

## **ІДЕНТИФІКАЦІЯ МОБІЛЬНИХ ПРИСТРОЇВ ПІД ВПЛИВОМ ШУМУ**

Василенко О. І.

e-mail: oleksandr.vasylenko1@nure.ua

Науковий керівник – к.т.н., старший викладач Василенко Т.О.

Харківський національний університет радіоелектроніки, каф. ІРТЗІ,  
м. Харків, Україна

This work studies the impact of signal-to-noise ratio (SNR) on spectral features used for identifying mobile devices in Wi-Fi networks via radio-frequency fingerprints. The mean square difference and skewness coefficient of spectra are analyzed, and simulation results show that identification remains reliable above certain SNR thresholds.

Зростання числа атак на бездротові мережі Wi-Fi, пов'язаних із підркобою ідентифікаційних даних, а також обмежена ефективність криптографічних методів у шумних каналах підвищують актуальність фізичних методів автентифікації. Одним із таких методів є використання радіочастотних відбитків мобільних пристроїв, які є унікальними для конкретного обладнання. Надійність цього підходу суттєво залежить від умов шуму, що обумовлює необхідність дослідження впливу співвідношення сигнал/шум на точність ідентифікації.

Метою роботи є визначення впливу шуму на точність ідентифікації мобільних пристроїв за спектральними ознаками та встановлення граничних значень SNR, за яких методи зберігають працездатність.

Аналізуються дві спектральні ознаки:

- середній квадрат різниці (Mean Square Difference, MSD) спектрів сигналів;
- коефіцієнт асиметрії (Skewness) взаємкореляційної функції спектрів сигналів.

Для перевірки того, наскільки вплине шум на можливість ідентифікації по спектру, було вирішено застосувати моделювання. Це вимушений крок, оскільки проводити експериментальні дослідження при значній відстані приймача від передавального пристрою наявна вимірювальна апаратура не дозволяла. Крім того, вимірювання в діючій мережі повинні виконуватися з урахуванням часового поділу абонентів. Але, з іншого боку, моделювання дозволило оцінити ймовірні характеристики запропонованого методу в самих різних умовах, що для реального експерименту було б важко.

Для порівняння можливості ідентифікації пристрою по його спектру проводилося імітаційне моделювання. Порядок дій при моделюванні наведений в табл. 1.

Таблиця 1. Порядок дій при імітаційному моделюванні

| Крок  | Опис процесу                                                       |
|-------|--------------------------------------------------------------------|
| 1     | Використовується збережений спектр                                 |
| 2     | Для заданого відношення сигнал/шум обробляються спектральні полоси |
| 2.1   | Для кожної частотної 2 кГц                                         |
| 2.1.1 | Формується випадкове значення $n$ згідно (1)                       |
| 2.1.2 | Формується випадкове значення фази згідно (2)                      |
| 2.1.3 | Розраховується модуль «зашумленого» відліку згідно (4)             |
| 2.2   | Формується кінцевий «зашумлений» спектр                            |
| 3     | Порівнюється «зашумлений» спектр з шаблоном згідно (5)             |

Наведений в табл. 1 алгоритм в процесі моделювання застосовувався неодноразово до різних пар спектрів, які були отримані в ході попередніх вимірювань. Для більшості значень було виконано по 1000 операцій додавання випадкового шуму.

Результати моделювання показали:

- метод MSD забезпечує ймовірність правильного розпізнавання  $>0,999$  за  $\text{SNR} \geq 30$  дБ;
- коефіцієнт асиметрії дозволяє ефективно розрізняти різні моделі пристроїв навіть при нижчих рівнях шуму;
- зниження SNR призводить до збільшення абсолютних значень спектральних ознак та згладжування відмінностей між пристроями;
- для пристроїв однієї моделі помилки ідентифікації виникають при  $\text{SNR} \approx 40$  дБ.

Ці результати дозволяють визначити граничні значення SNR, за яких методи ідентифікації залишаються ефективними у реальних мережевих умовах.

За отриманими даними були побудовані графіки залежностей ймовірності пропуску цілі  $P_m$  та хибної тривоги  $P_{fa}$ , де  $L$  – значення параметра для оцінки безпеки мережі, що показано на рис. 1.

Залежності ймовірності пропуску цілі  $P_m$  та помилкової тривоги  $P_{fa}$  відповідно до рис. 1 наведені на рис. 2 для SNR 40 дБ. Дані залежності зберігаються при SNR 30, 20 та 10 дБ.

