

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

МЕЛЬНИЧУК РОМАН СЕРГІЙОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
прикладної математики та
кібербезпеки,
д – р філософії з математики,
_____ А.В.Луценко
«__» _____ 20__ р.

**ЗАХИСТ NFC ПРИСТРОЇВ ВІД ПІДСЛУХОВУВАННЯ НА ЧАСТОТІ
ТРЕТЬОЇ ГАРМОНІКИ**

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:

Чернов Д. В., канд. техн. наук,
доцент, старш. викладач кафедри
прикладної математики та кібербезпеки

Оцінка: ____ / ____ / ____

(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____

(підпис)

Вінниця - 2024

АНОТАЦІЯ

Мельничук Р.С. Захист NFC пристроїв від підслуховування на частоті третьої гармоніки. Спеціальність 125 Кібербезпека. Донецький національний університет імені Василя Стуса. Вінниця, 2024.

У кваліфікаційній проблемі проаналізовано принцип підслуховування зв'язку NFC пристроїв на частоті третьої гармоніки. За результатом дослідження було розроблено ретранслятор, що гасить сигнал на частоті третьої гармоніки.

Ключові слова: третя гармоніка, підслуховування, NFC, ретранслятор, індуктивність.

57 с., 36 рис., 24 джерела

Melnychuk R.S. Protection of NFC devices from eavesdropping at the frequency of the third harmonic. Specialty 125 Cyber security. Donetsk National University named after Vasyl Stus. Vinnytsia, 2024.

In the qualification problem, the principle of eavesdropping on the communication of NFC devices at the frequency of the third harmonic is analyzed. As a result of the research, a repeater was developed that extinguishes the signal at the frequency of the third harmonic.

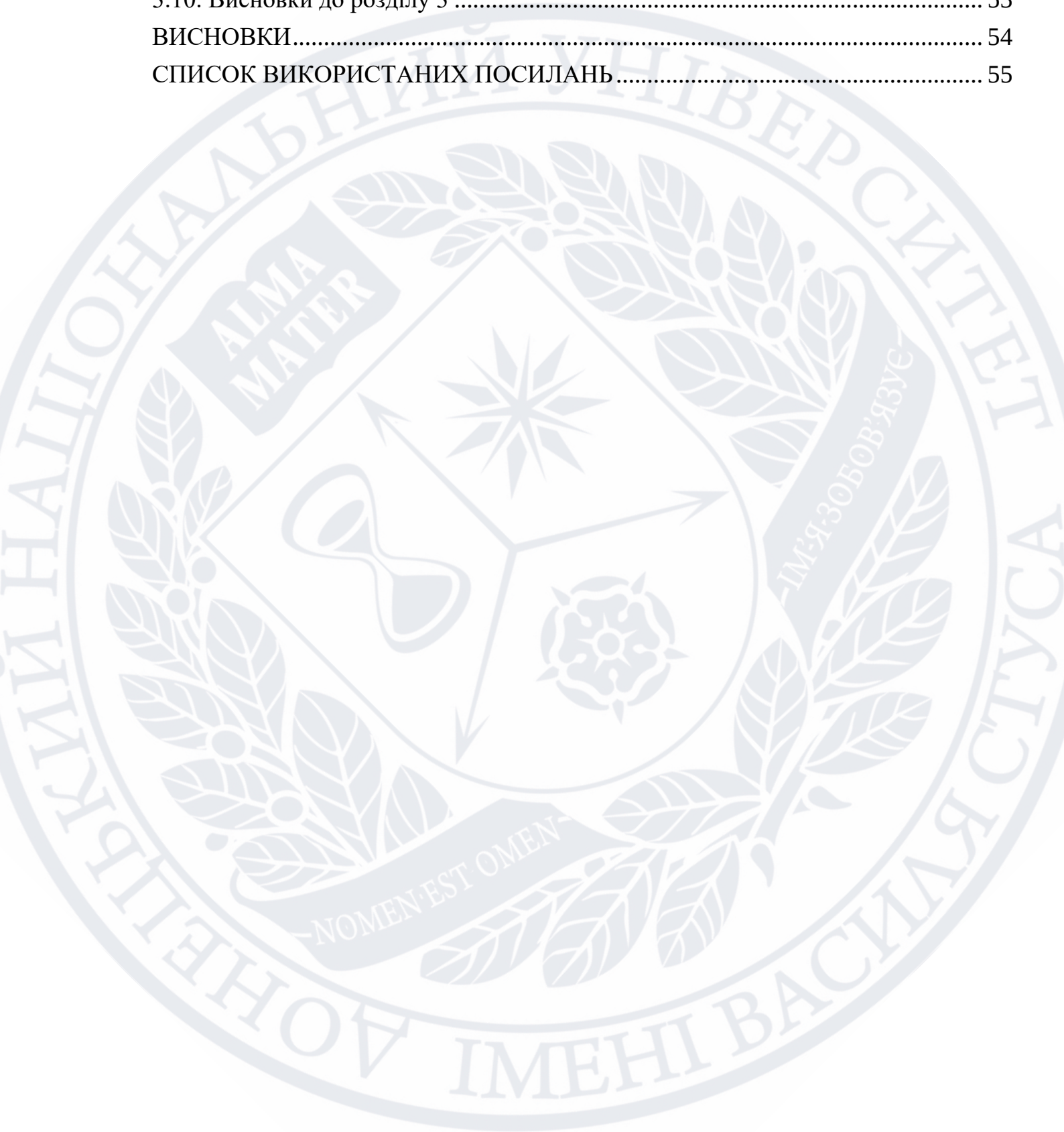
Keywords: third harmonic, eavesdropping, NFC, repeater, inductance.

57 pp., 36 figures, 24 sources

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. ТЕХНОЛОГІЇ NFC	6
1.1. Основні поняття	6
1.2. Обмін даними	7
1.3. Типи NFC-міток.....	8
1.4. Поширеність NFC-пристроїв	9
1.5. Принцип роботи NFC зв'язку	13
1.6. Архітектура NFC	14
1.7. Оперативні режими NFC	15
1.8. Режими комунікації NFC.....	17
1.9. Аналіз існуючих атак на NFC зв'язок	18
1.10. Аналіз способів протидії атакам на NFC зв'язок	20
1.11. Висновки до розділу 1	22
РОЗДІЛ 2. ПІДСЛУХОВУВАННЯ NFC-ПРИСТРОЇВ З ВИКОРИСТАННЯМ ТРЕТЬОЇ ГАРМОНІКИ. ПРОЄКТУВАННЯ РЕТРАНСЛЯТОРА.....	23
2.1. Принцип підслуховування	23
2.2. Аналіз способів протидії підслуховуванню на частоті третьої гармоніки ..	25
2.3. Репітер з функцією захисту від випромінювання третьої гармоніки	28
2.4. Висновки до розділу 2	30
РОЗДІЛ 3. РОЗРОБКА РЕТРАНСЛЯТОРА ДЛЯ ПРИДУШЕННЯ ЧАСТОТИ ТРЕТЬОЇ ГАРМОНІКИ	31
3.1. Створення резонансних контурів для прийому та передачі сигналу	31
3.2. Налаштування резонансних контурів для прийому та передачі на частоту NFC	33
3.3. Створення та налаштування фільтра на третю гармоніку	36
3.4. Вимірювання коефіцієнту передачі ретранслятора.....	37
3.5. Створення та тестування шунтувального контуру	38
3.6. Тестування ретранслятора на збільшеній відстані передачі	42
3.7. Тестування ретранслятора зі збільшеним екраном	45
3.8. Дослідження потужності передачі сигналу елементами ретраслятора	50
3.9. Дослідження потужності передачі сигналу ретранслятором	52

3.10. Висновки до розділу 3	53
ВИСНОВКИ.....	54
СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ.....	55



ВСТУП

Актуальність теми дослідження. Інформаційні технології це універсальний інструмент, який допомагає людству вирішувати все ширше коло проблем в усіх сферах життя. Все частіше різні технологічні області пересікаються між собою для створення різноманітних рішень тих чи інших завдань.

Широкого застосування також набула й технологія NFC з сімейства RFID яка є розвитком стандарту ISO 14443, яка дозволяє обмінюватися інформацією за принципом дотику, завдяки чому є надзвичайно зручним та практичним способом для передачі даних в найрізноманітніших галузях – від біомедицини та зарядки електромобілів, до ігрових автоматів та банківських операцій. Хоча NFC зв'язок є певною мірою захищеним завдяки малій дистанції взаємодії між зчитувачем та пасивною міткою, зазвичай до 4-10 см, існує можливість появи третьої гармоніки, при яких сигнал обміну даними між NFC-пристроями можна перехопити на більшій відстані завдяки використанню пристроїв зі спеціально налаштованими антенами правильної геометричної форми.

Завдяки відсутності універсального рішення для блокування третьої гармоніки для всіх NFC-пристроїв часто такі пристрої просто не мають жодного вбудованого захисту проти її появи, оскільки це може серйозно ускладнити еквівалентну схему пристрою. Ця невирішена проблема може бути фундаментальною причиною витоку конфіденційної інформації при використанні NFC-зв'язку для транзакцій.

Для запобігання загрозам для безпеки розглядається можливість створення ретранслятора NFC-зв'язку, який буде здатний передавати сигнал між двома пристроями та знижувати випромінювання третьої гармоніки до рівня, при якому було б неможливо перехопити сигнал з далекої відстані.

Мета – запобігання скімінгу в NFC системах

Об'єкт дослідження – процес розповсюдження електромагнітного поля у вільному середовищі

Предмет дослідження – спектр сигналу NFC

Практичне значення дослідження – запобігання витоку даних у системі NFC, що впливає на підвищення безпеки

РОЗДІЛ 1. ТЕХНОЛОГІЇ NFC

1.1. Основні поняття

NFC – це двонапрямлена технологія бездротового високочастотного зв'язку малого радіусу дії «в один дотик» [1] в діапазоні з'єднань від 4 до 10 сантиметрів, для використання якої необхідно щонайменше два пристрої з підтримкою даної технології. Тим часом NFC Forum вивчає діапазони, які в чотири-шість разів перевищують поточну робочу відстань [2].

RFID - це технологія, яка використовує радіохвилі для зчитування і передачі даних між так званими RFID-мітками або транспондерами та RFID-читачами. NFC є підвидом RFID зв'язку.

Транспондер в системі RFID, який частіше називається RFID-міткою або просто міткою, це пристрій, що містить інформацію, що зберігається і може передавати її через радіочастотні хвилі. Кожна мітка складається з антени для прийому і передачі сигналів та мікросхеми, що зберігає унікальний ідентифікатор і, можливо, іншу інформацію. Мітки бувають пасивні, які отримують енергію від читача і працюють тільки при його наявності, та активні, які мають власне джерело живлення, дозволяючи відправляти сигнали на більші відстані.

RFID-зчитувач - це пристрій, що використовується для зчитування (та іноді запису) інформації, збереженої на RFID-мітці. Читач генерує радіочастотний сигнал, який активізує мітку, дозволяючи їй передати збережену на ній інформацію назад до читача. Читачі можуть бути стаціонарними, призначеними для встановлення в певному місці (наприклад, на вході в будівлю для контролю доступу), або переносними, що дозволяє користувачеві сканувати мітки в різних місцях.

1.2. Обмін даними

Для обміну інформацією між мобільним телефоном NFC і NFC-мітками використовується формат обміну даними NFC (NDEF), який є стандартом специфікації формату даних, визначеним NFC Forum [3].

NDEF - це двійкове повідомлення, яке включає в себе від одного до кількох записів, кожен з яких складається з корисного навантаження до $2^{32} - 1$ октет. Для підтримки більшого корисного навантаження записи зазвичай об'єднуються в ланцюжок. Формат імені типу (TNF) є найважливішим полем запису NDEF та складається з 3-ох бітових даних. TNF описує тип запису, а також визначає структуру та зміст запису.

Існує кілька відомих типів записів NDEF, серед них:

- Простий текст - містять будь-який текстовий рядок, а також метадані про мову та спосіб кодування.
- URI - містять мережеві адреси. Цільовий пристрій, що отримує запис URI, передасть цей запис програмі, яка може його відобразити, наприклад веб-браузеру.
- Smart Poster - містять дані, які можна прикріпити до розумного плаката аби в подальшому їх зчитувати. Це можуть бути URI, так і звичайні текстові записи. Залежно від вмісту повідомлення цільовий пристрій, який отримує запис Smart Poster, може відкрити браузер, програму для SMS або електронної пошти тощо.
- Сигнатури - забезпечують спосіб надання надійної інформації про походження даних, що містяться в записі NDEF [4].

1.3. Типи NFC-міток

На форумі NFC визначено чотири типи тегів, усі вони базуються на описаних раніше протоколах керування RFID. Є п'ятий, який сумісний, але не є частиною специфікації NFC. Типи 1, 2 і 4 базуються на ISO 14443A, а тип 3 базується на ISO-18092. Детальні характеристики наведено нижче [4].

Технічні характеристики типу 1:

- На основі специфікації ISO-14443A.
- Може бути тільки для читання або з можливістю читання/запису.
- Пам'ять від 96 байт до 2 кілобайт.
- Швидкість зв'язку 106Kb.
- Немає захисту від колізії даних.

Прикладами цього типу є наступні екземпляри: Innovision Topaz, Broadcom BCM20203 .

Технічні характеристики типу 2:

- Подібний до типу 1; мітки базуються на специфікації NXP/Philips Mifare Ultralight tag (ISO-14443A).
- Може бути тільки для читання або з можливістю читання/запису.
- Пам'ять від 96 байт до 2 кілобайт.
- Швидкість зв'язку 106Kb.
- Підтримка захисту від колізії даних.
- Прикладом цього типу є наступний екземпляр: NXP Mifare Ultralight .

Технічні характеристики типу 3:

- На основі тегів Sony FeliCa (ISO-18092 і JIS-X-6319-4), без підтримки шифрування й автентифікації, яку надає FeliCa.
- Налаштовано лише для читання або читання/запису.
- Змінна пам'ять, до 1 Мб на обмін.

- Дві швидкості зв'язку, 212 або 424 Кбіт/с.
- Підтримка захисту від колізії даних.

Прикладом цього типу є наступний екземпляр: Sony FeliCa .

Технічні характеристики типу 4:

- Подібно до тегів типу 1, теги типу 4 базуються на специфікації тегу NXP DESFire (ISO-14443A).
- Налаштовано на заводі лише для читання або читання/запису.
- 2, 4 або 8 Кб пам'яті.
- Змінна пам'ять, до 32 Кб на обмін.
- Три швидкості зв'язку: 106, 212 або 424 Кбіт/с.
- Підтримка захисту від колізії даних.

Прикладами цього типу є наступні екземпляри: NXP DESFire, SmartMX-JCOR.

Технічні характеристики типу 5:

- Мітка Mifare Classic (ISO-14443A)
- Варіанти пам'яті: 192, 768 або 3584 байт.
- Швидкість зв'язку 106Kbps
- Підтримка захисту від колізії даних.

Прикладами цього типу є наступні екземпляри: NXP Mifare Classic 1K, Mifare Classic 4K, Mifare Classic Mini.

1.4. Поширеність NFC-пристроїв

Дана технологія набула надзвичайної популярності та великого поширення завдяки своїй дешевизні, простоті та зручності використання, а також завдяки своїй універсальності та гнучкості. Пристрої NFC поділяються на активні та пасивні, кожен вид має власні особливості та області застосування.

Пасивні NFC пристрої не вимагають власного джерела живлення і активуються тільки під дією електромагнітного поля від активного NFC пристрою. Це робить їх надзвичайно економічними для виробництва та використання. Ось деякі їхні характеристики:

- Містять обмежену кількість пам'яті, яка може вміщувати від кількох байтів до 2 кілобайтів даних, достатньо для зберігання URL-адрес, контактної інформації або інших коротких даних.

- Через пасивний характер, діапазон дії цих міток обмежений кількома сантиметрами, що забезпечує більшу безпеку та зменшує ризик атак.

Пасивні пристрої застосовуються у:

- маркетингу та рекламі - використання у рекламних буклетах або на постерах для надання додаткової інформації, спеціальних пропозицій або для переходу на веб-сайт компанії.

- транспорті - картки або жетони для систем оплати проїзду, які спрощують процес валідації та знижують час очікування.

- охороні та безпеці - картки доступу для систем контролю доступу до будівель, офісів або приватних територій.

- здоров'ї та медицині - мітки, які можуть бути використані для швидкого доступу до медичних записів пацієнта або інструкцій до медичних препаратів.

- роздрібній торгівлі - інформаційні мітки на полицях, які можуть містити інформацію про товар, ціну або спеціальні пропозиції.

Активні NFC пристрої є більш складними й функціональними компонентами технології ближнього поля, що можуть ініціювати комунікацію, мають власне джерело живлення, а також є дорожчими у виробництві та

обслуговуванні ніж пасивні пристрої. Ось деякі їхні характеристики:

- Мають можливість обробки складніших команд та виконання більш різноманітних завдань у порівнянні з пасивними NFC пристроями.
- Мають більше простору для зберігання даних, що розширює можливості їх застосування.

Активні пристрої застосовуються у:

- Смартфонах - використовуються для мобільних платежів, швидкого обміну контактами, а також ініціації бездротових з'єднань, таких як Bluetooth або Wi-Fi.
- Платіжних терміналах - забезпечують здійснення безконтактних платежів у магазинах, кафе та інших торговельних точках.
- Системах контролю доступу - використовуються для управління доступом до обмежених або захищених приміщень.
- Управлінні транспортом - Застосовуються у системах оплати проїзду та контролю за використанням транспортних послуг.

1.4.1 Відмінності та переваги NFC у порівнянні з Wi-Fi/Bluetooth

1. Дальність зв'язку

- NFC - зв'язок обмежений кількома сантиметрами (зазвичай до 10 см), що забезпечує високий рівень безпеки та зменшує ризик небажаних або випадкових підключень.
- Bluetooth/Wi-Fi - мають значно більшу дальність зв'язку, досягаючи від декількох метрів до кількох сотень метрів, що підходить для загальних бездротових зв'язків та мережевих підключень.

2. Швидкість налаштування зв'язку

- NFC - дозволяє миттєво налаштувати зв'язок між двома пристроями, оскільки не потребує парування або складних налаштувань. Це ідеально підходить для швидких платежів та ідентифікації.

- Bluetooth/Wi-Fi - вимагають більше часу для налаштування та парування, що може включати введення паролів або вибір зі списку доступних пристроїв.

3. Споживання енергії

- NFC - дуже енергоефективний, особливо в пасивному режимі, де пасивні пристрої не потребують власного живлення.

- Bluetooth/Wi-Fi - хоча сучасні версії Bluetooth, такі як Bluetooth Low Energy, теж ефективні з точки зору енергії, Wi-Fi зазвичай споживає більше енергії, особливо при передачі даних на великі відстані.

4. Складність інфраструктури

- NFC - вимагає мінімальної інфраструктури та простий у використанні, що робить його вигідним для простих аплікацій, таких як мітки доступу або електронні валети.

- Bluetooth/Wi-Fi - часто вимагають більш складної інфраструктури, включно з роутерами, серверами та іншим обладнанням, що підходить для створення стабільних та багатофункціональних мереж.

5. Безпека

- NFC - високий рівень безпеки за рахунок обмеженої дальності та простоти установки з'єднань. Це ускладнює перехоплення сигналу сторонніми особами.

- Bluetooth/Wi-Fi - хоча обидва стандарти мають засоби захисту, такі як шифрування та аутентифікація, вони більш схильні до атак ззовні через більшу дальність дії.

Ці особливості роблять NFC особливо привабливим для сценаріїв, які вимагають швидкості, безпеки та простоти, наприклад, в платіжних системах і системах швидкої ідентифікації. Його обмеження за дальністю також служить додатковим захистом, що робить NFC ідеальним для застосувань, де необхідна висока конфіденційність.

1.5. Принцип роботи NFC зв'язку

NFC використовує електромагнітну індукцію між двома рамковими антенами. Він працює в глобально доступному неліцензованому діапазоні промислових, наукових і медичних (ISM) радіочастот 13,56 МГц на повітряному інтерфейсі ISO/IEC 18000-3 зі швидкістю від 106 до 424 кбіт/с. Зв'язок у системах NFC заснований на індуктивному зв'язку між зчитувачем і антенами мітки. Антена приймача підключена до внутрішнього випрямляча міток, який отримує енергію від радіочастотного поля, яке використовується для живлення електроніки міток. Внутрішня логіка демодулює повідомлення амплітудної маніпуляції (ASK) від зчитувача. Транспондер мітки (який вважається пасивним) реагує, використовуючи техніку модуляції пасивного навантаження, змінюючи імпеданс антени мітки [5, 6]. Спектр модуляції пасивного навантаження складається з радіочастотної несучої, двох бічних смуг (12,712 МГц і 14,408 МГц) і модульованих бічних смуг цих двох сигналів піднесучої. Усі передані дані передаються у двох бічних діапазонах. Таким чином, радіочастотна несуча частота 13,56 МГц не повинна передаватися транспондером. Команди від зчитувача передаються в бічних смугах несучої, а модуляція навантаження переноситься в бічних смугах двох піднесучих, показаних синіми трикутниками [7].

1.6. Архітектура NFC

Щоб глибоко зрозуміти NFC, корисно мати уявну модель архітектури. Необхідно розглянути кілька рівнів. Найнижчий рівень — це фізичний рівень, процесор і радіостанції, які здійснюють зв'язок. Посередині знаходяться рівні пакетування та транспортування даних, потім рівні формату даних і, нарешті, код програми. На рис.1.1 показано різні рівні стеку NFC [4].

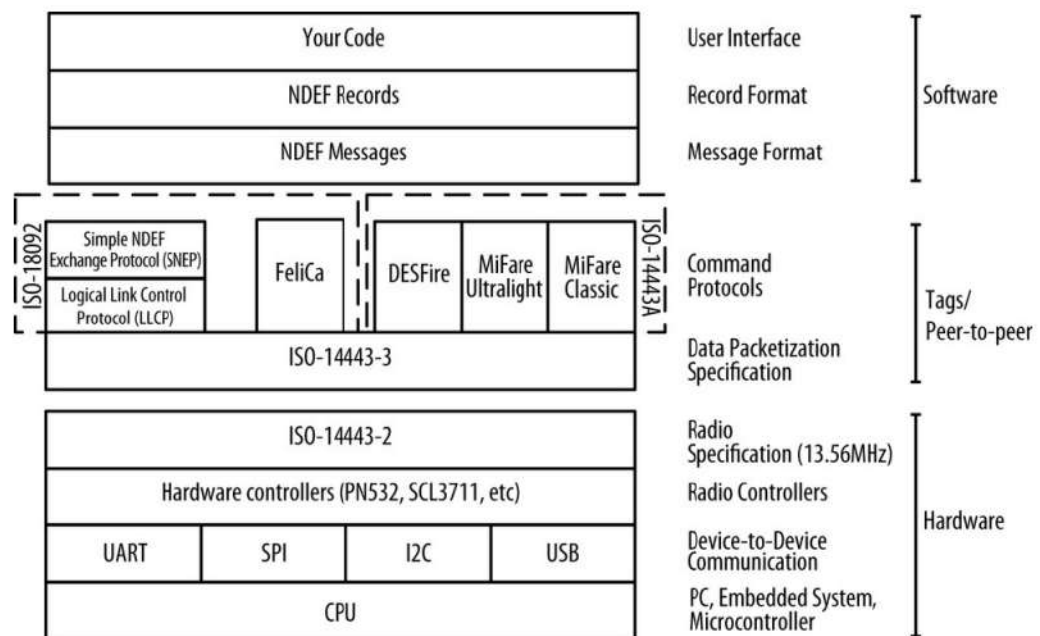


Рисунок 1.1 – Архітектура NFC [4]

На фізичному рівні NFC працює на основі специфікації радіочастотної ідентифікації ISO-14443-2, яка описує малопотужні радіостанції, що працюють на частоті 13,56 МГц. Далі йде рівень, який описує кадрівання байтів даних, надісланих по радіо, ISO-14443-3. Будь-які радіоприймачі є окремими апаратними компонентами, всередині телефону чи планшета, або приєднаними до мікроконтролера чи персонального комп'ютера. Вони спілкуються з головним процесором пристрою за допомогою одного або кількох стандартних послідовних протоколів між пристроями: універсального асинхронного

прийому-передачі (UART), послідовного периферійного інтерфейсу (SPI), зв'язку між інтегрованими схемами (I2C) або універсальної послідовної шини (USB). Вище наведено кілька протоколів команд RFID, заснованих на двох специфікаціях. Оригінальна специфікація керування RFID, на основі якої побудовано зчитування та запис тегів NFC, — ISO-14443A. Протоколи Philips/NXP Semiconductors Mifare Classic і Mifare Ultralight і NXP DESFire сумісні з ISO-14443A. Одноранговий обмін NFC побудований на основі протоколу керування ISO-18092. RFID-карти та мітки Sony FeliCa, здебільшого доступні в Японії, також базуються на цьому стандарті [4].

1.7. Оперативні режими NFC

Пристрої NFC можуть оперувати в одному з трьох режимів роботи: режим читання/запису, одноранговий режим або режим емуляції картки [8].

- **Режим читання/запису.**

Пристрій має мати можливість читати та записувати різні типи тегів NFC у режимі читання/запису. Таким чином один NFC-смартфон може обмінюватися даними з одним NFC-тегом. Більшість пристроїв NFC діють як зчитувачі та працюють в активному режимі для зчитування вмісту тегів, таких як безконтактні смарт-картки та теги RFID, у режимі зчитування/запису. Гаджет має розпізнавати відповідний тип тегу, щоб ефективно з ним взаємодіяти. Коли пристрій NFC стикається з двома тегами одночасно, він використовує алгоритм запобігання колізії даних, щоб вибрати один із них. У режимі запису пристрій NFC може записувати дані в теги, які мають програму запису, наприклад Tag-Writer [9]. Пристрої NFC сумісні з типами тегів схеми ISO/IEC 14443A/B або

Felica в режимі читання/запису [10]. Розумні плакати, дистанційні покупки та дистанційний маркетинг – лише деякі із застосувань режиму читання/запису [11] [12].

- Одноранговий режим.

Два пристрої з підтримкою NFC можуть обмінюватися даними в одноранговому режимі, наприклад з'єднувати пристрої Bluetooth або налаштовувати мережу WiFi, обмінюватися візитними картками чи надсилати текстові повідомлення. Для стандартизації цього режиму використовуються стандарти ISO/IEC, розділ 3. Зв'язок ближнього поля 82 18092 NFCIP-1. Під час зв'язку обидва пристрої знаходяться в активному режимі, а дані передаються через двонаправлений напівдуплексний канал, що означає, що другий пристрій може передавати дані лише тоді, коли перший пристрій NFC завершить передачу [10] [12].

- Режим емуляції карти.

У режимі емуляції картки пристрій NFC діє як стандартний безконтактний зовнішній зчитувач смарт-карт. Безконтактні платежі можна здійснювати за допомогою кредитних карток, дебетових карток, карток лояльності та інших пристроїв NFC, не вимагаючи жодних змін у існуючій інфраструктурі. Наприклад, мобільний пристрій із підтримкою NFC може містити численні програми для безконтактних смарт-карт на одному пристрої. Стандарти ISO/IEC 14443 типу A і B, а також стандарти Felica [10] підтримуються режимом емуляції карти [12].

1.8. Режими комунікації NFC

Пристрої NFC можуть спілкуватися в одному з двох режимів: активному або пасивному. Ці режими контролюють, як два пристрої з підтримкою NFC обмінюються даними один з одним. Диференціація режиму залежить від того, чи гаджет генерує власне радіочастотне поле чи використовує живлення від іншого пристрою. Ініціатор зв'язку — це пристрій, який його ініціює, а ціль — пристрій, який приймає сигнал від ініціатора.

- Активний режим

В активному режимі обидва пристрої NFC (ініціатор і ціль) використовують альтернативне радіочастотне поле для надсилання та отримання сигналів даних. Обидва NFC-пристрої мають автономне живлення, що означає, що їм не потрібно надсилати електроенергію до цілі, щоб завершити роботу, наприклад, смартфону або тегу з автономним живленням. В активному режимі дані передаються між двома пристроями за допомогою маніпуляції зі зсувом амплітуди (ASK), яка передбачає модулювання базового радіочастотного сигналу поля (13,56 МГц) даними з використанням методів кодування (кодування Міллера та Манчестера). Цей режим має вищу швидкість передачі даних і може використовуватися на більшій відстані[12].

- Пасивний режим

Ініціатор посилає радіочастотне поле для живлення цілі в пасивному режимі. Ціль, у свою чергу, використовує радіочастотне поле для передачі збережених даних назад за допомогою процесу, відомого як модуляція навантаження (манчестерське кодування) [13]. Це найбільш використовуваний режим NFC, оскільки для нього не потрібен акумулятор і він дешевший [12].

1.9. Аналіз існуючих атак на NFC зв'язок

Ретрансляційна атака

Ретрансляційна атака працює на принципі втручання в сеанс зв'язку між легітимним рідером та тегом таким чином, щоб у сторін обміну даними не виникало підозр присутності третього учасника. Через свій обмежений радіус дії пристрої безконтактного зв'язку використовують припущення, що інша сторона обміну даними знаходиться досить близько, якщо з нею встановлено зв'язок, а отже є легітимною. Для успішного проведення атаки зломисник використовує два пристрої-посередники, здатні між собою спілкуватися на дальній відстані та імітувати легальний пристрій, таким чином значно збільшуючи відстань передачі даних.



Рисунок 1.2 – Схема ретрансляційної атаки на NFC-платежі [14]

Наприклад, як зображено на рисунку 1.2, телефон 1 знаходиться поруч з картою NFC, а телефон 2 - близько до терміналу. Коли телефон 2 наближається

до терміналу, він імітує карту NFC, і термінал ініціалізує процес зв'язку. Щоразу, коли термінал надсилає команду на телефон 2 із запитанням про те, який це тип картки, телефон 2 надсилає ці дані через Wi-Fi на телефон 1, і цей телефон «задає» смарт-карті те саме запитання. Картка відповідає, і телефон 1 приймає цю інформацію і відправляє її назад на телефон 2, який відповідає на термінал [14].

Атака Man-in-the-Middle

Дана атака відрізняється від ретрансляційної тим, що на відміну від першої не просто передає дані між легальними пристроями без змін, а дозволяє перезаписувати інформацію, що переміщується у каналі зв'язку між пристроями. Для NFC-зв'язку з його малим радіусом дії вважається майже неможливою. Однак, у роботі [15] автор в дослідженні показує, що існує серйозна вразливість у EMV-протоколі, яка дозволяє зловмиснику використовувати дві картки під час проходження етапу автентифікації картки, де склонована зі справжньої картки зловмисна картка передає дані від легітимної картки, видаючи себе за неї. Банк не здатний виявити дану підміну, тому після підтвердження автентифікації картки на решті етапів проведення транзакції більше ніяк не перевіряє дану картку, тому зловмисник може розрахуватися за покупку з фальшивої картки.

Пошкодження переданих даних

Крім прослухоування даних, зловмисник може спробувати модифікувати дані, що передаються за допомогою NFC каналу. У найпростішому випадку атакуючий може спробувати перервати спілкування між пристроями, забивши канал випадковими даними, таким чином, цільовий пристрій не зможе зрозуміти дані, що надіслані іншим легітимним пристроєм Пошкодження даних

може бути досягнуто шляхом відсилання вірних частот в певний проміжок часу. Проміжок часу визначається з урахуванням використовуваної модуляції і схеми кодування. Дана атака не надто складна в реалізації, але не дозволяє атакуючому якимось маніпулювати переданими даними, таким чином дана атака є підвидом атаки відмови в обслуговуванні [16].

Вставка даних

Даний тип атаки має на увазі вставку свого повідомлення в NFC-канал передавання двох пристроїв. Як було зазначено раніше, NFC організовує передачу даних за принципом повідомлення-відповідь. У тому випадку, якщо пристрою, що відповідає, необхідний довгий проміжок часу щоб згенерувати відповідь, зломисник має можливість вставити в канал своє повідомлення, і воно буде сприйнято пристроєм, який ініціює спілкування як легітимна відповідь. Якщо для другого пристрою, що приймає участь в обміні інформації, необхідні тривалі розрахунки, то у атакуючого з'являється можливість послати відповідь швидше, ніж це зробить легітимний пристрій. Вставка даних буде успішною тільки в тому разі якщо передача даних зломисника почнеться строго раніше, ніж відповідь легітимного пристрою. Якщо обидва пристрої почнуть віщати одночасно, то їх радіочастоти перекриються і дані буде пошкоджено, що побічно але може рахуватися атакою пошкодження даних [16].

1.10. Аналіз способів протидії атакам на NFC зв'язок

Захист від ретрансляційних атак

Для захисту NFC пристроїв від даного типу атак існує декілька давно вивчених методів протидії. Найпростішим способом захисту платіжних карт від

цієї атаки може бути рішення носити декілька карток разом, таким чином спотворюючи можливість зв'язку для зловмисника. Інший підхід включає використання клітки Фарадея, або будь-якого іншого засобу, що дозволяє екранувати картку від небажаного стороннього впливу. У роботі [17] автор зосереджений на розробці протоколу дистанційного визначення відстані для RFID-тегів, який може захистити від ретрансляційних атак. Протокол використовує ультраширокопосмугове (UWB) імпульсне зв'язування та спрямований на реалізацію за допомогою простих, асинхронних, малопотужних пристроїв, що робить його особливо підходящим для застосування в пасивних та недорогих мітках. Основна ідея полягає в тому, щоб вимірювати часову затримку "туди і назад" радіосигналу, що дає можливість точно визначати верхню межу відстані між читачем та міткою. Важливим аспектом є те, що жодна інформація не може поширюватися швидше за світло, що дозволяє точно обмежувати відстань.

Захист від пошкодження даних

NFC-пристрої можуть протистояти даному типу атак шляхом перевірки РЧ поля під час передавання даних. Потужність, що витрачається для пошкодження даних, набагато більше потужності, використовуваної при штатній передачі даних. Таким чином, ці атаки легко виявляються [16].

Захист від вставки даних

Для даної атаки можливі три методи протидії. По-перше, пристрій, що дає відповідь повинен посилати відповідь без затримки. Таким чином, атакуючий не зможе послати своє повідомлення, так як основною умовою проведення даної атаки є довга генерація відповіді. Проте, даний метод не є вичерпним і не може бути застосований, якщо обчислення необхідні для роботи самої програми. По-друге, пристрій, що відповідає може прослуховувати канал під

час підготовки своєї відповіді. І, при наявності сторонніх повідомлень, припиняти спілкування. По-третє, рекомендується використовувати канал, захищений криптографією [16].

Захист від атаки Man-in-the-Middle

Як було зазначено раніше, реалізація атаки «людина посередині» практично неможлива при обміну інформацією за допомогою NFC. Проте за можливістю, рекомендується використовувати пристрої в конфігурації активний-пасивний, щоб в каналі завжди було згенеровано РЧ поле. Крім того пропонується використовувати методи вимірювання часових затримок між переданими даними.

1.11. Висновки до розділу 1

У цьому розділі розглянуто основні відомості про технологію NFC. Ця технологія стала популярною завдяки універсальності та зручності використання, а також відносно низькій вартості. Вона належить до сімейства RFID і забезпечує зв'язок на дуже малій відстані. Аналіз загроз показав, що NFC має значну перевагу в захищеності завдяки обмеженому діапазону роботи, але нові методи атак постійно розробляються, а старі вдосконалюються.

РОЗДІЛ 2. ПІДСЛУХОВУВАННЯ NFC-ПРИСТРОЇВ З ВИКОРИСТАННЯМ ТРЕТЬОЇ ГАРМОНІКИ. ПРОЄКТУВАННЯ РЕТРАНСЛЯТОРА

2.1. Принцип підслуховування

Зв'язок у близькому полі (NFC) є індуктивним зв'язком близько розташованих котушок індуктивності, пов'язаних спільним магнітним полем [18, 19]. Відповідно напруженість поля зменшується з відстанню за законом $1/r^3$, і на порівняно невеликих відстанях зв'язок стає неможливим, що є передумовою збереження конфіденційності транзакцій. Довжина електромагнітної хвилі на частоті 13,56 МГц складає 22,11 м, і елементи рідера не здатні скласти ефективну антену, але на частоті третьої гармоніки 40,68 МГц довжина хвилі у вільному просторі вже 7,37 м, тому можливе випромінювання цього сигналу [20] є доступним для підслуховування та скімінгу. На рисунку 2.1 зображено схему для пасивного та активного (скімінг) підслуховувань.

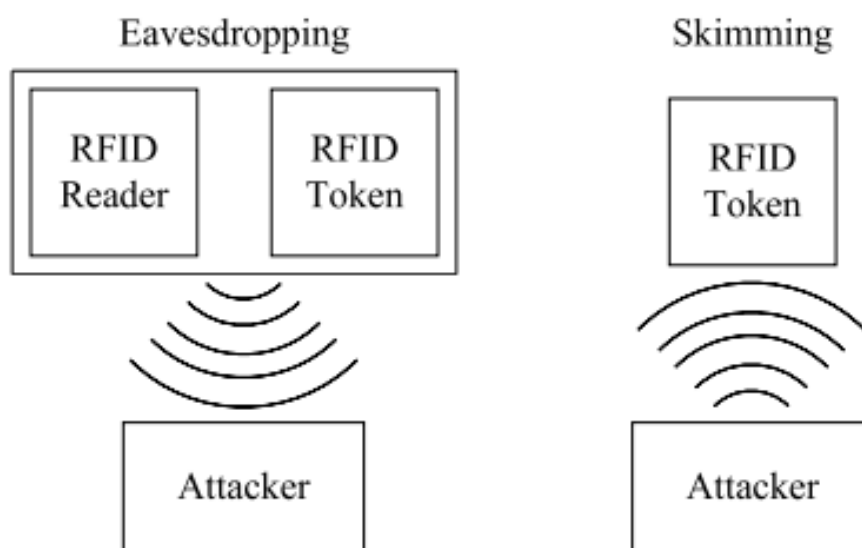


Рисунок 2.1 - Схема пасивного та активного підслуховування NFC зв'язку [21]

Для викрадення даних зловмисник може використовувати спеціальне обладнання, яке прослуховуватиме канал передачі даних. З метою вловити радіочастотний сигнал використовується антена для бездротової передачі даних. Якщо зловмисник працюватиме з укриття, то власник пристрою нічого не підозрюватиме, адже неможливо ніяк помітити таку атаку фізично, окрім як побачити людину, яка стоїть поруч з антеною. Відстань, на якій зловмисник зможе прослухати сигнал може варіюватися залежно від різноманітних параметрів та зазвичай не перевищує кількох метрів. Пасивний пристрій, що бере участь у довірєній передачі даних, не генерує власного радіочастотного поля і тому його буде прослухати значно важче, ніж активний пристрій.

Основним питанням є наскільки близько повинен знаходитися зловмисник, щоб зуміти перехопити радіочастотний сигнал, що буде придатним для подальшої роботи з ним. На жаль, однозначної відповіді на це питання не існує. Основною причиною є безліч факторів, що визначають цю відповідь:

- радіочастотні характеристики трансмітера (наприклад, геометрія антени, ефект екранування корпусу, оточення);
- радіочастотні характеристики антени атакуючого (наприклад, форма антени, можливість зміни положення у всіх трьох вимірах);
- якість приймача атакуючого;
- якість декодера атакуючого;
- локація в якій ведеться зняття сигналу (рівень радіошуму, бар'єри у вигляді стін);
- потужність з якою працює NFC пристрій

Теоретично прослуховування можливе в межах близько 1 метру для пасивного пристрою, наприклад, для банківської картки чи біометричного

пластикового паспорту, що містить конфіденційні дані в чіпові, вбудованому всередину. Для активного пристрою відстань прослуховування може сягати 10 метрів.

Варто зазначити, що підслуховування на відстані до 1 метру для пасивного пристрою стає можливим лише завдяки випромінюванню третьої гармоніки від цільового нього. Проблему може ускладнювати випромінювання третьої гармоніки провідниками, що приєднані до рідера [22].

Третя гармоніка – це гармоніка вищого порядку, побічний сигнал, що за своєю частотою тричі кратний основному сигналу величиною 13,56 МГц. Відповідно, частота третьої гармоніки дорівнює 40,68 МГц.

Шляхом вирішення проблеми може бути припинення генерації вищих гармонік у мітці NFC, але це ускладнить структуру мітки та потребує розробки нових стандартів зв'язку. Але можна спробувати зменшити рівень випромінювання третьої гармоніки у критичних застосуваннях, скориставшись репітером, який використовується для передачі сигналу NFC, тобто високочастотного індуктивного зв'язку, через металеві поверхні [23, 24] [22].

2.2. Аналіз способів протидії підслуховуванню на частоті третьої гармоніки

Загроза підслуховування сеансу бездротового зв'язку не є новою. Завдяки певній подібності до інших існуючих видів атак, що традиційно широко використовуються зловмисниками, є можливість використовувати вже давно відомі та добре відпрацьовані методи та засоби захисту для запобігання реалізації даної атаки, хоч і з певними обмеженнями.

Відеоспостереження

Встановлення відеокамер по периметру зони захисту дає можливість персоналу в постійному режимі спостерігати за діями користувачів та відслідковувати підозрілі дії. Таким чином можна зафіксувати момент, коли зловмисник викриє свої наміри, маніпулюючи в безпосередній близькості пристроєм, що не призначений для використання в даному місці. Оскільки такий пристрій зробити компактним та малопомітним може бути складним завданням для зловмисника, то ймовірно його буде легко побачити. В такій ситуації охорона об'єкту може вжити відповідних дій для запобігання зловмисним діям. Крім того відеоспостереження має перевагу в тому, що може записувати все, що відбувається. Навіть якщо персонал не побачив вчасно злочин, пізніше можна подивитися запис та встановити особу злочинця. Однак цей спосіб протидії малоефективний або недієвий у випадку наявності у камер сліпих зон або використання SDR-радіо, яке є більш компактним для прихованого підслуховування.

Шифрування

Шифрування даних, що передаються між транспондером та трансмітером є ефективним способом захисту від несанкціонованого доступу. Навіть якщо зловмисник шляхом підслуховування зможе перехопити дані, наприклад між банкоматом та платіжною картою, він не зможе їх прочитати. Сучасні платіжні картки мають вбудовані чіпи, які здатні підтримувати криптографічні операції з рівнем складності, достатнім для забезпечення надійного криптографічного перетворення даних, таких як PAN - номер картки та інших, необхідних для підтвердження транзакцій. Недолік цього способу полягає в тому, що не всі види NFC-пристроїв підтримують криптографічний захист даних, але при цьому можуть теж передавати конфіденційну чи секретну інформацію.

Автентифікація пристроїв

У випадку активного підслуховування (скімінгу) підслуховуючий пристрій надсилає сигнал на пасивний пристрій, аби отримати від нього відповідь, призначену лише для легітимних пристроїв. Для запобігання такому сценарію можливо використовувати протоколи автентифікації, завдяки яким пасивний тег визначатиме, чи легітимний пристрій ініціює з'єднання та відповідно до цього вирішуватиме чи надсилати відповідь. Однак цей спосіб також використовує криптографічні алгоритми, які не підтримуються всіма пристроями.

Генерація просторового зашумлення

В режимі пасивного підслуховування пристрій зломисника створює лише побічні електромагнітні випромінювання, які можуть розпізнаватися системою аналізу спектру частот для активації генератора просторового зашумлення в межах зони захисту в виявленому підозрілому діапазоні частот з метою завадити підслуховуванню. Реалізація даної системи захисту є складною та досить ненадійною. Підслуховуючий пристрій може генерувати побічні електромагнітні випромінювання широкого спектру, що перетинатимуться з випромінюванням звичайних електронних пристроїв, наприклад як смартфон, ноутбук, смарт-годинник тощо. Виокремити необхідний пристрій можна лише за відбитком його спектру випромінювання. Якщо цей відбиток зміниться, то зашумлення вже не працюватиме як слід. Крім того, зломисник легко може екранувати побічні випромінювання свого пристрою, таким чином унеможливаючи його виявлення системою захисту.

Придушення частоти для підслуховування

Використання клітки Фарадея чи іншого способу екранування NFC-пристроїв може бути дієвим способом для блокування спроб активного підслуховування пасивних тегів, коли вони не використовуються. При цьому коли пасивний тег використовується за призначенням, екранувати його випромінювання таким чином, щоб не порушити сеанс легітимного зв'язку та заблокувати витік сигналу може бути непростим завданням. Більш дієвим методом буде створити пристрій, що діятиме як ретранслятор та через екран передаватиме від трансміттера до транспондера і навпаки сигнал основної частоти, на якій відстань підслуховування є надто низькою для злоумисника, та придушуватиме сигнал на частоті третьої гармоніки, на яку налаштований пристрій злоумисника для підслуховування. Такий спосіб може стати універсальним захистом, оскільки підходить однаково як для пасивного, так і для активного підслуховування (скімінгу), захищатиме пасивні та активні NFC-пристрої однаково. Значною перевагою може бути відносно невисока вартість подібного рішення та відсутність необхідності підтримувати складну інфраструктуру в належному стані для надійного захисту.

2.3. Репітер з функцією захисту від випромінювання третьої гармоніки

Оскільки такий репітер повинен бути резонансною системою, пропонується використовувати цей принцип для захисту NFC від витіку третьої гармоніки. Розглянемо конструкцію репітера, який складається з двох котушок зв'язку з тегом (RFID пристроєм) та рідером, та двох котушок зв'язку скрізь металеву поверхню, в якій для цього розміщується феритовий магнітопровід, з двох сторін якого розташовується котушки. В [24] для цієї конструкції була складена еквівалентна електрична схема, яка в діапазоні

основної частоти вірно описувала імпедансні характеристики схеми репітера. Користуючись еквівалентною схемою репітера з цієї роботи були розраховані його передаточні характеристики в діапазоні до 50 МГц, які показали значне затухання сигналу третьої гармоніки. З іншого боку, в роботі [24] наведено експериментальні передаточні характеристики репітера до частоти 30 МГц, які свідчать про те, що після частоти 15 МГц починається збільшення коефіцієнту передачі пристрою, що може свідчити про підвищення ефективності передачі енергії через меншу котушку індуктивності та феритову вставку [22].

Для запобігання такого явища, спрощення конструкції репітера та посилення його здатності блокувати сигнал на частоті третьої гармоніки пропонується зробити гальванічний зв'язок між котушками репітера з обох боків і додати фільтр на основну частоту, який буде блокувати проходження сигналу на частоті третьої гармоніки. Еквівалентна схема такого варіанту показана на рисунку 2.2.

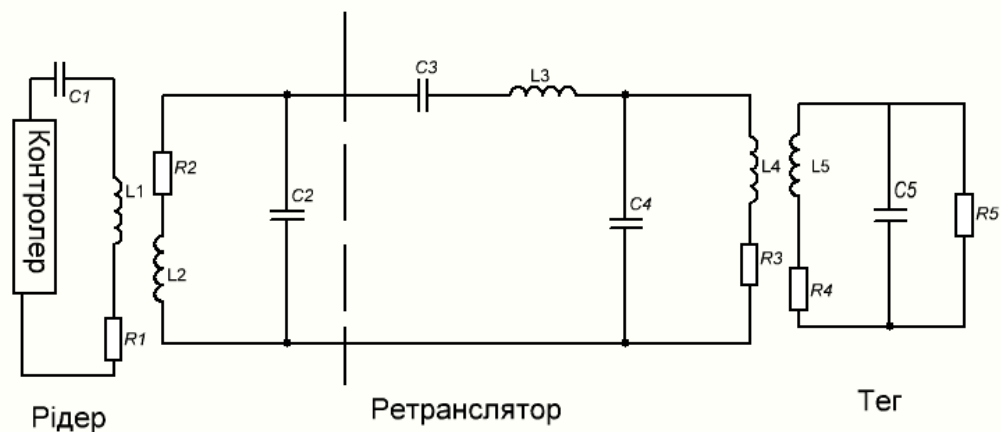


Рисунок 2.2 – Еквівалентна схема запропонованого пристрою

Розрахунок коефіцієнту передачі (рис. 2.3) показує, що така схема задовольняє вимогам до зменшення рівня третьої гармоніки як на рідері, так і

на зовнішній котушці репітера, що зменшить ймовірність підслуховування NFC-зв'язку (скімінгу) на частоті третьої гармоніки [22].

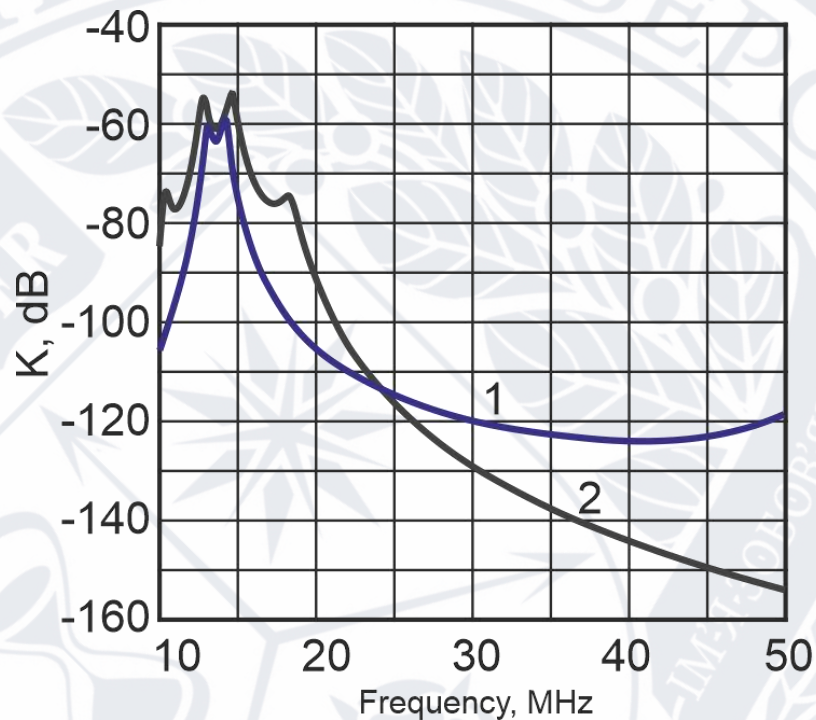


Рисунок 2.3 – Коефіцієнт передачі від тега до рідера, 1 – для схеми рис. 2, 2 – з роботи [5] [22].

2.4. Висновки до розділу 2

У другому розділі детально проаналізовано принцип підслуховування NFC на частоті третьої гармоніки. Точна відстань для скімінгу залишається невизначеною через фізичні фактори. Аналіз показав, що створення ретранслятора для блокування частоти третьої гармоніки є оптимальним рішенням з точки зору витрат та універсальності. На основі досліджень [23], [24] де досліджуються проблеми ефективної передачі сигналу було спроектовано дослідний варіант такого ретранслятора.

РОЗДІЛ 3. РОЗРОБКА РЕТРАНСЛЯТОРА ДЛЯ ПРИДУШЕННЯ ЧАСТОТИ ТРЕТЬОЇ ГАРМОНІКИ

3.1. Створення резонансних контурів для прийому та передачі сигналу

Два резонансні контури мають бути налаштовані на частоту 13,56 МГц. Було створено дві прямокутні котушки розмірами 80 на 50 мм. Намотано 10 витків дроту товщиною 0,1 мм з відстанню в 0,1 мм між ними, чого цілком достатньо в рамках експерименту. В якості підложки під котушки було обрано пластик, оскільки він має підходяще значення тангенціальних втрат та діелектричної проникності. Щоби проведення розрахунків ємності конденсаторів, було виміряно індуктивність котушок з допомогою вимірювача RLC E7-22.

Вимірювач підтримує вимірювання індуктивності на 2 частотах: 120 Гц та 1 КГц. Було обрано частоту 1 КГц, оскільки менша частота недостатня для вимірювання значень індуктивності таких котушок. Встановлено режим послідовного еквіваленту, оскільки втрати енергії в такої котушки невеликі. Обраний діапазон показує значення у мкГн. В результаті вимірювання отримана індуктивність першої котушки дорівнює 12,4 мкГн. Для другої котушки аналогічне вимірювання показує перше значення 11,2 мкГн.

Далі вираховуємо ємність двох конденсаторів. Для цього спочатку з формули резонансної частоти виводимо формулу для ємності:

$$f_0 = \frac{1}{2\pi\sqrt{LC}} \quad (3.1)$$

Де π – математична константа, відношення довжина кола до його радіусу;

f_0 – резонансна частота 13.56 МГц;

L – індуктивність котушки;

C – ємність конденсатора.

Спершу виражаємо $\sqrt{LC}$:

$$\sqrt{LC} = \frac{1}{2\pi f_0} \quad (3.2)$$

Підносимо обидві частини рівняння до квадрату:

$$LC = \left(\frac{1}{2\pi f_0}\right)^2 \quad (3.3)$$

Відокремлюємо C :

$$C = \frac{1}{(2\pi f_0)^2 L} \quad (3.4)$$

Підносимо до квадрату вираз у дужках в знаменнику та отримуємо необхідну формулу:

$$C = \frac{1}{4\pi^2 f_0^2 L} \quad (3.5)$$

Підставляємо значення індуктивності кожної котушки та резонансної частоти у формулу (3.4) для знаходження ємності обох конденсаторів:

$$C_1 = \frac{1}{4 \cdot \pi^2 \cdot 13,56 \text{ МГц}^2 \cdot 12,4 \text{ мкГн}} = 11.1 \text{ пФ} \quad (3.6)$$

$$C_2 = \frac{1}{4 \cdot \pi^2 \cdot 13,56 \text{ МГц}^2 \cdot 11,2 \text{ мкГн}} = 12,3 \text{ пФ} \quad (3.7)$$

Після цього відповідні котушки й конденсатори було послідовно з'єднано на пластиковій підложці.

3.2. Налаштування резонансних контурів для прийому та передачі на частоту NFC

Щоби коливальні контури працювали на необхідній резонансній частоті максимально ефективно, їх було налаштовано на дану частоту за допомогою векторного аналізатора, аби перевірити правильність наших розрахунків. Встановлені початкове та граничне значення діапазону частот на 5 МГц та 20 МГц відповідно. Для максимально детального відображення кривих на графіку встановлено 2501 точку для відображення. Додано маркер на частоту 13.56 МГц. Відкалібровано три точки: Open та Short та Load, що відповідають на діаграмі Сміта нескінченності, нулеві та одиниці. Далі під'єднано до вихідного порту аналізатора виводи конденсатора та котушки. За допомогою викрутки регулюємо ємність конденсаторів таким чином, щоб отримати правильні значення налаштування.

В першому випадку отримали майже ідеальний результат, як видно на рисунку 3.1, фаза коефіцієнту відбиття для даного контуру становить 0,1 градуса.

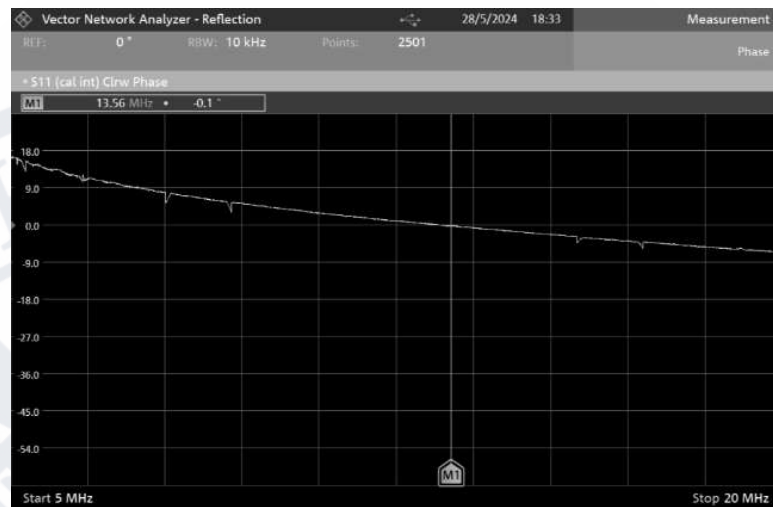


Рисунок 3.1 – Фаза коефіцієнту відбиття для першого коливального контуру на частоті 13,56 МГц

Для перевірки, чи входить контур в резонанс на даній частоті, перевірено значення на діаграмі Сміта, на рисунку 3.2 видно, що маркер частоти знаходиться посередині між індуктивним та ємнісним опорами, що вказує на те, що вони взаємокомпенсують одне одного та контур входить в резонанс.

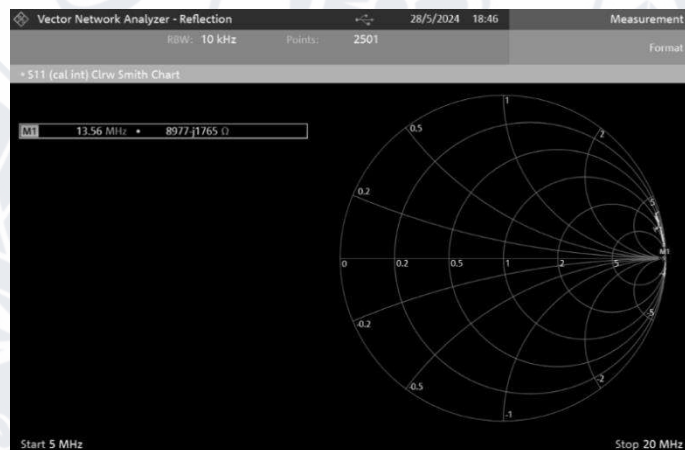


Рисунок 3.2 – Показник резонансу для першого контуру на діаграмі Сміта

Проведено аналогічні налаштування для другого контуру до якого було додано заземлення. На рисунку 3.3 зображено значення фази коефіцієнту відбиття - 3,4 градуси, що вказує на незначне відхилення, близьке до резонансу.



Рисунок 3.3 – Фаза коефіцієнту відбиття для другого коливального контуру на частоті 13,56 МГц

На рисунку 3.4 зображено результат перевірки за діаграмою Сміта чи знаходиться у резонансі необхідна частота, в порівнянні з першим контуром також є невелике, але прийнятне відхилення.

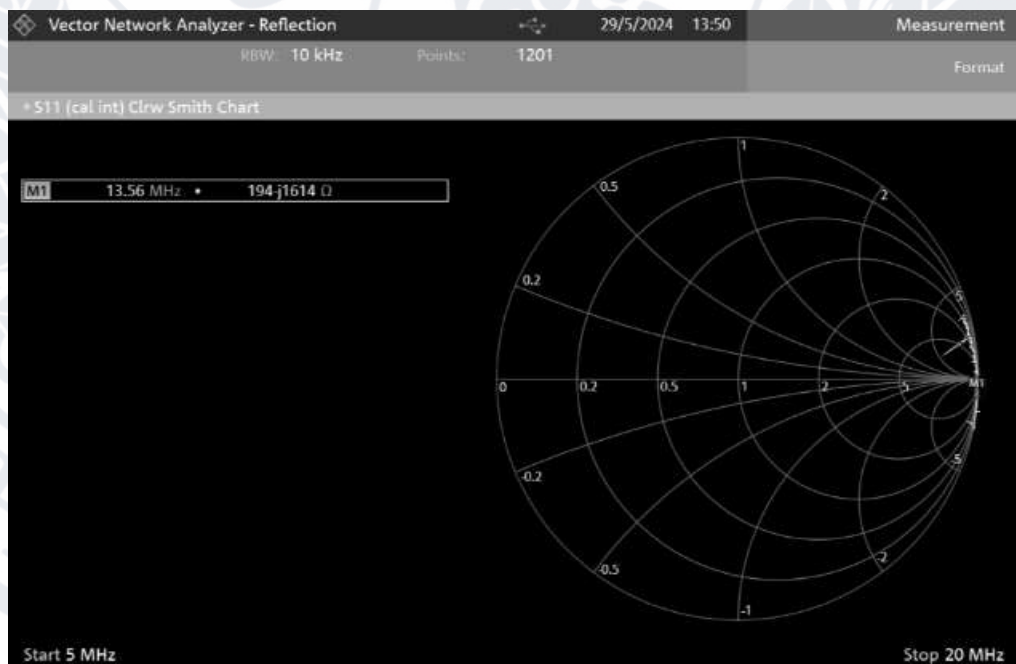


Рисунок 3.4 – Показник резонансу для другого контуру на діаграмі Сміта

3.3. Створення та налаштування фільтра на третю гармоніку

Для того, щоб сигнал проходив через екран, встановлений між контурами прийому та передачі було розраховано фільтр на третю гармоніку, який послідовно з'єднує обидва контури по різні сторони екрани через невеликий отвір для провідника. Для цього було використано готову котушку з індуктивністю 4.7 мкГн. Далі було проведено розрахунок значення для ємності, необхідної для конденсатора, що разом з обраною котушкою складатиме контур, налаштований на резонансну частоту 13,56 МГц. Розрахунок проведено за формулою (3.4):

$$C_3 = \frac{1}{4 \cdot \pi^2 \cdot 13,56 \text{ МГц}^2 \cdot 4,7 \text{ мкГн}} = 29.31 \text{ пФ} \quad (3.8)$$

Було обрано конденсатор, який має значення ємності, близьке до отриманого значення з розрахунку. Далі було налаштовано фільтр на частоту першої гармоніки. Для цього ми послідовно з'єднали за допомогою пайки котушку та конденсатор, та під'єднали до векторного аналізатора. Ємність під'єданого конденсатора відрегульовано діелектричною викруткою таким чином, щоб маркер обраної частоти на діаграмі Сміта опинився в позиції резонансу. На рисунку 3.5 зображено результат налаштування фільтру, як видно, значення досить точне, отже, фільтр налаштовано правильно.

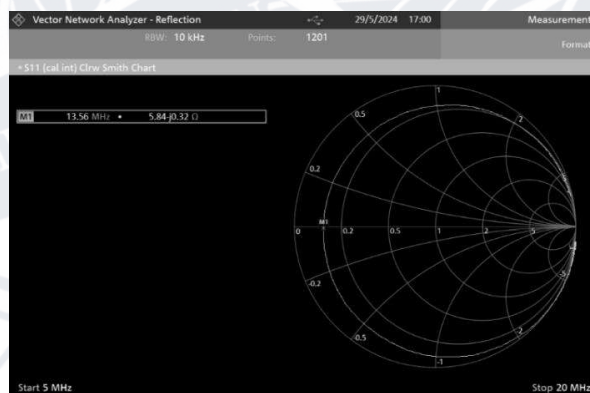


Рисунок 3.5 – Показник резонансу для фільтру на 3 гармоніку на діаграмі Сміта

3.4. Вимірювання коефіцієнту передачі ретранслятора

Щоб дізнатися, наскільки добре ретранслятор передаватиме сигнал, за допомогою векторного аналізатора було виміряно передаточну функцію для тестової установки. Для цього контури прийому та передачі були розміщені по різні боки екрану, таким чином, щоб їх позиції були максимально узгоджені. Далі було приєднано фільтр на третю гармоніку. Ретранслятор було розміщено його між двома котушками, приєднаними за допомогою коаксіального кабелю до векторного аналізатора, одна з яких випромінює, а інша приймає сигнал. Для коректного відображення результату спочатку вимірювальний пристрій було відкалібровано на модулі передачі S21 в діапазоні від 10 до 50 МГц. Котушки для випромінювання та прийому сигналу обрано зі схожою індуктивністю. Далі їх було під'єднано до векторного аналізатора на вхідний та вихідний порти, додатково заземливши їх. Ретранслятор було розміщено між котушками на відстані 3 см від кожної. На рисунку 3.6 показано експериментальне розміщення ретранслятора між котушками.

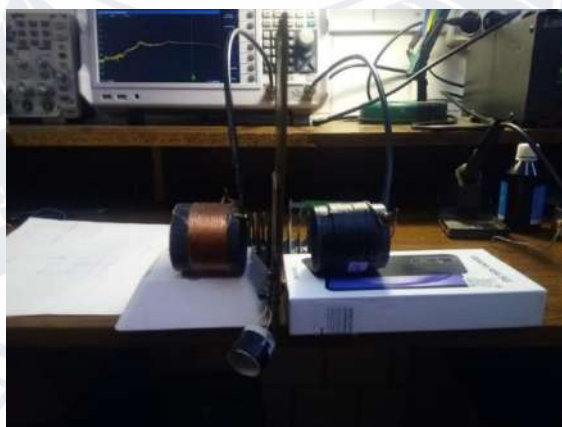


Рисунок 3.6 – Експериментальна установка для вимірювання передаточної функції ретранслятора

Вимірювання передаточної функції частоти третьої гармоніки показало рівень сигналу -10.6 dB, як вказано на рисунку 3.7. Таким чином, видно, що рівень сигналу першої гармоніки навіть нижчий ніж третьої приблизно на 10 децибел. Отже, на даному етапі фільтр не гасить третю гармоніку.

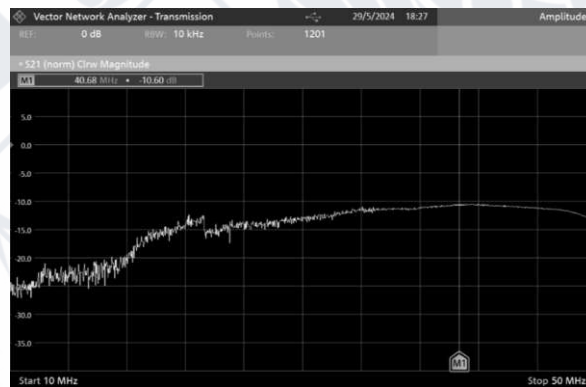


Рисунок 3.7 – Результат вимірювання передаточної функції для 3 гармоніки для ретранслятора із заземленням.

3.5. Створення та тестування шунтувального контуру

Для ефективнішого блокування сигналу частоти третьої гармоніки створено резонансний контур, що буде налаштований на 3 гармоніку та шунтуватиме частоту 3 гармоніки від нашого ретранслятора. Для цього було створено нову котушку з трьох витків, такої ж товщини, що й для контурів передачі та прийому та з також ж відстанню між витками.

Виміряна індуктивність котушки становить 1,4 мкГн. Розраховано необхідну ємність для конденсатора, достатню для утворення разом з котушкою коливального контуру на резонансній частоті 3 гармоніки 40,68 МГц за формулою (3.4):

$$C_4 = \frac{1}{4 \cdot \pi^2 \cdot 40,68 \text{ МГц}^2 \cdot 1,4 \text{ мкГн}} = 10.93 \text{ пФ} \quad (3.9)$$

Розрахунок показав, що необхідне значення ємності дорівнює 10.93 пФ. Далі було створено коливальний контур паралельно з'єднавши котушку та конденсатор та налаштовано його на частоту третьої гармоніки за допомогою векторного аналізатора. Як видно на рисунку 3.8, рівень налаштування на частоту 40,68 МГц досить задовільний.

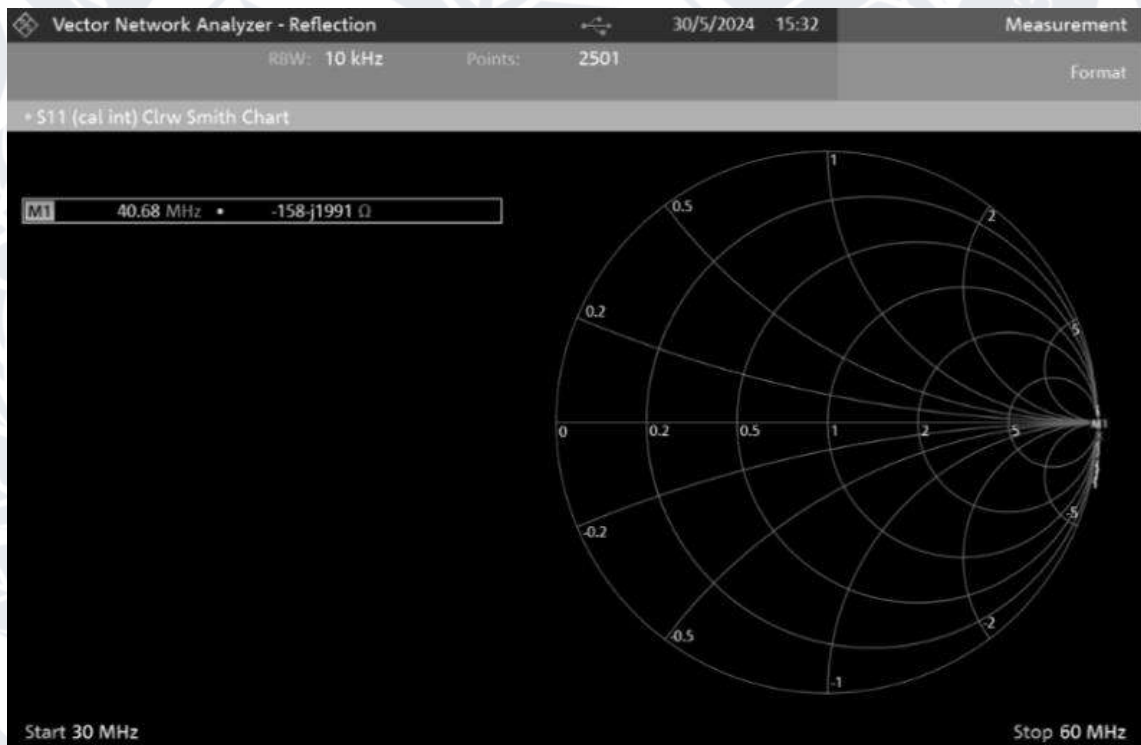


Рисунок 3.8 – Результат налаштування шунтувального контуру на частоту 3 гармоніки на діаграмі Сміта

Додатково перевіряємо значення фази коефіцієнту відбиття для шунтувального контуру. Як видно на рисунку 3.9, фаза коефіцієнту відбиття має значення -3,5 градуса, що є незначним прийнятним відхиленням.

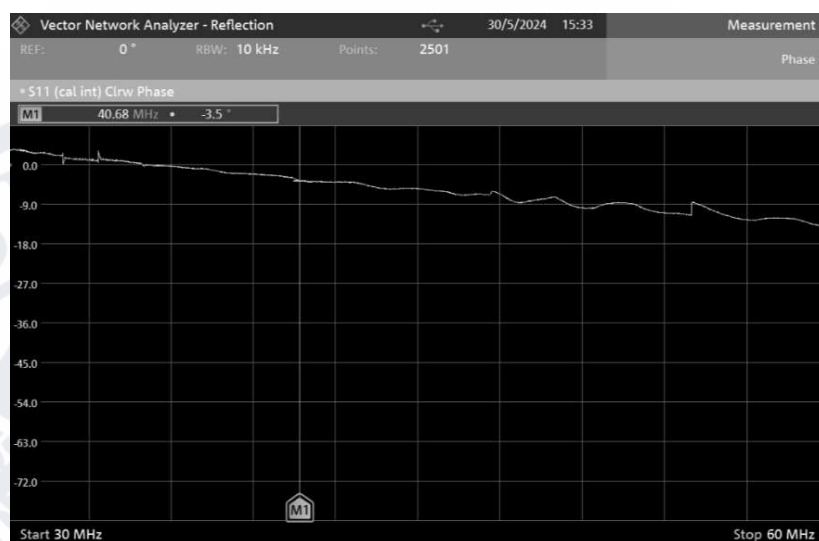


Рисунок 3.9 – Фаза коефіцієнту відбиття для шунтувального контуру, налаштованого на частоту 3 гармоніки

Даний контур виконує функцію шунтування - створює альтернативний шлях для струму в електричному колі, в нашому випадку цей контур налаштований саме на 3 гармоніку, тому має відводити сигнал на частоті третьої гармоніки на себе, не допускаючи його далі до ретранслятора.

Далі було встановлено шунтувальний контур впритул до заземленого ретранслятора з фільтром на 3 гармоніку (рис. 3.10)

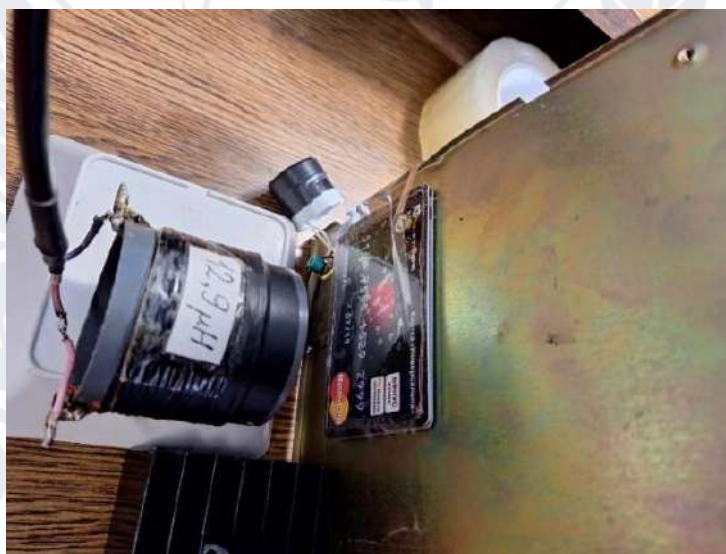


Рисунок 3.10 – Експериментальна установка з шунтувальним контуром, впритул зіставленим з заземленим ретранслятором

Векторний аналізатор був налаштований на вимірювання в моді S21 (передаточна функція). Вимірювання векторним аналізатором, як видно на рисунку 3.11, показало значення -6,27 dB для третьої гармоніки. Натомість для 1 гармоніки коефіцієнт передачі рівний -14,21 dB. Таким чином, різниця між коефіцієнтами передачі незначно зменшилася.

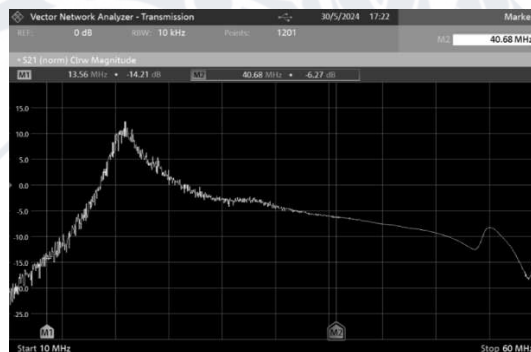


Рисунок 3.11 – Результат вимірювання коефіцієнту передачі для 1 та 3 гармонік для заземленого ретранслятора з приєднаним шунтувальним контуром

Для уточнення результатів було проведено аналогічне вимірювання коефіцієнту передачі для ретранслятора без заземлення, але з приєднаним шунтувальним контуром, результат видно на рисунку 3.12. Для 3 гармоніки - 8,71 dB, для 1 гармоніки -17,45 dB.



Рисунок 3.12 – Результат вимірювання передаточної функції для 1 та 3 гармоніки для ретранслятора без заземлення з приєднаним шунтувальним контуром

Також було проведене аналогічне вимірювання для ретранслятора без шунтувального контуру та без заземлення. Як видно на рисунку 3.13, для 3 гармоніки результат вимірювання становить -8,02 dB, а для 1 гармоніки -18,10 dB.



