https://www.proconference.org/index.php/gec/article/view/gec34-00-015
DOI: 10.30890/2709-1783.2024-34-00-015

УДК 004.7:621.396.96

ANALYSIS OF INFORMATION SECURITY AND THE PRESENCE OF PEOPLE IN THE CONTROLLED AREA BASED ON COMPUTER NETWORK TRAFFIC LISTENING

АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРИСУТНОСТІ ЛЮДЕЙ У КОНТРОЛЬОВАНІЙ ЗОНІ НА ОСНОВІ ПРОСЛУХОВУВАННЯ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Tohoiev O.R. / Тогоєв О. Р.,
PhD student / аспірант
ORCID: 0000-0003-3465-7767
Zhuravska I.M. / Журавська І. М.,
d.t.s., prof. / д.т.н., проф.
ORCID: 0000-0002-8102-9854
Petro Mohyla Black Sea National University, Mykolaiv, 68 Desantnykiv, 10, 54003
Чорноморський національний університет ім. Петра Могили, Миколаїв, вул. 68 Десантників, 10, 54003

Анотація. *Сервісні функції сучасних операційних систем дозволяють здійснювати пасивний моніторинг («прослуховування») трафіку комп'ютерної мережі без використання додаткового інструментарію та додаткового обладнання. Такі функції можна використати для контролю інформаційної безпеки шляхом виявлення появи нових об'єктів (як людей, так і матеріальних предметів) у контрольованій зоні. Дослідження спрямоване на розвиток методів виявлення об'єктів на основі аналізу інформації про стан каналу (CSI) мережі Wi-Fi та створення відповідного апаратно-програмного забезпечення. Актуальність роботи підкреслюється потенціалом використання таких систем для неінвазивного виявлення небезпечних предметів у навколишньому середовищі. Дослідження охоплює процес виявлення об'єктів шляхом аналізу сигналів Wi-Fi, зосереджуючи увагу на методах та алгоритмах обробки CSI для ефективної класифікації та ідентифікації об'єктів. Запропоновано метод виявлення об'єктів на основі аналізу сигналів мережі та досліджено зміну CSI-даних в залежності від матеріалу об'єкта, що створює перешкоду.*

Ключові слова: *інформаційна безпека, контрольована зона, мережа Wi-Fi, прослуховування мережевого трафіку, інформація про стан каналу (CSI), RSSI сигналу, виявлення об'єкта.*

Abstract. *Service functions of modern operating systems allow passive monitoring ("listening") of computer network traffic without the use of additional tools and additional equipment. Such functions can be used to control information security by detecting the appearance of new objects (both people and material objects) in the controlled area. The study is aimed at developing methods for detecting objects based on the analysis of channel state information (CSI) of the Wi-Fi network and creating appropriate hardware and software. The relevance of the work is emphasized by the potential of using such systems for non-invasive detection of dangerous objects in the environment. The study covers the process of detecting objects by analyzing Wi-Fi signals, focusing on CSI processing methods and algorithms for effective object classification and identification. A method for object detection based on network signal analysis is proposed. The change in CSI data depending on the material of the object that creates an obstacle is investigated.*

Keywords: *information security, controlled area, Wi-Fi network, network traffic listening, channel state information (CSI), RSSI of signal, object detection.*

Вступ.

Актуальність дослідження системи виявлення об'єктів на основі інформації про стан каналу (англ. Channel State Information, CSI) мережі Wi-Fi пояснюється кількома факторами. По-перше, сервісні функції сучасних операційних систем – у т. ч. тих, на базі яких будуються прошивки комутаційного обладнання – дозволяють здійснювати пасивний моніторинг («прослуховування») трафіку комп'ютерної мережі без використання додаткового інструментарію та додаткового обладнання [1]. Такі функції можна використати для контролю інформаційної безпеки шляхом виявлення появи нових об'єктів у контрольованій зоні (КЗ). Існуюча інфраструктура бездротових мереж робить впровадження такої системи економічно доцільним і простим. По-друге, використання радіочастотних сигналів замість звичайних датчиків або камер дозволяє здійснювати моніторинг середовища без перешкод, що є особливо важливим в певних умовах.

Таким чином, шляхом прослуховування трафіку мережевого обладнання можливо виявляти не тільки людей у КЗ, а й деякі матеріальні об'єкти (у т. ч. небезпечні), поява яких на шляху розповсюдження WiFi-сигналу змінює його CSI-характеристики.

Мета.

Метою роботи є подальший розвиток методів виявлення та визначення типу об'єктів на основі аналізу CSI-інформації про мережу Wi-Fi.

Основний текст та методи дослідження.

CSI (Channel State Information) – це дані про стан каналу, які характеризують особливості поширення радіохвиль у бездротових мережах. У WiFi-мережах CSI забезпечує детальну інформацію щодо амплітуди та фази прийнятих сигналів на різних частотних підканалах технології OFDM (Orthogonal Frequency Division Multiplexing) [2]. Ці дані відіграють важливу роль у виявленні об'єктів та відстеженні їх руху в межах зони покриття WiFi-мережі.

Структура CSI мережі Wi-Fi включає такі основні компоненти (рис. 1):

а) точки доступу (англ. Access Points, APs) – пристрої, що забезпечують безпроводове з'єднання для клієнтських пристроїв та збирають CSI-дані [3];

б) клієнтські пристрої (наприклад, ноутбуки, смартфони) – пристрої, що підключаються до точок доступу для отримання доступу до мережі та можуть надавати додаткові CSI-дані;

в) канал зв'язку – середовище, через яке поширюються радіохвилі між точками доступу та клієнтськими пристроями.

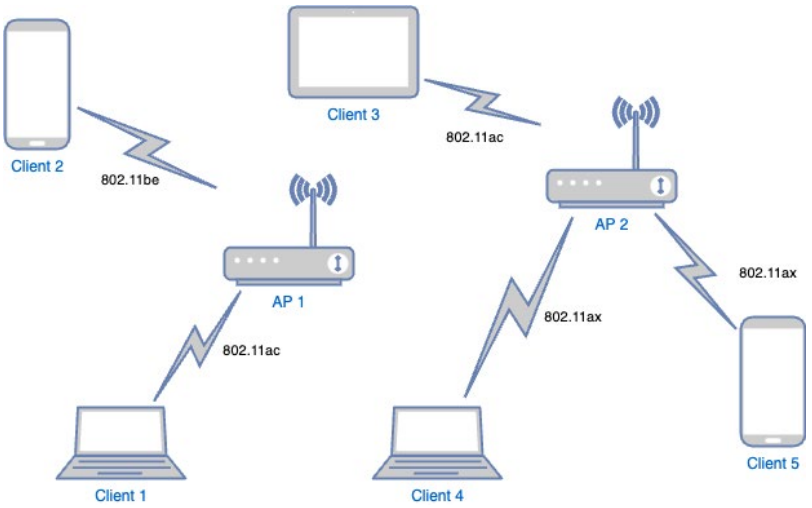


Рисунок 1 – Основні компоненти CSI мережі

Авторська розробка

Принцип роботи CSI у WiFi-мережах ґрунтується на аналізі поширення радіохвиль у каналі зв'язку. Сигнали, що передаються від точки доступу, відбиваються від різних об'єктів, таких як стіни, меблі, люди тощо, і досягають клієнтського пристрою різними шляхами. Ці багатопроменеві компоненти сигналу взаємодіють один з одним, що викликає зміни амплітуди та фази сигналу на різних підканалах OFDM. Такі зміни є унікальними для конкретного середовища і залежать від розташування та характеристик об'єктів у ньому.

Слід зауважити, що навіть при відключенні WiFi-модуля та геолокації в гаджеті (смартфоні, планшеті тощо), який користувач вносить із собою у КЗ, все одно сама його поява на шляху розповсюдження WiFi-сигналу від комутаційного обладнання, встановленого у КЗ, змінить CSI-характеристики. Ідентифікації нового об’єкта у КЗ також сприяють внутрішні протоколи

деанонімізації в ОС [4].

CSI містить інформацію про амплітуду та фазу для кожного підканалу OFDM, що дозволяє досліджувати характеристики багатопроменевого середовища з високою роздільною здатністю [5]. Ця інформація може бути використана для виявлення об'єктів та їх руху в межах зони покриття мережі Wi-Fi шляхом аналізу змін у CSI-даних, нп., як наведено на рис. 2 [6].

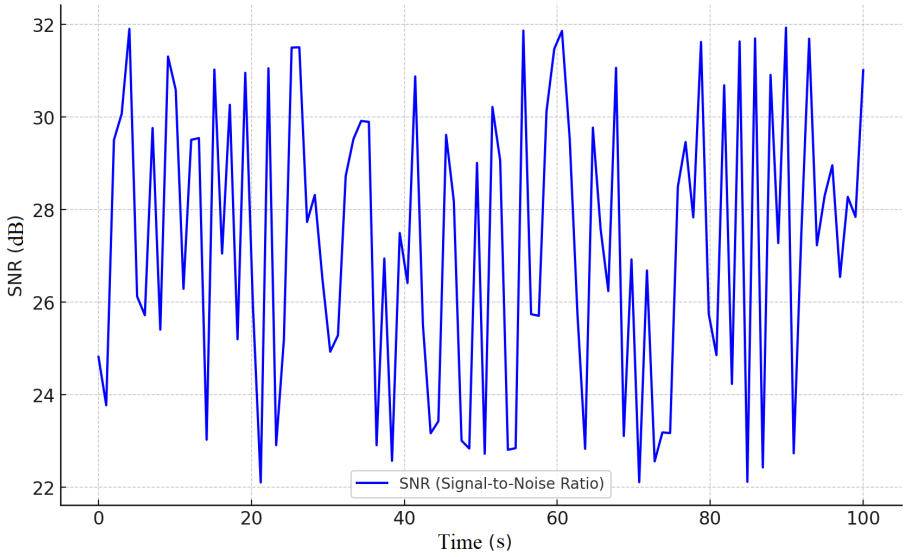


Рисунок 2 – Графік відношення сигнал/шум CSI

Джерело: [6]

CSI-дані є надзвичайно чутливими до найменших змін у навколишньому середовищі. Це обумовлено природою поширення радіохвиль, які взаємодіють з різними об'єктами та матеріалами на своєму шляху. Навіть незначний рух або зміна положення об'єкта може призвести до помітних змін в амплітуді та фазі сигналу на різних підканалах. Ступінь заломлення, відбиття та поглинання радіохвиль залежить від фізичних властивостей матеріалів, з якими вони взаємодіють. Наприклад, металеві поверхні сильно відбивають радіохвилі, тоді як об'єкти з води або біологічних тканин можуть спричиняти значне поглинання сигналу. Перешкоди з діелектричних матеріалів, таких як дерево, пластик або цегла, можуть викликати заломлення радіохвиль. Ефекти заломлення та відбиття радіохвиль найбільш помітні на вищих частотах, адже довжина хвилі стає порівнянною з розмірами перешкод. Тому дані CSI,

отримані на вищих частотних підканалах, зазвичай містять більше інформації про дрібні зміни в середовищі.

Крім того, поляризація радіохвиль також відіграє важливу роль. Вертикально поляризовані хвилі більш чутливі до вертикальних перешкод, таких як люди або меблі, тоді як горизонтально поляризовані хвилі краще взаємодіють з горизонтальними поверхнями, такими як підлога або стеля. Одним з ключових викликів у використанні CSI є необхідність ефективної фільтрації та обробки величезного обсягу даних, що надходять від різних частотних підканалів. Для цього часто використовуються складні алгоритми машинного навчання, які можуть виявляти закономірності та тренди у даних CSI, пов'язані з рухом або присутністю об'єктів.

Результати та обговорення.

Подальший розвиток описаного вище методу виявлення об’єктів полягає в розподілі системи на два основних етапи: збір еталонних даних та розпізнавання об'єктів. Відповідно основних функцій у ПЗ можна виділити також дві:

1) функція запису еталонних даних у БД;

2) функція порівняння вхідних даних з еталонними.

Функція збору еталонних CSI-даних реалізована наступним чином: Встановлюється таймер на 60 секунд для визначення проміжку часу збору даних. Після цього починається безперервне зчитування CSI-даних з послідовного порту сервера, куди вони передаються з WiFi-мережі, в зоні дії якої знаходиться об'єкт дослідження. Отримані CSI-дані проходять попередню обробку програмним забезпеченням (ПЗ) для виділення корисної інформації. Усереднені еталонні CSI-дані разом з міткою, що ідентифікує досліджуваний об'єкт. Після завершення 60-секундного таймера збір еталонних даних припиняється, і зібрані CSI-шаблони для даного об'єкта стають доступними для використання в режимі розпізнавання.