Спектральні ознаки мобільних пристроїв можуть слугувати надійними фізичними маркерами для їх ідентифікації у Wi-Fi мережах за умови контролю співвідношення сигнал/шум. Метод середнього квадрату різниці демонструє високу точність за відносно високих рівнів SNR, тоді як коефіцієнт асиметрії є більш ефективним у шумних каналах і дозволяє розрізняти пристрої навіть за низьких рівнів сигналу.

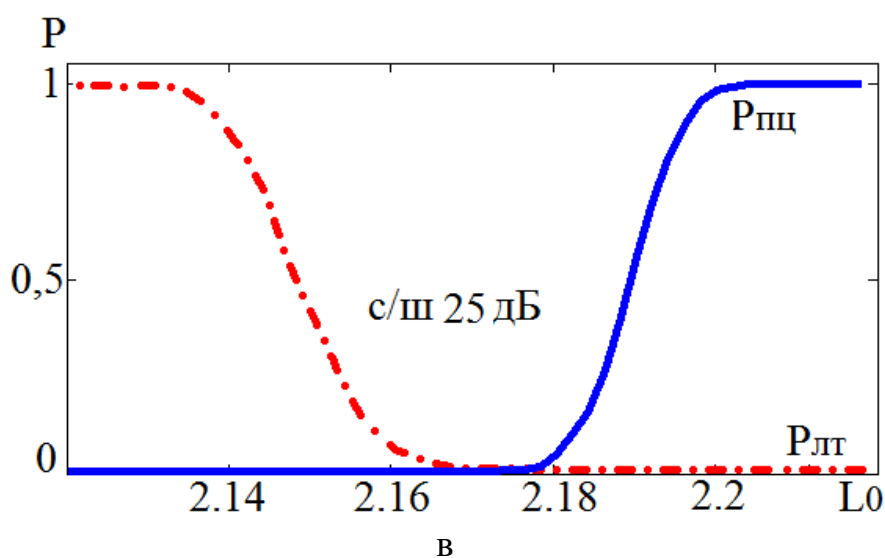
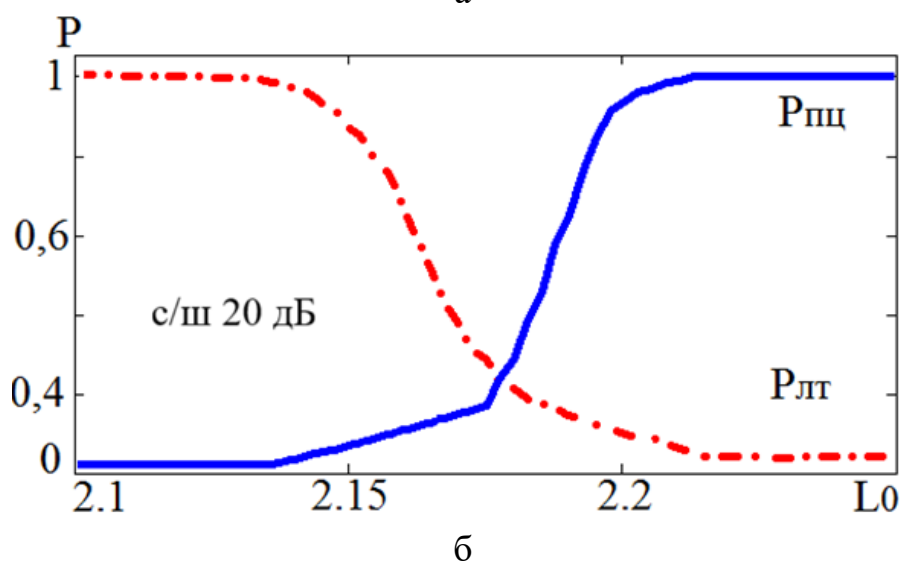
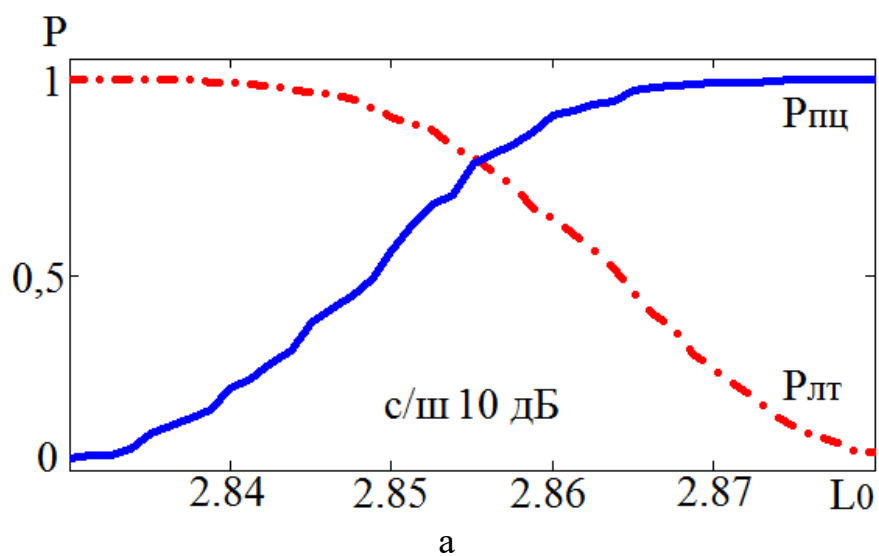


