТРМД з відвідним каналом

Враховуючи, що при великій базі сигналів, енергетичний приймач забезпечує коефіцієнт підсилення $\sqrt{T_c F}$, відношення сигнал/шум на його виході буде мати вигляд

$$q = \frac{G_B}{G_A}\frac{R_A}{R_B}\frac{1}{FT}\frac{2E_{біт}\sqrt{T_c F}}{(N_З + kT_0)}. \quad (7)$$

Якщо задатись порогом енергетичного виявлення сигналів в нелегітимному каналі λ, що забезпечує максимальне значення ймовірності виявлення сигналів при заданій ймовірності хибної тривоги, умова виявлення сигналів в нелегітимному каналі буде мати наступний вигляд

$$\frac{R_B}{R_A}\frac{N_З + N_0}{2E_{біт}}\frac{TF}{T_c} \le \frac{G_B}{G_A \lambda}. \quad (8)$$

З отриманого виразу видно, що збільшення бази сигналу підвищує енергетичну скритність системи, проте у випадку стандартизованих мереж із відкритою структурою сигналів (відомим псевдовипадковим кодуванням) вплив бази сигналу на скритість системи повністю нівелюється застосуванням, в приймачі відвідного каналу, узгодженого алгоритму. При цьому, також видно, що збільшення енергії сигналів в основному каналі також призводить до зниження його скритності, що є логічним.

Оскільки, антени, що застосовуються у відвідних каналах завжди характеризуються вищими значеннями коефіцієнта підсилення, а робота в легітимній зоні відбувається на гранично низькій швидкості і відповідно енергетиці, єдиним інструментом підвищення енергетичної скритності (відповідно формулі 8), є створення максимально корельованої із сигналами штучної завади зі спектральною щільністю, що значно перевищує власні шуми на вході приймача. Саме наявність такої завади дає змогу компенсувати спрямованість антени приймача відвідного каналу шляхом порушення роботи узгодженого алгоритму.

Література

1. Абдул-Хуссейн М. К. Моделирование и экспериментальное определение вероятности обнаружения функционирования Wi-Fi радиоканала / М. К. Абдул-Хуссейн, А. А. Стрельницкий, В. А. Назаренко, В. М. Шокало, Е. В. Ягудина // Научный вестник Черновицкого университета. – 2011. – Том 1, выпуск 1. Физика. Электроника. – С. 13–16.

2. Помехозащищенность радиосистем со сложными сигналами / Г. И. Тузов, В. А. Сивов, В. И. Прытков и др. ; под ред. Г. И. Тузова. – М. : Радио и связь, 1985. – 264 с.

3. Адресные системы управления и связи. Вопросы оптимизации : монография / Г.И. Тузов, Ю.Ф. Урядников, В. И. Прытков и др. ; под ред. Г.И. Тузова. – М. : Радио и связь, 1993. – 382 с.

4. Лукьянчук, А. Г. Влияние механизмов распространения радиоволн на вероятность обнаружения сигналов микроволновых систем связи / А.Г. Лукьянчук, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // МНПК Современные информационные и электронные технологии. – 2011. – № 12. – С. 164.

5. Шеннон К. Теория связи в секретных системах / К. Шеннон // Работы по теории информации и кибернетике. – 1963. – № 2. – С. 333–369.

Preferences

1. Modelirovanie i eksperimentalnoe opredelenie veroyatnosti obnaruzheniya funktsionirovaniya Wi-Fi radiokanala. M. K. Abdul-Husseyn, A. A. Strelnitskiy, V. A. Nazarenko, V. M. Shokalo, E. V. Yagudina. Nauchnyiy vestnik Chernovitskogo universiteta. 2011. Tom 1, vyipusk 1. Fizika. Elektronika. S. 13-16.

2. Pomehozaschischennost radiosistem so slozhnyimi signalami. G. I. Tuzov, V. A. Sivov, V. I. Pryitkov i dr.; Pod red. G. I. Tuzova. M.: Radio i svyaz, 1985. 264 s.

3. Adresnyie sistemyi upravleniya i svyazi. Voprosyi optimizatsii: monografiya. G.I. Tuzov, Yu.F. Uryadnikov, V. I. Pryitkov i dr.; pod red. G.I. Tuzova. M.: Radio i svyaz, 1993. 382 s.

4. Lukyanchuk, A. G. Vliyanie mehanizmov rasprostraneniya radiovoln na veroyatnost obnaruzheniya signalov mikrovolnovyih sistem svyazi. A.G. Lukyanchuk, A.A. Strelnitskiy, V.M. Shokalo, E.V. Yagudina. MNPK Sovremennyie informatsionnyie i elektronnyie tehnologii. 2011. №12. S. 164.

5. Shennon K. Teoriya svyazi v sekretnyih sistemah. Rabotyi po teorii informatsii i kibernetike. 1963. № 2. S. 333-369.

Рецензія/Peer review : 5.8.2015 р. Надрукована/Printed : 30.8.2015 р.
Рецензент: