УДК 621.398.39
DOI: 10.31673/2409-7292.2019.042733

М.М. Луценко, Г.В. Шуклін, В.М. Ахрамович

ТЕХНОЛОГІЯ ВЗАЄМОДІЇ В БЛИЖНЬОМУ ПОЛІ NFC

Near Field Communication (NFC) - одна з найновіших технологій бездротового зв'язку. Як технологія бездротового підключення короткого діапазону, NFC пропонує безпечний, але простий та інтуїтивний зв’язок між електронними пристроями. Користувачі пристроїв, що підтримують NFC, можуть просто вказувати або торкатися своїх пристроїв до інших елементів з підтримкою NFC в середовищі, щоб спілкуватися з ними, що робить додаток та використання даних легкими та зручними. За допомогою технології NFC зв’язок відбувається, коли пристрій, сумісний з NFC, розміщений у кількох сантиметрах від іншого пристрою NFC або тегу NFC. Великою перевагою короткого діапазону передачі є те, що він гальмує підслуховування транзакцій, що підтримуються NFC. Технологія NFC відкриває нові захоплюючі сценарії використання мобільних пристроїв.

Ключові слова: Взаємозвязок ближнього поля (NFC), RFID технології, амплитудна модуляція, Манчестерский код, фазова модуляція.

Near Field Communication (NFC) - це технологія безконтактної комунікації на короткому відстані. На основі радіочастотної ідентифікації (RFID) він використовує індукцію магнітного поля для забезпечення зв'язку між електронними пристроями. Кількість короткочасних застосувань для технології NFC постійно зростає, з’являється у всіх сферах життя. Особливо використання спільно з мобільними телефонами пропонує великі можливості.

Мета даної роботи полягає в ознайомленні з технологією бездротового зв'язку, взаємозвязок в ближньому полі (NFC), та дослідження її основних характеристик.

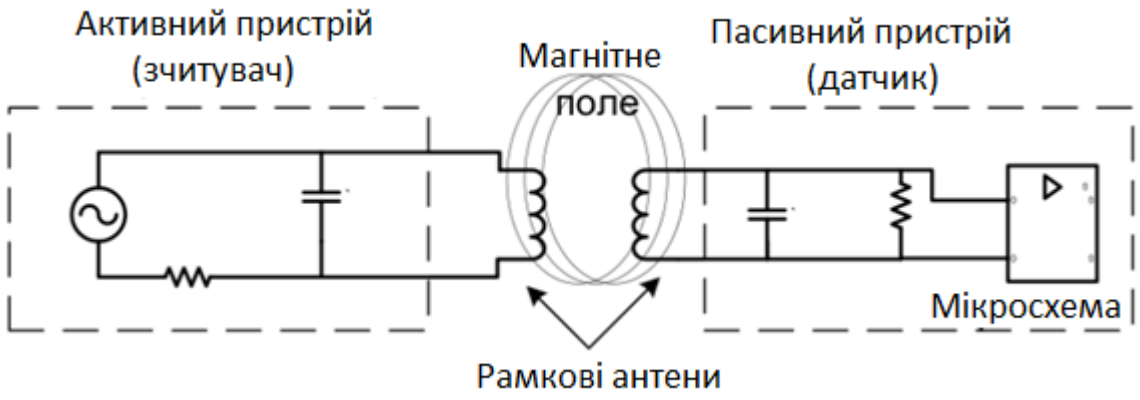

Рис.1. Конфігурація пристрою опитування (ініціатора) та прослуховуючого пристрою.

Однією з головних цілей технології NFC було надання переваг короткого безконтактного зв’язку доступним для споживачів у всьому світі. Наявна технологічна база радіочастот (РЧ) до цих пір була обумовлена різними потребами бізнесу, такими як логістика та відстеження предметів. Незважаючи на те, що технологія, що стоїть за NFC, є в існуючих додатках, особливо помітно змінився фокус у тому, як використовується технологія та що вона пропонує споживачам.

За допомогою лише точки або дотику, NFC дозволяє без зусиль використовувати пристрої та гаджети, якими ми користуємося щодня. Ось кілька прикладів того, що користувач може робити з мобільним телефоном NFC у середовищі з підтримкою NFC:

- Завантажте музику чи відео з смарт-плаката.
- Обмінюватися візитними картками з іншим телефоном.
- Сплачуйте вартість проїзду на автобусі чи поїзді.
- Роздрукуйте зображення на принтері.

