ПОРІВНЯЛЬНИЙ АНАЛІЗ РИЗИКІВ ПРИВАТНОСТІ ДЛЯ ГІБРИДНИХ ІНТЕЛЕКТУАЛЬНИХ ПОВЕРХОНЬ

Павленко Є.М., Сердюк Н.М.

Харківський Національний університет радіоелектроніки,
Україна.

E-mail: yevhen.pavlenko1@nure.ua

Abstract

This research investigates the risks to biometric privacy in 6G and ISAC systems using reconfigurable distributed antenna and reflecting surfaces (RDARS). We analyse data leakage channels comparatively across passive reconfigurable intelligent surfaces (RIS), active distributed antenna systems (DAS), and hybrid RDARS architectures. Our analysis reveals that the hybrid RDARS architecture poses the most significant threat. This architecture introduces a novel leakage channel: a dynamic sequence of system decisions about the operating modes of elements (active vs. passive). This 'selection gain' metadata creates a unique digital 'fingerprint' correlated to user movement, which is more informative and dangerous than leakage from purely passive or active systems.

Вступ

Розвиток бездротових мереж шостого покоління пов'язаний із впровадженням гнучких архітектур, таких як реконфігуровані розподілені антени та відбиваючі поверхні (Reconfigurable Distributed Antenna and Reflecting Surface, RDARS), що інтегрують функції зв'язку та зондування (Integrated Sensing and Communication, ISAC) [1]. Поєднуючи пасивне відбиття сигналу інтелектуальними поверхнями (RIS) та активне приймання/передавання розподіленими антенами (DAS), архітектура RDARS значно підвищує спектральну та енергетичну ефективність. Водночас, дослідження доводять, що стандартна інформація зворотного зв’язку про стан каналу (Channel State Information, CSI) може бути використана для біометричної ідентифікації користувачів за такими ознаками, як хода, жести чи навіть дихання [2]. Це створює ключову проблему безпеки: як саме архітектурні компоненти RDARS та їхні режими роботи впливають на інформативність каналу витоку біометричних даних. Аналіз цього питання є критичним для розробки безпечних систем 6G та ISAC.

Метою є порівняльний аналіз природи та інформативності каналів витоку біометричних даних для трьох архітектурних реалізацій, що узагальнюються фреймворком RDARS: чисто пасивної RIS, чисто активної DAS та гібридної RDARS.

Виклад основного матеріалу

Архітектура RDARS, описана в [1], дозволяє виділити три режими функціонування, кожен з яких створює унікальний за своєю природою канал витоку інформації. Джерелом атаки є пасивне перехоплення даних, що характеризують стан радіоканалу, який динамічно змінюється під впливом руху людини.

У випадку чисто пасивної архітектури RIS канал витоку формується на основі часових послідовностей оптимальних фазових зсувів елементів поверхні. Особливістю цього режиму є ефект мультиплікативного затухання, оскільки сигнал зазнає подвійного ослаблення на шляху "передавач-RIS-приймач", пропорційного добутку відстаней [3]. Це робить стан каналу надзвичайно чутливим до мікроскопічних змін середовища, спричинених рухами кінцівок людини. Однак така складна траєкторія поширення вносить додатковий шум та неоднозначність, що ускладнюється відсутністю у RIS власної радіочастотної частини для прямого вимірювання каналу та синхронізації. Це потенційно ускладнює виділення стабільних біометричних ознак зловмисником.

На противагу цьому, в чисто активній архітектурі DAS канал витоку базується на аналізі CSI для активних антенних елементів. На відміну від RIS, сигнал проходить пряміший шлях від користувача до активного елемента, що зменшує кількість багатопроменевих відбиттів та фазових спотворень. Це забезпечує вище відношення сигнал/шум (SNR) у вимірах CSI та формує чистішу, стабільнішу біометричну сигнатуру, що є аналогічною до тієї, яка експлуатується в класичних атаках на основі CSI. Інформативність цього каналу витоку висока, але просторово обмежена, що пов'язано з фіксованою геометрією розміщення активних антен.

Найбільш значний та раніше не досліджений ризик створює гібридна архітектура RDARS. Вона не лише поєднує вразливості обох попередніх сценаріїв, але й додає новий, поведінковий вимір для атаки. Канал витоку тут формується не тільки з фазових зсувів чи CSI, але й з послідовності рішень системи щодо вибору режиму роботи кожного елемента. Алгоритм керування RDARS у реальному часі вирішує оптимізаційну задачу: який елемент має відбивати, а який — активно приймати/передавати сигнал. Ця послідовність рішень, що забезпечує "виграш від вибору" (selection gain) [4], є унікальною мета-інформацією, оскільки вона корелює зі змінами в каналі, спричиненими рухом користувача. Фактично, це низькорозмірний, але надзвичайно інформативний часовий ряд. Аналізуючи його, зловмисник отримує доступ до результатів роботи вбудованого в систему механізму виділення ознак, що робить цей канал витоку особливо небезпечним.

Висновки

Аналіз показує, що гнучкість архітектури RDARS, яка є її ключовою перевагою, одночасно створює її найбільшу вразливість. Кожен рівень гнучкості (фаза, розподіл, вибір режиму) додає новий вимір до каналу витоку біометричної інформації. Найбільшу загрозу становить динамічний вибір режимів роботи елементів, оскільки послідовність цих рішень створює унікальний цифровий "відбиток" взаємодії користувача з середовищем. Цей відбиток потенційно є більш інформативним, ніж дані в чисто пасивних (RIS) чи активних (DAS) системах. Слід підкреслити необхідність розробки нових підходів до захисту каналів зворотного зв'язку в системах ISAC/6G, які мають унеможливити несанкціонований аналіз рішень про селекцію режимів роботи мережі.

Література

1. Integrated sensing and communication with reconfigurable distributed antenna and reflecting surface: joint beamforming and mode selection / P. Zhang et al. // IEEE internet of things journal. 2025. P. 1. URL: https://doi.org/10.1109/jiot.2025.3555001 (date of access: 12.11.2025).

2. Inference attacks. Encyclopedia of cryptography, security and privacy. Cham, 2025. P. 1207. URL: https://doi.org/10.1007/978-3-030-71522-9_300490 (date of access: 12.11.2025).

3. Ax-csi / F. Gringoli et al. // ACM mobicom '21: the 27th annual international conference on mobile computing and networking, New Orleans LA USA. New York, NY, USA, 2021. URL: https://doi.org/10.1145/3477086.3480833 (date of access: 12.11.2025).

4. Ma Y., Zhou G., Wang S. WiFi sensing with channel state information. // ACM computing surveys. 2019. Vol. 52, no. 3. P. 1–36. URL: https://doi.org/10.1145/3310194 (date of access: 12.11.2025).