Рисунок 1. – Залежність ймовірності помилкової тривоги і пропуску цілі від встановленого порогу для SNR:  
а) 10 дБ; б) 20 дБ; в) 25 дБ

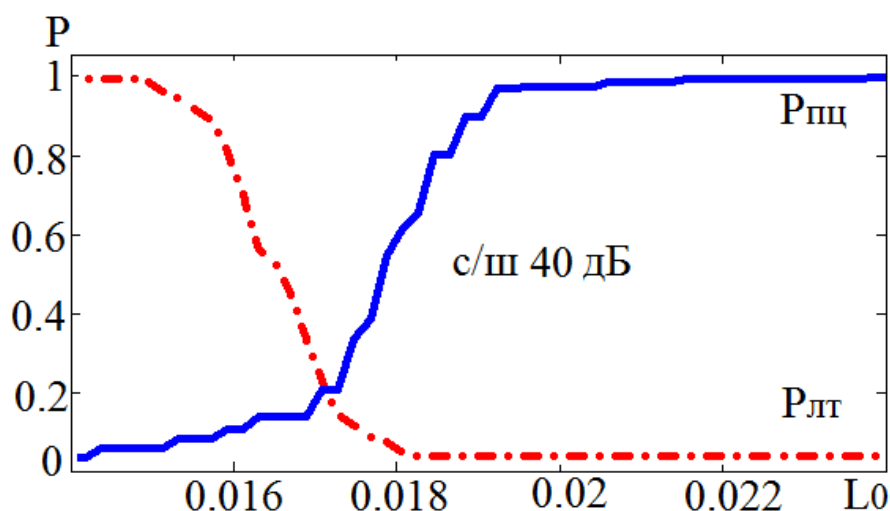


Рисунок 2 – Залежність ймовірності помилкової тривоги і пропуску цілі від установленого порогу для SNR 40 дБ для однакових моделей пристрою

Для підвищення надійності ідентифікації в умовах низького SNR доцільно застосовувати двопорогові алгоритми з елементами нечіткої логіки, що забезпечує додаткову стійкість до шуму. Отримані результати можуть бути використані для підвищення безпеки бездротових мереж за допомогою фізичних методів автентифікації та для розробки більш надійних систем контролю доступу на основі радіочастотних відбитків пристроїв.

Список використаних джерел:

1. Antipov I., Vasilenko T. Improving the model of decision making about abnormal network state using a positioning system // Eastern-European Journal of Enterprise Technologies. 2019. Vol. 1, № 9 (97). P. 6–11. DOI: <https://doi.org/10.15587/1729-4061.2019.157001>
2. Antipov I., Vasylenko T. Identification of mobile devices by correlation features of their signal spectra // Radio Electronics, Computer Science, Control. 2024. № 4. P. 6–12. DOI: <https://doi.org/10.15588/1607-3274-2024-4-1>
3. Антіпов І. Є., Василенко Т. О. Ідентифікація мобільних пристроїв за особливостями спектрів їх сигналів // Радіотехніка. 2020. Вип. 201. С. 91–97. DOI: <https://doi.org/10.30837/rt.2020.2.201.07>
4. Danev B., Zanetti D., Čapkun S. Physical-layer identification of wireless devices through RF fingerprinting // ACM Transactions on Information and System Security. 2012. Vol. 15, № 1. P. 1–30. DOI: <https://doi.org/10.1145/2133375.2133376>
5. Taşcıoğlu A., Alçın Ö. F., Yıldırım D. Transient-based RF fingerprinting using IEEE 802.11 transmitters // Electronics. 2024. Vol. 14, № 1. Art. 4. DOI: <https://doi.org/10.3390/electronics14010004>