• Використовуйте термінал торгового пункту для оплати покупки так само, як і за стандартною безконтактною кредитною карткою.

• З'єднайте два пристрої Bluetooth.

Телефон з підтримкою NFC функціонує як стандартні безконтактні смарт-карти, які використовуються у всьому світі в кредитних картках та в квитках для систем громадського транспорту. Після того, як заявка, наприклад, кредитна картка, надійно розмістилася на телефоні з підтримкою NFC, клієнт може оплатити, просто помахавши телефоном на зчитувальному пункті. Телефон NFC також пропонує підвищену безпеку, що дозволяє користувачеві захищати захищені програми через функції користувальницького інтерфейсу телефону.

Використання елементального дипольного поля

Визначаючи межу ближнього поля / дальнього поля, ми використовуємо суворо алгебраїчний підхід. Нам потрібні рівняння, які описують два важливі поняття: поля від елементарної, тобто малої електричної дипольної антени та від елементарної антени з магнітною петлею. С.К. Щелкунов отримав ці рівняння, використовуючи рівняння Максвелла. Ми можемо представляти ідеальну електричну дипольну антену коротким рівномірним струмовим елементом певної довжини,

1. Поля від електричного диполя:

$$E_0 = \frac{Il\beta^3}{4\pi\omega\varepsilon_0}\left[\frac{j*1}{\beta r} + \frac{1}{(\beta r)^2} + \frac{-j}{(\beta r)^3}\right]\sin(\theta)e^{-j\beta r} \quad \text{V/m} \quad (1)$$

$$H_\phi = \frac{Il\beta^2}{4\pi}\left[\frac{-1}{j\beta r} + \frac{1}{(\beta r)^2}\right]\sin(\theta)e^{-j\beta r} \quad \text{A/m} \quad (2)$$

$$Er = \frac{Il\beta^3}{4\pi\omega\varepsilon_0}\left[\frac{j}{\beta r} + \frac{1}{(\beta r)^2} + \frac{-j}{(\beta r)^3}\right]\cos(\theta)e^{-j\beta r} \quad \text{V/m} \quad (3)$$

2. Поля для магнітного дипольного контуру є:

$$E_\phi = -j\frac{\omega\mu_0 m\beta^2}{4\pi}\left[\frac{-1}{j\beta r} + \frac{1}{(\beta r)^2}\right]\cos(\theta)e^{-j\beta r} \quad \text{V/m} \quad (4)$$

$$H_r = 2j\frac{\omega\mu_0 m\beta^2}{4\pi\mathrm{p}_0}\left[\frac{-1}{j\beta r} + \frac{1}{(\beta r)^2}\right]\cos(\theta)e^{-j\beta r} \quad \text{A/m} \quad (5)$$

$$H_\theta = j\frac{\omega\mu_0 m\beta^2}{4\pi\mathrm{p}_0}\left[\frac{j}{\beta r} + \frac{1}{(\beta r)^2} + \frac{-j}{(\beta r)^3}\right]\sin(\theta)e^{-j\beta r} \quad \text{A/m} \quad (6)$$

де I - струм проводу в амперах; l - довжина дроту в метрах; b - електрична довжина на метр довжини хвилі, або v / c, 2 * п / л; v - кутова частота в радіанах за секунду, або 2 * p * f; e0 - проникність вільного простору, або 1/36 * p * 1029 F / м; m0 - проникність вільного простору, або 4 * p * 10-7 H / m; u - кут між осі дроту зеніту та точкою спостереження; f - частота в герцах; c - швидкість світла, або 3 * 108 м / сек; r - відстань від джерела до точки спостереження в метрах; і h0 - імпеданс вільного простору, або 376,7 В.

Рівняння з 1 по 6 містять доданки в 1 / r, 1 / r2 та 1 / r3. У ближньому полі в рівняннях переважають доданки 1 / r3. Зі збільшенням відстані умови1 / r3 та 1 / r2 швидко зменшуються, і, як наслідок, термін 1 / r домінує в дальньому полі. Щоб визначити межу між полями, вивчіть точку, в якій останні два доданки рівний.

Це момент, коли ефект другого доданка слабшає і останній член починає домінувати над рівняннями. Встановивши величину доданків у рівнянні 2, рівну один одному, разом з використанням деякої алгебри, отримаємо r, межа, за якою ми шукаємо:

$$\left[\frac{1}{\beta r} + \frac{1}{(\beta r)^2}\right]$$

і

$$r = \frac{\lambda}{2\pi}$$

Зауважимо, що рівняння визначають межу в довжинах хвиль, маючи на увазі, що межа рухається в просторі з частотою випромінювання антени. Судячи з наявної літератури, відстань, на якій рівні 1 / r та 1 / r2 рівні, є найбільш часто цитованою межею близько-поля / дальнього поля.

Основні характеристики

1. Як і ISO 14443, NFC зв'язується за допомогою індукції магнітного поля, де дві петлеві антени розміщені в межах ближнього поля один одного, ефективно утворюючи трансформатор з сердечником повітря. Він працює в межах глобально доступного та неліцензованого радіочастотного діапазону ISM 13,56 МГц, пропускна здатність майже 2 МГц.

2. Робоча відстань з компактними стандартними антенами: до 20 см.

• Підтримувані швидкості передачі даних: 106, 212 або 424 кбіт / с.

3. Є два режими:

• Режим пасивного зв'язку: Пристрій ініціатора забезпечує поле носія, а цільовий пристрій відповідає, модулюючи існуюче поле. У цьому режимі цільовий пристрій може черпати свою робочу потужність від Електромагнітного поля, забезпечене ініціатором, таким чином перетворює цільовий пристрій в транспондер.

• Режим активної комунікації: і ініціатор, і цільовий пристрій спілкуються, по черзі генеруючи власне поле. Пристрій деактивує своє радіочастотне поле під час очікування даних. У цьому режимі обидва пристрої, як правило, повинні мати джерело живлення.

Таблиця 1.

Режим зв'язку та швидкість передачі даних.

Бод	**Активний пристрій**	**Пасивний пристрій**
424 кБд	Манчестер, 10% Амплітудна модуляція	Манчестер, 10% Амплітудна модуляція
212 кБд	Манчестер, 10% Амплітудна модуляція	Манчестер, 10% Амплітудна модуляція
106 кБд	Модифікований код Miller, 100% Амплітудна модуляція	Манчестер, 10% Амплітудна модуляція

4. NFC використовує два різних кодування для передачі даних. Якщо активний пристрій передає дані зі швидкістю 106 кбіт / с, використовується модифіковане кодування Міллера зі 100% модуляцією. У всіх інших випадках використовується кодування Манчестера з коефіцієнтом модуляції 10%.

Пристрої NFC можуть одночасно приймати та передавати дані. Таким чином, вони можуть перевірити радіочастотне поле і виявити зіткнення, якщо прийнятий сигнал не збігається з переданим сигналом

Технологічний огляд

NFC працює у стандартній, загальнодоступній смузі частот 13,56 МГц. Можливі підтримувані швидкості передачі даних - 106, 212 та 424 кбіт / с, і є потенціал для

підвищення швидкості передачі даних. Ця технологія була розроблена для зв'язку на відстані 20 см, але зазвичай вона використовується в межах менше 10 см. Цей короткий діапазон не є недоліком, оскільки він посилює підслуховування.

Режими комунікації: активні та пасивні - Інтерфейс NFC може працювати в двох різних режимах: активному та пасивному. Активний пристрій генерує власне радіочастотне поле (РЧ), тоді як пристрій у пасивному режимі повинен використовувати індуктивну зв'язок для передачі даних. Для пристроїв, що живлять акумулятор, як мобільних телефонів, краще діяти в пасивному режимі. На відміну від активного режиму, внутрішнє джерело живлення не потрібно. У пасивному режимі пристрій може живитись радіочастотним полем активного пристрою NFC та передавати дані за допомогою модуляції навантаження. Отже, протокол дозволяє емуляцію картки, наприклад, використовується для використання квитків, навіть коли мобільний телефон вимкнено. Це дає два можливих випадки, які описані в табл. Випадок зв'язку між двома активними пристроями називається режимом активного зв'язку, тоді як зв'язок між активним та пасивним пристроєм називається режимом пасивного зв'язку.

Таблиця 2.

Різний режим зв'язку.

Режим зв'язку	Опис
Активний	Два активних пристрої взаємодіють один з одним. Кожен пристрій генерувати власне радіочастотне поле та пересилає дані.
Пасивний	спілкування відбувається між активний і пасивний пристрій. Пасивний пристрій немає блоку живлення і використовує радіочастотне поле, що генерується активний пристрій.

Загалом, щонайменше два пристрої спілкуються між собою одночасно. Однак в пасивному режимі ініціатор може спілкуватися з декількома цілями. Це реалізується методом часового інтервалу, який використовується для виявлення єдиного пристрою виявлення (SDD). Максимальна кількість часових інтервалів обмежена 16. Ціль відповідає у випадково вибраному часовому інтервалі, що може призвести до зіткнення з відповіддю іншої цілі. Щоб зменшити зіткнення, ціль може ігнорувати запит на опитування, встановлений ініціатором. Якщо ініціатор не отримає відповіді, він повинен знову надіслати запит на опитування.

Кодування та модуляція

Відмінність активних та пасивних пристроїв визначає спосіб передачі даних. Пасивні пристрої кодують дані завжди в Манчестерському кодуванні та 10% амплітудно. модуляцією. Натомість для активних пристроїв розрізняють модифіковане кодування Міллера зі 100% модуляцією, якщо дані

швидкість 106 кбіт/с, а манчестерське кодування з використанням коефіцієнта модуляції 10%, якщо швидкість передачі даних перевищує 106 кбіт/с. Коефіцієнт модуляції з використанням модифікованого кодування Міллера має велике значення для безпеки передачі даних NFC.

Манчестерське кодування залежить від двох можливих переходів у середині періоду. Перехід від низького до високого виражає 0 біт, тоді як перехід від високого до низького означає 1 біт. Отже, в середині кожного бітового періоду завжди є перехід. Переходи на початку періоду не враховуються.

Модифікований код міллера це рядковий код,що характеризується паузами, які виникають у носія в різних положеннях періоду. Залежно від інформації, що передається, біти кодуються, як показано на малюнку. Хоча 1 завжди кодується однаково, кодування 0 визначається на основі попереднього біта.

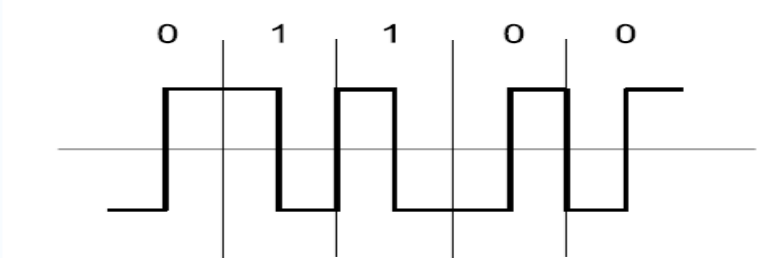

Рис. 2. Манчестерське кодування

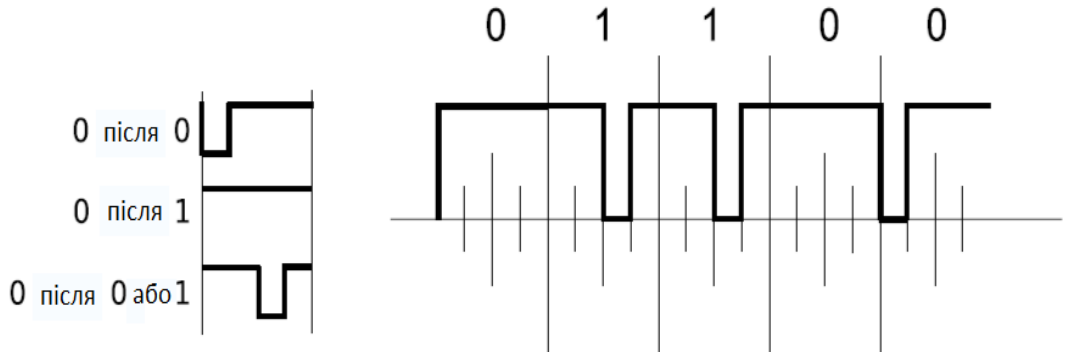

Рис. 3. Модифікований код Міллера

Ініціатор та об'єкт

Крім того, важливо дотримуватися розподілу ролі ініціатора та цілі. Ініціатор - це той, хто бажає спілкуватися і розпочинає спілкування. Ціль отримує запит на ініціатор зв'язку та надсилає відповідь. Ця концепція заважає цілі надсилати будь-які дані без попереднього отримання повідомлення. Щодо пасивного У режимі зв'язку пасивний пристрій завжди виступає як ціль NFC. Тут активним пристроєм є ініціатор, відповідальний за генерацію радіополя. У разі активної конфігурації, в якій поперемінно генерується радіочастотне поле, ролі ініціатора та цілі строго призначаються тим, хто починає спілкування. За замовчуванням усі пристрої є цілями NFC, і вони виконують роль пристрою ініціатора NFC лише тоді, коли цього вимагає програма. У випадку двох пасивних пристроїв зв’язок неможливий.

Таблиця 2.

Можливі комбінації, активні / пасивні з ініціатором / об'єктом.

	Ініціатор	**об'єкт**
Активний	Можливо	Можливо
Пасивний	Неможливо	Можливо

Аспекти безпеки

Перш за все слід зазначити, що короткий діапазон зв'язку в кілька сантиметрів, хоча і потребує свідомої взаємодії з користувачем, насправді не забезпечує безпечне спілкування. Для аналізу аспектів безпеки NFC було опубліковано дві дуже цікаві роботи. У роботі Ернст Хазельштейнер та Клеменс Брейтфус обговорюють "деякі загрози та рішення для безпеки

NFC", а також стаття "Аспекти безпеки та перспективні програми систем RFID" дає корисну інформацію.

Існують різні можливості атакувати технологію зв'язку поблизу. З одного боку, різними використаними пристроями можна керувати фізично. Це може бути вилучення тегу з міченого елемента або загортання їх у металеву фольгу, щоб захистити радіочастотний сигнал. Ще один аспект - порушення конфіденційності. Якщо власна інформація зберігається на тезі, важливо запобігти несанкціонованому доступу до читання та запису. Теги лише для читання захищені від несанкціонованого доступу до запису. У випадку перезаписуваних тегів, ми маємо припустити, що зловмисники можуть мати мобільні зчитувачі та відповідне програмне забезпечення, яке дає можливість несанкціонованого доступу для читання та запису, якщо відстань до читача нормальна. У цьому ми хочемо зосередити увагу на атаках щодо зв'язку між двома пристроями.

Для виявлення помилок NFC використовує перевірку циклічної надмірності (CRC). Цей метод дозволяє пристроям перевіряти, чи отримані дані були пошкоджені. Далі ми розглянемо різні можливі типи атак на зв'язок NFC. Для більшості цих атак є контрзаходи, щоб уникнути або хоча б зменшити загрози.

Підслуховування

NFC не забезпечує захисту від підслуховування. РЧ-хвилі для бездротової передачі даних з антеною дозволяють зловмисникам забрати передані дані моніторингу. На практиці зловмисникові доведеться дотримуватися більшу відстань, щоб не помітити. Короткий діапазон між ініціатором та ціллю для успішного спілкування не є суттєвою проблемою, оскільки зловмисники не пов'язані однаковими межами передачі. Отже, максимальна відстань для нормальної послідовності зчитування може бути перевищена. На питання про те, наскільки близько розташований зловмисник для отримання корисного радіочастотного сигналу, важко відповісти. Це залежить від "великої" кількості параметрів, таких як:

• RF подано характеристику даного відправника (тобто геометрія антени,
захисний ефект корпусу, друкованої плати, навколишнього середовища)

• Характеристика антени нападника (тобто геометрія антени, можливість зміни положення у всіх 3 вимірах)

• Якість приймача нападника.

• Якість декодера RF сигналу зловмисника.

• Налаштування місця, де виконується атака (наприклад, бар'єри, як стіни або метал, рівень підлоги)

• живлення, що передається пристроєм NFC.

Крім того, на підслуховування надзвичайно впливає режим зв'язку. Це тому, що на основі активного або пасивного режиму передані дані кодуються та модулюються по-різному. Якщо дані передаються з більш сильною модуляцією, їх можна атакувати легше. Таким чином, пасивний пристрій, який не генерує власне радіочастотне поле, атакувати набагато важче, ніж активний пристрій. Коли пристрій надсилає дані в активному режимі, підслуховування може здійснюватися на відстані близько 10 м, тоді як, коли передавальний пристрій перебуває в пасивному режимі, ця відстань значно скорочується приблизно до 1 м. Однак ми припускаємо, що такі напади будуть відбуватися, оскільки необхідне обладнання доступне для всіх. Оснащена такою антеною злісна людина, здатна пасивно контролювати радіочастотний сигнал, також може витягти звичайний текст. Для отримання необхідних знань можна використовувати експериментальні та літературні дослідження. Отже, конфіденційність NFC не гарантується. Для програм, які передають конфіденційні дані, єдиним рішенням є захищений канал.

Знищення даних

Зловмисник, який прагне знищення даних, має намір пошкодити зв'язок. Ефект полягає в тому, що послуга більше не доступна. І все-таки зловмисник не в змозі генерувати дійсне повідомлення. Замість підслуховування це не пасивна атака. Цей напад реалізувати порівняно легко. Однією з можливих порушень сигналу є використання так званого RFID

заслінки. Не можна запобігти такому нападу, але його можна виявити. Пристрої NFC можуть одночасно приймати та передавати дані. Це означає, що вони можуть перевірити радіочастотне поле і помітять зіткнення.

Модифікація даних

Несанкціонована зміна даних, що призводить до дійсних повідомлень, набагато складніше і вимагає глибокого розуміння. Як ми зазначимо далі, зміна даних можлива лише за певних умов. Для зміни переданих даних зловмисник повинен стосуватися одинарних бітів радіочастотного сигналу. Дані можна надсилати різними способами. Можливість цієї атаки, тобто, якщо можливо змінити біт значення 0 на 1 або навпаки, залежить від сили амплітудної модуляції. Якщо використовується 100% модуляція, можна усунути паузу радіочастотного сигналу, але не генерувати паузу там, де не було паузи. Це вимагатиме нездійсненного точного перекриття сигналу зловмисників оригінальним сигналом на антені приймача.

Однак технологія Near Field Communication використовує модуляцію на 100% у поєднанні з модифікованим кодуванням Міллера, що призводить до 4 можливих випадків. Єдиний випадок, коли біт може бути змінений зловмисником, коли 1 дотримується іншого. Заповнюючи паузу в двох половинах біт радіочастотного сигналу, декодер приймає сигнал третього випадку. Завдяки згоди попереднього біта декодер перевірив би дійсний. Інші три випадки не піддаються такому нападу.

Висновки

У цьому огляді було обговорено систему NFC. Увага була зосереджена на технології NFC, яка принесе нову перспективу у всіх аспектах нашого життя. З їх прогресуванням NFC в основному націлений на програми, що стосуються конфіденційності, зручності використання та безпеки. Отже, розробка захищеної системи та стратегій дизайну інтерфейсу користувача збільшує ефективність і зручність для використання в інших типах систем. Зокрема, це відкриває нові сценарії прикладного вдосконалення багатьох систем повязаних с безконтактними системами.

Перелік посилань

1. Клаус Фінкензеллер, “RFID Handbuch ”, Hanser, 2012.
2. Стандартний інтерфейс та протокол зв'язку поблизу поля ECMA-340 (NFCIP-1)
3. ISO / IEC 14443-2 Ідентифікаційні картки - Безконтактні карти інтегральної мікросхеми - Карти близькості - Частина 2: Інтерфейс радіочастоти та сигналу.
4. Специфікація протоколу безконтактного зв'язку EMV – 2019.
5. Aziza, H. Технологія NFC в послугах мобільного телефону наступного покоління. У матеріалах другий міжнародний семінар з питань комунікації поблизу, Монако, 20 квітня 2010 р .; С. 21–26.
6. Безпека та конфіденційність у галузі обчислювальної техніки та комунікацій, Пекін, Китай, 24–26 вересня 2014 року; С. 448–456.
7. Беньо, Б.; Вілмос, А.; Ковач, К .; Кутор, Л. Програми NFC та бізнес-модель

Надійшла: 5.10.2019 Рецензент: д.т.н., доцент Кожухівський А.Д.