Рисунок 3.13 – Результат вимірювання передаточної функції для 1 та 3 гармоніки для ретранслятора без заземлення та без шунтувального контуру

Отже, на даний момент, суттєвих змін в різниці між коефіцієнтами передачі для 1 та 3 гармонік при вимірюванні передаточної функції немає.

3.6. Тестування ретранслятора на збільшеній відстані передачі

Було вирішено збільшити відстань між котушками передачі та прийому, щоб подивитися, наскільки зміниться коефіцієнт передачі для 3 гармоніки. Спочатку було проведено вимірювання для ретранслятора без шунтувального контуру, як зображено на рисунку 3.14.

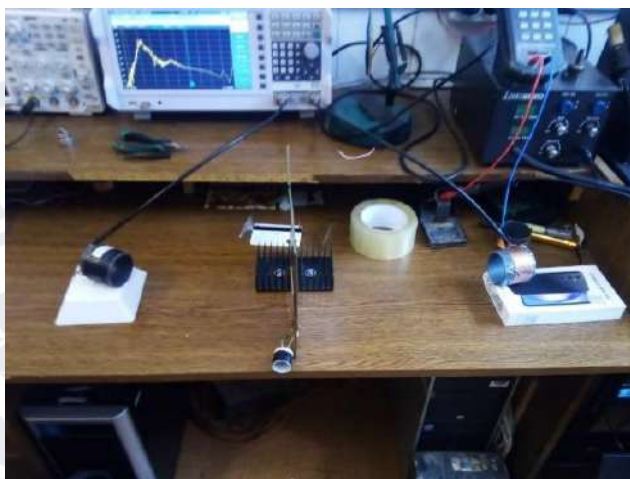


Рисунок 3.14 – Установка з ретранслятором без шунтувального контуру та збільшеною відстанню між котушками передачі та прийому

Як видно на рисунку 3.15, значення коефіцієнту передачі для 3 гармоніки становить -13,75 dB, а для 1 -22,84 dB.

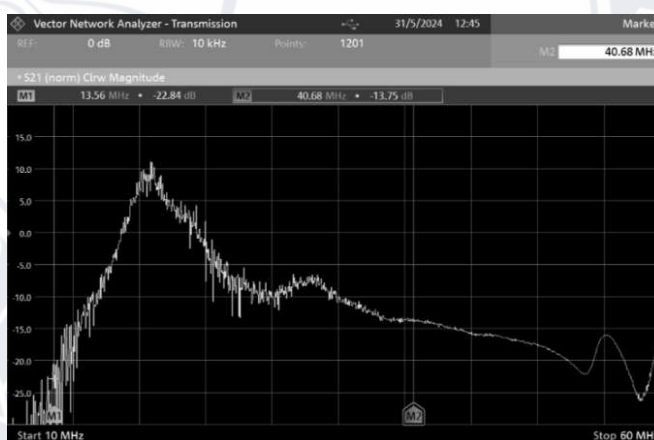


Рисунок 3.15 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором без шунтувального контуру та збільшеною відстанню між котушками прийому та передачі

Отже коефіцієнт передачі незначно знизився, при цьому різниця між зменшенням коефіцієнту між першою та третьою гармоніками лишається майже незмінною.

Наступним кроком проведено аналогічне вимірювання з під'єднаним шунтувальним контуром до ретранслятора, як показано на рисунку 3.16.



Рисунок 3.16 – Установка з ретранслятором з шунтувальним контуром та збільшеною відстанню між котушками передачі та прийому

На рисунку 3.17 видно, що коефіцієнт передачі трохи зменшився для 3 гармоніки, тепер він становить $-14,18$ dB, а для 1 гармоніки трохи збільшився, до $-21,29$ dB, однак різниця між коефіцієнтами передачі для 1 та 3 гармонік залишається майже такою самою.

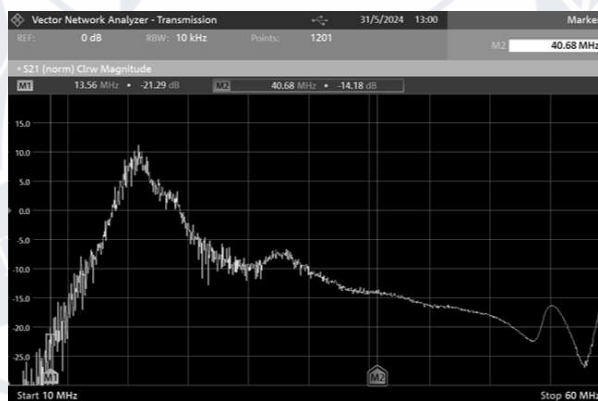


Рисунок 3.17 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором з шунтувальним контуром та збільшеною відстанню між котушками прийому та передачі

3.7. Тестування ретранслятора зі збільшеним екраном

Було прийнято рішення спробувати збільшити величину екрану, щоб дізнатися, чи вплине це на коефіцієнт передачі для 3 гармоніки. Також до шунтувального контуру було вирішено додати послідовно резистор, який створюватиме опір та таким чином забиратиме потужність сигналу 3 гармоніки.

Для покращення результатів вимірювання пік коефіцієнту передачі було підвищено, таким чином, щоб значення коефіцієнту для частоти 1 гармоніки було не нижче 0 dB, отже, щоб потужність сигналу в установці ретранслятора між котушкою передачі та котушкою прийому передавалася повністю, або й навіть посилювалася. Для цього було перекалібровано котушки передачі та прийому, збільшивши відстань між ними під час калібрування. Для збільшення швидкості розрахунку аналізатором значення коефіцієнту зменшено кількість точок до 101. Вимірювання проводилося на установці без шунтувального контуру та зі збільшеним екраном, як показано на рисунку 3.18.

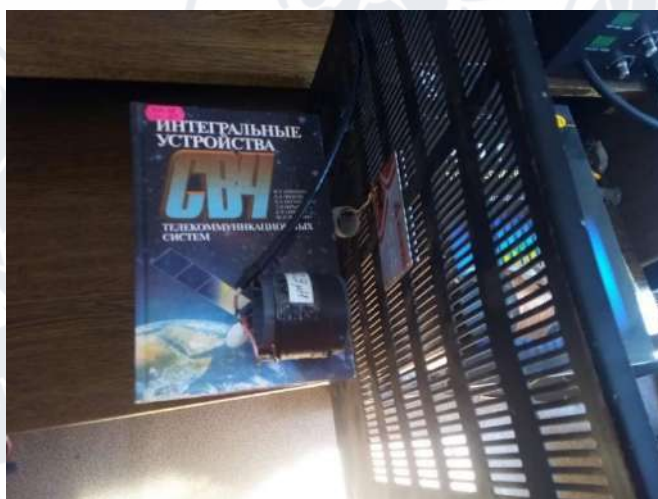


Рисунок 3.18 – Установка з ретранслятором без шунтувального контуру та зі збільшеним екраном

В результаті вимірювання для установки без шунтувального контуру було виявлено, що після перекалібрування коефіцієнт передачі 1 гармоніки збільшився, та перевищив коефіцієнт передачі для 3 гармоніки. На рисунку 3.19 видно, що коефіцієнт передачі для 1 гармоніки становить 7,97 dB, тоді як для 3 гармоніки -3,32 dB.



Рисунок 3.19 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором без шунтувального контуру та зі збільшеним екраном

Отже, після перекалібрування без шунтувального контуру зі збільшеним екраном у ретрансляторі коефіцієнт передачі для 1 гармоніки більший приблизно на 11 dB.

Після щільного розміщення до ретранслятора шунтувального контуру з послідовно розміщеним резистором номіналом 1 Ом, як показано на рисунку 3.20, було проведено повторне вимірювання коефіцієнту передачі.

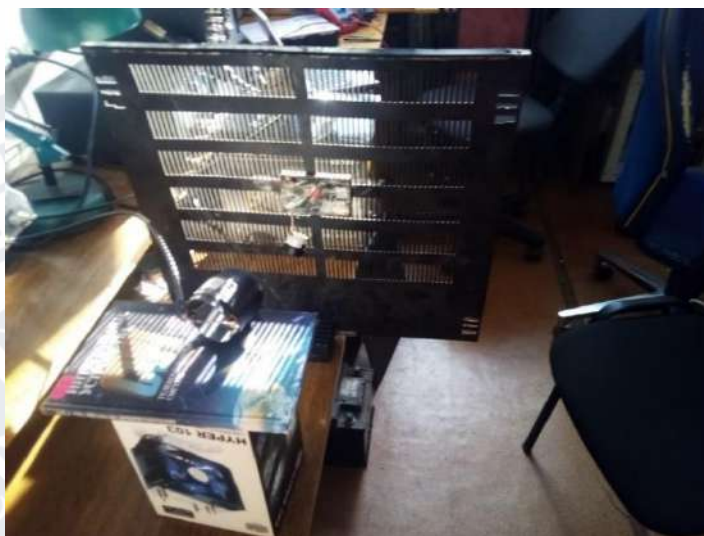


Рисунок 3.20 – Установка з ретранслятором з шунтувальним контуром, до якого послідовно приєднано резистор та зі збільшеним екраном

На рисунку 3.21 видно, що коефіцієнт передачі для 3 гармоніки -3,79 dB, отже майже не змінився.



Рисунок 3.21 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором з шунтувальним контуром, до якого приєднано резистор на 1 Ом та зі збільшеним екраном

Після заміни на шунтувальному контурі резистора на номінал 10 Ом та незначної зміни відстані було проведено повторне вимірювання, як видно на рисунку 3.22, коефіцієнт передачі для 3 гармоніки становить -5,54 dB, отже зменшився приблизно на 2 dB в порівнянні з попереднім вимірюванням.



Рисунок 3.22 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором з шунтувальним контуром, до якого приєднано резистор на 10 Ом та зі збільшеним екраном

Останнє вимірювання було проведене після приєднання до шунтувального контуру резистора номіналом 100 Ом. На рисунку 3.23 видно, що коефіцієнт передачі для 3 гармоніки становить -5,59 dB, отже зменшився зовсім незначно в порівнянні з приєднаним опором у 10 Ом.



Рисунок 3.23 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором з шунтувальним контуром, до якого приєднано резистор на 100 Ом та зі збільшеним екраном

Отже, додавання до шунтувального контуру опору не впливає суттєво на зміну коефіцієнту передачі потужності сигналу на частоті 3 гармоніки.

Після значного збільшення відстані між котушками передачі та прийому, як це вказано на рисунку 3.24, було проведено вимірювання з тим же резистором на 100 Ом в шунтувальному контурі.



Рисунок 3.24 - Установка зі значно збільшеною відстанню між котушками прийому та передачі

Як видно на рисунку 3.25, коефіцієнт передачі для частоти 3 гармоніки становить -7,52 dB та в порівнянні з попереднім вимірюванням на меншій відстані знизився всього лише приблизно на 2 dB. Отже, значна зміна відстані не вплинула суттєво на пониження коефіцієнту передачі для частоти 3 гармоніки.



Рисунок 3.25 – Результат вимірювання коефіцієнту передачі для установки з ретранслятором з шунтувальним контуром, до якого приєднано резистор на 100 Ом та зі збільшеним екраном при значно збільшеній відстані між котушками передачі та прийому

3.8. Дослідження потужності передачі сигналу елементами ретраслятора

Спочатку було виміряно максимальну відстань між допомогою рідером та NFC картою, на якій вони встановлюють зв'язок. Максимальна відстань становить 52 мм.

Далі було налаштовано спектроаналізатор на вимірювання потужності сигналу для 1 та 3 третьої гармонік. Опорна частота потужності сигналу налаштована на рівень -30 dBm. Фільтр смуги пропускання налаштований на 10 kHz, відеофільтр на 1 kHz. Діапазон частот встановлено від 10 до 50 МГц. Час сканування 10 секунд. Вбудований посилювач потужності відключений. Послаблення сигналу 0 dB. До спектроаналізатора було під'єднано котушку прийому, між котушкою прийому та рідером було встановлено картку. Після чого було виміряно потужність сигналу. На рисунку 3.26 видно, що потужність сигналу для 1 гармоніки становить -24,51 dBm, а для 3 -62,95 dBm.