Порівняння вхідних даних з еталонними відбувається шляхом підключення до послідовного порту сервера для зчитування вхідних CSI-даних. Далі

починається безперервне зчитування вхідних CSI-даних з послідовного порту в режимі реального часу. Отримані CSI-дані порівнюються з усіма еталонними даними, що зберігаються. Для кожного типу об'єкта з БД підтягуються відповідні еталонні CSI-дані, позначені міткою (маркером) цього типу об'єкта.

Процес порівняння полягає в наступному: береться кожна піднесуча вхідних CSI-даних та кожна піднесуча еталонних CSI-даних, і обчислюється коефіцієнт схожості між ними. Якщо середній коефіцієнт схожості всіх піднесучих складає не менше ніж 95 %, вважається, що об'єкт виявлено. Коефіцієнт схожості розраховується шляхом порівняння амплітуд та фаз піднесучих вхідних та еталонних CSI-даних. Чим ближче ці значення для кожної піднесучої, тим вищий коефіцієнт схожості. Якщо схожість всіх піднесучих перевищує поріг 95 %, система вважає, що поточні вхідні CSI-дані відповідають еталонним даним для певного типу об'єкта.

Центральним компонентом апаратної частини системи виявлення об'єктів у КЗ на основі CSI мережі Wi-Fi є мікроконтролер ESP32 від Espressif Systems. Зокрема, використовується плата розробки ESP32-DevKit-V1 на базі ESP32 [7]. Цей мікроконтролер був обраний due to свою високу продуктивність, низьке енергоспоживання та наявність вбудованого модуля Wi-Fi, що робить його вдалим рішенням для збору CSI-даних.

Система буде складатись з мікроконтролера ESP32-DevKit-V1, сервера з ПЗ та бази даних для зберігання еталонних CSI-даних. Взаємодію між цими компонентами відображено на рис. 3.

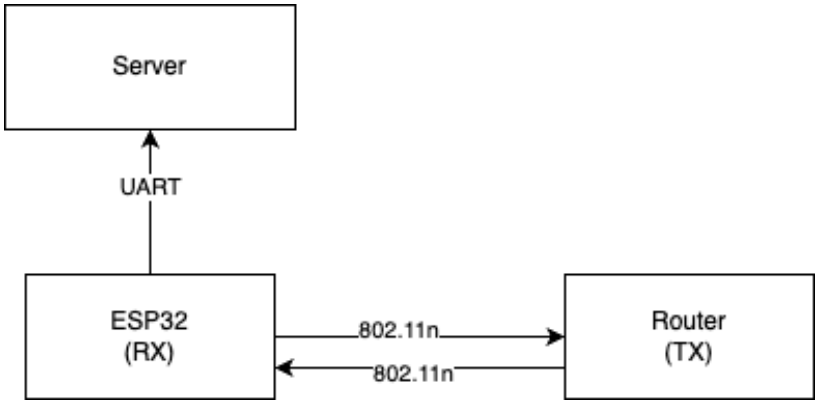
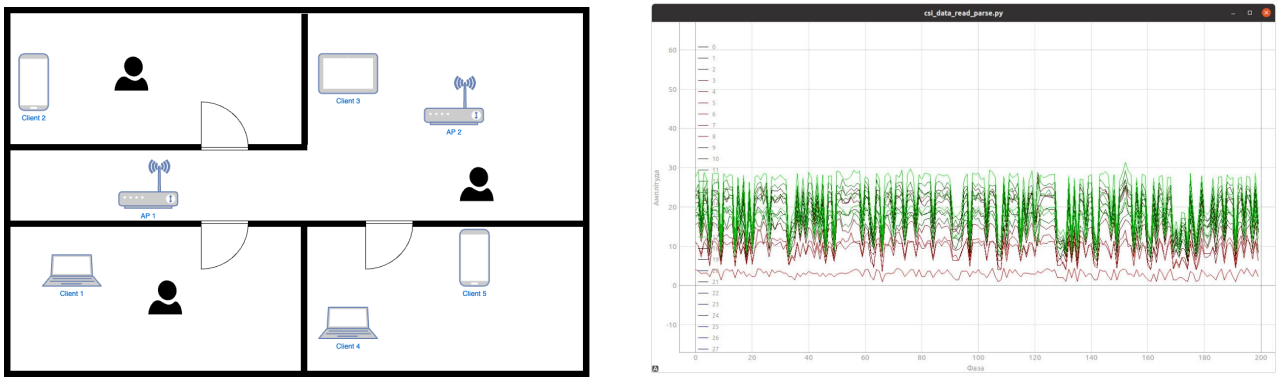


