

УДК 621.395.74:621.396.94]:629.783

## **ДОСЛІДЖЕННЯ МЕТОДІВ ВІДСТЕЖЕННЯ ТЕЛЕФОНІВ ЗА ДОПОМОГОЮ GPS ТА ЧЕРЕЗ ВІДПРАВКУ ПАКЕТІВ ДАНИХ ЗА НАЗВОЮ МЕРЕЖІ**

Запара О. С.

Науковий керівник – к.т.н., доцент Чуприна А. С.

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

e-mail: [oleksandr.zapara@nure.ua](mailto:oleksandr.zapara@nure.ua)

The object of research is methods of tracking phones using GPS and sending data packets by network name. The purpose of the work is to study methods for tracking phones using GPS and by sending data packets by network name to study comparative performance characteristics and implementation of similar methods. Methods and methods of tracking smartphones, ways of their implementation and final results for comparative characteristics are considered in the work. As a result of the work, the methods of tracking phones using GPS and sending data packets by network name were investigated, their implementation and methods of reproduction in the program for their use, a comparative characteristic of similar methods and their implementation was developed.

На сьогодні відстеження місцезнаходження смартфонів через GPS виявляє високу актуальність, коли технології невід'ємно влітаються в наше щоденне життя. Однак застосування таких методів відстеження супроводжується кількома суттєвими проблемами.

По-перше, питання викликають недотримання приватності та етики. Збір і використання цих даних може порушувати особисту приватність користувачів, створюючи конфлікт між необхідністю захисту та потребою використання цієї інформації. Технічні обмеження також впливають на ефективність методів відстеження. Перешкоди для GPS-сигналів та інші технічні аспекти можуть призводити до неточності визначення місцезнаходження, що ускладнює задачу забезпечення точності та достовірності отриманих даних.

Не менш важливою є проблема безпеки даних. Ризик кібератак та неправомірного доступу до зібраних інформаційних потоків може підірвати довіру та створити загрозу конфіденційності особистої інформації.

Додатково, недостатня регуляторна база відсутність чітких норм для легітимного використання технологій відстеження телефонів можуть стати причиною неправомірних дій та порушення прав громадян. З розвитком технологій необхідно не лише виявляти та розв'язувати поточні проблеми, але й адаптувати методи відстеження до нових викликів. Постійне оновлення та вдосконалення стають ключовими завданнями для забезпечення ефективності систем відстеження телефонів.

Нарешті, вирішення проблеми системних взаємодій вимагає встановлення стандартів для інтеграції та взаємодії різних технологій в єдиній системі відстеження. Одним із таких прикладів є два методи відстеження, перший з яких з використанням GPS-технології, а другий через аналіз відправлених пакетів даних за назвою мережі.

GPS-технології відстеження визначаються як методи, що використовують систему глобального позиціонування (GPS) для визначення точного місцезнаходження об'єкта, такого як мобільний телефон. GPS, розроблена Сполученими Штатами, складається з супутникової системи, що передає сигнали на Землю, та приймачів, вбудованих у пристрої користувачів. Ці технології дозволяють точно визначати географічні координати, такі як широта, довгота та висота, забезпечуючи надзвичайно точний метод відстеження місцезнаходження. У нашому дослідженні ми розглянемо якість цього методу, його застосування та можливі заходи забезпечення конфіденційності у порівнянні з іншими методами в контексті відстеження мобільних телефонів.

Аналіз відправлених пакетів даних за назвою мережі є методом відстеження місцезнаходження, який використовується для визначення положення пристроїв, зокрема мобільних телефонів, на основі інформації, яку вони передають через мережеві з'єднання. Кожна мережа має свою унікальну ідентифікаційну назву (наприклад, ім'я оператора зв'язку), і пристрої регулярно взаємодіють з цими мережами для передачі даних[1].

Аналіз пакетів даних за назвою мережі може включати в себе спостереження за змінами у мережевих параметрах, які вказують на підключення до конкретної мережі на певному місці та часі. Ця інформація може допомагати визначити, де знаходиться пристрій у конкретний момент. У рамках нашого дослідження ми розглянемо, наскільки точні і надійні наведені дані, а також ризики з точки зору конфіденційності. Питання безпеки та можливість неправомірного використання цієї інформації визначатимуться як частини загального аналізу, метою якого є вдосконалення стратегій захисту особистої інформації в цифровому середовищі.

Обидва методи мають власний набір плюсів і мінусів, і вибір між ними залежить від конкретних потреб проекту.

По-перше, наявність високої точності. GPS може забезпечити високу точність визначення місцезнаходження, що робить його ефективним для великої кількості застосувань.

По-друге, ефективність в місцях з обмеженим сигналом GPS. Там, де сигнал GPS може бути обмеженим (наприклад, всередині будівель або в глибоких ущелинах), аналіз пакетів даних може стати альтернативою для визначення місцезнаходження.

По-третє, глобальність. GPS працює практично в будь-якій точці земної поверхні, що робить його універсальним для використання в різних географічних областях.

Отже, обидва методи мають свої обмеження, і вибір між ними залежить від конкретних вимог застосувань та ситуацій. Комбінація різних методів може допомогти зменшити їхні недоліки та підвищити ефективність визначення місцезнаходження.

Щоб забезпечити перевірку методів працездатності відстеження смартфонів, будемо використовувати такі програмні засоби та підходи:

- автоматизоване тестування використовує інструменти автоматизації, такі як Selenium або Appium, для створення та виконання тестових сценаріїв, які імітують реальні умови використання смартфонів[2].

- модульне тестування для розробки тестів окремих компонентів програми, щоб переконатися, що кожен модуль працює належним чином перед інтеграцією в більшу систему.

- навантажувальне тестування для симуляція великої кількості запитів до сервера або API, щоб перевірити, як методи відстеження смартфонів ведуть себе під високим навантаженням.

- тестування безпеки забезпечує проведення тестів на проникнення та вразливості, щоб виявити потенційні слабкі місця в методах відстеження смартфонів.

Наше дослідження вирішує наведені проблеми за такими критеріями: точність для визначення похибки відстеження координат смартфона, приватність для забезпечення конфіденційності даних користувача, надійність для захисту від зовнішнього впливу (кібератак) та швидкість для миттєвої передачі даних.

Вивчення способів відстеження місцезнаходження телефонів через GPS та передачу пакетів даних за ім'ям мережі підкреслює необхідність гнучкості та адаптивності у розробці геолокаційних систем, ураховуючи різноманітні вимоги та умови використання. Ефективне застосування цих методів може сприяти виникненню інноваційних рішень у сфері визначення місцезнаходження та відстеження мобільних пристроїв у сучасному цифровому середовищі.

Список використаних джерел:

1. Бугай Д., Копоть М., Дудар З. Реалізація Програмного Забезпечення Системи Контролю Доступу до Приміщення. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/4d0031fd-87bf-4f80-9a97-635cc0434406/content> (дата звернення: 14.03.2024).

2. Олесків О., Кунець І., Микитин І. Аналітичний Огляд Процедур та Методів Метрологічної Перевірки Програмного Забезпечення Засобів Вимірювання. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3655/vtm75st04.pdf> (дата звернення: 14.03.2024).