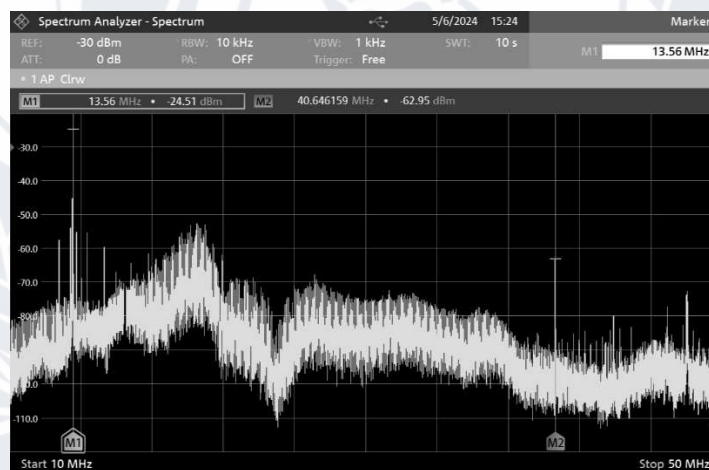


Рисунок 3.26 – Рівень потужності сигналу між картою та рідером для 1 та 3 гармонік

Далі було проведено вимірювання з розміщеним шунтувальним контуром між рідером та картою. Замість пониження потужності сигналу спостерігалось незначне покращення на 3 гармоніці. Було вирішено прибрати резистор та

проведено вимірювання без нього. На рисунку 3.27 видно, що що потужність сигналу для 1 гармоніки становить -24,52 dBm, а для 3 -62,20 dBm.

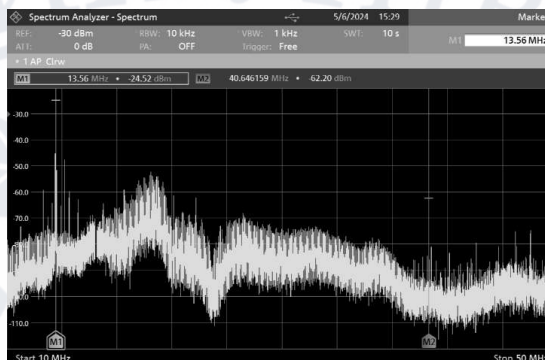


Рисунок 3.27 – Рівень потужності сигналу між картою та рідером для 1 та 3 гармонік з шунтувальним контуром без резистора

Отже, без резистора шунтувальний контур також не понижує рівень потужності обох сигналів та також трохи підвищує рівень сигналу для 3 гармоніки.

Наступним кроком між рідером та котушкою прийому було встановлено контур налаштований на частоту 1 гармоніки. Після чого зв'язок між картою та рідером перервався, при цьому, як видно на рисунку 3.28 рівень потужності сигналу для 1 гармоніки рівень сигналу становить -42.69 dBm , а для 3 -75.02 dBm.

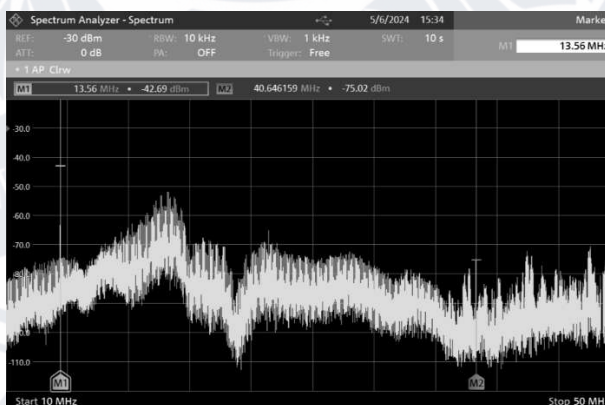


Рисунок 3.28 – Рівень потужності сигналу між картою та рідером для 1 та 3 гармонік з контуром, налаштованим на частоту 1 гармоніки.

Отже, контур налаштований на частоту 1 гармоніки понижує потужність сигналу для обох гармонік, при цьому рівень пониження потужності сигналу для 3 гармоніки нижчий, ніж для 1.

3.9. Дослідження потужності передачі сигналу ретранслятором

Було вирішено виміряти рівень потужності сигналу з ретранслятором, встановленим між котушкою передачі з одного боку та рідером з картою з іншого боку. Як видно на рисунку 3.29, рівень потужності сигналу для 1 гармоніки становить -49,10 dBm та -86,66 DBm для третьої гармоніки.



Рисунок 3.29 – Вимірювання потужності сигналу для установки з ретранслятором між котушкою передачі з одного боку та рідером з картою з іншого

Далі було проведено вимірювання з ретранслятором, встановленим між котушкою передачі та картою з одного боку та рідером з іншого боку. Як видно на рисунку 3.30, рівень потужності сигналу для 1 гармоніки становить -49,40 dBm та -82,30 DBm для третьої гармоніки. Отже, ретранслятор значно знижує потужність сигналу для 1 та 3 гармоніки приблизно однаково.



Рисунок 3.30 - Вимірювання потужності сигналу для установки з ретранслятором між котушкою передачі та карткою з одного боку та рідером з іншого

Також було проведено вимірювання для ретранслятора без екрану, встановленого між котушкою передачі та карткою з одного боку та рідером з іншого боку. Як видно на рисунку 3.31, рівень потужності сигналу для 1 гармоніки становить -36,18 dBm та -78,49 DBm для третьої гармоніки.

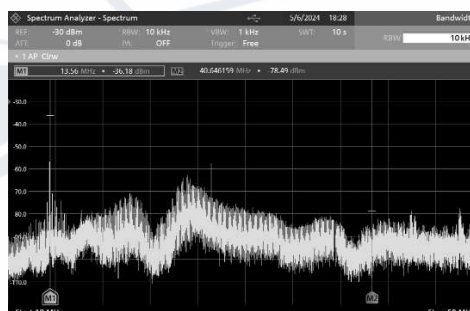


Рисунок 3.31 - Вимірюваний рівень потужності сигналу для ретранслятора без екрану

3.10. Висновки до розділу 3

Було розроблено та протестовано установку ретранслятора для придушення сигналу на частоті третьої гармоніки. Виявилось, що ретранслятор потребує вдосконалення. Шунтувальний контур незначно впливає на передаточну характеристику системи, в одному випадку спостерігалось навпаки посилення сигналу. Збільшення екрану ефективніше придушує сигнал третьої гармоніки, ніж основної частоти.

ВИСНОВКИ

Актуальність створення захисту від несанкціонованого доступу до сеансу зв'язку NFC залишається високою. Більшість досліджень даної технології переважно зосереджені на прикладному застосуванні в широкому переліку життєвих сфер. Роботи, що пов'язані з безпекою NFC, більше орієнтовані на створення сторонніх протоколів та програмного забезпечення з застосуванням криптографічних алгоритмів. Тому можна сказати, що дана робота зробила невеликий внесок в дослідження фізичних аспектів безпеки цієї технології.

На основі аналізу робіт, пов'язаних з покращенням передачі сигналу через посилювач зв'язку було спроектовано пристрій, що за своїми теоретичними характеристиками має ефективно блокувати випромінювання сигналу третьої гармоніки.

Під час тестування дослідного зразка ретранслятора було з'ясовано, що екран допомагає ефективно загасити сигнал вищої гармоніки. Збільшення екрану дещо посилило цей ефект, однак збільшення може бути непрактичним в умовах буденного життя, оскільки такий ретранслятор має бути максимально компактним. Шунтувальний контур, налаштований на частоту третьої гармоніки попри очікування майже не зменшував рівень коефіцієнту передачі та силу потужності сигналу. Було з'ясовано, що ретранслятор ефективно придушує сигнал третьої гармоніки, зберігаючи при цьому потужність сигналу основної гармоніки вищою. Проведені експерименти відкрили можливості для появи нових напрямків досліджень покращення ефективності придушення третьої гармоніки.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Попович, М. С. Застосування NFC технологій в бухгалтерському обліку [Текст] / М. С. Попович // Науковий вісник Ужгородського університету : Серія: Економіка / редкол.: В.П. Мікловда (гол. ред.), В.І. Ярема , Н.Н. Пойда-Носик та інші. – Ужгород: Вид-во УжНУ «Говерла», 2017. – Вип. 1(49). Том 1. – С. 351–355. – Бібліогр.: с. 354 (10 назв). – Рез. англ., рос.
2. NFC Forum Unveils NFC's Technology Roadmap Through 2028 URL: <https://nfc-forum.org/news/2023-06-nfc-forum-unveils-nfc-s-technology-roadmap-through-2028/> (дата звернення: 02.06.2024).
3. Coskun, V.; Ok, K.; Ozdenizci, B. Near Field Communication (NFC): From Theory to Practice, 1st ed.; John Wiley and Sons: London, UK, 2012. [Google Scholar].
4. Beginning NFC: Near Field Communication with Arduino, Android, and PhoneGap - Tom Igoe, D. Coleman, B. Jepson, Published 14 January 2014
5. Finkenzeller, K.; Müller, D. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication; Wiley: New York, NY, USA, 2010; ISBN 0470695064.
6. Paret, D. Design Constraints for NFC Devices; John Wiley & Sons Inc.: Hoboken, NJ, USA, 2016; ISBN 9781848218840.
7. Lazaro, A.; Villarino, R.; Girbau, D. A Survey of NFC Sensors Based on Energy Harvesting for IoT Applications. Sensors 2018, 18, 3746. URL: <https://doi.org/10.3390/s18113746>
8. M. Mareli, S. Rimer, B. S. Paul, K. Ouahada and A. Pitsillides, "Experimental evaluation of NFC reliability between an RFID tag and a smartphone," 2013 Africon, Pointe aux Piments, Mauritius, 2013, pp. 1-5, doi: 10.1109/AFRCON.2013.6757740.

9. NFCforum. 2013. URL: <https://nfc-forum.org/resources/what-arethe-operating-modes-of-nfc-devices/> (дата звернення: 02.03.2024).
10. Vedat Coskun, Busra Ozdenizci, and Kerem Ok. "A survey on near field communication (NFC) technology". In: Wireless personal communications 71.3 (2013), pp. 2259–2294.
11. Kevin Curran, Amanda Millar, and Conor Mc Garvey. "Near field communication". In: International Journal of Electrical and Computer Engineering 2.3 (2012), p. 371.
12. Kuka, Colin Sokol (2021) An innovative Memristor-based Wireless Power Transfer for NFC Security. PhD thesis, University of York.
13. SERIALIO.COM. The NFC Forum Standard. 1996. URL: <https://www.serialio.com/support/learn-rfid/what-near-field-communication-nfc#:~:text=The%5C%20NFC%5C%20device%5C%20in%5C%20Reader,magnetic%5C%20field%5C%20from%5C%20the%5C%20reader> (дата звернення: 28.04.2024).
14. Intro to NFC Payment Relay Attacks. URL: <https://salmg.net/2018/12/01/intro-to-nfc-payment-relay-attacks/> (дата звернення: 16.05.2024).
15. S. Akter, T. Chakraborty, T. A. Khan, S. Chellappan and A. B. M. Alim Al Islam, "Can You Get into the Middle of Near Field Communication?," 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017, pp. 365-373, doi: 10.1109/LCN.2017.39.
16. Haselsteiner, Ernst & Semiconductors, Philips. (2006). Security in Near Field Communication (NFC). Workshop on RFID Security.
17. Hancke, Gerhard & Kuhn, Markus. (2005). An RFID distance bounding protocol. 67-73. 10.1109/SECURECOMM.2005.56.

18. Чернов Д.В., Крыжановський В.Г. Усилитель класса Е в составе трансивера системы ближнеполевой коммуникации // Технічна електродинаміка. Тем. вип. Силова електроніка та енергоефективність. 2011. Ч. 1. С. 293-298
19. Finkenzeller K. RFID handbook: fundamentals and applications in contactless smart cards and Identification. ; 2nd ed. John Wiley & Sons Ltd, 2003. 427 p.
20. В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський. Підслуховування NFC-зв'язку на частотах вищих гармонік // Радиотехника. Межвед. науч.-техн. сб. 2021. Вып. 204. С. С. 99-104
21. Hancke G. P. Practical eaves dropping and skimming attacks on high-frequency RFID tokens // J. Comput. Security. Mar. 14, 2011. Vol. 19, no. 2, pp. 259–288
22. Володимир Крижановський, Юлія Рассохіна, Василь Комаров, Михайло Прокоф'єв. Захист NFC зв'язку від підслуховування на частотах вищих гармонік, "INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY". Proceedings of the IX-th International Scientific and Technical Conference May 25 – 26, 2023. С. 137, 138.
23. H. Saghlatoon, R. Mirzavand, M. M. Honari and P. Mousavi, "Investigation on Passive Booster for Improving Magnetic Coupling of Metal Mounted Proximity Range HF RFIDs," in IEEE Transactions on Microwave Theory and Techniques, vol. 65, no. 9, pp. 3401-3408, Sept. 2017, doi: 10.1109/TMTT.2017.2676095.
24. Gortschacher, L. J., Amtmann, F., Muehlmann, U., Merlin, E., Priller, P., & Grosinger, J. (2020). Passive HF RFID Repeater for Communicating with Tags in Metal Housings. IEEE Antennas and Wireless Propagation Letters, 1–1. doi:10.1109/lawp.2020.3012202