УДК 681.32

# ЗАХИСТ ДАНИХ В ЗАДАЧАХ НАВІГАЦІЇ В PHYSICAL WEB

*Семеренко Василь, Кошолап Микола*

Вінницький національний технічний університет

## Анотація

*Розглянуто навігацію в закритих приміщеннях в рамках технології Physical Web. Показана можливість виправлення помилок в повідомленнях від маячків iBeacon та AltBeacon за допомогою завадостійкого кодування. Пропонується використання в межах стандартизованих форматів повідомлень двох полів CRC для реалізації ітеративного декодування циклічних кодів з примітивними породжувальними поліномами.*

## Abstract

*The indoor navigation using beacons with Physical Web technology is considered. The capability to correct errors in messages from iBeacon and AltBeacon with the help of error correcting coding is shown. It is proposed to use two CRC fields within the standardized message formats to implement iterative decoding of cyclic codes with primitive generator polynomials.*

## Вступ

Ми знаходимось на початку якісно нового використання Інтернету – Інтернету Речей (Internet of Things, IoT). IoT дозволить підключити до традиційної мережі WWW широку сукупність електронних пристроїв, зв'язуючи між собою цифровий та фізичний світ [1].

В наш час багато об'єктів повсякденного життя ще не можуть безпосередньо встановити зв'язок із всесвітньою Мережею по традиційним інтерфейсам. Для підключення таких пристроїв були створені спеціальні ідентифікаційні мітки. Вперше ідея таких міток була реалізована ще на початку 2000-х років у вигляді радіоміток RFID та QR-кодів. Однак із-за складності реалізації та проблем із забезпечення захисту даних ці мітки не набули масового поширення.

Принципово інші підходи були закладені в рамках технології Physical Web [2], яка поєднала так звані "маячки" (англ. beacons) та посередницькі веб-сервіси. Хоча ідея цієї технології вперше була запропонована Google, сьогодні від цим загальним терміном розуміють проекти різних фірм: Apple, Radius Network та ін.

## Навігація в Physical Web

У світі існують три найбільш популярні стандарти маячків:

- *iBeacon* (від *Apple*);
- *AltBeacon* (від *Radius Network*);
- *Eddystone* (від *Google*).

Сучасні маячки – це мініатюрні передавачі, які регулярно передають *Bluetootch*-сигнали з низьким енергоспоживанням. Ці сигнали можуть бути прийняті мобільними телефонами (смартфонами) на деякій відстані (до 50 метрів на відкритій місцевості та дещо меншій відстані у закритих приміщеннях). Далі запити передаються на хмарні сервіси для подальшого аналізу та видачі необхідного результату. А самим маячкам не потрібен доступ до Інтернету, що значно спрощує їх структуру і вартість.

Така технологія обробки інформації дозволяє ефективно розв'язати зовсім нові задачі, зокрема задачу навігації [3]. На відміну від *GPS*, маячки в основному використовуються для *Indoor*-навігації, тобто для навігації в закритих приміщеннях великого обсягу: торгових залах, складах, лікарнях тощо. Завдяки своїх простоті можна використати велику кількість маячків і розташувати їх в різноманітних місцях [4] (рис. 1).


Рисунок 1 – приклади маячків від різних виробників

*GPS*-навігація та *Indoor*-навігація взаємно доповнюють одна одну і можуть використовуватись спільно. Варто відзначити, що математичні основи просторової навігації однакові в різних фізичних системах: є сукупність базових точок з відомими координатами і необхідно визначити координату однієї додаткової точки. В обох системах можна використовувати метод тріангуляції (вимірювати кути прикутників) та метод трилатерації (вимірювати сторони трикутників).

Обчислення відстані в *Indoor*-навігації виконується за декілька етапів [5]. Спочатку смартфон отримує індикатор потужності прийнятого сигналу (*Received Signal Strength Indicator – RSSI*) і порівнює його з еталоном (рівнем сигналу, який був виміряний на відстані 1 метра від передавача). На другому етапі вибираються три маячки з кращими середніми значеннями *RSSI*, які будуть виконувати роль трьох базових точок. Далі методом трилатерації по трьом базовим точкам будуються трикутники в тривимірному просторі для обчислення координат спостерігача.

Для уточнення результатів необхідна подальша математична обробка даних, наприклад, за допомогою фільтра Калмана.

## Організація захисту даних в Physical Web

Важливим складовою при роботі з інформацією в Інтернеті є її захист. Під цим розуміють два типи захисту: а) забезпечення секретності даних,що передаються; б) захист даних від спотворення внаслідок впливу навколишнього середовища.

Перший тип захисту – криптозахист на основі еліптичних кривих – використовується в маячках *Eddystone*, оскільки маячки в цьому форматі передають важливий контент (посилання на сайти та ін.).