Рисунок 3 – Концептуальна схема

Авторська розробка

Також можливе визначення локації людини (рис. 4). За допомогою аналізу цих CSI-даних можна здійснити локалізацію людини в приміщенні на території організації. CSI-дані можуть бути інтегровані з іншими датчиками та системами для створення інтелектуальних середовищ, таких як розумні будинки, розумні офіси чи розумні міста [8]. Такі інтегровані рішення дозволяють збирати різноманітні дані про середовище та поведінку людей для забезпечення автоматизації, енергозбереження та підвищення комфорту.



а) б)

Рисунок 4 – Сценарій зондування на основі CSI: а – розміщення людей у приміщеннях з Wi-Fi обладнанням; б – CSI-дані сигналу з приміщень

Авторська розробка

Перевагою інтеграції CSI-технологій в інтелектуальні середовища – це можливість створення більш розумних, зручних та енергоефективних систем.

CSI-дані надають цінну інформацію про присутність та поведінку людей, що дозволяє автоматизувати процеси та адаптувати середовище відповідно до їхніх потреб.

Висновки.

Подальший розвиток метод використання CSI-даних сигналу Wi-Fi від стандартного обладнання, вже встановленого на території підприємства будь-якої галузі, для виявлення об'єктів у середовищі має значні переваги над існуючими аналогами. Такими перевагами зокрема є безконтактність, відсутність необхідності в додаткових датчиках, можливість виявлення об'єктів за стінами тощо. Наукова новизна такого підходу полягає у вдосконаленні

алгоритмів обробки CSI, що підвищує точність класифікації та визначення відстані до об'єктів. Отримані результати цієї роботи надають можливість створення економічно вигідних систем моніторингу на основі вже існуючої інфраструктури бездротових мереж, що робить її особливо привабливою для застосування в різних галузях.

Література:

1. Linux iftop – Listen Network Traffic and Bandwidth. URL: https://www.geeksforgeeks.org/linux-iftop-listen-network-traffic-and-bandwidth/ (Last accessed: 21.08.2024).

2. Zhu Yi., Zhu Ya., Zhang Z., Zhao B. Y., Zheng H. 60GHz mobile imaging radar. *Mobile Computing Systems and Applications (HotMobile'15*) : Proc. of the 16th Internat. Workshop, Santa Fe, New Mexico, USA. New York, NY, USA, 2015. P. 75–80. DOI: 10.1145/2699343.2699363.

3. Тогоєв О. Р. Метод деанонімізації користувачів iOS через протокол AirDrop. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво* : наук. журн. / Луцьк. нац. техн. ун-т. 2022. Вип. 49. С. 12–-17. DOI: 10.36910/6775-2524-0560-2022-49-02.

4. Abazorius A. New system allows for high-accuracy, through-wall, 3-D motion tracking. Massachusetts Institute of Technology News : web site. Publ. Dec. 11, 2013. URL: https://news.mit.edu/2013/new-system-allows-for-high-accuracy-through-wall-3-d-motion-tracking-1211 (Last accessed: 23.08.2024).

5. Ma Y., Zhou G., Wang S. WiFi sensing with channel state information. *ACM Computing Surveys*. 2019. Vol. 52, no. 3. P. 1–36. DOI: 10.1145/3310194.

6. Al-ganess M. A. A., Elaziz M. A., Kim S., Ewees A. A., Abbasi A. A., Alhaj Yo. A., Hawbani A. Channel state information from pure communication to sense and track human motion: A survey. *Sensors.* 2019. Vol. 19, Is. 15, no. 3329. 27 p. DOI: 10.3390/S19153329.

7. ESP-IDF Programming Guide v5.0.2 documentation. Technical Documents | Espressif Systems. URL: https://docs.espressif.com/projects/esp-

idf/en/v5.0.2/esp32/get-started/index.html (Last accessed: 01.08.2024).

8. Ding J., Wang Y. WiFi CSI-based human activity recognition using Deep Recurrent Neural Network. *IEEE Access.* 2019. Vol. 7. P. 174257–174269. DOI: 10.1109/ACCESS.2019.2956952 (Last accessed: 01.08.2024).

Науковий керівник: д.т.н., проф. Журавська І. М.

Тези відправлено: 30.08.2024