Маячки *iBeacon* та *AltBeacon* використовуються лише для задач навігації, тому немає потреби в шифруванні їх повідомлень. Основною проблемою в цих задачах є забезпечення безпомилкової передачі ідентифікаційних даних маячка та значення *RSSI*. А на коректність передачі даних впливають багато факторів: структура антени маячків, рівень шумів, наявність різноманітних перешкод на шляху сигналів [3]. Вирішити цю проблему можна за допомогою завадостійкого кодування [6].

Розглянемо детальніше формати повідомлень від маячків *iBeacon* та *AltBeacon*, які містять поля ідентифікації маячка, поле *RSSI* та поле CRC (рис. 2). Перед кожною передачею повідомлення маячок-передавач формує для всіх інформаційних полів контрольну суму CRC. Після прийому повідомлення приймач (смартфон) знову обчислює контрольну суму і порівнює її із переданим значенням CRC.

| **поля ідентифікації** | **RSSI** | **CRC** |
|---|---|---|

Рисунок 2 – узагальнений формат маячків *iBeacon* та *AltBeacon*

При такому способі контролю передавання даних можна встановити факт наявності помилки і при додатковій обробці виправити лише один помилковий біт. Повторити передачу тих же даних неможливо, тому, що дані постійно змінюються. Збільшити

кількість виправлених помилок можуть більш потужні завадостійкі коди (наприклад, коди Ріда-Соломона), однак вони потребують складних обчислень та збільшення полів в форматах повідомлень.

І все ж ця проблема ефективно вирішується з тим же CRC-контролем і в межах стандартизованих форматів повідомлень. Для цього достатньо використати ітеративне декодування об'єднаних циклічних кодів [7]. Такими об'єднаними циклічними кодами можуть бути дві інтерпретації CRC-контролю [8]:

– Cyclic Redundancy Code, тобто CRC як циклічний надлишковий код,
– Cyclic Redundancy Check, тобто CRC як контрольна сума**.**

Оскільки в форматах маячків *iBeacon* та *AltBeacon* для поля CRC виділили лише три байти, тому в цьому полі повинні поміститись контрольне слово першого циклічного коду і контрольна сума другого циклічного коду. Розділимо поле CRC порівну і виберемо 12-розрядні породжувальні поліноми $g_1(x)$ та $g_2(x)$ для зазначених циклічних $(n,k)$-кодів. Нагадаємо, що ці поліноми степені $n-k=12$ повинні бути примітивними та різними, наприклад:

$$g_1(x)=1+x+x^2+x^5+x^6+x^9+x^{12},$$
$$g_2(x)=1+x^4+x^5+x^{10}+x^{12}.$$

Як було доведено в [7] такі поліноми дозволяють при ітеративному декодуванні з ймовірністю $p_m=1-2^{-12}$ виправити до 12 помилкових розрядів в повідомленнях від маячків.

## Висновки

Для забезпечення точності задач навігації в технології Physical Web ключову роль має безпомилковість передачі повідомлень від маячків**.** Розробники стандартів *iBeacon* та *AltBeacon* передбачили лише дуже простий метод завадостійкого контролю. Запропонований метод дозволяє при незначному збільшенні тривалості декодування збільшити коректувальну здатність завадостійкого коду в 12 разів.

## Список використаних джерел (References):

1.F. Hussain, "Internet of Things. Building Blocks and Business Models". – Springer, 2017. – 73 p.

2. M. Usama bin Aftab, "Building Bluetooth Low Energy Systems," Packt Publishing, Birmingham, UK, April 2017.

3. М. С. Васильева, А.В. Меженин Имитационная модель сигналов Beacon в среде Unity3D. – Научный альманах. – 2016. – N 12-2(26). – с.30-33.

4. https://www.amazon.com/iBeacon-Bluetooth-Energy-Proximity-Device/dp/B00JEGXITG.

5. P. Dickinson, G. Cielniak, O. Szymanezyk and M. Mannion, "Indoor Positioning of Shoppers Using a Network of Bluetooth Low Energy," Indoor Positioning and Indoor Navigation (IPIN), 2016 International Conference on, Alcala de Henares, Spain, Oct. 4-7.

6. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

7. Semerenko, V.P. Iterative hard-decision decoding of combined cyclic codes, Eastern-European Journal of Enterprise Technologies. 2018. Vol. 1, issue 9 (91). P. 61–72.

8. Семеренко, В. П. Теория и практика CRC кодов: новые результаты на основе автоматных моделей / В. П. Семеренко // Східно-Європейський журнал передових технологій. – 2015. – Т. 4, № 9 (76). – С. 38–48.